Syracuse University
Prelim Exam Solutions

Syracuse University Graduate Student Body

Last Updated: August 26, 2019

Contents

1 Acknowledgements and Usage

This solution set project was undertaken by Caleb McWhorter to eliminate the problems with former student preliminary solution binders, which could only be used by a single person at a time and could easily vanish or be otherwise damaged. However during the compilation and typesetting of these solutions, the Mathematics Department made changes to the exams rendering these solutions—while still useful—obsolete. The project was then abandoned. Hence, some solutions will have no given solution or may be incomplete.

Though the format of these exams are not the current exam style in the department, they are still a wealth of information and are still very useful when used correctly. When using these solutions, always attempt the problem first before looking at any solution. The absolute worst way to prepare for the preliminary exams would be to read through these solutions like a book. The onus is on you, as a Ph.D. student, to use these responsibly.

While the solutions were typeset by Caleb McWhorter, the solutions were contributed by many individuals. Solutions may contain errors, either from the sourced solution, the typesetting, or both. However, the solutions come as is. You have been warned. We thank Caleb McWhorter for his typesetting as well as the students who contributed to the solutions (the order being alphabetical):

- Jennifer Edmond
- Rachel Gettinger
- Caleb McWhorter
- Carl Ragsdale

2 Algebra Prelims

August 1992

1. Let $T : V \to W$ be a linear transformation of finite dimensional vector spaces. Assume that $\operatorname{rank} T = k$. Prove that there exists ordered bases B for V, and C for W, such that the matrix representation of T with respect to B and C has the following property: its (i,i)-entry equals 1 for $i = 1, 2, \ldots, k$, and all its other entries are zero.

Solution: Choose a basis $\{k_1, \ldots, k_r\}$ for $\ker T$. Extend this basis to a basis for V: $\mathcal{B} = \{k_1, \ldots, k_r, v_1, \ldots, v_k\}$. We claim $\{T(v_1), \ldots, T(v_k)\}$ is linearly independent: suppose $r_1 T(v_1) + \cdots + r_k T(v_k) = 0$, where $r_i \in k$, the underlying field. Then $0 = T(r_1 v_1 + \cdots + r_k v_k)$. Hence, $r_1 v_1 + \cdots + r_k v_k \in \ker T$. But then $\sum_{i=1}^{k} r_i v_i = \sum_{j=1}^{r} r'_j k_j$, where $r'_j \in k$. But this implies

$$0 = \sum_{j=1}^{r} r'_j k_j - \sum_{i=1}^{k} r_i v_i = r'_1 k_1 + \cdots + r'_r k_r + (-r_1) v_1 + \cdots + (-r_k) v_k.$$

Since $\mathcal{B} = \{k_1, \ldots, k_r, v_1, \ldots, v_k\}$ is a basis for V, we must have $0 = r'_1 = \cdots = r'_r = r_1 = \cdots = r_k$. Hence, $\{T(v_1), \ldots, T(v_k)\}$ is linearly independent. Therefore, $\{T(v_1), \ldots, T(v_k)\}$ can be extended to a basis for W: $\mathcal{C} = \{T(v_1), \ldots, T(v_k), w_1, \ldots, w_m\}$. With respect to this basis, we have

$$[T]_{\mathcal{B}}^{\mathcal{C}} = \left(\begin{array}{ccc|ccc} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ \hline & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{array}\right),$$

where all missing entries are 0. □

2. Suppose $V = W_1 \oplus W_2$ and that f_1 and f_2 are inner products on W_1 and W_2, respectively. Show that there is a unique inner product f on V such that

(a) $W_2 = W_1^{\perp}$;

(b) $f(\alpha, \beta) = f_k(\alpha, \beta)$, when α, β are in W_k, $k = 1, 2$.

3. Let V be an n-dimensional vector space and let T be a linear operator on V. Suppose that there exists a positive integer k such that $T^k = 0$. Prove that $T^n = 0$. What is the characteristic polynomial for T?

4. Suppose $B = \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & 2 \end{pmatrix}$. Find: (a) the characteristic polynomial and the eigenvalues of B; and (b) a maximal set S of linearly independent eigenvectors of B. (c) Is B diagonalizable?

5. If A is a square matrix with characteristic polynomial $f(x) = (x-2)^3(x+3)^4$ and minimal polynomial $g(x) = (x-2)(x+3)^2$, give all possible Jordan normal forms for A.

6. Let $T : V \to W$ be a linear transformation with $\dim V = n$, $\dim W = m$, and $\operatorname{rank} T = k$. Let $T^* : W^* \to V^*$ be the dual linear transformation. What are the rank and nullity of T^*?

August 1993

1. Let A be a real symmetric matrix satisfying $A^k = I$ for some positive integer k, where I is the identity matrix of the same size as A. Prove $A^2 = I$.

Solution: Every real symmetric matrix is diagonalizable. Therefore, there exists a (real orthogonal) matrix Q so that $Q^{-1}AQ = D$, where D is a diagonal matrix. [Note that $Q^{-1} = Q^T$.] Now we have $A = QDQ^{-1}$ so that

$$I = A^k = (QDQ^{-1})^k = QD^kQ^{-1}$$

Since D is real and diagonal, it must be that every diagonal entry is either 1 or -1. But then $D^2 = I$. But then $A^2 = (QDQ^{-1})^2 = QD^2Q^{-1} = QIQ^{-1} = I$, as desired. □

2. Let v be a nonzero vector of the Euclidean space $\mathbb{R}^n$. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be the linear operator given by the formula $T(x) = x - 2(x, v)v$ for all $x \in \mathbb{R}^n$, where $(\ ,\ )$ is the standard inner product. Prove that T can be represented by the matrix

$$\begin{pmatrix} I & 0 \\ 0 & -1 \end{pmatrix}$$

where I is the $(n-1) \times (n-1)$ identity matrix.

3. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator represented by the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

with respect to the standard basis. Show there exist nonzero T-invariant subspace U and V of $\mathbb{R}^3$ satisfying $\mathbb{R}^3 = U \oplus V$.

4. Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation of rank k. Show there exist linear transformations $U : \mathbb{R}^n \to \mathbb{R}^k$ and $V : \mathbb{R}^k \to \mathbb{R}^m$, where U is onto and V is one-to-one, satisfying $T = VU$.

5. Denote by $\mathrm{Mat}_n(\mathbb{R})$ the set of all real $n \times n$ matrices. A matrix $N \in \mathrm{Mat}_n(\mathbb{R})$ is called nilpotent if $N^k = 0$ for some positive integer k.

(a) Do all nilpotent matrices form a subspace of $\mathrm{Mat}_n(\mathbb{R})$?

(b) Prove $I + N$ is invertible, where $I \in \mathrm{Mat}_n(\mathbb{R})$ is the identity matrix.

(c) Show $I + N$ is diagonalizable if and only if $N = 0$.

6. Let $A = (a_{ij})$ be the $n \times n$ real matrix satisfying $a_{ij} = 1$ for all $i, j = 1, \ldots, n$. Denote by the same letter A the linear operator $\mathbb{R}^n \to \mathbb{R}^n$ whose representation matrix with respect to the standard basis is A.

(a) Describe $\ker A$ and $\operatorname{im} A$ as subsets of $\mathbb{R}^n$.

(b) What is the minimal polynomial of A?

(c) Show A is diagonalizable.

August 1995

1. Suppose A is a matrix over the complex numbers with characteristic polynomial $(x+2)^2(x-1)^5$. If the rank of $(A-I)^2$ is 3 and the rank of $(A+2I)$ is 5, where I denotes the identity matrix, what are the possibilities for the Jordan canonical form of A?

2. Suppose that E is an idempotent linear operator on a vector space, that is $E^2 = E$. Show that the only possible characteristic values for E are 0 and 1.

Solution: Let v be an eigenvector for E with associated eigenvalue λ. Then we have

$$\lambda v = Ev = E^2 v = E(Ev) = E(\lambda v) = \lambda(Ev) = \lambda^2 v$$

But then $(\lambda^2 - \lambda)v = 0$. Since v is an eigenvector, $v \neq 0$ so that $0 = \lambda^2 - \lambda = \lambda(\lambda - 1)$. But then $\lambda = 0$ or $\lambda = 1$. □

3. Suppose V is a vector space with a finite spanning set $S = \{v_1, \ldots, v_n\}$. Show that S contains a basis for V.

Solution: For notation purposes, let $S = \{a_1, \ldots, a_n\}$. If V is the trivial vector space, then it has an empty basis. If $V \neq \{0\}$, then $S \neq \{0\}$. Choose a vector $v_1 \in S$. If $S_1 := \text{Span}\{v_1\} = V$, then S_1 is a basis for V. Otherwise, choose $v_2 \in S \setminus S_1$. Define $S_2 := \text{Span}\{v_1, v_2\}$. If $S_2 = V$, then we are done. Otherwise, form S_3 as before and continue. Since S is finite of cardinality n, this process can continue at most n times since S spans V. Note that S_i is linearly independent by construction for $i = 1, 2, \ldots, n$. If the process terminates at S_i, then S_i is a basis for V. □

4. Assume V is a finite dimensional vector space of dimension n and let T and S be linear operators on V, both with rank strictly greater than $\frac{n}{2}$. Show that the composition $S_0 T$ is nonzero.

5.

(a) Suppose $T : V \to W$ is a linear transformation between the vector spaces V and W. What is meant by T^t, the transpose of T?

(b) Assume $S : \mathbb{R}^2 \to \mathbb{R}^2$ is given by $S(x, y) = (x + y, 2x - y)$. Let $\{f_1, f_2\}$ be the dual basis of the standard basis $\{e_1, e_2\}$ for $\mathbb{R}^2$, where $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Find $S^t(f_2)$.

6.

(a) Let V be an inner product space with inner product $(\ ,\ )$, and assume $T : V \to V$ is a linear operator on V. What does it mean to say that T is self adjoint? What does it mean to say that T is normal?

(b) Let P_2 be the inner product space of polynomials of degree at most two over the real numbers with inner product $(f, g) = \int_{-1}^{1} fg$. If ϕ is a linear functional defined on P_2 by $\phi(f) = f(0)$, find $h \in P_2$ with $\phi(f) = (f, h)$.

August 1997

1. Let A be a square matrix with characteristic polynomial $c(x) = x(x-3)^2(x+5)^4$ and minimal polynomial $m(x) = x(x-3)(x+5)^2$. Give all possible Jordan normal forms for A and for each possible form, indicate the algebraic and geometric multiplicities of the eigenvalue -5.

2. Give an example of linear operators ϕ and ψ on $\mathbb{R}^4$ satisfying the following conditions. Justify the answers.

(a) $\phi \neq 0$ is neither one-to-one nor onto and $\phi^2 = \phi$.

(b) $(\psi^2 + 1)^2 = 0$ and ψ is not a root of a polynomial of degree ≤ 3 with real coefficients, where 1 is the identity operator on $\mathbb{R}^4$.

3. In $\mathbb{R}^4$, let $U = \text{Span}\{(1,0,1,0), (0,1,0,-1), (0,1,1,0)\}$ and $V = \text{Span}\{(1,0,0,0), (0,0,1,0), (0,1,1,1)\}$. Find a basis for $U \cap V$.

4. Let $\phi : U \to V$ be a linear transformation of finite-dimensional vector spaces U, V over a field F, and let $\hat{\phi} : \hat{V} \to \hat{U}$ be the dual linear transformation. Prove that ϕ is one-to-one if and only if $\hat{\phi}$ is onto.

5. Prove that the eigenvalues of a real symmetric matrix are real.

Solution: Let v be an eigenvector of A associated with eigenvalue λ. Then $Av = \lambda v$. If M is a matrix, M^* denote the conjugate transpose and $\overline{M}$ denote the conjugate of M. Since A is symmetric, $A = A^T$. Furthermore since A is a real matrix, $A^* = A$. We compute v^*Av two different ways:

$$v^*Av = v^*(Av) = v^*(\lambda v) = \lambda(\overline{v} \cdot v)$$
$$v^*Av = (A\overline{v})^T v = (\overline{\lambda}\overline{v})^T v = \overline{\lambda}(\overline{v} \cdot v).$$

Since $v \neq 0$, $\overline{v} \cdot v \neq 0$. But then $\lambda = \overline{\lambda}$. Thus, $\lambda \in \mathbb{R}$. □

6. Let $A = (a_{ij})$ be an $n \times n$ real matrix, where $a_{ii} = 2$ for $i = 1, \ldots, n$, $a_{i,i+1} = a_{i+1,i} = 1$ for $i = 1, \ldots, n-1$, and the remaining elements of A are zeros. Using the Sylvester criterion or another method, determine whether a real quadratic form q represented by the matrix A with respect to a certain basis is positive definite.

August 1998

1. Let V be a finite dimensional vector space. Prove that the dimension of V is even if and only if there is a linear map $f : V \to V$ such that $\ker f = \operatorname{im} f$.

2. Let V be a finite dimensional complex vector space and let $\phi : V \to V$ be a linear map.

(a) Assume that for each natural number k, $\operatorname{trace}(\phi^k) = 0$. Prove that 0 is an eigenvalue of ϕ.

(b) Prove that ϕ is nilpotent if and only if for each natural number k, $\operatorname{trace}(\phi^k) = 0$.

3. Find two matrices having the same rank and the same characteristic polynomial, but not similar to each other.

4. Let A and B be two self-adjoint matrices. Show that AB is self-adjoint if and only if $AB = BA$.

Solution: By abuse of notation, let A and B represent the linear operator given by the matrices A, B on the vector space V, respectively. Recall a linear operator T is self-adjoint (hermitian) if and only if $\langle Tv, w \rangle = \langle v, Tw \rangle$ for all $v, w \in V$. Now A, B are self adjoint so that $\langle Av, w \rangle = \langle v, Aw \rangle$ and $\langle Bv, w \rangle = \langle v, Bw \rangle$ for all $v, w \in V$. Equivalently, $A^* = A$ and $B^* = B$, where $(-)^*$ denotes conjugate transpose. Now suppose that AB is self-adjoint so that $(AB)^* = AB$. But then $AB = (AB)^* = B^*A^* = BA$. Now suppose that $AB = BA$. Then

$$\langle (AB)v, w \rangle = \langle A(Bv), w \rangle = \langle Bv, Aw \rangle = \langle v, B(Aw) \rangle = \langle v, (BA)w \rangle = \langle v, (AB)w \rangle$$

so that AB is self-adjoint. □

5. Let V be an n-dimensional real vector space, and let q be a quadratic form on V. Let $A = (a_{ij})_{1 \le i,j \le n}$ be the symmetric matrix of q in an ordered basis. Show that if the form q is positive definite, then for each positive integer k, we have $\det A_k > 0$, where $A_k = (a_{ij})_{1 \le i,j \le k}$.

6.

(a) Show that every $n \times n$ matrix A can be uniquely written as the sum of a symmetric and a skew-symmetric matrix.

(b) Let A and B be two congruent $n \times n$ matrices. Show that A^T and B^T are also congruent.

(c) Again, let A and B be two congruent $n \times n$ matrices, and write $A = A_1 + A_2$ and $B = B_1 + B_2$, where A_1 and B_1 are symmetric and A_2 and B_2 are skew-symmetric. Show that A_1 is congruent to B_1, and that A_2 is congruent to B_2.

August 1999

1. Let $\mathbf{P}_4$ be the vector space of real polynomials of degree ≤ 4 in the indeterminate x. For $a \in \mathbb{R}$, we put $\mathbf{P}_4(a) = \{f \in \mathbf{P}_4 \colon f(a) = 0\}$.

(a) Prove $\mathbf{P}_4(a)$ is a subspace of $\mathbf{P}_4$.

(b) Find a basis for and the dimension of $\mathbf{P}_4(a)$.

(c) Find a basis for and the dimension of $\mathbf{P}_4(-3) \cap \mathbf{P}_4(2)$.

2. For the indicated values of $c(x)$ and $m(x)$, determine whether there exists a square complex matrix A for which $c(x)$ is the characteristic polynomial and $m(x)$ is the minimal polynomial. If such an A exists, find all possible Jordan normal forms of A. Justify your answers.

(a) $c(x) = x(x+1)(x-2)^3$ and $m(x) = x(x-2)^2$.

(b) $c(x) = (x-4)^2(x+3)^3$ and $m(x) = (x-4)(x+3)^2$.

3. Let A be a 4×3 matrix of rank 3 over a field F.

(a) Is there a matrix B satisfying $BA = I_3$, where I_3 is the 3×3 identity matrix?

(b) Let $T_A : F^3 \to F^4$ be the linear transformation given by $T_A(x) = Ax$ for all $x \in F^3$. Is T_A one-to-one? Is it onto?

Justify your answers.

4. Let $\phi : U \to V$ be a linear transformation of finite dimensional vector spaces U, V over a field F, and let $\hat{\phi} : \hat{V} \to \hat{U}$ be the dual linear transformation. Prove that ϕ is onto if and only if $\hat{\phi}$ is one-to-one.

5. Let U and V be subspaces of the Euclidean space $\mathbb{R}^n$. If $\dim U < \dim V$, prove that there is a non-zero vector in V orthogonal to all vectors in U.

6. Give an example of a normal linear operator on a finite dimensional unitary space that is neither self-adjoint nor unitary. Justify your answer.

January 2002

1. Let A be a matrix and assume A^2 has characteristic polynomial $x^3(x-1)^2$ and minimal polynomial $x^2(x-1)$. What are the possible Jordan canonical forms of A?

2. Let $T : V \to W$ be a linear transformation between two vector spaces V and W. Show that T is injective if and only if $\ker T = \{v \in V : T(v) = 0\}$ only contains the vector 0.

Solution: Suppose T is injective. Let $v \in \ker T$. Then $T(v) = 0 = T(0)$ so that $v = 0$. Therefore, $\ker T = \{0\}$. Now suppose that $\ker T = \{0\}$. If $T(v) = T(v')$ for some $v, v' \in V$, then $T(v) = T(v')$ implies $0 = T(v) - T(v') = T(v - v')$ so that $v - v' \in \ker T$. Therefore, $v - v' = 0$ so that $v = v'$. But then T is injective. □

3. Let $T : V \to W$ be a linear transformation between two finite dimensional vector spaces V and W. Show that T is an isomorphism if and only if the dual map $T^* : W^* \to V^*$ is an isomorphism.

4. Let $T : V \to V$ be a linear operator on a vector spaces V and assume $v_1, \ldots, v_k$ are eigenvectors of T corresponding to the distinct eigenvalues $\alpha_1, \alpha_2, \ldots, \alpha_k$. Show that $v_1, v_2, \ldots, v_k$ are linearly independent.

5. Suppose A is an $n \times n$ matrix over the real numbers $\mathbb{R}$. Show that A is diagonalizable over R if and only if we can find a basis for $\mathbb{R}^n$ consisting of eigenvectors for A.

6.

(a) Assume T is a normal linear operator on a finite dimensional complex inner product vector space. Show that eigenvectors corresponding to distinct eigenvalues are orthogonal.

(b) Show by example that this need not be true if T is not normal.

August 2002

1. Prove or disprove the following: if A is a complex square matrix such that $A^n = A$ for some integer $n > 1$, then A is diagonalizable.

Solution: We prove something slightly more general: let k be an algebraically closed field of characteristic 0 and A is a matrix with entries in k, if $A^n = A$ then A is diagonalizable. Now the matrix A satisfies $A^n - A = 0$, i.e. satisfies the polynomial $p(x) = x^n - 1$. Since $\operatorname{char} k = 0$, the roots of $p(x)$ are simple. Since k is algebraically closed, we can write

$$p(x) = x^n - 1 = \prod_{i=1}^{n}(x - r_i),$$

where r_i are the roots of A (in fact, $r_i^n = 1$ for all i). Since the roots of $p(x)$ are distinct, the characteristic and minimal polynomial for $p(x)$ are identical. But then A is diagonalizable. [Recall that a linear operator $A : V \to V$ is diagonalizable if and only if its minimal polynomial in $F[T]$ splits in $F[T]$ and has distinct roots, where F is an algebraically closed field of characteristic zero.] Note that the result is false if the field is not algebraically closed of characteristic 0. For example, $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ satisfies $A^4 = I$ but is not diagonalizable over $\mathbb{R}$ as it has complex eigenvalues. Furthermore, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\overline{\mathbb{F}}_2)$ satisfies $A^2 - 1 = (A-1)^2$ so that $A^2 = I$ but is not diagonalizable. □

2. Let V be the vector space of all the real polynomials of degree less or equal to 3, and let $T : V \to V$ be the linear transformation given by $T(f) = -f + f' + f''$.

(a) Find the matrix M of T with respect to the basis $\{1, x, x^2, x^3\}$ of V.

(b) Find the minimal polynomial of T.

(c) Is the matrix M diagonalizable? Why, or why not?

(d) Find the Jordan canonical form of M.

3. Let A be a fixed 5×8 real matrix for which there exists an 8×5 real matrix B satisfying $AB = I$, where I is the identity matrix.

(a) Prove that B can be chosen in such a way that three of its rows consist entirely of zeros.

(b) What are the necessary and sufficient conditions on the matrix A for the uniqueness of the matrix B satisfying (a).

(c) Suppose that now B is a fixed 8×5 matrix, and A varies. State, but do not prove the analogue of (a).

4. Let V be the vector space of all the real polynomials of degree less or equal 3. For all $p(x) \in V$, put $\phi(p(x)) = \int_1^2 p(x)\, dx$.

(a) Prove that ϕ is a linear functional on V.

(b) Let $\{\phi_0, \phi_1, \phi_2, \phi_3\}$ in V^* be the dual basis of the basis $\{1, x, x^2, x^3\}$ of V. Express ϕ as a linear combination of the ϕ_i.

(c) Give the definition of the evaluation map $e : V \to V^{**}$.

(d) Find $e(1 + x + x^2 + x^3)(\phi)$ where ϕ is defined above.

(e) Show that e is a monomorphism. Is it an isomorphism? Why, or why not?

5.

(a) Show that the eigenvalues of a real symmetric matrix are real.

(b) Let A be a real matrix. Show that $A^T A$ is diagonalizable.

6. For $A = \begin{pmatrix} 5 & 2 & 2 \\ 2 & 2 & -4 \\ 2 & -4 & 2 \end{pmatrix}$, find a real orthogonal matrix P and a diagonal matrix D such that $A = PDP'$. Hint: 6 is one of the eigenvalues.

January 2003

1. A 5-by-5 matrix A has characteristic polynomial $(x-2)^3(x+1)^2$, while the matrix $(A-2I_5)^2$ has rank 2 and $A+I_5$ has rank 4. What are the possible Jordan canonical forms of A?

2. If A is a Hermitian complex matrix, show that its characteristic values must be real. [Recall that A is called Hermitian (or self-adjoint) if it satisfies the equal $A = \overline{A^T}$, where $\overline{A^T}$ is the complex conjugate of the transpose of A.]

3. Let V be a vector space with basis $B = \{v_1, \ldots, v_n\}$ and let $w \in V$ be nonzero. Show directly, without quoting the dimension theorem, that we can find i such that we can replace v_i in V by w and still have a basis for V.

4. Let V, $(\ ,\ )$ be a finite dimensional inner product space over the real numbers. If W is a subspace of V, prove that we can write V as a direct sum $V = W \oplus W^\perp$, where $W^\perp = \{v \in V : (v,w) = 0 \text{ for all } w \in W\}$.

5. Let V and W be finite dimensional vector spaces over a field k and let $T : V \to W$ be a linear transformation.

(a) Define the transpose map $T^* : W^* \to V^*$, where $W^* = \mathrm{Hom}_k(W,k)$ is the dual of W.

(b) Show that T^* is injective if and only if T is surjective.

Solution:

(a) Define $T^* : W^* \to V^*$ as follows: given $f \in \mathrm{Hom}_k(W,k)$, i.e. a k-linear map $f : W \to k$, define $T^*(f)$ by $f \mapsto f \circ T$. Since f and T are linear, so too is fT. Moreover, $T : V \to W$ and $f : W \to k$ so that $fT : V \to k$, i.e. $fT \in V^* = \mathrm{Hom}_k(V,k)$.

(b) Note that functions f, g on a set S satisfy $fg = 1$ if and only if f is surjective and g is injective. Now T^* is injective if and only if there exists a map $R^* : W^* \to V^*$ such that $1 = R^*T^* = (TR)^*$. But this occurs if and only if $TR = 1$. Of course, this occurs if and only if T is surjective. □

6. Let V and W be finite dimensional vector spaces over a field k and let $T : V \to W$ be a linear transformation. Let $S = \{v_1, v_2, \ldots, v_m\}$ be a subset of V. For each of the following statements either prove it or give a counterexample to it.

(a) If S is linearly independent set in V, then $\{T(v_1), T(v_2), \ldots, T(v_m)\}$ must be a linearly independent set in W.

(b) If $\{T(v_1), T(v_2), \ldots, T(v_m)\}$ is a linearly independent set in W, then S must be a linearly independent set in V.

August 2003

1. Let A be a $n \times n$ complex matrix and let k be a positive integer. Show that μ is an eigenvalue of A^k if and only if $\mu = \lambda^k$ for some eigenvalue λ of A.

2. Let V be a finite dimensional vector space. A linear map $\sigma : V \to V$ is said to be a reflection if $\sigma^2 = 1_V$. What are the possible eigenvalues of a reflection? Must every reflection be diagonalizable? Why, or why not?

3. Let V be a finite dimensional vector space and let $\sigma : V \to V$ be a linear map whose range is 1-dimensional. Prove that σ is either nilpotent or diagonalizable.

4. Prove that if a real quadratic form with matrix A is positive definite, then A is invertible and the quadratic form with matrix A^{-1} is also positive definite.

5. Let ϕ be a linear operator on the unitary space $\mathbb{C}^n$.

(a) Prove if $(\phi\mathbf{x}, \mathbf{x}) > 0$ for all nonzero $\mathbf{x} \in \mathbb{C}^n$, then al the eigenvalues of ϕ are positive.

(b) Give an example showing that the converse of (a) is false.

(c) Prove that if ϕ is self-adjoint, then the converse of (a) is true.

6. Find the Jordan canonical form of the following matrices. Justify your answers.

(a)

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ \gamma & 0 & \alpha \end{pmatrix}$$

where $\gamma \neq 0$.

(b)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & 4 & \cdots & n \end{pmatrix}$$

January 2004

1. Let A be a complex matrix with characteristic polynomial $(x-1)^4(x+2)^3$. Assume that the rank of $(A-I_7)^2$ is 5 and the rank of $(A+2I_7)$ is 4. What is the Jordan canonical form of A? Justify your answer.

2.

(a) Let A be an n-by-n matrix over a field F. Then $C(A) = \{X \in M_n(F) \colon XA = AX\}$ is called the centralizer of A in $M_n(F)$. Let $Y \in M_n(F)$ be an invertible matrix. Show that $C(YAY^{-1}) = Y[C(A)]Y^{-1}$. (Note: $Y[C(A)]Y^{-1} = \{YXY^{-1} \colon X \in C(A)\}$.)

(b) If F is the field of complex numbers and $n = 2$, what is the smallest dimension $C(A)$ can have?

3. For each of the following statements, either prove it or give an example to show that it is false.

(a) Assume $\phi : V \to W$ is a linear transformation between vector spaces. If $\{v_1, v_2, \ldots, v_n\}$ is a subset for V with $\{\phi(v_1), \phi(v_2), \ldots, \phi(v_n)\}$ linearly independent in W, then $\{v_1, v_2, \ldots, v_n\}$ is linearly independent in V.

(b) Assume V is a 5-dimensional vector space and W is a 3 dimensional vector space with $X : V \to W$ and $Y : V \to W$ surjective linear transformations. Then there exists $v \in V$, nonzero, such that $X(v) = Y(v) = 0$.

4. Show that an n-by-n matrix A over a field F is similar to a diagonal matrix if and only if there is a basis for $F^{(n)}$, the space of n-by-1 matrices over F, consisting of eigenvectors for A.

5. Let P_2 be the vector space of polynomials of degree at most 2 over the real numbers togethet with the inner product $\langle f, g\rangle = \int_0^2 fg\, dx$. Let $\phi : P_2 \to \mathbb{R}$ be the functional given by $\phi(f) = f(1)$. Find $g \in P_2$, such that $\phi(f) = \langle f, g\rangle$, for all $g \in P_2$.

6. Let V be a finite dimensional inner product space over the complex numbers and let W be a subspace with orthonormal basis $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$. If $\beta \in V$, show that $\gamma = \sum_i \langle \beta, \alpha_i\rangle\, \alpha_i$ is the unique element of W with $\|\beta - \gamma\| = \sqrt{\langle \beta - \gamma, \beta - \gamma\rangle}$.

August 2004

1. Find all possible Jordan normal forms of a complex square matrix A with characteristic polynomial $x(x+1)^3(x-3)^2$ if $A+I$ has rank 4.

2. Let f be a bilinear form on a finite-dimensional vector space V over a field k, and let B be the matrix of f with respect to some basis for V. For each $\alpha \in V$ define a function $\phi_\alpha : V \to k$ by $\phi_\alpha(\beta) = f(\alpha, \beta)$.

(a) Prove that ϕ_α is a functional on V.

(b) If $\hat{V}$ is the dual space of V, prove that the map $\sigma : V \to \hat{V}$ given by $\sigma(\alpha) = \phi_\alpha$ is a linear transformation.

(c) Find and prove the necessary and sufficient conditions on B in order for σ to be an isomorphism.

3. Let l_1, l_2, l_3 be three distinct straight lines passing through the origin of the Euclidean plane $\mathbb{R}^2$. Prove that if m_1, m_2, m_3 are three distinct lines through the origin, then there exist a linear automorphism ϕ of $\mathbb{R}^2$ satisfying $\phi(l_i) = m_i$, $i = 1, 2, 3$.

4. Let $\mathrm{GL}_n(F)$ denote the group of $n \times n$ nonsingular matrices over a field F.

(a) Prove that the map sending a complex number $a + bi$ to the 2×2 real matrix $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ is a homomorphism of the field of complex numbers into the ring of 2×2 real matrices.

(b) Find a subgroup of $\mathrm{GL}_2(\mathbb{R})$ isomorphic to the multiplicative group of nonzero complex numbers.

(c) Prove that for every n, $\mathrm{GL}_n(\mathbb{C})$ is isomorphic to a subgroup of $\mathrm{GL}_{2n}(\mathbb{R})$.

5. Give a complete list of nonisomorphic groups of order 245, and prove your answer.

6. Let $\mathbb{Z}[X]$ be the ring of polynomials in the variable X with integer coefficients. Determine whether the following statements are true or false. If a statement is true, give a proof; if it is false, provide a counterexample.

(a) $\mathbb{Z}[X]$ is an integral domain.

(b) $\mathbb{Z}[X]$ is a Principal Ideal Domain.

(c) $\mathbb{Z}[X]$ is a Unique Factorization Domain.

(d) Let $\mathbb{Z}^3$ be the set of triples of integers. Given a matrix $A = \begin{bmatrix} 0 & 0 & -2 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$, we turn $\mathbb{Z}^3$ into a $\mathbb{Z}[X]$-module by putting $p(X) \cdot \boldsymbol{v} = p(A)\boldsymbol{v}$ for all $p(X) \in \mathbb{Z}^3$ and $\boldsymbol{v} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$. Then $\mathbb{Z}^3$ is a torsion $\mathbb{Z}[X]$-module.

7. Let R be a Principal Ideal Domain with field of fractions K. If $M \subseteq K$ is a finitely generated R-submodule of K, show that M is generated by one element.
8. Let α be the real cube root of 2. Compute the irreducible polynomial for $1 + \alpha^2$ over $\mathbb{Q}$.
9. Let $K = F(\alpha)$ be a field extension generated by an element α, and let $\beta \in K$, $\beta \notin F$. Prove that α is algebraic over the field $F(\beta)$.
10. Let $K \supset L \supset F$ be fields of characteristic 0. Prove or disprove:

(a) IF K/F is Galois, then K/L is Galois.

(b) If K/F is Galois, then L/F is Galois.

(c) If L/F and K/L are Galois, then K/F is Galois.

January 2005

1. Consider the following set of vectors in R^3

$$S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 5 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 7 \\ 4 \end{bmatrix}, \begin{bmatrix} 5 \\ 9 \\ 5 \end{bmatrix} \right\}$$

Find a subset $T \subset S$ such that T is a basis for the span of S.

Solution: Let the vectors of S be x_1, x_2, x_3, x_4 in the order given. Note that $x_1 + x_2 = x_3$ and $2x_1 + x_2 = x_4$ so that we can eliminate x_3 and x_4 from S without changing the span. It is clear that x_1 and x_2 are independent. Then $\{x_1, x_2\}$ is a basis for S. □

2. Let T be the linear transformation from R^2 to R^2 defined by $T(x, y) = (x + y, x - y)$. Determine all ordered bases B for R^2 such that the matrix representing T with respect to B (the same B being used as the ordered basis for both the domain R^2 and the target R^2) equals

$$\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

To help make it clear that you really understand your description of all such B, do the following: State explicitly whether the number of such B is 0, 1, a finite number greater than 1, or infinite. If the number is 1, 2, or 3, list them explicitly. If the number is greater than 3, list at least 3 different answers explicitly. If your description of all such B is a good one doing those explicit things should be a triviality.

Solution: The matrix of T is $\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$ so that

$$T(b_1) = -1b_1 + 1b_2 = b_2 - b_1$$
$$T(b_2) = 1b_1 + 1b_2 = b_1 + b_2$$

So if $\{b_1, b_2\} = \left\{ \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right\}$ is a basis, then

$$(x_1 + y_1, x_1 - y_1) = (x_2 - x_1, y_2 - y_1)$$
$$(x_2 + y_2, x_2 - y_2) = (x_1 + x_2, y_1 + y_2)$$

This implies

$$x_1 = y_2 = \frac{x_2 - y_1}{2}.$$

Hence, the number of possible ordered bases is infinite. Now choosing $x_2 = y_1 = 1$, $x_2 = y_1 = -1$, and $x_2 = 2, y_1 = -4$, we have corresponding bases

$$B = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$
$$B = \left\{ \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix} \right\}$$
$$B = \left\{ \begin{pmatrix} 3 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}$$

□

3. A square matrix A has characteristic polynomial $(x-1)^6(x-2)^4$, nullity $(A-I) = 3$, nullity $(A-I)^2 = 5$, nullity $(A-2I) = 2$, and nullity $(A-2I)^2 = 4$. What is the Jordan normal form for A?

Solution: Observe nullity $(A-I) = 3$ so that there are 3 Jordan blocks for the eigenvalue $\lambda = 1$. As nullity $(A-I)^2-$ nullity $(A-I) = 5-3 = 2$, there are two of the three Jordan blocks for $\lambda = 1$ have size at least two. Furthermore, nullity $(A-2I) = 2$ so that there are 2 Jordan blocks for $\lambda = 2$. As nullity $(A-2I)^2-$ nullity $(A-2I) = 4-2 = 2$, there are two Jordan blocks of size at least two for $\lambda = 2$. Then the invariant factors are $(x-1)$, $(x-1)^2(x-2)^2$, and $(x-1)^3(x-2)^3$ and the Jordan form, up to permutation of blocks, is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

□

4. Let V be an inner product space with inner product $(\ ,\ )$ and u and v vectors in V. Prove that $u = v$ if and only if $(u, w) = (v, w)$ for all $w \in V$.

Solution: Assume that $u = v$, then $(u, w) = (v, w)$ for all $w \in V$. Now assume that $(u, w) = (v, w)$ for all $w \in V$. Take $w := u - v$. Then as $(u, w) = (v, w)$, we have

$(u-v, u-v) = 0$. As $(\cdot\,,\,\cdot)$ is positive definite, it must be that $u - v = 0$. Then $u = v$. □

5. For this one you do not have to show work. We are just testing to see if you remember a famous theorem. Fill in the blanks to complete the following famous theorem.

Theorem: If A is a given $m \times n$ matrix, then

(a) The null space of A is the orthogonal complement of (blank).

(b) The null space of A^T is the orthogonal complement of (blank).

Solution:

(a) The null space of A is the orthogonal complement of the row space of A.

(b) The null space of A^T is the orthogonal complement of the column space of A. □

6. Let g, h be elements of a group G. If $g^4h = hg^4$ and $g^7 = 1$, prove that $gh = hg$.

Solution: Since $g^7 = 1$, we have $g^8 = g$. Then we have

$$gh = g^8h = g^4g^4h = g^4hg^4 = hg^4g^4 = hg^8 = hg$$

so that $gh = hg$. □

7. If H is a subgroup of a group G, then G acts on the set G/H of left cosets of H in G by $g \cdot xH = gxH$. Describe the stabilizer of the coset aH explicitly as a subgroup of G.

Solution: We have

$$\begin{aligned}
\text{stab } aH &= \{g \in G \colon g \cdot aH = aH\} \\
&= \{g \in G \colon gaH = aH\} \\
&= \{g \in G \colon a^{-1}gaH = H\} \\
&= \{g \in G \colon a^{-1}ga \in H\} \\
&= \{g \in G \colon g \in aHa^{-1}\}
\end{aligned}$$

But $aHa^{-1} = \{g \in G \colon g \in aHa^{-1}\}$ is a subgroup of G: $1 \in H$ so that $a1a^{-1} = aa^{-1} = 1 \in aHa^{-1}$ (showing that the set is nonempty). Now if $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$, we have $ah_1a^{-1} \cdot ah_2a^{-1} = a(h_1h_2)a^{-1}$ and as $h_1, h_2 \in H$, $h_1h_2 \in H$. Therefore, $a(h_1h_2)a^{-1} \in aHa^{-1}$. Finally, if $aha^{-1} \in aHa^{-1}$, $(aha^{-1})^{-1} = (a^{-1})^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1}$ and as H is a subgroup, $h^{-1} \in H$ so that $ah^{-1}a^{-1} \in aHa^{-1}$. □

8.

(a) Prove that an integral domain with finitely many elements is a field.

(b) Is there an integral domain containing exactly 10 elements?

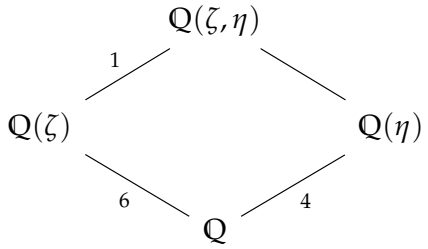
Solution:

(a) Let R be a finite integral domain and $0 \neq \alpha \in R$. Define $L_\alpha : R \to R$ via $x \mapsto \alpha x$. Now if $L_\alpha(x) = 0$, we have $\alpha x = 0$. Since R is an integral domain, it must be $\alpha = 0$ or $x = 0$. But $\alpha \neq 0$ so that $x = 0$. Then it must be that L_α is injective. But then L_α is an injective map between finite sets of the same cardinality. Therefore, L_α is surjective (hence a bijection). Then there exists $r \in R$ such that $1 = L_\alpha(r) = \alpha r$. But then α is a unit. As this holds for all $0 \neq \alpha \in R$, it must be that R is a field.

(b) Suppose R were a finite integral domain. By (a), R is a field. In particular, $\operatorname{char} R$ exists (this is defined even for an integral domain). Suppose $\operatorname{char} R = n < \infty$. If $n = pq$ for some integers $p, q \in \mathbb{Z}_{>1}<$ then $0 = n \cdot 1 = (pq) \cdot 1 = (p \cdot 1) \cdot (q \cdot 1)$. As R is an integral domain, $p \cdot 1 = 0$ or $q \cdot 1 = 0$. Since $p, q > 1$ divide n, we have $p, q < n$. But as $n = \operatorname{char} R$, it must be that $p \cdot 1, q \cdot 1 \neq 0$, a contradiction. Then the characteristic of a finite field must be prime. In particular, a finite field must have cardinality p^n for some n and fixed prime p. Now as a finite integral domain is a field and $10 = 2 \cdot 5$, it must be that there is no integral domain containing exactly 10 elements. □

9. For a prime p, the cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$. Use this fact to prove the following statement. If $\zeta = e^{2\pi i/7}$ and $\eta = e^{2\pi i/5}$ then $\eta \notin \mathbb{Q}(\zeta)$.

Solution: Suppose that $\eta \in \mathbb{Q}(\zeta)$. Then $\mathbb{Q}(\zeta, \eta) = \mathbb{Q}(\zeta)$ and consider $\mathbb{Q}(\zeta, \eta)$.



Now ζ is a root of $x^7 - 1 = (x-1)(x^6 + \cdots + 1)$. Now ζ is not a root of $x - 1$ so that ζ is a root of $x^6 + \cdots + 1$ and $x^6 + \cdots + 1$ is irreducible. Therefore, the minimal polynomial for ζ is $p_\zeta(x) = x^6 + \cdots + 1$ and $\deg p_\zeta(x) = 6$. Therefore, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. Similarly, the minimal polynomial of η is $p_\eta(x) = x^4 + \cdots + 1$ and $\deg p_\eta(x) = 4$. Therefore, $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$. By assumption, $[\mathbb{Q}(\zeta, \eta) : \mathbb{Q}(\eta)] = 1$ since $\mathbb{Q}(\zeta, \eta) = \mathbb{Q}(\zeta)$. But we have

$$\begin{aligned} [\mathbb{Q}(\zeta, \eta) : \mathbb{Q}] &= [\mathbb{Q}(\zeta, \eta) : \mathbb{Q}(\eta)]\,[\mathbb{Q}(\eta) : \mathbb{Q}] \\ 6 &= [\mathbb{Q}(\zeta, \eta) : \mathbb{Q}(\eta)] \cdot 4 \end{aligned}$$

But then $[\mathbb{Q}(\zeta, \eta) : \mathbb{Q}(\eta)] \notin \mathbb{Z}$, a contradiction. Therefore, $\eta \notin \mathbb{Q}(\zeta)$. □

10. Let K be a splitting field of an irreducible cubic polynomial $f(x)$ over a field F of characteristic 0 whose Galois group is S_3. If $\alpha \in K$ satisfies $f(\alpha) = 0$, determine the group of automorphisms $G(F(\alpha)/F)$ of the extension $F(\alpha)$.

Solution: Because K is the splitting field of f, we know that K/F is normal. Furthermore since K is the splitting field of f, K/F is algebraic. Since K/F is algebraic and $\operatorname{char} F = 0$, K/F is a separable extension. But as K/F is normal and separable, K/F is a Galois extension. But then $|\operatorname{Gal}(F(\alpha)/F)| = [F(\alpha) : F] = \deg p_\alpha(x) = 3$, where $p_\alpha(x)$ is the minimal polynomial of α (which must be f since $f(\alpha) = 0$ and f is irreducible). Therefore, $\operatorname{Gal}(F(\alpha)/F) \cong C_3$. □

August 2005

1.

(a) How many elements of order 6 are there in the symmetric group S_7?

(b) How many conjugacy classes in S_7 consist of elements of order 6?

Solution:

(a) Recall the order of an element of S_n is the least common multiple of the cycles in the cycle decomposition of the element. If $\sigma \in S_n$, the cycle decomposition of σ corresponds to a partition of n. Therefore, $\sigma \in S_7$ has order 6, the possible corresponding partition of 7 is among the following: $(6,1)$, $(3,2,2)$, $(3,2,1,1)$. [As a representative of each type, we could take $(1\ 2\ 3\ 4\ 5\ 6)$, $(1\ 2\ 3)(4\ 5)(6\ 7)$, and $(1\ 2\ 3)(4\ 5)$, respectively.]

For the first type, there are 7 ways to choose the elements of the 6-cycle and 6! ways to arrange the elements. Then there are $7 \cdot \frac{6!}{6}$ elements of the form $(1\ 2\ 3\ 4\ 5\ 6)$. [The division by 6 in $\frac{6!}{6}$ is the fact that any cyclic permutation of a cycle still represents the same cycle, .e.g. $(a\ b\ c) = (c\ a\ b) = (b\ c\ a)$ as 3-cycles.]

For the second type, there are $\binom{7}{3}$ ways to choose the elements to form the 3-cycle and $\frac{3!}{3}$ ways to uniquely determine the 3-cycle. Then there are 4 unused elements. If we form one of the 2-cycles, examining any remaining element, choosing where it is mapped (there are 3 choices) determines one of the two cycles. But with 2 elements remaining, it also determines the remaining 2-cycle. There are then $\binom{7}{3} \cdot \frac{3!}{3} \cdot 3$ elements of this form.

For the third type, there are again $\binom{7}{3}$ ways to choose the elements for the 3-cycle and $\frac{3!}{3}$ to uniquely determine the 3-cycle. There are then 4 unused elements so that there are $\binom{4}{2}$ ways to choose elements for the 2-cycle and the 2-cycle is uniquely determined by that choice. There are then $\binom{7}{3} \cdot \frac{3!}{3} \cdot \binom{4}{2}$ elements of this form.

Therefore, the number of elements of order 6 in S_7 is:

$$7 \cdot \frac{6!}{6} + \binom{7}{3} \cdot \frac{3!}{3} \cdot 3 + \binom{7}{3} \cdot \frac{3!}{3} \cdot \binom{4}{2} = 840 + 210 + 420 = 1470.$$

(b) In any group, conjugate elements have the same order (conjugation preserves order). Two elements of S_n are conjugate if and only if the elements have the same cycle decomposition, i.e. they have the same cycle type. The elements of order 6 in S_7 have cycle decompositions which can be represented by $(1\ 2\ 3\ 4\ 5\ 6)$, $(1\ 2\ 3)(4\ 5)(6\ 7)$, and $(1\ 2\ 3)(4\ 5)$, i.e. cycle decompositions corresponding to the following partitions of 7: $(6,1)$, $(3,2,2,\ )$, $(3,2,1,1)$, respectively. Therefore, there are three conjugacy classes consisting of elements of order 6.

□

2. Show that a group of order 48 cannot be simple.[1]

Solution: Let G be a group of order 48 and n_p denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_p \equiv 1 \mod p$ and $n_p \mid m$, where $|G| = p^r m$, where $(p, m) = 1$ and $r \in \mathbb{Z}$ is maximal (the largest power of p dividing $|G|$). Note $|G| = 48 = 2^4 \cdot 3$. By Sylow's Theorem, $n_2 \in \{1, 3\}$. If $n_2 = 1$, then G contains a unique (hence normal) Sylow 2-subgroup. But then G is not simple. Suppose then that $n_2 = 3$. Then the action of G on the set of Sylow 2-subgroups (the action being conjugation) induces a homomorphism of $\phi : G \to S_3$. If $\ker\phi$ were trivial, then G would be isomorphic to a subgroup of S_3. But $|G| = 48$ and $|S_3| = 6$ and $48 \nmid 6$. Therefore, $\ker\phi \neq \{1\}$. [Note that the action of G on the set of Sylow 2-subgroups is nontrivial so that $\ker\phi \neq G$.] But the kernel of a group homomorphism is always a normal subgroup so that G is then not simple. Therefore, no group of order 48 can be simple.

OR

The class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(a_i)]$$

where the $Z(G)$ is the center of G, $C_G(x)$ is the centralizer of x in G, and the summation is over $a_1, \ldots, a_r$ representatives for the distinct conjugacy classes of G. The center of a group is always normal. Then if $Z(G) \neq G$ and $|Z(G)| \neq 1$, then $Z(G) \leq G$ is a normal subgroup. If $|Z(G)| = |G|$, then G is abelian. By Cauchy's Theorem, G would then contain an element of order p for every prime $p \mid |G|$. But in an abelian group, every subgroup is normal so that then G would not be simple. Suppose then that $|Z(G)| = 1$. Then we have

$$\sum_{i=1}^{r} [G : C_G(a_i)] = |G| - |Z(G)| = 48 - 1 = 47.$$

Then there must be a conjugacy class of size 1 or 3. If $1 \neq x \in G$ has a conjugacy class of size 1, then $x \in Z(G)$ so that $Z(G)$ is nontrivial, a contradiction. If $x \in G$ has a conjugacy class of size 3, there is a homomorphism $\phi : G \to S_3$ given by the action of G on the set of conjugacy classes of $\langle x \rangle$ via conjugation. As $\operatorname{im}\phi \leq S_3$ and $|S_3| = 6$, using $\operatorname{im}\phi \cong G/\ker\phi$ (by the First Isomorphism Theorem), we must have $|\ker\phi| \geq 8$. Now if $\ker\phi = G$, then every element of G fixes the conjugacy classes of $\langle x \rangle$. But if $\{1\langle x\rangle 1^{-1}, g\langle x\rangle g^{-1}, h\rangle x\rangle h^{-1}\}$

[1] Note this is trivial by Burnside's Theorem: if G is a finite group of order $p^a q^b$, where $a, b \in \mathbb{Z}_{\geq 0}$ and p, q are primes, then G is solvable (so that G cannot be simple). Note that use of such a 'sledgehammer' for this problem would not be allowed.

are the distinct conjugacy classes of $\langle x \rangle$, where $g, h \in G$. But $g \cdot \langle x \rangle := g\langle x \rangle g^{-1} \neq \langle x \rangle$ so that the action cannot be trivial. Therefore, $\ker \phi$ is a proper nontrivial subgroup of G so that G cannot be simple.

OR

We claim that if G is a finite simple group of order at least 3 and H is a nontrivial proper subgroup of G with $|G\colon H| = n > 1$, then G is isomorphic to a subgroup of A_n: Since $H < G$ and $|G\colon H| = n > 1$, the action of G on the (left) cosets of H via left multiplication induces a map $\phi : G \to S_n$ with $\ker \phi \leq H$. But as G is simple, $\ker \phi = \{1\}$. By the First Isomorphism Theorem, $\operatorname{im} \phi \cong G/\ker \phi = G$. Suppose $\phi(G) \not\subseteq A_n$. Then we must be $A_n \phi(G) = S_n$. By the Second Isomorphism Theorem, $S_n/A_n = A_n\phi(G)/A_n \cong \phi(G)/(A_n \cap \phi(G))$. Now as G is simple, $A_n \cap \phi(G)$ is trivial or $A_n \cap \phi(G) = \phi(G)$. If $A_n \cap \phi(G) = \phi(G)$, then $S_n/A_n = 1$, a contradiction. If $A_n \cap \phi(G) = 1$, then $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z} \cong \phi(G) \cong G$, i.e. $|G| = 2$, a contradiction. Therefore, $\phi(G) \subseteq A_n$. □

3. Let G be a finite group with subgroups $H, K \leq G$. Consider the restriction to K of the left action of G on the left cosets of H in G.

(a) Show that the stabilizer in K of the coset $H = 1H$ is $H \cap K$.

(b) Show that $[K : H \cap K] \leq [G : H]$.

(c) Conclude $[G : H \cap K] \leq [G : H]\,[G : K]$.

Solution:

(a)

$$\begin{aligned} \operatorname{stab}_K(H) &= \{k \in K\colon k \cdot H = H\} \\ &= \{k \in K\colon kH = H\} \\ &= \{k \in K\colon k \in H\} \\ &= H \cap K \end{aligned}$$

(b) By the Orbit-Stabilizer Theorem, $|\mathcal{O}_H| = |G\colon \operatorname{stab}_H|$ so that $|\mathcal{O}_H \cap K| = |K\colon H \cap K|$ by (a). But $|\mathcal{O}_H| \leq |\mathcal{O}_H| = |G\colon G_H|$ and

$$G_H = \{g \in G\colon g \cdot H = H\} = \{g \in G\colon gH = H\} = \{g \in G\colon g \in H\} = H.$$

But then $|\mathcal{O}_H \cap K| \leq |\mathcal{O}| = |G\colon G_H| = |G\colon H|$. But then $|K\colon H \cap K| \leq |G\colon H|$.

(c) Using (b),

$$|G\colon H \cap K| = |G\colon K|\,|K\colon H \cap K| \leq |G\colon K|\,|G\colon H|$$

Therefore, $|G\colon H \cap K| \leq |G\colon K|\,|G\colon H|$.

□

4. Let A be a real, symmetric $m \times m$ matrix.

(a) Show that the eigenvalues of A are real.

(b) Show that eigenvectors corresponding to distinct eigenvalues are orthogonal.

Solution:

(a) Let v be an eigenvector of A associated with eigenvalue λ. Then $Av = \lambda v$. If M is a matrix, M^* denote the conjugate transpose and $\overline{M}$ denote the conjugate of M. Since A is symmetric, $A = A^T$. Furthermore since A is a real matrix, $A^* = A$. We compute v^*Av two different ways:

$$v^*Av = v^*(Av) = v^*(\lambda v) = \lambda(\overline{v} \cdot v)$$
$$v^*Av = (A\overline{v})^T v = (\overline{\lambda}\overline{v})^T v = \overline{\lambda}(\overline{v} \cdot v).$$

Since $v \neq 0$, $\overline{v} \cdot v \neq 0$. But then $\lambda = \overline{\lambda}$. Thus, $\lambda \in \mathbb{R}$.

(b) Note that if A is a real symmetric matrix, $\langle Ax, y\rangle = \langle x, A^T y\rangle = \langle x, Ay\rangle$. Let λ, μ be distinct eigenvalues with corresponding eigenvectors x, y, respectively. Then

$$\lambda\langle x, y\rangle = \langle \lambda x, y\rangle = \langle Ax, y\rangle = \langle x, A^T y\rangle = \langle x, Ay\rangle = \langle x, \mu y\rangle = \mu\langle x, y\rangle.$$

Therefore, $(\lambda - \mu)\langle x, y\rangle = 0$. Since λ, μ are distinct, $\lambda - \mu \neq 0$. Therefore, $\langle x, y\rangle = 0$ so that x and y are orthogonal.

□

5. Let $C_{[0,\pi]}$ be the real vector space of continuous real-valued functions defined on the closed interval $[0, \pi]$, and let V be teh subspace of $C_{[0,\pi]}$ spanned by the linearly independent functions $1, \cos t, \sin t, \cos^2 t$, and $\sin 2t$. For all $f, g \in V$ consider the expression $B(f, g) = \int_0^\pi (t+1) f(t) g(t)\, dt$.

(a) Prove that $B(f, g)$ is a bilinear form on V; first define a bilinear form.

(b) Give the definition of a symmetric bilinear form. Is $B(f, g)$ symmetric?

(c) Give the definition of a positive definite real quadratic form and determine whether the quadratic form associated to $B(f,g)$ is positive definite.

(d) Is there a basis $e_1,\dots,e_m$ for V, for some $m > 0$, with respect to which the $m \times m$ identity matrix I_m is the matrix of $B(f,g)$?

Solution:

(a) A bilinear form for a vector space V over a field K is a function $\langle\ ,\ \rangle : V \times V \to K$ such that

$$\begin{aligned}\langle u+v, w\rangle &= \langle u,w\rangle + \langle v,w\rangle\\ \langle u, v+w\rangle &= \langle u,v\rangle + \langle u,w\rangle\\ k\langle u,v\rangle &= \langle ku, v\rangle = \langle u, kv\rangle\end{aligned}$$

for all $u,v,w \in V$ and $k \in K$. Now let $f,g,h \in C_{[0,\pi]}$ and $r \in \mathbb{R}$. Then

$$\begin{aligned}B(f+g,h) &= \int_0^\pi (t+1)(f+g)h\ dt\\ &= \int_0^\pi (t+1)fh + (t+1)gh\ dt\\ &= \int_0^\pi (t+1)fh\ dt + \int_0^\pi (t+1)gh\ dt\\ &= B(f,h) + B(g,h)\end{aligned}$$

$$\begin{aligned}B(f,g+h) &= \int_0^\pi (t+1)f(g+h)\ dt\\ &= \int_0^\pi (t+1)fg + (t+1)fh\ dt\\ &= \int_0^\pi (t+1)fg\ dt + \int_0^\pi (t+1)fh\ dt\\ &= B(f,g) + B(f,h)\end{aligned}$$

$$B(rf,g) = \int_0^\pi (t+1)(rf)g\ dt = r\int_0^\pi (t+1)fg\ dt = rB(f,g)$$

$$B(f,rg) = \int_0^\pi (t+1)f(rg)\ dt = r\int_0^\pi (t+1)fg\ dt = rB(f,g)$$

Therefore, $B(f,g)$ is a bilinear form on V.

(b) The definition of a bilinear was given in (a). A bilinear form $\langle\cdot\ ,\cdot\rangle$ is symmetric if $\langle v,w\rangle = \langle w,v\rangle$ for all $v,w \in V$. The given form $B(f,g)$ (which is bilinear from (a), is symmetric since

$$B(f,g) = \int_0^\pi (t+1)f(t)g(t)\ dt = \int_0^\pi (t+1)g(t)f(t)\ dt = B(g,f).$$

(c) A quadratic form associated to a symmetric bilinear form $\langle \cdot\,,\, \rangle$ on V over a field K is a function $q : V \to K$ such that $q(v) = \langle v, v \rangle$. The form q is positive definite if $q(v) = 0$ if and only if $v = 0$. Now for the given bilinear form, $B(f, g)$

$$q(f) = \langle f, f \rangle = B(f, f) = \int_0^\pi (t+1) f^2(t)\, dt \geq 0$$

since $f^2(t) \geq 0$. Since $f, t+1, f^2$ are continuous on $[0, \pi]$, we have $(t+1)f^2(t)$ continuous on $[0, \pi]$. Then if $B(f, f) = 0$, we must have $(t+1)f^2(t) \equiv 0$ on $[0, \pi]$. But since $t + 1 \not\equiv 0$ on $[0, 1]$, we must have $f^2(t) \equiv 0$ on $[0, 1]$. Therefore, $f(t) = 0$ for all $t \in [0, 1]$. Clearly if $f \equiv 0$ on $[0, 1]$, then $B(f, f) = 0$. But then $q(f) = B(f, f)$ is positive definite.

6. Find all possible Jordan normal forms of a complex $m \times m$ matrix A with the characteristic polynomial $(x^2 + 3)^2(x + 5)^4$ if the matrix $A + 5I_m$ is of rank 7. No proof is needed.

7.

(a) Prove that the kernel of the homomorphism $\phi : \mathbb{C}[x, y] \to \mathbb{C}[t]$ of polynomial rings given by $\phi(x) = t^2$ and $\phi(y) = t^3$ is the principal ideal generated by the polynomial $y^2 - x^3$.

(b) Determine the image of ϕ explicitly.

Solution:

(a)

(b)

8.

(a) Give the definition of an integral domain.

(b) Give the definition of the characteristic of a nontrivial commutative ring.

(c) Is there an integral domain of characteristic 6? Explain.

(d) Is there an integral domain with 12 elements? Explain.

Solution:

(a) An integral domain is a commutative ring with identity with no zero divisors, i.e. for all $a, b \in R$, $ab = ba$ and if $ab = 0$, then $a = 0$ or $b = 0$.

(b) We demand $1 \in R$. The characteristic of a commutative ring R is the smallest integer positive integer $n \in \mathbb{Z}$ such that $n \cdot 1 = 0$. If no such n exists, we say R has characteristic 0.

(c) The characteristic of an integral domain is either 0 or prime: let R be an integral domain. If $\operatorname{char} R = 0$, we are done. If not, let $\operatorname{char} R = n$. If $n = rs$ for some integers r, s, neither of which are 1, then $1 < r, s < n$. But $0 = n \cdot 1 = (rs) \cdot 1 = (r \cdot 1)(s \cdot 1)$. Now since $r, s < n$, neither $r \cdot 1$ nor $s \cdot 1$ are 0. But then R contains zero divisors, a contradiction. Then it must be that either $r = 1$ or $s = 1$ so that n must be prime.

Since 6 is not prime, there can be no integral domain with characteristic 6.

(d) A finite integral domain is a field: let R be an integral domain and consider the map $\phi_a : R \to R$ given by $r \mapsto ar$, where $a \in R \setminus \{0\}$ is a fixed element. If $\phi_a(ra) = 0$, then $ra = 0$ so that either $r = 0$ or $a = 0$. But $a \neq 0$ so that $r = 0$. But then $\ker \phi = \{0\}$. Therefore, ϕ is injective. Since R is finite, ϕ is an injection map between finite sets, hence an isomorphism. But then there exists $r' \in R$ such that $1 = \phi_a(r') = ar'$. But then a is invertible. Since $a \in R \setminus \{0\}$ was arbitrary, R is a field.

Now since R is finite, we know $\operatorname{char} R \neq 0$. But then $\operatorname{char} R = p$, where p is a prime. Now R (a field) must contain the subfield $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ (since $1 \in R$ generates this subfield). But then R is a vector space over $\mathbb{F}_p$ so that it is free over $\mathbb{F}_p$. But R is finite and $\mathbb{F}_p$ has cardinality p so that $|R| \cong p^n$ for some $n \in \mathbb{Z}$.

Alternatively, if $q \mid |R|$, where $q \neq p$ and $\operatorname{char} R = p$, then by Cauchy's Theorem, R contains an element of order q, say $x \in R$. Now $q \cdot x = 0$ and $p \cdot x = 0$. Since $(p, q) = 1$, we can find $r, s \in \mathbb{Z}$ such that $rp + sq = 1$. But then $1 \cdot x = (rp + sq) \cdot x$. However,

$$1 \cdot x = (rp + sq) \cdot x = rp \cdot x + sq \cdot x = r(p \cdot x) + s(q \cdot x) = 0$$

so that $x = 0$. But since $|x| = q > 0$ in $(R, +)$, this is a contradiction. Then the only prime dividing $|R|$ is p so that $|R| = p^n$.

Now $12 = 2^2 \cdot 3$ has two distinct prime divisors. Therefore, no integral domain with 12 elements can be a field.

□

9. Determine the irreducible polynomial for $\beta = \sqrt{2} + \sqrt{7}$ over each of the following fields.

(a) $\mathbb{Q}(\sqrt{7})$

(b) $\mathbb{Q}(\sqrt{14})$

(c) $\mathbb{Q}$

10. Let $\zeta = e^{\frac{2\pi i}{5}}$.

(a) Prove that $K = \mathbb{Q}(\zeta)$ is a splitting field for the polynomial $x^5 - 1$ over $\mathbb{Q}$ and determine the degree $[K : \mathbb{Q}]$. Use the fact that for a prime p, the cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

(b) Determine the Galois group $G(K/\mathbb{Q})$ explicitly and up to isomorphism.

January 2006

1. Assume A is a n-by-n matrix such that $\text{rk}[A - 2I_n] - \text{rk}[(A - 2I_n)^2] = 5$. (Here rk denotes the rank of the matrix and I_n is the identity matrix.) How much can be concluded about the Jordan canonical form of A?

Solution: We have rk $A +$ nullity $A = n$. Then we have

$$\begin{aligned} 5 &= \text{rk}[A - 2I_n] - \text{rk}[(A - 2I_n)^2] \\ &= (n - \text{ nullity}(A - 2I_n)) - (n - \text{ nullity}(A - 2I_n)^2) \\ &= \text{ nullity}(A - 2I_n)^2 - \text{ nullity}(A - 2I_n) \end{aligned}$$

Then we know there are 5 Jordan blocks associated to $\lambda = 2$ that are of at least size 2. In particular, there are at least 5 Jordan blocks associated to $\lambda = 2$. □

2. Let $V = R^2$ be the Euclidean plane and assume that $T : V \to V$ is a linear operator. Let l_1, l_2, and l_3 be three distinct lines passing through the origin with $T(l_i) = l_i$ for $i = 1, 2, 3$. Show that T is a dilation, that is, T is multiplication by some constant.

3. Let k be a field and let $T : V \to W$ be a linear transformation between two vector spaces over k.

(a) Define the adjoint[2] $T^* : W^* \to V^*$ of the linear operator T.

(b) Show that T^* is injective if and only if T is onto.

4. Show that a finite group of order 24 cannot be simple.

Solution: The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24. By Sylow's Theorem $n_2(G) \equiv 1$ mod 2 and divides 24. The only possibilities are $n_2(G) = 1$ or $n_2(G) = 3$. If $n_2(G) = 1$, then G contains a unique 2-Sylow subgroup, which is necessarily normal. This implies that G has a nontrivial, proper, normal subgroup. Thus, G is not simple.

Suppose that $n_2(G) = 3$. Let X denote the set of 2-Sylow subgroups. Note that G acts on X by conjugation. This induces a homomorphism $\phi : G \to S_X$. Since $|G| = 24$ and $|S_X| = 3! = 6$, ϕ is not injective. Therefore, $|\ker \phi| > 1$. Note that $|\ker \phi| \neq 24$ since any two 2-Sylow subgroups are conjugate (so they all can not be fixed by the action of conjugation). Thus, $\ker \phi$ is a proper, nontrivial, normal subgroup of G, which implies that G is not simple. □

[2]The exam says transpose but clearly the adjoint is meant.

5. Let S_n denote the symmetric group on n letters and let A_n denote the alternating subgroup. Recall that if $\sigma \in G$, where G is a group, the *centralizer* of σ in G is the subgroup $C_G(\sigma) = \{\tau \in G \colon \tau\sigma = \sigma\tau\}$.

(a) If $\sigma \in A_n$, use the sign homomorphism from S_n to $\{\pm 1\}$, to show that $C_{A_n}(\sigma)$, the centralizer of σ in A_n, is either equal to $C_{S_n}(\sigma)$ or it is a subgroup of $C_{S_n}(\sigma)$ of index 2.

(b) If $n = 5$ and $\sigma \in A_n$ is a 3-cycle, show that $[C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2$.

(c) We know that all 3-cycles are conjugate in S_5. Use this and part (b) to show that all 3-cycles are conjugate in A_5.

Solution:

(a) If $H \leq S_n$, we claim either all permutations in H are even or exactly half of them are even. If all permutations of H are even, then we are done. So suppose $\sigma \in H$ is an odd permutation. Let H_E be the set of even permutations of H and H_O be the set of odd permutations of H. Define a map $\phi : H_E \to H_O$ by $\rho \mapsto \sigma\rho$. First, we show that ϕ is well defined. If $\rho_1 = \rho_2$, then $\sigma\rho_1 = \sigma\rho_2$ which implies $\phi(\rho_1) = \phi(\rho_2)$. Furthermore, if $\phi(\rho_1) = \phi(\rho_2)$, then $\sigma\rho_1 = \sigma\rho_2$, which implies $\rho_1 = \rho_2$. But then ϕ is injective. Let $\gamma \in H_O$. Then $\sigma^{-1}\gamma \in H_E$ since $\sigma^{-1}\gamma$ is even. But then $\gamma = \sigma(\sigma^{-1}\gamma) = \phi(\sigma^{-1}\gamma)$ so that ϕ is surjective. Then ϕ is a bijection between finite sets. Therefore, $|H_E| = |H_O|$. Then $|H| = |H_E| + |H_O| = 2|H_E|$, half the permutations of H are even. As $C_{S_n}(\sigma) \leq S_n$, either $C_{S_n}(\sigma) = C_{A_n}(\sigma)$ or $|C_{S_n}(\sigma) \colon C_{A_n}(\sigma)| = 2$.

(b) There are $\binom{5}{3}2! = 20$ 3-cyles. So $|\text{orb}\,\sigma| = |S_n \colon C_{S_n}(\sigma)|$ so that $20 = \frac{120}{|C_{S_n}(\sigma)|}$. But then $|C_{S_n}(\sigma)| = 6$. By the work below in (c), the 3-cycles are conjugate in A_5. Therefore, $20 = \frac{60}{|C_{A_5}|}$ and then $|C_{A_5}(\sigma)| = 3$. Therefore, $|C_{S_5}(\sigma) \colon C_{A_5}(\sigma)| = \frac{6}{3} = 2$.

(c) Consider $(\sigma_1\ \sigma_2\ \sigma_3)$. Any other 3-cycle will either have 1, 2, or 3 indices in common. Without loss of generality, consider $(\sigma_1\ \sigma_4\ \sigma_5)$, $(\sigma_1\ \sigma_2\ \sigma_4)$, $(\sigma_1\ \sigma_3\ \sigma_2)$, respectively. Define $\tau := (\sigma_2\ \sigma_4)(\sigma_3\ \sigma_5)$. Then $\tau(\sigma_1\ \sigma_2\ \sigma_3)\tau^{-1} = (\sigma_1\sigma_3\sigma_2)$. Since $\tau \in A_5$, $(\sigma_1\ \sigma_2\ \sigma_3)$ and $(\sigma_1\ \sigma_4\ \sigma_5)$ are conjugates. Furthermore, $\tau = (\sigma_3\ \sigma_4\ \sigma_5)$ so that $\tau(\sigma_1\ \sigma_2\ \sigma_3)\tau^{-1} = (\sigma_1\ \sigma_2\ \sigma_4)$ so that $(\sigma_1\ \sigma_2\ \sigma_3)$ and $(\sigma_1\ \sigma_2\ \sigma_4)$ are conjugates. Finally, $\tau = (\sigma_2\ \sigma_3)(\sigma_4\ \sigma_5)$ so that $\tau(\sigma_1\ \sigma_2\ \sigma_3)\tau^{-1} = (\sigma_1\ \sigma_3\ \sigma_2)$. Therefore, $(\sigma_1\ \sigma_2\ \sigma_3)$ and $(\sigma_1\ \sigma_3\ \sigma_2)$ are conjugates. But then all 3-cycles are conjugate in A_5.

□

6. Let G be a finite p-group for some prime p. Show that the center of G is not trivial.

Solution: Let $|G| = p^n$ for some $n \geq 0$. If $n = 0$, the result is trivial. If $p = 1$, then $G \cong \mathbb{Z}/p\mathbb{Z}$, which is abelian. So suppose $p > 1$. The Class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G\colon C_G(a_i)]$$

where the $Z(G)$ is the center of G, $C_G(x)$ is the centralizer of x in G, and the summation is over $a_1, \ldots, a_r$ representatives for the distinct conjugacy classes of G. Note that each summand of the class equation is a divisor of $|G|$ and $[G\colon C_G(a_i)] > 1$ since $a_i \notin Z(G)$. The Class equation for G can be rewritten as

$$|Z(G)| = |G| - \sum_{i=1}^{r} [G\colon C_G(a_i)].$$

Each term on the right hand side is a divisor of $|G| = p^n$. Furthermore, each term on the right hand side is strictly larger than 1. Therefore, p divides every term on the right hand side, which implies that p divides the left hand side. Thus, p divides $|Z(G)|$ so that $|Z(G)| \neq 1$. □

7. Let Q denote the field of rational numbers and let $f = x^3 + 2x^2 + 7 \in Q[x]$.

(a) Show that f has precisely one real root.

(b) Show that f is irreducible in $Q[x]$.

(c) Show that the Galois group of f over Q is isomorphic to the symmetric group S_3.

Solution:

(a) Observe that $f(-3) = -14$ and $f(-1) = 8$ so that by the Intermediate Value Theorem, there is $\alpha \in (-3, -1)$ such that $f(\alpha) = 0$. By Descartes Rule of Signs, f can have no positive root and only one negative root. But then it must be that f has only one real root.

(b) Since f is degree 3, f is reducible if and only if f has a rational root. By the Rational Root Theorem, the only possible roots of $f(x)$ are $\pm 1, \pm 7$. But $f(1) = 10$, $f(-1) = 8$, $f(7) = 448$, and $f(-7) = -238$. Therefore, f has no root in $\mathbb{Q}$ so that f is irreducible in $Q[x]$.

(c) Let K denote the splitting field of f. We know K/Q is Galois so that $[K\colon Q] = \#\mathrm{Gal}(K/Q)$. Since there are 3 roots, we know $\mathrm{Gal}(K/Q) \leq S_3$. Then $\#\mathrm{Gal}(K/Q)$ is either 3 or 6, i.e. $\mathrm{Gal}(K/Q) = A_3$ or S_3. If $f(x) \in K[x]$ has one real root and a two complex roots, we may consider complex conjugation as an automorphism of order

2. But then this complex conjugation generates a subgroup of order two in $\mathrm{Gal}(K/Q)$. Then any irreducible and separable extension of a cubic with a unique real root must have Galois group isomorphic to S_3 since $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ has no subgroup of order 2.

□

8.

(a) Let K/F be a finite extension of fields. Show that K/F is algebraic.

(b) Let L/K and K/F be algebraic field extensions. Show that L/F is also algebraic.

Solution:

(a) Let $\alpha \in K$. We have $F \subseteq F(\alpha) \subseteq K$. Since K/F is a finite extension, $F(\alpha)/F$ is a finite extension since $[K\colon F] = [K\colon F(\alpha)][F(\alpha)\colon F]$. Suppose $[F(\alpha)\colon F] = n$. Then α is a root of a polynomial of at most degree n over F so that α is algebraic. Therefore, K/F is algebraic.

(b) Let $\alpha \in L$. Since L/K is algebraic, α satisfies some polynomial equation, say $f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, where $a_i \in K$. Consider the extension $F(\alpha, a_0, \ldots, a_n)$. Since K/F is a finite extension, a_i is algebraic over F for all i by (a). Now α generates an extension of at most degree n since the minimal polynomial must divide $f(x)$. Then

$$[F(\alpha, a_0, \ldots, a_n)\colon F] = [F(\alpha, a_0, \ldots, a_n)\colon F(a_0, \ldots, a_n)]\,[F(a_0, \ldots, a_n)\colon F]$$

is also finite and $F(\alpha, a_0, \ldots, a_n)/F$ is algebraic. But then the element α is algebraic over F. Therefore, L/F is an algebraic extension.

□

9.

(a) Assume R is a commutative ring and $I \subseteq R$ is an ideal. Show that $I[X] \subseteq R[X]$ is an ideal.

(b) Using the First Isomorphism Theorem or otherwise, show that $R[X]/I[X]$ is isomorphic to $(R/I)[X]$.

Solution:

(a) Clearly, $I[x]$ is nonempty since I is nonempty. Furthermore, it is clear that $0 \in I[x]$. Now suppose $f(x), g(x) \in I[x]$. Then $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g(x) =$

$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$, where $a_i, b_i \in I$. Without loss of generality, assume $n \geq m$. Then

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i \in I[x],$$

where we take $b_i = 0$ if $i > m$, since $a_i + b_i \in I$ for $i = 0, 1, \ldots, n$. Now let $h(x) \in R[x]$. Write $h(x) = c_r x^r + c_{r-1}x^{r-1} + \cdots + c_0$, where $c_i \in R$ for $i = 0, 1, \ldots, r$. Then

$$h(x)f(x) = \sum_{i=0}^{r+n} \sum_{j=0}^{i} c_j a_{i-j} x^i$$

where we take $c_j = 0$ if $j > r$ and $a_{i-j} = 0$ if $i - j > n$. Since I is an ideal and $a_i \in I$, $c_j \in R$, we have $c_j a_{i-j} \in I$. But then $h(x)f(x) \in I[x]$. Therefore, $I[x]$ is an ideal of $R[x]$.

(b) Define a map $\phi : R[x] \to (R/I)[x]$ via reducing coefficients mod I, i.e. $r_n x^n + \cdots + r_0 \mapsto (r_n + I)x^n + \cdots + (r_0 + I)$. We first check this is a homomorphism. Clearly, $\phi(1) = 1 + I$ and $\phi(0) = 0 + I = I$. Suppose $f(x), g(x) \in R[x]$ are as given in (a) but with $a_i, b_i \in R$ (again taking $n \geq m$ and $b_i = 0$ if $i > m$). Then

$$\begin{aligned}
\phi(f(x) + g(x)) &= \phi\left(\sum_{i=0}^{n} (a_i + b_i)x^i\right) \\
&= \sum_{i=0}^{n} \big((a_i + b_i) + I\big)x^i \\
&= \sum_{i=0}^{n} (a_i + I)x^i + \sum_{i=0}^{n} (b_i + I)x^i \\
&= \sum_{i=0}^{n} (a_i + I)x^i + \sum_{i=0}^{m} (b_i + I)x^i \\
&= \phi(f(x)) + \phi(g(x))
\end{aligned}$$

Finally, assume $h(x), f(x) \in R[x]$, where we again assume $c_j = 0$ if $j > r$ and $a_{i-j} = 0$

if $i - j > n$. Then

$$\begin{aligned}
\phi(h(x)f(x)) &= \phi\left(\sum_{i=0}^{r+n}\sum_{j=0}^{i} c_j a_{i-j} x^i\right) \\
&= \sum_{i=0}^{r+n}\sum_{j=0}^{i}(c_j a_{i-j} + I)x^i \\
&= \sum_{i=0}^{r+n}\sum_{j=0}^{i}(c_j + I)(a_{i-j} + I)x^i \\
&= \left(\sum_{i=0}^{r}(c_i + I)x^i\right)\left(\sum_{i=0}^{n}(a_i + I)x^i\right) \\
&= \phi\left(\sum_{i=0}^{r}(c_i + I)x^i\right)\phi\left(\sum_{i=0}^{n}(a_i + I)x^i\right) \\
&= \phi(h(x))\phi(f(x))
\end{aligned}$$

Therefore, ϕ is a homomorphism. It is clear that ϕ is surjective: if $\sum_{i=0}^{n}(r_i + I)x^i \in (R/I)[x]$, then $\phi(r_n x^n + \cdots + r_0) = \sum_{i=0}^{n}(r_i + I)x^i$. We claim $\ker\phi = I[x]$. If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in I[x]$, then

$$\begin{aligned}
\phi(f(x)) &= \phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \\
&= (a_n + I)x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_0 + I) \\
&= (0 + I)x^n + (0 + I)x^{n-1} + \cdots + (0 + I) \\
&= 0 + I = I
\end{aligned}$$

so that $I[x] \subseteq \ker\phi$. Finally, if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \ker\phi$, then

$$\begin{aligned}
\phi(f(x)) &= \phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \\
&= (a_n + I)x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_0 + I) \\
&= (0 + I)x^n + (0 + I)x^{n-1} + \cdots + (0 + I)
\end{aligned}$$

but then $a_i \in I$ for all i. Therefore, $f(x) \in I[x]$ so that $\ker\phi \subseteq I[x]$. Then we have $\ker\phi = I[x]$. By the First Isomorphism Theorem,

$$R[x]/I[x] \cong (R/I)[x].$$

□

10.

(a) Let S be a commutative ring and assume that $I = Sf + Sg$ is the ideal generated by two elements f and g. Show that if $h \in S$ is any element, then I is also generated by the elements f and $g - hf$.

(b) Let Z be the ring of integers and assume I is an ideal of $Z[x]$ generated by the set $f, g \in Z[x]$. Show that we can replace f and g by two generators, one of which has a zero constant term.

Solution:

(a) Let $h \in S$. We need to show that $I = \langle f, g - hf \rangle$. Let $x \in I$, then

$$x = s_1 f + s_2 g = s_1 f + s_2(g - hf) + s_2 hf = (s_1 + s_2 h)f + s_2(g - hf) \in \langle f, g - hf \rangle$$

Therefore, $I \subseteq \langle f, g - hf \rangle$. Now suppose $x \in \langle f, g - hf \rangle$. Then

$$x = s_1 f + s_2(g - hf) = s_1 f + s_2 g - s_2 hf = (s_1 - s_2 h)f + s_2 g \in \langle f, g \rangle = I.$$

But then $\langle f, g - hf \rangle \subseteq I$. Therefore, $I = \langle f, g - hf \rangle$. But then I is generated by f and $g - hf$.

(b) Clearly, $I := \langle f(x), g(x) \rangle \subset Z[x]$ is an ideal. By (a) for any $h(x) \in Z[x]$, $I = \langle f(x), g(x) - h(x)f(x) \rangle$.

□

August 2006

1.

(a) If G is an abelian group, prove that the map $\phi : G \to G$ defined by $\phi(g) = g^m$, for all $g \in G$ and some integer $m > 0$, is an endomorphism.

(b) Give an example showing that one cannot drop the assumption that G is abelian in (a).

(c) In the setting of (a), suppose that the order of G is n and that the integers m and n are coprime. Prove that the map $\phi : G \to G$ is an automorphism.

Solution:

(a) Let $g, h \in G$. Since $\phi(gh) = (gh)^m$ and $\phi(g)\phi(h) = g^m h^m$, it suffices to show that $(gh)^m = g^m h^m$ for all $g, h \in G$, $m \in \mathbb{N}$. We prove this with induction on m. If $m = 1$, then $(gh)^1 = gh = g^1 h^1$. Assume that $(gh)^m = g^m h^m$ for some m. Then

$$(gh)^{m+1} = (gh)(gh)^m = ghg^m h^m = gg^m hh^m = g^{m+1} h^{m+1}$$

By induction, $(gh)^m = g^m h^m$ for all $m \in \mathbb{N}$ and $g, h \in G$. Thus, ϕ is an endomorphism.

(b) Let $G = D_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2$ and $m = 2$. Of course, D_3 is a nonabelian group. As defined above, ϕ is *not* a homomorphism since

$$\phi(\sigma\tau) = \sigma\tau\sigma\tau = \tau\sigma^2\sigma\tau = \tau^2 = 1$$
$$\phi(\sigma)\phi(\tau) = \sigma^2\tau^2 = \sigma^2$$

and $\sigma^2 \neq 1$.

(c) Let $x \in \ker\phi$, then $x^m = 1$. This implies that $|x|$ divides m. However, $|x|$ divides n. Since m and n are relatively prime, $|x| = 1$. Thus, $|x| = 1$. But then $x = 1$. This implies that $\ker\phi$ is trivial so that $|phi$ is injective. But G is a finite group and $\phi : G \to G$ is an injective map from a finite set to itself, therefore surjective. But then ϕ is an automorphism.

□

2.

(a) If G is a group, S is a left G-set, and Perm S is the group of permutations of S, the map $\Phi : G \to$ Perm S defined by $\Phi(g)(s) = gs$, for all $s \in S$, is a homomorphism of groups. Using this fact, prove that $N = \{g \in G \colon gs = s \text{ for all } s \in S\}$ is a normal subgroup of G.

In the rest of the problem, let H be a subgroup of G and let S be the set of left cosets of H in G.

(b) Prove that $N \subset H$.

Let $|G| = n < \infty$ and $[G : H] = k > 1$.

(c) Prove that if $n > k!$ then $\{1\} \neq N \neq G$.

(d) If k is the least prime dividing n, prove $H = N$. Hint: Find the cardinality of $\operatorname{im} \Phi$.

(a)

$$\begin{aligned}\ker \Phi &= \{g \in G \colon \Phi(g) = 1\} \\ &= \{g \in G \colon \Phi(g)s = s \text{ for all } s \in S\} \\ &= \{g \in G \colon gs = s \text{ for all } s \in S\} \\ &= N\end{aligned}$$

Since N is the kernel of a group homomorphism, N is a normal subgroup of G.

(b) If $g \in N$ and $a \in G$, then $g \cdot aH = gaH = aH$ for all $a \in G$. In particular, this is true when $a = 1$. But then $g \cdot H = gh = H$. Thus, $g \in H$ and $N \subseteq H$.

(c) Note that $|S| = [G : H] = k$, so $|\text{Perm } S| = k!$. From above, we know there is a homomorphism

$$\Phi : G \to \text{Perm } S.$$

Since $|G| = n > k! = |\text{Perm } S|$, Φ cannot be injective. Therefore, $\ker \Phi = N \neq \{1\}$. Also, $N \subset H \subsetneq G$, so $\ker \Phi = N \neq G$. Thus, $\{1\} \neq N \neq G$, as needed.

(d) By the First Isomorphism Theorem, $G/N \cong \operatorname{im} \Phi$. Therefore, $|G| = |N| \, |\operatorname{im} \Phi|$, so $|\operatorname{im} \Phi|$ divides both n and $k!$. It is clear that $\operatorname{im} \Phi \neq \{1\}$. The claim is that $|\operatorname{im} \Phi| = k$. Suppose not. Then there exists a prime integer $p \neq k$ dividing $|\operatorname{im} \Phi|$ (since k^2 does not divide $k!$). However, k is the largest prime divisor of $k!$, so $p < k$ and p divides n. This contradicts the minimality of k, so $|\operatorname{im} \Phi| = k = [G : N]$ and

$$\begin{aligned}[G : N] &= [G : H][H : N] \\ k &= k[H : N]\end{aligned}$$

Thus, $[H : N] = 1$ and $H = N$.

□

3. Prove that a group of order 35 is cyclic.

Solution: The divisors of 35 are 1, 5, 7, and 35. Let G be a group of order 35. For $p = 5, 7$, let $n_p(G)$ denote the number of p-Sylow subgroups of G. By Sylow's Theorem, $n_5(G) \equiv 1 \mod 5$ and divides 7. The only possibility is $n_5(G) = 1$. Similarly, $n_7(G) \equiv 1 \mod 7$ and divides 5 so this implies that $n_7(G) = 1$.

Let H denote the unique 5-Sylow subgroup of G, let J denote the unique 7-Sylow subgroup of G and consider $x \in G \setminus (H \cup J)$. Now $|x|$ divides $|G| = 35$. If $|x| = 1$, then $x = 1 \in H \cup J$, a contradiction. If $|x| = 5$, then $|\langle x \rangle = 5$. This implies that $\langle x \rangle = H$, so $x \in H$, a contradiction. Therefore, $|x| \neq 5$. Similarly, $|x| \neq 7$. Thus, $|x| = 35$, which implies that $G = \langle x \rangle$. Therefore, G is cyclic. □

4. Let V be a fixed vector space of finite dimension $n > 0$ over a field F, and let $\lambda \in F$. If $T : V \to V$ is a linear operator with an eigenvalue λ, let m be the maximal number of linearly independent eigenvectors with eigenvalue λ.

(a) Prove that the multiplicity of λ as a root of the characteristic polynomial T is at least m.

(b) Among all linear operators on V with an eigenvalue λ, what are the smallest and largest possible values of m? Justify your answer (remember, n is arbitrary but fixed).

Solution:

(a) Let $\mathcal{I} = \{e_1, \ldots, e_m\}$ be a maximal set of linearly independent eigenvectors in V with eigenvalue λ. Since $\mathcal{I}$ is linearly independent, it can be extended to a basis $\mathcal{B} = \{e_1, \ldots, e_m, b_{m+1}, \ldots, b_m\}$ of V. The matrix of T with respect to $\mathcal{B}$ is the block matrix

$$A = \left[\begin{array}{c|c} \lambda I_M & B \\ \hline 0 & C \end{array}\right].$$

Therefore, $\det(xI - T) = \det(xI - A) = \det(xI_m - \lambda I_m) \det(xI_{n-m} - C) = (x - \lambda)^m \det(xI_{n-m} - C)$ and the multiplicity of λ as a root of the characteristic polynomial of T is at least m.

(b) The smallest possible value of m is 1. Since V is finite dimensional, $V \cong F^n$ when a basis $\mathcal{B}$ is chosen. Consider a linear operator whose matrix with respect to $\mathcal{B}$ is a diagonal matrix with a λ in the a_{11} spot and $\lambda + 1$ in the $a_{22}, a_{33}, \ldots$, and a_{nn} spots. Then the characteristic polynomial of T is $(x - \lambda)(x - (\lambda + 1))^{n-1}$. By part (a), $m \leq 1$ so $m = 1$.

The largest possible value of m is n. Consider the linear operator $T : V \to V$ defined by $T(v) = \lambda v$. Then every nonzero vector in V is an eigenvector with eigenvalue λ, so the maximal number of linearly independent eigenvectors with eigenvalue λ is the maximal number of linearly independent vectors in V, which is n.

□

5. Let V be a finite-dimensional complex vector space with a positive definite Hermitian form $\langle\ ,\ \rangle$, and let $T : V \to V$ be a linear operator.

(a) Give the definition of the adjoint operator $T^* : V \to V$.

(b) Give the definition of when T is a *normal* linear operator.

(c) Assuming T is normal, prove that $\ker T = (\operatorname{im} T)^\perp$ where, for a subspace W of V, $W^\perp$ denotes the orthogonal complement of W.

Solution:

(a) For any vector v, $T^*(v)$ is the unique element of V satisfying $\langle T^*v, w\langle = \langle v, Tw\rangle$ for all $w \in V$.

(b) T is a normal operator if $TT^* = T^*T$.

(c) First, we show $\ker T = \ker T^*$. Observe that

$$\begin{aligned} x \in \ker T &\iff Tx = 0 \\ &\iff \langle Tx, Tx\rangle = 0 \\ &\iff \langle x, T^*Tx\rangle = 0 \\ &\iff \langle x, TT^*x\rangle = 0 \\ &\iff \langle T^*x, T^*x\rangle = 0 \\ &\iff T^*x = 0 \\ &\iff x \in \ker T^* \end{aligned}$$

proving the claim. If $x \in \ker T$, then $x \in \ker T^*$, so for any $y \in V$, $0 = \langle y, T^*x\rangle = \langle Ty, x\rangle$. This implies that $x \in (\operatorname{im} T)^\perp$. Thus, $\ker T \subset (\operatorname{im} T)^\perp$.

If $x \in (\operatorname{im} T)^\perp$, then $\langle Ty, x\rangle = 0$ for all $y \in V$. This implies that $\langle y, T^*x\rangle = 0$ for all $y \in V$. Take $y = T^*x$. Then $\langle T^*x, T^*x\rangle = 0$, which implies that $T^*x = 0$. Thus, $x \in \ker T^* = \ker T$. Therefore, $(\operatorname{im} T)^\perp \subset \ker T$ and $\ker T = (\operatorname{im} T)^\perp$.

□

6. Let R be a commutative ring with identity and let $I \subset R$ be an ideal. Define the radical of I, denoted $\sqrt{I}$, by $\sqrt{I} = \{r \in R \colon r^n \in I \text{ for some positive integer } n\}$.

(a) Prove that $\sqrt{I}$ is an ideal of R.

(b) We ay that I is a radical ideal if and only if $I = \sqrt{I}$. Recall that an element r is called nilpotent if and only if $r^n = 0$ for some positive integer n. Prove that I is a radical ideal if and only if $0 + I$ is the only nilpotent element of the quotient ring R/I.

Solution:

(a) It is clear that $I \subset \sqrt{I}$, which implies that $\sqrt{I}$ is nonempty. Let $a, b \in \sqrt{I}$. There then exist $m, n \in \mathbb{N}$ such that $a^m, b^n \in I$. Then

$$(a+b)^{2(m+n)} = a^{2(m+n)} + a^{2(m+n)-1}b + \cdots + a^{m+n}b^{m+n} + \cdots + b^{2(m+n)}$$

Each of the terms above is of the form $a^j b^k$ for some $j, k \geq 0$. The claim is that either $j \geq m$ or $k \geq n$ in each term. Note that $j + k = 2(m+n)$ so if $j < m$, $k = 2m + 2n - j > 2m_2 n - m = m + 2n > n$. This implies that in each term of the above, either $a^j \in I$ or $b^k \in I$. Since I is an ideal, this implies that every term is an element of I so $(a+b)^{2(m+n)} \in I$. Thus, $a + b \in \sqrt{I}$ and $\sqrt{I}$ is closed under addition. If $r \in R$, $a \in \sqrt{I}$, then there is a $n \in \mathbb{N}$ such that $a^n \in I$. Therefore, $(ra)^n = r^n a^n \in I$ since I is an ideal. Thus, $ra \in \sqrt{I}$. Therefore, $\sqrt{I}$ is an ideal.

(b) Assume that I is a radical ideal and let $r + I$ be a nilpotent element of R/I. Then there is a $n \in \mathbb{N}$ such that $(r+I)^n = r^n + I = I$. Thus, $r^n \in I$. Thus implies that $r \in \sqrt{I} = I$, so $r + I = 0 + I$. Therefore, $0 + I$ is the only nilpotent element of R/I.

Now assume that $0 + I$ is the only nilpotent element of R/I. It was noted above that $I \subset \sqrt{I}$; it remains to show that $\sqrt{I} \subset I$. Let $r \in \sqrt{I}$, then there exists a $n \in \mathbb{N}$ such that $r^n \in I$. This implies that $(r+I)^n = r^n + I = I$. Thus, $r + I$ is a nilpotent element of R/I, so $r + I = 0 + I$. This implies that $r \in I$. Therefore, $\sqrt{I} \subset I$ and $I = \sqrt{I}$. But then I is a radical ideal.

□

7. Let R be a PID and let a and b be two nonzero nonunits in R.

(a) Give the definition of the greatest common divisor of a and b.

(b) Prove that a greatest common divisor of a and b exists.

(c) Let c be a greatest common divisor of a and b. Prove there exists $x, y \in R$ such that $c = xa + yb$.

Solution:

(a) An element $d \in R$ is a greatest common divisor of a and b if $d \mid a$ and $d \mid b$ and for any $c \in R$ such that $c \mid a$ and $c \mid b$, $c \mid d$.

(b) Since R is a PID, the ideal (a, b) is principal, so there exists $d \in R$ such that $(d) = (a, b)$. The claim is that d is a greatest common divisor of a and b. Since $a, b \in (d)$, $d \mid a$ and $d \mid b$. If $c \in R$, $c \mid a$ and $c \mid b$, then $a \in (c)$, $b \in (c)$, which implies that $(a, b) \subset (c)$. So $(d) \subset (c)$, which implies that $d \in (c)$. Thus, $c \mid d$. But then d is a greatest common divisor of a, b.

(c) If c is a greatest common divisor of a and b, then $(c) = (a, b)$ by the previous part. In particular, $c \in (a, b)$, so there exists $x, y \in R$ such that $xa + yb = c$.

□

8. Let F be a finite field, $F[x]$ the polynomial ring over F, and M and $F[x]$-module.

(a) Explain why M is also an F-vector space in a natural way. Denote by $\dim_F(M)$ the dimension of M as a F-vector space.

(b) Prove that for each positive integer n, there exists a simple $F[x]$-module M_n such that $n < \dim_F(M_n) < \infty$.

Solution:

(a) Since M is an $F[x]$-module, M is an abelian group with an action of $F[x]$ on M. Since $F \subset F[x]$, this action can be restricted to F, leading to a scalar multiplication which makes M into an F-vector space. Also for any $m, m' \in M$, $a \in F$, $x \cdot (m + m') = xm + xm'$ and $x \cdot (am) = a(xm)$, so x can be viewed as a linear operator on the F-vector space M.

(b) If there were finitely many irreducible polynomials $f_1, f_2, \ldots, f_k$, then the polynomial $p = f_1 f_2 \cdots f_k + 1$ is an irreducible polynomial distinct from each f_i, which is a contradiction. hence, the claim holds.

Let $q = |F|$. Then there are q^k polynomials of degree k for each k. Let n be a positive integer. Then there are only finitely many irreducible polynomials in $F[x]$ of degree at most n and infinitely many irreducible polynomials in $F[x]$, so there exists an irreducible polynomial $p(x) \in F[x]$ of degree $m > n$.

View $F[x]$ as a module over itself. The submodules of $F[x]$ are precisely the ideals of $F[x]$. Since $p(x)$ is irreducible, the ideal ($F[x]$-submodule) $(p(x)) \subset F[x]$ is maximal. By the Fourth/Correspondence/Lattice Isomorphism Theorem, there are no proper, nontrivial submodules of $F[x]/(p(x))$, so $F[x]/(p(x))$ is a simple $F[x]$-module. A basis for $F[x]/(p(x))$ as a vector space over F is $\{\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{m-1}}\}$, so $F[x]/(p(x))$ has dimension $m > n$ as a vector space over F.

□

9. Let A be a square matrix over the complex numbers. Assume the characteristic polynomial of A is $(x-2)^4(x-3)^5$. Also assume that nullity $(A-2I) = 4$ and nullity $(A-3I) = 1$.

(a) What are the possible Jordan normal forms of A?

(b) For each possible Jordan normal form of A give its minimal polynomial.

Solution:

(a) The two eigenvalues of A are 2 and 3. Since nullity $(A-2I)$ is 4, there are four Jordan blocks corresponding to the eigenvalue 2. Since the power of $(x-2)$ in the characteristic polynomial is 4, each Jordan block is a 1×1 block. For the eigenvalue 3, since nullity $(A-3I) = 1$, there is only one Jordan block corresponding to the eigenvalue 3. This block must have size 5 since the power of $(x-3)$ in the characteristic polynomial is 5. Thus, there is only one possibility for the Jordan canonical form of A (up to the order of Jordan blocks), given below:

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

(b) Note that the elementary divisors of A are $(x-2)$ (with multiplicity 4) and $(x-3)^5$. The minimal polynomial is the product of the largest power of $(x-2)$ and the largest power of $(x-3)$ in the elementary divisors, which is $(x-2)(x-3)^5$. Thus, $m(x) = (x-2)(x-3)^5$.

□

10. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic polynomial ($\mathbb{Q}$ is of course the rational numbers) and let F be the splitting field for $f(x)$ over $\mathbb{Q}$.

(a) Prove that the Galois group of F over $\mathbb{Q}$ is isomorphic to either S_3 or $\mathbb{Z}/3\mathbb{Z}$.

For (b) and (c) suppose that $f(x) = x^3 - x + 2$.

(b) Prove that $f(x)$ is irreducible over $\mathbb{Q}$.

(c) Still denoting by F the splitting field for $f(x)$ over $\mathbb{Q}$ decide which of the two possibilities in (a) for the Galois group of F over $\mathbb{Q}$ is the vase for this $f(x)$.

Solution:

(a) Since f is an irreducible polynomial and $\mathbb{Q}$ has characteristic 0, f is separable. Let $G = \text{Gal}(F/\mathbb{Q})$ denote the Galois group of F over $\mathbb{Q}$. Since F is the splitting field of a separable polynomial, $|G| = [F : \mathbb{Q}]$. Let α_1, α_2, and α_3 denote the roots of f. Since $\mathbb{Q}(\alpha_1) \subset F$ and $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$, it follows that $[F : \mathbb{Q}] \geq 3$. Note that if $\sigma \in G$, $\sigma(\alpha_i)$ is a root of f for $i = 1, 2, 3$. Therefore, there exists an action of G on the three roots of f which induces a homomorphism $\phi : G \to S_3$. If $\sigma \in \ker \phi$, then $\sigma(\alpha_i) = \alpha_i$ for $i = 1, 2, 3$. Since F is generated by $\mathbb{Q}, \alpha_1, \alpha_2$, and α_3, this implies that σ is the identity on F. Hence, $\ker \phi = \{1\}$ and ϕ is an injection. This implies that G is isomorphic to a subgroup of S_3, so $|G| = 3$ or $|G| = 6$ by Lagrange's Theorem. If $|G| = 3$, then $G \cong \mathbb{Z}/3\mathbb{Z}$. If $|G| = 6$, then $G \cong S_3$.

(b) Since f has degree 3, f is irreducible if and only if f has no rational roots. By the Rational Roots Theorem, the only possible rational roots are $\pm 1, \pm 2$. However, $f(\pm 1) = 2$ and $f(2) = 8$, $f(-2) = -4$. Hence, f has no rational roots and is irreducible over $\mathbb{Q}$.

(c) The claim is that f has only one real root. It is clear that there is at least one. If $0 \leq x \leq 1$, $x^3 - x + 2 \geq x^2 - 1 + 2 = x^3 + 1 > 0$. If $x \geq 1$, then $x^3 \geq x$ and $x^3 - x + 2 \geq 2 > 0$. If $-1 \leq x \leq 0$, then $x^3 - x + 2 \geq (-1)^3 - 0 + 2 = 1 > 0$. Finally, if $x < -1$, then $f'(x) = 3x^2 - 1 \geq 3 - 1 = 2$, so f is strictly increasing when $x < -1$. Hence f will have exactly one real root, as claimed.

Let α denote the unique real root of f. Then $\mathbb{Q}(\alpha) \subset \mathbb{R}$ cannot be the splitting field of f over $\mathbb{Q}$. Hence, $\mathbb{Q}(\alpha) \subsetneq F$ and

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha : \mathbb{Q}] = 3\,[F : \mathbb{Q}(\alpha)] > 3$$

so $[F : \mathbb{Q}] = 6$ and $\text{Gal}(F/\mathbb{Q}) \cong S_3$.

□

January 2007

1. Let G be a finite group having exactly one nontrivial proper subgroup. Prove that G is cyclic of order p^2 for some prime number p.

Solution: Let H denote the one nontrivial, proper subgroup of G and consider $g \in G \setminus H$. Then $\langle g \rangle$ is a nontrivial subgroup of G (since $g \neq 1$) distinct from H. Therefore, $\langle g \rangle = G$ and G is cyclic. Let $n = |G|$. Then G contains a subgroup of order d for every d that divides n. This implies that n is a number with exactly order d for every d that divides n. This implies that n is a number with exactly one divisor other than 1 and n. This immediately rules out the possibility that n is prime and the possibility that n has more than one prime divisor. Therefore, $n = p^k$ for some prime $p \in \mathbb{N}$, $k \in \mathbb{N}$, $k > 1$. If $k > 2$, then p and p^2 are divisors of $p^k = n$, contrary to the choice of n. Thus, $n = p^2$ for some prime p, as desired. □

2. Let G be a finite group having n distinct conjugacy classes.

(a) Prove the identity $\sum_{x \in G} |C(x)| = n|G|$.

(b) Compute the probability that two randomly chosen elements of G commute. The random selection is done "with replacement" so that choosing the same element twice is a possible outcome.

Solution:

(a) Let G act on itself by conjugation. The orbits of this action are the conjugacy classes of G. The stabilizer of any $g \in G$ is $C(x)$, the centralizer of x. Let $\mathcal{O}_x$. denote the conjugacy class of x. The Orbit-Stabilizer Theorem implies that

$$|\mathcal{O}_x| = [G : C(x)] = \frac{|G|}{|C(x)|},$$

which implies that $|C(x)| = \dfrac{|G|}{|\mathcal{O}_x|}$. Therefore,

$$\begin{aligned} \sum_{x \in G} |C(x)| &= \sum_{x \in G} \frac{|G|}{|\mathcal{O}_x|} \\ &= |G| \sum_{x \in G} \frac{1}{|\mathcal{O}_x|}. \end{aligned}$$

Now let $x_1, x_2, \ldots, x_n$ be representatives of the n distinct conjugacy classes of G. In the sum above, $1/\mathcal{O}_x$ is counted for every element of $\mathcal{O}_x$. Hence, it is counted a total of

$|\mathcal{O}_x|$ times. This implies that

$$\sum_{x\in G}|C(x)| = |G| = \sum_{i=1}^{n}\frac{1}{|\mathcal{O}_{x_i}|}|\mathcal{O}_{x_i}| = |G|\sum_{i=1}^{n}1 = n|G|,$$

as desired.

(b) The probability is p/q, where q is the number of ways to choose two elements from the group G with replacement and p is the number of ways to choose two commuting elements of G with replacement. It is clear that $q = |G|^2$. If two elements $x, y \in G$ are chosen, then x and y commute if and only if $y \in C(x)$. Therefore, the total number of ways to choose two commuting elements is $\sum_{x\in G}|C(x)| = n|G|$. Thus,

$$\frac{p}{q} = \frac{n|G|}{|G|^2} = \frac{n}{|G|}$$

□

3. Let A be an $n \times n$ real matrix, and prove that the following (criteria for A to be orthogonal) are equivalent.

(a) $\|AX\| = \|X\|$ for all $X \in \mathbb{R}^n$

(b) $\langle AX, AY\rangle = \langle X, Y\rangle$ for all $X, Y \in \mathbb{R}^n$

(c) $A^TA = I_n$

Solution: Suppose (a) holds and let $X, Y \in \mathbb{R}^n$ be arbitrary. By (a), $\|A(X+Y)\|^2 = \|X+Y\|^2$. In other words, $\langle A(X+Y), A(X+Y)\rangle = \langle X+Y, X+Y\rangle$. The left hand side of this equation simplifies as

$$\begin{aligned}\langle A(X+Y), A(X+Y)\rangle &- \langle AX+AY, AX+AY\rangle \\ &= \langle AX, AX\rangle + 2\langle AX, AY\rangle + \langle AY, AY\rangle \\ &= \|AX\|^2 + 2\langle AX, AY\rangle + \|AY\|^2 \\ &= \|X\|^2 + 2\langle AX, AY\rangle + \|Y\|^2\end{aligned}$$

Also,

$$\langle X+Y, X+Y\rangle = \langle X, X\rangle + 2\langle X, Y\rangle + \langle Y, Y\rangle = \|X\|^2 + 2\langle X, Y\rangle + \|Y\|^2$$

Combining these leads to

$$\begin{aligned}\|X\|^2 + 2\langle AX, AY\rangle + \|Y\|^2 &= \|X\|^2 + 2\langle X, Y\rangle + \|Y\|^2 \\ 2\langle AX, AY\rangle &= 2\langle X, Y\rangle \\ \langle AX, AY\rangle &= \langle X, Y\rangle,\end{aligned}$$

as desired.

Assume that (b) holds, use the matrix notation $A^TA = (a_{ij})$. Let $\{e_i\}_{i=1}^n$ denote the standard basis for $\mathbb{R}^n$. Then

$$\langle Ae_i, Ae_j\rangle = (Ae_i)^T(Ae_j) = e_i^TA^TAe_j = a_{ij}.$$

Using (b), we have

$$\langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle = \begin{cases}1, & \text{if } i = j \\ 0, & \text{if } i \neq j.\end{cases}$$

Thus,

$$a_{ij} = \begin{cases}1, & \text{if } i = j \\ 0, & \text{if } i \neq j.\end{cases}$$

This implies that $A^TA = I_n$.

Now suppose (c) holds. Then for any $X \in \mathbb{R}^n$,

$$\|AX\|^2 = \langle AX, AX\rangle = (AX)^T(AX) = X^TA^TAX = X^TX = \langle X, X\rangle = \|X\|^2.$$

Since $\|AX\|$ and $\|X\|$ are both nonnegative, this implies that $\|AX\| = \|X\|$, as needed. □

4. Let G be a simple group of order 60. Prove that G has 10 Sylow 3-subgroups. (Do not use the fact that $G \cong A_5$.)

Solution: The divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60. Let $n_3(G)$ denote the number of 3-Sylow subgroups of G. By Sylow's Theorem, $n_3(G) \equiv 1 \mod 3$ and divides 20. The only possibilities are $n_3(G) = 1$, $n_3(G) = 4$, or $n_3(G) = 10$. If $n_3(G) = 1$, then G contains a unique 3-Sylow subgroup, which must be normal. Thus, G has a proper, nontrivial, normal subgroup, contrary to the assumption that G is simple.

Suppose $n_3(G) = 4$. Let S denote the set of 3-Sylow subgroups. Let G act on S by conjugation. This action is nontrivial since any two 3-Sylow subgroups are conjugate (by Sylow's Theorem). Therefore, this action induces a homomorphism $\phi : G \to S_4$ with $\ker\phi \neq G$. However, since $|G| = 60$ and $|S_4| = 4! = 24$, it is impossible for ϕ to be injective. Therefore, $|\ker\phi| > 1$. Thus, $\ker\phi$ is a proper, nontrivial subgroup of G. Since the kernel of a group homomorphism is a normal subgroup, this implies that G has a proper, nontrivial, normal subgroup, which again is a contradiction. Therefore, $n_3(G) = 10$, as desired. □

5. Let S_5 denote the symmetric group on five elements.

Cycle Type	Representative	Size of Conjugacy Class
(a b c d e)	(1 2 3 4 5)	$4! = 24$
(a b c d)	(1 2 3 4)	$\binom{5}{4}\, 3! = 30$
(a b c)	(1 2 3)	$\binom{5}{3}\, 2! = 20$
(a b c)(d e)	(1 2 3)(4 5)	$\binom{5}{3}\, 2! = 20$
(a b)(c d)	(1 2)(3 4)	$\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$
(a b)	(1 2)	$\binom{5}{2} = 10$
1	1	1

(a) Find a representative for each conjugacy class of S_5, and determine the number of elements in each class.

(b) Find all elements of S_5 that commute with the 4-cycle (1234). Justify your answer.

Solution:

(a) Note that two permutations in S_5 are conjugate if and only if they have the same cycle type. Note that $|S_5| = 120 = 24 + 30 + 20 + 20 + 15 + 10 + 1$.

(b) We need to compute $C((1234))$. In general, if G is a group acting on itself by conjugation, $x \in G$ and G_x is the stabilizer of G, then

$$G_x = \{g \in G \colon g \cdot x = x\}\{g \in G \colon gxg^{-1} = x\} = C(x).$$

Return to the situation where $G = S_5$. By the Orbit-Stabilizer Theorem, $[S_5 : C((1234))]$ is equal to the size of the conjugacy class containing (1234), i.e. $[S_5 : C((1234))] = 30$. Therefore, $|C((1234))| = \frac{120}{30} = 4$. Since (1234) has order 4, this implies that $C(1234) = \langle (1234) \rangle$, so the elements of S_5 that commute with (1234) are 1, (1234), $(1234)^2$, and $(1234)^3$, which are

$$\begin{aligned} &1 \\ &(1234)(1234) = (13)(24) \\ &(1234)^3 = (1234)(13)(24) = (1432). \end{aligned}$$

□

6. Let $\mathbb{Q}$ be the rational numbers.

(a) Find the minimal polynomial for $\sqrt{6} + \sqrt{10}$ over $\mathbb{Q}$. Be sure to prove that it is the minimal polynomial.

(b) What is the degree of the field extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt{6}+\sqrt{10}]$?

Solution:

(a) Observe that $(\sqrt{6}+\sqrt{10})^2 = 6+10+2\sqrt{6}\sqrt{10}$. Therefore,

$$\begin{aligned}(\sqrt{6}+\sqrt{10})^2 - 16 &= 2\sqrt{6}\sqrt{10}\\ ((\sqrt{6}+\sqrt{10})^2 - 16)^2 &= 4(6)(10)\\ (\sqrt{6}+\sqrt{10})^4 - 32(\sqrt{6}+\sqrt{10})^2 + 256 &= 240\\ (\sqrt{6}+\sqrt{10})^4 - 32(\sqrt{6}+\sqrt{10})^2 + 16 &= 0\end{aligned}$$

Therefore, $\sqrt{6}+\sqrt{10}$ is a root of the polynomial $m(x) = x^4 - 32x^2 + 16$. To show that $m(x)$ is the minimal polynomial of $\sqrt{6}+\sqrt{10}$ over $\mathbb{Q}$, it suffices to prove that $m(x)$ is irreducible over $\mathbb{Q}$. By Gauss' Lemma, it is sufficient to prove that $m(x)$ is irreducible over $\mathbb{Z}$. Write $m(x) = x^4 - 2^5x^2 + 2^4$. By the Rational Roots Theorem, the only possible rational roots are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16$. However, none of these are a zero of $m(x)$.

The only other possibility for $m(x)$ to be reducible is that $m(x)$ is a product of irreducible quadratics. Suppose that $m(x) = (x^2+ax+b)(x^2+cx+d) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$ for some $a, b, c, d \in \mathbb{Z}$. Comparing the constant term yields $bd = 16$. The only possibilities are $b = 2, d = 8$ or $b = -2, d = -8$ or $b = 4, d = 4$ or $b = -4, d = -4$. Comparing the x^3 terms yields $a = -c$. Comparing the x^2 terms yields $d + b - c^2 = -32$, so $c^2 = d + b + 32$. All of these yield a contradiction. For example in the first case, $b = 4, d = 4$, we would then have $c^2 = 2 + 8 + 32 = 42$, a contradiction since 42 is not a perfect square. The other cases are handled the same way. But then $m(x)$ must be an irreducible polynomial.

(b) Since the minimal polynomial of $\sqrt{6}+\sqrt{10}$ over $\mathbb{Q}$ has degree 4, the extension must also have degree 4.

□

7. Let $F \subset K \subset L$ be a tower of field extensions. Provide either a proof or a counterexample for the following statement: If $F \subset K$ and $K \subset L$ are both Galois extensions then $F \subset L$ is a Galois extension.

Solution: The statement is false. Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, and $L = \mathbb{Q}(\sqrt[4]{2})$. Then $K \subset K$ is Galois since K is the splitting field of the separable polynomial $p(x) = x^2 - 2 \in F[x]$. Also, $K \subset L$ is Galois since L is the splitting field of the separable polynomial $q(x) = x^2 - \sqrt{2} \in K[x]$. The polynomial $m(x) = x^4 - 2 \in F[x]$ has a root in L (namely, $\sqrt[4]{2}$). However, $m(x) = (x+\sqrt[4]{2})(x-\sqrt[4]{2})(x^2+\sqrt{2})$ does not split completely since $x^2 + \sqrt{2}$

has no real roots and $L \subset \mathbb{R}$. This implies that $F \subset L$ is not a Galois extension. $\square$

8. Let R be a commutative ring with identity and let I and J be ideals of R. Prove: if $I + J = (1)$ then $IJ = I \cap J$.

Solution: Note that IJ is an ideal generated by products of the form xy, where $x \in I$ and $y \in J$. Since I and J are both ideals, it is clear that every such product is contained in $I \cap J$. Therefore, $IJ \subset I \cap J$. Now since $1 \in I + J$, there exist $a \in I$ and $b \in J$ such that $1 = a + b$. For any $c \in I \cap J$, $c = c \cdot 1 = c(a + b) = ca + cb$. Since $a \in I$, $c \in J$, $ca \in IJ$ and $b \in J$, $c \in I$, $cb \in IJ$. Therefore, $ca + cb = c \in IJ$. Thus, $I \cap J \subset IJ$. Therefore, $IJ = I \cap J$. $\square$

9. Let A be a square matrix over the complex numbers. Assume that the minimal polynomial of A is $(x-2)^2$ and the characteristic polynomial of A is $(x-2)^5$.

(a) Give all the possible Jordan canonical forms for such an A.

(b) For each of the possibilities in (a) compute the nullity of $(A - 2I)^k$ for all positive integers k. (I is the identity matrix of the same size as A.)

Solution:

(a) First, the possible invariant factors are:

$$(x-2), (x-2), (x-2), (x-2)^2$$
$$(x-2), (x-2)^1, (x-2)^2$$

In each case, the elementary divisors are the same as the invariant factors. In the first case, the Jordan canonical form is, up to permutation of the Jordan blocks,

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

In the second case, the Jordan canonical form is, up to permutation of the Jordan blocks,

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

(b) The nullity of $(A - 2I)$ is the number of Jordan blocks corresponding to the eigenvalue 2. In the first case, there are 4 Jordan blocks, so the nullity of $(A - 2I)$ is 4. The difference fo the nullity $(A - 2I)^2-$ nullity $(A - 2I)$ is the number of Jordan blocks of at least size 2. Since there is only one such block, nullity $(A - 2I)^2 - 4 = 1$, so nullity $(A - 2I)^2 = 5$. Since there are no Jordan blocks of at least size 3, nullity $(A - 2I)^k = 5$ for all $k \geq 3$.

In the second case, there are 3 Jordan blocks, so nullity $(A - 2I) = 3$. There are 2 blocks of at least size 2, so nullity $(A - 2I)^2 - 3 = 2$. Thus, nullity $(A - 2I)^2 = 5$. Since there are no Jordan blocks of at least size 3, nullity $(A - 2I)^k = 5$ for all $k \geq 3$.

□

10. An abelian group is generated by w, x, y, and z subject to the relations: $w + 3x + 3y + 5z = 0$, $w + x + y + y = 0$, $2x + 2y + 2z = 0$, and $3z = 0$. Express what group that is in each of the two ways that appear in the structure theorem for finitely generated abelian groups.

Solution: The generators satisfy the relations

$$\begin{aligned} w + 3x + 3y + 5z &= 0 \\ w + x + y + 0z &= 0 \\ 0w + 2x + 2y + 2z &= 0 \\ 0w + 0x + 0y + 3z &= 0 \end{aligned}$$

The coefficient matrix for this system of equations is then

$$\begin{pmatrix} 1 & 3 & 3 & 5 \\ 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Performing the following row/column operations

$$\begin{aligned}
-R_1 + R_2 &\longrightarrow R_2 \\
R_2 + R_3 &\longrightarrow R_3 \\
R_3 + R_4 &\longrightarrow R_4 \\
-C_2 + C_3 &\longrightarrow C_3 \\
-2C_2 + C_4 &\longrightarrow C_4 \\
-3C_1 + C_2 &\longrightarrow C_2 \\
-2C_1 + C_4 &\longrightarrow C_4 \\
-R_3 + R_2 &\longrightarrow R_2 \\
C_3 &\longleftrightarrow C_4 \\
-C_3 &\longrightarrow C_3 \\
-C_4 &\longrightarrow C_4
\end{aligned}$$

yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Thus,

$$A \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2 \ \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$$

The above is the elementary divisor decomposition of A. By the Chinese Remainder Theorem, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, this gives the invariant factor decomposition $A \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$. □

August 2007

1. Let G be a group of order p^2 for some prime number p. Prove that G is abelian.

Solution: Let $Z(G)$ denote the center of G. Consider the class equation for G:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_i]$$

where C_i denotes the stabilizer of some $x \in \mathcal{O}_i$ for every distinct orbit $\mathcal{O}_i$ which contains more than one element (for otherwise the element is in the center). In particular, $[G : C_i] > 1$ and divides p^2 for each i. Therefore, p divides $[G : C_i]$ for each i. This also implies that p divides $|Z(G)|$. Since $|Z(G)|$ divides $|G|$, there are then two possibilities: $|Z(G)| = p^2$ or $|Z(G)| = p$. If $|Z(G)| = p^2$, then $G = Z(G)$ and G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$ so that $G/Z(G)$ must by cyclic. But then G is abelian. □

2. Prove that a finite group of order 24 is not simple.

Solution: The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24. By Sylow's Theorem $n_2(G) \equiv 1 \mod 2$ and divides 24. The only possibilities are $n_2(G) = 1$ or $n_2(G) = 3$. If $n_2(G) = 1$, then G contains a unique 2-Sylow subgroup, which is necessarily normal. This implies that G has a nontrivial, proper, normal subgroup. Thus, G is not simple.

Suppose that $n_2(G) = 3$. Let X denote the set of 2-Sylow subgroups. Note that G acts on X by conjugation. This induces a homomorphism $\phi : G \to S_X$. Since $|G| = 24$ and $|S_X| = 3! = 6$, ϕ is not injective. Therefore, $|\ker \phi| > 1$. Note that $|\ker \phi| \neq 24$ since any two 2-Sylow subgroups are conjugate (so they all can not be fixed by the action of conjugation). Thus, $\ker \phi$ is a proper, nontrivial, normal subgroup of G, which implies that G is not simple. □

3. Let $H \subset K \subset G$ be groups. Prove that H is normal in K if and only if $K \subset N_G(H)$ where $N_G(H)$ is the normalizer of H in G.

Solution: Suppose that H is normal in K and that $x \in K$. Then $xHx^{-1} \subset H$, which implies that $x \in N_G(H)$. Therefore, $K \subset N_G(H)$. Now suppose that $K \subset N_G(H)$. Then for any $x \in K$, $xHx^{-1} \subset H$, which implies that H is normal in K. □

4. Let $T : \mathbb{C}^n \to \mathbb{C}^n$ be a linear operator. Prove that $\ker T = (\operatorname{im} T^*)^\perp$, where the orthogonal complement is taken with respect to the usual Hermitian inner product on $\mathbb{C}^n$.

Solution: Suppose $x \in \ker T$, then for all $y \in \mathbb{C}^n$, $\langle T^*y, x\rangle = \langle x, Tx\rangle = \langle y, 0\rangle = 0$. Therefore, $x \in (\operatorname{im} T^*)^\perp$ and $\ker T \subset (\operatorname{im} T^*)^\perp$. Suppose that $x \in (\operatorname{im} T^*)^\perp$. Then for all $y \in \mathbb{C}^n$, $0 = \langle T^*y, x\rangle = \langle y, Tx\rangle$. In particular, $\langle Tx, Tx\rangle = 0$, so $Tx = 0$. This implies that $x \in \ker T$,

so $\ker T = (\operatorname{im} T^*)^\perp$. $\square$

5. Let A be an $n \times n$ real matrix with transpose A^T, and prove that the following (criteria for A to be orthogonal) are equivalent.

1. $\|AX\| = \|X\|$ for all $X \in \mathbb{R}^n$, where $\| \cdot \|$ is the usual norm on $\mathbb{R}^n$;

2. $\langle AX, AY \rangle = \langle X, Y \rangle$ for all $X, Y \in \mathbb{R}^n$, where $\langle \cdot, \cdot \rangle$ is the usual inner product on $\mathbb{R}^n$;

3. $A^T A = I_n$, the $n \times n$ identity matrix.

Solution: Suppose that (1.) holds. Then $\langle AX, AX \rangle = \|AX\|^2 = \|X\|^2 = \langle X, X \rangle$ for all $X \in \mathbb{R}^n$. If $X, Y \in \mathbb{R}^n$, then

$$\langle A(X+Y), A(X+Y) \rangle = \langle X+Y, X+Y \rangle = \langle X, X \rangle + 2\langle X, Y \rangle + \langle Y, Y \rangle.$$

On the other hand,

$$\begin{aligned} \langle A(X+Y), A(X+Y) \rangle &= \langle AX + AY, AX + AY \rangle \\ &= \langle AX, AX \rangle + 2\langle AX, AY \rangle + \langle AY, AY \rangle \\ &= \langle X, X \rangle + 2\langle AX, AY \rangle + \langle Y, Y \rangle. \end{aligned}$$

Combining these yields

$$\langle X, X \rangle + 2\langle X, Y \rangle + \langle Y, Y \rangle = \langle X, X \rangle + 2\langle AX, AY \rangle + \langle AY, AY \rangle$$

so that $2\langle X, Y \rangle = 2\langle AX, AY \rangle$ so that $\langle X, Y \rangle = \langle AX, AY \rangle$.

Now suppose that (2.) holds. Observe that for $X, Y \in \mathbb{R}^n$, $\langle AX, AY \rangle = (AX)^T (AY) = X^T A^T AY$. Let $\{e_i\}_{i=1}^n$ denote the standard basis for $\mathbb{R}^n$ and write $A^T A = (a_{ij})$. Then

$$\langle Ae_i, Ae_j \rangle = e_i^T A^T A e_j = a_{ij} = \langle e_i, e_j \rangle = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}.$$

Thus, $A^T A = I_n$.

Finally, suppose that (3.) holds. Then for any $X \in \mathbb{R}$,

$$\|AX\|^2 = \langle AX, AX \rangle = (AX)^T (AX) = X^T A^T AX = X^T X = \langle X, X \rangle = \|X\|^2.$$

Since $\|AX\| \geq 0$ and $\|X\| \geq 0$, this implies that $\|AX\| = \|X\|$, as desired. $\square$

6. Let $\mathbb{Q}$ be the rational numbers. Prove the degree of the field extension $[\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) : \mathbb{Q}]$ equals 4 and not 8.

Solution: Now that $\sqrt{6}\sqrt{10} = 2\sqrt{15}$. Therefore, $\sqrt{15} = \frac{1}{2}\sqrt{6}\sqrt{10} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$. Thus, $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$. Consider the extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \sqrt{10})$. The minimal polynomial of $\sqrt{6}$ over $\mathbb{Q}$ is $m(x) = x^2 - 6$. This polynomial is irreducible over $\mathbb{Q}$ using Eisenstein's criterion with $p = 3$ (or $p = 2$). Therefore, $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$ and

$$[\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}, \sqrt{10} : \mathbb{Q}(\sqrt{6})]\,[\mathbb{Q}(\sqrt{6} : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{6})].$$

It remains to show that $[\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{6})] = 2$. Note that $\sqrt{10}$ is a root of the polynomial $p(x) = x^2 - 10 = (x + \sqrt{10})(x - \sqrt{10})$. If $p(x)$ is reducible over $\mathbb{Q}(\sqrt{6})$, then $\sqrt{10} \in \mathbb{Q}(\sqrt{6})$. This implies that there exist $a, b \in \mathbb{Q}$ such that $\sqrt{10} = a + b\sqrt{6}$. Squaring yields $10 = a^2 + 6b^2 + 2ab\sqrt{6}$. Now $2ab = 0$, so either $a = 0$ or $b = 0$. If $a = 0$, then $6b^2 = 10$ so $b^2 = \frac{5}{3}$, impossible since $b \in \mathbb{Q}$. If $b = 0$, then $a^2 = 10$, which is impossible since $a \in \mathbb{Q}$. Therefore, $\sqrt{10} \notin \mathbb{Q}(\sqrt{6})$, implying $p(x)$ is irreducible over $\mathbb{Q}(\sqrt{6})$. Thus, $[\mathbb{Q}(\sqrt{6}, \sqrt{10} : \mathbb{Q}(\sqrt{6})] = 2$ and $[\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15} : \mathbb{Q}] = 2 \cdot 2 = 4 \neq 8$, as desired. □

7. Let $K \subset L$ be a finite field extension, and let f be an irreducible polynomial with coefficients in K. Assume that the degree of f, and $[L : K]$ are relatively prime. Prove that f has no roots in L.

Solution: Without loss of generality, it may be assumed that f is monic. Assume that there exists $\alpha \in L$ such that $f(\alpha) = 0$. Then $K \subset K(\alpha) \subset L$ and $[L : K] = [L : K(\alpha)]\,[K : (\alpha) : K]$. Since f is irreducible and monic, f is the minimal polynomial of α over K. Therefore, $[K(\alpha) : K] = \deg f$ and $\deg f$ divides $[L : K]$. Thus, the greatest common divisor of the degree of f and $[L : K]$ is the degree of f. This contradicts the assumption that the degree of f and $[L : K]$ are relatively prime. Thus, f has no roots in L. □

8. Let R be a commutative ring with identity and let I and J be ideals of R. Prove: if $I + J = R$ then we also have $I^2 + J^3 = R$.

Solution: It suffices to show that $1 \in I^2 + J^3$. Since $1 \in I + J$, there exist $a \in I, b \in J$ such that $1 = a + b$. Using the Binomial Theorem,

$$1 = 1^4 = (a + b)^4 = a^4 + 4 \cdot a^3 b + 6 \cdot a^2 b^2 + 4 \cdot ab^3 + b^4$$

where $n \cdot x$ denotes the n-fold sum of x with itself. Since $a \in I$ and I^2 is an ideal, $a^4, a^3 b, a^2 b^2 \in I^2$. Similarly, $ab^3, b^4 \in J^3$. Then 1 is a sum of elements from I^2 and J^3, implying $1 \in I^2 + J^3$. Thus, $I^2 + J^3 = R$. □

9. Let R be a commutative ring and let M be a cyclic R-module, that is, M is generated by a single element. Prove that there exists an ideal I in R such that $M \cong R/I$.

Solution: By assumption, there exists $x \in M$ such that $M = Rx$. Therefore, there is a natural R-module homomorphism $\phi : R \to M$ given by $r \mapsto rx$. To show that ϕ is a homomorphism, let $r, s \in R$. Then

$$\begin{aligned} \phi(r+s) &= (r+s)x = rx + sx = \phi(r) + \phi(s) \\ \phi(rs) &= (rs)x = r(sx) = r\phi(s) \end{aligned}$$

Therefore, ϕ is a homomorphism. It is clear that ϕ is surjective (since $1 \in R$). By the First Isomorphism Theorem, $R/\ker\phi \cong M$. Now $\ker\phi$ is a submodule of R. But the submodules of R are precisely ideals. Taking $\ker\phi = I$, completing the proof. □

10. Let A

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$$

be the presentation matrix for the abelian group X, that is we have the presentation

$$\mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^3 \longrightarrow X \longrightarrow 0$$

Find a direct sum of cyclic groups which is isomorphic to X.

Solution: Perform the following row/column operations

$$\begin{aligned} R_3 - R_1 &\longrightarrow R_3 \\ R_2 - R_2 &\longrightarrow R_2 \\ -R_2 &\longrightarrow R_2 \\ -R_3 &\longrightarrow R_3 \\ R_2 &\longleftrightarrow R_3 \\ R_1 - R_2 &\longrightarrow R_1 \\ R_1 - R_3 &\longrightarrow R_1 \end{aligned}$$

which yields

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Thus, $X \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

January 2008

1. Let G, H be cyclic groups generated by elements x, y of finite orders m, n respectively.

(a) Determine the necessary and sufficient condition on m, n so that sending x^i to y^i, for all $i \in \mathbb{Z}$, is a well-defined homomorphism of groups.

(b) Describe all homomorphisms of the cyclic group of order 6 into the cyclic group of order 24.

Solution:

(a) Let $\phi : G \to H$ be defined by $\phi(x^i) = y^i$. Then $\phi(x^m) = \phi(1) = 1 = \phi(x)^m$. Since H has order n, n divides m. It is clear that this condition is necessary. We claim this condition is also sufficient.

Suppose that n divides m. We need show that ϕ is well-defined. If $x^i = x^j$ for some $i, j \in \mathbb{Z}$, then $j = i + mk$ for some $k \in \mathbb{Z}$. This implies that $\phi(x^i) = y^i = y^{j+mk} = y^j y^{mk} = y^j (y^m)^k = y^j = \phi(x^j)$. Thus, ϕ is well-defined. Notice that ϕ is a homomorphism since for any $i, j \in \mathbb{Z}$, $\phi(x^i x^j) = \phi(x^{i+j}) = y^{i+j} = y^i y^j$. Therefore, it is necessary and sufficient that n divide m.

(b) Let $C_6 = \langle x \rangle$ be the cyclic group of order 6 and $C_{24} = \langle y \rangle$ be the cyclic group of order 24. If $\phi : C_6 \to C_{24}$ is a homomorphism, then $\phi(x)$ generates a cyclic subgroup of C_{24}, which has order at most 6. Furthermore since ϕ is a homomorphism, $\phi(x^i) = \phi(x)^i$. By the previous part, this means that ϕ is well-defined if and only if $|\phi 9x)|$ divides $|C_6| = 6$, i.e. if $\phi(x)^6 = 1$. This implies that $\phi(x) \in \{1, y^4, y^8, y^{12}, y^{16}, y^{20}\}$. Thus, there are 6 such homomorphisms.

□

2. Given a subgroup K of a group G, the set S of left cosets of K in G is a left G-set by means of $g \cdot xK = gxK$, for all $g, x \in G$. If H is another subgroup of G, then S is a left H-set by restriction. Recall that the set $HxK = \{y \in G : y = hxk \text{ for some } h \in H, k \in K\}$ is called a *double coset*. For any set X, $|X|$ denotes the cardinality of X.

(a) Prove that the orbit of the element xK of the H-set S is the set of left cosets of K in G contained in the double coset HxK and compute the stabilizer of xK.

(b) Prove that the double cosets form a partition of G.

In the rest of the problem, assume $|G| < \infty$.

(c) Prove that $|HxK| = |K|\,[H : H \cap xKx^{-1}] = |H|\,[K : K \cap x^{-1}Hx]$.

(d) Do all double cosets have the same cardinality? If yes, give a proof; if no, give a counterexample.

Solution:

(a) Let $\mathcal{O}(xK)$ denote the orbit of xK in S. Then

$$\mathcal{O}(xK) = \{h \cdot xK \colon h \in H\} = \{hxK \colon h \in H\}.$$

This shows that $\mathcal{O}(xK)$ is a subset of the set of left cosets of K contained in HxK. If aK is a coset contained in HxK, then $aK \subset HxK$. In particular, $a = hxk$ for some $h \in H$, $k \in K$, so $h \cdot xK = hxK = hxkK = aK$. This shows that $aK \in \mathcal{O}(xK)$. This proves that $\mathcal{O}(xK)$ is equal to the set of left cosets of K in G contained in HxK. Note that $a \cdot xK = xK$ if and only if $x^{-1}ax \in K$, which is true if and only if $a \in xKx^{-1}$. Therefore, the stabilizer of xK in H is $H \cap xKx^{-1}$.

(b) Define a relation on G by $x \sim y$ if and only if $x \in HyK$. We claim that this is an equivalence relation.

- $x = 1x1 \in HxK$ for all $x \in G$, so $x \sim x$ for all $x \in G$
- If $x \sim y$, then $x \in HyK$ so $x = hyk$ for some $h \in H$, $k \in K$. Then $y = h^{-1}xk^{-1} \in HxK$ so $y \sim x$
- If $x \sim y$, $y \sim z$, then $x \in HyK$ so $x = hyk$ for some $h \in H$, $k \in K$. Similarly, $y = h'zk'$ for some $h' \in H$, $k' \in K$. Then $x = hyk = hh'zk'k \in HzK$ so $x \sim z$

This proves that $\sim$ is an equivalence relation. Notice the equivalence classes of $\sim$ are the double cosets HxK for $x \in G$. This implies that the double cosets form a partition of G, as desired.

(c) By part (a), the orbit of xK is the set of left cosets of K contained in HxK. By the Orbit-Stabilizer Theorem, there are $[H : H \cap xKx^{-1}]$ elements of $\mathcal{O}(xK)$, i.e. $[H : H \cap xKx^{-1}]$ cosets of K contained in HxK. Furthermore, every element of HxK is contained in one of these cosets of K. Since the cardinality of all left cosets of K is $|K|$,

$$|HxK| = |K|\,[H : H \cap xKx^{-1}].$$

The equality $|HxK| = |H|\,[K : x^{-1}Hx]$ is obtained by letting K act on the set of right cosets Hx for $x \in G$ (via $Hx \cdot y = Hxy$ for $y \in K$) and repeating parts (a) and (b) above.

(d) Not all double cosets have the same cardinality. Consider $G = S_3$, $H = \langle(12)\rangle$, $K = \langle(13)\rangle$, $x = (23)$, and $y = (123)$. Then

$$HxK = \{(23), (123)\}$$
$$HyK = \{(123), (132), (13), (12)\}$$

So $2 = |HxK| \neq |HyK| = 4$.

□

3. Prove that if a group has order $p^e a$ where p is a prime, $1 \leq a < p$, and $e \geq 1$, then the group has a proper normal subgroup.

Solution: Let G be a group of order $p^e a$, where p, e, and a are given above. The divisors of p are $1, p, p^2, \ldots, p^{e-1}, p^e, \ldots, pa, p^2a, \ldots, p^{e-1}a, p^e a$. Let $n_p(G)$ denote the number of p-Sylow subgroups of G. By Sylow's Theorem, $n_p(G) \equiv 1 \mod p$ and divides $|G| = p^e a$. Now p does not divide $n_p(G)$, so the only possibilities are $n_p(G) = 1$ or $n_p(G) = a$. However, if $1 < a < p$, then a is not congruent to $1 \mod p$ (since $a - 1$ cannot be divisible by p), so the only possibility is $n_p(G) = 1$. Thus, G has a unique p-Sylow subgroup. This unique p-Sylow subgroup is a normal subgroup of order p^e. Thus, G contains a proper, nontrivial, normal subgroup. □

4. Let A be a square matrix over the field $\mathbb{C}$ of complex numbers.

(a) Prove that the matrix is invertible if and only if all of its eigenvalues are different from zero.

(b) Prove that the matrix is nilpotent if and only if zero is its only eigenvalue. Recall that a square matrix B is called *nilpotent* if $B^m = 0$ for some positive integer m.

(c) Prove that if A is nilpotent, it is similar to an upper triangular matrix with diagonal entries zero. Recall that matrix X and Y are called *similar* if $X = CYC^{-1}$ for some invertible matrix C.

Solution:

(a) Suppose that A is an invertible $n \times n$ matrix. Then the linear operator on $\mathbb{C}^n$ defined by multiplication by A has a trivial kernel. Therefore, there are no nonzero vectors $v \in \mathbb{C}^n$ satisfying $Av = 0v = 0$. Thus, 0 is not an eigenvalue of A.

Suppose all the eigenvalues of A are nonzero. Note that A is invertible if and only if $Av \neq 0$ for all nonzero $Av \neq 0$ for all nonzero $v \in \mathbb{C}^n$. Since 0 is not an eigenvalue of A, the latter condition is satisfied.

(b) Suppose that A is an $n \times n$ matrix and assume A has a nonzero eigenvalue λ. Then there exists a nonzero $v \in \mathbb{C}^n$ such that $Av = \lambda v$. For any $m \in \mathbb{N}$, $A^m v = \lambda^m v$, which is nonzero since λ^m and v are both nonzero. Therefore, A is not nilpotent.

Suppose that the only eigenvalue of A is zero. Since A is a matrix over the complex numbers, its characteristic polynomial splits. This implies that the characteristic polynomial of A is $c_A(x) = x^n$. Therefore, $c_A(A) = A^n = 0$ and A is nilpotent.

(c) Assume that A is nilpotent. Since $c_A(x) = x^n$, every elementary divisor of A is of the form x^k, where $k \leq n$. The Jordan block corresponding to the elementary divisor x^k is a $k \times k$ matrix of the following form:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Therefore, the Jordan canonical form of A is an upper triangular matrix with zeros along the diagonal. Since A is similar to its Jordan canonical form, the result follows.

□

5. Let A be a real symmetric $n \times n$ matrix, and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be the linear operator on the Euclidean space $\mathbb{R}^n$ given by $T(X0 = AX$, for all column vectors $X \in \mathbb{R}^n$.

(a) Prove that every vector in $\ker T$ is orthogonal vector in $\operatorname{im} T$.

(b) Prove that $\mathbb{R}^n = \ker T \oplus \operatorname{im} T$.

(c) Prove that T is an orthogonal projection onto $\operatorname{im} T$ if and only if A, in addition to being symmetric, satisfies $A^2 = A$. Recall that for any subspace $W \subset \mathbb{R}^n$, the equality $\mathbb{R}^n = W \oplus W^\perp$ says that every vector $v \in \mathbb{R}^n$ can be uniquely written as $v = w + w'$, where $w \in W$ and $w' \in W^\perp$. The linear operator on $\mathbb{R}^n$ sending v to w, for all v, is called the *orthogonal projection* onto W.

Solution:

(a) Let $x \in \ker T$, $y \in \mathbb{R}^n$. Then $\langle x, Ay\rangle = x^T Ay$ and $\langle Ax, y\rangle = (Ax)^T y = x^T A^T y = x^T Ay = \langle x, Ay\rangle$. Therefore, $\langle x, Ay\rangle = \langle Ax, y\rangle = \langle 0, y\rangle = 0$, i.e. every vector in $\ker T$ is orthogonal to every vector in $\operatorname{im} T$.

(b) By the previous part, if $v \in \ker T \cap \operatorname{im} T$, then $\langle v, v\rangle = 0$, so $v = 0$. Thus, $\ker T \cap \operatorname{im} T = 0$. By the Rank-Nullity Theorem, $\dim \ker T + \dim \operatorname{im} T = n$. Therefore,

$$\dim(\ker T + \operatorname{im} T) = \dim \ker T + \dim \operatorname{im} T - \dim(\ker T \cap \operatorname{im} T) = n.$$

Thus, $\ker T + \operatorname{im} T = \mathbb{R}^n$ and $\ker T \cap \operatorname{im} T = 0$. Therefore, $\mathbb{R}^n = \ker T \oplus \operatorname{im} T$.

(c) Suppose T is an orthogonal projection onto $\operatorname{im} T$. Let $y \in \mathbb{R}^n$ be arbitrary and let $x \in \ker T$. Then $T(x + Ty) = Ty$ since T is an orthogonal projection onto $\operatorname{im} T$. On the

other hand, $T(x+Ty) = Tx + T^2y = 0 + T^2y = T^2y$. Thus, $T^2y = T(x+Ty) = Ty$ and $A^2y = Ay$ for every $y \in \mathbb{R}^n$. Therefore, $A^2 = A$.

Suppose that $A^2 = A$. For $v \in \mathbb{R}^n$, write $v = a + b$, where $a \in \ker T$, $b \in \operatorname{im} T$. Then $b = Tw$ for some $w \in \mathbb{R}^n$. Clearly, $v = a + Tw = a + Aw$. Now $Tv = T(a) + T(Aw) = 0 + T(Aw) = A(Aw) = A^2w = Aw = Tw$. Then T is the orthogonal projection onto $\operatorname{im} T$.

□

6. Let $\mathbb{Z}[x]$ be the ring of polynomials in one variable with coefficients in the integers. Let $(3, x) = M \subset \mathbb{Z}[x]$ be the ideal generated by 3 and x. Prove that M is a maximal ideal.[3]

Solution: If $p(x) \in M$, $p(x) = 3q(x) + xr(x)$ for some $p(x), r(x) \in \mathbb{Z}[x]$. This implies that $p(x) = 3k + s(x)$ for some $s(x) \in x\mathbb{Z}[x]$. Conversely, every element of this form is contained in M. Suppose I is an ideal in $\mathbb{Z}[x]$ properly containing M. Consider $f(x) \in I \setminus M$. Let a be the constant term of f and let $g(x) = f(x) - a$. Observe that $g(x) \in (x) \subset M \subset I$, which implies that $a \in I$. By the remarks above, a is not a multiple of 3. Observe that $3k \in (3) \subset M \subset I$. If $a = 3k + 1$, then $1 = a - 3k \in I$, which implies $I = \mathbb{Z}[x]$. If $a = 3k + 2$, then $2 = a - 3k \in I$, so $3 - 2 = 1 \in I$. Thus, $I = \mathbb{Z}[x]$. But then M is maximal.

OR

Define a map $\phi : \mathbb{Z}[x] \to \mathbb{Z}/3\mathbb{Z}$ given by $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto a_0 \mod 3$, i.e. evaluation at 0 modulo 3 ($p(0) \mod 3$). If $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and

[3] All the maximal ideals of $\mathbb{Z}[x]$ are of the form $(p, f(x))$, where p is a prime and $f(x)$ is a polynomial in $\mathbb{Z}[x]$ which is irreducible mod p, i.e. $\overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is irreducible. To see this, take p and $f(x)$ as stated. We have

$$\mathbb{Z}[x]/(p, f(x)) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f}(x))$$

But $(\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f}(x))$ is a field since $\overline{f}(x)$ is irreducible. But then $(p, f(x))$ is maximal. We now prove the converse. Suppose $M \subset \mathbb{Z}[x]$ is a maximal ideal. Then $k = \mathbb{Z}[x]/M$ is a field. Let $\phi : \mathbb{Z} \to k$ be the given by $\phi = \pi \circ i$, where $i : \mathbb{Z} \to \mathbb{Z}[x]$ is the canonical inclusion and $\pi : \mathbb{Z}[x] \to k$ is the canonical projection. If ϕ were injective, then ϕ extends to an injection $\Phi : \mathbb{Q} \to k$. Choosing $x \mapsto \pi(x)$, π extends to a morphism $\Pi : \mathbb{Q}[x] \to k$. Clearly, Π is surjective. If Π were injective, there would be an isomorphism $\mathbb{Q}[x] \cong k$. However, $\mathbb{Q}[x]$ is not a field (x is not invertible). Then Π is not injective which shows $\ker \Pi = (g(x))$ for some nonzero polynomial g, which necessarily be irreducible. Without loss of generality, we may assume that g is primitive. Then $\mathbb{Q}[x]/(g) \cong k$. But then $\mathbb{Z}[x] \to \mathbb{Q}[x]$ gives surjection $\mathbb{Z}[x] \to \mathbb{Q}[x]/(g)$. Therefore, we have an isomorphism $\mathbb{Z}[x]/(g) \cong \mathbb{Q}[x]/(g)$. Write $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$. In $\mathbb{Q}[x]/(g)$, we have $\overline{g(x)} = 0$. But then $\overline{x}^n = (-a_0/a_n) + (-a_1/a_n)\overline{x} + \cdots + (-a_{n-1}/a_n)\overline{x}^{n-1}$. Then every element of $\mathbb{Q}[x]/(g)$ can be written as a linear combination of the set $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ with coefficients in $\mathbb{Z}[1/a_n]$. But $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ is linearly independent in $\mathbb{Q}[x]/(g)$. Choose a prime not dividing a_n. Then $1/p$ is not spanned by $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ with coefficients in $\mathbb{Z}[1/a_n]$. Then $\ker \phi = (n)$ for some $n \in \mathbb{Z} \setminus \{0\}$. But $\operatorname{im} \phi$ is an integral domain, n must be prime, say p. Then $p \in M$. The maximal ideals in $\mathbb{Z}[x]$ containing p are the maximal ideals in $\mathbb{Z}[x]/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})[x]$. But then $M/(p) = (\overline{f}(x))$ for some irreducible polynomial $\overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Therefore, $M = (p, f(x))$ for some polynomial $f(x) \in \mathbb{Z}[x]$.

$q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ are elements of $\mathbb{Z}[x]$ and $r \in \mathbb{Z}$, then

$$\phi(p(x) + q(x)) = \phi((a_0 + b_0) + (a_1 + b_1)x + a_2x^2 + \cdots + (a_n + b_n)x^n) = (a_0 + b_0) \mod 3$$
$$\phi(p(x)) + \phi(q(x)) = a_0 \mod 3 + b_0 \mod 3 \equiv (a_0 + b_0) \mod 3$$
$$\phi(rp(x)) = ra_0 \mod 3$$
$$r\phi(p(x)) = r \cdot (a_0 \mod 3) \equiv (r \mod 3)(a_0 \mod 3) \equiv ra_0 \mod 3$$

Clearly, ϕ is surjective. Let K denote the kernel of ϕ. If $p(x) \in (3, x)$, $p(x)$ has constant term divisible by 3. Then $\phi(p(x)) \equiv 0 \mod 3$ so that $p(x) \in K$. Therefore, $(3, x) \subset K$. Now if $p(x) \in K$, then $\phi(p(x)) = a_0 \mod 3$ and $\phi(p(x)) \equiv 0 \mod 3$. Then $a_0 \in (3)$. But then for some $k \in \mathbb{Z}$, $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 3k + a_1x + a_2x^2 + \cdots + a_nx^n = 3k + x(a_1 + a_2x + \cdots + a_nx^{n-1})$. But then $p(x) \in (3, x)$. Therefore, $K = (3, x)$. By the First Isomorphism Theorem, $\mathbb{Z}[x]/K \cong \mathbb{Z}/3\mathbb{Z}$. However, $\mathbb{Z}/3\mathbb{Z}$ is a field so that K must be maximal.

OR

Using the Second Isomorphism Theorem

$$\mathbb{Z}[x]/(3, x) \cong \frac{\mathbb{Z}[x]/(x)}{(3, x)/(x)} \cong \mathbb{Z}/3\mathbb{Z}$$

But $\mathbb{Z}/3\mathbb{Z}$ is a field so that the ideal $(3, x)$ must be maximal. □

7. Let R be a commutative ring with identity. Let I and J be ideals of R. Recall that IJ equals the ideal generated by $\{ij : i \in I, j \in J\}$.

(a) Prove that $IJ \subset I \cap J$

(b) Give an example where $IJ = I \cap J$. Make the example nontrivial in the sense that neither I nor J equals either 0 or R.

(c) Give an example where $IJ \neq I \cap J$.

Solution:

(a) Since $I \cap J$ is an ideal, it is sufficient to show that $I \cap J$ contains every element of the form xy, where $x \in I$, $y \in J$. Since $x \in I$ and I is closed under multiplication by R, $xy \in I$. Mutatis mutandis, $xy \in J$. Thus, $xy \in I \cap J$ and $IJ \subset I \cap J$.

(b) Take $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, and $J = 3\mathbb{Z}$. Then $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ since $a \in 2\mathbb{Z} \cap 3\mathbb{Z}$ if and only if $2 \mid a$ and $3 \mid a$ so that $6 \mid a$ (as $6 = \text{lcm}(2, 3)$). We claim $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z}$. Since $6 = 2 \cdot 3$, $6 \in (2\mathbb{Z})(3\mathbb{Z})$ implying $6\mathbb{Z} \subseteq (2\mathbb{Z})(3\mathbb{Z})$. If $a \in (2\mathbb{Z})(3\mathbb{Z})$, then $a = (2j)(3k) = 6(jk)$ for some $j, k \in \mathbb{Z}$. But then $a \in 6\mathbb{Z}$. Therefore, $6\mathbb{Z} = (2\mathbb{Z})(3\mathbb{Z})$ and $2\mathbb{Z} \cap 3\mathbb{Z} = (2\mathbb{Z})(3\mathbb{Z})$.

(c) Take $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, and $J = 4\mathbb{Z}$. Then $I \cap J = 4\mathbb{Z}$. We claim $4 \notin IJ$. If $4 \in IJ$, then $4 = a_1b_1 + \cdots + a_kb_k$, where $a_i \in 2\mathbb{Z}$ and $b_i \in 4\mathbb{Z}$. For each i, there exist $m_i, n_i \in \mathbb{Z}$ such that $a_i = 2m_i$ and $b_i = 4n_i$ so that $a_ib_i = 8m_in_i \in 8\mathbb{Z}$. Hence, $a_1b_1 + \cdots + a_kb_k = 4 \in 8\mathbb{Z}$, a contradiction. Thus, $4 \notin (2\mathbb{Z})(4\mathbb{Z})$, then $2\mathbb{Z} \cap 4\mathbb{Z} \neq (2\mathbb{Z})(4\mathbb{Z})$.

□

8. Let F be a field and $F[x]$ the ring of polynomials in one variable with coefficients in F.

(a) Show that a module M over $F[x]$ is also in a natural way a vector space over F.

(b) Assume that F is algebraically closed and that M is a simple module over $F[x]$. Prove that the dimension of M as a vector space over F is one.

(c) Assume that F is not algebraically closed. Prove that there exists a simple module M over $F[x]$ such that the dimension of M as a vector space over F is greater than one.

Solution:

(a) Since M is an $F[x]$-module, there exists an action of $F[x]$ on M. Note $F \subset F[x]$. The restriction of the action of $F[x]$ to F gives a scalar multiplication of F on M, making M into an F-vector space. Furthermore for any $m, m' \in M$, $a \in F$, $x \cdot (m + m') = xm + xm'$ and $x \cdot (am) = axm$ so x is a linear operator on the F-vector space M.

(b) Let $m \in M$ be nonzero. Then $F[x]m$ is a nonzero submodule of M. Since M is simple, $F[x]m = M$. This implies that the function $\phi : F[x] \to M$ given by $\phi(f(x)) = f(x) \cdot m$ is a surjective $F[x]$-homomorphism. By the First Isomorphism Theorem, $F[x]/\ker\phi \cong M$. Since M is simple, the Lattice Isomorphism Theorem implies there are no $F[x]$-submodules (ideals of $F[x]$) I such that $\ker\phi \subsetneq I \subsetneq F[x]$. Thus, $\ker\phi$ is a maximal ideal of $F[x]$. This implies that $\ker\phi = (p(x))$ for some irreducible $p(x) \in F[x]$. Since F is algebraically closed, p must have degree 1. Without loss of generality, assume that p is monic so that $p(x) = (x - \alpha)$ for some $\alpha \in F$. Viewing $F[x]$ as an F-vector space, define $T : F[x] \to F$ via $f(x) \mapsto f(\alpha)$. Then T is a surjective linear transformation with kernel $(x - \alpha)$. By the First Isomorphism Theorem,

$$M \cong F[x]/\ker\phi \cong F,$$

so M has dimension 1 as an F-vector space.

(c) Since F is not algebraically closed, there exists an irreducible polynomial $p(x) \in F[x]$ with degree greater than 1. Then the maximal ideal $(p(x))$ is a maximal submodule of $F[x]$, so the module $M = F[x]/(p(x))$ is a simple $F[x]$-module.

View M as an F-vector space. We claim the set $\{\overline{1}, \overline{x}\}$ is linearly independent. Suppose $a\,\overline{1} + b\,\overline{x} = \overline{0}$. Then $a + bx \in (p(x))$, so $p(x)$ divides $a + bx$. Since $\deg p(x) > 1$, this implies that $a + bx = 0$ so $a = b = 0$. Then $\dim_F M \geq 2$.

□

9. Let T be a linear operator on a finite dimensional vector space over the complex numbers. Assume that T has two eigenvalues: 3, 4. Assume that the Jordan canonical form of a matrix representing T has the following form. For the eigenvalue 3 there are 2 blocks of size 1, 2 blocks of size 2, and 1 block of size 4. For the eigenvalue 4 there are 1 block of size 1, 3 blocks of size 3, and 1 block of size 5.

(a) What is the characteristic polynomial of T?

(b) What is the minimal polynomial of T?

(c) What is the nullity of $(T - 3I)^3$? I is the identity linear transformation.

Solution:

(a) The elementary divisors of T are $(x-3), (x-3), (x-3)^2, (x-3)^2, (x-3)^4$, $(x-4), (x-4)^3, (x-4)^3, (x-4)^3$, and $(x-4)^5$. The characteristic polynomial of T is the product of the elementary divisors: $c(x) = (x-3)^{10}(x-4)^{15}$.

(b) The minimal polynomial is the product of the largest power of $(x-3)$ and the largest power of $(x-4)$ that are elementary divisors, which is $m(x) = (x - 30^4(x-4)^5$.

(c) Since there are 5 blocks corresponding to the eigenvalue 3, the nullity of $(T-3I)$ is 5. The quantity nullity $(T-3I)^2-$ nullity $(T-3I)$ is the number of Jordan blocks corresponding to the eigenvalue 3 that have size at least 2. Since there are 3 such blocks, it follows that nullity $(T-3I)^2 = 3+5 = 8$. By a similar reasoning, nullity $(T-3I)^3-$ nullity $(T-3I)^2 =$ nullity $(T-3I)^3 - 8 = 1$. Therefore, nullity $(T-3I)^3 = 9$.

□

10. Let $F \subset K$ be an extension of fields of characteristic 0. Let G be the Galois group of K over F. We do not assume that the field extension $F \subset K$ is a Galois extension. Assume that G is a finite group and that p is a prime number that divides the order of G. Prove that there exists a field L with $F \subset L \subset K$ satisfying all of the following properties.

(a) $L \subset K$ is a Galois field extension with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

(b) The degree of the field extension $L \subset K$ is p.

(c) There does not exist any field strictly between L and K.

Solution: By Cauchy's Theorem, G contains an element of order p and hence a subgroup of order p. Let $H \subset G$ be a subgroup of order p. Let $F = \text{Fix}\, H$ be the subfield of K that is fixed by H. Then $\text{Gal}(K/L) = H$ and $|\text{Gal}(K/L)| = [K : L] = p$, so $L \subset K$ is a Galois extension whose Galois group has order p. Hence, $\text{Gal}(K/L) \cong \mathbb{Z}/p\mathbb{Z}$. But $[K : L] = p$ so that (a) and (b) hold. Suppose there exist a field F' such that $L \subset F' \subset K$. Then $p = [K : L] = [K : F'][F' : L]$, so either $[K : F'] = 1$ or $[F' : L] = 1$. That is, either $K = F'$ or $L = F'$. This proves (c). $\square$

August 2008

1. Let $\mathbb{R}^2$ be the Euclidean plane with the standard basis $e_1 = \begin{bmatrix}1\\0\end{bmatrix}$, $e_2 = \begin{bmatrix}0\\1\end{bmatrix}$.

(a) The counterclockwise rotation about the origin through an angle α, where $-\infty < \alpha < \infty$, is a linear operator on $\mathbb{R}^2$. Find the representation matrix of this linear operator with respect to the standard basis $\{e_1, e_2\}$.

(b) The orthogonal reflection about a linear through the origin is a linear operator on $\mathbb{R}^2$. Denote by L_1 the x-axis, and by L_2 the line obtained by rotating L_1 about the origin through a counterclockwise angle θ, where $0 < \theta < \pi/2$. Denote by r_i the orthogonal reflection about L_i, $i = 1, 2$. Find the representation matrices of r_1, r_2, and the composition $r_2 r_1$ with respect to the standard basis $\{e_1, e_2\}$.

(c) Using part (a), prove that $r_2 r_!$ is the counterclockwise rotation about the origin through the angle 2θ.

Solution:

(a) Let R_α denote the rotation about the origin through an angle α. Let $\mathcal{B}$ denote the standard basis for $\mathbb{R}^2$. Then the matrix of R_α, with respect to $\mathcal{B}$, is

$$A = \begin{bmatrix} [R_\alpha(e_1)]_\mathcal{B} & [R_\alpha(e_2)]_\mathcal{B} \end{bmatrix}$$

where $R_\alpha(e_1) = \begin{bmatrix}\cos\alpha\\ \sin\alpha\end{bmatrix}$ and $R_\alpha(e_2) = \begin{bmatrix}\cos(\alpha+\pi/2)\\ \sin(\alpha+\pi/2)\end{bmatrix}$. Thus,

$$A = \begin{bmatrix}\cos\alpha & \cos(\alpha+\pi/2)\\ \sin\alpha & \sin(\alpha+\pi/2)\end{bmatrix} = \begin{bmatrix}\cos\alpha & \cos\alpha\cos(\pi/2) - \sin\alpha\sin(\pi/2)\\ \sin\alpha & \sin\alpha\cos(\pi/2) + \sin(\pi/2)\cos\alpha\end{bmatrix} = \begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}$$

(b) The matrix of r_1 with respect to $\mathcal{B}$ is

$$\begin{bmatrix} [r_1(e_1)]_\mathcal{B} & [r_1(e_2)]_\mathcal{B} \end{bmatrix}$$

Note that e_1 is fixed by r_1 and that $r_1(e_2) = -e_2$. Therefore,

$$\begin{bmatrix} [r_1(e_1)]_\mathcal{B} & [r_1(e_2)]_\mathcal{B} \end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

The matrix of r_2 with respect to $\mathcal{B}$ is

$$\begin{aligned}\begin{bmatrix} [r_2(e_1)]_\mathcal{B} & [r_2(e_2)]_\mathcal{B}\end{bmatrix} &= \begin{bmatrix}\cos 2\theta & \cos(\theta - (\pi/2 - \theta))\\ \sin 2\theta & \sin(\theta - (\pi/2 - \theta))\end{bmatrix} = \begin{bmatrix}\cos 2\theta & \cos(2\theta - \pi/2)\\ \sin 2\theta & \sin(2\theta - \pi/2)\end{bmatrix}\\ &= \begin{bmatrix}\cos 2\theta & \cos 2\theta\cos(\pi/2) + \sin 2\theta\sin(\pi/2)\\ \sin 2\theta & \sin 2\theta\cos(\pi/2) - \cos 2\theta\sin(\pi/2)\end{bmatrix}\\ &= \begin{bmatrix}\cos 2\theta & \sin 2\theta\\ \sin 2\theta & -\cos 2\theta\end{bmatrix}.\end{aligned}$$

Now the matrix of the composition $r_2 r_1$ is

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}$$

(c) Let A denote the matrix of the counterclockwise rotation about the origin through the angle 2θ with respect to the standard basis. Let B denote the matrix of $r_2 r_1$ with respect to the standard basis. By parts (a) and (b), $A = B$. Therefore, $r_2 r_!$ is the counterclockwise rotation about the origin through the angle 2θ.

□

2.

(a) Prove that the set of elements of finite order in an abelian group is a subgroup.

Denote by $\mathrm{GL}(\mathbb{R}^2)$ the group of invertible linear operators on $\mathbb{R}^2$. In the rest of the problem, use the notation and results of Problem 1, without necessarily solving that problem.

(b) Determine the orders of r_1 and r_2 in $\mathrm{GL}(\mathbb{R}^2)$.

(c) Prove that $r_2 r_1$ is of finite order if and only if the quotient θ/π is a rational number. Find the order of $r_2 r_1$ if $\theta = \pi/m$ where $m > 2$ is an integer.

(d) Explain that (a) will fail if one drops the assumption that the group is abelian.

Solution:

(a) Let G be an abelian group. The claim is that for any $n \in \mathbb{N}$ and $g, h \in G$, $(gh)^n = g^n h^n$. For $n = 1$, this is $(gh)^1 = gh = g^1 h^1$. Suppose the claim is true for some given n. Then

$$(gh)^{n+1} = (gh)^n (gh) = g^n h^n (gh) = g^n g h^n h = g^{n+1} h^{n+1}$$

Therefore, the claim follows by induction.

Let H denote the set of elements of finite order in G. The set H is nonempty as $1 \in H$. If $g, h \in H$, then g, h have finite order, say n, m, respectively. Then $(gh)^{nm} = g^{nm} h^{nm} = (g^n)^m (h^m)^n = 1^m 1^n = 1$. Therefore, $gh \in H$. For g as stated, we also have $(g^{-1})^n = 1$ as $1 = (gg^{-1})^n = g^n (g^{-1})^n = (g^{-1})^n$. But then $g^{-1} \in H$ and H is then a subgroup of G.

(b) Geometrically, each has order 2 since a vector in $\mathbb{R}^2$ that is reflected twice about the same line will return to where it started. Alternatively, use the matrixes for r_1 and r_2 to see that

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $|r_1| = 2$. Similarly,

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} = \begin{bmatrix} \cos^2(2\theta) + \sin^2(2\theta) & \cos 2\theta \sin 2\theta - \sin 2\theta \cos 2\theta \\ \sin 2\theta \cos 2\theta - \cos 2\theta \sin 2\theta & \sin^2(2\theta) + \cos^2(2\theta) \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, $|r_2| = 2$.

(c) Suppose that $r_2 r_1$ is of finite order. Note that for $n \in \mathbb{N}$, $(r_2 r_1)^n$ is a counterclockwise rotation about the origin through angle $2n\theta$. If $(r_2 r_1)^n$ is the identity transformation, then $2n\theta = 2\pi m$ for some $m \in \mathbb{Z}$. Therefore, $\frac{\theta}{\pi} = \frac{m}{n} \in \mathbb{Q}$.

If $\frac{\theta}{\pi} \in \mathbb{Q}$, then $\frac{\theta}{\pi} = \frac{p}{q}$ for some $p \in \mathbb{Z}$, $q \in \mathbb{N}$. This implies that $p\theta = q\pi$. For any $n \in \mathbb{N}$, $(r_2 r_1)^n$ is a counterclockwise rotation about the origin through angle $2n\theta$. This implies that $(r_2 r_1)^p$ is a counterclockwise rotation about the origin through the angle $2p\theta = 2\pi q$. This implies that $(r_2 r_!)^p$ is the identity transformation. Hence $r_2 r_1$ has finite order.

(d) Take $G = \mathrm{GL}_2(\mathbb{R})$. Let $\theta = \pi^2$. Let r_1, r_2 be as above. Then $|r_1| = |r_2| = 2$, but since $\frac{\pi^2}{\pi} = \pi \notin \mathbb{Q}$. Part (c) implies that $|r_2 r_1| = \infty$. Thus, the subset of elements of finite order of G is not closed under multiplication.

□

3. Let H and K be subgroups of a group G, and set $HK = \{hk \colon h \in H, k \in K\}$.

(a) Prove that if $HK \subset KH$ then KH is a subgroup of G.

(b) Prove that if $K \cap H = \{1\}$ then the map $\rho : K \times H \to G$ given by $\rho(k, h) = kh$ is injective and $\operatorname{im} \rho = KH$.

(c) Let G be of order $n = pm$ where p is a prime that does not divide m, let S be the set of all Sylow p-subgroups of G, and let $H \in S$. Then S is a left G-set by means of $g \circ K = gKg^{-1}$ for all $g \in G$, $K \in S$, so S is a left H-set by restriction. Using (a) and (b), prove that exactly one orbit of the H-set S consists of a single element, and each of the remaining orbits consists of p elements.

Solution:

(a) The set KH is clearly nonempty ($1 = 1 \cdot 1 \in KH$). Let $x, y \in KH$ be arbitrary. Then $x = kh$, $y = k'h'$ for some $k, k' \in K$, $h, h' \in H$. Therefore, $xy^{-1} = hk(h'k')^{-1} = hk(k')^{-1}(h')^{-1}$. Now $hk(k')^{-1} \in HK \subset KH$, so there exists $h'' \in H$, $k'' \in K$ such that $hk(k')^{-1} = k''h''$. Therefore, $xy^{-1} = k''h''(h')^{-1} \in KH$. Therefore, KH is a subgroup of G.

(b) If $x \in KH$, then $x = kh$ for some $k \in K$, $h \in H$. Therefore, $\rho(k, h) = kh = x$. This shows that $KH \subset \operatorname{im}\rho$. It is clear that $\operatorname{im}\rho \subset KH$, so $\operatorname{im}\rho = KH$.

Suppose $h, h' \in H$, $k, k' \in K$ and that $\rho((h, k)) = \rho((h', k'))$. Then $hk = h'k'$, so $(h')^{-1}h = k'k^{-1} \in H \cap K$, so $(h')^{-1}h = k'k^{-1} = 1$. Thus, $h = h'$ and $k = k'$. Therefore, ρ is injective.

Notice that this implies that $|KH| = |K \times H|$ (this will play a role in part (c)).

(c) For $K \in S$, let $H_K = \{x \in H \colon xK = K\} = \{x \in H \colon xKx^{-1} = K\}$. It is clear that $H_H = H$. By the Orbit-Stabilizer Theorem, $[H \colon H_H] = 1 = |\mathcal{O}_H|$, where $|\mathcal{O}_H|$ denotes the orbit of H in S. Now, suppose $K \neq H$. Since $|H| = p$, either $H_K = \{1\}$ or $H_K = H$. If $H_K = H$, then $xKx^{-1} = K$ for all $x \in H$. This implies that $xK = Kx$ for all $x \in H$. Therefore, $HK = KH$. By part (a), KH is a subgroup of G. By part (b),

$$|KH| = |K \times H| = |K|\,|H| = p^2,$$

and p^2 does not divide $|G| = pm$ since p does not divide m. This contradicts Lagrange's Theorem. Hence, $H_K = \{1\}$, and Orbit-Stabilizer Theorem,

$$|\mathcal{O}_K| = [H \colon H_K] = \frac{|H|}{|H_K|} = p.$$

Thus, exactly one orbit of S consists of a single element and each of the remaining orbits of S consists of p elements.

□

4. Prove that a group of order 77 is cyclic.

Solution: Let G be a group of order $77 = 7 \cdot 11$. The divisors of 77 are 1, 7, 11, and 77. For $p = 7, 11$, let $n_p(G)$ denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_7(G) \equiv 1 \mod 7$ and divides 77. Therefore, $n_7(G) = 1$. Also, $n_{11}(G) \equiv 1 \mod 11$ and divides 77, so $n_{11}(G) = 1$. Let H denote the unique Sylow 7-subgroup and let J denote the unique Sylow 11-subgroup.

It is clear that $G \neq H \cup J$ (since $|G| = 77$ and $|H| = 7$ and $|J| = 11$), so let $x \in G \setminus (H \cup J)$ be arbitrary. The claim is that $G = \langle x \rangle$. If $|x| = 1$, then $x = 1 \in H \cup J$, contrary to the assumption $x \notin H \cup J$. If $|x| = 7$, then $\langle x \rangle$ is a subgroup of G or order 7. Since the Sylow

7-subgroup of H is unique, this implies that $H = \langle x \rangle$. Thus, $x \in H$, a contradiction. Similarly, if $|x| = 11$, then $x \in J$, a contradiction. Thus, $|x| = 77$, which proves the claim. Thus, G is cyclic. □

5. Let w be a vector of length 1 in the Euclidean space $\mathbb{R}^n$ of $n \times 1$ matrices.

(a) Prove that the matrix $P = I_n - ww^T$ is orthogonal. Here I_n is the $n \times n$ identity matrix, and w^T is the transpose of w.

(b) Prove that multiplication by P is a reflection about $\langle w \rangle^\perp$, the orthogonal complement of the subspace spanned by w, that is, prove that if we write an arbitrary $v \in \mathbb{R}^n$ in the form $v = cw + w'$ where $c \in \mathbb{R}$ and $w' \perp w$, then $Pv = -cw + w'$.

(c) Let X, Y be arbitrary vectors in $\mathbb{R}^n$ of the same length. Determine a vector w satisfying $PX = Y$.

Solution:

(a) Observe that

$$P^T = I_n^T - 2(ww^T)^T = I_n - 2(w^{TT}w^T) = I_n - 2ww^T = P.$$

Therefore, P is symmetric. It is therefore sufficient to prove $P^2 = I_n$. This can be shown directly:

$$\begin{aligned} P^2 &= (I_n - 2ww^T)^2 \\ &= I_n^2 - 2ww^T - 2ww^T + 4(ww^T)^2 \\ &= I_n - 4ww^T + 4ww^Tww^T. \end{aligned}$$

Since w is a unit vector, $w^Tw = 1$ and

$$P^2 = I_n - 4ww^T + 4ww^T = I_n.$$

Thus, P is orthogonal.

(b) IF $v = cw + w'$ with c, w, w' as above, then

$$\begin{aligned} Pv = P(cw + w') &= cP(w) + P(w') \\ &= c(I_n - 2ww^T)w + (I_n - 2ww^T)w' \\ &= cw + w' - 2cww^Tw - 2ww^Tw'. \end{aligned}$$

Since w is a unit vector, $w^Tw = 1$. Since $w' \perp w$, $w^Tw' = 0$ and

$$Pv = cw + w' - 2cw = -cw + w',$$

as required.

(c) First suppose there exists a $w \in \mathbb{R}^n$ such that $PX = Y$. Then there are unique $c, c' \in \mathbb{R}$, $w', w'' \in \langle w \rangle^\perp$ such that $X = cw + w'$, $Y = c'w + w''$. Using part (b), $PX = -cw + w' = c'w + w''$. So $c' = -c$ and $w' = w''$. Therefore, $Y = -cw + w'$ and $X - Y = (cw + w') - (-cw + w') = 2cw$. Thus, $X - Y \in \text{Span}\{w\}$. If $X = Y$, then take $w = 0$. Otherwise, $w \in \text{Span}\{X - Y\}$ and w must be a unit vector. Take $w = \frac{X-Y}{\|X-Y\|}$.

Now, it needs to be checked that if $w = \frac{X-Y}{\|X-Y\|}$, then $PX = Y$. Note that

$$X = \frac{\|X - Y\|}{2}\left(\frac{X - Y}{\|X - Y\|}\right) + \frac{X + Y}{2}.$$

Also,

$$\begin{aligned}\left\langle X - Y, \frac{X + Y}{2}\right\rangle &= \frac{1}{2}\langle X - Y, X + Y\rangle \\ &= \frac{1}{2}\left(\langle X, X\rangle + \langle X, Y\rangle - \langle X, Y\rangle - \langle Y, Y\rangle\right) \\ &= \frac{1}{2}(1 + \langle X, Y\rangle - \langle X, Y\rangle - 1) \\ &= 0\end{aligned}$$

which shows that $\frac{X+Y}{2} \in \langle w \rangle^\perp$. Finally,

$$PX = \frac{\|X - Y\|}{2}\left(\frac{Y - X}{\|X - Y\|}\right) + \frac{X + Y}{2} = \frac{Y - X}{2} + \frac{X + Y}{2} = Y,$$

as desired.

□

6.

(a) Let R be a commutative ring with S a subring of R which contains the identity. If P is a prime ideal of R, show that $P \cap S$ is a prime ideal of S.

(b) Let $\mathbb{Z}[x]$ be the ring of polynomials in one variable with coefficients in the integers. Assume P is a prime ideal of $\mathbb{Z}[x]$. Show that P is generated as an ideal by at most two elements.

Solution:

(a) The set $P \cap S$ is certainly nonempty — $0 \in P \cap S$. If $x, y \in P \cap S$, then $x + y \in P$ since P is closed under addition and $x + y \in S$ since S is closed under addition. Hence,

$x + y \in P \cap S$ and $P \cap S$ is closed under addition. Suppose $x \in P \cap S$ and $s \in S$. Since $x, y \in S$, $sx \in S$. Since P is an ideal of R, $xs \in P$. This shows that $xs \in P \cap S$, so $P \cap S$ is an ideal of S. Also, $P \cap S$ is a proper ideal of S since $1 \in S$ but $1 \notin P \cap S$.

If $a, b \in S$ and $ab \in P \cap S$, then $ab \in P$. Since P is a prime ideal of R, either $a \in P$ or $b \in P$. If $a \in P$, then $a \in P \cap S$. If $b \in P$, then $b \in P \cap S$. Hence, either $a \in P \cap S$ or $b \in P \cap S$. This prove that $P \cap S$ is prime ideal of S.

(b) Note that $\mathbb{Z} \subset \mathbb{Z}[x]$ is a subring that contains the identity. By part (a), $P \cap \mathbb{Z}$ is a prime dieal of $\mathbb{Z}$, so $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime integer p. Define

$$\begin{aligned} \phi : \mathbb{Z}[x] &\longrightarrow (\mathbb{Z}/p\mathbb{Z})[x] \\ q(x) &\mapsto \overline{q}(x), \end{aligned}$$

where $\overline{q}(x)$ is the polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$ given by reducing the coefficients of q mod p. Since ϕ is surjective, $\phi(P)$ is an ideal of $(\mathbb{Z}/p\mathbb{Z})[x]$. Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID, $\phi(P) = (\overline{f}(x))$ for some $\overline{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Choose $f \in P$ such that $\phi(f) = \overline{f}$. The claim is that $P = (p, f(x))$.

It is clear that $(p, f(x)) \subset P$. If $g(x) \in P$, then $\overline{g}(x) = \phi(g(x)) \in \phi(P)$, so there exists $\overline{h}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. In other words, $g(x) - f(x)h(x) = pq(x)$ for some $q(x) \in \mathbb{Z}[x]$. This implies that $g(x) = f(x)h(x) + pq(x) \in (p, f(x))$. Thus, $P \subset (p, f(x))$ and $P = (p, f(x))$.

In the case that $P \cap \mathbb{Z} = 0$, the problem remains unsolved.

□

7. Let R be an integral domain.

(a) Let p be a prime ideal of R. Must p be irreducible? Give either a proof or a counterexample.

(b) Let x be an irreducible element of R. Must x be prime? Give either a proof of a counterexample.

Solution:

(a) The answer is in the affirmative. Suppose $p = ab$ for some $a, b \in R$. Then p divides ab or so either p divides a or p divides b. Without loss of generality, suppose p divides a. Then $a = pr$ for some $r \in R$. This implies that $p = prb$. Cancel a p from both sides to see that $1 = rb$, so that b is a unit. This implies that p is irreducible.

(b) The answer is in the negative. For a counterexample, consider $R = \mathbb{Z}[\sqrt{-5}]$. There is norm N on R defined by $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$. Note that for any $x, y \in R$, $N(xy) = N(x)N(y)$. Observe that

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

The claim is that 2 is an irreducible element of R which is not prime. If $2 = ab$ for some $a, b \in R$, then $4 = N(2) = N(a)N(b)$. If $N(a) = 2$, for some $a = x + y\sqrt{-5}$, then $x^2 + 5y^2 = 2$, so $y = 0$ and $x^2 = 2$, a contradiction since x is rational. Mutatis mutandis, $N(b) \neq 2$. Therefore, either $N(a) = 1$ or $N(b) = 1$. If $N(a) = 1$, with a as before, then $N(a) = x^2 + 5y^2 = 1$ so that $y = 0$ and $x = \pm 1$. But then $a = \pm 1$ is a unit. Mutatis mutandis, if $N(b) = 1$, then b is a unit. Therefore, either a or b is a unit and 2 is irreducible.

Note that 2 divides $(1+\sqrt{-5})(1-\sqrt{-5})$. If 2 divides $1+\sqrt{-5}$, then $1+\sqrt{-5} = 2a$ for some $a \in R$. But then $6 = N(1+\sqrt{-5}) = N(2)N(a) = 4N(a)$, a contradiction as $4 \nmid 6$. Thus, 2 does not divide $1+\sqrt{-5}$ or $1-\sqrt{-5}$ despite the fact that 2 divides the product. Hence, 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Note: If R were assumed to be a UFD, then the answer is yes. So when looking for counterexamples, one need search for integral domains which are not UFDs (hence, not fields, Euclidean domains or PIDs).

□

8. Let A be a matrix with characteristic polynomial $(x-2)^6(x-3)^2$. Assume $A - 12I_8$ has rank 5, while $(A-2I_8)^2$ has rank 3. What are the possible Jordan canonical forms for A?

Solution: Note that A is an 8×8 matrix since its characteristic polynomial has degree 8. By the Rank-Nullity Theorem,

$$\text{nullity}(A - 2I_8) = 8 - \text{rank}(A - 2I_8) = 8 - 5 = 3$$
$$\text{nullity}((A - 2I_8)^2) = 8 - \text{rank}[(A - 2I_8)^2] = 8 - 3 = 5$$

Since $\text{nullity}(A - 2I_8) = 3$, there are 3 Jordan blocks corresponding to the eigenvalue 2 in the Jordan canonical form of A. Since

$$\text{nullity}[(A - 2I_8)^2] - \text{nullity}(A - 2I_8) = 5 - 3 = 2$$

there are two Jordan blocks corresponding to the eigenvalue 2 which have size at least 2. This means that there is one Jordan block of size 1. Since the multiplicity of the eigenvalue 2 is 6. This means that there is one Jordan block of size 3 and one Jordan block of size 2.

For the eigenvalue 3, there are two possibilities: either there are two Jordan blocks of size 1 or one Jordan block of size 2. This means that there are two possible Jordan canonical forms for A, up to permutation of the Jordan blocks, given below:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 \end{bmatrix}$$

□

9. Let a be a positive rational number that is not a square in $\mathbb{Q}$. Prove that $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$.

Solution: Note that $\sqrt[4]{a}$ is a root of the polynomial

$$m(x) := x^4 - a = (x - \sqrt[4]{a})(x + \sqrt[4]{a})(x - i\sqrt[4]{a})(x + i\sqrt[4]{a})$$

The claim is that $m(x)$ is irreducible over $\mathbb{Q}$. It is clear that $m(x)$ contains no rational roots. [For instance, by the Rational Roots Theorem, the only possible roots are $\pm 1, \pm 2, \pm 4$ — none of which are a root of $m(x)$.] It remains to show that $m(x)$ cannot be factored into products of irreducible quadratic polynomials over $\mathbb{Q}$. If such a factorization exists, then the quadratic polynomials must have the same irreducible factors in $\mathbb{C}[x]$ as $m(x)$ (since $\mathbb{C}[x]$ is a UFD). If $(x - \sqrt[4]{a})(x + \sqrt[4]{a}) \in \mathbb{Q}[x]$, then $\sqrt{a} = \sqrt[4]{a}\sqrt[4]{a} \in \mathbb{Q}$, contrary to the assumption that a is not a square in $\mathbb{Q}$. Any possible quadratic factor for $m(x)$ in $\mathbb{Q}[x]$ can be a product of either $x - i\sqrt[4]{a}, x + i\sqrt[4]{a}$ with either of $x - \sqrt[4]{a}, x + \sqrt[4]{a}$ as then the product will not be in $\mathbb{Q}[x]$. Finally, $(x - i\sqrt[4]{a})(x + i\sqrt[4]{a}) = x^2 + \sqrt{a}$. However, $\sqrt{a}$ is not rational since a is not a square in $\mathbb{Q}$. Thus, $m(x)$ is irreducible over $\mathbb{Q}$ and $m(x)$ is the minimal polynomial of $\sqrt[4]{a}$. Hence, $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$. □

10. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine the degree of the extension $[K : \mathbb{Q}]$, prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

Solution: Observe that K is the splitting field of the separable polynomial $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$, so K is a Galois extension of $\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, σ is completely determined by $\sigma(\sqrt{2})$, $\sigma(\sqrt{3})$, and $\sigma(\sqrt{5})$. Since σ permutes the roots of $x^2 - 2$, there are two possibilities for $\sigma(\sqrt{2})$: $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$. Similarly, $\sigma(\sqrt{3}) = \pm\sqrt{3}$ and $\sigma(\sqrt{5}) = \pm\sqrt{5}$. Hence, there are eight elements of $\mathrm{Gal}(K/\mathbb{Q})$. Let $\sigma_{i,j,k}$ denote the

element of $\mathrm{Gal}(K/\mathbb{Q})$ sending $\sqrt{2}$ to $(-1)^i\sqrt{2}$, $\sqrt{3}$ to $(-1)^j\sqrt{3}$, and $\sqrt{5}$ to $(-1)^k\sqrt{5}$ for $i, j, k \in \{0, 1\}$. It is clear that $\sigma_{i,jk}$ commutes with $\sigma_{i',j',k'}$ for all $i, j, k, i', j', k' \in \{0, 1\}$. Moreover, each of these elements has order 2 (except $\sigma_{0,0,0}$ which has order 1) and are distinct from every other element. By the Fundamental Theorem of Finitely Generated Abelian Groups, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $K/\mathbb{Q}$ is a Galois extension, $[K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})| = 8$. □

January 2009

1. Let G be a group of order $132 = 2^2 \cdot 3 \cdot 11$. prove that G is not simple.

Solution: Note that the divisors of 132 are $1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66$, and 132. For any prime p, let $n_p(G)$ denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_p(G)$ divides $|G| = 132$ and $n_p(G) \equiv 1 \mod p$. Therefore, the only possibilities are:

$$\begin{aligned} n_2(G) &\in \{1, 3, 11, 33\} \\ n_3(G) &\in \{1, 4\} \\ n_{11}(G) &\in \{1, 12\} \end{aligned}$$

If $n_p(G) = 1$ for $p \in \{2, 3, 11\}$, then the Sylow p-subgroup is unique and therefore normal. But then G is not simple.

Suppose then that $n_p(G) > 1$. Then it must be that $n_{11}(G) = 12$. Since the intersection of any two Sylow 11-subgroups is the identity. Then there are $12(11-1) = 12(10) = 120$ distinct non-identity elements of G in these two distinct subgroups. Similarly since $n_3(G) = 4$, the 4 Sylow 3-subgroups contain $4(3-1) = 4(2) = 8$ distinct non-identity elements. Together, these account for 128 distinct elements of G.

Now, let S_1, S_2, and S_3 denote three distinct Sylow 2-subgroups of G. Notice it is possible to have $|S_1 \cap S_3| = 2$. Observe that for $i \neq j$, $|S_i \cap S_j| \leq 2$. The Inclusion-Exclusion Principle implies that

$$\begin{aligned} |S_1 \cup S_2 \cup S_3| &= |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3| \\ &\geq 4 + 4 + 4 - 2 - 2 - 2 + 1 = 7 \end{aligned}$$

Therefore, there are at least $128 + 7 = 135$ distinct elements of G, a contradiction. Therefore, one of $n_2(G)$, $n_3(G)$, or $n_{11}(G)$ is 1, implying that G is not simple. □

2. Let H and K be normal subgroups of a group G, and assume that $G = HK$. Prove that there is an isomorphism

$$G(H \cap K) \cong G/H \times G/K$$

(Formal manipulations with isomorphism theorems will not be enough; you'll need to explicitly define a map.)

Solution: Define $\phi : G \to G/H \times G/K$ by $g \mapsto (gH, gK)$. The map ϕ is a homomorphism since for all $g, g' \in G$

$$\phi(gg') = (gg'H, gg'K) = (gHg'H, gKg'K) = (gH, gK) \cdot (g'H, g'K) = \phi(g)\phi(g').$$

To see that ϕ is surjective, suppose $(gH, g'K) \in G/H \times G/K$. Since $G = HK$, $g = h_1k_1$ for some $h_1 \in H, k_1 \in K$. This implies that $g = (h_1k_1h^{-1})h_1 = k_2h_1$ for $k_2 = h_1k_1h_1^{-1} \in K$ (since

K is normal in G). Therefore, $gH = k_2h_1H = k_2H$. Also, $g' = h_2k_3$ for some $h_2 \in H$, $k_3 \in K$, so $g'K = h_2k_3K = h_2K$. Define $g'' = h_2k_2 = k_2(k_2^{-1}h_2k_2) = k_2h_3$ for $h_3 = k_2^{-1}h_2k_2 \in H$ (since H is normal in G). Then $\phi(g'') = (k_2h_3H, h_2k_2K) = (k_2H, h_2K) = (gH, g'K)$ so that ϕ is surjective.

Now $g \in \ker\phi$ if and only if $(gH, gK) = (H, K)$ if and only if $g \in H$ and $g \in K$, i.e. $g \in H \cap K$. Thus, $\ker\phi = H \cap K$. By the First Isomorphism Theorem,

$$G/(H \cap K) \cong G/H \times G/K.$$

□

3. Let A be a complex square matrix of size n.

(a) Define what it means for A to be Hermitian.

(b) If XAX^* has real entries for every $X \in \mathbb{C}^n$, prove that A is Hermitian.

Solution:

(a) A is a hermitian matrix is a matrix which is its own conjugate transpose, i.e. if $a_{ij} = \overline{a}_{ji}$.

(b) Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ denote the standard basis for $\mathbb{C}^n$ and A^* denote the conjugate transpose of A. Let $A = (a_{ij})$. Then $e_iAe_i^* = a_{ii}$ is real so that $a_{ii} = \overline{a}_{ii}$. For $i \neq j$, take $X = e_i + e_j$. Then XAX^* is real, so

$$(e_i + e_j)A(e_i + e_j)^* = e_iAe_i^* + e_jAe_j^* + e_iAe_j^* + e_jAe_i^*$$

is a real number. By assumption, $e_iAe_i^*$ and $e_jAe_j^*$ are both real. This implies that $e_iAe_j^* + e_jAe_i^*$ is real. Now $e_iAe_j^* + e_jAe_i^* = a_{ij} + a_{ji}$ has imaginary part zero. Therefore, $\mathrm{Im}(a_{ij}) = -\mathrm{Im}(a_{ji})$, where for $z \in \mathbb{C}$, Im z is the imaginary part of z.

Now for $i \neq j$, take $X = ie_i + e_j$. By hypothesis, XAX^* is real. Therefore,

$$\begin{aligned}(ie_i + e_j)A(ie_i + e_j)^* &= ie_iA(-i)(e_i^*) + ie_iAe_j^* + e_jA(-i)(e_i^*) + e_jAe_j^* \\ &= e_iAe_i^* + e_jAe_j^* + i(e_iAe_j^* - e_jAe_i^*) \\ &= a_{ii} + a_{jj} + i(a_{ij} - a_{ji})\end{aligned}$$

Since XAX^*, a_{ii} and a_{jj} are real, $i(a_{ij} - a_{ji})$ must be real. Therefore, $\mathrm{Re}(a_{ij}) = \mathrm{Re}(a_{ji})$. For each $i \neq j$, it has been shown that $\mathrm{Re}(a_{ij}) = \mathrm{Re}(a_{ji})$ and that $\mathrm{Im}(a_{ij}) = \mathrm{Im}(a_{ji})$. This implies that $a_{ji} = \overline{a}_{ij}$. Since this is true when $i = j$, this implies that $A = A^*$.

□

4. Let F be a field and V a vector space over F, not necessarily of finite dimension. Let S and T be subsets of V such that S is linearly independent and T spans V. Prove that V has a basis B with $S \subseteq N \subseteq S \cup T$.

Solution: Consider the set

$$\mathcal{I} = \{I \colon S \subset I \subset S \cup T \text{ and } I \text{ is linearly independent}\}.$$

Note that $\mathcal{I}$ is nonempty since $S \in \mathcal{I}$. Also, $\mathcal{I}$ is a partially ordered set under the inclusion relation. Let $\mathcal{C}$ be a chain in $\mathcal{I}$. The claim is that $\mathcal{C}$ has an upper bound in $\mathcal{I}$. To prove this consider the set

$$I = \bigcup_{C \in \mathcal{C}} C.$$

It is clear that $C \subset I$ for all $C \in \mathcal{C}$. It is also clear that $S \subset I \subset S \cup T$. Thus, to prove the claim, it suffices to show that I is a linearly independent set. Let $x_1, x_2, \ldots, x_n \in I$ and let

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$

be a relation of linear dependence among the x_i. Notice that each $x_i \in C_i$ for some $C_i \in \mathcal{C}$. Let $C = \max\{C_i \colon i = 1, 2, \ldots, n\}$. Then $x_i \in C$ for all i and the above is a relation of linear dependence among elements of C. Since C is linearly independent, $a_1 = a_2 = \cdots = a_n = 0$. Thus, I is linearly independent and $I \in \mathcal{I}$. Thus, the chain $\mathcal{C}$ has an upper bound in $\mathcal{I}$, as claimed. By Zorn's Lemma, there exists a maximal element $B \in \mathcal{I}$.

The claim is that B is a basis for V. Since $B \in \mathcal{I}$, B is a linearly independent subset of V. Notice that if $T \subset \operatorname{Span} B$, then $\operatorname{Span} B = V$ since T spans V. If the claim is false, there exists $v \in T$ such that $v \notin \operatorname{Span} B$. Then $B \cup \{v\}$ is linearly independent, contradicting the maximality of B. Thus, B is a basis for V. Since $B \in \mathcal{I}$, $S \subset B \subset S \cup T$. □

5. A linear operator $T : V \to V$, with V a finite-dimensional vector space, is called *nilpotent* if some power of T is zero.

(a) Prove that T is nilpotent if and only if its characteristic polynomial is $p(t) = t^k$ for some k.

(b) Prove that if T is nilpotent then $T^{\dim V} = 0$.

Solution:

(a) Assume that T is nilpotent. Then there exists a $n \in \mathbb{N}$ such that $T^n = 0$. Let $m(t)$ denote the minimal polynomial of T. Then $m(t)$ divides t^n. This implies that $m(t) = t^j$ for some $j \leq n$. Every irreducible factor of the characteristic polynomial is a factor of the minimal polynomial, which implies that $p(t) = t^k$ for some k.

If $p(t) = t^k$, then $m(t) = t^j$ for some $j \leq k$. Therefore, $0 = m(T) = T^j$. Thus, T is nilpotent, as required.

(b) By part (a), $m(t) = t^j$ for some $j \leq \dim V$. This implies that $T^j = 0$, so $T^l = 0$ for all $l \geq j$. Since $\dim V \geq j$, $T^{\dim V} = 0$.

□

6. Let R be an integral domain and let a and b be nonzero elements of R. Recall that we say an element c of R is a least common multiple of a and b if and only if c satisfies the following two conditions

(a) $a \mid c$ and $b \mid c$

(b) For any nonzero $d \in R$ if $a \mid d$ and $b \mid d$ then $c \mid d$.

Prove that if R is a Principal Ideal Domain and a and b are nonzero elements of R then a least common multiple of a and b exists. (The problem does not require facts about UFDs. If you use any, you should prove them.)

Solution: Since R is a PID and $(a) \cap (b)$ is an ideal, there exists $c \in R$ such that $(c) = (a) \cap (b)$. The claim is that c is a least common multiple of a and b. Since $c \in (a)$, a divides c. Similarly, b divides c. Now suppose $d \in R$ is nonzero and that $a \mid d$ and $b \mid d$. Then $d \in (a) \cap (b) = (c)$. Therefore, $c \mid d$, as needed. □

7. Let A be a 10×10 matrix over the complex numbers, and let I be the 10×10 identity matrix. Assume the characteristic values of A are 2 and $2i$. Assume further that $(A - 2I)$ has nullity 3, $(A - 2I)^2$ has nullity 5, $(A - 2I)^3$ has nullity 6, $(A - 2iI)$ has nullity 2, and $(A - 2iI)^2$ has nullity 4.

(a) Find the Jordan canonical form of A.

(b) Find the characteristic polynomial of A.

(c) Find the minimal polynomial of A.

Solution:

(a) Since $(A - 2I)$ has nullity 3, there are 3 Jordan blocks associated to the eigenvalue 2. Since

$$\text{nullity}[(A - 2I)^3] - \text{nullity}[(A - 2I)^2] = 6 - 5 = 1,$$

the eigenvalue 2 has one Jordan block of at least size 3. Since

$$\text{nullity}[(A - 2I)^2] - \text{nullity}(A - 2I) = 5 - 3 = 2,$$

the eigenvalue 2 has two Jordan blocks of size at least 2, so exactly one Jordan block of size 2. Therefore, the remaining Jordan block has size 1.

Now consider the eigenvalue 2i. Since $(A - 2iI)$ has nullity 2, there are 2 Jordan blocks associated to the eigenvalue $2i$. Since

$$\text{nullity}[(A - 2iI)^2] - \text{nullity}(A - 2iI) = 4 - 2 = 2,$$

there are two Jordan blocks of size at least 2 for the eigenvalue $2i$. Now since

$$3 + 2 + 1 + 2 + 2 = 10,$$

this means that the Jordan block associated to the eigenvalue 2 that has size at least 3 is a 3×3 Jordan block. It also means that each of the Jordan blocks associated to $2i$ has size exactly 2. Thus, the Jordan canonical form is, up to permutation of the Jordan blocks,

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2i \end{bmatrix}$$

(b) The elementary divisors of A are $(x-2)^3$, $(x-2)^2$, $(x-2)$, $(x-2i)^2$, and $(x-2i)^2$. Since the characteristic polynomial is the product of the elementary divisors, it follows that

$$c(x) = (x-2)^3(x-2)^2(x-2)(x-2i)^2(x-2i)^2 = (x-2)^6(x-2i)^4$$

(c) The minimal polynomial is the product of the largest power of $(x-2)$ and the largest power of $(x-2i)$ in the elementary divisors, which is $m(x) = (x-2)^3(x-2i)^2$.

□

8. Consider the following group

$$G = \frac{\mathbb{Z}}{120\mathbb{Z}} \times \frac{\mathbb{Z}}{50\mathbb{Z}}$$

(a) Express G as a direct sum of groups of the form $\mathbb{Z}/p^k\mathbb{Z}$ for (not necessarily distinct) prime integers p and positive integers k.

(b) Express G in the form

$$G \cong \bigoplus_{i=1}^{u} \frac{\mathbb{Z}}{m_i\mathbb{Z}},$$

where m_i divides m_{i+1} for each $i < u$.

Solution:

(a) Note that $120 = 2^3 \cdot 3 \cdot 5$. By the Chinese Remainder Theorem,

$$\mathbb{Z}/120\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Also, $50 = 2 \cdot 5^2$. By the Chinese Remainder Theorem,

$$\mathbb{Z}/50\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}.$$

Thus,

$$\begin{aligned} G &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\ &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}. \end{aligned}$$

(b) Using the Chinese Remainder Theorem, write

$$\mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \cong \mathbb{Z}/600\mathbb{Z}$$

Similarly,

$$Z/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}.$$

Therefore,

$$G \cong \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/600\mathbb{Z},$$

and $10 \mid 600$.

□

9. Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Make sure you prove that it is the minimal polynomial, not just some polynomial of which it is a root.

Solution: Let $\alpha = \sqrt{2} + \sqrt{3}$. Observe

$$\begin{aligned} \alpha &= \sqrt{2} + \sqrt{3} \\ \alpha^2 &= 5 + 2\sqrt{2}\sqrt{3} \\ (\alpha^2 - 5)^2 &= 4(2)(3) \\ \alpha^4 - 10\alpha^2 + 25 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0 \end{aligned}$$

Then α is a root of the polynomial $m(x) = x^4 - 10x^2 + 1$. It remains to show that $m(x)$ is the minimal polynomial of α by showing that $m(x)$ is irreducible over $\mathbb{Q}$. By Gauss' Lemma, it is sufficient to show that $m(x)$ is irreducible over $\mathbb{Z}$.

By the Rational Roots Theorem, the only possible roots of $m(x)$ are ± 1, neither of which are roots of $m(x)$. Therefore, $m(x)$ has no linear factors. Suppose $m(x)$ can be written as a product of two irreducible quadratic polynomials. Without loss of generality, assume these factors are monic. Write $m(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd$ for some $a, b, c, d \in \mathbb{Z}$. Comparing the constant terms, $bd = 1$, so either $b = d = 1$ or $b = d = -1$. Comparing the x^3 terms of the two polynomials, $a + c = 0$, so $a = -c$. Now comparing the x^2 terms: $b + d + ac = 2b - a^2 = -10$. If $b = 1$, then $a^2 = 10$, a contradiction since $a \in \mathbb{Z}$ and 10 is not a perfect square in $\mathbb{Z}$. If $b = -1$, then $a^2 = 8$, again a contradiction. Therefore, $m(x)$ cannot be written as a product of quadratic polynomials, implying that $m(x)$ is irreducible. Hence, $m(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. □

Note: If $p(x)$ is monic and $p(x) = (ax^2 + bx + c)(rx^2 + sx + t)$, then $ar = 1$. So $p(x) = (ax^2 + bx + c)(rx^2 + sx + t) = (ar)(ax^2 + bx + c)(rx^2 + sx + t) = r(ax^2 + bx + c)(a(rx^2 + sx + t) = (rax^2 + rbx + rc)(arx^2 + asx + at) = (x^2 + rbx + rc)(x^2 + asx + at)$, so you may assume that the factors are also monic.

10. Let $F \subset K \subset L$ be field extensions. Assume that $F \subset L$ is a Galois field extension and that its Galois group is abelian. Be sure to give reasons for your answers to (a) and (b).

(a) Is $K \subset L$ a Galois field extension?

(b) Is $F \subset K$ a Galois field extension?

Solution:

(a) Since $F \subset L$ is a Galois extension, L is the splitting field of a separable polynomial $f(x) \in F[x]$ over F. Since $F[x] \subset K[x]$, L is also the splitting field of a separable polynomial over K. Thus, $K \subset L$ is a Galois field extension.

(b) By the Fundamental Theorem of Galois Theory, $F \subset K$ is a Galois extension if and only if the subgroup of $\mathrm{Gal}(L/F)$ that fixes K is normal. Since $\mathrm{Gal}(L/F)$ is abelian, every subgroup of $\mathrm{Gal}(L/F)$ is normal, so $F \subset K$ is a Galois field extension.

□

August 2009

1. Let V be a real vector space with subspaces A, B and X and with $A \subseteq B$. Prove that if $A + X = B + X$ and $A \cap X = B \cap X$, then $A = B$.

Solution: Let $b \in B$. If $b \in X$, then $b \in B \cap X = A \cap X \subset A$, as required. Otherwise, $b \notin X$ but $b \in B + X = A + X$. Therefore, there exist $a \in A$, $x \in X$ such that $b = a + x$. Since $x = b - a$ and B is a vector space, $x \in B$. But then $x \in B \cap X = A \cap X$. Therefore, $x \in A$ and $b = a + x \in A$ since A is a vector space. Thus, $B \subset A$ and $A = B$. □

2.

(a) Let G be a finite abelian and let p be a prime number that divides the order of G. Without using the Fundamental Theorem of Finite Abelian Groups, prove that G contains an element of order p.

(b) Let $G = \{1 = g_1, g_2, \ldots, g_n\}$ be a finite abelian group. If $g_1 g_2 \cdots g_n \neq 1$, prove that the order of G must be even.

Solution:

(a) We prove this by induction on $|G|$. If $|G| = p$, then G is cyclic of order p (essentially by Lagrange's Theorem), so any generator of G has order p. Suppose $p \mid n$, let G be a group of order n, and suppose the conclusion holds for all groups of order $m < n$ such that $p \mid m$. Let $x \in G$. If p divides $|x|$, then $|x| = pk$ for some $k \in \mathbb{N}$, and it is clear that x^k has order p.

Suppose p does not divide $|x|$. Let $N = \langle x \rangle$. Since G is abelian, N is normal in G. Note that N is proper since p does not divide $|N|$. Now $|G/N| = \frac{|G|}{|N|}$, so

$$|G| = |N| \cdot |G/N|.$$

Since p is prime and p divides $|N| \cdot |G/N|$, either p divides $|N|$ or p divides $|G/N|$. But p does not divide $|N|$, so p divides $|G/N|$. By the inductive hypothesis, G/N contains an element of order p. Let yN be an element of G/N of order p. Then $(yN)^p = y^p N = N$, which implies that $y^p \in N$. However, $y \notin N$ since $p > 1$. This implies that $\langle y^p \rangle \subsetneq \langle y \rangle$ since the former is contained in N and the latter is not. Therefore, $|y^p| < |y|$. Since $|y^p| = \frac{|y|}{\gcd(p,|y|)} < |y|$, $\gcd(p, |y|) > 1$, so $\gcd(p, |y|) = p$. Thus, p divides $|y|$. But then G has an element of order p.

OR

Let $\#G$ denote the order of G. If $\#G = p$, then any non-identity element has order p as p is prime. So assume $n > p$, $p \mid n$, and the result is true for all groups with size less than n and divisible by p. Since $p \mid n$ and $n > p$, $\#G$ is not prime. Then G has a proper non-trivial subgroup, say G. Since G is abelian, H is normal and G/H is a group. Now

$$\#H \cdot \#(G/H) = \#G = n,$$

either p divides $\#H$ or $\#(G/H)$. By induction, H or G/H has an element of order p. If H does, so too does G. Now suppose G/H has an element of order p, say $\overline{g}$. Let m denote the order of g in G. Then $g^m = 1$ in G so that $\overline{g}^m = \overline{1}$ in G/H. But then $p \mid m$. Thus, g has order divisible by p so that $g^{m/p}$ is an element of G with order p.

(b) Suppose that the order of G is odd. Then $2 \nmid |G|$, implying that G has no element of order 2. Therefore, if $g \neq 1$, then $g \neq g^{-1}$. Reindex the elements of G as follows: $g_1 = 1$ and for each even k, $g_{k+1} = g_k^{-1}$. Therefore, $g_1 g_2 g_3 \cdots g_{n-1} g_n = 1(g_2 g_3)(g_4 g_5) \cdots (g_{n-1} g_n) = 1$.

□

Note: One need only consider the primes dividing $|G|$ since Lagrange's Theorem forces G to contain no elements of prime order not dividing $|G|$.

3. Prove that no group of order 48 is simple.

Solution: Let G be a group of order $48 = 2^3 \cdot 3$. The divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24, and 48. For each prime p, let $n_p(G)$ denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_2(G) \equiv 1 \mod 2$ and $n_2(G)$ divides 48. The only possibilities are $n_2(G) = 1$ and $n_2(G) = 3$. If $n_2(G) = 1$, then G has a unique Sylow 2-subgroup, which is necessarily normal. In this case, G has a proper, nontrivial, normal subgroup, implying that G is not simple.

Otherwise, $n_2(G) = 3$. In this case, let X denote the set of Sylow 2-subgroups and let G act on X by conjugation, i.e. $g \cdot S = gSg^{-1}$ for all $g \in G, S \in X$. Since any two Sylow 2-subgroups are conjugate in G, this action must be nontrivial. Therefore, the action of G on X induces a nontrivial homomorphism $\phi : G \to S_3$. Since $|G| = 48$ and $|S_3| = 3! = 6$, this homomorphism cannot be injective. Therefore, $\ker \phi$ is a proper, nontrivial, normal subgroup of G. Thus, G is not simple. □

4.

(a) Let E be an Euclidean space—that is, a finite dimensional vector space over $\mathbb{R}$, the real numbers, with a positive definite, symmetric, inner product denoted by $(\ ,\ )$. Let $E^* = \mathrm{Hom}_{\mathbb{R}}(E, \mathbb{R})$ be the dual space. Prove that the map $\phi : E \to E^*$, given by $\phi(v) = \rho_v$, where $\rho_v(w) = (w, v)$ for all $v, w \in E$, is an isomorphism.

(b) Let E be the Euclidean space consisting of all polynomials in one variable with real coefficients of degree less than or equal to 2 with inner product given by $(f,g) = \int_0^1 f(t)g(t)\,dt$. Let α be the element of E^* given by $\alpha(f) = f(1)$. In the notation of part (a), find the $v \in E$ such that $\phi(v) = \alpha$.

Solution:

(a) Let $v, v' \in V$, $a \in |R$. Observe $\rho_{v+v'}(w) = (w, v+v') = (w,v) + (w,v') = \rho_v(w) + \rho_{v'}(w)$ for all $w \in V$. Thus, $\rho_{v+v'} = \rho_v + \rho_{v'}$. This proves that $\phi(v+v') = \phi(v) + \phi(v')$. For any $w \in$, $\rho_{av}(w) = (w, av) = a(w,v) = a\rho_v(w)$. Therefore, $\phi(av) = a\phi(v)$. But then ϕ is a linear transformation.

Suppose $v \in \ker\phi$. Then $\rho_v(w) = 0$ for all $w \in V$. In particular, $\rho_v(v) = (v,v) = 0$. Since the form is positive definite, $v = 0$. But then $\ker\phi = 0$ so ϕ is injective.

Note that E has a orthonormal basis $\{e_1, e_2, \ldots, e_n\}$. If $f \in E^*$, let $c_i = f(e_i)$ for $i = 1, 2, \ldots, n$. Define $v = c_1e_1 + \cdots + c_ne_n$. Then for any $w = a_1e_1 + \cdots + a_ne_n \in E$,

$$\begin{aligned}(w,v) &= (a_1e_1 + \cdots + a_ne_n, c_1e_1 + \cdots + c_ne_n)\\ &= a_1c_1(e_1,e_1) + \cdots + a_nc_n(e_n,e_n)\\ &= a_1f(e_1) + \cdots + a_nf(e_n)\\ &= f(a_1e_1 + \cdots + a_ne_n)\\ &= f(w).\end{aligned}$$

Therefore, $\rho_v = f$, which implies that ϕ is surjective. Therefore, ϕ is an isomorphism.

(b) The goal is to find a $v \in V$ such that $\rho_v(w) = (w,v) = w(1)$ for all $w \in E$. Take $w = 1$, $w' = x$, $w'' = x^2$. Write $v = a_0 + a_1x + a_2x^2$. Since $w(1) = w'(1) = w''(1) = 1$, it follows that

$$1 = (w,v) = \int_0^1 (a_0 + a_1x + a_2x^2)\,dx = \left(a_0x + \frac{1}{2}a_1x^2 + \frac{1}{3}a_2x^3\right)\Big|_0^1 = a_0 + \frac{1}{2}a_1 + \frac{1}{3}a_2$$

$$1 = (w',v) = \int_0^1 (a_0x + a_1x^2 + a_2x^3)\,dx = \left(\frac{1}{2}a_0x^2 + \frac{1}{3}a_1x^3 + \frac{1}{4}a_2x^4\right)\Big|_0^1 = \frac{1}{2}a_0 + \frac{1}{3}a_1 + \frac{1}{4}a_2$$

$$1 = (w'',v) = \int_0^1 (a_0x^2 + a_1x^3 + a_2x^4)\,dx = \left(\frac{1}{3}a_0x^3 + \frac{1}{4}a_1x^4 + \frac{1}{5}a_2x^5\right)\Big|_0^1 = \frac{1}{3}a_0 + \frac{1}{4}a_1 + \frac{1}{5}a_2$$

This leads to a system of three equations in three unknowns which can be solved:

$$\begin{aligned}a_0 + \frac{1}{2}a_1 + \frac{1}{3}a_2 &= 1\\ \frac{1}{2}a_0 + \frac{1}{3}a_1 + \frac{1}{4}a_2 &= 1\\ \frac{1}{3}a_0 + \frac{1}{4}a_1 + \frac{1}{5}a_2 &= 1\end{aligned}$$

The solution to this is $a_0 = 3$, $a_1 = -24$, $a_2 = 30$. Hence, $v = 3 - 24x + 30x^2$.

□

5. Let S_n denote the symmetric group on n letters with A_n the alternating subgroup. Let $\alpha \in A_n$. $C_{S_n}(\alpha)$ denotes the centralized in S_n of α. Similarly, $C_{A_n}(\alpha)$ denotes the centralizer in A_n of α.

(a) Prove that $[A_n : C_{A_n}(\alpha)]$ is equal to either $[S_n : C_{S_n}(\alpha)]$ or $\frac{1}{2}[S_n : C_{S_n}(\alpha)]$. (Hint: Consider the natural homomorphism from S_n to S_n/A_n.)

(b) Prove that if α is centralized by some permutation not in A_n, then the conjugacy class of α in A_n is equal to the conjugacy class of α in S_n.

Solution:

(a) Consider the homomorphisms

$$C_{A_n}(\alpha) \xrightarrow{i} C_{S_n}(\alpha) \xrightarrow{\phi} S_n \xrightarrow{\sigma} \{\pm 1\},$$

where i and ϕ are the identity functions and σ is the sign map. There are two cases: either $\operatorname{im}(\sigma \circ \phi) = \{1\}$ or $\operatorname{im}(\sigma \circ \phi) = \{\pm 1\}$. If $\operatorname{im}(\sigma \circ \phi) = \{1\}$, then every permutation that centralizes α must be even. Therefore, $C_{A_n}(\alpha) = C_{S_n}(\alpha)$. This implies that

$$[S_n \colon C_{S_n}(\alpha)] = [S_n \colon A_n]\ [A_n \colon C_{A_n}(\alpha)] = 2[A_n \colon C_{A_n}(\alpha)].$$

Thus, $[A_n \colon C_{A_n}(\alpha)] = \frac{1}{2}[S_n \colon C_{S_n}(\alpha)]$.

Otherwise, $\operatorname{im}(\sigma \circ \phi) = \{\pm 1\}$. Note that $\ker(\sigma \circ \phi) = C_{A_n}(\alpha)$. By the First Isomorphism Theorem,

$$C_{S_n}(\alpha)/C_{A_n}(\alpha) \cong \{\pm 1\}.$$

In particular, $[C_{S_n}(\alpha) \colon C_{A_n}(\alpha)] = 2$. Therefore,

$$2 = \frac{|C_{S_n}(\alpha)|}{|C_{A_n}(\alpha)|} = \frac{|S_n|}{|A_n|},$$

which implies that

$$[S_n \colon C_{S_n}(\alpha)] = \frac{|S_n|}{|C_{S_n}(\alpha)|} = \frac{|A_n|}{|C_{A_n}(\alpha)|} = [A_n \colon C_{A_n}(\alpha)],$$

as required.

(b) Note that if S_n acts on itself by conjugation, then the stabilizer of α is $C_{S_n}(\alpha)$. If A_n is acting on S_n by conjugation, then the stabilizer of α is $C_{A_n}(\alpha)$. Let $\mathcal{O}_{A_n}(\alpha)$ and $\mathcal{O}_{S_n}(\alpha)$ denote the orbit of α in the action of A_n on S_n and the action of S_n on itself, respectively. If α is centralized by some permutation not in A_n, then $\text{im}(\sigma \circ \phi) \neq \{\pm 1\}$, so $\text{im}(\sigma \circ \phi) = \{\pm 1\}$. In this case, $[S_n \colon C_{S_n}(\alpha)] = [A_n \colon C_{A_n}(\alpha)]$. By the Orbit-Stabilizer Theorem,

$$|\mathcal{O}_{A_n}(\alpha)| = [A_n \colon C_{A_n}(\alpha)] = [S_n \colon C_{S_n}(\alpha)] = |\mathcal{O}_{S_n}(\alpha)|.$$

Since $\mathcal{O}_{A_n}(\alpha) \subset \mathcal{O}_{S_n}(\alpha)$ and both sets are finite. It follows that $\mathcal{O}_{A_n}(\alpha) = \mathcal{O}_{S_n}(\alpha)$. Hence, the conjugacy class of α in A_n is equal to the conjugacy class of α in S_n.

□

6.

(a) Let A be an n-by-n matrix over the complex numbers, λ a complex number, and k a nonnegative integer. Explain the significance of $\text{rank}[(A - \lambda I_n)^{k+1}] - \text{rank}[(A - \lambda I_n)^k]$ in the Jordan canonical form of A.

(b) Let A and B be n-by-n matrices over the complex numbers such that for every complex number λ and every positive integer k, $\text{rank}[(A - \lambda I_n)^k] = \text{rank}[(B - \lambda I_n)^k]$. Prove that A and B are similar.

Solution:

(a) Using the Rank-Nullity Theorem,

$$\begin{aligned}\text{rank}[(A - \lambda I_n)^{k+1}] - \text{rank}[(A - \lambda I_n)^k] &= (n - \text{nullity}[(A - \lambda I_n)^{k+1}]) - (n - \text{nullity}[(A - \lambda I_n)^k]) \\ &= \text{nullity}[(A - \lambda I_n)^k] - \text{nullity}[(A - \lambda I_n)^{k+1}]\end{aligned}$$

Therefore, $|\,\text{rank}[(A - \lambda I_n)^{k+1}] - \text{rank}[(A - \lambda I_n)^k]\,|$ is the number of Jordan blocks in the Jordan canonical form with eigenvalue λ and size at least $k + 1$.

(b) By the Rank-Nullity Theorem, it is clear that $\text{nullity}[(A - \lambda I_n)^k] = \text{nullity}[(B - \lambda I_n)^k]$ for all $\lambda \in \mathbb{C}$, $k \in \mathbb{N}$. The claim is that A and B have the same Jordan canonical form. Let $\lambda \in \mathbb{C}$. Since $\text{nullity}(A - \lambda I_n) = \text{nullity}(B - \lambda I_n)$, A and B have the same number of Jordan blocks associated to the number λ. Since

$$\text{nullity}[(A - \lambda I_n)^2] - \text{nullity}(A - \lambda I_n) = \text{nullity}[(B - \lambda I_n)^2] - \text{nullity}(B - \lambda I_n),$$

A and B have the same number of Jordan blocks associated to the number λ of size at least 2. Therefore, A and B have the same number of Jordan blocks associated to

the number λ of size 1. Assume that A and B have the same number of Jordan blocks associated to the number λ of size $1, 2, \ldots,$ and k. Since

$$\text{nullity}[(A-\lambda I_n)^{k+2}] - \text{nullity}[(A-\lambda I_n)^{k+1}] = \text{nullity}[(B-\lambda I_n)^{k+2}] - \text{nullity}[(B-\lambda I_n)^{k+1}],$$

A and B have the same number of Jordan blocks of size at least $k+2$ and since they have the same number of blocks of size at most k, they must have the same number of Jordan blocks of size $k+1$. By induction on k, A and B have the same number of Jordan blocks of size k for all $k \in \mathbb{N}$ associated to each complex number λ. Therefore, A and B have the same Jordan canonical form, which implies that A and B are similar.

□

7. Let $\alpha = \sqrt{7} + \sqrt{2}$.

(a) Find the minimal polynomial of α over $\mathbb{Q}$, the field of rational numbers.

(b) Find the Galois group of the field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$. (Hint: First prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{7}, \sqrt{2})$.)

Solution:

(a) Observe that

$$\begin{aligned} \alpha &= \sqrt{7} + \sqrt{2} \\ \alpha^2 &= 9 + 2\sqrt{2}\sqrt{7} \\ (\alpha^2 - 9) &= 4(2)(7) \\ \alpha^4 - 18\alpha^2 + 81 &= 56 \\ \alpha^4 - 18\alpha^2 + 25 &= 0 \end{aligned}$$

Therefore, α is a root of $m(x) = x^4 - 18x^2 + 25$. It remains to show that $m(x)$ is irreducible over $\mathbb{Q}$. By Gauss' Lemma, it is sufficient to show that $m(x)$ is irreducible over $\mathbb{Z}$. By the Rational Roots Theorem, the only possible rational roots of $m(x)$ are $\pm 1, \pm 5, \pm 25$, none of which are zeros for $m(x)$. Therefore, $m(x)$ has no factors of degree 1. It remains to show that $m(x)$ cannot be factored into a product of irreducible quadratic equations over $\mathbb{Z}$. Suppose that $m(x) = (x^2 + az + b)(x^2 + cx + d)$ for $a, b, c, d \in \mathbb{Z}$ (we can without loss of generality assume that the factors are monic). Then

$$m(x) = (x^2 + az + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.$$

Comparing coefficients, $bd = 25$. If $b = 1, d = 25$, then $b + d = 26$ so comparing the coefficients of x^2, x^3, we have

$$0 = a + c$$
$$0 = ac + 26$$

Implying $a = -c$ so that $c^2 = 26$, a contradiction as $c \in \mathbb{Z}$. If $b = 2, d = 5$, then $b + d = 10$. Repeating the process from above,

$$0 = a + c$$
$$0 = ac + 10$$

Then $a = -c$ so that $c^2 = 10$, a contradiction as before. The negative cases are handled mutatis mutandis. Note this completes the cases as we can always switch the ordering/labeling of the quadratic factors. Thus, $m(x)$ is not the product of two irreducible quadratic polynomials over $\mathbb{Z}$, so $m(x)$ is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$.

(b) It is clear that $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{7})$. Since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{7})$, it follows $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{7}, \sqrt{2})$. Notice that

$$(\sqrt{7} + \sqrt{2})(\sqrt{7} - \sqrt{2}) = 7 - 2 = 5.$$

This implies that $(\sqrt{7} + \sqrt{2})^{-1} = \frac{1}{5}(\sqrt{7} - \sqrt{2}) \in \mathbb{Q}(\alpha)$. Then $\sqrt{7} - \sqrt{2} \in \mathbb{Q}(\alpha)$. Now

$$\frac{1}{2}\big((\sqrt{7} + \sqrt{2}) + (\sqrt{7} - \sqrt{2})\big) = \sqrt{7} \in \mathbb{Q}(\alpha)$$
$$\frac{1}{2}\big((\sqrt{7} + \sqrt{2}) - (\sqrt{7} - \sqrt{2})\big) = \sqrt{2} \in \mathbb{Q}(\alpha)$$

Thus, $\mathbb{Q}(\alpha)$ is a field containing $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{7}$. Since $\mathbb{Q}(\sqrt{2}, \sqrt{7})$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{7}$, $\mathbb{Q}(\sqrt{2}, \sqrt{7}) \subset \mathbb{Q}(\alpha)$. Therefore, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{7})$.

Now consider $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Since σ fixes $\mathbb{Q}$, σ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{7})$. Now since $(\sqrt{2})^2 - 2 = 0$,

$$\sigma((\sqrt{2})^2 - 2) = \sigma(0)$$
$$\sigma(\sqrt{2})^2 - \sigma(2) = \sigma(0)$$
$$\sigma(\sqrt{2})^2 - 2 = 0,$$

i.e. that $\sigma(\sqrt{2})$ is a root of $m(x) = x^2 - 2$. There are now two possibilities: either $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$.

Similarly, there are two possibilities for $\sigma(\sqrt{7})$: either $\sigma(\sqrt{7}) = \sqrt{7}$ or $\sigma(\sqrt{7}) = -\sqrt{7}$. Thus, there are four elements of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

$$\begin{aligned} \sigma_1(\sqrt{2}) &= \sqrt{2} & \sigma_2(\sqrt{2}) &= \sqrt{2} \\ \sigma_1(\sqrt{7}) &= \sqrt{7} & \sigma_2(\sqrt{7}) &= -\sqrt{7} \\ \sigma_3(\sqrt{2}) &= -\sqrt{2} & \sigma_4(\sqrt{2}) &= -\sqrt{2} \\ \sigma_3(\sqrt{7}) &= \sqrt{7} & \sigma_4(\sqrt{7}) &= -\sqrt{7} \end{aligned}$$

It is clear that σ_1 is the identity of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ and that every non-identity element has order 2. Thus, $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V_4$, the Klein 4-group.

□

8. Let R be a Principal Ideal Domain.

(a) Let $I = (x)$ be a nonzero ideal of R. Prove that I is a maximal ideal if and only if x is irreducible.

(b) Let I be a nonzero ideal of R. Prove that I is a maximal ideal if and only if I is a prime ideal.

Solution:

(a) Suppose that I is a maximal ideal and that $x = rs$ for some $r, s \in R$. Without loss of generality, suppose r is not a unit. Then $x \in (r)$ so that $(x) \subset (r)$. Since r is not a unit, $(r) \neq R$. So $(x) = (r)$ by the maximality of (x). This implies that $r = ux$ for some $u \in R^\times$. Therefore, $x = rs = uxs$, which implies $1 = us$, i.e. that s is a unit. Therefore, x is irreducible.

Suppose that x is irreducible and J is an ideal such that $I \subset J \subset R$. Then $J = (y)$ for some $y \in R$. Since $x \in J$, $x = ry$ for some $r \in R$. However, x was assumed to be irreducible, so either r is a unit or y is a unit. If r is a unit, then $(x) = (y)$, i.e. $I = J$. If y is a unit, then the ideal J contains a unit, which implies that $J = R$. Therefore, I is a maximal ideal.

(b) Since I is a maximal ideal, the quotient ring R/I is a field. But then R/I is an integral domain so that I must be prime. [Recall, I is a prime ideal if and only if R/I is an integral domain.]

Suppose $I = (x)$ is a prime ideal. We claim that x is irreducible. If $x = ry$ for some $r, y \in R$, then $y \in I$. Since I is a prime ideal, either $r \in I$ or $y \in I$. Without loss of generality, assume that $r \in I$. Then $r = xu$ for some $u \in R$. This implies $x = ry = xuy$. Then $1 = uy$. Therefore, y is a unit. But then x is irreducible. Therefore, $I = (x)$ is maximal.

□

9.

(a) Give an example of a commutative ring with at least two simple modules that are not isomorphic.

(b) Let R be a commutative ring and let M be a simple R-module. Prove that any nonzero endomorphism of M is an isomorphism.[4]

Solution:

(a) Take the commutative ring $\mathbb{Z}$ and the $\mathbb{Z}$-modules $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. These modules are not isomorphic since they have different cardinalities. Clearly, $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ have no proper, nontrivial subgroups, which implies they are both simple.

(b) Let $f : M \to M$ be a nonzero endomorphism. Then $\ker f$ is a submodule of M. Since M is simple, either $\ker f = 0$ or $\ker f = M$. It was assumed that f is nonzero, so $\ker f \neq M$. Thus, $\ker f = 0$ and f is injective. Furthermore, the image of f is a submodule of M. Since M is simple, either $\operatorname{im} f = 0$ or $\operatorname{im} f = M$. Since f is nonzero, $\operatorname{im} f \neq 0$. Therefore, $\operatorname{im} f = M$ and f is surjective. Therefore, f is an isomorphism.

□

10. Suppose E is a finite field. Prove that the order of E is p^n, where p is a prime number and n is a positive integer.

Solution: Since E is a finite field, it has characteristic p for some prime number p. In this case, E contains a subfield isomorphic to $\mathbb{F}_p$, the field with p elements. In this case, E can be viewed as a vector space over $\mathbb{F}_p$, so $E \cong \mathbb{F}_p^n$ for some $n \in \mathbb{N}$, the latter clearly has order p^n. □

[4] This is Schur's Lemma.

January 2010

1. Recall that a subgroup H of a group G is called *characteristic* if $\phi(H) \subseteq H$ for every automorphism ϕ of G.

(a) Prove that characteristic subgroups are always normal.

(b) Let P be a p-Sylow subgroup of a finite group G and assume that P is normal in G. Prove that P is a characteristic subgroup of G.

Solution:

(a) Let $x \in G$ and define $\phi_x : G \to G$ via $\phi_x(g) = xgx^{-1}$. We claim that ϕ_x is an automorphism of G. Clearly, ϕ is a homomorphism as

$$\phi_x(g)\phi_x(h) = (xgx^{-1})(xhx^{-1}) = x(gh)x^{-1} = \phi_x(gh)$$

Now $g \in \ker\phi_x$ if and only if $xgx^{-1} = 1$ if and only if $g = x^{-1}x = 1$. Therefore, $\ker\phi_x = \{1\}$ so that ϕ_x is injective. Furthermore for any $g \in G$, $\phi_x(x^{-1}gx) = x(x^{-1}gx)x^{-1} = g$ so that ϕ_x is surjective. But then ϕ is an automorphism of G.

By assumption, $\phi_x(H) \subset H$ for all $x \in G$. That is, $xHx^{-1} \subset H$ for all $x \in G$. Then H is a normal subgroup of G.

(b) We claim that P is the unique Sylow p-subgroup of G (hence normal). Suppose Q is also a Sylow p-subgroup of G. Then by Sylow's Theorem, P and Q are conjugate, i.e. there is a $x \in G$ such that $xPx^{-1} = Q$. By assumption, P is normal in G so that $Q \subset P$. But P and Q have the same (finite) order, but then $P = Q$, as claimed.

Now if ϕ is an automorphism of G, then $\phi(P)$ is a subgroup of G with the same order as P, i.e. $\phi(P)$ is a Sylow p-subgroup of G. But by uniqueness (proved above), it must be that $\phi(P) = P$. Thus, P is a characteristic subgroup of G.

□

2. Prove that there are no simple groups of order 20 or 57.

Solution: Note that if $|G| = 20 = 2^2 \cdot 5$. Let $n_5(G)$ denote the number of Sylow 5-subgroups of G. By Sylow's Theorem, $n_5(G) \equiv 1 \mod 5$ and $n_5(G)$ divides 4. But then it must be that $n_5(G) = 1$ so that G contains a unique Sylow 5-subgroup. But by Sylow's Theorem, unique Sylow p-subgroups are normal so that this Sylow 5-subgroup is necessarily normal. Hence, a group of order 20 must contain a proper, nontrivial, normal subgroup and therefore cannot be simple.

If $|G| = 57 = 3 \cdot 19$, let $n_{19}(G)$ denote the number of Sylow 19-subgroups of H. By Sylow's Theorem, $n_{19}(H) \equiv 1 \mod 19$ and $n_{19}(H)$ divides $|H| = 57$. But then $n_{19}(G) = 1$.

Then as above, G must contain a proper, nontrivial, normal subgroup. Therefore, G cannot be simple. □

3. Let G be an abelian group of order n and assume that G has at most one subgroup of order d for each $d \mid n$. Prove that G is a cyclic group.

Solution: By the Fundamental Theorem of Finitely Generated Abelian Groups (or Fundamental Theorem of Finite Abelian Groups, if one prefers), we have

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}$$

where the p_i are (not necessarily distinct) primes and $\alpha_i \in \mathbb{N}$. If $p_i = p_j$, then $\mathbb{Z}/p_i^{\alpha_i}$ and $\mathbb{Z}/p_j^{\alpha_j}$ each contain a subgroup of order p_i. Hence, G has at most one subgroup for every divisor of n. This implies that the p_i as distinct primes, hence relatively prime. But then by the Chinese Remainder Theorem,

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k} \cong \mathbb{Z}/(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})\mathbb{Z}$$

which is cyclic. □

4. Let R be a commutative ring such that the polynomial ring $R[x]$ is a PID. Prove that R is a field.

Solution: Let (x) denote the ideal generated by x in R. If (x) were a maximal ideal of $R[x]$, then $R[x]/(x) \cong R$ would be a field. It remains then to show that (x) is maximal. However since $R[x]$ is assumed to be a PID, (x) is maximal if and only if (x) is irreducible if and only if x is irreducible. Suppose $x = p(x)q(x)$ for some $p(x), q(x) \in R[x]$. Clearly, $p(x)$ and $q(x)$ must have degree at most 1 and cannot both be degree 1. Without loss of generality, assume that $p(x)$ has degree 0, i.e. $p(x) := p \in R$ is a 'constant'. Now $q(x)$ has degree one. Write $q(x) = ax + b$ for some $a, b \in R$. Then $x = pax + pb$ which implies $pa = 1$. But then p is a unit. Therefore, x is irreducible. The result then follows. □

5. Recall that a $n \times n$ matrix A is normal if $AA^* = A^*A$. Prove that if A is a normal lower triangular matrix over the complex numbers, the A is a diagonal matrix.

Solution: We prove this by induction on n. If $n = 1$, the result is trivial. If $n = 2$, suppose $A = (a_{ij})$. Then

$$AA^* = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} \\ 0 & \overline{a_{22}} \end{pmatrix} = \begin{pmatrix} a_{11}\overline{a_{11}} & a_{11}\overline{a_{21}} \\ \overline{a_{11}}a_{21} & a_{22}\overline{a_{22}} + a_{21}\overline{a_{21}} \end{pmatrix}$$

$$A^*A = \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} \\ 0 & \overline{a_{22}} \end{pmatrix}\begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11}\overline{a_{11}} + a_{21}\overline{a_{21}} & a_{22}\overline{a_{21}} \\ a_{21}\overline{a_{22}} & a_{22}\overline{a_{22}} \end{pmatrix}$$

Since $AA^* = A^*A$, $a_{11}\overline{a_{11}} = a_{11}\overline{a_{11}} + a_{21}\overline{a_{21}}$. Thus, $a_{21}\overline{a_{21}}$. Thus, $a_{21}\overline{a_{21}} = |a_{21}|^2 = 0$ so $a_{21} = 0$. This implies that

$$A = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}$$

so that A is diagonal.

Now assume that the result is true for any normal lower triangular $(n-1) \times (n-1)$ matrix and let $A = (a_{ij})$ be a normal lower triangular $n \times n$ matrix. Then

$$AA^* = \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} & \overline{a_{31}} & \cdots & \overline{a_{n1}} \\ 0 & \overline{a_{22}} & \overline{a_{32}} & \cdots & \overline{a_{n2}} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \overline{a_{nn}} \end{pmatrix}$$

From this, observe that the $(1,1)$-entry in AA^* is $|a_{11}|^2$. Now observe that

$$A^*A = \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} & \overline{a_{31}} & \cdots & \overline{a_{n1}} \\ 0 & \overline{a_{22}} & \overline{a_{32}} & \cdots & \overline{a_{n2}} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \overline{a_{nn}} \end{pmatrix} \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}$$

The $(1,1)$-entry of A^*A is $|a_{11}|^2 + |a_{21}|^2 + \cdots + |a_{n1}|^2$. Since $AA^* = A^*A$, it follows that

$$\begin{aligned} |a_{11}|^2 &= |a_{11}|^2 + |a_{21}|^2 + |a_{31}|^2 + \cdots + |a_{n1}|^2 \\ 0 &= |a_{21}|^2 + |a_{31}|^2 + \cdots + |a_{n1}|^2 \end{aligned}$$

Since $|a_{k1}|^2$ is a positive real number for each k, it follows that $a_{k1} = 0$ for $k > 1$. Thus,

$$C = \left[\begin{array}{c|c} a_{11} & 0 \\ \hline 0 & B \end{array}\right]$$

where B is an $(n-1) \times (n-1)$ is a lower triangular matrix. Since A is normal, it is immediate that B is normal. The inductive hypothesis implies that B is a diagonal matrix. Hence, A is also a diagonal matrix. The result now follows by induction. □

6. Let $R = \mathbb{Z}[x]$ and let $I = (2, x)$. Prove that I is not a free R-module but it is torsion free.

Solution: Since $\mathbb{Z}$ is an integral domain, $\mathbb{Z}[x]$ is an integral domain. Moreover, I is an ideal of R. If $r(x) \in R$ and $p(x) \in I$ are such that $r(x) \cdot p(x) = 0$, it must be that $r(x) = 0$ since R is an integral domain. But then $\text{Tor}(I) = \{0\}$, i.e. I is torsion free.

Now if I is an ideal in an integral domain R and I is a free R-module, it must be that I is principal. To see this, suppose $\mathcal{B}$ were a basis for I as an R-module and $|\mathcal{B}| > 1$. Let

$x, y \in \mathcal{B}$ be distinct. Then $x \cdot y + (-y) \cdot x = 0 = 0 \cdot x + 0 \cdot y$ are two different expressions for 0 as a linear combination of basis elements of $\mathcal{B}$, a contradiction. Then it must be that $\mathcal{B} = 1$ and I is principal.

Therefore, to show I is not free as an R-module, it suffices to show that I is not a principal ideal in R. Suppose to the contrary $I = (p(x))$ for some $p(x) \in R$. Then $2 \in (p(x))$ so that $2 = r(x)p(x)$. But then $p(x)$ must be a constant polynomial. Now $\mathbb{Z}[x]$ is a UFD, implying that then $p(x) \in \{\pm 1, \pm 2\}$. If $p(x) = \pm 1$, then $I = \mathbb{Z}[x]$, which cannot be since$3 \in \mathbb{Z}[x]$ and $3 \notin I$. If $p(x) = \pm 2$, we can without loss of generality assume $p(x) = 2$ (since $(2) = (-2)$). We know $x \in (p(x)) = (2)$ so that $x = 2r(x)$ for some $r(x) \in \mathbb{Z}[x]$. But then $r(x)$ must have degree 1. Write $r(x) = ax + b$ for some $a, b \in R$. But then we must have $2a = 1$, a contradiction as $a \in \mathbb{Z}$. Therefore, $I \neq (p(x))$ so that I cannot be principal. Hence, I is not a free R-module.

OR

By the proof above, we only need show that I is not principal. Suppose to the contrary that $(2, x) = I = (p(x))$. Certainly if $f(x) \in (2, x) = (p(x))$, then $f = 2g(x) + xh(x)$ for some $g(x), h(x) \in R$. But then evaluating at 0 yields $f(0) = 2g(0)$. Then $f(0)$ must be even. Furthermore, we know $2 \in (2, x) = (p(x))$ so that $2 = p(x)g(x)$ for some $g(x) \in R$. But then it must be that $\deg p = 0$ so that $p(x)$ is constant, i.e. $p(x) = p(0) = 2n$ for some $n \in \mathbb{N}$. [Note that $p(x) = \pm 1$ is not possible since $(p(x)) = (2, x) \neq R[x]$.] Now $x \in (p(x))$ so that $x = p(x)h(x) = 2nh(x)$ for some $h(x) \in R$. But evaluating at $x = 1$ gives $1 = 2nh(1)$. But this implies that 1 is even, a contradiction.[5]

□

7. Let F be a finite field. Prove that the product of the non-zero elements of F is -1.

Solution: Suppose that $\operatorname{char} F \neq 2$, i.e. $1 \neq -1$. If $a \in F^\times$ and $a^2 = 1$, then a is a root of the polynomial $p(x) = x^2 - 1 = (x + 1)(x - 1)$, so $a \in \{\pm 1\}$. Therefore, if $a \notin \{\pm 1\}$, $a^{-1} \neq a$. Therefore, the product of the nonzero elements of F is

$$(-1)(1)a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_n a_n^{-1} = -1,$$

as required.

If $\operatorname{char} F = 2$, then $1 = -1$ and $x^2 - 1 = (x - 1)(x + 1) = (x - 1)^2$, which has a unique root of 1. Thus, if $a \in F^\times$ and $a \neq 1$, then $a^{-1} \neq a$. Therefore, the product of the nonzero elements of F is

$$1a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_n a_n^{-1} = 1 = -1,$$

as required. □

[5]Note: it will generally be the case that for a domain D, (a, x) will not be a principal ideal in $D[x]$ for any nonunit $a \in D$.

8. Let $\xi = \sqrt{2+\sqrt{2}}$. Find the minimal polynomial of ξ over $\mathbb{Q}$ and show that $\xi = \sqrt{2-\sqrt{2}}$ is another root of this minimal polynomial. Show that the degree of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$ is 4. Prove that sending ξ to $\xi = \sqrt{2-\sqrt{2}}$ is an automorphism of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$. Describe the Galois group of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$.

Solution: Observe that

$$\begin{aligned} \xi &= \sqrt{2+\sqrt{2}} \\ \xi^2 &= 2+\sqrt{2} \\ (\xi^2-2)^2 &= 2 \\ \xi^4 - 4\xi^2 + 4 &= 2 \\ \xi^4 - 4\xi^2 + 2 &= 0 \end{aligned}$$

Therefore, ξ is a root of the polynomial $m(x) = x^4 - 4x^2 + 2$. Notice that $m(x)$ is irreducible as it is Eisenstein with $p = 2$. Therefore, $m(x)$ is the minimal polynomial of ξ over $\mathbb{Q}$. Since $m(x)$ has degree 4, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg m(x) = 4$.

The same computation as above shows that $\sqrt{2-\sqrt{2}}$ is a root of $m(x)$. Since $m(x)$ is even, we know that $\pm\sqrt{2+\sqrt{2}}$ and $\pm\sqrt{2-\sqrt{2}}$ are roots of $m(x)$. Since $m(x)$ has degree 4, these are the complete roots of $m(x)$.

We claim that $\mathbb{Q}(\xi)$ is the splitting field of $m(x)$ over $\mathbb{Q}$. It is clear that if $m(x)$ splits over a field $F \supset \mathbb{Q}$, then $\mathbb{Q}(\xi) \subset F$. It is then sufficient to show that $\mathbb{Q}(\xi)$ contains all the roots of $m(x)$. Obviously, $\pm x = \pm\sqrt{2+\sqrt{2}} \in \mathbb{Q}(\xi)$. Observe that $(\sqrt{2+\sqrt{2}})^2 = 2+\sqrt{2} \in \mathbb{Q}(\xi)$, so $\xi^2 - 2 = \sqrt{2} \in \mathbb{Q}(\xi)$. Now

$$\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2},$$

which implies that $\sqrt{2-\sqrt{2}} = \dfrac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}(\xi)$. Therefore, $-\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$. Therefore, $\mathbb{Q}(\xi)$ is the splitting field of $m(x)$ over $\mathbb{Q}$.

Since $\mathbb{Q}(\xi)$ is the splitting field of a separable polynomial over $\mathbb{Q}$, $\mathbb{Q}(\xi)/\mathbb{Q}$ is a Galois extension and $|\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})| = [\mathbb{Q}(\xi) : \mathbb{Q}] = 4$. If $\sigma \in \operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, then σ is completely determined by $\sigma(\xi)$. Note that $\sigma(\xi)$ must be a root of the minimal polynomial ξ, so there are only four possibilities for $\sigma(\xi)$. Since $|\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})| = 4$, each of these possible automorphisms must actually be an automorphism. Therefore, sending ξ to $\sqrt{2-\sqrt{2}}$ is an automorphism of $\mathbb{Q}(\xi)$ over $|Q$.

We claim $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Let σ be the automorphism that sends ξ to $\sqrt{2-\sqrt{2}}$. Note that

$$2 + \sigma(\sqrt{2}) = \sigma(2+\sqrt{2}) = \sigma(\xi^2) = \sigma(\xi)^2 = 2-\sqrt{2},$$

which implies that $\sigma(\sqrt{2}) = -\sqrt{2}$. But by a previous computation,

$$\sigma\left(\sqrt{2-\sqrt{2}}\right) = \frac{\sigma(\sqrt{2})}{\sigma(\xi)} = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\xi.$$

Therefore, $\sigma^2(\xi) = \sigma(\sqrt{2-\sqrt{2}}) = -\xi$, which shows that $\sigma^2 \neq 1$. By Lagrange's Theorem, $|\sigma| = 4$. This implies that $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$. □

August 2010

1. Prove that there is no simple group of order 42.

Solution: Let G be a group of order 42. Observe $42 = 2 \cdot 3 \cdot 7$. Let $n_7(G)$ denote the number of Sylow 7-subgroups of G. By Sylow's Theorem, $n_7(G) \equiv 1 \mod 7$ and $n_7(G)$ divides 6. But then it must be that $n_7(G) = 1$. Therefore, the Sylow 7-subgroup is unique and hence normal. But then G contains a proper, nonzero, normal subgroup. Therefore, G is not simple. □

2. Let G, H and K be groups with $|G| = 35$, $|H| = 60$, and $|K| = 42$. Assume there exist group homomorphisms $\phi : G \to H$ and $\psi : G \to K$ with $\ker \phi \neq G$ and $\ker \psi \neq G$. Prove that $\ker \phi \cap \ker \psi$ consists of one element.

Solution: By the First Isomorphism Theorem, $G/\ker \phi \cong \operatorname{im} \phi$. Lagrange's Theorem implies that $\frac{|G|}{|\ker \phi|}$ divides $|H| = 60$. Further, Lagrange's Theorem implies that $|\ker \phi|$ divides $|G| = 35$. The divisors of 35 are 1, 5, 7, and 35. Since $\ker \phi \neq G$, $|\ker \phi| \neq 35$. Also notice that $\frac{35}{5} = 7$ does not divide 60, $\frac{35}{1} = 35$ does not divide 60, but $\frac{35}{7} = 5$ divides 60. This implies that $|\ker \phi| = 7$.

Similarly, $\frac{35}{|\ker \psi|}$ must divide $|K| = 42$. Since $\ker \psi \neq G$, $|\ker \psi| \neq 35$. Since $\frac{35}{7} = 5$ and $\frac{35}{1} = 35$ do not divide 42, this implies that $|\ker \psi| \neq 7$, $|\ker \psi| \neq 1$. The only possibility is $|\ker \psi| = 5$ (this works as $\frac{35}{5} = 7$ divides 42).

Recall that the intersection of two subgroups is again a subgroup. By Lagrange's Theorem, $|\ker \psi \cap \ker \psi|$ divides both $|\ker \phi| = 7$ and $|\ker \psi| = 5$. Therefore, $|\ker \phi \cap \ker \psi| = 1$, as required. □

3. Let $T : V \to W$ be a surjective linear transformation of vector spaces. Let W_1 and W_2 be subspaces of W such that $W = W_1 + W_2$. Prove that $V = T^{-1}(W_1) + T^{-1}(W_2)$.

Solution: Let $v \in V$. Then $T(v) \in W$ so that $T(v) = w_1 + w_2$ for some $w_1 \in W_1$, $w_2 \in W_2$. Since T is surjective, $w_1 = T(v_1)$ for some $v_1 \in T^{-1}(W_1)$. Similarly, $w_2 = T(v_2)$ for some $v_2 \in T^{-1}(W_2)$. Observe that

$$T(v - (v_1 + v_2)) = w_1 + w_2 - w_1 - w_2 = 0,$$

so $v - (v_1 + v_2) \in \ker T$. This implies that $v - (v_1 + v_2) = u$, where $Tu = 0$. Rearranging this equality gives $v = (u + v_1) + v_2$. Now $T(u + v_1) = T(v_1) = w_1$, so $u + v_1 \in T^{-1}(W_1)$. Since $v_2 \in T^{-1}(W_2)$, this implies that $v \in T^{-1}(W_1) + T^{-1}(W_2)$. Thus, $V = T^{-1}(W_1) + T^{-1}(W_2)$, as required. □

4. Let G be a group of order 77 acting on a set X with 20 elements. Prove that the action has at least 2 fixed points.

Solution: For any $x \in X$, let $\mathcal{O}_x$ be the orbit of x and let G_x denote the stabilizer of x in G. By the Orbit-Stabilizer Theorem, $|\mathcal{O}_x| = [G\colon G_x]$, so in particular $|\mathcal{O}_x|$ divides $|G| = 77$. Obviously, $|\mathcal{O}_x| \neq 77$, so the only possibility is $|\mathcal{O}_x| \in \{1, 7, 11\}$. Since the orbits of the action of G on X partition, consider the equation $20 = 11a + 7b + c$, where a, b, and c are nonnegative integers. The claim is that $c \geq 2$, so suppose for the sake of contradiction that $c < 2$. If $c = 0$, then the equation reduces to $20 = 11a + 7b$. Clearly, $a \leq 1$. If $a = 0$, then this reduces to $2- = 7b$, which has no integer solutions. Therefore, $c \neq 0$.

If $c = 1$, then $20 = 11a + 7b + c$ reduces to $19 = 11a + 7b$. The only possibilities are $a = 0$ or $a = 1$. If $a = 0$, then this reduces to $19 = 7b$, which has no integer solutions. If $a = 1$, then $19 = 11 + 7b$, so $8 = 7b$. This has no integer solutions. Therefore, $c \neq 1$. This implies $c \geq 2$. In other words, there are at least two orbits which only contain one element of X. Thus, the action has at least two fixed points. □

5. Let V be a finite dimensional vector space over the complex numbers. Let $\langle\ ,\ \rangle$ be a Hermitian form on V. Let W be a subspace of V and assume that the restriction of $\langle\ ,\ \rangle$ to W is nondegenerate. Prove that V is the direct sum $V = W \oplus W^{\perp}$, where $W^{\perp}$ is the orthogonal complement of W computed with respect to $\langle\ ,\ \rangle$.

Solution: If $W = 0$, then the conclusion is obvious. Suppose $W \neq 0$. Note that if $w \in W \cap W^{\perp}$, then $\langle w, w' \rangle = 0$ for all $w' \in W$. Since the restriction of the form to W is nondegenerate, this implies that $w = 0$. Since the restriction of $\langle\ \cdot\ ,\ \cdot\ \rangle$ to W is nondegenerate, there exists an orthonormal basis $\{w_1, w_2, \ldots, w_m\}$ of W. This can be extended to a (not necessarily orthonormal) basis $\{w_1, w_2, \ldots, w_m, v_{m+1}, \ldots, v_n\}$ of V. The matrix of this form with respect to this basis is

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A is a $m \times n$ matrix, D is an $(n-m) \times (n-m)$ matrix, etc.. Note that the a_{ij} entry of A is $\langle w_i, w_j \rangle$ and that the b_{ij} entry of A is $\langle w_i, v_j \rangle$. Consider the change of basis matrix,

$$P = \begin{pmatrix} I & Q \\ 0 & I \end{pmatrix},$$

where Q is an arbitrary matrix. Then

$$P^* \begin{pmatrix} A & B \\ C & D \end{pmatrix} P = \begin{pmatrix} A & AQ + B \\ * & * \end{pmatrix}$$

Notice that the basis of this matrix is $\{w_1, w_2, \ldots, w_m, v'_{m+1}, \ldots, v'_n\}$ for some $v'_i \in V$. Now choose $Q = -A^{-1}B$. Then $AQ + B = 0$, which implies that $\langle w_i, v'_j \rangle = 0$ for all indices i, j. Hence, $v'_j \in W^\perp$ for all $j \in \{m+1, \ldots, n\}$.

Therefore, any $v \in V$ can be written as $v = (a_1 w_1 + a_2 w_2 + \cdots + a_m w_m) + (b_{m+1} v'_{m+1} + \cdots + b_n v'_n) \in W + W^\perp$. Therefore, $V = W + W^\perp$. Since $W \cap W^\perp = 0$, this implies that $V = W \oplus W^\perp$, as required. □

6. An ideal I in a commutative ring R is called primary whenever for all $a, b \in R$, if $ab \in I$, then either $a \in I$ or $b^n \in I$ for some integer $n \geq 1$. Let R be a UFD and r an irreducible element of R. For any fixed integer $m \geq 1$, prove that the ideal $I = (r^m)$ is primary. Be sure to justify the use of UFD carefully.

Solution: Suppose $ab \in I$ for some $a, b \in R$. This implies that $ab = r^m c$ for some $c \in R$. Since R is a UFD, each of a, b, c can be factored into a product of irreducible elements (note that r^m is written as a product of irreducible elements):

$$\begin{aligned} a &= a_1^{j_1} \cdots a_p^{j_p}, \\ b &= b_1^{l_1} \cdots b_r^{l_s}, \\ c &= c_1^{n_1} \cdots c_s^{n_t}, \end{aligned}$$

where a_i, b_i, c_i are irreducible elements of R for each index i and $j_i, l_i, n_i \in \mathbb{N}$ for all indices i. This implies that

$$a_1^{j_1} \cdots a_p^{j_p} b_1^{l_1} \cdots b_r^{l_s} = r^m c_1^{n_1} \cdots c_s^{n_t}$$

Now each side of the factorization of ab into irreducible elements. Since such a factorization is unique, r is equal to some a_i or b_i (in fact, at least m copies of r show up on the left hand side). This implies that either r^m is a factor of a or r^k is a factor of b for some $k \geq 1$. If r^m is a factor of a, then $a = r^m x$ for some $x \in R$, which implies that $a \in I$. If r^k is a factor of b for some $k \geq 1$, then $b = r^k y$ for some $y \in R$. This implies that $b^m = (r^m)^k y^m \in I$. Therefore, I is primary. □

7. Let R be a commutative ring and M a Noetherian R-module. Let $f : M \to M$ be a surjective R-module homomorphism. Prove that f is an isomorphism. Hint: Consider the kernels of the composition $f^n = f \circ f \circ \cdots \circ f$ for $n = 1, 2, \ldots$.[6]

Solution: By assumption, f is surjective. It remains to show that f is injective. If $x \in M$, $n \in \mathbb{N}$, and $f^n(x) = 0$, then $f^{n+1}(x) = f(f^n(x)) = f(0) = 0$. Therefore, $\ker f^n \subset \ker f^{n+1}$ for all $n \in \mathbb{N}$. This implies we have a chain of ideals

$$\ker f \subset \ker f^2 \subset \cdots \subset \ker f^n \subset \cdots$$

[6] This is an example of Fitting's Lemma.

Since M is a noetherian R-module, the chain must stabilize, i.e. there is a $m \in \mathbb{N}$ such that $\ker f^m = \ker f^{m+1} = \ker f^{m+2} = \cdots$. Now suppose $x \in \ker f$ and $x \neq 0$. Since f is surjective, f^n is surjective for all $n \in \mathbb{N}$. This implies there exists a $y \in M$ such that $f^m(y) = x$. However, $f^{m+1}(y) = f(x) = 0$. Thus, $y \in \ker f^{m+1}$, $y \notin \ker f^m$, a contradiction as $\ker f^m = \ker f^{m+1}$. Therefore, $\ker f = \{0\}$, implying that f is injective. Therefore, f is an isomorphism. □

8. Let A be a matrix over $\mathbb{C}$ whose only eigenvalues over $\mathbb{C}$ are $\lambda = 7$, and $\lambda = 3$ and suppose that

$$\begin{aligned}
\dim \ker(A - 7I) &= 2 \\
\dim \ker(A - 7I)^2 &= 3 \\
\dim \ker(A - 7I)^3 &= 3 \\
\dim \ker(A - 3I) &= 2 \\
\dim \ker(A - 3I)^2 &= 2
\end{aligned}$$

(a) Find the Jordan form of the matrix A. (Just the Jordan matrix J, not the basis.)

(b) Find the minimal polynomial of A.

(c) Let $F = \mathbb{C}$, $V = F^n$, where A is an $n \times n$ matrix and make V into an $F[T]$-module by setting $T \cdot v = Av$ and extending linearly. Write V as a direct sum

$$V = \bigoplus_{i=1}^{r} \frac{F[T]}{m_i(T)}$$

with $m_1 \mid m_2 \mid \ldots \mid m_r$.

Solution:

(a) Since $\dim \ker(A - 7I) = 2$, there are two Jordan blocks associated to the eigenvalue 7. Since $\dim \ker(A - 7I)^3 - \dim \ker(A - 7I)^2 = 3 - 3 = 0$, there are no Jordan blocks with size at least 3. Since $\dim \ker(A - 7I)^2 - \dim \ker(A - 7I) = 3 - 2 = 1$, there is one Jordan block of size at least 2 which must have size exactly 2. Thus for the eigenvalue 7, there is one Jordan block of size 1 and one Jordan block of size 2.

Since $\dim \ker(A - 3I) = 2$, there are two Jordan blocks associated to the eigenvalue 3. Since $\dim \ker(A - 3I)^2 - \dim \ker(A - 3I) = 2 - 2 = 0$, there are no Jordan blocks of size at least 2, so both Jordan blocks must have size 1. Therefore, the Jordan canonical

form for A is, up to permutation of the Jordan blocks,

$$\begin{pmatrix} 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 \\ 0 & 1 & 7 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

(b) Using the Jordan canonical form of A, the elementary divisors of A are $x-7$, $(x-7)^2$, $x-3$, $(x-3)$. The minimal polynomial is the product of the largest power of $x-7$ and $x-3$, so the minimal polynomial is $(x-7)^2(x-3)$.

(c) The largest m_r is the minimal polynomial, so $m_r(T) = (T-7)^2(T-3)$. The polynomial m_{r-1} is formed by taking the product of the next largest power of $T-7$ and the next largest power of $T-3$, which is $(T-7)(T-3)$. Therefore,

$$V = F[T]/((T-7)^2(T-3)) \oplus F[T]/((T-7)(T-3)).$$

□

9. Let K be the splitting field for $x^7 - 11x + 11$ over $\mathbb{Q}$.

(a) Prove that there exist at least 7 automorphisms in $\mathrm{Aut}(K/\mathbb{Q})$. (That is, $|\mathrm{Aut}(K/\mathbb{Q})| \geq 7$.)

(b) Can there be exactly 10 automorphisms in $\mathrm{Aut}(K/\mathbb{Q})$?

Solution:

(a) Let $f(x) = x^7 - 11x + 11$. The polynomial f is irreducible over $\mathbb{Q}$ using Eisenstein's criterion with $p = 11$. Since $\mathbb{Q}$ has characteristic 0, f is separable. Thus, K is the splitting field of a separable polynomial over $\mathbb{Q}$, which implies that $K/\mathbb{Q}$ is Galois. Thus, $|\mathrm{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}]$.

Let $\alpha \in K$ be a root of $f(x)$. Then $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$ and $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg f(x) = 7$. This implies that

$$|\mathrm{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha):\mathbb{Q}] = 7[K:\mathbb{Q}(\alpha)] \geq 7.$$

(b) Notice that (a) implies that 7 divides $|\mathrm{Aut}(K/\mathbb{Q})|$. Since 7 does not divide 10, it is impossible to have $|\mathrm{Aut}(K/\mathbb{Q})| = 10$, i.e. there can never be exactly 10 automorphisms in $\mathrm{Aut}(K/\mathbb{Q})$.

□

10. Find the Galois group of the splitting field of $x^3 - 41$ over $\mathbb{Q}$.

Solution: Let $\zeta = e^{2\pi i/3}$ and $p(x) = x^3 - 41$. Then $p(x)$ has three roots: $\sqrt[3]{41}, \zeta\sqrt[3]{41}$, and $\zeta^2\sqrt[3]{41}$. The splitting field of $p(x)$ over $\mathbb{Q}$ is the smallest field extension of $\mathbb{Q}$ containing these three roots, which is $E := \mathbb{Q}(\zeta, \sqrt[3]{41})$. Note that ζ is a root of the irreducible polynomial (over $\mathbb{Q}$) $m(x) = x^2 + x + 1$, the third cyclotomic polynomial. Since $\mathbb{Q}(\sqrt[3]{41}) \subset \mathbb{R}$, $\zeta, \zeta^2 \notin \mathbb{Q}(\sqrt[3]{41})$. This implies that $m(x)$ is irreducible over $\mathbb{Q}(\sqrt[3]{41})$ (since it has no root in the field). Hence,

$$[E\colon \mathbb{Q}] = [E\colon \mathbb{Q}(\sqrt[3]{41})]\,[\mathbb{Q}(\sqrt[3]{41})\colon \mathbb{Q}] = 3 \cdot 2 = 6$$

Notice that E is the splitting field of a separable polynomial over $\mathbb{Q}$, which implies that $E/\mathbb{Q}$ is Galois. Thus, $|\operatorname{Gal}(E/\mathbb{Q})| = [E\colon \mathbb{Q}] = 6$.

Any $\sigma \in \operatorname{Gal}(E/\mathbb{Q})$ is completely determined by $\sigma(\zeta)$ and $\sigma(\sqrt[3]{41})$. Note that σ permutes the roots of the irreducible polynomial $x^2 + x + 1$, so $\sigma(\zeta) = \zeta$ or $\sigma(\zeta) = \zeta^2$ are the only two possibilities for $\sigma(\zeta)$. Similarly, $\sigma(\sqrt[3]{41})$ is a root of $p(x)$, so either $\sigma(\sqrt[3]{41}) = \sqrt[3]{41}$, $\sigma(\sqrt[3]{41}) = \zeta\sqrt[3]{41}$, or $\sigma(\sqrt[3]{41}) = \zeta^2\sqrt[3]{41}$. Thus, there are only six possible automorphisms:

$$\begin{aligned}
\sigma_1(\zeta) &= \zeta & \sigma_1(\sqrt[3]{41}) &= \sqrt[3]{41} \\
\sigma_2(\zeta) &= \zeta & \sigma_2(\sqrt[3]{41}) &= \zeta\sqrt[3]{41} \\
\sigma_3(\zeta) &= \zeta & \sigma_3(\sqrt[3]{41}) &= \zeta^2\sqrt[3]{41} \\
\sigma_4(\zeta) &= \zeta^2 & \sigma_4(\sqrt[3]{41}) &= \sqrt[3]{41} \\
\sigma_5(\zeta) &= \zeta^2 & \sigma_5(\sqrt[3]{41}) &= \zeta\sqrt[3]{41} \\
\sigma_6(\zeta) &= \zeta^2 & \sigma_6(\sqrt[3]{41}) &= \zeta^2\sqrt[3]{41}
\end{aligned}$$

Since $|\operatorname{Gal}(E/\mathbb{Q})| = 6$, each σ_i is an automorphism. Observe that $(\sigma_2 \circ \sigma_4)(\sqrt[3]{41}) = \sigma(\sqrt[3]{41}) = \zeta\sqrt[3]{41}$ and $(\sigma_4 \circ \sigma_2)(\sqrt[3]{41}) = \sigma_4(\zeta\sqrt[3]{41}) = \sigma_4(\zeta)\sigma_4(\sqrt[3]{41}) = \zeta^2\sqrt[3]{41}$. This implies that $\sigma_2 \circ \sigma_4 \neq \sigma_4 \circ \sigma_2$, so $\operatorname{Gal}(E/\mathbb{Q})$ is a non-abelian group of order 6. Up to isomorphism, there is only one nonabelian group of order 6, namely S_3. Therefore, $\operatorname{Gal}(E/\mathbb{Q}) \cong S_3$.

OR

Show that $[E\colon \mathbb{Q}] = 6$ and that $E/\mathbb{Q}$ is Galois as in the proof above. Observe that $\mathbb{Q}(\sqrt[3]{41})/\mathbb{Q}$ is not Galois since $p(x)$ does not split over $\mathbb{Q}(\sqrt[3]{41})$. Therefore, if H is the subgroup of $\operatorname{Gal}(E/\mathbb{Q})$ which fixes $\mathbb{Q}(\sqrt[3]{41})$, then the Fundamental Theorem of Galois Theory implies that H is not normal in $\operatorname{Gal}(E/\mathbb{Q})$. Hence, $\operatorname{Gal}(E/\mathbb{Q})$ is a nonabelian group of order 6, so $\operatorname{Gal}(E/\mathbb{Q}) \cong S_3$. □

January 2011

1. Let P be the real vector space of polynomials $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ of degree $\leq n$, and let D denote the derivative $\dfrac{d}{dx}$ considered as a linear operator on P.

(a) Find the matrix of D with respect to a convenient basis, and prove that D is a nilpotent operator.

(b) Determine all the D-invariant subspaces. Hint: Consider a polynomial of the highest degree in a D-invariant subspace.

Solution:

(a) Let $\mathcal{B} = \{1, x, \ldots, x^n\}$. It is clear that $\mathcal{B}$ is a basis for P. Now $D(x^i) = ix^{i-1}$ for $i \geq 1$. In $\mathcal{B}$-coordinates, this is the column vector with a 1 in the $(i-1)$th position and zeroes in the other positions. Also, $D(1) = 0$, so the matrix of D with respect to $\mathcal{B}$ is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

There are three ways to see that D is a nilpotent operator. First, note that $D^{k+1}(x^k) = 0$. This can be proven by induction on k. For $k = 0$, $D(x^0) = D(1) = 0$. For $k = 1$, $D^2(x) = D(1) = 0$. Now suppose this is true for some $k < n$ and note that $D^{k+2}(x^{k+1}) = D^{k+1}((k+1)x^k) = (k+1)D^{k+1}(x^k) = (k+1) \cdot 0 = 0$. This proves the claim. Thus, D^{n+1} is the zero operator and D is nilpotent.

Another way is to note that the characteristic polynomial of D is $c(x) = x^{n+1}$. Therefore, the minimal polynomial of D is of the form $m(x) = x^k$ for some $k \leq n+1$. This implies that $m(D) = D^k = 0$, so D is a nilpotent operator.

Another way is by direct matrix multiplication and induction.

(b) The zero subspace is of course D-invariant. It is clear that a subspace of the form $P_k = \{p(x) \in P\colon \deg p \leq k\} \cup \{0\}$ is a D-invariant subspace (since for every nonconstant $p(x) \in P_K$, $\deg(Dp(x)) < \deg(p(x))$; if p is constant, $Dp = 0$.) The claim is that every nonzero D-invariant subspace is of this form.

Let P' be a D-invariant subspace and let $p(x)$ denote a polynomial of maximal degree in P'. Since P' is closed under scalar multiplication, it can be assumed that $p(x)$ is monic. Let k denote the degree of P. The claim is that every polynomial of degree at most k is contained in P'. Consider the polynomial $D^k p$. In this polynomial, the only nonzero

term is $k!$. Since P' is closed under scalar multiplication, every constant polynomial is contained in P'. Note that $D^{k-1}(p(x)) = ax + b \in P'$. Then $D^{k-j-1}(p(x)) = ax^{j+1} + b(x)$, where $a \neq 0$ and $\deg b \leq j$. By the induction hypothesis, $b(x) \in P'$. Therefore,

$$\frac{1}{a}(D^{k-j-1}(p(x) - b(x))) = x^{j+1} \in P'$$

Thus, $\{1, x, \ldots, x^{j+1}\} \subset P'$, so every polynomial of degree at most $j+1$ is in P'. By induction on j, every polynomial of degree at most k is contained in P', so $P' = P_k$.

□

2. Let G be a group with a subgroup H (H need not be normal). The set G/H of left cosets of H in G is a left G-set by means of $g \circ xH = gxH$, $g, x \in G$.

(a) Prove that for each $a \in G$, the G-sets G/H and G/aHa^{-1} are isomorphic. Recall that a map $\phi : X \to Y$ of left G-sets is a *homomorphisms* if $\phi(gx) = g\phi(x)$ for all $g \in G$, $x \in X$; an *isomorphism* is a bijective homomorphism; and X, Y are *isomorphic* if there exists an isomorphism $X \to Y$. Hint: The right multiplication by a^{-1} is a bijective map $G \to G$.

(b) Let K be a subgroup of G. Prove that if the G-sets G/H and G/K are isomorphic, then $K = aHa^{-1}$ for some $a \in G$. Hint: If $\phi : X \to Y$ is an isomorphism of G-sets, compare the stabilizers of $x \in X$ and $\phi(x) \in Y$.

(c) State the necessary and sufficient condition for the G-sets G/H and G/K to be isomorphic.

Solution:

(a) Let $K = aHa^{-1}$ and define $\phi : G/H \to G/K$ via $gH \mapsto ga^{-1}K$. First, we need check that ϕ is well defined. If $gH = g'H$ for some $g, g' \in H$, then $g^{-1}g' \in H$ so that $ag^{-1}g'a^{-1} \in K$. In other words, $(ga^{-1})^{-1}(g'a^{-1}) \in K$, which implies that $ga^{-1}K = g'a^{-1}K$. Thus, ϕ is well defined.

For any $g, g' \in G$, $\phi(g \cdot g'H) = \phi(gg'H) = gg'a^{-1}K = g \cdot g'a^{-1}K = g \cdot \phi(g'H)$. Thus, ϕ is a homomorphism of G-sets.

If $\phi(gH) = \phi(g'H)$, then $ga^{-1}K = g'a^{-1}K$, so $ag^{-1}g'a^{-1} \in K$. Since $K = aHa^{-1}$, $ag^{-1}g'a^{-1} = aha^{-1}$ for some $h \in H$. This implies that $g^{-1}g' = h \in H$. Therefore, $gH = g'H$ and ϕ is injective.

If $gK \in G/K$, then $\phi(gaH) = gaa^{-1}K = gK$ so that ϕ is surjective. Thus, ϕ is an isomorphism of G-sets and G/H is isomorphic to $G/K = G/(aHa^{-1})$.

(b) Since G/H and G/K are isomorphic G-sets, there exists a homomorphism $\phi : G/H \to G/K$. Now $\phi(H) = gK$ for some $g \in G$. For any $h \in H$, $gK = \phi(H) = \phi(hH) = h\phi(H) = hgK$, which implies that $g^{-1}hg \in K$. Thus, $g^{-1}Hg \subset K$.

Since ϕ is an isomorphism, $\phi^{-1} : G/K \to G/H$ exists. Since $\phi(g^{-1}H) = g^{-1}\phi(H) = g^{-1}(gK) = K$, $\phi^{-1}(K) = g^{-1}H$. For any $k \in K$, $g^{-1}H = \phi^{-1}(K) = \phi^{-1}(kK) = k\phi^{-1}(K) = kg^{-1}H$. Thus, $gkg^{-1} \in H$, so $gkg^{-1} = h$ for some $h \in H$. This implies that $k = g^{-1}hg \in g^{-1}Hg$. This shows that $K \subset g^{-1}Hg$, so $K = g^{-1}Hg$. Take $a = g^{-1}$ to see that $K = aHa^{-1}$, as desired.

(c) The G-sets G/H and G/K are isomorphic if and only if $K = aHa^{-1}$ for some $a \in G$.

□

3.

(a) Prove that no group of order 56 is simple.

(b) Prove that a group of order 77 is cyclic.

Solution:

(a) The divisors of 56 are 1, 2, 4, 7, 8, 14, 28, and 56 and $56 = 2^3 \cdot 7$. Let n_p denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_p(G) \equiv 1 \mod p$ and $n_p(G)$ divides G. For $n_2(G)$, the only possibilities are $n_2(G) = 1$ or $n_2(G) = 7$. If $n_2(G) = 1$, then G contains a unique Sylow 2-subgroup, which is necessarily normal. But then G is not simple. Otherwise, $n_2(G) = 7$.

For $n_7(G)$, the only possibilities are $n_7(G) = 1$ or $n_7(G) = 8$. Again, if $n_7(G) = 1$ then G cannot be simple by the logic above. Otherwise, $n_7(G) = 8$.

It remains to show that $n_2(G) = 7$ and $n_7(G) = 8$ cannot occur. By Lagrange's Theorem, the intersection of any Sylow 2-subgroup and any Sylow 7-subgroup must be trivial. Then there are $8 \cdot 6 = 48$ elements of order 7 (since the Sylow 7-subgroup has order 7 and must be cyclic generated by any nontrivial element). Then there are $56 - 48 = 8$ elements. Since all Sylow 2-subgroups have order 8 and are contained in the complement of the set of elements of order 7, there must then only be one Sylow 2-subgroup, which is necessarily normal. Therefore, G cannot be simple.

(b) Note that the divisors of 77 are 1, 7, 11, and 77 and $77 = 7 \cdot 11$. By Sylow's Theorem, $n_7(G) \equiv 1 \mod 7$ and divides 77. Then it must be that $n_7(G) = 1$. Similarly, $n_{11}(G) = 1$. But the Sylow 7-subgroup and Sylow 11-subgroup account for only $7 + 11 - 1 = 17$ elements of G. By Lagrange's Theorem, the remaining elements of G must have order 77. But then any of these elements are necessarily generators for G so that G is cyclic.

□

4. Let A be the matrix of a real symmetric bilinear form $\langle\ ,\ \rangle$ with respect to some basis. Prove or disprove: The eigenvalues of A are independent of the basis.

Solution: Let $V = \mathbb{R}^2$ and let $\langle\ ,\ \rangle$ denote the dot product. Matrix that represent the dot product are of the form P^TP, where P is an invertible 2×2 matrix. Take $P = I_n$. Then $A = P^TP = I_n$, which has unique eigenvalue 1. Now take

$$P = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Then $A = P^TP = P^2 = 4I_2$. Thus, the unique eigenvalue of A is 4. Then the eigenvalues of the matrix of a bilinear form are not uniquely determined by the basis.

As another counterexample, let k be a field with characteristic not 2 with at least four elements. Let $\langle\ ,\ \rangle$ be a real symmetric bilinear form on the vector space $V := k$ given by $\langle x, y\rangle = xy$. Consider the basis $\{b\}$. Then we can represent $\langle\ ,\ \rangle$ by $A = (b^2)$. But we can choose $b, b' \in K$ so that $b^2 \neq b'^2$. □

5. Let R be a commutative ring and I an ideal of R.

(a) Let $I[X] \subseteq R[X]$ be the subset of the polynomial ring consisting of polynomials with coefficients in I. Prove that $I[X]$ is an ideal of $R[X]$.

(b) The quotients $R[X]/I[X]$ and $R[X]/(I, X)$ are isomorphic to $(R/I)[X]$ and R/I, not necessarily in that order. Decide which is which and prove your answers.

Solution:

(a) It is clear that $I[X]$ is nonempty. If $p(x), q(x) \in I[X]$. Without loss of generality, assume that the degree of $p(X)$ is at least the degree of $q(X)$. Writing $p(X) = \sum a_k X^k$ and $q(X) = \sum b_j X^j$, where $a_k, b_j \in I$) and all but finitely many of the a_k, b_j are 0, it follows that

$$p(X) + q(X) = \sum_k a_k X^k + \sum_j b_j X^j = \sum_i (a_i + b_i) X^i.$$

Since I is an ideal, $a_i + b_i \in I$ for all $k \leq m$. But then $p(X) + q(X) \in I[X]$.

Suppose $p(X) \in I[X]$, $r(X) \in R[X]$. Then $p(X) = \sum a_k X^k$ and $r(X) = \sum c_j X^j$, where $a_k \in I$, $c_j \in R$. Suppose that p has degree n and r has degree n. Then

$$p(X)r(X) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j c_{i-j} \right) X^i.$$

Now fro every pair of indices i, j, since $a_j \in I$, $a_j c_{i-j} \in I$, which implies that $\sum a_j c_{i-j} \in I$. Hence, $p(X)r(X) \in I[X]$. Hence, $I[X]$ is an ideal of $R[X]$.

(b) The claim is that $R[X]/I[X] \cong (R/I)[X]$. Define $\phi : R[X] \to (R/I)[X]$ via reducing coefficients mod I, i.e.

$$a_0 + a_1 X + \cdots + a_n X^n \mapsto \overline{a}_0 + \overline{a}_1 X + \cdots + \overline{a}_n X^n.$$

It is clear that ϕ is a surjective ring homomorphism with kernel $I[x]$. By the First Isomorphism Theorem, the claim is proved.

Define $\psi : R[x] \to R/I$ via $\psi(p(x)) = \phi(p(x))(\overline{0})$. Then ψ is a surjective homomorphism (since it is the composition of two surjective homomorphisms). It is clear that $\ker \psi = (I, X)$. Then by the First Isomorphism Theorem,

$$R[X]/(I, X) \cong R/I.$$

□

6. Let A be a square matrix over the complex numbers. Assume that the minimal polynomial of A is $x^2(x-5)$ an the characteristic polynomial of A is $x^5(x-5)^2$.

(a) Give all the possible rational canonical forms for A.

(b) Give all the possible Jordan canonical forms for A.

Solution:

(a) Note that the minimal polynomial is the largest invariant factor and that the product of the invariant factors is the characteristic polynomial. Therefore, the possibilities for the invariant factors are

$$x^2(x-5), x^2(x-5), x$$
$$x^2(x-5), x(x-5), x, x.$$

Expanding each polynomial gives

$$x^3 - 5x^2, x^3 - 5x^2, x$$
$$x^3 - 5x^2, x^2 - 5x, x, x.$$

The blocks look like

$$x^3 - 5x^2 : \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 5 \end{pmatrix}$$
$$x : \begin{pmatrix} 0 \end{pmatrix}$$
$$x^2 - 5x : \begin{pmatrix} 0 & 0 \\ 1 & 5 \end{pmatrix}$$

Therefore, the two possible rational canonical forms, up to block permutations, are

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(b) There are two possible sets of elementary divisors, corresponding to the two possibilities for the invariant factors:

$$x, x^2, x^2, x-5, x-5$$
$$x, x, x, x^2, x-5, x-5.$$

Therefore, the two possible Jordan canonical forms are

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

□

7. An abelian group is generated by four elements $\{a, b, c, d\}$, subject to the relations $a + 3b + 3c + 5d = 0$, $2b + 2c + 2d = 0$, and $3c = 0$. Express this group as a direct sum of cyclic groups.

Solution: The elements a, b, c, and d satisfy a system of equations with a coefficient matrix

$$\begin{pmatrix} 1 & 3 & 3 & 5 \\ 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

Performing the following row and column operations:

$$\begin{aligned} -R_1 + R_2 &\longrightarrow R_2 \\ -C_2 + C_3 &\longrightarrow C_3 \\ -3C_1 + C_2 &\longrightarrow C_2 \\ -5C_1 + C_4 &\longrightarrow C_4 \\ -C_2 + C_4 &\longrightarrow C_4 \\ R_3 + R_2 &\longrightarrow R_2 \\ -R_2 &\longrightarrow R_2 \\ R_2 &\longleftrightarrow R_3 \\ R_3 &\longleftrightarrow R_4 \end{aligned}$$

obtains the following diagonal matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Hence, the given abelian group is isomorphic to

$$\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

□

8. Let p be a prime integer and set $f(x) = x^p - 2 \in \mathbb{Q}[x]$. Determine the splitting field of f and the elements of its Galois group over $\mathbb{Q}$. (You do not need to classify the structure of the group up to isomorphism, just its elements.)

Solution: Note that f is irreducible by using Eisenstein's criterion with $p = 2$. Let ζ be a primitive pth root of unity. Then the p distinct roots of $f(x)$ in $\mathbb{C}$ are

$$\sqrt[p]{2}, \zeta\sqrt[p]{2}, \zeta^2\sqrt[p]{2}, \ldots, \zeta^{p-1}\sqrt[p]{2}.$$

Therefore, any field that contains all the roots of $f(x)$ must contain all powers of ζ and $\sqrt[p]{2}$. This implies that the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[p]{2}, \zeta)$. Since $\mathbb{Q}$ has characteristic 0 and f is irreducible over $\mathbb{Q}$, f is separable in $\mathbb{Q}(\sqrt[p]{2}, \zeta)$. This implies that the extension $\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q}$ is normal and separable so $\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q}$ is a Galois extension.

There are now two cases: if $p = 2$, then $\zeta = -1 \in \mathbb{Q}$, so the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$. Since $m(x) = x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ be arbitrary. Since σ fixes $\mathbb{Q}$, σ is uniquely determined by $\sigma(\sqrt{2})$. Note that σ permutes the roots of $m(x) = x^2 - 2$, so the only two possible automorphisms of $\mathbb{Q}(\sqrt{2})$ and $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Since $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension,

$$|\operatorname{Gal}(\sqrt{2})/\mathbb{Q}| = [\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2,$$

so σ_1 and σ_2 are the two elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

The other case is when p is an odd prime. In this case, ζ is a root of the irreducible polynomial $m(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Note that

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta)\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}, \zeta)\colon \mathbb{Q}(\sqrt[p]{2})]\,[\mathbb{Q}(\sqrt[p]{2})\colon \mathbb{Q}] = p[\mathbb{Q}(\sqrt[p]{2}, \zeta)\colon \mathbb{Q}(\sqrt[p]{2})].$$

Since $m(x)$ contains no real roots, $m(x)$ is irreducible over $\mathbb{Q}(\sqrt[p]{2})$. Hence, $[\mathbb{Q}(\sqrt[p]{2}, \zeta)\colon \mathbb{Q}(\sqrt[p]{2})] = p - 1$ and

$$|\operatorname{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})| = [\mathbb{Q}[(sqrt[p]2, \zeta)\colon \mathbb{Q}] = p(p-1)$$

Any $\sigma \in \mathrm{Gal}(\sqrt[p]{2}, \zeta)/\mathbb{Q}$ is completely determined by $\sigma(\sqrt[p]{2})$ and $\sigma(\zeta)$. Since $\sigma(\sqrt[p]{2})$ is a root of $f(x)$, there are p possibilities: $\sigma(\sqrt[p]{2}) = \zeta^k\sqrt[p]{2}$ for $k = 1, \ldots, p$. Similarly, there are $p - 1$ possibilities for $\sigma(\zeta)$: $\sigma(\zeta) = \zeta^j$ for $j = 1, \ldots, p - 1$. This implies that there are $p(p-1)$ possible elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})$, so each of these possible elements is actually an element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})$. □

August 2011

1. Let G be a group and let H, K be two normal subgroups of G with $H \cap K = 1$. Prove that $HK \cong H \times K$.

Solution: Let $h \in H$, $k \in K$. Since K is normal in G, there exist $k' \in K$ such that $hk = k'h$. Since H is normal in G, there exists $h' \in H$ such that $hk = k'h = h'k'$. Now $h^{-1}h' = k'k^{-1} \in H \cap K$, so $h^{-1}h' = k'k^{-1} = 1$. Thus, $h = h'$, $k = k'$, and $hk = kh$.

Define $\phi : H \times K \to HK$ via $\phi((h,k)) = hk$. It is obvious that ϕ is surjective. It suffices to prove that ϕ is an injective homomorphism. Let $(h,k), (h',k') \in H \times K$. Using the observation above,

$$\phi\big((h,k)(h',k')\big) = \phi(hh',kk') = hh'kk' = hkh'k' = \phi\big((h,k)\big)\phi\big((h',k')\big).$$

Thus, ϕ is a homomorphism. If $(h,k) \in \ker\phi$, then $\phi((h,k)) = hk = 1$. Then $h = k^{-1} \in H \cap K$ so that $h = k = 1$. Thus, the kernel of ϕ is trivial which implies that ϕ is injective. Therefore, ϕ is an isomorphism and $HK \cong H \times K$. □

2. Let G be group of order p^2q where p, q are prime. Prove that G is not simple.

Solution: Suppose $p = q$. Then G is a finite p-group since $|G| = p^3$. But by the Class Equation, G must then have a nontrivial center. The center of a group is a normal subgroup so that G cannot be simple.

Now the number of Sylow p-subgroups, $n_p(G)$, divides q so that $n_p(G) = 1$ or $n_p(G) = q$. If $n_p(G) = 1$, then the Sylow p-subgroup is unique and hence necessarily normal (so that G is not simple). Assume then that $n_p(G) = q$. But $n_p(G) \equiv 1 \mod q$ so that $q > p$. The number of Sylow q-subgroups, $n_q(G)$, divides p^2. Now if $n_q(G) = 1$, then G is not simple using the comments above. Assume then that $n_q(G) > 1$. Now $n_q(G) \neq p$ for then $p \equiv 1 \mod q$, implying $p > q$.

Then if G is simple, $n_p(G) = q$ and $n_q(G) = p^2$. Then the total number of non-identity elements in the Sylow q-subgroup is $p^2(q-1)$. Since the intersection of any two distinct Sylow p-subgroups can have size at most p, the number of elements in the Sylow p-subgroups is at least $2p^2 - p$. Then G contains at least

$$p^2(q-1) + 2p^2 - p = p^2 + p(p-1) > p^2q,$$

a contradiction. Therefore, at least one of n_p, n_q is 1 so that G cannot be simple. □

3. Let G be a group of order 15 acting on a set of order 22. Assume there are no fixed points. Determine how many orbits there are.

Solution: Let X denote the set of order 22 and $x \in X$. Let G_x denote the stabilizer of x in G and $\mathcal{O}_x$ be the orbit of x. By the Orbit-Stabilizer Theorem, $|\mathcal{O}_x| = [G\colon G_x]$. In particular,

$|\mathcal{O}_x|$ divides $|G| = 15$ for all $x \in X$. Since there are no fixed points, $|\mathcal{O}_x| > 1$, so the only possibilities are $|\mathcal{O}_x| = 3, 5, 15$.

If there is an orbit with 15 elements, then the remaining orbits must have a combined 7 elements. However, this is clearly impossible. Therefore, the only possibilities are $|\mathcal{O}_x| = 3, 5$. It remains to solve the equation $3a + 5b = 22$. Clearly, $b \leq 4$. But for $0 \leq b \leq 4$, this it must be that $3a$ is in $\{2, 7, 12, 17, 22\}$, a contradiction as each element in this set is not divisible by 3. Then it must be that $a = 4$ and $b = 2$, meaning there are 6 orbits: 2 orbits with 5 elements and 4 orbits with 3 elements each. □

4. Let $T : V \to V$ be a linear operator and let $\{v_1, \ldots, v_n\}$ be eigenvectors with distinct eigenvalues. Prove that if $a_1v_1 + \cdots + a_nv_n$ is an eigenvector, then *exactly one* of the coefficients is non-zero.

Solution: For each index i, let λ_i be the eigenvalue of v_i. The first thing is to prove that the set $\{v_1, \ldots, v_n\}$ is independent. We proceed by induction on n. For $n = 2$, suppose $b_1v_1 + b_2v_2 = 0$ is a linear dependence relation on the v_i. Then

$$\begin{aligned} T(b_1v_1 + b_2v_2) &= 0 \\ b_1T(v_1) + b_2T(v_2) &= 0 \\ b_1\lambda_1v_1 + b_2\lambda_2v_2 &= 0 \end{aligned}$$

Also, $\lambda_1(b_1v_1 + b_2v_2) = b_1\lambda_1v_1 + b_2\lambda_1v_2 = 0$. This implies that

$$\begin{aligned} (b_1\lambda_1v_1 + b_2\lambda_2v_2) - (b_1\lambda_1v_1 + b_2\lambda_1v_2) &= 0 \\ (\lambda_2 - \lambda_1)b_2v_2 &= 0 \end{aligned}$$

Since $v_2 \neq 0$ and $\lambda_1 \neq \lambda_2$, it follows that $b_2 = 0$. But then $b_1v_1 = 0$ so that $b_1 = 0$. Thus, the claim is proved for $n = 2$.

Suppose the claim is true for n eigenvectors and consider the set $\{v_1, \ldots, v_{n+1}\}$. Let $b_1v_1 + \cdots + b_{n+1}v_{n+1} = 0$ be a linear dependence relation. Then

$$\begin{aligned} T(b_1v_1 + \cdots + b_{n+1}v_{n+1}) &= 0 \\ b_1\lambda_1v_1 + \cdots + b_{n+1}\lambda_{n+1}v_{n+1} &= 0. \end{aligned}$$

Also, $b_1\lambda_1v_1 + \cdots + b_{n+1}\lambda_1v_{n+1} = 0$. Thus,

$$\begin{aligned} (b_1\lambda_1v_1 + \cdots + b_{n+1}\lambda_{n+1}v_{n+1}) - (b_1\lambda_1v_1 + \cdots + b_{n+1}\lambda_1v_{n+1}) &= 0 \\ b_2(\lambda_2 - \lambda_1)v_2 + b_3(\lambda_3 - \lambda_1)v_3 + \cdots + b_{n+1}(\lambda_{n+1} - \lambda_1)v_{n+1} &= 0. \end{aligned}$$

The induction hypothesis implies that all coefficients are 0. Since the λ_i's are distinct, $b_2 = b_3 = \cdots = b_{n+1} = 0$. Then $b_1v_1 = 0$ so that $b_1 = 0$. This proves the claim.

Now suppose that $a_1v_1 + \cdots + a_nv_n$ is an eigenvector of T with eigenvalue λ. Then

$$\begin{aligned}\lambda a_1v_1 + \cdots + \lambda a_nv_n &= T(a_1v_1 + \cdots + a_nv_n)\\ &= a_1T(v_1) + \cdots + a_nT(v_n)\\ &= \lambda_1a_1v_1 + \cdots + \lambda_1a_nv_n\end{aligned}$$

This implies that

$$(\lambda - \lambda_1)a_1v_1 + \cdots + (\lambda - \lambda_n)a_nv_n = 0.$$

Since the set $\{v_1, \ldots, v_n\}$ is linearly independent, all of the coefficients are zero. Since $a_1v_1 + \cdots + a_nv_n$ is an eigenvector of T, it is nonzero and at least one a_i is nonzero. If $a_i \neq 0$, then $\lambda = \lambda_i$. If $i \neq j$, a_i, a_j are both nonzero. But then $\lambda_i = \lambda = \lambda_j$, a contradiction. Therefore, only one coefficient is nonzero. □

5. Let W be a subspace of a Euclidean space V. (A Euclidean space is a finite dimensional real inner product space.) Prove that $W = W^{\perp\perp}$.

Solution: If $w \in W$ and $v \in W^{\perp}$, then $\langle w, v\rangle = 0$ so that $w \perp v$ and $w \in W^{\perp\perp}$. Hence, $W \subseteq W^{\perp\perp}$. Note that $V = W \oplus W^{\perp} = W^{\perp} \oplus W^{\perp\perp}$, so

$$\dim V = \dim W + \dim W^{\perp} = \dim W^{\perp} + \dim W^{\perp\perp}.$$

Therefore, $\dim W = \dim W^{\perp\perp}$. Since $W \subset W^{\perp\perp}$, this forces $W = W^{\perp\perp}$. □

6. Let F be a finite field.

(a) Prove that the polynomial ring $F[x]$ contains infinitely many irreducible elements.

(b) Deduce from (a) that $F[x]$ contains an irreducible element of degree greater than 1.

(c) Deduce from (b) that F is not algebraically closed, hence any algebraically closed field is infinite.

Solution:

(a) Suppose $F[x]$ has finitely many irreducible elements. Let $f_1, \ldots, f_n$ denote the irreducible elements of $F[x]$. Define $p(x) = f_1(x) \cdots f_n(x) + 1$. Then $p(x) \neq f_k(x)$ for any k. Thus, $p(x)$ is reducible. Since $F[x]$ is a UFD, $p(x)$ can be factored into a product of irreducible elements. If $f_k(x) \mid p(x)$ in $F[x]$, then $f_k(x)$ also divides $p(x) - f_1(x) \cdots f_n(x) = 1$ in $F[x]$. But then f_k is a unit in $F[x]$, contrary to the assumption that f_k was irreducible. Thus, $p(x)$ is a reducible polynomial which cannot be factored into a product of irreducibles in a UFD, a contradiction. Therefore, there are infinitely many irreducible elements in $F[x]$.

(b) Suppose $|F| = q$. Note that if $p(x) \in F[x]$ has degree 1 or is constant, then $p(x) = ax + b$ for some $a, b \in F$. Thus, there are only q^2 elements of $F[x]$ and only finitely many elements that are constant or have degree 1, there must be an irreducible element of degree at least 2.

(c) If F were algebraically closed, then every irreducible polynomial in $F[x]$ would have degree 1. From (b), there is an irreducible polynomial in $F[x]$ of degree at least 2. Thus, F is not algebraically closed and every algebraically closed field is infinite.

□

7. Let $\mathbb{Q} \subset F$ be a field extension. Assume it is a Galois extension with Galois group isomorphic to the symmetric group S_3. Prove that F is the splitting field over $\mathbb{Q}$ for an irreducible cubic polynomial $f(x) \in \mathbb{Q}[x]$.

Solution: Let $G = \text{Gal}(F/\mathbb{Q}) = S_3 \cong D_6 = \langle \sigma, \tau \colon \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle$. By the Fundamental Theorem for Galois Theory, there exists a bijective correspondence between the subgroups of G and the subfields of F containing $\mathbb{Q}$. Note that $\langle \tau \rangle$ is a subgroup of G. This subgroup is not normal since $\sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \sigma^2\tau \notin \langle \tau \rangle$.

Therefore, if L is the fixed field of $\langle \tau \rangle$, then $L/\mathbb{Q}$ is not a Galois extension. Notice that $[L \colon \mathbb{Q}] = [G \colon \langle \tau \rangle] = 3$. For any $\alpha \in L \setminus \mathbb{Q}$,

$$3 = [L \colon \mathbb{Q}] = [L \colon \mathbb{Q}(\alpha)] \, [\mathbb{Q}(\alpha) \colon \mathbb{Q}].$$

Since $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] > 1$ and 3 is prime, $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] = 3$ and $[L \colon \mathbb{Q}(\alpha)] = 1$, so $L = \mathbb{Q}(\alpha)$. If $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$, then $m_\alpha(x) \in \mathbb{Q}[x]$ is an irreducible cubic polynomial. Note that this polynomial is separable since $\mathbb{Q}$ has characteristic 0. Clearly, the splitting field of $m_\alpha(x)$ over $\mathbb{Q}$ contains $\mathbb{Q}(\alpha)$ (since $m_\alpha(\alpha) = 0$). If $\mathbb{Q}(\alpha)$ was the splitting field of $m_\alpha(x)$ over $\mathbb{Q}$, then $\mathbb{Q}(\alpha)/\mathbb{Q}$ would be a normal, separable extension, i.e. $\mathbb{Q}(\alpha)/\mathbb{Q}$ would be a Galois extension, which is a contradiction.

Therefore, the splitting field of $m_\alpha(x)$ over $\mathbb{Q}$ is a field E such that $\mathbb{Q}(\alpha) \subsetneq E \subset F$. Note that $[F \colon \mathbb{Q}(\alpha)] = 2$ by the Fundamental Theorem of Galois Theory. Therefore,

$$2 = [F \colon \mathbb{Q}(\alpha)] = [F \colon E] \, [E \colon \mathbb{Q}(\alpha)].$$

Since $E \neq \mathbb{Q}(\alpha)$, $[E \colon \mathbb{Q}(\alpha)] > 1$. Thus, $[E \colon \mathbb{Q}(\alpha)] = 2$, $[F \colon E] = 1$, and $E = F$. This proves that F is the splitting field of $m_\alpha(x)$, an irreducible cubic polynomial in $\mathbb{Q}[x]$. □

8. Let A be an 18×18 matrix over $\mathbb{C}$ with characteristic polynomial equal to $(x-1)^6(x-2)^6(x-3)^6$ and minimal polynomial equal to $(x-1)^4(x-2)^4(x-3)^3$. Assume $(A - I)$ has nullity 2, $(A - 2I)$ has nullity 3, and $(A - 3I)^2$ has nullity 4. Find the Jordan canonical form of A.

Solution: Since $(A - I)$ has nullity 2, there are two Jordan blocks associated to the eigenvalue 1. One of these must have size 4 since $(x-1)^4$ is an elementary divisor of A. Therefore, the other must have size 2. Since $(A - 2I)$ has nullity 3, there are 3 Jordan blocks associated to the eigenvalue 2. One of these blocks has size 4 so the other two must have size 1.

Since the nullity of $(A - 3I)^2$ is 4, the nullity of $(A - 3I)$ can be at most 4. If the nullity of $(A - 3I)$ is 1, there is only one Jordan block associated to the eigenvalue 3, which is impossible since there is a Jordan block of size 2 (determined from the minimal polynomial). If the nullity of $(A - 3I)$ were 3, then there would be one block of size at least 2. This block must have size 3 (by the minimal polynomial). But then the remaining two blocks must have size 1, impossible as $6 \neq 3 + 1 + 1$. If the nullity of $(A - 3I)$ were 4, then there would be no blocks of size at least 2, a contradiction.

Therefore, the nullity of $(A - 3I)$ is 2, which implies there are two Jordan blocks with $\lambda = 3$. Each of these blocks has size 3. Therefore, the Jordan canonical form of A is

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3
\end{pmatrix}$$

9. Let R be a Noetherian integral domain with the property that any ideal that can be generated by 2 elements can actually be generated by 1 element[7]. Prove that R is a Principal Ideal Domain.

Solution: The ring R is an integral domain by assumption to it suffices to show that every ideal of R is principal. Since R is noetherian, every ideal of R is finitely generated. Let I

[7]Such a ring is called a Bézout Domain.

be an ideal of R and let n be the cardinality of the smallest generating set for I. Suppose $n > 1$. Let $\{x_1, \ldots, x_n\}$ be such a generating set. Then the ideal (x_1, x_2) can be generated by a single element, i.e. $(x_1, x_2) = (x)$ for some $x \in I$. Let $a \in I$ be arbitrary. Then there exist $r_1, \ldots, r_n$ such that

$$a = rx + r_3x_3 + \cdots + r_nx_n,$$

so $a \in (x, x_3, \ldots, x_n)$. This proves that $I \subset (x, x_3, \ldots, x_n)$ and it is clear that $(x, x_3, \ldots, x_n) \subset I$, so $I = (x, x_3, \ldots, x_n)$ can be generated by $n - 1$ elements, contrary to the choice of n. Therefore, $n = 1$ and the ideal I is principal. Thus, R is a PID. □

10.

(a) Let R be a commutative ring with identity. Assume that $\mathbb{Z}$ is a subring of R. You have seen that this makes R into a $\mathbb{Z}$-module. Assume that R is a finitely generated $\mathbb{Z}$-module. Prove that R is not a field.

(b) Find a field F such that the additive group $(F, +)$ is a finitely generated $\mathbb{Z}$-module.

Solution:

(a) Since $\mathbb{Z}$ is a noetherian ring and R is a finitely generated $\mathbb{Z}$-module, R is a noetherian $\mathbb{Z}$-module. Suppose for the sake of contradiction that R is a field. Then R contains the field of fractions of $\mathbb{Z}$, i.e. $\mathbb{Q} \subset R$. Since R is a noetherian $\mathbb{Z}$-module, this implies that $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-module. It suffices to prove that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.

If $\mathbb{Q}$ were a finitely generated $\mathbb{Z}$-module, then $\mathbb{Q} = \left(\frac{m_1}{n_1}, \cdots, \frac{m_k}{n_k}\right)$, where $m_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$, and $\gcd(m_i, n_i) = 1$ for each $i \in \{1, \ldots, k\}$. Consider the rational number

$$\frac{1}{1 + n_1 \cdots n_k}.$$

By assumption, there exist $a_i \in \mathbb{Z}$ such that

$$\frac{1}{n_1 \cdots n_k} = a_1 \frac{m_1}{n_1} + \cdots + a_k \frac{m_k}{n_k}.$$

Clearing denominators via multiplication by $n_1 \cdots n_k$, we obtain

$$\frac{n_1 \cdots n_k}{1 + n_1 \cdots n_k} = a_1 m_1 n_2 \cdots n_k + \cdots + a_k m_k n_1 \cdots n_{k-1}.$$

This is a contradiction as the right side is an integer while the left side is clearly a non-integer. But then $\mathbb{Q}$ cannot be a finitely generated $\mathbb{Z}$-module, contradicting the fact that R is noetherian. Therefore, R is not a field.

(b) Take $F = \mathbb{Z}/3\mathbb{Z}$. Then $(F, +)$ is a finite $\mathbb{Z}$-module, which is necessarily finitely generated.

□

January 2012

1. Show that a group of order 105 is not simple.

Solution: Let n_p denote the number of Sylow p-subgroups of G. By Sylow's Theorems, $n_2 \equiv 1 \mod 3$ and divides 35. Then n_3 is 1 or 7. Similarly, $n_5 \equiv 1 \mod 5$ and divides 21 so that n_5 is either 1 or 21. If either n_3, n_5 were 1, then the corresponding Sylow p-subgroup would be unique, hence normal. But then G would not be simple. Assume then that $n_3, n_5 > 1$. By Lagrange's Theorem, any Sylow p-subgroup and Sylow q-subgroup, $p \neq q$, must intersect trivially. Then these two Sylow subgroups constitute $21(4) + 7(2) + 1 = 99$ elements of G. Since a Sylow 7-subgroup exists, these 7 elements must form a Sylow 7-subgroup, which is unique. But then G is not simple. □

2. Let G be a group with subgroups H and K.

(a) Let $x, y \in H$ with $x(H \cap K) = y(H \cap K)$. Prove that $xK = yK$.

(b) Show that $[H : H \cap K] \leq [G : K]$, where $[G : K]$ denotes the index of K in G.

(c) If $[G : K]$ and $[G : H]$ are both finite, show that $[G : H \cap K]$ is finite.

Solution:

(a) Observe that $x(H \cap K) \subset xK$ since $H \cap K \subset K$. Similarly, $y(H \cap K) \subset yK$. Since $x(H \cap K) = y(H \cap K)$, this implies that $xK \cap yK$ is not empty. Since cosets partition the group G, this implies $xK = yK$.

(b) Let G/K denote the set of left cosets of K in G and $H/(H \cap K)$ denote the set of left cosets of $H \cap K$ in H. Define a function $\phi : H/(H \cap K) \to G/K$ via $H \cap K \mapsto xK$.

Part (a) shows that ϕ is well defined. We claim that ϕ is injective. If $x, y \in H$ with $xK = yK$, then $x^{-1}y \in K$, so $x^{-1}y \in H \cap K$. This implies that $x(H \cap K) = y(H \cap K)$. But then ϕ is injective. But then

$$[H\colon H \cap K] = |H/(H \cap K)| \leq |G/K| = [G\colon K],$$

as desired.

(c) Observe that

$$[G\colon H \cap K] = [G\colon H]\,[H\colon H \cap K] \leq [G\colon H]\,[G\colon K].$$

Therefore, $[G\colon H \cap K]$ is finite since both $[G\colon H]$ and $[G\colon K]$ are finite.

□

3.

(a) Let G be a finite abelian group and assume that m divides $|G|$. Show that G has a subgroup of order m.

(b) Give an example to show that the result in (a) is false if G is not assumed to be abelian.

Solution:

(a) We proceed by induction on $|G|$. If $|G| = 1$ or $|G| = 2$, then the result is trivial. Now suppose that $|G| = n$ and the statement holds for $k < n$. Let d be a divisor of n. We can write $d = kp$ for some prime p and $k \in \mathbb{N}$. By Cauchy's Theorem, there exists a subgroup $H \leq G$ of order p. Since G is abelian, we can form the quotient G/H. Now $|G/H| < |G|$ so that by the induction hypothesis, G/H contains a subgroup of every order dividing $|G/H|$. In particular, $k \mid |G/H|$ so that there is a subgroup of G/H of order k. By the Correspondence Theorem, this subgroup corresponds to a subgroup K such that $H \leq K \leq G$, $K/H \leq G/H$, and $|K/H| = k$. Since H is finite, this implies $|K| = k|H| = kp = d$. But then there is a subgroup of order d.

OR

The result is obvious if $|G| = 1$, so suppose $|G| > 1$. Note the conclusion holds if G is cyclic. Suppose that $|G| = p^m$ for some positive integer m and prime p. It is clear that G contains a subgroup of order p^m and 1. Any other divisor of $|G|$ is of the form p^l, where $1 \leq l \leq m$. Fix $l \in \{1, 2, \ldots, m\}$. By the Fundamental Theorem of Finitely Generated Abelian Groups,

$$G \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_k}\mathbb{Z},$$

where $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$ and $\alpha_1 + \cdots + \alpha_k = m$. Let $N = \max\{i \colon \alpha_1 + \cdots + \alpha_i \leq l\}$. Then

$$\mathbb{Z}/p^{\alpha_N}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_1}\mathbb{Z}$$

is a subgroup of G of order $p^{\alpha_1+\cdots+\alpha_N}$. If $\alpha_1 + \cdots + \alpha_N = l$, then the proof is complete. Otherwise by the choice of N,

$$\alpha_1 + \cdots + \alpha_N + \alpha_{N+1} > l \Longrightarrow \alpha_{N+1} > l - \alpha_1 - \cdots - \alpha_N,$$

which implies that $p^{l-\alpha_1-\cdots-\alpha_N}$ divides $p^{\alpha_{N+1}}$. Therefore, $\mathbb{Z}/p^{\alpha_{N+1}}\mathbb{Z}$ contains a subgroup H of order $p^{l-\alpha_1-\cdots-\alpha_N}$. Thus,

$$H \times \mathbb{Z}/p^{\alpha_N}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_1}\mathbb{Z}$$

is a subgroup of G of order $p^{l-\alpha_1-\cdots-\alpha_N}p^{\alpha_1+\cdots+\alpha_N} = p^l$. This proves the result in the case where $|G| = p^m$.

Now if $|G| = p_1^{k_1} \cdots p_l^{k_l}$, where the p_i are distinct primes and $k_i \geq 0$, then by the Fundamental Theorem of Finitely Generated Abelian Groups,

$$G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_l},$$

where $|G_{p_i}| = p_i^{k_i}$ for each i. If $m \mid n$, then $m = p_1^{j_1} \cdots p_l^{j_l}$, where $j_i \geq 0$ for each i. By the work above, each G_{p_i} contains a subgroup H_{p_i} of order $p_i^{j_i}$. Then

$$H = H_{p_1} \times \cdots \times H_{p_l}$$

is a subgroup of G of order $p_1^{j_1} \cdots p_l^{j_l} = m$, as required.

(b) Take $G = A_5$. Note that $|G| = 60$ and that $30 \mid 60$. If G contained a subgroup H of order 30, then $[G\colon H] = \frac{60}{30} = 2$, which would imply that H is normal in G. But G is a simple group so that this is impossible. Then G does not contain a subgroup of order 30.

□

4. Let $A \in M_n(\mathbb{C})$ be a matrix over the complex numbers $\mathbb{C}$ with $A^* = -A$, where A^* denotes the complex conjugate transpose of A. Let $\langle x, y\rangle = x^*y$ be the usual inner product on $\mathrm{Col}_n(\mathbb{C})$.

(a) Show that the eigenvalues of A are purely imaginary.

(b) If λ and μ are distinct eigenvalues of A with eigenvectors v and w in $\mathrm{Col}_n(\mathbb{C})$, respectively, show that $\langle v, w\rangle = 0$.

Solution:

(a) Let $\lambda \in |C$ be an eigenvalue of A with eigenvector $v \in \mathbb{C}^n$. Notice that $A^*v = -Av = -\lambda v$, which implies that $-\lambda$ is an eigenvalue of A^* with eigenvector v. We compute the quantity $\langle v,\, Av\rangle$ in two different ways:

$$\langle v,\, Av\rangle = \langle v,\, \lambda v\rangle = \lambda\langle v,\, v\rangle$$
$$\langle v,\, Av\rangle = \langle A^*v,\, v\rangle = \langle -\lambda v,\, v\rangle = -\overline{\lambda}\langle v,\, v\rangle.$$

Since v is nonzero, $\langle v, v\rangle$ is nonzero. Therefore, $\lambda = -\overline{\lambda}$, i.e. $\lambda + \overline{\lambda} = 0$. But then $\mathrm{Re}\ \lambda = \frac{\lambda+\overline{\lambda}}{2} = 0$ so that λ is purely imaginary.

(b) By (a), $-\lambda$ is an eigenvalue of A^* with eigenvector v. Observe that since λ is purely imaginary, $-\overline{\lambda} = -(-\lambda) = \lambda$. We compute $\langle v,\, Aw\rangle$ in two different ways:

$$\langle v,\, Aw\rangle = \langle v,\, \mu\rangle = \mu\langle v,\, w\rangle$$
$$\langle v,\, Aw\rangle = \langle A^*v,\, w\rangle = \langle -\lambda v,\, w\rangle = -\overline{\lambda}\langle v,\, w\rangle = \lambda\langle v,\, w\rangle.$$

Therefore, $\mu\langle v,\, w\rangle = \lambda\langle v,\, w\rangle$. Since $\lambda \neq \mu$, $\langle v,\, w\rangle = 0$.

□

5. Let $A \in M_n(\mathbb{C})$ be a matrix over the complex numbers $\mathbb{C}$.

(a) If A is similar to a diagonal matrix and $f(x) \in \mathbb{C}[x]$ is a polynomial, show that $f(A)$ is similar to a diagonal matrix.

(b) If A^2 is similar to a diagonal matrix, does it follow that A is similar to a diagonal matrix?

Solution:

(a) Let $D \in M_n(\mathbb{C})$ be a diagonal matrix which is similar to A. Then there exist $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PAP^{-1} = D$. Observe that $D^k = PA^kP^{-1}$ is a diagonal matrix for all $k \in \mathbb{N}$. Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Then

$$\begin{aligned} Pf(A)P^{-1} &= P(a_n A^n + \cdots + a_0 I)P^{-1} \\ &= a_n PA^n P^{-1} + \cdots + a_0 I \\ &= a_n D^n + \cdots + a_0 I \end{aligned}$$

is a sum of diagonal matrices so that $Pf(A)P^{-1}$ is a diagonal matrix. But then $f(A)$ is similar to a diagonal matrix.

(b) A need not be similar to a diagonal matrix. Take

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Then $A^2 = 0$ so that A^2 is a diagonal matrix. But the characteristic polynomial of A is $c_A(x) = x^2$. Since $A \neq 0$, the minimal polynomial of A is $m(x) = x^2$. Since $m(x)$ has a repeated root, A is not diagonalizable.

□

6. Let $i \in \mathbb{C}$ be the square root of -1.

(a) Prove that $\mathbb{Z}[i] := \{a + bi \colon a, b \in \mathbb{Z}\}$ is isomorphic to $\mathbb{Z}[x]/(x^2 + 1)$.

(b) Let $p \in \mathbb{Z}$ be a prime integer. Prove that p is a prime element in $\mathbb{Z}[i]$. (a "Gaussian prime") if and only if $x^2 + 1$ is an irreducible element of $\mathbb{F}_p[x]$. (Here $\mathbb{F}_p$ is the field with p elements. You may use without proof the fact that $\mathbb{F}_p[x]$ is a PID.)

Solution:

(a) Define a function $f : \mathbb{Z}[x] \to \mathbb{Z}[i]$ via $p(x) \mapsto p(i)$, i.e. f is evaluation at i. It is clear that f is a homomorphism. For $a + bi \in \mathbb{Z}[i]$, consider $p(x) = a + bx$. Then $f(p(x)) = a + bi$ so that f is surjective. Finally as $i^2 + 1 = 0$, it is clear that $(x^2 + 1) \subset \ker f$. If $p(x) \in \ker f$, write $p(x) = r_1(x) \cdots r_n(x)$ for irreducible polynomials $r_k(x) \in \mathbb{Z}[x]$ (this exists since $\mathbb{Z}[x]$ is a UFD). The only irreducible polynomials in $\mathbb{Z}[x]$ with i as a root are $a(x^2 + 1)$, where $a \in \mathbb{Z}$ (since the minimal polynomial for i is $x^2 + 1$). Hence, $x^2 + 1$ divides $p(x)$ and $p(x) \in (x^2 + 1)$. But then $\ker f = (x^2 + 1)$. By the First Isomorphism Theorem, $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i]$.

(b) This follows by abstract nonsense:

$$
\begin{aligned}
p \text{ prime in } \mathbb{Z}[i] &\iff \mathbb{Z}[i]/(p) \text{ is an integral domain} \\
&\iff \frac{\mathbb{Z}[x]/(x^2+1)}{f((p))} \text{ is an integral domain} \\
&\iff \frac{\mathbb{Z}[x]/(x^2+1)}{(p)} \text{ is an integral domain} \\
&\iff \mathbb{Z}[x]/(x^2+1, p) \text{ is an integral domain} \\
&\iff \frac{\mathbb{Z}[x]/(p)}{(x^2+1)} \text{ is an integral domain} \\
&\iff \frac{(\mathbb{Z}/p)[x]}{(x^2+1)} \text{ is an integral domain} \\
&\iff \mathbb{F}_p[x]/(x^2+1) \text{ is an integral domain} \\
&\iff (x^2+1) \text{ is a prime ideal of } \mathbb{F}_p[x] \\
&\iff (x^2+1) \text{ is maximal ideal in } \mathbb{F}_p[x] \\
&\iff x^2+1 \text{ is irreducible in } \mathbb{F}_p[x]
\end{aligned}
$$

where we have used that $\mathbb{F}_p[x]$ is a PID (so an ideal in $\mathbb{F}_p[x]$ is prime if and only if it is maximal).

□

7. Let $\omega \in \mathbb{C}$ be a primitive 8^{th} root of unity and set $F = \mathbb{Q}(\omega)$.

(a) Prove that there are exactly three subfields $E \subset F$ with $[E : \mathbb{Q}] = 2$.

(b) For each E above, find (with justification) an element $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$.

Solution:

(a) Since ω is a primitive 8^{th} root of unity, F contains all the 8^{th} roots of unity, which implies that $F/\mathbb{Q}$ is the splitting field of the separable polynomial $p(x) = x^8 - 1$. This implies that $F/\mathbb{Q}$ is a Galois extension. Note that $p(x) = (x^4+1)(x^2+1)(x+1)(x-1)$. Since $\omega \notin \{\pm 1, \pm i\}$, it follows that the minimal polynomial of ω is $m(x) = x^4 + 1$. Thus, $[F\colon \mathbb{Q}] = 4 = |\operatorname{Gal}(F/\mathbb{Q})|$.

Without loss of generality, assume $\omega = e^{2\pi i/8} = e^{\pi i/4}$. If $\sigma \in \operatorname{Gal}(F/\mathbb{Q})$, then σ is uniquely determined by $\sigma(e^{\pi i/4})$. Note that σ permutes the roots of $m(x)$, so the possibilities are

$$\begin{aligned}\sigma_1(\omega) &= \omega\\ \sigma_2(\omega) &= \omega^3\\ \sigma_3(\omega) &= \omega^5\\ \sigma_4(\omega) &= \omega^7.\end{aligned}$$

Note that σ_1 is the identity and that every other element has order 2. For example, $\sigma_2^2(\omega) = \sigma(\omega^3) = \sigma(\omega)^3 = \omega^9 = \omega$, which implies that $\sigma_2^2 = \sigma_1$. Thus, $\operatorname{Gal}(F/\mathbb{Q}) \cong V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $F/\mathbb{Q}$ is a Galois extension, the Fundamental Theorem of Galois Theory implies that there is a bijection between the subgroups $H \subset \operatorname{Gal}(F/\mathbb{Q})$ and the fields E such that $\mathbb{Q} \subset E \subset F$. Since $\operatorname{Gal}(F/\mathbb{Q})$ contains three subgroups of index 2, there are exactly three subfields $E \subset F$ such that $[E\colon \mathbb{Q}] = 2$, as required.

(b) As in part (a), we can assume

$$\omega = e^{\pi i/4} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}.$$

Therefore, $F = \mathbb{Q}(\omega) = \mathbb{Q}\left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right) = \mathbb{Q}\left(\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2}\right) = \mathbb{Q}(\sqrt{2} + i\sqrt{2})$. We claim that $F = \mathbb{Q}(\sqrt{2}, i)$. It is obvious that $F \subset \mathbb{Q}(\sqrt{2}, i)$. Observe that

$$(\sqrt{2} + i\sqrt{2})\left(\frac{\sqrt{2} - i\sqrt{2}}{4}\right) = 1$$

which shows that $\frac{\sqrt{2}-i\sqrt{2}}{4} \in F$. Hence, $\sqrt{2} - i\sqrt{2} \in F$. This implies that

$$\frac{1}{2}\left[(\sqrt{2} + i\sqrt{2}) + (\sqrt{2} - i\sqrt{2})\right] = \sqrt{2} \in F.$$

Therefore,

$$\frac{1}{2\sqrt{2}}\left[(\sqrt{2} + i\sqrt{2}) - (\sqrt{2} - i\sqrt{2})\right] = i \in F.$$

Thus, $F = \mathbb{Q}(\sqrt{2}, i)$, as claimed. Therefore, the three subfields $E_1, E_2, E_3 \subset F$ satisfying $[E_i\colon \mathbb{Q}] = 2$ for $i \in \{1, 2, 3\}$ are $E_1 = \mathbb{Q}(\sqrt{2})$, $E_2 = \mathbb{Q}(i)$, and $E_3 = \mathbb{Q}(i\sqrt{2})$.

□

8. Let R be a commutative ring and M an R-module. An R-submodule N of M is called *maximal* if $N \neq M$ and there are no proper R-submodules of M properly containing N.

(a) Suppose M is finitely generated. Prove that there exists at least one maximal R-submodule of M.

(b) Prove that if N is a maximal R-submodule of M, then $M/N \cong R/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal of R.

Solution:

(a) Let $\mathcal{M}$ denote the collection of all proper R-submodules of M. The set $\mathcal{M}$ is partially ordered under the inclusion relation. Let $\mathcal{C}$ be a chain in $\mathcal{M}$. It needs to be shown that $\mathcal{C}$ has an upper bound in $\mathcal{M}$. Let

$$L = \bigcup_{C \in \mathcal{C}} C.$$

The first claim is that L is a submodule of M. It is obvious that L is nonempty. If $x, y \in L$, then there exists $C \in \mathcal{C}$ such that $x \in C$ and there exists $C' \in \mathcal{C}$ such that $y \in C'$. In this case, either $C \subset C'$ or $C' \subset C$. Without loss of generality, assume that $C \subset C'$. Then $x, y \in C'$, which implies that $x + y \in \mathbb{C}' \subset L$. Therefore, L is closed under addition. Now let $x \in L$, $r \in R$. Then there exist $C \in \mathcal{C}$ such that $x \in C$. Since C is a submodule of M, $rx \in C \subset L$. This shows that L is a submodule of M, as claimed.

We need now show that L is a proper submodule of M. Since M is finitely generated, there exists a finite generating set $\{x_1, \ldots, x_k\}$. If $L = M$, then there exist submodules $C_n \in \mathcal{C}$ such that $x_n \in C_n$. Let C be the maximal element of the set $\{C_n : n \in \{1, \ldots, k\}\}$. Then $\{x_1, \ldots, x_k\} \subset C$, so $C = M$. This contradicts the assumption that C was a proper submodule of M. Therefore, L is a proper submodule of M. Then an arbitrary chain $\mathcal{C}$ has an upper bound in $\mathcal{M}$. By Zorn's Lemma, $\mathcal{M}$ has a maximal element, which must be a maximal R-submodule of M.

(b) By the Correspondence Theorem, the R-submodule of M/N are in one-to-one correspondence to the R-submodules of M containing N. Since the only R-submodules of M containing N are N and M, the only R-submodules of M/N are 0 and M/N. In other words, M/N is a simple R-module.

Let $\overline{x} \in M/N$ be nonzero. Then the R-submodule $R\overline{x}$ is nonzero. This implies that $M/N = R\overline{x}$. Then the function $f : R \to M/N$ given by $r \mapsto r\overline{x}$ is surjective. By the First Isomorphism Theorem, $R/\ker f \cong M/N$. Since $R/\ker f$ is a simple R-module, the Correspondence Theorem implies that $\ker f$ is a maximal R-submodule of R. Since the R-submodules of R are exactly the ideals of R, $\ker f$ is a maximal ideal of R, as required.

□

9. Reduce the matrix

$$A = \begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix}$$

to diagonal form over $\mathbb{Z}$ and express the cokernel of A (that is, $\mathrm{Col}_3(\mathbb{Z})/\mathrm{image}(A)$) as a direct sum of cyclic groups.

Solution: Perform the following row and column operations:

$$\begin{aligned} 3R_1 + R_2 &\longrightarrow R_2 \\ -6R_1 + R_3 &\longrightarrow R_3 \\ R_2 + R_3 &\longrightarrow R_3 \\ C_1 + C_3 &\longrightarrow C_3 \\ -3C_2 + C_1 &\longrightarrow C_1 \\ C_2 + C_3 &\longrightarrow C_3 \\ R_1 &\longleftrightarrow R_2 \end{aligned}$$

This obtains the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Therefore, $\mathrm{im}\, A \cong \mathbb{Z} \times 11\mathbb{Z} \times 0 \cong \mathbb{Z} \times 11\mathbb{Z}$. Also, $\mathrm{coker}\, A \cong \mathrm{Col}_3(\mathbb{Z})/\,\mathrm{im}\, A \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. □

10. Let F be a finite field. Prove that the multiplicative group $F^\times$ of non-zero elements of F is a cyclic group. (Hint: a polynomial of degree n over a field has at most n roots.)

Solution: It is clear that $F^\times$ is a finite abelian group. Let C_r denote the cyclic group with r elements. By the Fundamental Theorem of Finitely Generated Abelian Groups,

$$F^\times \cong C_{r_1} \times \cdots \times C_{r_k}$$

for some $k \geq 1$ and $r_1 \mid r_2 \mid \cdots \mid r_k$. We claim that $k = 1$. Suppose to the contrary that $k \geq 2$. Consider the polynomial $p(x) = x^{r_1} - 1$. Any element of $F^\times$ is of the form $(a, 1, 1, \ldots, 1)$ and is clearly a root of $p(x)$. This accounts for r_1 distinct roots of $p(x)$. Since $r_1 \mid r_2$ and C_{r_2} is abelian, C_{r_2} contains a subgroup H or order r_1. Now every element of the form $(1, a, 1, \ldots, 1)$ with $a \in H$ is a root of $p(x)$. This implies that there are at least $2r_1$ roots of $p(x)$, but $p(x)$ has degree r_1, a contradiction. Therefore, $k = 1$ and $F^\times C_{r_1}$. Thus, $F^\times$ is a cyclic group.

OR

Let $q = |F|$ so that $|F^\times| = q - 1$. Let m be the maximal order of the elements of $F^\times$. By Lagrange's Theorem, $m \mid (q-1)$. This implies $m \leq q - 1$. We claim $m = q - 1$ so that we only need show $q - 1 \leq m$. In any finite abelian group, the order of every element divides the maximal order of all the elements. Then every element $x \in F^\times$ satisfies $x^m = 1$. Then every element of $F^\times$ is a root of $x^m - 1$. The number of possible roots of $x^m - 1$ is m so that $q - 1 \leq m$. But then $m = q - 1$. Therefore, some element of $F^\times$ has order $q - 1$. Hence, $F^\times$ is cyclic.

OR

We first prove that if G is a finite group with n elements such that for every divisor d of n, the number of elements dividing d is at most d, then G is cyclic.

Suppose $d \mid n$ and let G_d be the set of elements of G with order d. If $G_d \neq \emptyset$, there is a $y \in G_d$. We have $\langle y \rangle \subseteq \{x \in G \colon x^d = 1\}$. But $\langle y \rangle$ has cardinality d. But then $\langle y \rangle = \{x \in G \colon x^d = 1\}$. Then G_d is the set of generators of $\langle y \rangle$ of order d. Therefore, $\#G_d = \phi(d)$.

We have shown G_d is either empty or possesses cardinality $\phi(d)$ for each $d \mid n$. Then

$$n = \#G = \sum_{d|n} \#G_d \leq \sum_{d|n} \phi(d) = n$$

Therefore, $\#G_d = \phi(d)$ for each $d \mid n$. In particular, $G_n \neq \emptyset$. But then G is cyclic.

Now in our case we have $G = F^\times$, a finite group. If $|F^\times| = n$ and $d \mid n$ then $x^d = 1$ if and only if $x^d - 1 = 0$ as in the ring. This polynomial can have at most d roots. But then the claim above applies so that $F^\times$ is then a cyclic group.

OR

Suppose that $|F^\times| = n$ and $d \mid n$. Let $\psi(d)$ denote the number of elements of order d in $F^\times$. Suppose there exists an element $x \in F^\times$ of order d. Consider $\langle x \rangle$. Then every element of $\langle x \rangle$ satisfies $y^d = 1$. But the number of solutions of $x^d = 1$ is at most d (since x is a solution if and only if $x^d - 1 = 0$). Then $\langle x \rangle = \langle x \in F^\times \colon x^d = 1\}$. But then $\psi(d) = 0$ or $\phi(d)$. But

$$\sum_{d|n} \psi(d) = n = \sum_{d|n} \phi(d)$$

so that $\psi(d) = \phi(d)$ for all $d \mid n$. In particular, $\psi(n) = \phi(d)$, meaning there exists an element of order n in $F^\times$.

OR

Let $G := F^\times$. By the Fundamental Theorem of Finitely Generated Abelian Groups, we have

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$$

where the p_i are primes, not necessarily distinct, and $n_r \geq 1$. Each $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ is a cyclic group of order $p_i^{n_i}$. Let $m = \text{lcm}\{p_1^{n_1}, \ldots, p_r^{n_r}\}$. We know $m \leq p_1^{n_1} \cdots p_r^{n_r}$. If $a_i \in \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, then $a_i^{p_i^{n_i}} = 1$, hence $a_i^m = 1$. But then for all $\alpha \in G$, $\alpha^m = 1$, i.e. every element of G is a root of $x^m = 1$. But G contains $p_1^{n_1} \cdots p_r^{n_r}$ elements while the polynomial $x^m - 1$ has at most m roots in F. Then $m = p_1^{n_1} \cdots p_r^{n_r}$. As the p_i are distinct, the group G is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.

OR

Let $G := F^\times$ and $n = \max\{|y| : y \in G\}$. Let $|G| = N$. Choose $a \in G$ so that $|a| = n$. If we can show that $n = N$, then $|a| = |G|$ which implies $G = \langle a \rangle$ and G is then cyclic. Now $a \in G$ so that $|a| = n \mid N$ and $n \leq N$. We need show $n \geq N$. In any abelian group with elements of finite order r, s, the group contains an element of order $\text{lcm}(r, s)$. Then G contains an element of order $\text{lcm}(|a|, |g|)$ so $\text{lcm}(n, |g|) \leq n$. But then $|g| \mid n$ and then $g^n = 1$ for every $g \in G$. Then $x - g$ is a factor of the polynomial $x^n - 1$ for every $g \in G$. Therefore, $\prod_{g \in G}(x - g)$ divides $x^n - 1$. However, $\prod_{g \in G}(x - g)$ has degree N so that $N \leq n$. □

August 2012

1.

(a) Let G be a group and let $g \in G$ be an element of order $n > 0$. For any integer r, prove that the order of g^r is $\frac{n}{d}$, where $d = \gcd(n, r)$.

(b) Find and describe up to isomorphism the group of automorphisms of a cyclic group of order 8.

Solution:

(a) Since d divides r, $\frac{r}{d} \in \mathbb{Z}$. Therefore,

$$(g^r)^{n/d} = g^{(rn)/d} = (g^n)^{r/d} = 1^{r/d} = 1.$$

If $(g^r)^k = g^{rk} = 1$ for some $k \in \mathbb{N}$, then n divides rk. Therefore, $\frac{n}{d}$ divides $\frac{r}{d}k$. Since $\frac{n}{d}$ and $\frac{r}{d}$ are relatively prime, $\frac{n}{d}$ divides k, this impies $k \geq \frac{n}{d}$. Thus, $|g^r| = \frac{n}{d}$, as required.

(b) Note that any cyclic group of order 8 is isomorphic to $\mathbb{Z}/8\mathbb{Z}$. Consider $\phi \in \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$. The homomorphism ϕ is completely determined by $\phi(1 + 8\mathbb{Z})$. Now ϕ is an isomorphism if and only if $\phi(1 + 8\mathbb{Z})$ has order 8. Since $k + 8\mathbb{Z} = k(1 + 8\mathbb{Z})$, part (a) implies that this is only the case if $(k, 8) = 1$. Therefore, there are four automorphisms of $\mathbb{Z}/8\mathbb{Z}$:

$$\begin{aligned}
\phi_1 &: 1 + 8\mathbb{Z} \mapsto 1 + 8\mathbb{Z} \\
\phi_2 &: 1 + 8\mathbb{Z} \mapsto 3 + 8\mathbb{Z} \\
\phi_3 &: 1 + 8\mathbb{Z} \mapsto 5 + 8\mathbb{Z} \\
\phi_4 &: 1 + 8\mathbb{Z} \mapsto 7 + 8\mathbb{Z}
\end{aligned}$$

Note that the element ϕ_1 is the identity and that the order of every other element is 2. Therefore, $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein 4-group.

□

2.

(a) Let T be a linear operator on a two-dimensional vector space V over a fixed field F. Assuming T is not multiplication by a scalar, prove that there is a vector $v \in V$ for which $(v, T(v))$ is a basis for V and describe the first column of the matrix of T with respect to that basis.

(b) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2×2 matrix over a field F. Prove that there exists an invertible 2×2 matrix E for which $B = EAE^{-1} = \begin{bmatrix} 0 & * \\ 1 & * \end{bmatrix}$, unless $b = c = 0$ and $a = d$.

(a) Since V has dimension 2, it is sufficient to show that there exists a vector $v \in V$ such that $(v, T(v))$ is linearly independent. Suppose to the contrary that this is not the case. Then for all $v \in V$, $Tv = \lambda_v v$, where $\lambda_v \in F$ depends on v. Let $\mathcal{B} = \{e_1, e_2\}$ be a basis for V. Then

$$T(e_1 + e_2) = T(e_1) + T(e_2) = \lambda_{e_1} e_1 + \lambda_{e_2} e_2 = \lambda_{e_1+e_2} + \lambda_{e_1+e_2} e_2.$$

Since any vector in V can be written uniquely as a linear combination of e_1 and e_2, this implies that $\lambda_{e_1} = \lambda_{e_1+e_2} = \lambda_{e_2}$. Let $\lambda = \lambda_{e_1}$. Then for any $v \in V$, $v = a_1 e_1 + a_2 e_2 a$ for some $a_1, a_2 \in F$. Now

$$T(v) = T(a_1 e_1 + a_2 e_2 a) = a_1 T(e_1) + a_2 T(e_2) = a_1 \lambda e_1 + a_2 \lambda e_2 = \lambda(a_1 e_1 + a_2 e_2 a).$$

This implies that T is multiplication by a scalar, a contradiction. Therefore, there exists $v \in V$ such that $Tv \neq \lambda v$ for all $\lambda \in F$, which implies that (v, Tv) is linearly dependent. Thus, there exists $v \in V$ such that (v, Tv) is a basis for V. Let $\mathcal{B}'$ denote the basis. The first column of T with respect to $\mathcal{B}'$ is

$$[T(v)]_{\mathcal{B}'} = [0 \cdot v + 1 \cdot T(v)]_{\mathcal{B}'} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(b) Suppose that A is not of the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

for any $a \in F$. We claim that the linear transformation represented by A is not multiplication by a scalar. Suppose to the contrary that $Av = \lambda v$ for some $\lambda \in F$ and all $v \in F^2$. Then λ is an eigenvalue of A with multiplicity 2. Therefore, the characteristic polynomial of A is $c(x) = (x - \lambda)^2$ and the minimal poynomial of A is $m(x) = x - \lambda$. Now A is similar to the matrix λI_2. If $\lambda \neq 0$, then $\lambda I_2 \in Z(\mathrm{GL}_2(F))$, so $A = \lambda I_2$. If $\lambda = 0$, then A is similar to the zero matrix, which implies that A is the zero matrix. In either case, we have a contradiction. This proves the claim.

By part (a), there exists a basis of F^2 of the form (v, Av). Writing A as a matrix with respect to this basis implies that A is similar to a matrix of the form

$$B = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix},$$

so there exists an invertible matrix E such that $B = EAE^{-1}$.

□

3.

(a) A set X consisting of n elements is a left G-set, for some group G. Show that there exists a homomorphism $G \to S_n$, where S_n is the symmetric group.

(b) If $n = 4$ and G is a cyclic group of order 9, how many distinct structures of a left G-set are possible on X? How many nonisomorphic G-sets are among them? Describe the orbits for each of the G-sets.

Solution:

(a) For every $g \in G$, define a function $\sigma_g : X \to X$ via $\sigma_g(x) := g \cdot x$. We claim that σ_g is a permutation of X (a bijection $X \to X$). If $\sigma_g(x) = \sigma_g(y)$, then $g \cdot x = g \cdot y$. After multiplication by g^{-1} on the left on both sides, we have $x = y$. But then σ_g is injective. Now for $x \in X$, $\sigma_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = x$. Therefore, σ_g is surjective. Therefore, $\sigma_g : X \to X$ is a bijection so that σ_g is a permutation of X.

Let S_X denote the symmetric group on X, and define $\phi : G \to S_X$ via $g \mapsto \sigma_g$. For any $g, h \in G$, $x \in X$,

$$\sigma_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot \sigma_h(x) = \sigma_g(\sigma_h(x)) = (\sigma_g \circ \sigma_h)(x).$$

Thus, $\sigma_{gh} = \sigma_g \sigma_h$, so that ϕ is a homomorphism. Since $S_X \cong S_n$, there exists a homomorphism $\phi : G \to S_n$.

(b) The number of distinct possible left G-sets on X is equal to the number of homomorphisms $\phi : G \to S_4$. Let g be a generator of G. Then ϕ is completely determined by $\phi(g)$. Notice that $\phi(g)^9 = \phi(g^9) = \phi(1) = 1$, so $|\phi(g)|$ divides both 9 and 24. Hence, either $|\phi(g)| = 1$ or $|\phi(g)| = 3$. If $|\phi(g)| = 1$, then $\phi(g) = 1$ and the action is trivial, i.e. every element of X is a fixed point.

If $|\phi(g)| = 3$, then $\phi(g)$ is a 3-cycle. Since there are $\binom{4}{3} \cdot 2 = 8$ distinct 3-cycles in S_4, there are a total of 9 distinct choices for $\phi(g)$, so there are 9 distinct structures of a left G-set on X.

Now write $X = \{a, b, c, d\}$ and $Y = \{a', b', c', d'\}$ and suppose $\phi : G \to S_X$ and $\phi : G \to S_Y$ are homomorphisms such that $\phi(g) = (a\ b\ c)$ and $\phi(g) = (a'\ b'\ c')$. Then it is easy to see that the function

$$a \mapsto a' \quad b \mapsto b' \quad c \mapsto c' \quad d \mapsto d'$$

is an isomorphism of G-sets. Taking $X = Y$, it follows that there are only two nonisomorphic G-sets on X: the trivial one and sending a generator to a 3-cycle.

□

4.

(a) Prove that a group of order 85 is cyclic.

(b) Prove that a group of order 55 is generated by two elements x, y satisfying $x^{11} = 1, y^5 = 1$, and $yxy^{-1} = x^r$, for some r, $1 \leq r < 11$. Show that $r = 2$ is not possible. You need not render a decision about the possibility of $r = 1$ or $3 \leq r \leq 10$. Is it a simple group?

Solution:

(a) Let $n_p(G)$ denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_{17}(G) \equiv 1 \mod 17$ and divides 5. Then $n_{17} = 1$. By similar logic, we have $n_5(G) = 1$. But then the Sylow 5-subgroup and the Sylow 17-subgroup are unique, hence normal. Furthermore by Lagrange's Theorem, the intersection of these groups must be trivial. Call these subgroups H and K, respectively. Notice that HK is a subgroup of G of order $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{17 \cdot 5}{1} = 85$. Let $x \in H$ and $y \in K$ be non-identity elements. We have $G \cong H \times K$, which is cyclic generated by (x, y). Alternatively, $\langle xy \rangle = G$ since its order is $\text{lcm}(|x|, |y|) = 85$. Alternatively, the unique Sylow 5-subgroup and Sylow 17-subgroup make up $17 + 5 - 1 = 21$ elements of G. The remaining elements of G must be of order 85, any of which will generated G. Therefore, G is cyclic.

OR

We claim that G must be abelian and the result will follow: if G is abelian, by Cauchy's Theorem (or considering $|HK| = \frac{|H||K|}{|H \cap K|}$), G must have elements of order 5 and 17, say x and y, respectively. But then xy is an element of G of order $\text{lcm}(5, 17) = 85$. But then G is cyclic. We now need show that G is abelian.

If G is nonabelian, we know $Z(G) < G$ and must have order 1, 5, or 17 by Lagrange's Theorem. However, $|Z(G)| \neq 5$ or 17 since then $G/Z(G)$ would be cyclic, implying that G is abelian. By the Class Equation

$$|G| = |Z(G)| + |C_G(x_1)| + \cdots + |C_G(x_r)|,$$

where $x_1, \ldots, x_r$ are distinct representatives for the conjugacy classes of G. Let $|C_G(x_i)| = n_i$. We have $85 = 1 + n_1 + \cdots + n_r$.

Now let $g \in G$ be a nonidentity element. If $|g| = 85$, then G is cyclic. If $|g| = 5$, then $C_G(g)$ has order at least 5 and dividing $|G|$. Since $Z(G) = \{1\}$, we have $|C_G(g)| = 85/5 = 17$. Mutatis mutandis, if $|g| = 17$, then $|C_G(g)| = 5$. Then one of n_i is 5 and

another 17. In particular, $n_i \geq 5$ so that $r \leq 16$, i.e. G has at most 17 conjugacy classes. By a result of Burnside's in Representation Theory, if $|G|$ is odd, then $|G| \equiv r \mod 16$, where r is the number of conjugacy classes. In our case, $(r+1) \equiv 85 \mod 16$ and $r+1 \leq 17$. But then $r = 4$. Hence $84 = 1 + n_1 + \cdots + n_4$ with $n_i \in \{5, 17\}$. This is impossible since the left side is at most 69. But then it must be that G is abelian, and by the work above, cyclic.

(b) Let G be a group of order $55 = 5 \cdot 11$. Notice that $n_{11}(G) \equiv 1 \mod 11$ and divides 55. This implies $n_{11}(G) = 1$. Therefore, G has a unique, hence normal, Sylow 11-subgroup. But then G is not simple. Let P_5 denote a Sylow 5-subgroup of G and P_{11} denote the unique Sylow 11-subgroup of G. Both P_5 and P_{11} are cyclic, say $P_5 = \langle y \rangle$ and $P_{11} = \langle x \rangle$. Then $|P_5 \cap P_{11}| = 1$ by Lagrange's Theorem, so

$$|P_5 P_{11}| = \frac{|P_5|\,|P_{11}|}{|P_5 \cap P_{11}|} = 55.$$

Therefore, $P_5 P_{11} = G$, which implies that xy generates G. Since P_{11} is normal in G, $yxy^{-1} \in P_{11}$ which implies $yxy^{-1} = x^r$ for some r, $1 \leq r \leq 11$. Note that $r = 11$ is not possible since $|x^r| = |yxy^{-1}| = |x| = 11 \neq 1$. Suppose $r = 2$, then $x^2 = yxy^{-1}$. Since $y^5 = 1$,

$$\begin{aligned}
x = y^5 x y^{-5} &= y^4 (yxy^{-1}) y^{-4} \\
&= y^4 x^2 y^{-4} \\
&= y^3 y x^2 y^{-1} y^{-3} \\
&= y^3 (yxy^{-1})^2 y^{-3} \\
&= y^3 x^4 y^{-3} \\
&= y^2 y x^4 y^{-1} y^{-2} \\
&= y^2 (yxy^{-1})^4 y^{-2} \\
&= y^2 x^8 y^{-2} \\
&= y (y x^8 y^{-1}) y^{-1} \\
&= y (yxy^{-1}) y^{-1} \\
&= y (yxy^{-1})^8 y^{-1} \\
&= y x^{16} y^{-1} = (yxy^{-1})^{16} = x^{32} = x^{10}.
\end{aligned}$$

Thus, $x^9 = 1$, a contradiction to the fact that $|x| = 11$. Then $r = 2$ is not possible, leaving $3 \leq r < 11$.

□

5. Prove that an $n \times n$ complex matrix A is Hermitian if and only if X^*AX is real for all complex vectors X; here $*$ denotes the conjugate transpose.

Solution: Assume that A is Hermitian, i.e. $A^* = A$. For any $X \in \mathbb{C}^n$,

$$(X^*AX)^* = X^*A^*X^{**} = X^*AX.$$

Viewing X^*AX as a complex number in the obvious way, this implies $\overline{X^*AX} = X^*AX$. Hence, X^*AX is real.

Now assume that X^*AX is real for all $X \in \mathbb{C}^n$. Let $\{e_1, \ldots, e_n\}$ denote the standard basis for $\mathbb{C}^n$. Let $A = (a_{ij})$. By assumption, $e_i^*Ae_i$ is real for each index i. Since $a_{ii} = e_i^*Ae_i$, a_{ii} is real for $1 \leq i \leq n$, i.e. $a_{ii} = \overline{a_{ii}}$.

Now take $X = e_i + e_j$ for indices i, j. By hypothesis, X^*AX is real. Notice that

$$X^*AX = (e_i + e_j)^*A(e_i + e_j) = e_i^*Ae_i + e_j^*Ae_j + e_i^*Ae_j + e_j^*Ae_i = a_{ii} + a_{jj} + a_{ij} + a_{ji}.$$

Furthermore by assumption, $e_i^*Ae_i$ and $e_j^*Ae_j$ are real. This implies that $a_{ij} + a_{ji}$ is real. Thus, $\mathrm{Im}(a_{ij}) = -\mathrm{Im}(a_{ji})$.

Take $X = ie_i + e_j$ for indices i, j. By assumption, X^*AX is real. Now

$$\begin{aligned} X^*AX &= (ie_i + e_j)^*A(ie_i + e_j) \\ &= -ie_i^*Aie_i - ie_i^*Ae_j + e_j^*Aie_i + e_j^*Ae_j \\ &= e_i^*Ae_i + e_j^*Ae_j + i(e_j^*Ae_i - e_i^*Ae_j) \end{aligned}$$

By assumption, $e_i^*Ae_i$ and $e_j^*Ae_j$ are real, so $i(e_j^*Ae_i - e_i^*Ae_j)$ is real. This implies $i(a_{ji} - a_{ij})$ is real. But then $\mathrm{Re}(a_{ji} - a_{ij}) = 0$ which implies $\mathrm{Re}(a_{ji}) = \mathrm{Re}(a_{ij})$. Since $\mathrm{Re}(a_{ij}) = \mathrm{Re}(a_{ji})$ and $\mathrm{Im}(a_{ij}) = -\mathrm{Im}(a_{ji})$, $a_{ij} = \overline{a_{ji}}$ for any $1 \leq i, j \leq n$. But then $A = A^*$, i.e. A is Hermitian. □

6. Determine whether each of the following ideals is a maximal ideal in $\mathbb{C}[x, y]$. Each is worth 5 points.

(a) $\langle (x-1)^2 + y^2 - 1, (x+1)^2 + y^2 - 1, x^2 + (y-1)^2 - 1, x^2 + (y+1)^2 - 1 \rangle$

(b) $\langle x^2 + y^2 - 9, x^2 + (y-4)^2 - 25, x^2 + (y+4)^2 - 25 \rangle$

Solution:

(a) Graphing the circles $(x-1)^2 + y^2 = 1$, $(x+1)^2 + y^2 = 1$, $x^2 + (y-1)^2 = 1$, $x^2 + (y+1)^2 = 1$ gives Figure 1, seen below.

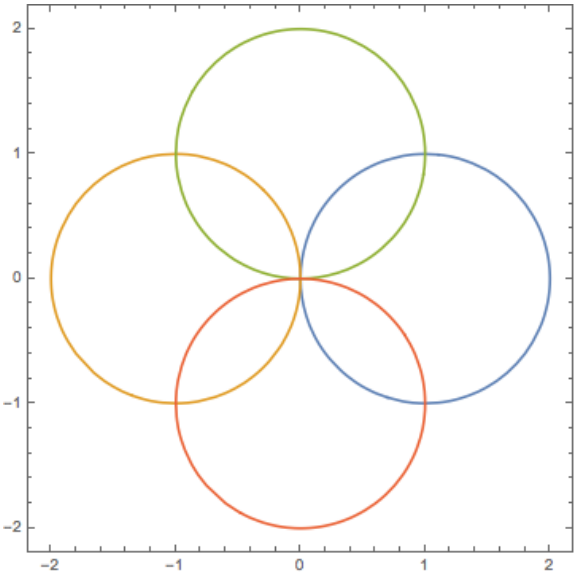


Figure 1: Graphical representations of the ideal $\langle (x-1)^2+y^2-1, (x+1)^2+y^2-1, x^2+(y-1)^2-1, x^2+(y+1)^2-1\rangle$.

Since these circles intersect at the origin, the ideal is the ideal (x,y), which is maximal since $\mathbb{C}[x,y]/(x,y) \cong \mathbb{C}$ is a field. Alternatively, note that (x,y) is contains the given ideal. Observe

$$(x^2+(y-1)^2-1)-(x^2+(y+1)^2-1) = -4y$$
$$((x-1)^2+y^2-1)-((x+1)^2+y^2-1) = -4x$$

But then (x,y) is contained in the given ideal. Therefore, $(x,y) = \langle (x-1)^2+y^2-1, (x+1)^2+y^2-1, x^2+(y-1)^2-1, x^2+(y+1)^2-1\rangle$ and (x,y) is maximal as $\mathbb{C}[x,y]/(x,y) \cong \mathbb{C}$ is a field.

(b) Graphing the circles $x^2+y^2=9$, $x^2+(y-4)^2=25$, and $x^2+(y+4)^2=25$ gives Figure 2, seen below.

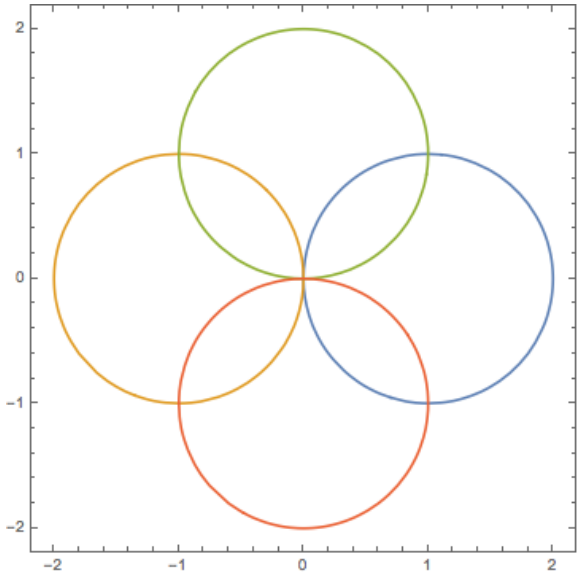


Figure 2: Graphical representations of the ideal $\langle x^2+y^2-9, x^2+(y-4)^2-25, x^2+(y+4)^2-25\rangle$.

The circles intersect at the points $(3,0)$ and $(-3,0)$. This implies that the given ideal is $(3+x,y)\cap(3-x,y)$ which is not maximal since it is properly contained in the ideal $(3+x,y)$.

□

7. Let R be a commutative ring with identity and let I be a nonzero ideal of R. This makes I into an R-module. Prove that I is a free R-module if and only if I is a principal ideal generated by an element that is not a zero divisor.

Solution: Suppose that I is a free R-module. There exists a basis $\mathcal{B}$ for I. Recall that if $\mathcal{B}$ is a basis for I, every element in I can be written *uniquely* as a linear combination of elements of $\mathcal{B}$. We claim $|\mathcal{B}|=1$. If $|\mathcal{B}|>1$, then we can choose distinct $x,y\in\mathcal{B}$. Then $0=0\cdot x+0\cdot y=y\cdot x+(-x)\cdot y$, a contradiction to the fact that $\mathcal{B}$ is a basis. Therefore, $|\mathcal{B}|=1$, i.e. $\mathcal{B}=\{x\}$ for some $x\in I$. It is clear that $I=(x)$. If $rx=0$ for some $r\in R$, then $rx=0=0x$, a contradiction to the fact that $\mathcal{B}$ is a basis. Hence, x is not a zero divisor.

Suppose that $I=(x)$ is a nonzero ideal, where x is not a zero divisor. We claim that $\{x\}$ is a basis for I as an R-module. It is clear that every element of I is of the form rx for some $r\in R$. It remains to show that this expression is unique. If $rx=sx$ for some $r,s\in R$,

then

$$rx - sx = 0$$
$$(r - s)x = 0$$

Since x is nonzero and not a zero divisor, $r - s = 0$. Thus, $r = s$, proving uniqueness. Therefore, I is a free R-module. □

8. A 9×9 matrix M with complex entries has characteristic polynomial equal to $(x - 1)^4(x - 2)^5$.

(a) List all the possible minimal polynomials for M.

(b) Of all the possibilities in (a) which one(s) lead to the largest number of possible Jordan Canonical forms for M?

Solution:

(a) The minimal polynomial need have roots $x = 1$ and $x = 2$, i.e. divisors $x - 1$ and $x - 2$ and divide the characteristic polynomial. Then there are 20 possibilities: $\{(x - 1)^i(x - 2)^j : 1 \leq i \leq 4, 1 \leq j \leq 5\}$.

(b) Let $m(x)$ denote the minimal polynomial of M. The number of possible Jordan canonical forms is the same as the number of possible elementary divisors. For $(x - 1)$, let k denote the power of $(x - 1)$ in $m(x)$. Note that k is the largest power of $(x - 1)$ that can be an elementary divisor. If $k = 1$, there is only one possibility for the elementary divisors associated to the eigenvalue 1: $(x - 1)$ four times. If $k = 2$, there are two possibilities: $(x - 1)$, $(x - 1)$, $(x - 1)^2$ or $(x - 1)^2$ twice. If $k = 3$, then the only possibility for the elementary divisors is $(x - 1)$, $(x - 1)^3$. If $k = 4$, then the only possibility for the elementary divisors is $(x - 1)^4$. Therefore, the most possible Jordan canonical forms will occur when $k = 2$.

Let j denote the power of $(x - 2)$ in $m(x)$. If $j = 1, 4$, or 5, then there is only one possibility for the elementary divisors (similar reasoning to above). If $j = 2$, then there are two possibilities: $(x - 2)^2$, $(x - 2)^2$, $(x - 2)$ or $(x - 2)$, $(x - 2)$, $(x - 2)$. If $j = 3$, then there are two possibilities: $(x - 2)^3$, $(x - 2)^2$ or $(x - 2)^3$, $(x - 2)$, $(x - 2)$.

Thus, the largest number of possible Jordan canonical forms occurs when $k = 2$ and $j = 2$ or $j = 3$. Thus, the two minimal polynomials that leads to the largest number of Jordan canonical forms is $m(x) = (x - 1)^2(x - 2)^2$ and $m(x) = (x - 1)^2(x - 2)^3$, which each lead to 4 possible Jordan canonical forms.

□

9. Find a primitive element for the following field extensions. Be sure to prove it is a primitive element. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, i)$. As usual $i^2 = -1$.

Solution: We claim $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. Since $\sqrt{2}, i \in \mathbb{Q}(\sqrt{2}, i)$, $\sqrt{2} + i \in \mathbb{Q}(\sqrt{2}, i)$. Since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, i)$, it follows that $\mathbb{Q}(\sqrt{2} + i) \subset \mathbb{Q}(\sqrt{2}, i)$. Observe that

$$(\sqrt{2} + i)\left(\frac{\sqrt{2} - i}{3}\right) = \frac{2 + 1}{3} = 1.$$

Therefore, $\frac{\sqrt{2}-i}{3} \in \mathbb{Q}(\sqrt{2} + i)$. It follows that $\sqrt{2} - i \in \mathbb{Q}(\sqrt{2} + i)$. Thus,

$$\frac{1}{2}\Big((\sqrt{2} + i) + (\sqrt{2} - i)\Big) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$$
$$\frac{1}{2}\Big((\sqrt{2} + i) - (\sqrt{2} - i)\Big) = i \in \mathbb{Q}(\sqrt{2} + i)$$

Since $\mathbb{Q}(\sqrt{2} + i)$ contains $\mathbb{Q}$, $\sqrt{2}$, and i, $\mathbb{Q}(\sqrt{2}, i) \subset \mathbb{Q}(\sqrt{2} + i)$. Since the reverse containment holds, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$, i.e. $\sqrt{2} + i$ is a primitive element for the given field extension. □

10. Let $F \subsetneq E$ be a finite extension of fields of characteristic 0.

(a) Prove that there exists a field $K \supset E$ such that $F \subset K$ is a finite Galois extension.

(b) Prove that there are at most finitely many distinct fields L with $F \subset L \subset E$.

Solution:

(a) Since $F \subset E$ is a finite extension of fields, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $n \in \mathbb{N}$ and some collection $\alpha_i \in E$ algebraic over F. For $i = 1, \ldots, n$, let $m_{\alpha_i}(x)$ denote the minimal polynomial of α_i over F. Let

$$m(x) = \prod_{i=1}^{n} m_{\alpha_i}(x),$$

and let $n = \deg m(x)$. Let K be the splitting field of $m(x)$ over F. Note that $E \subset K$ since $F \subset K$ and $\alpha_i \in K$ for $i = 1, \ldots, n$. The extension $F \subset K$ is finite since $[K\colon F] \leq n! < \infty$. Since F and K are fields of characteristic 0, the extension $F \subset K$ is separable, and this extension is also normal since K is the splitting field of a polynomial $m(x) \in F[x]$. Hence, $F \subset K$ is a normal, separable extension, which implies that $F \subset K$ is a Galois extension, as required.

(b) Let K be as in (a) and let $G = \mathrm{Gal}(K/L)$. Then

$$|G| = [K\colon L] < \infty$$

so that G is a finite group. This implies that G has finitely many subgroups. By the Fundamental Theorem of Galois Theory, there is a bijection between subgroups of G and fields L such that $F \subset L \subset K$. Hence, there are only finitely many such fields. In particular, there are only finitely many distinct fields $F \subset L \subset E$.

□

January 2013

1. Let G be a finite group and $p \in \mathbb{Z}$ a prime integer.

(a) Write down the characteristic equation for G and explain the notation.

(b) If $|G| = p^k$ for $k \geq 1$, show that $|Z(G)| \neq 1$, where $Z(G)$ denotes the center of G.

(c) If $|G| = p^2$, show that G is abelian.

Solution:

(a) The Class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G\colon C_G(a_i)]$$

where the $Z(G)$ is the center of G, $C_G(x)$ is the centralizer of x in G, and the summation is over $a_1, \ldots, a_r$ representatives for the distinct conjugacy classes of G. Note that each summand of the class equation is a divisor of $|G|$ and $[G\colon C_G(a_i)] > 1$ since $a_i \notin Z(G)$.

(b) The Class equation for G can be rewritten as

$$|Z(G)| = |G| - \sum_{i=1}^{r} [G\colon C_G(a_i)].$$

Each term on the right hand side is a divisor of $|G| = p^k$. Furthermore, each term on the right hand side is strictly larger than 1. Therefore, p divides every term on the right hand side, which implies that p divides the left hand side. Thus, p divides $|Z(G)|$ so that $|Z(G)| \neq 1$.

(c) By part (b), $|Z(G)| \neq 1$. Since $|Z(G)|$ divides p^2, either $|Z(G)| = p$ or $|Z(G) = p^2$. Therefore, either $|G/Z(G)| = p$ or $|G/Z(G)| = 1$. In the former case, $G/Z(G)$ is then cyclic by Lagrange's Theorem so that G is abelian, and in the latter case $Z(G) = G$ so that G is abelian.

The fact that $G/Z(G)$ is cyclic implies G is abelian deserved a proof: if $G/Z(G)$ is cyclic, there is a generator $\alpha Z(G)$ for some $\alpha \in G$. Let $a, b \in G$. Then $a = \alpha^n z$, $b = \alpha^m z'$ for some $n, m \in \mathbb{N}$, $z, z' \in Z(G)$. Thus,

$$ab = \alpha^n z \alpha^m z' = \alpha^n \alpha^m z z' = \alpha^m \alpha^n z' z = \alpha^m z' \alpha^n z = ba,$$

which implies that G is abelian.

□

2. Show that there is no simple group of order 30.

Solution: Let n_p denote the Sylow p-subgroup. By Sylow's Theorem, $n_5 \equiv 1 \mod 5$ and divides 30, so that it must be 1 or 6. Similarly, $n_3 \equiv 1 \mod 3$ and divides 30 so that n_p is 1 or 10. If either n_5 or n_3 is 1, then the Sylow 5-subgroup or Sylow 3-subgroup, respectively, is unique, hence normal.By Lagrange's Theorem, the intersection of any Sylow 5-subgroup and Sylow 3-subgroup is trivial. But if $n_5, n_3 > 1$, then G contains at least $4 \cdot 6 + 2 \cdot 10 + 1 = 45$ elements, a contradiction. Then one of n_5, n_3 is 1 so that G contains a normal subgroup and cannot be simple. □

3. Assume V is a finite dimensional vector space over the complex numbers $\mathbb{C}$ with a (positive definite) Hermitian form $\langle\ ,\ \rangle$ and let $B = \{v_1, v_2, \ldots, v_n\}$ be an orthonormal basis for V. Assume $T : V \to V$ is a linear transformation. What condition must the matrix of T with respect to B satisfy in order for $\langle T(u), T(v)\rangle = \langle u, v\rangle$ for all $u, v \in V$.

Solution: Let A denote the matrix of T with respect to B. Then for any indices i, j,

$$\langle A(v_i), A(v_j)\rangle = \langle v_i, v_j\rangle = \begin{cases} 1, & i = j, \\ 0, & \text{otherwise} \end{cases}$$

On the other hand, if a_i denotes the i^{th} column of A, then

$$\langle A(v_i), A(v_j)\rangle = \langle a_i, a_j\rangle.$$

Combining these two observations, it follows that the columns of A must form an orthonormal basis for V. Therefore, A is an orthogonal matrix. □

4. Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear operator.

(a) If $f \in F[x]$ is a polynomial with $f(T) = 0$, show that every eigenvalue of T is a root of f.

(b) If $g \in F[x]$ splits over F and $g(T)$ is *not* an isomorphism, show that at least one root of g is an eigenvalue of T.

Solution:

(a) Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let v be an eigenvector of T with eigenvalue λ. Then

$$0 = f(T)v = a_n T^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1 T(v) + a_0.$$

The claim is that $T^k v = \lambda^k v$ for all $k \in \mathbb{N}$ and we proceed by induction. The result is clear for $k = 1$. Suppose it holds for $k \in \mathbb{N}$. Then $T^{k+1}(v) = (T \circ T^k)(v) = T(\lambda^k v) = \lambda^k T(v) = \lambda^{k+1} v$. But then the claim follows by induction. Then we have

$$\begin{aligned} 0 = f(T)v &= a_n \lambda^n v + a_{n-1}\lambda^{n-1} v + \cdots + a_1 \lambda v + a_0 v \\ &= (a_n \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1 \lambda + a_0)v. \end{aligned}$$

Since $v \neq 0$, $f(\lambda) = a_n \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1 \lambda + a_0 = 0$.

(b) Without loss of generality, assume that $g(x)$ is monic with degree n. Let $\alpha_1, \ldots, \alpha_n$ denote the roots (not necessarily distinct) of $g(x)$. Then

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

Now $g(T)$ is not an isomorphism so that $\ker g(T) \neq 0$. Let $w \in \ker g(T)$ be nonzero. Then

$$0 = [(T - \alpha_1 I) \circ (T - \alpha_2 I) \circ \cdots \circ (T - \alpha_n I)](w).$$

If $(T - \alpha_n I)(w) = 0$, then $Tw = \alpha_n w$ and w is an eigenvector of T with eigenvalue α_n. Since α_n is a root of $g(x)$, this would complete the proof.

Now suppose $(T - \alpha_i)(w) \neq 0$ for $\alpha_1, \ldots, \alpha_n$. Define $m = \min\{k \in \{1, \ldots, n\} : [(T - \alpha_k I) \circ (T - \alpha_{k+1} I) \circ \cdots \circ (T - \alpha_n I)](w) \neq 0\}$ and $v = [(T - \alpha_m I) \circ (T - \alpha_{m+1} I) \circ \cdots \circ (T - \alpha_n I)](w)$. Then $(T - \alpha_{m-1})(v) = 0$ with $v \neq 0$ by the choice of m. Thus, $Tv = \alpha_{m-1} v$ and v is then an eigenvalue of T with eigenvalue α_{m-1}. Thus, at least one root of $g(x)$ is an eigenvalue of T.

□

5. Let $V = \mathbb{C}^4$ and let $T : V \to V$ be given by $T(v_1, v_2, v_3, v_4) = (v_3, v_1, v_2, v_3)$. Find all the eigenvalues for T and for each eigenvalue, find a basis for its characteristic space.

Solution: Let e_i denote the i^{th} standard basis vector and write T as a matrix relative to the bases $\mathcal{B} = \{e_1, \ldots, e_4\}$:

$$\begin{aligned} A &= [T(e_1)_{\mathcal{B}} \;\; T(e_2)_{\mathcal{B}} \;\; \cdots \;\; T(e_4)_{\mathcal{B}}] \\ &= [(e_2)_{\mathcal{B}} \;\; (e_3)_{\mathcal{B}} \;\; (e_4)_{\mathcal{B}} \;\; (e_1)_{\mathcal{B}}] \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

Now,

$$\begin{aligned} c_A(x) &= \det(xI - A) \\ &= \det \begin{pmatrix} x & 0 & 0 & -1 \\ -1 & x & 0 & 0 \\ 0 & -1 & x & 0 \\ 0 & 0 & -1 & x \end{pmatrix} \\ &= \det \begin{pmatrix} -1 & x & 0 \\ 0 & -1 & x \\ 0 & 0 & -1 \end{pmatrix} + x \det \begin{pmatrix} x & 0 & 0 \\ -1 & x & 0 \\ 0 & -1 & x \end{pmatrix} \\ &= -1 + x^4 \end{aligned}$$

This implies that the eigenvalues are the roots of $c_A(x) = x^4 - 1$, which are $1, -1, i$, and $-i$. Since the multiplicity of each root of $c_A(x)$ is 1, each characteristic space has dimension 1.

For the eigenvalue 1, a basis is $(1,1,1,1)$ since $T(1,1,1,1) = (1,1,1,1)$. For the eigenvalue -1, a basis is $(-1,1,-1,1)$ since $T(-1,1,-1,1) = (1,-1,1,-1) = -1(-1,1,-1,1)$. For the eigenvalue i, a basis is $(1,-i,-1,i)$ since $T(1,-i,-1,i) = (i,1,-i,-1) = i \cdot (1,-i,-1,i)$. For the eigenvalue $-i$, a basis is $(1,-i,1,-i)$ since $T(1,-i,1,-i) = (-i,1,-i,1) = -i \cdot (1,-i,1,-i)$. □

6. Consider the ring $\mathbb{Z}[x]$. For each pair of given ideals I and J, determine whether (i) $I \subsetneq J$, (ii) $J \subsetneq I$, (iii) $I = J$, or (iv) none of (i), (ii), or (iii)

(a) $I = \langle 3, x \rangle$, $J = \langle 3x \rangle$

(b) $I = \langle 3, x \rangle$, $J = \langle 3 - x, 3 + x \rangle$

(c) $I = \langle 3, x \rangle$, $J = \langle 6, 9, 2x, 3x \rangle$

Solution:

(a) Since $3x = 3 \cdot x$, $3x \in \langle 3, x \rangle$. This implies that $J \subset I$. Now $x + 3 \in I$. If $x + 3 \in J$, then $x + 3 = 3xp(x)$ for some $p(x) \in \mathbb{Z}[x]$. Comparing degrees, it must be that $p(x)$ is constant, i.e. $x + 3 = 3xp$ for some $p \in \mathbb{Z}$. By comparing leading coefficients, it follows that $3p = 1$, a contradiction since $p \in \mathbb{Z}$. Therefore, $x + 3 \in I \setminus J$, which implies that $I \not\subset J$.

(b) Clearly, $3 \pm x \in I$ so that $J \subset I$. Now $3 \in I$ and we claim $3 \notin J$. If $3 \in J$, then

$$3 = p(x)(3 - x) + q(x)(3 + x) = 3\big(p(x) + q(x)\big) + x\big(q(x) - p(x)\big)$$

for some $p(x), q(x) \in \mathbb{Z}[x]$. The right hand side of the above equation must be constant. But then $q(x) - p(x) = 0$ so that $p(x) = q(x)$. But then $3 = 3(p(x) + q(x)) =$

$3(p(x) + p(x)) = 6p(x)$. By degree comparison, it must be that $p(x)$ is constant, i.e. $p(x) = p \in \mathbb{Z}$. But then $3 = 6p$, a contradiction since $p \notin \mathbb{Z}$. Therefore, $3 \notin J$ implying that $I \not\subset J$.

(c) Notice that $6 = 2 \cdot 3 \in I$, $9 = 3 \cdot 3 \in I$, $2x = 2 \cdot x \in I$, and $3x = 3 \cdot x \in I$. Therefore, $J \subset I$. Since $3 = 9 - 6 \in J$ and $x = 3x - 2x \in J$, $I \subset J$. Thus, $I = J$.

□

7. Let G be a finitely generated abelian group. Use additive notation so g^m is written as mg. Prove that G is infinite if and only if there exists $g \in G$ such that $mg \neq 0$ for all nonzero $m \in \mathbb{Z}$.

Solution: Suppose that there exists $g \in G$ such that $mg \neq 0$ for all $0 \neq m \in \mathbb{Z}$. If G were finite, then for $n = |G|$, $ng = 0$, a contradiction. Therefore, G is infinite.

Now suppose that G was infinite. By the Fundamental Theorem of Finitely Generated Abelian Groups,

$$G \cong \mathbb{Z}^l \oplus \mathbb{Z}/p_1^{a_1} \oplus \cdots \oplus \mathbb{Z}/p_n^{a_n},$$

for some $l \geq 0$, $a_i \geq 1$, and the p_i (not necessarily distinct) primes. Since G is infinite, it must be that $l \geq 1$. Let $g = (1, 0, \ldots, 0) \in G$ via the isomorphism above. Then $mg = (m, 0, \ldots, 0)$ for $m \in \mathbb{Z}$. If $m \neq 0$, then $mg \neq 0$, as required. □

8. A 15×15 matrix M with complex entries has characteristic polynomial equal to $(x-1)^7(x-2)^8$. Find all possible minimal polynomials for M such that the characteristic and minimal polynomials together completely determine the Jordan canonical form of M up to ordering the blocks. Give the Jordan canonical form for each of these.

Solution: The Jordan canonical form is completely determined by the elementary divisors. If $(x-1)^7$ is the largest power of $(x-1)$ that is an elementary divisor, then no other power of $(x-1)$ can be an elementary divisor. If $(x-1)^6$ is the largest power of $(x-1)$ that is an elementary divisor, then the only other elementary divisor must be $(x-1)$. If $(x-1)^5$ is the largest power of $(x-1)$ that is an elementary divisor, then there are two possibilities: there could be two $(x-1)$ elementary divisors or one $(x-1)^2$ elementary divisor. The remaining possibilities are summarized below:

$(x-1)^4$: Could have $(x-1)^3$, $(x-1)(x-1)^2$ — not unique
$(x-1)^3$: Could have $(x-1)^3(x-1)$, $(x-1)^2(x-1)$ — not unique
$(x-1)^2$: Could have $(x-1)(x-1)(x-1)(x-1)(x-1)$, $(x-1)^2(x-1)^2(x-1)$ — not unique
$(x-1)$: Only possibility is $(x-1)(x-1)(x-1)(x-1)(x-1)(x-1)$

Using a similar reasoning, the powers of $(x-2)$ that uniquely determine the $(x-2)$-elementary divisors are $(x-2)^8$, $(x-2)^7$, and $(x-2)$. This means there are nine minimal polynomials that uniquely determine the Jordan canonical form of M:

1. $m(x) = (x-1)^7(x-2)^8$
2. $m(x) = (x-1)^7(x-2)^7$
3. $m(x) = (x-1)^7(x-2)$
4. $m(x) = (x-1)(x-2)^8$
5. $m(x) = (x-1)(x-2)^7$
6. $m(x) = (x-1)(x-2)$
7. $m(x) = (x-1)^6(x-2)^8$
8. $m(x) = (x-1)^6(x-2)^7$
9. $m(x) = (x-1)^6(x-2)^1$

We now compute the Jordan canonical form in each case.

1. $c(x) = (x-1)^7(x-2)^8 = m(x)$. The two elementary divisors of M are $(x-1)^7$ and $(x-2)^8$ so there are two Jordan blocks. The Jordan canonical form of M, up to reordering of blocks, is

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{pmatrix}$$

2. $m(x) = (x-1)^7(x-2)^7$. The elementary divisors of M are $(x-1)^7$, $(x-2)^7$, and $(x-2)$, so there are two Jordan blocks. The Jordan canonical form of M, up to reordering

of blocks, is

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

3. $m(x) = (x-1)^7(x-2)$. The elementary divisors of M are $(x-1)^7$, $(x-2)$ with multiplicity eight. So there are nine Jordan blocks. The Jordan canonical form of M, up to reordering of blocks, is

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

4. $m(x) = (x-1)(x-2)^8$. The elementary divisors of M are $(x-1)$ with multiplicity seven and $(x-2)^8$, so there are eight Jordan blocks. The Jordan canonical form of M,

up to reordering of blocks, is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

5. $m(x) = (x-1)(x-2)^7$. The elementary divisors of M are $(x-1)$ with multiplicity seven, $(x-2)^7$, and $(x-2)$, so there are nine Jordan blocks. The Jordan canonical form of M, up to reordering of blocks, is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

6. $m(x) = (x-1)(x-2)$. The elementary divisors of M are $(x-1)$ with multiplicity seven and $(x-2)$ with multiplicity eight, so the Jordan canonical form of M, up to reordering

of blocks, is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

7. $m(x) = (x-1)^6(x-2)^8$. The elementary divisors of M are $(x-1)$, $(x-1)^6$, and $(x-2)^8$, so the Jordan canonical form, up to reordering of blocks, is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

8. $m(x) = (x-1)^6(x-2)^7$. The elementary divisors of M are $(x-1)$, $(x-1)^6$, $(x-2)$,

and $(x-2)^7$, so the Jordan canonical form, up to reordering of blocks, is

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{pmatrix}$$

9. $m(x) = (x-1)^6(x-2)$. The elementary divisors of M are $(x-1)$, $(x-1)^6$, and $(x-2)$ with multiplicity eight, so the Jordan canonical form, up to reordering of blocks, is

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{pmatrix}$$

□

9. Prove that a field extension is finite if and only if it is both finitely generated and algebraic. Show by example that neither finitely generated no algebraic alone implies finite.

Solution: Suppose that E/F is a finite extension of fields. Then E has finite dimension as an F-vector space. Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis for E as an F-vector space. Then $E = F(b_1, \ldots, b_n)$ so that E is finitely generated. Let $\alpha \in E$. Since E has dimension n as an F-vector space, the set $\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ is linearly dependent over F, i.e. there are $a_0, \ldots, a_n \in F$, not all zero, such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. But then α is a root of the nonzero polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ so that α is algebraic over F. But then all $\alpha \in E$ are algebraic over F so that E/F is algebraic.

Now suppose that E/F is a field extension which is both finitely generated and algebraic. Since E is finitely generated over F, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. Furthermore, each α_i is algebraic over F since the extension E is algebraic over F. For each i, let $a_i = \deg \alpha_i$. Then $[F\colon E] \leq a_1 a_2 \cdots a_n < \infty$, os E/F is a finite extension.

Now the extension $\overline{Q}/\mathbb{Q}$ is algebraic, by definition. To see the extension is infinite, suppose $\overline{Q}/\mathbb{Q}$ were finite and let $n = [\overline{Q}\colon \mathbb{Q}]$. Define $m = n + 1$ and let $\alpha \in \overline{Q}$ by a root of $f(x) = x^m - 2$. By Eisenstein with $p = 2$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ since $f \in \mathbb{Z}[x]$ and $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$. Then f is the minimal polynomial of α in $\mathbb{Q}[t]$. Then $m = \deg f = [\mathbb{Q}(\alpha)\colon \mathbb{Q}] \leq [\overline{Q}\colon \mathbb{Q}] = n = m - 1$, a contradiction. Therefore, algebraic extensions need not be finite.

Now consider the field extension $\mathbb{Q}(\pi)/\mathbb{Q}$. This extension is generated by $\{1, e\}$. If this extension were finite, then e would be algebraic over $\mathbb{Q}$, a contradiction to the fact that e is transcendental. Therefore, finitely generated extensions need not be finite. □

10. Let $F \subsetneq E$ be an extension of fields of characteristic 0. Let L and K be two intermediate fields so that $F \subset K \subset E$ and $F \subset L \subset E$. Assume that $K \cap L = F$ and that K and L are both finite Galois extensions of F. Define KL to be the smallest subfield of E containing $K \cup L$.

(a) Prove that the definition of KL makes sense; that is, prove that there does indeed exists a unique smallest subfield of E containing $K \cup L$.

(b) Prove that KL is a finite Galois extension of F.

Solution:

(a) Define

$$KL = \bigcap_{\substack{K \cup L \subseteq F' \\ F' \text{ field}}} F'.$$

It is clear that $K \cup L \subset KL$ and that if $K \cup L \subset F'$, then $KL \subset F'$. It remains to show that KL is a field. The intersection of commutative rings is a commutative ring (when the intersection makes sense), so it suffices to show that every nonzero element of KL is a unit. Let $x \in KL$ be nonzero. Then $x \in F'$ for all $F' \supset K \cup L$. But then $x^{-1} \in F'$ for all $F' \supset K \cup L$. Therefore, $x^{-1} \in KL$. But then KL is a field.

(b) Since K is a finite extension, $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$, where each α_i has finite degree over F. Similarly, $L = F(\beta_1, \ldots, \beta_m)$ for some $\beta_1, \ldots, \beta_m \in L$, where each β_j has finite degree over F. Then $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ is a field containing $K \cup L$, so $KL \subset F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$. However, any field containing $K \cup L$ must contain each α_i and each β_j, so

$$KL = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

Therefore, KL is a finite extension of F.

Since K is a Galois extension, K is the splitting field of some separable polynomial $f(x) \in F[x]$. Now KL is the splitting field of the polynomial $f(x)g(x)$. Now $f(x)g(x)$ need not be separable. By removing repeated roots, there exist polynomials $\tilde{f}, \tilde{g}$ so that $\tilde{f}\tilde{g}$ has no repeated roots and KL contains all the roots of $\tilde{f}\tilde{g}$. But then KL is the splitting field of a separable polynomial. Therefore, KL is Galois.

□

August 2013

1. Set $\omega = (123\cdots n) \in S_n$, the symmetric group on n letters. Compute:

(a) The size of the conjugacy class containing ω.

(b) The order of the centralizer of ω.

(c) The order of the normalizer of $\langle\omega\rangle$, assuming that $n = p$ is prime.

Solution:

(a) Two elements of S_n are conjugate if and only if they have the same cycle type. Therefore, the size of the conjugacy class of ω is the number of n-cycles in S_n. This is $(n-1)!$.

(b) Suppose $\sigma \in C_{S_n}(\omega)$. Then $\sigma\omega(k) = \omega\sigma(k)$ for all $k \in \{1,\ldots,n\}$. Note that $\omega(k) = k+1 \mod n$, so this implies $\sigma(k+1) = \sigma(k)+1 \mod n$. Then σ is completely determined by $\sigma(1)$. Since there are n choices for $\sigma(1)$, the order of the centralizer of ω is n.

OR

Let S_n act on itself by conjugation. The stabilizer of ω is the centralizer of ω and the orbit of ω is the conjugacy class containing ω. By the Orbit-Stabilizer Theorem and part (a)

$$(n-1)! = [S_n \colon C_{S_n}(\omega)] = \frac{n!}{|C_{S_n}(\omega)|}$$

Therefore, $|C_{S_n}(\omega)| = \frac{n!}{(n-1)!} = n$.

(c) Notice that $\langle\omega\rangle$ is a cyclic group of order p. Let $\mathrm{Inn}(\langle\omega\rangle)$ denote the inner automorphism group of $\langle\omega\rangle$. Then

$$N_{S_n}(\langle\omega\rangle)/C_{S_n}(\langle\omega\rangle) \cong \mathrm{Inn}(\langle\omega\rangle) \cong \mathrm{Inn}(\mathbb{Z}/p\mathbb{Z}),$$

where $N_{S_n}(H)$ denotes the normalizer of H in S_n. Note that $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ via the map $a \mapsto \phi_a$, where $\phi_a(b+p\mathbb{Z}) := ab + p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is abelian, any two elements are conjugate if and only if they are equal. Therefore, if $ab + p\mathbb{Z} = b + p\mathbb{Z}$, then $ab - b \in p\mathbb{Z}$. This implies that $b(a-1) \in p\mathbb{Z}$, so either $b \in p\mathbb{Z}$ or $a-1 \in p\mathbb{Z}$ (this is Euclid's lemma: if $p \mid ab$ then $p \mid a$ or $p \mid b$). Since this must hold for any b, it can be assumed that $b \notin p\mathbb{Z}$. Thus, $a-1 \in p\mathbb{Z}$ and $a \equiv 1 \mod p$. Therefore, $a = 1$ and the only inner automorphism of $\mathbb{Z}/p\mathbb{Z}$ is the identity. Hence, $|\mathrm{Inn}(\mathbb{Z}/p\mathbb{Z})| = 1$ and $|N_{S_n}(\langle\omega\rangle)| = |C_{S_n}(\langle\omega\rangle)| = n$.

□

2. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$.

(a) Prove that G has a unique Sylow-11 subgroup.

(b) Prove that the Sylow-11 subgroup is contained in the center of G.

Solution:

(a) Let n_p denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_{11} \equiv 1$ mod 11 and divides 231. But the only divisor of 231 congruent to 1 mod 11 is 1. Therefore, $n_p = 1$ and the Sylow 11-subgroup of G is unique, hence normal. Note that G cannot be a simple group.

(b) Let S denote the Sylow 11-subgroup of G. Since $|S| = 11$, S is cyclic. By the remarks in (a), S is normal in G. In particular, S is fixed under conjugation by elements of G. Let $\phi_x : S \to S$ be given by $a \mapsto xax^{-1}$. Note that ϕ_x is an automorphism of the cyclic group S for all $x \in G$> For any $x, y \in G$ and $a \in S$,

$$(\phi_x \circ \phi_y)(a) = \phi_x(yay^{-1}) = xyay^{-1}x^{-1} = (xy)a(xy)^{-1} = \phi_{xy}(a).$$

In particular, the function $f : G \to \mathrm{Aut}(S)$ given by $g \mapsto \phi_g$ is a group homomorphism (noting also $1_G \mapsto \phi_{1_G} = 1_S$). But this holds if and only if $x \in C_G(S)$. Since S is cyclic of order 11, we have $S \cong \mathbb{Z}/11\mathbb{Z}$ so that $\mathrm{Aut}(S) \cong (\mathbb{Z}/11\mathbb{Z})^\times$, a group with 10 elements. By the First Isomorphism Theorem, $\frac{231}{|C_G(S)|}$ divides both 231 and 10. Since 231 and 10 are relatively prime, $\frac{231}{|C_G(S)|} = 1$ so $|C_G(S)| = 231$. But then $G = C_G(S)$. Therefore, the elements of S commute with every element of G. Therefore, $S \subseteq Z(G)$.

□

3. Let Q denote the quaternion group of order 8.

(a) Prove that Q is isomorphic to a subgroup of S_8.

(b) Prove that Q is *not* isomorphic to a subgroup of S_n for $n \leq 7$.

(c) Prove that $C_2 \times C_4$ is isomorphic to a subgroup of S_6.

Solution:

(a) Let Q act on itself by left multiplication — defining $g \cdot x = gx$ for all $g, x \in Q$. For each $g \in Q$, there is a permutation $\sigma_g : Q \to Q$ via $x \mapsto gx$. It remains to show that the map $\phi : Q \to S_Q$ given by $g \mapsto \sigma_g$ is an injective group homomorphism. Observe that for any $g, h \in Q$, $\phi(gh) = \sigma_{gh} = \sigma_g \circ \sigma_h$ since

$$\sigma_{gh}(x) = (gh)(x) = g(hx) = g\sigma_h(x) = \sigma_g(\sigma_h(x)).$$

This shows that ϕ is a group homomorphism. To show that ϕ is injective, note that $g \in \ker \phi$ if and only if $gx = x$ for all $x \in G$. In particular, $g(1) = 1$ so that $g = 1$. This implies that ϕ is injective, as required. Since $|Q| = 8$, we must have $S_Q \subset S_8$.

(b) Let $n \leq 7$ and $\phi : Q \to S_n$ be a homomorphism. The claim is that ϕ is not injective. The existence of a homomorphism ϕ is equivalent to the existence of a group action of Q on the set S of n elements. For any orbit $\mathcal{O}_x$ of the group action,

$$7 \geq |\mathcal{O}_x| = [Q \colon Q_x] = \frac{8}{|Q_x|},$$

where Q_x is the stabilizer of x in Q (note that the inequality above makes use of the Orbit-Stabilizer Theorem). This implies that $|Q_x| > 1$. We claim that $-1 \in Q_x$ for all $x \in S$.

It is clear that there is at least one non-identity element in Q_x. Note that

$$i^2 = j^2 = k^2 = (-i)^2 = (-j)^2 = (-k)^2 = -1.$$

If $-1 \in Q_x$, then there is nothing left to prove. If $i \in Q_x$, then $i^2 = -1 \in Q_x$ since Q_x is a group. Mutatis mutandis, if any of $j, k, -i, -j, -k$ are in Q_x, then $-1 \in Q_x$ since Q_x is closed under multiplication. Therefore, $-1 \cdot x = x$ for all $x \in S$; therefore, $-1 \in \ker \phi$ which implies that $\ker \phi \neq \{1\}$. Therefore, ϕ cannot be injective. But then there are no homomorphisms $\phi : Q \to S_n$ for $n \leq 7$ is injective, which implies that Q is not isomorphic to a subgroup of S_n for $n \leq 7$.

(c) Let a be a generator of C_2 and let b be a generator of C_4. Let $\phi((a, 1)) = (1\ 2)$ and $\phi((1, b)) = (3\ 4\ 5\ 6)$. Since $C_2 \times C_4$ is generated by $(a, 1)$ and $(1, b)$, these choices completely define ϕ:

$$\begin{aligned}
\phi((1, b^2)) &= (3\ 4\ 5\ 6)(3\ 4\ 5\ 6) = (3\ 5)(4\ 6) \\
\phi((1, b^3))7 &= (3\ 4\ 5\ 6)(3\ 5)(4\ 6) = (3\ 6\ 5\ 4) \\
\phi((a, b)) &= (1\ 2)(3\ 4\ 5\ 6) \\
\phi((a, b^2)) &= (1\ 2)(3\ 5)(4\ 6) \\
\phi((a, b^3)) &= (1\ 2)(3\ 6\ 5\ 4) \\
\phi((1, 1)) &= 1
\end{aligned}$$

It is clear that $\phi : C_2 \times C_4 \to S_6$ is an injective group homomorphism.

□

4. Prove that the following conditions on an $n \times n$ real matrix A are equivalent:

(i) $\|AX\| = \|X\|$ for all $X \in \mathbb{R}^n$, where $\|\cdot\|$ is the usual Euclidean norm

(ii) $AX \cdot AY = X \cdot Y$ for all $X, Y \in \mathbb{R}^n$

(iii) $A^T A = I$

Solution:
(i)⇒(ii): If $\|AX\| = \|X\|$ then clearly $\|AX\|^2 = \|X\|^2$. Let $X, Y \in \mathbb{R}^n$. We compute $\langle A(X+Y), A(X+Y)\rangle$ in two different ways:

$$\begin{aligned}\langle A(X+Y), A(X+Y)\rangle &= \langle X+Y, X+Y\rangle = \langle X, X\rangle + 2\langle X, Y\rangle + \langle Y, Y\rangle \\ \langle A(X+Y), A(X+Y)\rangle &= \langle AX+AY, AX+AY\rangle = \langle AX, AX\rangle + 2\langle AX, AY\rangle + \langle AY, AY\rangle \\ &= \langle X, X\rangle + 2\langle AX, AY\rangle + \langle Y, Y\rangle\end{aligned}$$

Therefore for any $X, Y \in \mathbb{R}^n$,

$$\langle X, X\rangle + 2\langle X, Y\rangle + \langle Y, Y\rangle = \langle X, X\rangle + 2\langle AX, AY\rangle + \langle Y, Y\rangle,$$

which implies that $\langle AX, AY\rangle = \langle X, Y\rangle$.

(ii)⇒(iii): Write $A^T A = (a_{ij})$. Then $\langle Ae_i, Ae_j\rangle = e_i^T A^T A e_j = a_{ij}$. On the other hand, $\langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle$, so

$$a_{ij} = \langle e_i, e_j\rangle = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Therefore, $A^T A = I$.

(iii)⇒(i): Suppose $A^T A = I$. Then for any $X \in \mathbb{R}^n$,

$$\|AX\|^2 = \langle AX, AX\rangle = (AX)^T(AX) = X^T A^T A X = X^T X = \langle X, X\rangle = \|X\|^2.$$

Thus, $\|AX\| = \|X\|$. □

5. Let V be a Hermitian space (a finite-dimensional complex vector space carrying a positive definite Hermitian form). Let $T : V \to V$ be a linear operator with adjoint T^*. Prove that $\ker T = (\operatorname{im} T^*)^\perp$.

Solution: Let $x \in \ker T$ so that $Tx = 0$ which implies that $\langle y, Tx\rangle = 0$ for all $y \in V$. But then $\langle T^* y, x\rangle = 0$ for all $y \in V$. Thus, $x \in (\mathrm{Im} T^*)^\perp$. But then $\ker T \subset (\mathrm{Im} T^*)^\perp$.

If $y \in (\text{Im}T^*)^\perp$, then $\langle T^*x, y\rangle = 0$ for all $x \in V$. Take $x = Ty$, then $\langle T^*Ty, y\rangle = 0$, which implies that $\langle Ty, Ty\rangle = 0$. Since the Hermitian form is positive-definite, this implies that $Ty = 0$. Thus, $y \in \ker T$ and $\ker T = (\text{Im}T^*)^\perp$. □

6. Let R be a nonzero commutative ring with identity and let F be a finitely generated R-module.

(a) Give the definition of when F is a free R-module

(b) Suppose that every nonzero ideal I of R is a finitely generated free R-module. Prove that R is a PID.

Solution:

(a) F is a free R-module if there exists a subset $\mathcal{B} \subset F$ such that every element of F can be written uniquely in the form $r_1x_2 + \cdots + r_nx_n$ for some $r_i \in R$ and $x_i \in \mathcal{B}$.

(b) There are two things to show: R is an integral domain and every ideal of R is principal. Let I be a nonzero ideal of R. By hypothesis, I has a basis $\mathcal{B}$. We claim $|\mathcal{B}| = 1$. Suppose $|\mathcal{B}| > 1$ and let $x, y \in \mathcal{B}$ be distinct (taking note that x, y are certainly nonzero). Then $0 = 0x + 0y = (-y)x + (x)y$ are two unique ways of writing 0, which is certainly in every ideal generated by any basis $\mathcal{B}$, contradicting the fact that $\mathcal{B}$ generates a free R-module. But then $|\mathcal{B}| = 1$. Then every ideal is principal.

Suppose that $0 \neq a$ is a zero divisor in R, i.e. there is a nonzero $b \in R$ such that $ba = 0$. We claim a cannot be contained in a basis for an ideal I of R. Since $0 \in I$ for any ideal I and I is free, if a were a basis element then $0 = 0a = ba$ can be written in two different ways, contradicting the fact that I is free. Now let $I = \langle a\rangle$. Since $a \neq 0$, I is nonzero. By assumption, I has basis $\mathcal{B}$ which by the work above we can write $\mathcal{B} = \{x\}$ for some x. We know that $a \neq x$. Now $\langle x\rangle = I$ so that $\langle x\rangle = \langle a\rangle$. But then $x = ra$ for some $r \in R$. But $xb = (ra)b = r(ab) = 0$, implying that $x \in \mathcal{B}$ is a zero divisor, a contradiction. But then no element of R can be a zero divisor. Therefore, R is an integral domain.

□

7. Denote by $\mathbb{C}[x]$ the ring of polynomials in the variable x with coefficients in the field of complex numbers $\mathbb{C}$.

(a) Describe the maximal ideals of $\mathbb{C}[x]$.

(b) Describe the simple $\mathbb{C}[x]$-modules up to isomorphism. First, give the definition of a simple module.

(c) Let S be an arbitrary simple $\mathbb{C}[x]$-module. What is the dimension as a vector space over $\mathbb{C}$?

(d) Let S be an arbitrary simple $\mathbb{R}[x]$-module. What is the dimension of S as a vector space over $\mathbb{R}$?

(a) Since $\mathbb{C}[x]$ is a PID, every ideal is principal. If $p(x), q(x) \in \mathbb{C}[x]$ and $\langle p(x) \rangle \subset \langle q(x) \rangle$, then $q(x)$ divides $p(x)$ (since $p(x) \in \langle q(x) \rangle$). Note that $\langle p(x) \rangle = \mathbb{C}[x]$ if and only if $p(x)$ is a unit if and only if $p(x)$ is a nonzero constant polynomial. Therefore, the maximal ideals are precisely the ideals of the form $\langle p(x) \rangle$, where $p(x)$ is an irreducible polynomial. Since $\mathbb{C}$ is algebraically closed, every polynomial in $\mathbb{C}[x]$ splits completely. Therefore, the only maximal ideals of $\mathbb{C}[x]$ are $\langle p(x) \rangle$, where $p(x)$ has degree 1.

(b) An R-module M is simple if it contains no proper, nontrivial submodules. Note that if M is a simple $\mathbb{C}[x]$-module, then for any nonzero $m \in M$, the module $\mathbb{C}[x]m$ is a nontrivial submodule of M, so it must equal M. Furthermore, the function $\phi : \mathbb{C}[x] \to \mathbb{C}[x]m$ given by $p(x) \mapsto p(x)m$ is a surjective $\mathbb{C}[x]$-module homomorphism. By the First Isomorphism Theorem, $\mathbb{C}[x]/\ker\phi \cong \mathbb{C}[x]m$. Since $\mathbb{C}[x]m$ is a simple module, it contains no proper, nontrivial submodules. By the Correspondence Theorem, the only submodules of $\mathbb{C}[x]$ containing $\ker\phi$ are $\ker\phi$ and $\mathbb{C}[x]$. In other words, $\ker\phi$ is a maximal submodule of $\mathbb{C}[x]$. But then $\ker\phi$ is a maximal ideal in $\mathbb{C}[x]$.

By part (a), $\ker\phi = \langle p(x) \rangle$, where the degree of $p(x)$ is 1. But $M \cong \mathbb{C}[x]/\langle p(x) \rangle$, where the degree of $p(x)$ is 1. Let α be the unique root of $p(x)$. We claim that $\mathbb{C}[x]/\langle p(x) \rangle$ is isomorphic to $\mathbb{C}$, where scalar multiplication is defined by $f(x) \cdot a = f(\alpha)a$ for all $f(x) \in \mathbb{C}[x]$. There is a homomorphism $\phi : \mathbb{C}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(\alpha)$. This is a surjective homomorphism with kernel $\langle p(x) \rangle$. By the First Isomorphism Theorem, $\mathbb{C}[x]/\langle p(x) \rangle \cong \mathbb{C}$.

(c) By part (b), S is isomorphic to $\mathbb{C}$ as a module over $\mathbb{C}[x]$. The restriction of scalar multiplication to $\mathbb{C}$ is just the usual multiplication of complex numbers. Therefore, the dimension of S as a $\mathbb{C}$ vector space is 1.

(d) Let S be a simple $\mathbb{R}[x]$-module. Then the same argument as above shows that $S \cong \mathbb{R}[x]/\langle p(x) \rangle$, where $p(x)$ is an irreducible polynomial in $\mathbb{R}[x]$. If $p(x)$ has degree 1, then again the same arguments used above implies that S is a one-dimensional $\mathbb{R}$-vector space. If $p(x)$ has degree 2, then as a set

$$\mathbb{R}[x]/\langle p(x) \rangle = \{a + bx + \langle p(x) \rangle : a, b \in \mathbb{R}\}.$$

It is easy to see that this has dimension two as a vector space over $\mathbb{R}$ (for example, a possible basis is $\{1 + \langle p(x) \rangle, x + \langle p(x) \rangle\}$). Any polynomial of degree at least 3 over $\mathbb{R}$ is reducible (every polynomial in $\mathbb{R}[x]$ can be written as the product linear and quadratic polynomials). Therefore, S either has dimension one or two as a vector space over $\mathbb{R}$.

□

8. A square matrix M with complex entries has characteristic polynomial

$$c(x) = (x^2+3)(x^2-4x+5)(x+1)^4$$

Denote by $m(x)$ the minimal polynomial of M.

(a) Is it possible that $m(x) = (x^2+3)(x-2-i)(x+1)^2$?

(b) Suppose $m(x) = (x^2+3)(x^2-4x+5)(x+1)^2$. List all possible Jordan canonical forms for M.

Solution:

(a) Observe $x^2-4x+5 = (x-(2+i))(x-(2-i))$. Recall every divisor of $c(x)$ is also a divisor of $m(x)$. For this choice of $m(x)$, $(x-(2-i))$ is a divisor of $c(x)$ but not a divisor of $m(x)$. Therefore, the given $m(x)$ is impossible.

(b) For the given $m(x)$, there are two possibilities for the invariant factors

$$(x+1), (x+1), (x+3i)(x-3i)(x-(2+i))(x-(2-i))(x+1)^2$$
$$(x+1)^2, (x+3i)(x-3i)(x-(2+i))(x-(2-i))(x+1)^2$$

In the first case, the elementary divisors are $x+1$, $x+1$, $(x+1)^2$, $x+3i$, $x+3i$, $x-3i$, $x-(2+i)$, and $(x-(2-i))$. Then the Jordan canonical form is

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2+i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2-i \end{pmatrix}$$

In the second case, the elementary divisors are $(x+1)^2$, $(x+1)^2$, $x+3i$, $x-3i$, $x-(2+i)$, and $x-(2-i)$. Then the Jordan canonical form is

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2+i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2-i \end{pmatrix}$$

□

9. Let $F \subset E$ be a field extension.

(a) Give the definition of when the extension is finite.

(b) Give the definition of when the extension is algebraic.

(c) Give an example of an algebraic extension that is not finite and prove that it is not finite.

Solution:

(a) A field extension E/F is finite if E, viewed as an F-vector space, is finite dimensional, i.e. $[E\colon F]$ is finite.

(b) An element $a \in E$ is algebraic over F if a is the root of a polynomial in $F[x]$. The extension E/F is algebraic over F is every element of E is algebraic over F.

(c) Let $F = \mathbb{Q}$, $E = \overline{Q}$, the algebraic closure of $\mathbb{Q}$, where we view E as a subfield of $\mathbb{C}$. The field E is algebraic over F by definition. It remains to show that E is not a finite extension. Note that the polynomial $p(x) = x^n - 2$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion with $p = 2$. The polynomial $p(x)$ is thus the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$. Since $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ for all n, it follows that

$$[\overline{\mathbb{Q}}\colon \mathbb{Q}] = [\overline{\mathbb{Q}}\colon \mathbb{Q}(\sqrt[n]{2})]\,[\mathbb{Q}(\sqrt[n]{2})\colon \mathbb{Q}] = [\overline{\mathbb{Q}}\colon \mathbb{Q}(\sqrt[n]{2})]n \geq n$$

for all $n \in \mathbb{N}$. But then $[\overline{\mathbb{Q}}\colon \mathbb{Q}] = \infty$.

□

10. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$.

(a) Compute the degree of the extension.

(b) Compute the group of automorphisms of the extension.

(c) Is this a Galois extension?

Solution:

(a) We claim $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2})/\mathbb{Q}$ is a degree 6 extension since $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$ and $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$.[8] By the Eisenstein criterion with $p = 2$, $p(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$. Obviously, $p(\sqrt[3]{2}) = 0$. Therefore, $p(x)$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. This implies that $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$. Mutatis mutandis, $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 3$.

[8] This holds more generally, if K_1/F is an extension of degree n and K_2/F is an extension of degree m, with $(n, m) = 1$, then K_1K_2/F is an extension of degree nm, where K_1K_2 is the compositum of K_1, K_2.

We claim that $q(x) = x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$. If not, then $q(x)$ splits in $\mathbb{Q}(\sqrt[3]{2})$, which implies that $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$. This implies that $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2})$. Therefore,

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})]$$

which is impossible since the right side is even. Then $q(x)$ is the minimal polynomial for $\sqrt{3}$ over $\mathbb{Q}(\sqrt[3]{2})$. Therefore, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. But then

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

(b) Note that $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subset \mathbb{R}$. Viewed a function on $\mathbb{R}$, $p(x)$ is increasing ($p'(x) = 3x^2 \geq 0$). Therefore, $p(x)$ has a unique real root, namely $\sqrt[3]{2}$. [Alternatively, by Descartes Rule of Signs, $p(x)$ can have at most one real root — one positive root and no negative root — and since $p(\sqrt[3]{2}) = 0$, $\sqrt[3]{2}$ is the unique real root of $p(x)$.] For any $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}))$, the function σ is completely determined by $\sigma(1)$, $\sigma(\sqrt{3})$, and $\sigma(\sqrt[3]{2})$. Since σ is a nonzero homomorphism, $\sigma(1) = 1$. Note that $\sigma(\sqrt{3})^2 = \sigma(3) = 3$ so there are two choices for $\sigma(\sqrt{3})$. Finally, observe that $\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$ so that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. This implies there are only two automorphisms: the identity map and σ given by $\sigma(1) = 1$, $\sigma(\sqrt{3}) = -\sqrt{3}$, and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ and extending by linearity. Therefore, $\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$.

(c) This is not a Galois extension since $|\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})/\mathbb{Q})| = 2 \neq 6 = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}]$.

□

January 2014

1. Let A be a finite multiplicative abelian group. Let $a, b \in A$ and suppose m is the order of a and n is the order of b. Prove the following:

(a) If 1 is the greatest common divisor of m and n, then mn is the order of ab.

(b) There exists an element $c \in A$ whose order is the least common multiple of m and n.

(c) Suppose a is an element of maximal order in A. Then the order of every element of A is a divisor of m.

Solution:

(a) If $a = 1$, then $|ab| = |1b| = |b| = 1 \cdot n$, so the claim holds when $a = 1$. By symmetry, this also holds when $b = 1$. Suppose $a, b \neq 1$. This implies that $m, n > 1$. Since A is an abelian group, it follows that $(xy)^k = x^k y^k$ for any $x, y \in A$ and $k \in \mathbb{Z}$. But then

$$(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1.$$

Now suppose $|ab| = k < mn$. Then k divides mn, say $mn = kl$. Note that $(ab)^k = a^k b^k = 1$ so that $a^k = b^{-k}$. But then $|a^k| = |b^{-k}| = |b^k|$. Now $(a^k)^l = a^{kl} = a^{mn} = 1 = a^{km} = (a^k)^m$ so that $|a^k|$ divides both l and m. Similarly, $|b^k| = |b^{-k}| = |a^k|$ divides both l and n so that $|a^k| = |b^k|$ divides both m and n. This implies $|a^k| = |b^k| = 1$ so $a^k = b^k = 1$. Since $|a| = m$, m divides k. But $|b| = n$ implies n divides k. Hence, $mn = \operatorname{lcm}(m, n)$ divides k, a contradiction. Therefore, $|ab| = mn$.

(b) Note that the least common multiple of m and n is $\frac{mn}{(m,n)}$, where (m, n) is the gcd of m and n. We claim the order of $b^{(m,n)}$ is $\frac{n}{(m,n)}$. Observe

$$\left(b^{(m,n)}\right)^{\frac{n}{(m,n)}} = b^{\frac{n(m,n)}{(m,n)}} = b^n = 1.$$

If $k < \frac{n}{(m,n)}$, then $(m, n)k < n$ which implies $(b^{(m,n)})^k \neq 1$, which proves the claim. Now observe $\frac{n}{(m,n)}$ and m are relatively prime. By part (a), $ab^{(m,n)}$ has order $m\frac{n}{(m,n)} = \frac{mn}{(m,n)}$, which is the least common multiple of m and n.

(c) Suppose $b \in A$ has order n and does not divide m. Then $\operatorname{lcm}(m, n) > m$ and by part (b), there exist $c \in A$ such that the order of c is $\operatorname{lcm}(m, n)$, contradicting the maximality of m. Therefore, the order of every element of A is a divisor of m.

□

2. Prove that a finite subgroup of the multiplicative group formed by the nonzero elements of a field is cyclic.

Solution: Solution: It is clear that $F^\times$ is a finite abelian group. Let C_r denote the cyclic group with r elements. By the Fundamental Theorem of Finitely Generated Abelian Groups,

$$F^\times \cong C_{r_1} \times \cdots \times C_{r_k}$$

for some $k \geq 1$ and $r_1 \mid r_2 \mid \cdots \mid r_k$. We claim that $k = 1$. Suppose to the contrary that $k \geq 2$. Consider the polynomial $p(x) = x^{r_1} - 1$. Any element of $F^\times$ is of the form $(a, 1, 1, \ldots, 1)$ and is clearly a root of $p(x)$. This accounts for r_1 distinct roots of $p(x)$. Since $r_1 \mid r_2$ and C_{r_2} is abelian, C_{r_2} contains a subgroup H or order r_1. Now every element of the form $(1, a, 1, \ldots, 1)$ with $a \in H$ is a root of $p(x)$. This implies that there are at least $2r_1$ roots of $p(x)$, but $p(x)$ has degree r_1, a contradiction. Therefore, $k = 1$ and $F^\times C_{r_1}$. Thus, $F^\times$ is a cyclic group.

OR

Let $q = |F|$ so that $|F^\times| = q - 1$. Let m be the maximal order of the elements of $F^\times$. By Lagrange's Theorem, $m \mid (q-1)$. This implies $m \leq q - 1$. We claim $m = q - 1$ so that we only need show $q - 1 \leq m$. In any finite abelian group, the order of every element divides the maximal order of all the elements. Then every element $x \in F^\times$ satisfies $x^m = 1$. Then every element of $F^\times$ is a root of $x^m - 1$. The number of possible roots of $x^m - 1$ is m so that $q - 1 \leq m$. But then $m = q - 1$. Therefore, some element of $F^\times$ has order $q - 1$. Hence, $F^\times$ is cyclic.

OR

We first prove that if G is a finite group with n elements such that for every divisor d of n, the number of elements dividing d is at most d, then G is cyclic.

Suppose $d \mid n$ and let G_d be the set of elements of G with order d. If $G_d \neq \emptyset$, there is a $y \in G_d$. We have $\langle y \rangle \subseteq \{x \in G \colon x^d = 1\}$. But $\langle y \rangle$ has cardinality d. But then $\langle y \rangle = \{x \in G \colon x^d = 1\}$. Then G_d is the set of generators of $\langle y \rangle$ of order d. Therefore, $\#G_d = \phi(d)$.

We have shown G_d is either empty or possesses cardinality $\phi(d)$ for each $d \mid n$. Then

$$n = \#G = \sum_{d \mid n} \#G_d \leq \sum_{d \mid n} \phi(d) = n$$

Therefore, $\#G_d = \phi(d)$ for each $d \mid n$. In particular, $G_n \neq \emptyset$. But then G is cyclic.

Now in our case we have $G = F^\times$, a finite group. If $|F^\times| = n$ and $d \mid n$ then $x^d = 1$ if and only if $x^d - 1 = 0$ as in the ring. This polynomial can have at most d roots. But then the claim above applies so that $F^\times$ is then a cyclic group.

OR

Suppose that $|F^\times| = n$ and $d \mid n$. Let $\psi(d)$ denote the number of elements of order d in $F^\times$. Suppose there exists an element $x \in F^\times$ of order d. Consider $\langle x \rangle$. Then every element of $\langle x \rangle$ satisfies $y^d = 1$. But the number of solutions of $x^d = 1$ is at most d (since x is a solution if and only if $x^d - 1 = 0$). Then $\langle x \rangle = \langle x \in F^\times : x^d = 1 \}$. But then $\psi(d) = 0$ or $\phi(d)$. But

$$\sum_{d|n} \psi(d) = n = \sum_{d|n} \phi(d)$$

so that $\psi(d) = \phi(d)$ for all $d \mid n$. In particular, $\psi(n) = \phi(d)$, meaning there exists an element of order n in $F^\times$.

OR

Let $G := F^\times$. By the Fundamental Theorem of Finitely Generated Abelian Groups, we have

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$$

where the p_i are primes, not necessarily distinct, and $n_r \geq 1$. Each $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ is a cyclic group of order $p_i^{n_i}$. Let $m = \text{lcm}\{p_1^{n_1}, \ldots, p_r^{n_r}\}$. We know $m \leq p_1^{n_1} \cdots p_r^{n_r}$. If $a_i \in \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, then $a_i^{p_i^{n_i}} = 1$, hence $a_i^m = 1$. But then for all $\alpha \in G$, $\alpha^m = 1$, i.e. every element of G is a root of $x^m = 1$. But G contains $p_1^{n_1} \cdots p_r^{n_r}$ elements while the polynomial $x^m - 1$ has at most m roots in F. Then $m = p_1^{n_1} \cdots p_r^{n_r}$. As the p_i are distinct, the group G is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.

OR

Let $G := F^\times$ and $n = \max\{|y| : y \in G\}$. Let $|G| = N$. Choose $a \in G$ so that $|a| = n$. If we can show that $n = N$, then $|a| = |G|$ which implies $G = \langle a \rangle$ and G is then cyclic. Now $a \in G$ so that $|a| = n \mid N$ and $n \leq N$. We need show $n \geq N$. In any abelian group with elements of finite order r, s, the group contains an element of order $\text{lcm}(r, s)$. Then G contains an element of order $\text{lcm}(|a|, |g|)$ so $\text{lcm}(n, |g|) \leq n$. But then $|g| \mid n$ and then $g^n = 1$ for every $g \in G$. Then $x - g$ is a factor of the polynomial $x^n - 1$ for every $g \in G$. Therefore, $\prod_{g \in G}(x - g)$ divides $x^n - 1$. However, $\prod_{g \in G}(x - g)$ has degree N so that $N \leq n$. □

3. For a positive integer n, denote by Z_n, the ring of residue classes module n and by $Z_n^\times$ the multiplicative group of units of Z_n.

(a) Prove that the group of automorphisms of a cyclic group of order n is isomorphic to $Z_n^\times$.

(b) Determine (up to isomorphism as in the Fundamental Theorem of Finitely Generated Abelian Groups) the groups of automorphisms of the following groups

(i) A cyclic group of order 6.

(ii) A cyclic group of order 12.

(iii) A cyclic group of order 29.

Solution:

(a) Note that any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, viewed as an abelian group. Therefore, it suffices to consider automorphisms of $\mathbb{Z}/n\mathbb{Z}$. Any homomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is completely determined by $\phi(1+n\mathbb{Z})$ since $\phi(k+n\mathbb{Z}) = k\phi(1+n\mathbb{Z})$. Therefore for any $k \in \{0,1,\ldots,n-1\}$, define a homomorphism $\phi_k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $a+n\mathbb{Z} \mapsto a(k+n\mathbb{Z}) = ka+n\mathbb{Z}$.

We need show that ϕ_k is well defined: if $a+n\mathbb{Z} = b+n\mathbb{Z}$, then $a-b \in n\mathbb{Z}$ which implies $k(a-b) = ka-kb \in n\mathbb{Z}$ and thus $ka+n\mathbb{Z} = kb+n\mathbb{Z}$. Therefore, ϕ_k is well defined for $k \in \{0,\ldots,n-1\}$. It is clear that ϕ_k is a group homomorphism. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, ϕ_k is an automorphism if and only if ϕ_k is injective (recall a map between finite sets is injective if and only if it is surjective). We claim ϕ_k is injective if and only if $k+n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. If ϕ_k is injective, it is surjective (hence an automorphism). Then there exists $a+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ such that $\phi(a+n\mathbb{Z}) = 1+n\mathbb{Z}$. Now $\phi(a+n\mathbb{Z}) = ka+n\mathbb{Z} = (k+n\mathbb{Z})(a+n\mathbb{Z})$ so that $(k+n\mathbb{Z})(a+n\mathbb{Z}) = 1+n\mathbb{Z}$. Therefore, $k+n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Now if $k+n\mathbb{Z}$ is a unit, to show ϕ_k is an automorphism, it suffices to show that ϕ_k is injective. Suppose $\phi_k(a+n\mathbb{Z}) = 0$ then $(k+n\mathbb{Z})(a+n\mathbb{Z}) = ka+n\mathbb{Z} = 0+n\mathbb{Z}$. Therefore, $a+n\mathbb{Z} = n\mathbb{Z}$ since a unit is never a zero divisor. But then $\ker\phi_k = \{0+n\mathbb{Z}\}$ so that ϕ_k is injective.

Let $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ denote the group of automorphisms of $\mathbb{Z}/n\mathbb{Z}$ and define $\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ by $k+n\mathbb{Z} \mapsto \phi_k$. By the work above, ψ is a well defined surjective function. We need show that ψ is an injective homomorphism. To show it is a map, let $a+n\mathbb{Z}, b+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then

$$\psi((a+n\mathbb{Z})(b+n\mathbb{Z})) = \psi(ab+n\mathbb{Z}) = \phi_{ab} = \phi_a \circ \phi_b = \psi(a+n\mathbb{Z}) \circ \psi(b+n\mathbb{Z}),$$

since $\phi_{ab}(k+n\mathbb{Z}) = abk+n\mathbb{Z} = a(bk)+n\mathbb{Z} = (\phi_a \circ \phi_b)(k+n\mathbb{Z})$ for all $k+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. Now if $\psi(a+n\mathbb{Z}) = 1+n\mathbb{Z}$, then $ak+n\mathbb{Z} = k+n\mathbb{Z}$ for all $k+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. In particular, this is true for $k=1$, which implies that $a+n\mathbb{Z} = 1+n\mathbb{Z}$. Therefore, $\ker\psi = \{1+n\mathbb{Z}\}$. Therefore, ψ is injective and is then an isomorphism of groups.

(b) (i) By part (a), the group of automorphisms of a cyclic group of order 6 is isomorphic to $(\mathbb{Z}/6\mathbb{Z})^\times = \{1+6\mathbb{Z}, 5+6\mathbb{Z}\}$. This is a group of order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(ii) By part (a), the group of automorphisms of a cyclic group of order 12 is isomorphic to $(\mathbb{Z}/12\mathbb{Z})^\times = \{1+12\mathbb{Z}, 5+12\mathbb{Z}, 7+12\mathbb{Z}, 11+12\mathbb{Z}\}$. This is the Klein 4-group, i.e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iii) By part (a), the group of automorphisms of a cyclic group of order 29 is isomorphic to $(\mathbb{Z}/29\mathbb{Z})^\times$. Because 29 is prime, the unit group of $\mathbb{Z}/29\mathbb{Z}$ is all nonzero elements of $\mathbb{Z}/29\mathbb{Z}$, which is a group of order 28. Therefore, $(\mathbb{Z}/29\mathbb{Z})^\times \cong \mathbb{Z}/28\mathbb{Z}$.

□

4. Let p be the smallest prime divisor of the order of a finite group G. If H is a subgroup of G of index p, prove that H is a normal subgroup.

Solution: Define an action of G on the set of left cosets of H in G by $g \cdot aH = gaH$ for all $g, a \in G$. Since $[G\colon H] = p$, there are p left cosets of H in G so that the above action of G induces a group homomorphism $\phi : G \to S_p$. We claim H is the kernel of ϕ. Note that $\phi(g) = \sigma_g$, where $\sigma_g(aH) = gaH$. If $\sigma_g = 1$, then $\sigma_g(1H) = gH = H$, which implies $g \in H$. Therefore, $\ker\phi \subset H$.

Then using the First Isomorphism Theorem, $p = [G\colon H] = \frac{|G|}{|H|} \leq \frac{|G|}{|\ker\phi|} = |\operatorname{im}\phi|$. In particular, $\frac{|G|}{|\ker\phi|}$ divides $|S_p| = p!$. Factoring $\frac{|G|}{|\ker\phi|}$ into prime numbers, it follows that $\frac{|G|}{|\ker\phi|} = p_1 \cdots p_l$, where $p_i \leq p$. However, each p_i divides $|G|$ and each $p_i \leq p$. This implies $i = 1$ and $p_1 = p$. Therefore, $\frac{|G|}{|\ker\phi|} = p$, as claimed.

Now since G is finite and $[G\colon H] = [G\colon \ker\phi]$, it follows that $|H| = |\ker\phi|$. Because $\ker\phi \subset H$ and H is finite, it must be that $H = \ker\phi$. Thus, H is the kernel of a group homomorphism, implying that H is a normal subgroup of G. □

5. Denote by $\mathbb{R}^n$ the n-dimensional Euclidean space with the usual dot product. Prove that if the columns of an $n \times n$ real matrix A form an orthonormal basis for $\mathbb{R}^n$, then the rows do too.

Solution: Notice that the columns of A are linearly independent since they are orthogonal. Thus, A is invertible. Let x_i denote the i$^{\text{th}}$ column of A. Since $\{x_i\colon i = 1, \ldots, n\}$ is an orthogonal basis for $\mathbb{R}^n$,

$$\langle x_i, x_j \rangle = x_i^T x_j = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Therefore, this is equivalent to the assertion that $A^T A = I$. Multiplying both sides of this equality on the right side by A^{-1}, it follows that $A^{-1} = A^T$. Therefore, $AA^T = I$. Denoting the columns of A^T by y_i, the (i, j) entry of I is the dot product, $\langle y_i, y_j \rangle = y_i^T y_j$. Therefore,

the columns of A^T are orthogonal, implying that the rows of A are orthogonal. Since there are n orthogonal rows of A and the dimension of $\mathbb{R}^n$ is n, the rows of A form an orthonormal basis for $\mathbb{R}^n$. □

6. Find an ideal $I \subset \mathbb{R}[x,y]$ such that

$$\frac{\mathbb{R}[x,y]}{I} \cong \frac{\mathbb{C}[z]}{(z^2)}$$

Write down the isomorphism explicitly and prove it is an isomorphism.

Solution: Let $I = (x^2, y^2+1)$.[9] Note throughout the proof for simplicity, we will ignore 'bars', e.g. we say $1 \in \mathbb{R}[x,y]/I$ instead of $\overline{1}$. In the quotient, $\mathbb{R}[x,y]/I$, $y^2+1=0$ so that $y^2=-1$ (neglecting this is in the quotient). This also implies the largest power of y with a nonzero coefficient in the quotient $\mathbb{R}[x,y]/I$ is 1. Define

$$\phi : \mathbb{R}[x,y]/I \to \mathbb{C}[z]/(z^2)$$

by $\phi(p(x,y)+I) = p(z,i)+(z^2)$. We claim that ϕ is a ring isomorphism. We need check that ϕ is a ring homomorphism: for $p,q \in \mathbb{R}[x]$,

$$\begin{aligned}\phi\big((p(x,y)+I)+(q(x,y)+I)\big) &= \phi\big((p(x,y)+q(x,y))+I\big)\\ &= (p(z,i)+q(z,i))+(z^2)\\ &= (p(z,i)+(z^2))+(q(z,i)+(z^2))\\ &= \phi(p(x,y)+I)+\phi(q(x,y)+I)\end{aligned}$$

and

$$\phi\big((p(x,y)+I)(q(x,y)+I)\big) = \phi(p(x,y)q(x,y)+I).$$

Now write $p(x,y) = a_0+a_1x+a_2y+a_3xy$ and $q(x,y) = b_0+b_1x+b_2y+b_3xy$, where $a_i, b_i \in \mathbb{R}$ (noting in the quotient any higher powers of x,y disappear so we need only consider terms of at most degree 2). Then

$$\begin{aligned}p(x,y)q(x,y) = a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_2b_0)y+a_1b_1x^2+a_2b_2y^2\\ +(a_0b_3+a_1b_2+a_2b_1+a_3b_0)xy+(a_1b_3+a_3b_1)x^2y+(a_2b_3+a_3b_2)xy^2+a_3b_3x^2y^2\end{aligned}$$

Therefore, noting $y^2=-1$ and the only power of x which survives in the quotient is x,

$$\begin{aligned}p(x,y)q(x,y)+I = (a_0b_0-a_2b_2)+(a_0b_1+a_1b_0-a_2b_3+a_3b_2)x\\ +(a_0b_2+a_2b_0)y+(a_0b_3+a_1b_2+a_2b_1+a_3b_0)xy+I.\end{aligned}$$

[9] The idea is that $\mathbb{R}[y]/(y^2+1) \cong \mathbb{C}$ so $\mathbb{R}[x,y]/(y^2+1) \cong \mathbb{C}[x]$ and then we simply map tread x as z.

But then

$$\phi(p(x,y)q(x,y)+I) = (a_0b_0+a_2b_2)+i(a_0b_2+a_2b_0)+ \\ z\big[(a_0b_1+a_1b_0-a_2b_3-a_3b_2)+i(a_0b_3+a_1b_2+a_2b_1+a_3b_0)\big]+(z^2).$$

Now observe that

$$\phi(p(x,y)+I)\phi(q(x,y)+I) = (a_0+a_1z+a_2i+a_3iz)(b_0+b_1z+b_2i+b_3iz) \\ = (a_0b_0-2_ab_2)+i(a_0b_2+a_2b_0)+ \\ z\big[a_0b_1+b_0a_1-a_2b_3-a_3b_2+i(a_2b_1+b_3a_0+a_3b_0+a_1b_2)\big]+(z^2).$$

It remains to show that ϕ is bijective. Suppose $p(x,y)+I \in \ker\phi$ (written as above). Then $p(z,i)+(z^2) = (z^2)$, i.e. z^2 divides $p(z,i)$. But then either x^2 divides $p(x,y)$, i.e. $p(z,i) \neq 0$, or y^2+1 divides $p(x,y)$, i.e. $p(z,i) = 0$. In either case, $p(x,y) \in (x^2, y^2+1)$, which implies that $\ker\phi = \{0+(x^2,y^2+1)\}$. To show that ϕ is surjective, let $p(z)+(z^2) \in \mathbb{C}[z]/(z^2)$. Write $p(z) = w_0+w_1z$ for some $w_0, w_1 \in \mathbb{C}$. Write $w_0 = a_0+ib_0$, $w_1 = a_1+ib_1$ for $a_0, b_0, a_1, b_1 \in \mathbb{R}$. Define $q(x,y) = a_0+b_0y+a_1x+b_1xy$. Then

$$\phi(q(x,y)+I) = q(z,i)+(z^2) = a_0+b_0i+a_1z+b_1iz+(z^2) = w_0+w_1z+(z^2).$$

Therefore, ϕ is surjective. But then ϕ is an isomorphism of rings. □

7. Recall that an abelian group is a $\mathbb{Z}$-module in a natural way.

(a) Let $\mathbb{Q}$ be the group of rational numbers under addition. Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

(b) Let $\mathbb{Q}^*$ be the group of nonzero rational numbers under multiplication. Prove that Q^* is not a free $\mathbb{Z}$-module.

(c) Let $\mathbb{Q}^+$ be the group of nonzero positive rational numbers under multiplication. Prove that $\mathbb{Q}^+$ is a free $\mathbb{Z}$-module of infinite rank.

Solution:

(a) Suppose that $\mathbb{Q}$ were a free $\mathbb{Z}$-module. Let $\mathcal{B}$ be a basis for $\mathbb{Q}$ over $\mathbb{Z}$. If $|\mathcal{B}| > 1$, let $x, y \in \mathcal{B}$ be distinct. Then $x = p_1/q_1$ and $y = p_2/q_2$ for some $p_1, p_2, q_1, q_2 \in \mathbb{Z}$ with $q_1, q_2 > 0$. This implies that

$$(q_1p_2)\frac{p_1}{q_1}+(-q_2p_1)\frac{p_2}{q_2} = p_1p_2-p_1p_2 = 0 = 0x+0y.$$

But then 0 can be written as a linear combination in two distinct ways, contradicting the fact that $\mathcal{B}$ is a basis.

If $|\mathcal{B}| = 1$, then $\mathcal{B} = \{p/q\}$ for some $p \in \mathbb{Z}$, $q \in \mathbb{N}$. Since $\mathcal{B}$ is a basis for $\mathbb{Q}$, there exists $m \in \mathbb{Z}$ such that $m \cdot \frac{p}{q} = \frac{1}{2q}$, then $mp = \frac{1}{2}$. But this contradicts the fact that $p, m \in \mathbb{Z}$. Therefore, $\mathcal{B}$ is not a basis for $\mathbb{Q}$, proving that $\mathbb{Q}$ does not have a basis as a $\mathbb{Z}$-module. Thus, $\mathbb{Q}$ cannot be a free $\mathbb{Z}$-module.

(b) Suppose that $\mathbb{Q}^\times$ were a free $\mathbb{Z}$-module and $\mathcal{B}$ were a basis for $\mathbb{Q}^\times$. Notice that $-1 \in \mathbb{Q}^\times$, implying that $-1 = a_1^{k_1} \cdots a_n^{k_n}$, where $a_i \in \mathcal{B}$ and $k_i \in \mathbb{Z}$ for all i. Without loss of generality, assume $k_i \neq 0$. Therefore,

$$1 = (-1)^2 = a_1^{2k_1} \cdots a_n^{2k_n} = a_1^0.$$

This implies that the representation of 1 as a linear combination of basis elements is not unique, contradicting the fact that $\mathcal{B}$ is a basis. But then $\mathbb{Q}^\times$ is not a free $\mathbb{Z}$-module.

(c) Let $\mathcal{B}$ denote the set of all positive prime integers. We claim that $\mathcal{B}$ is a basis for $\mathbb{Q}^+$ as a $\mathbb{Z}$-module. Since there are infinitely many primes, $\mathcal{B}$ is infinite and proving $\mathcal{B}$ is a basis proves the result. For any rational $x > 0$, there exist $p, q \in \mathbb{N}$ such that $x = p/q$ and $(p, q) = 1$. Write $p = p_1^{k_1} \cdots p_n^{k_n}$ and $q = q_1^{l_1} \cdots q_m^{l_m}$, where the p_i and q_i are distinct primes and $k_i, l_i \geq 1$ (these factorizations are unique). Since $(p, q) = 1$, the factorizations share no common primes. Therefore,

$$x = p_1^{k_1} \cdots p_n^{k_n} q_1^{-l_1} \cdots q_m^{-l_m}$$

is a linear combination of basis elements. Since this expression is unique up to reordering, $\mathcal{B}$ is a basis for $\mathbb{Q}^+$.

□

8. Let A be a $n \times n$ matrix over the complex numbers and let A^T be its transpose.

(a) Prove that A and A^T have the same Jordan canonical form.

(b) Explain why (a) implies that A and A^T are similar to each other.

Solution:

(a) Let J denote the Jordan canonical form of A. Since the Jordan canonical form of A is unique, up to reordering of blocks, it suffices to prove that A^T is similar to J. Now since A is similar to J, there exists a matrix P such that $PAP^{-1} = J$. Taking transposes, $(P^{-1})^T A^T P^T = J^T$. Observe that $(P^{-1})^T = (P^T)^{-1}$ since $PP^{-1} = I$ implies $(P^{-1})^T P^T = I^T = I$.

This implies that A^T is similar to J^T. It remains to show that J^T is similar to J. Conjugating J by a block diagonal matrix, where the size and order of the blocks are the same as the size and order of the Jordan blocks of J, with each block of the form

$$\begin{pmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

we see that J and J^T are conjugate.

(b) Any matrix is similar to its Jordan canonical form. If J is the Jordan canonical form of A (choosing an ordering of blocks), then part (a) implies that A and A^T are both similar to J. Since similarity of matrices is an equivalence relation, this implies that A and A^T are similar.

□

9. Let $F \subset K$ be an extension of fields. Assume that we have an infinitely long strictly increasing sequence of fields $F \subsetneq F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq \cdots$ with all $F_i \subset K$.

(a) Prove that $F \subset K$ is not a finite field extension.

(b) Show by example that $F \subset K$ could be an algebraic field extension.

Solution:

(a) We need show $[K\colon F] = \infty$. We claim $[F_n\colon F] \geq 2^n$ for every $n \in \mathbb{N}$. For $n = 1$ and since $F_1 \neq F$, $[F_1\colon F] \geq 2$. Suppose the claim holds for n. Then

$$[F_{n+1}\colon F] = [F_{n+1}\colon F_n]\,[F_n\colon F] \geq 2 \cdot 2^n = 2^{n+1}.$$

The claim then follows by induction. Now for any $n \in \mathbb{N}$,

$$[K\colon F] = [K\colon F_n][F_n\colon F] \geq [K\colon F_n]2^n \geq 2^n,$$

which implies that $[K\colon F] = \infty$.

(b) Consider $F = \mathbb{Q}$, $K = \overline{\mathbb{Q}}$ (viewed as a subfield of $\mathbb{C}$). Since K is the algebraic closure of F, K is algebraic over F. Let $F_1 = \mathbb{Q}(\sqrt{2})$ and $F_n = F_{n-1}(\sqrt[n]{2})$. With this choice of F_i, F and K satisfy $F \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$ with $F_i \subset K$, but K is algebraic over F (as noted above).

□

10. Let $F \subset K$ and $F \subset L$ be two field extensions. Let $g : K \to L$ be an isomorphism of fields such that $g(f) = f$ for all $f \in F$. Prove that g induces an isomorphism of Galois groups $\tilde{g} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$.

Solution: For $\sigma \in \mathrm{Gal}(K/F)$, define $\tilde{g}(\sigma) = g\sigma g^{-1}$. We need check that $\tilde{g}(\sigma) \in \mathrm{Gal}(L/F)$. It is clear that $g\sigma g^{-1} : L \to L$ is an isomorphism as it is the composition of isomorphisms. Furthermore since $g(f) = g^{-1}(f) = \sigma(f)$ for all $f \in F$, $(g\sigma g^{-1})(f) = f$ for all $f \in F$. Therefore, $g\sigma g^{-1} \in \mathrm{Gal}(L/F)$.

Let $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$. Then

$$\tilde{g}(\sigma_1)\tilde{g}(\sigma_2) = g\sigma_1 g^{-1} g\sigma_2 g^{-1} = g\sigma_1\sigma_2 g^{-1} = \tilde{g}(\sigma_1\sigma_2).$$

This shows that $\tilde{g}$ is a group homomorphism. Let 1_K and 1_L denote the identity functions on K and L, respectively. If $\sigma \in \ker \tilde{g}$, then $g\sigma g^{-1} = 1_L$, which implies that $g\sigma = g$. Multiply both sides on the left by g^{-1}, we obtain $\sigma = 1_K$. Thus, $\ker \tilde{g} = \{1_K\}$, which implies that $\tilde{g}$ is injective.

Now we need only show $\tilde{g}$ is surjective. Let $\sigma \in \mathrm{Gal}(L/F)$. Define $\sigma' = g^{-1}\sigma g$. It is clear that $\sigma' \in \mathrm{Gal}(K/F)$. Furthermore,

$$\tilde{g}(\sigma') = g\sigma' g^{-1} = g(g^{-1}\sigma g)g^{-1} = (gg^{-1})\sigma(gg^{-1}) = \sigma.$$

Therefore, $\tilde{g}$ is surjective. But then $\tilde{g}$ is an isomorphism of Galois groups. □

August 2014

1. Let K be a field. A square matrix A over K is called *unit upper triangular* if it has 1s on the diagonal and 0s below the diagonal; that is, $A = [a_{ij}]$, where

$$a_{ij} = \begin{cases} 1, & i = j \\ 0, & i > j \end{cases}$$

The *unipotent group* $U_n(K)$ is the set of all $n \times n$ unit upper triangular matrices over K with the usual matrix multiplication.

(a) Prove that $\mathrm{U}_n(K)$ is a subgroup of $\mathrm{GL}_n(K)$.

(b) If $K = \mathbb{F}_p$ is a field of order $q = p^n$, where p is a prime number, show that $\mathrm{U}_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$.

Solution:

(a) It is clear that $U_n(K)$ is a subset of $\mathrm{GL}_n(K)$ as $\det A = 1$ for $A \in U_n(K)$ as the determinant of a triangular matrix is the product of its diagonal elements. Let $A = [a_{ij}]$ and $B = [b_{ij}]$, where $A, B \in U_n(K)$. Then $AB_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. But $a_{ij}, b_{ij} = 0$ for $i > j$. Then it is clear from the matrix product that $AB \in U_n(K)$. So $U_n(K)$ is closed under products. It is also clear that $AB_{ij} = 1$ from the definition of a matrix product. Therefore, $U_n(K)$ is closed under matrix products. It is tedious to show that if $AB = I$ and A is upper triangular, then B is upper triangular. But it is nevertheless true. This shows that $U_n(K)$ is closed under inverses. Therefore, $U_n(K) \leq \mathrm{GL}_n(K)$.

(b)

2. Let G be a finite group with center Z. Let p be a prime number. Prove the following statements:

(a) If $|G| = p^e$ for some $e \geq 1$, then Z is nontrivial.

(b) If G is nonabelian and $|G| = p^e m$ for some $e \geq 1$ and some m with $p > m$, then G is not a simple group. (You will want to use the previous part.)

Solution:

(a) Let $|G| = p^n$ for some $n \geq 0$. If $n = 0$, the result is trivial. If $p = 1$, then $G \cong \mathbb{Z}/p\mathbb{Z}$, which is abelian. So suppose $p > 1$. The Class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G \colon C_G(a_i)]$$

where the $Z(G)$ is the center of G, $C_G(x)$ is the centralizer of x in G, and the summation is over $a_1, \ldots, a_r$ representatives for the distinct conjugacy classes of G. Note that each summand of the class equation is a divisor of $|G|$ and $[G\colon C_G(a_i)] > 1$ since $a_i \notin Z(G)$. The Class equation for G can be rewritten as

$$|Z(G)| = |G| - \sum_{i=1}^{r} [G\colon C_G(a_i)].$$

Each term on the right hand side is a divisor of $|G| = p^n$. Furthermore, each term on the right hand side is strictly larger than 1. Therefore, p divides every term on the right hand side, which implies that p divides the left hand side. Thus, p divides $|Z(G)|$ so that $|Z(G)| \neq 1$.

(b) If $m = 1$, then G is a p-group so that by (a), G cannot be simple. Assume then that $1 < m < p$. In particular, $(p, m) = 1$. Let n_p denote the number of Sylow p-subgroups of G. By Sylow's Theorem, $n_p \equiv 1 \mod p$ and $n_p \mid m$, i.e. $n_p = 1 + kp$ for some k and $(1 + kp) \mid m$. As $p > m$, $1 + kp > m$ if $k > 1$, a contradiction. Then $k = 0$ so that $n_p = 1$. Therefore, the Sylow p-subgroup is unique, hence normal. But then G cannot be simple.

□

3. Let T be a self-adjoint (that is Hermitian) linear operator on a finite-dimensional inner product space V and assume that $T^n = \mathrm{id}_V$ for some $n \geq 1$. Prove that $T^2 = \mathrm{id}_V$.

Solution: Since T is a Hermitian (or self-adjoint) linear operator on V, we can only interpret V as being a hermitian inner product product space. Then by the Spectral Theorem, there is an orthonormal basis of V consisting of eigenvectors of T. As V is finite dimensional, there are finitely many such eigenvectors, call these $v_1, v_2, \cdots, v_n$ with eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$, respectively. We know also by the Spectral Theorem, $\lambda_i \in \mathbb{R}$. It suffices to show that T^2 fixes v_i for $i = 1, 2, \cdots, n$. By induction, we know $T^n(v_i) = \lambda_i^n v_i$. But by assumption, $T^n(v_i) = v_i$. Therefore, $\lambda_i^n v_i = v_i$ so that $\lambda_i^n = 1$ implying $\lambda_i = \pm 1$, depending on n. However, then $T^2(v_i) = \lambda_i^2 v_i = v_i$. □

4.

(a) Let V be a finite dimensional real vector space with nondegenerate bilinear form $\langle\ ,\ \rangle$. Let $T : V \to V$ be a linear operator. Prove that there exists an adjoint for T; that is, a linear operator $T^* : T \to V$ such that $\langle v, T^* w\rangle = \langle Tv, w\rangle$ for all $v, w \in V$. You may assume that V has an orthonormal basis $\mathcal{B}$.

(b) Let V be the real vector space of all polynomial functions $f(t)$ with inner product $\langle f, g\rangle = \int_0^1 f(t)g(t)\, dt$. Let $D : V \to V$ be the derivative $D(f) = f'$. Prove that there

does not exist an adjoint D^* for D. (Hint: consider $D^*(1)$.)

Solution:

(a) Let $B = \{v_1, v_2, \cdots, v_n\}$ be a orthonormal basis for V. Given a linear operator T on V, there is a unique $u \in V$ such that $T(v) = \langle u, v\rangle$ for all $v \in V$. To see this, let $u = \sum_{i=1}^{n} (T(v_i))^* v_i$. Define T_u on V by $T_u(v) = \langle u, v\rangle$. Then

$$T_u(v_i) = \langle u, v_j\rangle = \langle \sum_{i=1}^{n} (T(v_i))^* v_i, v_j\rangle = \sum_{i=1}^{n} T(v_i)\langle v_j, v_i\rangle = T(v_i)$$

As T and T_u agree on the basis for V, $T(v) = T_u(v)$ for all $v \in V$. To see uniqueness, suppose u, u' are two such vectors in V with the above property. Then $T_u(v) = \langle u, v\rangle$ and $T_{u'}(v) = \langle u', v\rangle$ so that $\langle u - u', v\rangle = 0$. As v was arbitrary, choose $v = u - u'$. Then $\langle u - u', u - u'\rangle = 0$, as this form is positive definite, we know $u - u' = 0$ so that $u = u'$.

Now given T, define L_u by $L_u(v) = \langle u, Tv\rangle$. This function is clearly linear so that by the previous part, we know that there is a unique $u' \in V$ such that $L_u(v) = \langle u', v\rangle$. But then $\langle u, Tv\rangle = \langle u', v\rangle$. Define $T^* : V \to V$ by $T*(u) = u'$. The mapping is unique as u' is unique for any given u. So that if $T^{*'}u = u' = T^*u$, then $(T^{*'} - T)(u) = 0$ so that $T^{*'} = T^*$. That is, we define T^* as $\langle T^*u, v\rangle = \langle u, Tv\rangle$. Then T^* has the desired property. We need only show that T^* is linear. But for $u_1, u_2, v \in V$ and $a, b \in \mathbb{C}$, we have

$$\begin{aligned}\langle T^*(au_1 + bu_2), v\rangle &= \langle au_1 + bu_2, Tv\rangle \\ &= a^*\langle u_1, Tv\rangle + b^*\langle u, Tv\rangle \\ &= a^*\langle T^*u_1, v\rangle + b^*\langle T^*u_2, v\rangle \\ &= \langle aT^*u_1 + bT^*u_2, v\rangle\end{aligned}$$

We can do this quickly by noting $\{v_i\}$ is an orthonormal basis for V so that the elements of T are given by $a_{ij} = \langle v_u, Te_j\rangle$. Define T^* to have elements $b_{ij} = \overline{a_{ji}}$.

(b) Suppose there were an adjoint D^* for D. Then on this real vector space, $D^* = D$. Then we also have $\langle Df, g\rangle = \langle f, D^*g\rangle = \langle f, Dg\rangle$. Take $f(x) = x$ and $g(x) = 1$. Then

$$\langle Df, g\rangle = \langle x, 1\rangle = \int_0^1 x\, dx = \frac{1}{2}$$
$$\langle f, Dg\rangle = \langle x, 0\rangle = \int_0^1 0\, dx = 0$$

a contradiction. Notice here the previous part "fails" as the space is not finite dimensional.

□

5. Let $R \neq 0$ be a commutative ring with identity.

(a) Let I be an nontrivial ideal of R. Prove that I is a free module if and only if it is a principal ideal generated by a nonzerodivisor.

(b) Prove that if *every* finitely generated R-module is free, then R is a field.

Solution:

(a) Suppose that $I \lhd R$ be a free R-module. Let $\{x_\alpha\}_\alpha$ be a basis for I, not necessarily countable. Observe that if we choose $a, b \in \{x_\alpha\}_\alpha$, where a, b are distinct, we have $ab + (-ab) = 0$ is a nontrivial relation, contradicting the fact that $\{x_\alpha\}_\alpha$ is a basis. Then it must be that $I = (x)$ for some $x \in R$. We only need show that x is a non-zerodivisor. Suppose that x were a zero divisor, then there is a $0 \neq y \in x$ such that $xy = 0$, contradicting the fact that $\{x\}$ is a basis for I. Then $I = (x)$ is a principal ideal generated by a non-zerodivisor.

Now assume that $I = (x)$ is a principal ideal generated by a non-zerodivisor. The result is then immediate as $I = Rx$ so that $\{x\}$ serves as a basis for I so that I is free. To confirm this, observe that if $ax = 0$ for $0 \neq a \in R$, then x is a zero divisor, contrary to the assumption.

(b) If R has no nonzero ideals, then $R = \{0\}$ or R is a field for otherwise if $0 \neq x \in R$ had no inverse, then Rx is a proper (as $1 \notin Rx$) nonzero ideal. Suppose that every proper ideal I of R were free. Let I be a proper ideal of R. Then R/I is a finitely generated R-module spanned by $\overline{1}$. If I were not the zero deal, then R/I is not isomorphic to R^n for any n.

□

6. Let A be a 3×3 matrix with entries in $\mathbb{Q}$ such that $A^8 = I$. Prove that $A^4 = I$.

Solution: Let $p_A(x)$ denote the characteristic polynomial for A. By the Cayley-Hamilton Theorem, $p_A(A) = 0$. Write $q_A(x) = x^8 - 1$. By assumption, $q_A(A) = 0$. Since $\mathbb{Q}[x]$ is a Euclidean domain ($\mathbb{Q}$ is a field), we can find a gcd of $p_A(x), q_A(x)$: $d_A(x) := \gcd(p_A(x), q_A(x))$. Since $d_A(x) = r(x)p_A(x) + s(x)q_A(x)$ for some $r(x), s(x) \in \mathbb{Q}[x]$, we know

$$d_A(A) = r(A)p_A(A) + s(A)q_A(A) = r(A) \cdot 0 + s(A) \cdot 0 = 0.$$

But we know also that

$$q_A(x) = x^8 - I = (x^4 - I)(x^4 + I) = (x^2 - I)(x^2 + I)(x^4 + I) = (x - I)(x + I)(x^2 + I)(x^4 + I).$$

Now $d_A(x)$ is a factor of $p_A(x)$ and $q_A(x)$ of degree at most 3. Furthermore as $\mathbb{Q}[x]$ is a UFD, we know that $d_A(x)$ is relatively prime to $x^4 + I$. But then $d_A(x)$ must divide $(x - I)(x + I)(x^2 + I) = (x^2 - I)(x^2 + I) = x^4 - I$. As $d_A(A) = 0$, we must have $A^4 - I = 0$, i.e. $A^4 = I$. □

7. Let $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[4]{2}$. Let $E = \mathbb{Q}(\alpha, \beta)$. Prove that $[E : \mathbb{Q}] = 12$.

Solution: Now that $p_\alpha(x) := x^3 - 2$ is irreducible over $\mathbb{Q}$ (it is Eisenstein with $p = 2$) and $p_\alpha(\alpha) = 0$. Furthermore, $p_\beta(x) := x^4 - 2$ is irreducible over $\mathbb{Q}$ (it is Eisenstein with $p = 2$) and $p_\beta(\beta) = 0$. Therefore, $p_\alpha(x), p_\beta(x)$ are the minimal polynomials for α, β, respectively. So $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] = 3$ and $[\mathbb{Q}(\beta) \colon \mathbb{Q}] = 4$. Generally, if K_1, K_2 are finite extensions of a field F, say of degree n, m, respectively, then $[K_1K_2 \colon F] \leq [K_1 \colon F][K_2 \colon F]$. Suppose $(n, m) = 1$. Now $[K_1K_2 \colon F]$ is divisible by both $[K_1 \colon F]$ and $[K_2 \colon F]$ as $K_1, K_2 \subseteq K_1K_2$. However, $(n, m) = 1$ so that $[K_1K_2 \colon F]$ is divisible by nm. Therefore, $[K_1K_2 \colon F] = nm$.

Let $K_1 := \mathbb{Q}(\alpha)$ and $K_2 := \mathbb{Q}(\beta)$. Note that $[K_1 \colon \mathbb{Q}] = 3$ and $[K_2 \colon \mathbb{Q}] = 4$ and $(3, 4) = 1$. By the work above, $[K_1K_2 \colon \mathbb{Q}] = 3\dot{4} = 12$. It only remains to show that $K_1K_2 = E$. But this follows by abstract nonsense: K_1K_2 is the smallest field containing $K_1 = \mathbb{Q}(\alpha)$ (the smallest field containing $\mathbb{Q}$ and α) and $K_1 = \mathbb{Q}(\beta)$ (the smallest field containing $\mathbb{Q}$ and β) while $E = \mathbb{Q}(\alpha, \beta)$ is the smallest field containing $\mathbb{Q}$, α, and β. Therefore, $\mathbb{Q}(\alpha, \beta) = E = K_1K_2$. □

8. Let F be a field and let $f \in F[x]$ be an irreducible polynomial of degree n. Let E be a splitting field of f. Prove that $[E : F] \leq n!$[10]

Solution: If $f(x)$ has degree 1, then f is irreducible. If $f(\alpha) = 0$ then $\alpha \in F$. But then the splitting field of f is F and $[F \colon F] = 1 \leq 0! = 1$. Assume the result holds for $n = k$. Let $f \in F[x]$ be an irreducible polynomial of degree $k + 1$. Let α be a root of f. Since f is irreducible, f is the minimal polynomial for α. In particular, $[F(\alpha) \colon F] = k + 1$. Now $F(\alpha)$ contains a root of f, namely α, so that $F(\alpha) \subseteq E$. Furthermore, f factors in $F(\alpha)[x]$ as $f = (x - \alpha)g(x)$ for some polynomial $g(x)$ of degree k. By considering $F' = F(\alpha)$, the inductive hypothesis says $[E \colon F(\alpha)] \leq k!$. But then

$$[E \colon F] = [E \colon F(\alpha)][F(\alpha) \colon F] \leq k! \cdot (k + 1) = (k + 1)!.$$

Therefore, the result holds by induction. □

[10] This holds, in some sense, more generally: if $f(x) \in F[x]$ is a polynomial of degree n, adjoining a root of $f(x)$ to F generates an extension F_1 of F of degree at most n (equal to n if and only if $f(x)$ were irreducible). Over F_1, the polynomial has at least one linear factor so that any other root of $f(x)$ satisfies a polynomial of at most degree $n - 1$ over the field F_1. Adjoining such a root to F_1 forms an extension F_2 of at most degree $n - 1$. This process can continue at most n times (since $\deg f = n$) and each time produces an extension of at most degree i at the ith stage. Note $F \subseteq F_1 \subseteq \cdots \subseteq F_n$. Since $[F_n \colon F] = [F_n \colon F_{n-1}][F_{n-1} \colon F_{n-2}] \cdots [F_1 \colon F] \leq n \cdot (n - 1) \cdot \cdots \cdot 1 = n!$.

9.

(a) Let R be a commutative ring with identity. Assume that $\mathbb{Z}$ is a subring of R. You have seen that this makes R into a $\mathbb{Z}$-module. Assume that R is a finitely generated $\mathbb{Z}$-module. Prove that R is not a field.

(b) Find a field F such that the additive group $(F, +)$ is a finitely generated $\mathbb{Z}$-module.

January 2015

1. Show that a group of order 24 cannot be simple. [Hint: If $|\operatorname{Syl}_3(G)| = 4$, then there is a group homomorphism from G to S_4.]

Solution: We know that $24 = 2^4 \cdot 3$. Let n_p denote the number of Sylow p-subgroups. It is clear by Sylow's Theorem and the fact that G has order 24 that $n_2 \not\geq 4$ and $n_3 \not\geq 9$. Then $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4\}$. If either n_2, n_3 are 1 then the Sylow p-subgroup is unique, hence normal. Assume that neither are unit. Then as $n_2 = 3$, the action of G by conjugation on its Sylow 2-subgroups determines a map $\varphi : G \to S_3$. The image of G under φ in S_3 acts transitively on these subgroups. Therefore, $\operatorname{im} \varphi \neq 0$. By the First Isomorphism Theorem, $\operatorname{im} \varphi \cong G/\ker \varphi$. So we know that $\ker \varphi \neq G$. If $\ker \varphi = \{1\}$, then $\operatorname{im} \varphi \cong G$. But then $24 = |G| = |\operatorname{im} \varphi| \leq |S_3| = 6$, impossible. Then $\ker \varphi$ is a nonempty proper subgroup of G. But $\ker \varphi \lhd G$. Therefore, G is not simple. □

2. Let G be a group. For an element $w \in G$, let $[w]$ denote its conjugacy class in G and let $C_G(x)$ denote its centralizer in G.

(a) If G is a finite group and $x \in G$, show that $|\,[x]\,| = [G : C_G(x)]$.

(b) If $N \lhd G$ with $[G : N] = 2$ and $y \in N$, show that $[y]$ is either a conjugacy class of N or the union of 2 conjugacy classes in N.

Solution:

(a) We create a bijection between $[x]$ and left cosets of $C_G(x)$. If $y \in [x]$, then $y = axa^{-1}$ for some $a \in G$. Define a map φ from $[x]$ to the set of left cosets of $C_G(x)$ be $y = axa^{-1} \mapsto aC_G(x)$. We need show that this map is well defined. Suppose $y = axa^{-1} = bxb^{-1}$. Then $b^{-1}ax = xb^{-1}a$ so that $b^{-1}a$ commutes with x. But then $b^{-1}a \in C_G(x)$. But then $b^{-1}aC_G(x) = C_G(x)$ so that $aC_G(x) = bC_G(x)$. Therefore, φ is well defined.

It is immediate that this map is onto so it only remains to show that it is injective. Suppose $\varphi(a) = \varphi(b)$. Then $aC_G(x) = bC_G(x)$. But then $ak = b$ for some $k \in C_G(x)$. But then $k = a^{-1}b \in C_G(x)$. Therefore, $a^{-1}b$ commutes with x so $a^{-1}bx = xa^{-1}b$. But then this shows that $axa^{-1} = bxb^{-1}$.

(b)

3. Let G be a finite group and P be a Sylow p-subgroup. Let $H = N_G(P) = \{g \in G \mid g^{-1}Pg \subseteq P\}$ be the normalizer of P in G. Prove that for any $g \in G$, $g^{-1}Hg = H$ if and only if $g \in H$.

Solution: We prove that $N_G(N_G(P)) = N_G(P)$: we have $P \leq N_G(P) \leq N_G(N_G(P))$. Now P is a Sylow p-subgroup of $N_G(P)$ and $N_G(N_G(P))$. If $g \in N_G(N_G(P))$, then $gPg^{-1} \leq$

$gPg^{-1} = N_G(P)$. Since all Sylow p-subgroups are conjugate, there exists $h \in N_G(P)$ such that $gPg^{-1} = hPh^{-1}$. Since $h \in N_G(P)$, it must be that $hPh^{-1} = P$ so that $gPg^{-1} = P$. Therefore, $g \in N_G(P)$ showing that $N_G(N_G(P)) = N_G(P)$. The result then follows from the fact that:

$$g^{-1}Hg = H \iff H = gHg^{-1} \iff g \in N_G(H) = N_G(N_G(P)) = N_G(P) = H$$

□

4. Let V and W be vector spaces and let $f : V \to W$ and $g : W \to V$ be linear transformations with $f \circ g = 1_W$. Prove that V decomposes as the direct sum of subspaces

$$V = \operatorname{im} g \oplus \ker f$$

where $\operatorname{im}(g)$ is the image of g and $\ker(f)$ is the kernel of f.

Solution: Let $x \in V$ and consider the element $x - gf(x)$. Observe that

$$f(x - gf(x)) = f(x) - (fgf)(x) = f(x) - (fg)f(x) = f(x) - f(x) = 0$$

so that $x - gf(x) \in \ker f$. That is, there is a $k \in \ker f$ such that $k = x - gf(x)$. But then $x = gf(x) + k$. Then every element of V is the sum of some element in the image of g, namely $gf(x)$, and an element $k \in \ker f$. We need now only show that the sum is direct. Let $t \in \operatorname{im} g \cap \ker f$. As $t \in \operatorname{im} g$ so that there is a $w \in W$ such that $t = g(w)$. As $t \in \ker f$, we know that $f(t) = 0$. But then $0 = f(t) = fg(w) = 1(w) = w$. But then $t = g(w) = 0$. Therefore, the sum is direct. □

5.

(a) Prove that in a UFD (unique factorization domain), any ascending chain of *principal* ideals must stabilize.

(b) Give an example of a UFD that is not noetherian.

Solution:

(a) Suppose

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

is a chain of principal ideals in a UFD. As a_i is in a UFD, it has a unique prime factorization. We know that $a_1 \in (a_2)$. It is then clear that $a_2 \mid a_1$. Similarly, we know that $a_i \in (a_{i+1})$ so that $a_{i+1} \mid a_i$. So the prime factors of a_{i+1} appear in the prime factorization of a_i. But then the prime factors of a_i appear in a_1 for all i.

Suppose that $a_1 = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ is the prime factorization for a_1, where the p_i are prime. As the containment of each ideal is proper, a_{i+1} must have one less prime (counting multiplicity) than a_i. But as a_1 has finitely many primes (counting multiplicity) – namely, $N = \sum_{i=1}^{n} r_i$ – it must be that the chain stabilizes in at most $N + 1$ steps.

(b) The UFD $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ is such an example. Easier to see is $k[x_1, x_2, \cdots]$, where k is a field. Let $R = k[x_1, x_2, \cdots]$. Note that $k[x_1, \ldots, x_n]$ is a UFD for all $n \in \mathbb{N}$ since k is a field. Note given $f \in R$, f must involve finitely many variables, say the largest subscript occurring in f is N. Then $f \in k[x_1, \ldots, x_N]$, a UFD. Then f factors uniquely in $k[x_1, \ldots, x_N]$. But the only possible nontrivial factorizations in R for f can only involve these variables. Then f factors uniquely into irreducibles in R so that R is a UFD. However, R cannot be noetherian as it contains a non finitely generated ideal $(x_1, x_2, \cdots)$ (since any finite generating set contains a x_i with maximal subscript, say x_N, so that x_{N+1} is not generated by the chosen finite subset) or that

$$(x_1) \leq (x_1, x_2) \leq (x_1, x_2, x_3) \leq \cdots$$

is an infinite ascending chain of ideals of R.

□

6. Prove from the definition that any *nonzero* prime ideal in a PID (principal ideal domain) is maximal.

Solution: Let R be a PID. We need only consider a prime ideal generated by a single prime as we are in a PID. Let $P = (p)$ be a nonzero prime ideal. Suppose $M = (m)$ is a maximal ideal with $M \supset P$. We want to show that $M = R$ or $M = P$. As $M \supset P$, $p \in M = (m)$. Therefore, $p = rm$ for some $r \in R$. But as P is a prime ideal and p is prime, $r \in (p) = P$ or $m \in (p) = P$. If $m \in P$, then $M = P$ and we are done. Suppose then that $r \in P$. So $r = ps$ for some $s \in R$. But then $p = rm = psm = p(sm)$. This shows that $sm = 1$ (as R is a domain). Now as R is a PID, it must be that m is a unit. So $1 = sm \in P$. However, this implies that $P = R$. □

7. If G is a finite *abelian* group with the property that

$$|\{x \in G \mid x^n = 1\}| \leq n$$

for all $n \geq 1$, show that G must be cyclic.

Solution: Let $|G| = n$ and let S_d be the set of elements of G of order d. Suppose there were more than $\phi(d)$ elements of d. If $g \in S_d$, the cyclic group $\langle g \rangle$ has $\phi(d)$ elements of order d. But then by assumption, there exists $h \in G \setminus \langle g \rangle$ of order d. But then there are at least $|\langle g \rangle| + 1 = d + 1$ solutions to $g^n = 1$, a contradiction.

Then we have $\#S_d \leq \phi(d)$. Observe that $G = \sqcup_{d|n} S_d$. However,

$$n = |G| = \sum_{d|n} \#S_d \leq \sum_{d|n} \phi(d) = n$$

But then it must be that $\#S_d = \phi(d)$ for all $d \mid n$. In particular, $\#S_d \geq 1$ for all $d \mid n$. But then G must contain an element of order n. Therefore, G is cyclic.

OR

Suppose that $|\{x \in G \mid x^n = 1\}| \leq n$ for all n. Consider a prime $p \mid |G|$. If there were more than one Sylow p-subgroup of G, then there would be more than p^r solutions to $g^{p^r} = 1$, where r is the largest power of p dividing $|G|$. A Sylow p-subgroup is cyclic as $g^{p^{r-1}} = 1$ has less than p^r solutions so that there exists an element g with $g^{p^r} = 1$ and $g^{p^{r-1}} \neq 1$. Therefore, each Sylow p-subgroup of G is unique, hence normal and cyclic (by the work above). But then the group G is cyclic since G is the product of its Sylow p-subgroups if each Sylow p-subgroup is unique.

OR

Suppose $|G| = p^r$ for some prime p and $r \geq 1$. By Lagrange's Theorem, any nonidentity element $g \in G$ has order p^a for some $1 \leq a \leq r$. Choose r to be maximal. The elements $1, g, g^2, \ldots, g^{p^a-1}$ are p^a distinct solutions to $x^{p^a} = 1$. By assumption, these are all the solutions. Then if $h \in G$, then its order is p^t, where $t \leq r$. Therefore, $h^{p^r} = (h^{p^t})^{p^{t-r}} = 1$. But then $h = g^i$ for some i. But then $G = \langle g \rangle$. Therefore, G is cyclic.

Now since G is a finite abelian group, by the Fundamental Theorem of Finitely Generated Abelian Groups, we have $G = S_{p_1} \oplus S_{p_2} \oplus \cdots \oplus S_{p_k}$, where the p_i are the distinct prime divisors of $|G|$ and the S_{p_i} are the Sylow p-subgroups of G. Through this isomorphism, we can write uniquely as $g = s_1 s_2 \cdots s_k$, where $s_i \in S_i$. Any solution $x^n = 1$ in S_{p_i} is also a solution of $x^n = 1$ for $x \in G$. By the work above, it must be that each S_{p_i} is cyclic. Let g_i be a generator for S_{p_i}. We claim $g = g_1 \cdots g_k$ is a generator for G. It is sufficient to show that $|G| \mid |g_1 \cdots g_k|$. Since G is abelian, $(g_1 \cdots g_k)^n = g_1^n \cdots g_k^n = 1$. But if m is the order of g, then $g^m = g_1^m \cdots g_k^m = 1$. Since every element of G is unique represented as a product of the s_i, it must be that $g_i^m = 1$. But then $|S_{p_i}| \mid m$ for all $i = 1, \ldots, k$. But then $|G| = |S_{p_1}| \cdot |S_{p_2}| \cdot \cdots \cdot |S_{p_k}| \mid m$. But $|m| \mid |G|$ so that $|G| = m$. Therefore, g generates g and G is cyclic. □

8.

(a) If $M = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \cdots & \lambda \end{bmatrix}$ is a Jordan block with $\lambda \in \mathbb{C}$. What is the Jordan canonical form of M^2 over $\mathbb{C}$?

(b) If A is a matrix such that A and A^2 have the same Jordan canonical form, what are the possible Jordan forms of A?

9. Let $L \supseteq K \supseteq F$ be field extensions, not necessarily of finite degree, with K algebraic over F. If $\alpha \in L$ is algebraic over K, prove that α is algebraic over F.

Solution: As α is algebraic over K, we know there is a polynomial equation

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

where $a_i \in K$. Consider $F^* = F(a_0, a_1, \cdots, a_n)$. As K/F is algebraic, $a_0, \cdots, a_n$ are algebraic over F. So F^*/F is a finite extension as F^* is generated by a finite number of algebraic elements. Then α generates an extension of degree at most n as the minimal polynomial for α must divide $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$. But then

$$[F^* : F] = [F(\alpha, a_0, a_1, \cdots, a_n) : F(a_0, a_1, \cdots, a_n)]]\ [F(a_0, a_1, \cdots, a_n) : F]$$

is finite. So $F(\alpha, a_0, \cdots, a_n)/F$ is an algebraic extension so that α is algebraic over F. □

10. Consider the number $\alpha = \sqrt{\sqrt{2} - 1}$ and the field extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$.

(a) Find the minimal polynomial of α over $\mathbb{Q}$.

(b) Find the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ of the field extension.

(c) Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

Solution:

(a) We know

$$\begin{aligned} \alpha &= \sqrt{\sqrt{2} - 1} \\ \alpha^2 &= \sqrt{2} - 1 \\ \alpha^2 + 1 &= \sqrt{2} \\ (\alpha^2 + 1)^2 &= 2 \\ \alpha^4 + 2\alpha^2 - 1 &= 0 \end{aligned}$$

So we suspect that the minimal polynomial for α is $f(x) = x^4 + 2x - 1$. The only rational roots can be ± 1 by the Rational Root Theorem. Both are easily seen not to be zeros. But then $f(x)$ has no rational roots so that it must be irreducible over $\mathbb{Q}$. Then $f(x)$ is an irreducible polynomial with root α. Therefore, $f(x)$ is the minimal polynomial for α.

(b) The degree of the extension is the same as the degree of the minimal polynomial, which we found in the previous part. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(c)

August 2015

1. Let p, q be primes, not necessarily distinct. Show that a group of order pq is not simple.

Solution: If $p = q$, then $|G| = pq = p^2$. We have a more general result: any p-group (a group of order p^n) cannot be simple for $n > 1$. Suppose $|G| = p^n$ for $n > 1$. Recall the Class Equation:

$$|G| = |Z(G)| + \sum_{g_1,\cdots,g_r} |G\colon C_G(g_i)|,$$

where $Z(G)$ is the center of G, $C_G(g_i)$ is the centralizer of g_i, and $g_1, \ldots, g_r$ are representatives for the distinct conjugacy classes of G with more than one element (for otherwise it is in the center). The centralizer of g_i, $C_G(g_i)$, is a subgroup of G so that by Lagrange's Theorem its order must divide $|G|$. Since $|G| = p^n$, $|C_G(g_i)| = p^k$ for some $k < n$ (it cannot be that $k = n$ for then $C_G(g_i) = G$ and then $g_i \in Z(G)$). Then $|G\colon C_G(g_i)| = \frac{|G|}{|C_G(g_i)|} = p^{n-k}$. Now we have $|G| - |G\colon C_G(g_i)| = |Z(G)|$. Since p divides the left side, we must have $p \mid |Z(G)|$. In particular, $Z(G)$ is non-trivial. But $Z(G)$ is always a normal subgroup so that G cannot be simple. The result then follows with $n = 2$.[11]

Now if $p \neq q$, without loss of generality, assume that $p > q$. Let n_p denote the number of Sylow p-subgroups. We know that $n_p \equiv 1 \mod p$ and that $n_p \mid q$. As $n_p \mid p$, it must be that $n_p \in \{1, q\}$. But as $n_p \equiv 1 \mod p$, $n_p = 1 + np$ for some $n \in 0, 1, 2, \cdots$. If $n > 1$, then $(1 + np) > p > q$ so that $1 + np \nmid q$, a contradiction. Therefore, $n = 0$ so that $n_p = 1$. Then the Sylow p-subgroup is unique, hence normal, so that G is not simple. □

2. Let G be a group with subgroup H (the subgroup need not be normal). The set G/H of left cosets of H in G is a left G-set by means of $g \cdot xH = gxH$, where $g, x \in G$.

(a) For $a \in G$, compute the stabilizer G_{aH} of aH.

(b) Let X, Y be left G-sets. A map $\phi : X \to Y$ is a homomorphism if $\phi(gx) = g\phi(x)$ for all $g \in G$, $x \in X$, and it is an isomorphism if there exists a homomorphism $\psi : Y \to X$ satisfying $\psi\phi = 1_X$ and $\phi\psi = 1_Y$. The G-sets X, Y are isomorphic if there exists an isomorphism $X \to Y$. For $x \in X$, denote G_x the stabilizer of x.

  (i) If $\phi : X \to Y$ is a homomorphism of G-sets, prove that $G_x \leq G_{\phi(x)}, x \in X$.

  (ii) If $\phi : X \to Y$ is an isomorphism, prove that $G_x = G_{\phi(x)}, x \in X$.

(c) Let H, K be subgroups of G.

[11] Since $n = 2$, the group must be abelian for there are only two groups up to isomorphism of order p^2 for any prime: $\mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}/p^2\mathbb{Z}$, neither of which are simple since they have nontrivial center by the work above. You should be able to prove this classification. Note that a p-group need not be abelian. Take $p = 2$ and $n = 3$ so that $|G| = 8$. The dihedral group of order 8 is non-abelian nor is the quaternion group. Finally in the case of $n = 1$, the group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and is simple.

(i) If G/H and G/K are isomorphic G-sets, prove that H and K are conjugate subgroups of G. *Hint:* use (a) and part (ii) of (b).

(ii) Prove the converse of (i). *Hint:* Use a relevant theorem, or construct an isomorphism explicitly: if $H = aKa^{-1}$ for some $a \in G$, right multiplication by a is a bijective map $G \to G$.

Solution:

(a)

$$\begin{aligned} g \in G_{aH} &\iff gaH = aH \\ &\iff a^{-1}gaH = H \\ &\iff (a^{-1}ga)H = H \\ &\iff a^{-1}ga \in H \\ &\iff a^{-1}ga = h \text{ for some } h \in H \\ &\iff g = aha^{-1} \\ &\iff g \in \{aha^{-1} \mid h \in H\} \\ &\iff g \in N_a(H) \end{aligned}$$

(b,i) Let $g \in G_x$ so that $gx = x$. But then

$$\phi(x) = \phi(gx) = g\phi(x)$$

so that $g \in G_{\phi(x)}$. But then $G_x \leq G_{\phi(x)}$.

(b,ii) Let $\phi : X \to Y$ be an isomorphism with inverse $\psi : Y \to X$. By the previous part, we know that $G_x \leq G_{\phi(x)}$. But also by the previous part, we have $G_{\phi(x)} \leq G_{\psi(\phi(x))}$, but $G_{\psi(\phi(x))} = G_x$. Therefore, $G_x = G_{\phi(x)}$.

(c,i) Suppose that $G/H \cong G/K$. Then there is a map $\phi : G/H \to G/K$ that is an isomorphism with inverse $\psi : G/K \to G/H$. Then there is a $g \in G$ (not necessarily unique) such that

$$\phi(1H) = \phi(H) = gK$$

Now let $h \in H$. Then

$$gK = \phi(H) = \phi(hH) = h\phi(H) = hgK$$

But then $h \in G_{gK}$ so $g^{-1}hg \in K$. But then $g^{-1}Hg \leq K \leftrightarrow H \leq gKg^{-1}$. Applying this same logic to ψ and K gives $\psi(K) = g^{-1}H$ so that $gKg^{-1} \leq H$. This shows that $H = gKg^{-1}$ for some $g \in G$ (again, not necessarily unique). But then H and K are conjugate subgroups.

(c,ii) Suppose that H, K are conjugate subgroups in G. Then there is a $g \in G$ (not necessarily unique), such that $H = gKg^{-1}$. Define $\phi : G/H \to G/K$ be given by $rH \mapsto rgK$. We need show that this map is well defined, a homomorphism, injective, and surjective. Suppose that $rH = sH$. Then $H = r^{-1}sH$ so that $r^{-1}s \in H$. That is, $r^{-1}s = h$ for some $h \in H$. This shows $s = rh$. Then $\phi(sH) = \phi(rhH) = \phi(rH)$ so that ϕ is well defined. We need see that ϕ is a homomorphism. But this follows easily as if $g \in G$ and $rH \in G/H$, then

$$\phi(grH) = grgK = g(rgK) = g\phi(rH)$$

To see injectivity, suppose that $\phi(rH) = \phi(sH)$. Then $rgK = sgK$ so that $K = g^{-1}r^{-1}sgK$. But this shows that $g^{-1}r^{-1}sg \in K$. Then there is a $k \in K$ such that $g^{-1}r^{-1}sg = k$. Therefore, $r^{-1}s = gkg^{-1}$. By assumption, $gkg^{-1} \in H$ so that there is an $h \in H$ such that $r^{-1}s = h$. This shows that $s = rh$. This finally shows $sH = rhH = rH$. Therefore, ϕ is injective. Now let $sK \in G/K$. Take $r = sg^{-1}$ and observe $\phi(rH) = rgK = sg^{-1}gK = sK$ so that ϕ is surjective. Therefore, ϕ is an isomorphism and $G/H \cong G/K$.

□

3. Let $\phi : F^n \to F^m$ be left multiplication by an $m \times n$ matrix A. Prove that the following are equivalent:

(i) A has a left inverse, a matrix B such that $BA = 1_{F^n}$

(ii) ϕ is injective

(iii) The rank of A is n.

Solution: Choose a basis of F^n, say $\{e_1, e_2, \ldots, e_n\}$ (there must be n basis elements since $\dim F^n = n$) and let A be the matrix of ϕ with respect to that basis. We show each is equivalent to the others directly. [Choosing an ordering of the if and only if certainly gives a short more direct proof.]

(i) $\iff$ (ii) Let A have a left inverse B. Suppose $\phi(X) = \phi(Y)$ for $X, Y \in \mathbb{F}^n$, i.e. $AX = AY$. Then we have $X = 1(X) = BAX = BAY = 1(Y) = Y$ so that $X = Y$. But then ϕ is injective.

Now let ϕ be injective. We know that $\{\phi(e_1), \phi(e_2), \ldots, \phi(e_n)\}$ are linearly independent and can be extended to a basis of F^m, say by adding vectors $f_1, f_2, \ldots, f_{m-n} \in F^m$ (it must be that $n \leq m$ by linear independence) to $\{\phi(e_1), \phi(e_2), \ldots, \phi(e_n)\}$.

For every basis $\{v_1, \ldots, v_m\}$ of F^m and collection of vectors $w_1, \ldots, w_m$ (which need not be distinct—they will not be how we use them below), there is a linear transformation sending each v_i to w_i: simply take the map sending each v_i to w_i and extend

by linearity. By the linear independence of the $\{v_i\}$, this linear transformation must also be unique.

Now we have basis $\{\phi(e_1), \phi(e_2), \ldots, \phi(e_n), f_1, f_2, \ldots, f_{m-n}\}$ of F^m. Let l be the unique linear transformation sending $\phi(e_i)$ to e_i for $1 \leq i \leq n$ and $l(f_j) = 0$ for $1 \leq j \leq m-n$. By construction, $l\phi(e_i) = e_i$ for all i and is linear. But then $l\phi = 1_{F^n}$. Since l is a linear transformation, we may represent it as a matrix L (using the chosen basis, so $L = (l(e_1)\ l(e_2) \cdots l(e_n))$). But then taking $B = L$ gives the result.

(ii) $\Longleftrightarrow$ (iii) Let ϕ be injective. We know rank $A \leq n$. Note n is the number of columns of A. Without loss of generality, we can assume that A is in reduced-row echelon form (applying row reduction does not change the rank of A or injectivity). Since ϕ is injective, $AX = 0$ has at most one solution. But then there are no free variables, i.e. A has a pivot in every column. But A has n columns so that rank $A \geq n$. Therefore, rank $A = n$.

Let the rank A be n. We know row operations do not affect the injectivity of multiplication by A (that is, the injectivity of ϕ) and do not affect the rank of A. So again without loss of generality, we may assume that A is reduced-row echelon form. Then A has a pivot in every column since rank $A = n$. Therefore, there is at most one solution for every system $AX = B$. But then ϕ is necessarily injective.

□

4. Let V denote the vector space of real $n \times n$ matrices.

(a) Prove that $\langle A, B \rangle = \text{trace}(A^T B)$ defines a positive definite bilinear form on V.

(b) Find an orthonormal basis for this form.

Solution:

(a) We first show that this is indeed a bilinear form on V. Let $c \in \mathbb{R}$ and $A, B, C \in V$. Then we have (using the fact that the trace is linear)

$$\begin{aligned}
\langle\, cA,\, B\,\rangle &= \text{trace}((cA^T)B) = c\text{trace}(A^T B) = c\,\langle\, A,\, B\,\rangle \\
\langle\, A,\, cB\,\rangle &= \text{trace}(A^T(cB)) = c\text{trace}(A^T B) = c\,\langle\, A,\, B\,\rangle \\
\langle\, A+B,\, C\,\rangle &= \text{trace}((A+B)^T C) = \text{trace}((A^T + B^T)C) = \text{trace}(A^T C + B^T C) \\
&= \text{trace}(A^T C) + \text{trace}(B^T C) = \langle\, A,\, C\,\rangle + \langle\, B,\, C\,\rangle \\
\langle\, A,\, B+C\,\rangle &= \text{trace}(A^T(B+C)) = \text{trace}(A^T B + A^T C) \\
&= \text{trace}(A^T B) + \text{trace}(A^T C) = \langle\, A,\, B\,\rangle + \langle\, A,\, C\,\rangle
\end{aligned}$$

so that $\langle \cdot, \cdot \rangle$ is bilinear. To see that it is positive definite, observe that

$$\langle A, A \rangle = \text{trace}(A^T A) = \sum_{i,j}^{n} a_{i,j}^2 \geq 0.$$

But as $a_{i,j} \in \mathbb{R}$ and $a_{i,j}^2 = 0$ if and only if $a_{i,j} = 0$, clearly the sum is 0 only if $a_{i,j} = 0$ for all i, j. But then A is the zero matrix. Furthermore, if A is the zero matrix, clearly $\langle A, A \rangle = 0$. Then $\langle \cdot, \cdot \rangle$ is positive definite.

(b) An obvious choice of basis would be $\{M_{i,j}\}_{1 \leq i,j \leq n}$, where $M_{i,j}$ is the matrix with 1 in the ith, jth entry and 0 elsewhere. Clearly, this is a basis for V. We need only show that it is orthogonal. Observe $M_{i,j}^T M_{i,j} = M_{j,j}$ so that

$$\langle M_{i,j}, M_{i,j} \rangle = \text{trace}(M_{i,j}^T M_{i,j}) = \text{trace}(M_{j,j}) = 1$$

Finally suppose $M_{a,b} \neq M_{x,y}$,

$$\begin{aligned}
\langle M_{a,b}, M_{x,y} \rangle &= \text{trace}(M_{a,b}^T M_{x,y}) \\
&= \sum_{i=1}^{n} (M_{a,b}^T M_{x,y})_{ii} \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (M_{a,b}^T)_{i,j} (M_{x,y})_{j,i} \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \delta_{a,j} \delta_{b,i} \delta_{x,j} \delta_{y,i} \\
&= 0
\end{aligned}$$

where δ is the Kronecker delta. [Observe the above is truly zero unless $a = j$, $b = i$, $x = j$, $y = i$ so that $a = x = j, b = y = i$ so that $M_{a,b} = M_{x,y}$.] But then $\{M_{i,j}\}_{1 \leq i,j \leq n}$ is an orthonormal basis.

□

5. Let R be a commutative ring.

(i) If P and Q are prime ideals of R, determine when $P \cap Q$ is again a prime ideal of R.

(ii) If A, B, and I are ideals of R with $I \subset A \cup B$, show that I is contained in either A or B.

Solution:

(i) We show that $P \cap Q$ is a prime ideal if and only if P contains Q or Q contains P. Clearly, $P \cap Q$ is an ideal of R as P, Q are ideals. Let $P \cap Q$ be a prime ideal. Suppose that $P \subsetneq Q$ and $Q \subsetneq P$. Then there exists $p \in P \setminus Q$ and $q \in Q \setminus P$. Now $pq \in P$ since $p \in P$ and P is an ideal. Similarly, $pq \in Q$. But then $pq \in P \cap Q$. Since $P \cap Q$ is prime, either $p \in P \cap Q$ or $q \in P \cap Q$. Without loss of generality, assume $p \in P \cap Q$. But then $p \in P$ and $q \in Q$, a contradiction. Therefore, either $P \subseteq Q$ or $Q \subseteq P$, i.e. $P \cap Q = P$ or $P \cap Q = Q$.[12][13]

Now suppose that P, Q are prime with one containing the other. Assume one ideal contains the other. Without loss of generality assume $P \subseteq Q$. Now $P \cap Q$ is an ideal and since $P \cap Q = P$ and P is prime, $P \cap Q$ is a prime ideal.[14]

(ii) Suppose that the statement is false. Then there are $a, b \in I$ such that $a \in A$ but $a \notin B$ and $b \in B$ but $b \notin A$. As I is a subring, $a + b \in I$. But then $a + b \in A \cup B$ so that $a + b \in A$ or $a + b \in B$. If $a + b \in A$, then $(a + b) - a = b \in A$, a contradiction. However, if $a + b \in B$ then $(a + b) - b = a \in B$, a contradiction.

□

6.

(i) Find the minimal polynomial of $\alpha = \sqrt{\sqrt{3} - 1}$ over $\mathbb{Q}$.

(ii) Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

Solution:

[12]Note this did not require that either P or Q be prime but just that $P \cap Q$ was prime. But the work shows that $P \cap Q = P$ or $P \cap Q = Q$ so that one is merely assuming P or Q is prime. The second part will use P, Q prime — trivially.

[13]Note the intersection of prime ideals is not generally prime. Take $R = k[x, y]$, where k is a field. Since $R/(x) \cong k[y]$ and $R/(y) \cong k[x]$, $(x), (y)$ are prime ideals. However, $(x) \cap (y) = (xy)$. But (xy) cannot be prime since $R/(xy)$ has zero divisors as $\overline{x} \cdot \overline{y} = 0$ in $R/(xy)$.

[14]Note one can easily verify that the intersection of ideals is an ideal. But kernels are always ideals and $I \cap J$ is the kernel of the map $\phi : R \to R/I \times R/J$ given by $x \mapsto (x \mod I, x \mod J)$. Now if I, J are prime ideals, $R/I, R/J$ are integral domains since I, J are prime. But then $R/I \times R/J$ is never a domain unless one of the summands is zero. Since $R/\ker\phi \cong \mathrm{im}\,\phi$, one would need either this image to 'be in only one summand'. However, we have $\ker\phi = I \cap J$. This gives intuition how one would come to the conclusion that one ideal must contain the other.

(i) We have

$$\begin{aligned}\alpha &= \sqrt{\sqrt{3}-1}\\ \alpha 2 &= \sqrt{3}-1\\ \alpha 2+1 &= \sqrt{3}\\ (\alpha^2+1)^2 &= 3\\ \alpha^4+\alpha^2+1 &= 3\\ \alpha^4+2\alpha^2-2 &= 0\end{aligned}$$

So that α is clearly a root of the polynomial $p(x) = x^4 + 2x^2 - 2$. However, observe that $p(x)$ is Eisenstein with $p = 2$ so that it is irreducible over $\mathbb{Q}$. But then $p(x)$ is the minimal polynomial for α. Note as $p(x)$ is irreducible, we know that $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg p(x) = 4$.

(ii) Notice that $p(x) = x^4 + 2x^2 - 2$ is even. Now as $p(\alpha) = 0$, we know that $p(-\alpha) = 0$. Let $\beta = \sqrt{-\sqrt{3}-1}$. Observe that

$$\alpha\beta = \sqrt{\sqrt{3}-1}\,\sqrt{-\sqrt{3}-1} = \sqrt{(\sqrt{3}-1)(-\sqrt{3}-1)} = \sqrt{3-\sqrt{3}+\sqrt{3}+1} = \sqrt{4} = 2$$

so that $\alpha\beta \in \mathbb{Q}(\alpha)$. But as $\alpha \in \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha)$ is a field, this implies $\alpha^{-1} \in \mathbb{Q}(\alpha)$. Therefore, $\alpha^{-1} \cdot \alpha\beta = \beta \in \mathbb{Q}(\alpha)$. This shows that $\pm\alpha, \pm\beta \in \mathbb{Q}(\alpha)$. But the same computation that showed α is a root of $p(x)$, shows that β is a root of $p(x)$. Since $p(x)$ is even, $-\beta$ is a root of $p(x)$. But then $\pm\alpha, \pm\beta \in \mathbb{Q}(\alpha)$ must be all the roots of $p(x)$. Therefore, $\mathbb{Q}(\alpha)$ is a splitting field for $p(x)$. Then $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then $|\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. There are only two groups of order 4 up to isomorphism: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

7.

(i) Let A be a matrix over the complex numbers $\mathbb{C}$ with elementary divisors $f_1 = (x-2)^2, f_2 = (x-2)^2(x+3)^2$, and $f_3 = (x-2)^3(x+3)^2$. Find the Jordan Canonical Form of A.

(ii) Let R be a PID and M an R-module. If $f : M \to R$ is an R-module homomorphism, show that there exists a submodule X of M such that $M = X \oplus \ker f$.

8. Let $F = \mathbb{Z}_p$ be the integers module a prime p.

(a) If $n > 0$, show that there is a field K of order p^n containing F.

(b) Show that $F[x]$ contains an irreducible polynomial of degree n.

9.

(i) If R is an integral domain with field of fractions $K \neq R$, show that K is not finitely generated as an R-module.

(ii) True or False: "A unique factorization domain must be Noetherian." Justify your answer.

Solution:

(i) Suppose that K were finitely generated as an R-module. Let $\langle k_1, k_2, \cdots, k_n \rangle$ be a generating set for K, where $k_i = a_i/b_i$, where $a_i, b_i \in R$. Then given $r \in R$, there are $r_i \in R$ such that

$$\frac{1}{r} = r_1 \frac{a_1}{b_1} + r_2 \frac{a_2}{b_2} + \cdots + r_n \frac{a_n}{b_n}$$

Obtaining a common denominator on the left shows that given $r \in R$, there are $a, b \in R$ such that

$$\frac{1}{r} = \frac{a}{b}$$

That is, given $r \in R$, there are $a, b \in R$ such that $ar = b$. In particular, this is true for $r = b^2$. But then we have $ar = ab^2 = b$ so that $b(ab - 1) = 0$. But as R is an integral domain, we have $ab - 1 = 0$ so that $ab = 1$. But then every element of R is invertible. But then if $x, y \in R$ with $xy = b$, then $axy = 1 \in R$. But then $R = F$, a contradiction.

(ii) The statement is false. The UFD $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ is such an example. It is simpler to justify the following answer: let k be a field. Then $R = k[x_1, x_2, \cdots]$ is a UFD: note that $k[x_1, \ldots, x_n]$ is a UFD for all $n \in \mathbb{N}$ since k is a field. Note given $f \in R$, f must involve finitely many variables, say the largest subscript occurring in f is N. Then $f \in k[x_1, \ldots, x_N]$, a UFD. Then f factors uniquely in $k[x_1, \ldots, x_N]$. But the only possible nontrivial factorizations in R for f can only involve these variables. Then f factors uniquely into irreducibles in R so that R is a UFD. However, R cannot be noetherian as it contains a non finitely generated ideal $(x_1, x_2, \cdots)$ (since any finite generating set contains a x_i with maximal subscript, say x_N, so that x_{N+1} is not generated by the chosen finite subset) or that

$$(x_1) \leq (x_1, x_2) \leq (x_1, x_2, x_3) \leq \cdots$$

is an infinite ascending chain of ideals of R.

□

January 2016

1. Let G be a group of order $351 = 3^3 \cdot 13$. Prove that G is simple.

Solution: Let n_p denote the number of Sylow p-subgroups of G. If $n_3 = 1$, then the Sylow 3-subgroup is unique, hence normal. Similarly, if $n_{13} = 1$, then the Sylow 13-subgroup is unique and hence normal. In either case, G would not be simple. Assume then that $n_3, n_{13} > 1$. As $n_3 \equiv 1 \mod 3$ and $n_3 \mid 13$, we must have $n_3 = 13$. Furthermore as $n_{13} \equiv 1 \mod 13$ and $n_{13} \mid 3^3$, we must have $n_{13} = 27$. By Lagrange's Theorem, the intersection of any distinct Sylow 13-subgroups must be trivial for any non-identity element would be a generator for the subgroup. Then there are $27 \cdot 12$ elements of order 13. But then there are $|G| - 27 \cdot 12 = 27$ elements of G not of order 13. But then there are 27 elements of G having order a power of 3. But this contradicts the fact that there are 13 distinct Sylow 3-subgroups. Therefore, either $n_3 = 1$ or $n_{13} = 1$ so that G contains a normal subgroup (hence cannot be simple). □

2. Let G be a group with subgroups H and K. Consider the action of H on the coset space G/K by left multiplication: $h \cdot aK = haK$ for all $h \in H$ and $a \in G$. Recall that the set $HaK = \{b \in G \mid b = hak \text{ for some } h \in H, k \in K\}$ is called a *double coset*.

(a) Prove that the orbit of a coset $aK \in G/K$ under the action of H is the set of left cosets of K in G which are contained in the double coset HaK.

(b) Compute the stabilizer of aK.

(c) If G is finite, prove that $|HaK| = |K| \, |H : H \cap aKa^{-1}|$ for every $a \in G$.

Solution:

(a) Let $\mathcal{O}_{aK}$ denote the orbit of aK. Observe that $\cup_{xK \in \mathcal{O}_{aK}} xK$ is contained in HaK. Now if $hak \in HaK$, then $hak \in haK$. However, $haK = h \cdot aK$ so that $hak \in haK \in \mathcal{O}_{aK}$. But then $ak \in \cup_{xK \in_{aK}} xK$. Therefore, $HaK = \cup_{xK \in \mathcal{O}_{aK}} xK$. Since the set of cosets partition G, the sets xK are disjoint. Therefore,

$$HaK = \bigsqcup_{xK \in \mathcal{O}_{aK}} xK$$

Then if $aK \in G/K$, the orbit is precisely the set of left cosets aK in G contained in the double coset HaK.

(b) We claim stab $aK = H \cap aKa^{-1}$. If $h \in H \cap aKa^{-1}$, then $h = aka^{-1}$ for some $k \in K$. But then $h \cdot aK = aka^{-1} \cdot aK = aka^{-1}aK = akK = aK$ so that $h \in$ stab aK. Then $H \cap aKa^{-1} \subseteq$ stab aK. Let $h \in$ stab aK. Then $aK = h \cdot aK = haK$. Then there exists $k \in K$ so that $ak = ha$. But then $h = aka^{-1}$ so that $h \in H \cap aKa^{-1}$. Therefore, stab $aK \subseteq H \cap aKa^{-1}$, showing that stab $aK = H \cap aKa^{-1}$.

(c) By (a), we have

$$|HaK| = \text{card}\left(\bigsqcup_{xK \in \mathcal{O}_{aK}} xK\right) = \sum_{xK \in \mathcal{O}_{aK}} |xK| = |K|\,|\mathcal{O}_{aK}|.$$

By the Orbit-Stabilizer Theorem, $|\mathcal{O}_{aK}| = |H\colon \text{stab } aK|$. But by (b), $\text{stab } aK = H \cap aKa^{-1}$. But then

$$|HaK| = |K|\,|\mathcal{O}_{aK}| = |K|\,|H\colon \text{stab } aK| = |K|\,|H\colon H \cap aKa^{-1}|$$

as desired. Note that considering the action of K on G/H (proving everything mutatis mutandis), we would obtain

$$|HaK| = |H|\,|K\colon K \cap aHa^{-1}|$$

□

3. Let S_5 denote the symmetric group on five elements.

(a) Find a representative for each conjugacy class of S_5 and compute the number of elements in each class.

(b) Find all elements of S_5 that commute with the 3-cycle (123).

4. Let A be a real symmetric $n \times n$ matrix, and let $T : \mathbb{R}^n \to \mathbb{R}^n$ be the linear operator given by left multiplication by A.

(a) Prove that $\ker T = (\text{im } T)^{\perp}$ with respect to the usual Euclidean dot product on $\mathbb{R}^n$.

(b) Prove that $\mathbb{R}^n = \ker T \oplus \text{im } T$.

5. Let E be a finite field extension of F and let $f \in F[t]$ be an irreducible polynomial. Assume that the degree of f and $[E : F]$ are relatively prime. Prove that f has no roots in E.

Solution: Note that if f had a root $\alpha \in F$, then $t - \alpha \in F[t]$ would be a factor of f so that f would be reducible, a contradiction. Suppose that f had a root $\alpha \in E$. By the preceding remarks, $\alpha \in E \setminus F$. Since f is irreducible in $F[t]$ and $f(\alpha) = 0$, then f is the minimal polynomial of α. Now $F(\alpha) \subseteq E$. Furthermore,

$$[E\colon F] = [E\colon F(\alpha)][F(\alpha)\colon F] = \deg f[E\colon F(\alpha)]$$

Let p be a prime dividing $\deg f$. Since $p \mid \deg f[E\colon F(\alpha)]$, it must be that $p \mid [E\colon F]$. But $[E\colon F]$ and $\deg f$ are relatively prime. Then no prime divides $\deg f$ so that $\deg f = 1$. But then $\alpha \in F$, a contradiction. Therefore, E contains no root of f. □

6.

(a) Construct a splitting field for the polynomial $t^3 + 2t + 1$ over the field $\mathbf{F}_3$ with three elements.

(b) Construct a splitting field for the polynomial $t^3 + t^2 + t + 2$ over $\mathbf{F}_3$. It is isomorphic to the splitting field constructed in part (a)?

Solution:

(a) The polynomial $p(t) = t^3 + 2t + 1$ is reducible over $\mathbf{F}_3$ if and only if $p(t)$ has a zero in $\mathbf{F}_3$. However, $p(0) = \overline{1}$, $p(1) = \overline{1}$, and $p(2) = \overline{1}$. Therefore, $p(t)$ is irreducible over $\mathbf{F}_3[t]$. We claim $F = \mathbf{F}_3[t]/\langle t^3 + 2t + 1\rangle$ is a splitting field for $p(t)$. Now $p(t)$ has a root in F by construction, namely $\bar{t} = t + \langle t^3 + 2t + 1\rangle$. However, observe

$$p(\bar{t}+1) = (\bar{t}+1)^3 + 2(\bar{t}+1) + 1 = \bar{t}^3 + 1 + 2\bar{t} + 2 + 1 \equiv \bar{t}^3 + 2\bar{t} + 1 = \overline{0}.$$

Therefore, $p(t)$ has two roots in F so that the third $(\bar{t} - 1)$ must also be in F. Therefore, F is the splitting field for $p(t)$.

(b) The polynomial $q(t) = t^3 + t^2 + t + 2$ is reducible over $\mathbf{F}_3$ if and only if $q(t)$ has a zero in $\mathbf{F}_3$. However, $q(0) = \overline{2}$, $q(1) = \overline{2}$, and $q(3) = \overline{1}$. Therefore, $q(t)$ is irreducible over $\mathbf{F}_3[t]$. We claim $F' = \mathbf{F}_3/\langle t^3 + t^2 + t + 2\rangle$ is a splitting field for $q(t)$. Now $q(t)$ has a root in F' by construction, namely $\bar{t} = t + \langle t^3 + t^2 + t + 2\rangle$. Moreover, since F' has characteristic 3, Frobenius is an automorphism, i.e. the map Frob: $x \mapsto x^3$ is an automorphism (it is an injective map between finite fields). Since $\bar{t}$ is a root of $q(t)$ over F', we have $\bar{t}^3$ a root of $q(t)$ over F'. [Note that $\bar{t}^3 \neq \bar{t}$ over F' as then $\bar{t}(\bar{t}^2 - 1) = 0$ so that $\bar{t} \in \{0, \pm 1\}$, a contradiction.] But then the third root of $q(t)$ must also be in F'. Therefore, F' is a splitting field of $q(t)$.

Now $F = \mathbf{F}_3[u]/\langle u^3 + 2u + 1\rangle = \{au^2 + bu + c \colon a, b, c \in \mathbf{F}_3\}$ is a field with cardinality $3^3 = 27$. Similarly, F' is a field with cardinality $3^3 = 27$. Let $\phi : F \to F'$ be given by $\overline{u} \mapsto \bar{t}$ and extending by linearity. The map ϕ is clearly a homomorphism. Since $\overline{1} \mapsto \overline{1}$, the map is nonzero. Since maps between fields are either injective or the zero map, it must be that ϕ is injective. But then ϕ is a injective map between finite sets, hence surjective. But then ϕ is an isomorphism.

□

7. Let R be a PID and let M be a finitely generated torsion-free R-module.

(a) Let S be a finite set of elements generating M. Prove that S contains a maximal linearly independent subset.

(b) Prove that M is free by showing that it is isomorphic to a submodule of a free R-module.

8. Let $R = \mathbb{C}[x, y]$ be the polynomial ring in two indeterminates over the complex numbers. Let $I = \langle x, y \rangle$. Prove or disprove: I is a free R-module.

Solution: We prove something stronger: let I be an nontrivial ideal of a commutative ring R with identity. Then I is a free module if and only if it is a principal ideal generated by a nonzerodivisor. We proceed with this proof:

Suppose that $I \lhd R$ be a free R-module. Let $\{x_\alpha\}_\alpha$ be a basis for I, not necessarily countable. Observe that if we choose $a, b \in \{x_\alpha\}_\alpha$, where a, b are distinct, we have $ab + (-ab) = 0$ is a nontrivial relation, contradicting the fact that $\{x_\alpha\}_\alpha$ is a basis. Then it must be that $I = (x)$ for some $x \in R$. We only need show that x is a non-zerodivisor. Suppose that x were a zero divisor, then there is a $0 \neq y \in x$ such that $xy = 0$, contradicting the fact that $\{x\}$ is a basis for I. Then $I = (x)$ is a principal ideal generated by a non-zerodivisor.

Now assume that $I = (x)$ is a principal ideal generated by a non-zerodivisor. The result is then immediate as $I = Rx$ so that $\{x\}$ serves as a basis for I so that I is free. To confirm this, observe that if $ax = 0$ for $0 \neq a \in R$, then x is a zero divisor, contrary to the assumption.

This proves the claim. Now in our case, $R = k[x, y]$, where k is a field, is a commutative ring with identity. Clearly, I is an ideal of R (in fact it is maximal as $R/(x, y) \cong k$, a field). It then suffices to show that (x, y) is not principal.

Suppose (x, y) were principal, i.e. $(x, y) = (f)$ for some polynomial $f \in R$. Then g would divide x, y, both of which are irreducible and not associated. But then g would be a unit so that $(x, y) = R$, a contradiction.

OR

If $(x, y) = (f)$ for some $f \in R = k[x, y]$, then for $g(x, y), h(x, y) \in R$, there exists $m(x, y) \in R$ so that $gx + hy = mf$. But then $x = m_1 f$ and $y = m_2 f$ for some $m_1, m_2 \in R$. In particular, f is a polynomial of at most degree 1 in x and y. Hence, $f = ax + bc + c$ for some $a, b, c \in k$. BUt then $x = m_1(ax + by + c)$, implying $b = 0$. Similarly, $y = m_2(ax + c)$ so that $a = 0$. But then f has degree 0, i.e. $f \in k$ is a unit. But then $(x, y) = (f) = R = k[x, y]$, a contradiction.

OR

For principal ideals I, J in an integral domain, $I \subseteq J$ if and only if $J \mid I$. Now as x is irreducible, the only principal ideal containing (x) is $(1) = R = k[x, y]$. But $(x, y) \neq 1$ as evaluating at $x = y = 0$ would give a contradiction. Therefore, (x, y) cannot be principal. □

9. Prove that every square matrix with entries in the field of complex numbers is similar to its transpose. Hint: A theorem about a certain canonical form for matrices may come in

handy.

Solution: Let A be a square matrix over $\mathbb{C}$. Consider the Jordan canonical form for A, J. If the Jordan canonical form for A consists of a single Jordan block, its transpose consists of the eigenvalue λ along the diagonal and 1's directly underneath each λ (except the bottom-right most λ). Let P be the matrix with $P_{ij} = 1$ if $i + j = n$ and 0 otherwise. Left multiplication by P reverses order of the rows while right multiplication by P reverses the order of the columns. But then $J^T = PJP^{-1}$. [Note that $P^{-1} = P$.] Now A is similar to J, which is similar to J^T, which is similar to A^T. Since similarity is transitive, A is similar to A^T.

Now if the Jordan canonical form for A is the diagonal matrix consisting of Jordan blocks $J_1, \ldots, J_n$. For each Jordan block J_i, construct P_i as above so that $J_i^T = P_i J_i P_i^{-1}$. But then let P be the block diagonal matrix consisting of $P_1, \ldots, P_n$. We have $J^T = PJP^{-1}$. Now A is similar to J, which is similar to J^T, which is similar to A^T. Since similarity is transitive, A is similar to A^T. Therefore, A is similar to A^T.

OR

Let A be a square matrix over $\mathbb{C}$. The Smith normal form over $\mathbb{C}[x]$ of $XI_n - A$ and $XI_n - A^T$ are the same by symmetry. But then A and A^T have the same invariant factors. But then A and A^T must have the same rational canonical form. Hence, A and A^T have the same Jordan canonical form. Since a matrix is similar to its Jordan canonical form and similarity is transitive, A and A^T are similar. □

May 2016

1. Let G be a finite group and H, K subgroups.

(a) Prove that the number of distinct conjugates of K by elements of H is $|H : H \cap N_G(K)|$, where $N_G(K)$ is the normalizer of K in G.

(b) Take $H = G$ in part (a) to conclude that G is not the union of all the conjugates of K.

2. Consider A_5, the alternating group on 5 letters, a simple group of order $60 = 2^2 \cdot 3 \cdot 5$.

(a) Prove that every element of A_5 has prime-power order, and conclude that A_5 is the union of its Sylow subgroups.

(b) Compute the number of Sylow p-subgroups for $p = 3, 5$.

3. Write $\langle\ ,\ \rangle$ for the standard Euclidean dot product on $\mathbb{R}^n$, and $\|\ \|$ for the standard Euclidean norm, so that $\|x\|^2 = \langle x, x\rangle$. Let A be an $n \times n$ real matrix. Prove that the following conditions (for A to be orthogonal) are equivalent.

(i) $A^T A = I_n$, the $n \times n$ identity matrix.

(ii) $\|Ax\| = \|x\|$ for all $x \in \mathbb{R}^n$.

(iii) $\langle Ax, Ay\rangle = \langle x, y\rangle$ for all $x, y \in \mathbb{R}^n$.

(iv) The columns of A are orthonormal.

Solution:
(i)$\rightarrow$(ii): Observe for all $x \in \mathbb{R}^n$,

$$\|Ax\|^2 = \langle Ax, Ax\rangle = (Ax)^T(Ax) = x^T A^T Ax = x^T I_n x = x^T x = \langle x, x\rangle = \|x\|^2.$$

Therefore, $\|Ax\| = \|x\|$ for all $x \in \mathbb{R}^n$.

(ii)$\rightarrow$(iii): For all $x, y \in \mathbb{R}^n$,

$$\begin{aligned}\langle Ax, Ay\rangle + \langle Ax, Ax\rangle + \langle Ay, Ax\rangle + \langle Ay, Ay\rangle &= \langle A(x+y), A(x+y)\rangle \\ &= \|A(x+y)\|^2 \\ &= \|x+y\|^2 \\ &= \langle x+y, x+y\rangle \\ &= \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle\end{aligned}$$

Hence, we have shown

$$\langle Ax, Ay\rangle + \langle Ay, Ax\rangle + \|Ax\|^2 + \|Ay\|^2 = \langle x, y\rangle + \langle y, x\rangle + \|x\|^2 + \|y\|^2.$$

But as $\langle Ax, Ax\rangle = \|x\|$ and $\langle Ay, Ay\rangle = \|y\|^2$, this implies that $2\langle Ax, Ay\rangle = 2\langle x, y\rangle$ (using the fact that $\langle \cdot\,, \cdot\rangle$ is symmetric) so that $\langle Ax, Ay\rangle = \langle x, y\rangle$.

(iii)→(iv): Let $e_1, \ldots, e_n$ be the standard basis vectors for $\mathbb{R}^n$. The columns of A, say a_i is the ith column, are given by $a_i = Ae_i$ for $i = 1, \ldots, n$. Then

$$\langle a_i, a_j\rangle = \langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle = \delta_{i,j}$$

for all $i, j \in \{1, \ldots, n\}$. But then the columns of A are orthogonal.

(iv)→(i): Using the notation from above, we have

$$A^TA = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} a_1^Ta_1 & \cdots & a_1^Ta_n \\ \vdots & \ddots & \vdots \\ a_n^Ta_1 & \cdots & a_n^Ta_n \end{pmatrix} = (b_{i,j})_{i,j=1,\ldots,n}$$

where $b_{i,j} = a_i^Ta_j = \delta_{ij}$. But then $A^TA = (\delta_{i,j})_{i,j=1,\ldots,n} = I_n$. □

4. Let $\langle\ ,\ \rangle$ be a symmetric bilinear form of $\mathbb{R}^n$, and let A be the matrix of the form with respect to some basis. True or false: the eigenvalues of A are independent of the choice basis. Justify.[15]

5.

(a) Find an isomorphic direct sum of cyclic groups for an abelian group A generated by x, y, z with the relations $x + y = 0$, $2x = 0$, $4x + 2z = 0$, and $4x + 2y + 2z = 0$.

(b) Prove that $\mathbb{Q}$, the additive group of rational numbers, is not a free $\mathbb{Z}$-module.

6.

(a) Given a field F and any elements $a_1, \ldots, a_n \in F$, $n \geq 1$, denote by $\phi : F[x_1, \ldots, x_n] \to F$ the unique ring homomorphism satsifying $\phi(x_i) = a_i$, $i = 1, \ldots, n$. Find an explicit finite set of generators for the ideal $\ker\phi$ of $F[x_1, \ldots, x_n]$. Is $\ker\phi$ a prime ideal?

[15]The statement is false if you take a general field. Consider $V = k$, where k is a field of characteristic not 2, having at least four elements. Now $f(x, y) = xy$ is a symmetric bilinear form. Choose a basis $B = \{b\}$. Now the matrix for f is $A = (b^2)$. But one can choose nonzero $b, b' \in K$ with $b^2 \neq (b')^2$.

(b) Let $M = F[x]/I$ where I is a proper ideal of $F[x]$. Viewing M as an $F[x]$-module, state and prove the necessary and sufficient condition (in terms of the decomposition of I into a product of prime ideals of $F[x]$) for when M is indecomposable.

7. The characteristic polynomial of a square matrix with complex entries is $(x-2)^3(x^2+1)^2$ and the minimal polynomial is $(x-2)^2(x^2+1)$. List all possible Jordan canonical forms of the matrix.

8. Let $K = \mathbb{Q}(-2-i, 1+\sqrt{3})$ be the subfield of $\mathbb{C}$ obtained by adjoining the elements $-2-i$ and $1+\sqrt{3}$ to $\mathbb{Q}$.

(a) Find the degree $[K : \mathbb{Q}]$ of the field extension $K/\mathbb{Q}$.

(b) Describe explicitly each automorphism in the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

(c) Describe $\mathrm{Gal}(K/\mathbb{Q})$ abstractly: what well known group is isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$?

(d) Is $K/\mathbb{Q}$ a Galois extension? Explain.

(e) Is K a splitting field of a polynomial in $\mathbb{Q}[x]$? If yes, find such a polynomial. If no, explain why.

(f) Find all the intermediate fields L satisfying $\mathbb{Q} \subsetneq L \subsetneq K$.

August 2016

1. Let G be a group that may either be infinite or finite. Let N be a normal subgroup of G. Assume that $[G : N]$ is finite. Prove that there are only finitely many subgroups H of G such that $N \subseteq H \subseteq G$.

2. Let V be a vector space and let $W_1, \ldots, W_n$ be subspaces of V. We say that $W_1, \ldots, W_n$ are *independent* if and only if the following condition holds:

$$\begin{aligned}&\text{If } w_1 + \cdots + w_n = 0 \text{ with } w_i \in W_i \text{ for all } i = 1, \ldots, n,\\ &\text{then } w_i = 0 \text{ for all } i = 1, \ldots, n.\end{aligned}$$

Now to make life a little easier, we consider only three subspaces W_1, W_2, W_3. For each of the following statements either prove if or provide a counterexample and disprove it.

(a) W_1, W_2, W_3 are independent if and only if $W_1 \cap W_2 = \{0\}$ and $(W_1 + W_2) \cap W_3 = \{0\}$.

(b) W_1, W_2, W_3 are independent if and only if $W_i \cap W_j = \{0\}$ for all $1 \leq i < j \leq 3$.

Solution:

(a) We prove a more general result: if M is a R-module and $W_1, \ldots, W_n$ are R-submodules, then $M = W_1 \oplus W_2 \oplus \cdots \oplus W_n$ if and only if $W_i \cap (W_1 + \cdots + \hat{W}_i + \cdots + W_n) = \{0\}$, where $\hat{W}_i$ indicates W_i is omitted from the sum.

If $M = W_1 \oplus W_2 \oplus \cdots \oplus W_n$ and $m \in W_i \cap (W_1 + \cdots + \hat{W}_i + \cdots + W_n)$, then $m = m_i$ for some $m_i \in W_i$ and $m_i = \sum_{j \neq i} r_j m_j$, where $m_j \in W_j$ and $r_j \in R$. But if $r_j \neq 0$ for all j, then

$$0 = -m_i + \sum_{j \neq i} r_j m_j = 0 + 0 + \cdots + 0$$

has two distinct expressions, a contradiction. Then $m_i = \sum_{j \neq i} r_j m_j = \sum_{j \neq i} 0 \cdot m_j = 0$.

Now assume that $V = W_1 + W_2$, where $W_1 \cap W_2 = \{0\}$. It is then immediate that $V = W_1 \oplus W_2$. Assume then that the result holds for $n = k$. Define $V' = W_1 + \cdots + W_k$ so that $V = V' + W_{k+1}$. Now by hypothesis, $V' = W_1 \oplus \cdots \oplus W_k$. If $v \in V$, we have $v = w' + x$, where $w' \in V'$ and $x \in W_{k+1}$. Since the expression for w' is unique and $W_i \cap (W_1 + \cdots + \hat{W}_i + \cdots + W_n) = \{0\}$, the expression for v is unique. [If there were two: $v = w_1' + x_1 = w_2' + x_2$, then $0 = (w_1' - w_2') + (x_1 - x_2)$. Since $W_i \cap (W_1 + \cdots + \hat{W}_i + \cdots + W_n) = \{0\}$ and the expression in V' is unique $w_1' = w_2$. But then $x_1 - x_2 = 0$ so that $x_1 = x_2$.] Therefore, $V = W_1 \oplus \cdots \oplus W_{k+1}$. The result then follows by induction.

Now the stated result follows with V a k-module, i.e. a vector space with submodules (subspaces) W_1, W_2, W_3.

(b) The statement if false. Let V be a vector space of dimension 2 over k. Let $\{x, y\}$ be a basis for V. Then $V = X \oplus Y$, where X is the subspace spanned by x and Y is the space spanned by y. Let Z be the space spanned by $x + y$. Observe that $X \cap Y = \{0\}$, $Y \cap Z = \{0\}$, and $X \cap Z = \{0\}$. We have $V = X + Y + Z$ but X, Y, Z are not independent as $0 = 0 + 0 + 0$ and $0 = (x + y) + (-x) + (-y)$.

□

3. Prove that there is no simple group of order 30.

Solution: Let G be a group of order 30 and let n_p denote the number of Sylow p-subgroups of G. Observe $|G| = 30 = 2 \cdot 3 \cdot 5$. By Sylow's Theorem, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 6$. Therefore, $n_5 \in \{1, 6\}$. Similarly, we know $n_3 \equiv 1 \mod 3$ and $n_3 \mid 10$. Therefore, $n_3 \in \{1, 10\}$. At least one of n_3 or n_5 is 1 since otherwise

$$30 = |G| \geq 1 + 10(3 - 1) + 6(5 - 1) = 1 + 20 + 24 = 45,$$

a contradiction. But then G contains a unique, hence normal, Sylow subgroup. Therefore, G cannot be simple.

OR

By Cayley's Theorem, if G is a group of order 30, then G is isomorphic to a subgroup of S_{30}. Now G acts on G by right translation and the only identity fixes any point under this action. Therefore, this embedding of G into S_{30} has no fixed point. By Cauchy's Theorem, there must be an element of order 2 in G. This element is represented (by the embedding of G into S_{30}) as a product of 15 2-cycles. But then this representation is an odd permutation. The elements of G represented by an even permutation form a normal subgroup of index 2. However, index 2 subgroups are always normal. Therefore, G cannot be simple.[16] □

4. Let G be a group with $|G| = 55$ and let S be a set with $|S| = 24$. Assume that G acts on S. Prove that the action has at least two points.

Solution: For $s \in S$, let $\text{stab}_G(s)$ denote the stabilizer of s and $\text{orb}(s)$ denote the orbit of s. By the Orbit-Stabilizer Theorem $|G| = |\text{stab}_G(s)||\text{orb}(s)|$. Furthermore, $\text{stab}_G(s) \leq G$ so that by Lagrange's Theorem $|\text{stab}_G(s)| \mid |G|$. Therefore for all $s \in S$, $|\text{stab}_G(s)| \in \{1, 5, 11, 55\}$. But then for all $s \in S$, $|\text{orb}(s)| \in \{55, 11, 5, 1\}$. Let x denote the number of distinct orbits of size 55, y denote the number of distinct orbits of size 11, z denote the number of distinct orbits of size 5, and w denote the number of distinct orbits of size 1. Note that $|\text{orb}(s)| = 1$ if and only if $|\text{stab}_G(s)| = |G|$ if and only if s is a fixed point of G.

[16] This same proof works for any group of order $2n$, where $n > 1$ is odd. Therefore, there are no simple groups of order $2n$, where n is odd.

The set of distinct orbits partition S. Therefore, $55x + 11y + 5z + w = 24$ with $x, y, z, w \in \mathbb{Z}_{\geq 0}$. It is clear then that $x = 0$ so that $11y + 5z + w = 24$. It is clear that $0 \leq y \leq 2$ and $0 \leq z \leq 4$. Furthermore, if $z > 2$, then $11y = 24 - 5z - w < 14$ so that $y \leq 1$. Also, if $y > 0$, then $5z = 24 - 11y - w < 13$ so that $z \leq 2$. If S had no fixed point under the action of G, then $w = 0$. Then $11y + 5z = 24$.

The only possible solutions are

$$y = 0, z = 0 y = 0, z = 1 y = 0, z = 2 y = 0, z = 3 y = 0, z = 4 y = 1, z =$$

5. Does there exist a Hermitian matrix with characteristic polynomial equal to $x^4 - 1$? If there does, construct one and prove it is one. If there does not, prove there does not. You will get no points for a simple yes or no without supporting reasoning.

6. Let R be a UFD and I a **proper principal** ideal. Prove that R has a proper principal ideal that is maximal with respect to the property of containing I and identify its generator in terms of the generator of I.

7. Let R be a commutative ring and I an ideal of R. Define the *radical* of I to be the ideal

$$\sqrt{I} \stackrel{\text{def}}{=} \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}$$

(a) Prove that $\sqrt{I}$ is an ideal of R.

(b) Define an ideal I to be *primary* if, for each element $r \in R$, its image $\overline{r}R/I$ is either nilpotent (that is, $\overline{r}^m = 0$ for some $m \geq 1$) or a nonzerodivisor.

If I is a primary ideal, prove that $\sqrt{I}$ is a prime ideal.

Solution:

8.

(a) Find all the possible rational canonical forms for a 8×8 matrix A over $\mathbb{Q}$ that satisfies $(A - 3I)^3(A^2 + 1) = 0$ and has *characteristic polynomial* $(x - 3)^4(x^2 + 2)^2$.

(b) Find the Jordan canonical forms (over $\mathbb{C}$) for the matrices from part (a).

(c) If, in addition to the information above, you also know that A satisfies

$$\dim \ker(A - 3I) = 2 \quad \dim \ker(A - 3I)^2 = 4$$

what is the Jordan canonical form of A? Why?

9. Let K be the splitting field of the polynomial $p(x) = x^4 - 2 \in \mathbb{Q}[x]$.

(a) Show K is equal to an extension of the form $\mathbb{Q}(\alpha, \zeta)$, where α is a real number and ζ is a roof of unity (which one?).

(b) Find the degree of the extension $K/\mathbb{Q}$. Justify completely.

(c) Determine whether the extension $K/\mathbb{Q}$ is Galois. Justify your answer. If it is Galois, find the cardinality of its Galois group.

(d) Determine the group of automorphisms $\mathrm{Aut}(K/\mathbb{Q})$ (as an abstract group) using the information above. Justify completely for any credit.
Hint: Determine all the automorphisms $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ in terms of α and ζ.

10.

(a) Let $K = \mathbb{Q}(\zeta, \sqrt[5]{5})$, where ζ is a primitive 7th root of unity. Find the degree of the extension $K/\mathbb{Q}$.

(b) Let $K = \mathbb{F}_2(\alpha)$, where α is a nonzero root of $x^4 + x^2 + x \in \mathbb{F}_2[x]$. Determine whether the polynomial is separable. Find the degree of the extension $K/\mathbb{F}_2$ and the cardinality of K.

May 2017

1. Let G be a group of order 30.

(a) Prove that either the Sylow 5-subgroup K or the Sylow 3-subgroup H is normal.

(b) Prove that HK is a cyclic subgroup of G.[17][18]

Solution:

(a) Let n_p denote the number of Sylow p-subgroups of G. We know that $n_5 \equiv 1 \mod 5$ and $n_p \mid 6$. This implies $n_5 \in \{1, 6\}$. Furthermore, $n_3 \equiv 1 \mod 3$ and $n_3 \mid 10$. This implies $n_3 \in \{1, 10\}$. If $n_5 \neq 1$ and $n_3 \neq 1$, then $n_5 = 6$ and $n_3 = 10$. Then we must have

$$|G| \geq 1 + 6(5-1) + 10(3-1) = 1 + 24 + 20 = 45,$$

a contradiction. Therefore, at least one of n_3, n_5 is 1. But then G contains either a unique Sylow 3-subgroup or a unique Sylow 5-subgroup. Since unique Sylow subgroups are normal, either H is normal or K is normal.

(b) By (a), either H or K is normal. But then HK is a subgroup of G. Now as $|G| = 2 \cdot 3 \cdot 5$, $|H| = 3$ and $|K| = 5$. By Lagrange's Theorem, it must be that H and K are cyclic since they are of prime order. Furthermore by Lagrange's Theorem since $\gcd(|H|, |K|) = 1$, we know that $H \cap K = \{1\}$. But then $|HK| = \frac{|H||K|}{|H \cap K|} = 3 \cdot 5 = 15$. But every group of order 15 is cyclic: if $\mathcal{G}$ is a group of order 15, then $n_3 \equiv 1 \mod 3$ and $n_3 \mid 5$. But then $n_3 = 1$. Similarly, $n_5 = 1$. But then both Sylow subgroups of $\mathcal{G}$ are unique, hence normal, and then $\mathcal{G}$ is a product of cyclic subgroups of relatively prime order. Therefore, $\mathcal{G}$ is cyclic. Furthermore, we can even say HK is normal in G as its is an index 2 subgroup of G.

□

2. Let G be a group with subgroup H (the subgroup need not be normal). If G acts on a set X from the left, then we will say that X is a *left G-set*.

The set G/H of left cosets of H in G is a left G-set by means of $g \circ xH = gxH$, $g, x \in G$.

[17] It is generally true that if p, q are distinct primes with $p < q$, if $q \not\equiv 1 \mod p$, then all groups of size pq are cyclic (hence isomorphic) and if $q \equiv 1 \mod p$, then up to isomorphism there are two groups of size pq: Now let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. We know $n_p \mid q = \frac{|G|}{p}$ and $n_p \equiv 1 \mod p$. Then $n_p \equiv 1$ or q but $q \not\equiv 1 \mod p$ by assumption. Therefore, $n_p = 1$. Similarly, $n_q = 1$. Then P, Q are normal subgroups of G. Since P, Q are cyclic, let their generators be x, y, respectively. We know $P \cap Q = \{1\}$. Now $xyx^{-1}y^{-1} \in H \cap K$ as $xyx^{-1} \in K$ by normality. Similarly, $yx^{-1}y^{-1} \in H$. Therefore, $xy = yx$. Since $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq$ so that $PQ = \langle xy \rangle$. Thus, HK is cyclic.

[18] In fact, if G is a group of order pqr, where $p < q < r$ are primes, then one of the Sylow subgroups is normal.

(a) For $a \in G$, compute the stabilizer G_{aH} of aH.

(b) Let X, Y be left G-sets. A map $\phi : X \to Y$ is a *homomorphism* if $\phi(gx) = g\phi(x)$ for all $g \in G$, $x \in X$, and it is an *isomorphism* if there exists a homomorphism $\psi : Y \to X$ satisfying $\psi\phi = 1_X$ and $\phi\psi = 1_Y$. The G-sets X, Y are *isomorphic* if there exists an isomorphism $X \to Y$. For $x \in X$, denote G_x the stabilizer of x.

  (i) If $\phi : X \to Y$ is a homomorphism of G-sets, prove that $G_x \leq G_{\phi(x)}, x \in X$.

  (ii) If $\phi : X \to Y$ is an isomorphism, prove that $G_x = G_{\phi(x)}, x \in X$.

(c) Let H, K be subgroups of G.

  (i) If G/H and G/K are isomorphic G-sets, prove that H and K are conjugate subgroups of G. *Hint:* use (a) and part (ii) of (b).

  (ii) Prove the converse of (i). *Hint.* Use a relevant theorem, or construct an isomorphism explicitly: if $H = aKa^{-1}$ for some $a \in G$, right multiplication by a is a bijective map $G \to G$.

Solution:

(a)

$$\begin{aligned} g \in G_{aH} &\iff gaH = aH \\ &\iff a^{-1}gaH = H \\ &\iff (a^{-1}ga)H = H \\ &\iff a^{-1}ga \in H \\ &\iff a^{-1}ga = h \text{ for some } h \in H \\ &\iff g = aha^{-1} \\ &\iff g \in \{aha^{-1} \mid h \in H\} \\ &\iff g \in N_a(H) \end{aligned}$$

(b,i) Let $g \in G_x$ so that $gx = x$. But then

$$\phi(x) = \phi(gx) = g\phi(x)$$

so that $g \in G_{\phi(x)}$. But then $G_x \leq G_{\phi(x)}$.

(b,ii) Let $\phi : X \to Y$ be an isomorphism with inverse $\psi : Y \to X$. By the previous part, we know that $G_x \leq G_{\phi(x)}$. But also by the previous part, we have $G_{\phi(x)} \leq G_{\psi(\phi(x))}$, but $G_{\psi(\phi(x))} = G_x$. Therefore, $G_x = G_{\phi(x)}$.

(c,i) Suppose that $G/H \cong G/K$. Then there is a map $\phi : G/H \to G/K$ that is an isomorphism with inverse $\psi : G/K \to G/H$. Then there is a $g \in G$ (not necessarily unique) such that

$$\phi(1H) = \phi(H) = gK$$

Now let $h \in H$. Then

$$gK = \phi(H) = \phi(hH) = h\phi(H) = hgK$$

But then $h \in G_{gK}$ so $g^{-1}hg \in K$. But then $g^{-1}Hg \leq K \leftrightarrow H \leq gKg^{-1}$. Applying this same logic to ψ and K gives $\psi(K) = g^{-1}H$ so that $gKg^{-1} \leq H$. This shows that $H = gKg^{-1}$ for some $g \in G$ (again, not necessarily unique). But then H and K are conjugate subgroups.

(c,ii) Suppose that H, K are conjugate subgroups in G. Then there is a $g \in G$ (not necessarily unique), such that $H = gKg^{-1}$. Define $\phi : G/H \to G/K$ be given by $rH \mapsto rgK$. We need show that this map is well defined, a homomorphism, injective, and surjective. Suppose that $rH = sH$. Then $H = r^{-1}sH$ so that $r^{-1}s \in H$. That is, $r^{-1}s = h$ for some $h \in H$. This shows $s = rh$. Then $\phi(sH) = \phi(rhH) = \phi(rH)$ so that ϕ is well defined. We need see that ϕ is a homomorphism. But this follows easily as if $g \in G$ and $rH \in G/H$, then

$$\phi(grH) = grgK = g(rgK) = g\phi(rH)$$

To see injectivity, suppose that $\phi(rH) = \phi(sH)$. Then $rgK = sgK$ so that $K = g^{-1}r^{-1}sgK$. But this shows that $g^{-1}r^{-1}sg \in K$. Then there is a $k \in K$ such that $g^{-1}r^{-1}sg = k$. Therefore, $r^{-1}s = gkg^{-1}$. By assumption, $gkg^{-1} \in H$ so that there is an $h \in H$ such that $r^{-1}s = h$. This shows that $s = rh$. This finally shows $sH = rhH = rH$. Therefore, ϕ is injective. Now let $sK \in G/K$. Take $r = sg^{-1}$ and observe $\phi(rH) = rgK = sg^{-1}gK = sK$ so that ϕ is surjective. Therefore, ϕ is an isomorphism and $G/H \cong G/K$.

□

3. For each permutation $\sigma \in S_n$ denote by $f(\sigma) : \mathbb{R}^n \to \mathbb{R}^n$ the linear operator given by $f(\sigma)(e_j) = e_{\sigma(j)}$, $j = 1, \ldots, n$. Prove that:

(a) $f(\sigma)$ is an orthogonal linear operator.

(b) The map $f : S_n \to \mathrm{GL}(\mathbb{R}^n)$ sending each σ to $f(\sigma)$ is a monomorphism of groups.

(c) What are the eigenvalues of $f(\sigma)$? Is $f(\sigma)$ diagonalizable? Explain.

4. Prove that

(a) The matrix, relative to any basis, of a positive definite hermitian form on the complex vector space $\mathbb{C}^n$ is nonsingular.

(b) For any complex $n \times n$ matrix A, the matrix $I + A^*A$ is nonsingular, where I is the $n \times n$ identity matrix and A^* is the conjugate transpose of A.

5. Let I and J be ideals of a commutative ring R with identity. Assume that $I + J = R$[19].

(a) Prove that $IJ = I \cap J$.[20]

(b) Prove that $R/I \times R/J \cong R/IJ$.[21]

Solution:

(a) It is clear that IJ and $I \cap J$ are ideals. Consider $ij \in IJ$, where $i \in I$ and $j \in J$. Since R is commutative and I, J are ideals, we have $ij = ji \in I$ and $ij \in J$ so that $ij \in I \cap J$. Now if $x \in IJ$, then $x = i_1j_1 + \cdots + i_nj_n$, where $i_1, \ldots, i_n \in I$ and $j_1, \ldots, j_n \in J$. By the work above, $i_rj_r \in I \cap J$ for $r = 1, \ldots, n$. But then $x = i_1j_1 + \cdots + i_nj_n \in I \cap J$. Therefore, $IJ \subseteq I \cap J$.

Now suppose $x \in I \cap J$. Now $1 \in R = I + J$ so that $1 = i + j$ for some $i \in I$ and $j \in J$. Then $x = 1 \cdot x = (i + j)x = ix + jx$. But since $x \in I \cap J$, $x \in I$ and $x \in J$ so that $ix \in I$ and $jx \in J$. But we also have $ix \in J$ and $jx \in I$. Then $ix, jx \in I \cap J$ so that $ix + jx \in I \cap J$. Therefore, $x = ix + jx \in I \cap J$, proving $I \cap J \subseteq IJ$. Therefore, $IJ = I \cap J$. Alternatively on the level of ideals,

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) = I(I \cap J) + J(I \cap J) \subseteq IJ + JI = IJ + IJ = IJ.$$

Since we have $IJ \subseteq I \cap J$, we must have $IJ = I \cap J$.

(b) First, we prove that if $I + J = R$, then if $a + I \in R/I$ and $b + J \in R/J$, there exists $r \in R$ such that $r + I = a + I$ and $r + J = b + J$. Since $I + J = R$, there exist $i \in I$ and $j \in J$ such that $i + j = 1$. Then consider $r := bi + aj$. We have $(bi + aj) + I = aj + I = (aj + ai) + I = a(i + j) + I = a + I$ in R/I and $(bi + aj) + J = bi + J = (bi + bj) + J = b(i + j) + J = b + J$ in R/J.

[19] Such ideals are coprime

[20] If R is a commutative ring, it is always the case that $IJ \subseteq I \cap J$. It is not the case that $IJ = I \cap J$: Take $a \in \mathbb{Z}_{>1}$. Now let $I = (a)$ and $J = (a)$. Then $IJ = (a^2)$ and $I \cap J = (a)$. Since $a \in I \cap J$ and $a \notin (a^2)$, we have $IJ \subsetneq I \cap J$. Even if $I + J = R$ with R commutative, it is not the case that $IJ = I \cap J$, R need have identity: let G be a nontrivial finite abelian group. Make G into a ring by defining multiplication $g \cdot g' = 0$ for all $g, g' \in G$. Then R given by $(G, +, \cdot)$ is a ring. Take $I = J = R$. Clearly, I, J are ideals of R. We have $I + J = R + R = R$, $I \cap J = R \cap R = R$, $IJ = RR = 0$ so that $IJ \neq I \cap J$.

[21] This is a simple case of the Chinese Remainder Theorem.

Now consider the map $\phi : R \to R/I \times R/J$ given by $r \mapsto (r+I, r+J)$. We first show ϕ is a homomorphism. Observe $\phi(1) = (1+I, 1+J)$ and $\phi(0) = (0+I, 0+J) = (I, J)$. If $r, s \in R$, then

$$\begin{aligned}\phi(r+s) = \big((r+s)+I, (r+s)+J\big) &= \big((r+I)+(s+I), (r+J)+(s+J)\big) \\ &= (r+I, r+J) + (s+I, s+J) = \phi(r) + \phi(s) \\ \phi(rs) = (rs+I, rs+J) = \big((r+I)(s+I), (r+J)(s+J)\big) &= (r+I, r+J)(s+I, s+J) \\ &= \phi(r)\phi(s).\end{aligned}$$

Therefore, ϕ is a ring homomorphism. By the work above, if $(a+I, b+J) \in R/I \times R/J$, then there exists $r \in R$ such that $\phi(r) = (a+I, b+J)$. Therefore, ϕ is surjective. Now if $r \in IJ = I \cap J$ (using part (a)), then $\phi(r) = (r+I, r+J) = (0+I, 0+J)$ so that $r \in \ker\phi$. But if $r \in \ker\phi$, $(0+I, 0+J) = \phi(r) = (r+I, r+J)$ so that $r \in I$ and $r \in J$, i.e. $r \in I \cap J = IJ$. Therefore, $\ker\phi = IJ$. Then by the First Isomorphism Theorem, $R/IJ \cong R/I \times R/J$.

□

6. Let A be a complex matrix with characteristic polynomial $c_A(x) = (x+1)^7(x-2)^5$. Assume the following data about A, where I is the identity matrix of the appropriate size:

$$\begin{aligned}\text{null}(A+I) &= 4 \\ \text{null}(A+I)^2 &= 5 \\ \text{null}(A-2I) &= 3\end{aligned}$$

(a) Write down the possible Jordan canonical forms for A.

(b) If in addition you know that $(A-2I)^2 = 4$, what is the minimal polynomial of A?

This is a computational problem, and minimal justification is required.

7. Let $F \subseteq K$ be a finite field extension. Prove that K can be generated by a finite number of elements, each algebraic over F.[22]

Solution: Let K/F be finite and define $n := [K\colon F]$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K as an F-vector space. We know $[F(\alpha_i)\colon F]$ divides $[K\colon F]$ for $i = 1, \ldots, n$. Then $[F(\alpha_i)\colon F] \leq [K\colon F] = n < \infty$. Recalling that a finite extension is algebraic, each α_i is algebraic over F (since the degree of $F(\alpha_i)/F$ is finite). But then K, being generated by $\alpha_1, \ldots, \alpha_n$, is generated by a finite number of algebraic elements over F. □

[22] K/F is finite if and only if K is generated by a finite number of algebraic elements over F. The converse is simple to show.

8. Let K be a splitting field for the polynomial $p(x) = x^7 - 2 \in \mathbb{Q}[x]$. Completely justify your responses to each of the following questions.

(a) What is $[K\colon \mathbb{Q}]$?

(b) Is K a Galois extension of $\mathbb{Q}$?

(c) Is every permutation of the roots of $p(x)$ given by an automorphism of K?

(d) Is $\mathrm{Aut}_{\mathbb{Q}}(K)$? abelian?

August 2017

1. Let $A \leq B \leq G$ be subgroups of a group G. Recall that a subgroup H of a group G is called *characteristic*, if it is invariant under every automorphism of G, that is, $f(H) = H$ for every automorphism f of G. (In particular, by looking at all the inner automorphisms, one sees that every characteristic subgroup is normal.)

(a) Show that if A is characteristic in B, and B is normal in G, then A is normal in G.

(b) Show that if B is cyclic and normal in G, then A is normal in G.

Solution:

(a) Let $g \in G$. We need show that $gAg^{-1} = A$. Now B is normal in G so that $gBg^{-1} = B$; that is, conjugation by g is an automorphism of B. But A is characteristic in B so that conjugation by g must fix A, i.e. $gAg^{-1} = A$, as desired.

(b) Let $g \in G$. Since B is cyclic and $A \leq B$, A must be cyclic. However, cyclic groups have unique subgroups. Since order is preserved under automorphisms, any automorphism of B must send A to itself. But then A is characteristic in B. By (a), we know that A is then normal in G.

OR

Since B is cyclic and $A \leq B$, we know that A is cyclic as subgroups of cyclic groups are cyclic. Then if $B = \langle x \rangle$ for some $x \in G$, we know $A = \langle x^j \rangle$ for some integer j. Let $g \in G$. Since B is normal in G, $gxg^{-1} = x^d$ for some integer d. But then for any integer k

$$g(x^j)^k g^{-1} = (gxg^{-1})^{jk} = (x^d)^{jk} = (x^j)^{dk} \in A$$

But then A is normal in G.

□

2. Let A, B and C be three finite abelian groups. Prove or disprove the following statement: "If $A \oplus C \cong B \oplus C$, then "$A \cong B$".[23]

Solution: By the Fundamental Theorem of Finitely Generated Abelian Groups (applying it to the case of finite abelian), we can write $A \cong \mathbb{Z}/p_i^{e_i} \oplus \cdots \oplus \mathbb{Z}/p_k^{e_k}$, $B \cong \mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z} \oplus$

[23] A group C is called cancellable if $A \times C \cong B \times C$ then $A \cong B$. It turns out all finite groups are cancellable and was proven by B. Jónsson and A. Tarski in 1947, see their book *Direct Decompositions of Finite Algebraic Systems*.

$\cdots \oplus \mathbb{Z}/p_{k+n}^{e_{k+n}}\mathbb{Z}$, and $C \cong \mathbb{Z}/q_1^{f_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m^{e_m}\mathbb{Z}$, where p_i, q_i are prime for all i (not necessarily distinct) and $e_i, f_i \in \mathbb{Z}_+$. Then we have

$$A \oplus C \cong \mathbb{Z}/p_i^{e_i} \oplus \cdots \oplus \mathbb{Z}/p_k^{e_k} \oplus \mathbb{Z}/q_1^{f_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m^{e_m}\mathbb{Z}$$
$$B \oplus C \cong \mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_{k+n}^{e_{k+n}}\mathbb{Z} \oplus \mathbb{Z}/q_1^{f_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m^{e_m}\mathbb{Z}$$

The powers of the primes on each side and the number of quotients appearing on each side of the congruences are unique. Therefore, $n = m$ and it must be possible to re-arrange terms so that $q_j = p_{k+j}$ for $1 \leq n \leq n$. But then we must have $A \cong \mathbb{Z}/p_i^{e_i} \oplus \cdots \oplus \mathbb{Z}/p_k^{e_k} \cong B$. □

3.

(a) Let p be a prime number. Let G be a finite group of order $|G| = pn$, where $p > n$. Show that every subgroup H of G of order p is normal.

(b) Let G be a group of order 99, show that G is abelian.

Solution:

(a) Note that n cannot have a factor of p since $p > n$. Let $n_p(G)$ denote the number of Sylow p-subgroups of G. We know that $n_p \mid n$ and $n_p \equiv 1 \mod p$. That is, $n_p \in \{1, p+1, 2p+1, \ldots\}$. However, $p > n$ so that $kp + 1 \nmid n$ for $k \geq 1$. Therefore, it must be that $k = 0$ and $n_p = 1$. But then the Sylow p-subgroup is unique, hence normal.

(b) Observe $|G| = 99 = 3^2 \cdot 11$. We know that $n_{11} \mid 9$ so that $n_{11} = 1$. We know also that $n_3 \mid 11$ so that $n_3 = 1$. Since these subgroups are unique, they are normal in G. Let P_p denote the Sylow p-subgroups. By Lagrange's Theorem, $P_3 \cap P_{11} = \{1\}$. But then we have $G = P_3P_{11}$ and $G \cong P_3 \times P_{11}$. But then G is abelian.

□

4. Let A be a square matrix over $\mathbb{C}$. Let A^* denote its adjoint (i.e., its conjugate transpose).

(a) Prove A^*A has no negative eigenvalues.

(b) Prove that 0 is an eigenvalue of A^*A if and only if A is singular.

Solution:

(a) Let λ be an eigenvalue of A^*A and $0 \neq v$ be an associated eigenvector. Then we have

$$\lambda\|v\| = \lambda\langle v, v\rangle = \langle A^*Av, v\rangle = \langle Av, Av\rangle = \|Av\| \geq 0$$

Therefore, $\lambda \geq 0$.

(b) This is true more generally, a matrix is singular if and only if 0 is an eigenvalue. Applying this claim to the matrix A^*A gives the result—we need only prove the claim. But observe

$$A \text{ singular} \iff \det A = 0 \iff \det(A - 0 \cdot I) = 0 \iff 0 \text{ eigenvalue of } A.$$

□

5.

(a) Suppose that R is a PID. Prove that R does not have an infinite collection of ideals such that $I_1 \subsetneq I_2 \subsetneq I_3 \subseteq \cdots$.[24]

(b) Let R be a commutative ring. A proper ideal $I \subset R$ is called *primary* if for all elements $r, a \in R$ such that $ra \in I$, if $a \notin I$ then $r^k \in I$ for some $k > 0$. For instance, every prime ideal is primary.

If R is a PID, identify all the primary ideals of R.

Solution:

(a) If $I_1 \subsetneq I_2 \subsetneq I_3 \subseteq \cdots$ is a chain of ideals in a PID, then $I = \cup I_k$ is an ideal. Note that $I_k \subseteq I$ for all k. Since R is a PID, $I = (r)$ for some $r \in I$. But since $I = \cup I_k$, $r \in I_k$ for k. But then $I \subseteq I_{k+n} \subseteq I$ for all $n \in \mathbb{N} \cup \{0\}$. Therefore, $I = I_k = I_{k+n}$ for all $n \in \mathbb{N}$.

(b) Recall that if I is an ideal of a commutative ring R, $\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$ — the radical of I. It is clear that $I \subseteq \sqrt{I}$. We show that if I is a nonzero primary ideal in a PID, then $\sqrt{I}$ is prime. Let I be a nonzero primary ideal in a PID, then $I = (r)$ for some nonzero $r \in R$. If $ab \in \sqrt{I}$, then $(ab)^n = a^n b^n \in I$ for some $n \in \mathbb{N}$. Since I is primary, either $a^n \in I$ or $(b^n)^m = b^{nm} \in I$. Without loss of generality, assume $a^n \in I$. Since $aa^{n-1} \in I$, either $a \in I$ or $a^{n-2} \in I$. If $a \in I \subseteq \sqrt{I}$, we are done. If not, $a^{n-2} \in I$. Repeating this process inductively, we see that $a \in I \subseteq \sqrt{I}$. Therefore, I is prime. [In what follows, we use primes. But in a UFD (hence PID), an element is prime if and only if it is irreducible.]

Now if I is a primary ideal in a PID, we know $\sqrt{I}$ is a prime ideal by the work above. In a PID, an ideal is prime if and only if it is of the form (p), where p is prime. Therefore, $\sqrt{I} = (p)$ for some prime $p \in R$. Since I is an ideal in a PID, we can write $I = (r)$ for some $r \in R$. As $p \in \sqrt{I}$, $p^n \in I = (r)$ for some $n \in \mathbb{N}$. But if q is a prime appearing in the factorization of r (R is a UFD since R is a PID), then $q \mid r$ so that $q \mid p^n$. But as p is prime (recalling primes are irreducible), this implies $p = q$, up to associates. Therefore,

[24] Rings which satisfy this property (the ascending chain condition) are called noetherian.

the only prime appearing in the factorization of r is p. Therefore, $r = up^k$ for $k \in \mathbb{N}$ and u a unit in R. Therefore, $I = (r) = (up^k) = (p^k)$.

Finally, suppose $I = (p^k)$, where $k \in \mathbb{N}$ and p is a prime of R. We claim I is primary. Suppose $ab \in I = (p^k) \subseteq (p)$. If $a \in I = (p^k)$, we are done. So suppose $a \notin I$. We have $ab \in (p)$ so that $p \mid ab$. Since p is prime, this implies $a \in (p)$ or $b \in (p)$. But if $a \in (p)$, then $a^k \in (p^k) = I$, a contradiction. Suppose $b \in (p)$, then $b^k \in (p^k) = I$. Therefore, I is primary. This shows that the primary ideals of R are precisely the ideals of the form $I = (p)$, where p is a prime element of R and the zero ideal.

□

6. Let $N \subseteq M$ be R-modules, where R is a ring.

(a) If both N and M/N are free, prove that so is M.[25][26]

(b) If M/N is free, prove that $M \cong (M/N) \oplus N$.[27]

(c) Show with an example that the above need not hold when M/N is not free.

Solution:

(a) If N and M/N are free, they have a basis as an R-module. Let $\{n_\alpha\}_{\alpha \in \mathcal{I}}$ be an R-basis for N, where $n_\alpha \in N$ for all $\alpha \in \mathcal{I}$. Let $\{m_\beta + N\}_{\beta \in \mathcal{J}}$ be a R-basis for M/N, where $m_\beta + N \in M/N$ for all $\beta \in \mathcal{J}$. [Note that $m_\beta \in M$ for all $\beta \in \mathcal{J}$.] Let $m \in M$. In M/N, write $m + N = r_1(m_{\beta,1} + N) + r_2(m_{\beta,2} + N) + \cdots + r_k(m_{\beta,k} + N) = \sum_{i=1}^k r_i(m_{\beta,i} + N)$, where $r_i \in R$. Then $m - \sum_{i=1}^k r_i m_{\beta,i} \in N$ since in M/N

$$\begin{aligned}\left(m - \sum_{i=1}^k r_i m_{\beta,i}\right) + N &= (m+N) - \left[\left(\sum_{i=1}^k r_i m_{\beta,i}\right) + N\right] \\ &= (m+N) - \sum_{i=1}^k (r_i m_{\beta,i} + N) \\ &= (m+N) - \sum_{i=1}^k r_i (m_{\beta,i} + N).\end{aligned}$$

[25]The 'converse' is false: if M is free, it is not necessarily the case that $N, M/N$ is free. Take $M = R$, where R is any integral domain with a non-principal ideal I. There are other prelim problems based on this idea, e.g. August 2012 Problem 7.

[26]Another similar and important exercise is to show that M is noetherian if and only if $N, M/N$ is noetherian.

[27]This is a general concept that is seen in later course work. If M/N is free, then it is projective as an R-module. Since there is an exact sequence $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$, the sequence splits and $M \cong M/N \oplus N$.

Since $m - \sum_{i=1}^{k} r_i m_{\beta,i} \in N$, write $m - \sum_{i=1}^{k} r_i m_{\beta,i} = r_1 n_{\alpha,1} + r_2 n_{\alpha,2} + \cdots + r_q n_{\alpha,q} = \sum_{j=1}^{q} r_j n_{\alpha,j}$, where $r_j \in R$. Therefore, we have

$$m = \sum_{i=1}^{k} r_i m_{\beta,i} + \sum_{j=1}^{q} r_j n_{\alpha,j}.$$

Therefore, $S := \{n_\alpha\}_{\alpha\in\mathcal{I}} \cup \{m_\beta\}_{\beta\in\mathcal{J}}$ spans M as an R-module. It remains to show that the elements of S are linearly independent. Suppose to the contrary that

$$0 = \sum_{i=1}^{k} r_i m_{\beta,i} + \sum_{j=1}^{q} r_j n_{\alpha,j},$$

where the r_i, r_j are not all zero. Then in M/N, we have

$$\begin{aligned}
\overline{0} &= \overline{\sum_{i=1}^{k} r_i m_{\beta,i} + \sum_{j=1}^{q} r_j n_{\alpha,j}} \\
&= \left(\sum_{i=1}^{k} r_i m_{\beta,i} + \sum_{j=1}^{q} r_j n_{\alpha,j}\right) + N \\
&\overset{*}{=} \sum_{i=1}^{k} r_i m_{\beta,i} + N \\
&= \sum_{i=1}^{k} (r_i m_{\beta,i} + N) \\
&= \sum_{i=1}^{k} r_i (m_{\beta,i} + N),
\end{aligned}$$

where $\overset{*}{=}$ follows from the fact that $\sum_{j=1}^{q} r_j n_{\alpha,j} \in N$. But since $\{m_\beta + N\}_{\beta\in\mathcal{J}}$ is a basis for M/N, it must be that $r_i = 0$ for $i = 1, \ldots, k$. But then we have

$$0 = \sum_{i=1}^{k} r_i m_{\beta,i} + \sum_{j=1}^{q} r_j n_{\alpha,j} = \sum_{j=1}^{q} r_j n_{\alpha,j}.$$

However, $\{n_\alpha\}_{\alpha\in\mathcal{I}}$ is a basis for N so that this implies $r_j = 0$ for $j = 1, \ldots, q$. But then S is linearly independent. Therefore, M is a free R-module with basis S. Indeed, $M \cong R^{\text{card}\,(\mathcal{I}\cup\mathcal{J})}$ as R-modules, where card represents set cardinality.

(b) Consider the map $\phi : M \to M/N$, where ϕ is reduction modulo N, i.e. $m \mapsto m + N$. Clearly, this map is surjective: if $m + N \in M/N$, then $\phi(m) = m + N$. Now M/N is a free R-module so that is has a basis. Let $\{m_\alpha + N\}_{\alpha\in\mathcal{I}}$ be an R-basis for M/N,

where $m_\alpha + N \in M/N$ for all $\alpha \in \mathcal{I}$. [Note that $m_\alpha \in M$ for all $\alpha \in \mathcal{I}$.] Define a map $\psi : M/N \to M$ as follows: if $m + N \in M/N$, write $m + N = r_1(m_{\alpha,1} + N) + r_2(m_{\alpha,2} + N) + \cdots + r_k(m_{\alpha,k} + N) = \sum_{i=1}^k r_i(m_{\alpha,i} + N)$, then $\psi(m + N) = \sum_{i=1}^k r_i m_{\alpha,i}$. We must first show that ψ is well defined. However, each element of M/N has a *unique* representation of the form $\sum_{i=1}^k r_i(m_{\alpha,i} + N)$ since M/N is free. Therefore, ψ is well defined.

Now observe that if $m + N = \sum_{i=1}^k r_i(m_{\alpha,i} + N) \in M/N$, then

$$\begin{aligned}
\phi(\psi(m+N)) = \phi\left(\psi\left(\sum_{i=1}^k r_i(m_{\alpha,i}+N)\right)\right) &= \phi\left(\sum_{i=1}^k r_i m_{\alpha,i}\right) \\
&= \left(\sum_{i=1}^k r_i m_{\alpha,i}\right) + N \\
&= \sum_{i=1}^k (r_i m_{\alpha,i} + N) \\
&= \sum_{i=1}^k r_i(m_{\alpha,i} + N) \\
&= m + N.
\end{aligned}$$

Therefore, $\phi\psi = 1_{M/N}$ — the identity map id: $M/N \to M/N$. We claim $\ker\phi = N$. Clearly, if $n \in N \subseteq M$, then $\phi(n) = n + N = N = 0 + N$ so that $n \in \ker\phi$, i.e. $N \subseteq \ker\phi$. If $m \in \ker\phi$, we have $0 + N = \phi(m) = m + N$ so that $m \in N$, i.e. $\ker\phi \subseteq N$. Therefore, $N = \ker\phi$. Finally, recall we have the canonical inclusion $\iota : N \hookrightarrow M$, i.e. $n \mapsto n$. [From the previous work, we have $\operatorname{im}\iota = \ker\phi$.]

Define a map $\theta : M/N \oplus N \to M$ via $(m + N, n) \mapsto \psi(m + N) + \iota(n)$. Since ψ is well defined, so too is θ. We need show that θ is an R-homomorphism. Since the notation in the specific case is tedious, we show this holds more generally. Suppose $\psi : T \to S$ and $\iota : W \to S$ are R-homomorphisms. Define $\theta : T \oplus W \to S$ via $\theta(t, w) := \psi(t) + \iota(w)$. Then for $t, t' \in T$, $w, w' \in W$, and $r \in R$,

$$\begin{aligned}
\theta((t+t', w+w')) = \psi(t+t') + \iota(w+w') &= \psi(t) + \psi(t') + \iota(w) + \iota(w') \\
&= \psi(t) + \iota(w) + \psi(t') + \iota(w') \\
&= \theta((t,w)) + \theta((t',w')) \\
r\theta((t,w)) = r\left(\psi(t) + \iota(w)\right) = r\psi(t) + r\iota(w) &= \psi(rt) + \iota(rw) = \theta((rt, rw))
\end{aligned}$$

Therefore, θ is an R-map. [It is also immediate that θ is an R-map from the fact that ψ, ι are R-homomorphisms.] We claim that θ is in fact an isomorphism. We need show θ is injective and surjective.

To see that θ is injective, suppose $\theta(m+N,n)=0$. Then using the fact that $\phi\psi = 1_{M/N}$,

$$\begin{aligned}
0 &= \phi(\theta(m+N,n)) \\
&= \phi(\psi(m+N)+\iota(n)) \\
&= \phi(\psi(m+N)+n) \\
&= \phi(\psi(m+N))+\phi(n) \\
&= (m+N)+(n+N) \\
&= (m+N)+(0+N) \\
&= m+N
\end{aligned}$$

Since M/N is free, it must be that $m+N = 0+N$, i.e. $m=0$. But then $0=\theta(m+N,n)=\theta(0+N,n)=\psi(0+N)+\iota(n)=0+n=n$, i.e. $n=0$. But then $(m+N,n)=(0+N,0)$ so that θ is injective. We need only show that θ is surjective. Let $m\in M$. Define $p:=\phi(m)\in M/N$. Then $\psi(p)\in M$ and using the fact that $\phi\psi=1_{M/N}$,

$$\phi(m-\psi(p)) = \phi(m)-\phi(\psi(p)) = \phi(m)-\phi(\psi(\phi(m))) = \phi(m)-\phi(m) = 0+N$$

But then $m-\psi(p)\in\ker\phi = N$, i.e. there exists $n\in N$ so that $m-\psi(p)=n$. Therefore, $m=\psi(p)+n=\psi(\phi(m))+n=\psi(\phi(m))+\iota(n)=\theta((p,n))$. Therefore, θ is surjective. But then θ is an isomorphism. This shows $M/N\oplus N\cong M$.

(c) Consider the $\mathbb{Z}$-modules (abelian groups) $M=\mathbb{Z}$ and $N=n\mathbb{Z}$ for $n\in\mathbb{Z}_{>1}$. Clearly, $N\subseteq M$, M is a free $\mathbb{Z}$-module (generated by 1), and N is a free $\mathbb{Z}$-module (generated by n). However, $M/N=\mathbb{Z}/n\mathbb{Z}$ is not a free $\mathbb{Z}$-module as $n\cdot(m+N)=nm+N=0+N$ for all $m\in M/N$, i.e. M/N has torsion (all free modules over an integral domain are torsion free). We cannot have $M\cong M/N\oplus N$ since M has no nonzero elements of finite additive order while $M/N\oplus N$ has elements of finite additive order, e.g. $(1+N,0)$.

□

7.

(a) Prove that any two 3×3 matrices over $\mathbb{Q}$ with the same characteristic polynomial and the same minimal polynomial must be similar over $\mathbb{Q}$.

(b) Give an example of two 4×4 matrices over $\mathbb{Q}$ which are not similar over $\mathbb{Q}$ but have the same characteristic polynomial and the same minimal polynomial. Justify.

8. Suppose K and L are field extensions of F such that $\gcd([K\colon F],[L\colon F])=1$. Suppose $f\in F[x]$ is irreducible and has a root $\alpha\in K$ with $\alpha\notin F$. Prove that f has no roots in L.

Solution: Assume to the contrary that there exists $\beta \in L$ with $f(\beta) = 0$. Since f is irreducible and $f(\beta) = 0$, f is the minimal polynomial for $\beta \in L$. Let $d := \deg f$. Since f is irreducible and $f(\alpha) =)$, f is the minimal polynomial for $\alpha \in K$. Now $\alpha \in F$ if and only if $\deg p_\alpha(x) = 1$, where $p_\alpha(x)$ is the minimal polynomial for α over F, it must be that $\deg p_\alpha(x) = \deg f > 1$. Let $m = [K\colon F]$ and $n = [L\colon F]$. Now

$$m = [K\colon F] = [K\colon F(\alpha)][F(\alpha)\colon F] = d[K\colon F(\alpha)]$$
$$n = [L\colon F] = [L\colon F(\beta)][F(\beta)\colon F] = d[L\colon F(\beta)]$$

Let p be any prime dividing d. Since $p \mid d[K\colon F(\alpha)]$, we have $p \mid m$. Similarly, $p \mid d[L\colon F(\beta)]$ so that $p \mid n$. But then $\gcd(m, n) = \gcd([K\colon F], [L\colon F]) > p$, a contradiction. Therefore, $p = 1$. But then $\deg p_\alpha(x) = \deg f = 1$ so that $\alpha \in F$, a contradiction. Therefore, L contains no root of f. □

9. Let K be the splitting field of $x^6 - 3$ over $\mathbb{Q}$. Determine $[K\colon \mathbb{Q}]$ and find $\mathrm{Gal}(K/\mathbb{Q})$.

Solution: The polynomial $x^6 - 3$ is irreducible over $\mathbb{Q}$ as it is Eisenstein with $p = 3$. Define $K := \mathbb{Q}(\sqrt[6]{3}, \zeta)$, where ζ is a primitive sixth root of unity. Explicitly, set $\zeta = \frac{1+i\sqrt{3}}{2}$. Observe $\pm\sqrt[6]{3}\zeta^i$ is a roof of $x^6 - 3$, where $i \in \{0, 1, 5\}$. But each of these are elements of K. Since $x^6 - 3$ has 6 roots over $\mathbb{C}$, it must be that K is the splitting field of $x^6 - 3$ over $\mathbb{Q}$. Now by the work above, $[\mathbb{Q}(\sqrt[6]{3})\colon \mathbb{Q}] = 6$. Furthermore, $[\mathbb{Q}(\zeta)\colon \mathbb{Q}] = \phi(6) = 2$. Since $\mathbb{Q}(\sqrt[6]{3}) \subseteq \mathbb{R}$, it must be that $\zeta \notin \mathbb{Q}(\sqrt[6]{3})$. But then $\mathbb{Q}(\sqrt[6]{3}, \zeta) = \mathbb{Q}(\sqrt[6]{3})(\zeta)$ has degree $[\mathbb{Q}(\sqrt[6]{3}, \zeta)\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{3}, \zeta)\colon \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta)\colon \mathbb{Q}] = 6 \cdot 2 = 12$.

If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then σ is determined by its action on $\sqrt[6]{3}$ and ζ. Define

$$\sigma : \zeta \mapsto \zeta^{-1} \quad \sqrt[6]{3} \mapsto \sqrt[6]{3}$$
$$\tau : \zeta \mapsto \zeta \quad \sqrt[6]{3} \mapsto \zeta\sqrt[6]{3}$$

It is routine to verify that $\sigma, \zeta \in \mathrm{Gal}(K/\mathbb{Q})$. Now $\sigma^2 = 1$ and $\tau^6 = 1$. Furthermore, $(\sigma\tau)(\zeta) = \zeta^5 = (\tau^{-1}\sigma)(\zeta)$ and $(\sigma\tau)(\sqrt[6]{3}) = \zeta^{-1}\sqrt[6]{3} = (\tau^{-1}\sigma)(\sqrt[6]{3})$. As any element of $\mathrm{Gal}(K/\mathbb{Q})$ takes ζ to either ζ or ζ^{-1} and $\sqrt[3]{6}$ to $\zeta^i\sqrt[3]{6}$ for some i. Therefore, σ and τ generate $\mathrm{Gal}(K/\mathbb{Q})$. But then

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^2 = 1, \tau^6 = 1, \sigma\tau = \sigma^{-1}\sigma \rangle,$$

which is precisely the presentation of the dihedral group D_6. □

May 2018

1. Let V be a vector space over the real numbers. Let U and W be subspaces of V. Prove that $U \cup W$ is a subspace of V if and only if either $U \subseteq W$ or $W \subseteq U$.

Solution: If either $U \subseteq W$ or $W \subseteq U$, then $U \cup W = W$ or $U \cup W = U$, respectively, which are subspaces. Assume that $U \cup W$ is a subspace of V. Suppose to the contrary that neither U nor W are subsets of the other. Choose then $x \in U \setminus W$ and $y \in W \setminus U$. Since $U \cup W$ is a subspace, $x + y \in U \cup W$. But then $x + y \in U$ or $x + y \in W$. If $x + y \in U$, then $y = (x + y) - x \in U$, a contradiction. If $x + y \in W$, then $x = (x + y) - y \in W$, a contradiction. Therefore, it must be that at least one of $U \setminus W$ or $W \setminus U$ is empty. This implies $U \subseteq W$ or $W \subseteq U$. □

2. Let G and H be groups and consider the product group $G \times H$. Let e_G be the identity element of G. Consider the set $X \subseteq G \times H$ defined by $X = \{(e_G, h) \mid h \in H\}$. Construct a bijective correspondence between $\{$subgroups of $G\}$ and $\{$subgroups of $G \times H$ that contain $X\}$. Be sure to prove your bijection works.

Solution:

3. Prove that there is no simple group of order 56.

Solution: Note that $56 = 2^3 \cdot 7$. Let n_p denote the number of Sylow p-subgroups. By Sylow's Theorem, $n_2 \equiv 1 \mod 2$ and $n_2 \mid 7$ so that $n_2 \in \{1, 7\}$. Similarly, we know that $n_7 \in \{1, 8\}$. If n_2 or $n_7 = 1$, then the Sylow 2-subgroup, respectively Sylow 7-subgroup, is unique, hence normal. But then the group would not be simple. Suppose then that $n_7 > 1$. Then there are $n_7 \cdot 6 = 8 \cdot 6 = 48$ non-identity elements of order 7. But then there are $56 - 48 = 8$ remaining elements of the group, which must be the Sylow 2-subgroup (which exists by Sylow's Theorem). But then the Sylow 2-subgroup is unique, hence normal. Therefore, no group of order 56 is simple. □

4. Let A and B be $n \times n$ matrices over the complex numbers.

(a) Prove that if A is similar to B, then A and B have the same characteristic polynomial.

(b) Prove that if A and B are both diagonalizable and A and B have the same characteristic polynomial, then A is similar to B.

(c) Show by example that if at least one of A of B is not diagonalizable, then it can be the case that A and B have the same characteristic polynomial but A is not similar to B. Be sure to prove your example is valid.

5. Let G be the abelian group generated by four elements w, x, y, z, subject to the relations

$$\begin{cases} y + 3z = 0 \\ -2w + x + y + 3z = 0 \\ -2w + 4x + y + 3z = 0 \\ -3x + y + 5z = 0 \end{cases}$$

Write G as a direct sum of cyclic groups in *two* ways, corresponding to the two versions of the Fundamental Theorem of Finitely Generated Abelian Groups.

6. Let R be a commutative ring and M an R-module. Recall that M is said to be *finitely generated* if there are elements $x_1, \ldots, x_n \in M$ such that $M = Rx_1 + \cdots + Rx_n$.

(a) If $N \subseteq M$ is a submodule such that both N and M/N are finitely generated, prove that M is finitely generated.

(b) Give an example, with justification, of a finitely generated module M and a submodule N which is not finitely generated.

7. Suppose that A is a square complex matrix with characteristic polynomial $c_A(x) = (x-1)^4(x+3)^5$. Assume that $A - I$ has nullity 4 and $A + 3I$ has nullity 1, where I is the identity matrix of the same size as A. Find, with justification, all possible Jordan canonical forms of A, and give the minimal polynomial for each.

8. Set $K = \mathbb{Q}(i, \sqrt[4]{2})$, where i is the complex root of -1 and $\sqrt[4]{2}$ is the real fourth root of 2.

(a) Find the degree $[K\colon \mathbb{Q}]$.

(b) Identify all the elements of $\mathrm{Aut}_{\mathbb{Q}}(K)$.

(c) Identify the isomorphism type of the group $\mathrm{Aut}_{\mathbb{Q}}(K)$.

Justify all your conclusions.

3 Analysis Prelim

August 1991

1. Show that every uncountable subset of the real numbers has a limit point.

Solution: We prove the contrapositive: if a nonempty subset $A \subset \mathbb{R}$ has no limit points, it must be at most countable. Suppose that A has no limit points. Let $A_n = A \cap [-n, n]$ for $n \in \mathbb{N}$. Observe that each n is bounded and must contain no limit points. Note that every bounded infinite subset of $\mathbb{R}$ has a limit point. As A has no limit point, it must be that A_n is empty or finite for each n. But $A = \cup_{n=1}^{\infty} A_n$ so that A is at most countable.

OR

Suppose that A is an uncountable subset of $\mathbb{R}$. For $n \in \mathbb{Z}$, let $A_n = A \cap [n, n+1]$. We know that $A = \cup_{n \in \mathbb{Z}} A_n$. If A_n were finite for each n, then A would be countable, a contradiction. Then A_n is infinite for some n, say n_0. We know that $A_{n_0} \subseteq [n_0, n_0 + 1]$. As this is an infinite subset of a compact bounded subset of $\mathbb{R}$, we know that A_{n_0} has a limit point, say x_0. But then A has a limit point as any neighborhood of x_0 U in $\mathbb{R}$ has neighborhood $U \cap [n_0, n_0 + 1]$ in $[n_0, n_0 + 1]$. □

2. The sequence of real numbers $\{x_n\}$ is defined by recursively by $x_1 = 1$ and

$$x_{n+1} = \left(x_n + x_n^2\right)^{1/3}$$

Prove that x_n converges and find the limit.

Solution: Observe that $x_1 = 1$ and $x_2 = (1 + 1^2)^{1/3} = 2^{1/3} > 1 = x_1$. Now assume that the sequence x_n is increasing for $n = 1, 2, 3, \cdots, k$. Then using the fact that $\sqrt[3]{x}$ is an increasing function,

$$\begin{aligned} n_k &> n_{k-1} \\ n_k^2 &> n_{k-1}^2 \\ n_k + n_k^2 &> n_{k-1} + n_{k-1}^2 \\ (n_k + n_k^2)^{1/3} &> (n_{k-1} + n_{k-1}^2)^{1/3} \\ n_{k+1} &> n_k \end{aligned}$$

Therefore by induction, n_k is an increasing sequence. As $x_1 = 1$ and x_n is increasing, $x_n > 0$ for all $n \in \mathbb{N}$. Observe also that $x_1 < 2$ and $x_2 < 2$. Assume that this is true for

$n = 1, 2, 3, \cdots, k$. Then

$$\begin{aligned} x_k &< 2 \\ x_k^2 &< 4 \\ x_k + x_k^2 &< 6 \\ (x_k + x_k)^{1/3} &< 6^{1/3} < 2 \\ x_{k+1} &< 2 \end{aligned}$$

so that $x_n < 2$ for all $n \in \mathbb{N}$. Then the sequence x_n is increasing and bounded above. By the Monotone Convergence Theorem, the sequence x_n has a limit in $\mathbb{R}$, say x. Then x satisfies $x = (x + x^2)^{1/3}$. Then

$$\begin{aligned} x &= (x + x^2)^{1/3} \\ x^3 &= x + x^2 \\ x^3 - x^2 - x &= 0 \\ x(x^2 - x - 1) &= 0 \end{aligned}$$

so that $x = 0$ or $x = \frac{1 \pm \sqrt{5}}{2}$. As $0 < x_n < 2$ and $\{x_n\}$ is increasing, $x = 0$ and $x = \frac{1-\sqrt{5}}{2}$ are not possible. Therefore, the sequence x_n converges to $\frac{1+\sqrt{5}}{2}$. □

3. Let $\{f_n\}$ be a sequence of continuous functions defined on a compact metric space K and suppose f_n converges uniformly on K to a function f. Prove that f_n^2 converges uniformly to f^2 on K.

Solution: As the $f_n(x)$ are continuous on a compact metric space, they are bounded. Say $|f_i(x)| \leq M_i$ for some $M_i \in \mathbb{R}$, depending on i. Moreover as $f_n(x) \to f(x)$ uniformly and the f_n are continuous, we know that $f(x)$ is continuous. Therefore, $f(x)$ is continuous on a compact metric space and hence is bounded. Suppose $|f(x)| < B$ for some $B \in \mathbb{R}$.

Furthermore as $f_n(x) \to f(x)$ uniformly, given $\epsilon > 0$ there is an $N \in \mathbb{N}$ such that $|f_n(x) - f(x)| < \epsilon$ for $n > N$, no matter the choice of $x \in K$. But then $|f_n(x)| \leq B + \epsilon$ for $n > N$. Let $M = \max\{M_1, M_2, \cdots, M_N, B + \epsilon\}$. Then $|f_n(x)| < M$ for all $n \in \mathbb{N}$ so that $\{f_n(x)\}$ is uniformly bounded.

Now given $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that $|f_n(x) - f(x)| < \epsilon/2M$ for $n > N$. Then we have

$$\begin{aligned} |f_n^2(x) - f^2(x)| &= |f_n(x) - f(x)|\,|f_n(x) + f(x)| \\ &\leq |f_n(x) - f(x)|\,\big(|f_n(x)| + |f(x)|\big) \\ &\leq \frac{\epsilon}{2M} \cdot (M + M) = \epsilon \end{aligned}$$

so that $f_n^2(x) \to f^2(x)$ uniformly. $\square$

4. Prove the following: if f is continuous, real valued function on $[0,1]$ such that $f(0) = 0$ and

$$\int_0^1 x^n f(x)\, dx = 0 \qquad \text{for } n = 1, 2, 3, \cdots$$

then $f(x) = 0$ for all $x \in [0,1]$.

Solution: Observe that

$$\int_0^1 a x^n f(x)\, dx = a \int_0^1 x^n f(x)\, dx = 0$$

for all $a \in \mathbb{R}$. But then given any polynomial with zero constant term $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x$, we have

$$\begin{aligned}
\int_0^1 p(x)f(x)\, dx &= \int_0^1 a_n x^n f(x) + a_{n-1}x^{n-1}f(x) + \cdots + a_1 x f(x)\, dx \\
&= a_n \int_0^1 x^n f(x)\, dx + a_{n-1}\int_0^1 x^{n-1} f(x)\, dx + \cdots + a_1 \int_0^1 x f(x)\, dx \\
&= 0 + 0 + \cdots + 0 \\
&= 0
\end{aligned}$$

As $f(x)$ is continuous on the compact interval $[0,1]$, there is a sequence of polynomials $\{p_n(x)\}$ converging uniformly to $f(x)$ on $[0,1]$. Then given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|f(x) - p_n(x)| < \epsilon$ for all $x \in [0,1]$ and $n > N$. As $f(x)$ is continuous on the compact interval $[0,1]$, it is bounded. Say $|f(x)| < M$ on $[0,1]$. Observe then that $p_n(x)f(x)$ converges uniformly to $f(x)^2$ as $|f(x)^2 - p_n(x)f(x)| = |f(x)|\,|f(x) - p_n(x)| < M\epsilon$. Furthermore, observe that $p_n(0) = 0$ for $n > N$, i.e. the $p_n(x)$ have 0 constant term as $|f(0) - p_n(0)| = |0 - p_n(0)| = |p_n(0)| < \epsilon$. But then

$$0 = \lim_{n\to\infty} \int_0^1 p_n(x)f(x)\, dx = \int_0^1 \lim_{n\to\infty} p_n(x)f(x)\, dx = \int_0^1 f(x)^2\, dx$$

As $f(x)$ is continuous, if there were any interval in $[0,1]$ on which $f(x) \neq 0$, then $\int_0^1 f^2(x)\ dx > 0$, a contradiction. Therefore, it must be that $f(x)^2 = 0$. But then $f^2(x) = f(x)f(x) = 0$ forces $f(x) = 0$ for all $x \in [0,1]$. $\square$

5. Let $F(x,y,z) = 3x + 2y + z - y\sin(xz)$.

(a) Can the equation $F(x,y,z) = 0$ be solved for $z = f(x,y)$ in a neighborhood of the point $(0,-1)$ satisfying $f(0,-1) = 2$? Justify your answer.

(b) State a precise version of what is asked for in (a). Be as complete as possible.

6. The function f maps $[0,1]$ onto $[0,1]$ and is monotone. Prove f is continuous on $[0,1]$.

Solution: Note that f is continuous if and only if $-f$ is continuous. If f is monotone decreasing, then $-f$ is monotone increasing. Therefore without loss of generality, we assume that f is monotone increasing. Suppose to the contrary that f is not continuous. Since f is monotone, it has no discontinuities of the second kind. Therefore, f has a simple discontinuity at some point $x_0 \in [0,1]$. Let $y_0^- := \lim_{x \to x_0^-} f(x)$ and $y_0^+ := \lim_{x \to x_0^+} f(x)$. At least one of the intervals $(y_0^-, f(x_0))$, $(f(x_0), y_0^+)$ must be nonempty. Choose one of the nonempty intervals (if they both are nonempty, arbitrarily choose the first), and denote it I. Then $I \subset (y_0^-, y_0^+) \subset (f(0), f(1))$. But then the image of f is not $[0,1]$, a contradiction. $\square$

August 1992

1. Let $\{x_n\}$ be a sequence of complex numbers converging to a. Show that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n} x_j = a.$$

Solution: First, observe that

$$\begin{aligned}
\left|\frac{1}{n}\sum_{j=1}^{n} x_j - s\right| &= \left|\frac{x_1+x_2+x_3+\cdots+x_n}{n} - a\right| \\
&= \left|\frac{x_1+x_2+\cdots+x_n}{n} - \frac{na}{n}\right| \\
&= \left|\frac{(x_1-a)+(x_2-a)+\cdots+(x_n-a)}{n}\right| \\
&= \left|\frac{1}{n}\sum_{j=1}^{n}(x_j-a)\right| \\
&\leq \frac{1}{n}\sum_{j=1}^{n}|x_j-a| = \frac{1}{n}\sum_{j=1}^{N-1}|x_j-a| + \frac{1}{n}\sum_{j=N}^{n}|x_j-a|
\end{aligned}$$

Since $\lim_{n\to\infty} x_n = a$, given $\epsilon > 0$ there exists a $N \in \mathbb{N}$ such that $|x_n - a| < \frac{\epsilon}{2}$ for $n \geq N$. Moreover, since x_n is a convergent sequence, the sequence $\{x_n\}$ is bounded. In particular as $x_n \to a$, the sequence $\{|x_n \to a|\}$ converges to 0 so that the sequence $\{|x_n - a|\}$ is bounded. Then there exists a $M \in \mathbb{N}$ such that $|x_n - a| \leq M$ for all n. Then

$$\frac{1}{n}\sum_{j=1}^{N-1}|x_n-a| \leq \frac{NM}{n}$$

Choose $P \in \mathbb{N}$ such that $P > \frac{2NM}{\epsilon}$. Then this implies $P+1 > \frac{2NM}{\epsilon} + 1 > \frac{2NM}{\epsilon}$. But then $\frac{NM}{P+1} < \frac{\epsilon}{2}$. Therefore,

$$\frac{1}{n}\sum_{j=1}^{N-1}|x_j-a| < \frac{\epsilon}{2}$$

for $n > P$.

Let $\mathcal{J} = \max\{P, N\}$, then

$$\left|\frac{1}{n}\sum_{j=1}^{n} x_j - s\right| \leq \frac{1}{n}\sum_{j=1}^{N-1}|x_j-a| + \frac{1}{n}\sum_{j=N}^{n}|x_j-a| < \frac{\epsilon}{2} + \frac{(n-N+1)\frac{\epsilon}{2}}{n} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

for $n > \mathcal{J}$. Therefore, $\frac{1}{n}\sum_{j=1}^{n} x_j$ converges to a. □

2.

(a) If $f_n \in C^1(0,2)$, $n = 1, 2, \ldots$, and f_n' converges uniformly to zero, while $f_n(1)$ converges to 1, prove that f_n converges uniformly on $(0,2)$.

(b) Is the result true if each f_n is only differentiable on $(0,2)$?

3. Let (X, ρ) be a compact metric space and (Y, d) be a metric space.

(a) If $f : X \to Y$ is continuous and onto show that (Y, d) is complete.

(b) If f is also one-to-one, prove that $f^{-1} : Y \to X$ is continuous.

Solution:

(a) The image of a compact set under a continuous mapping is compact. But as f is onto, we have $Y = f(X)$ so that Y is compact. But then Y is a compact metric space so that Y is complete.

(b) Since f is injective, it has an inverse f^{-1}. We need show that f^{-1} is continuous (showing that f is a homeomorphism). We know that f^{-1} is continuous if and only if f maps closed sets to closed sets. Let C be closed in X. Since C is closed and X is compact, we know that C is compact. Then as f is continuous, $f(C)$ is compact. But as Y is a metric space and $f(C)$ is compact, we know that $f(C)$ is closed. □

4. Suppose $f : \mathbb{R}^2 \to \mathbb{R}$ is C^1. If f_{xy} exists in a neighborhood of $(0,0)$ and is continuous at $(0,0)$, prove that f_{yx} exists at $(0,0)$ and $f_{yx}(0,0) = f_{xy}(0,0)$.

5. Let $p(x,y) = (xy-1)^2 + x^2$ for $(x,y) \in \mathbb{R}^2$. Find $\inf\{p(x,y) \colon (x,y) \in \mathbb{R}^2\}$.

Solution: Clearly, $p(x,y) \geq 0$ for all $(x,y) \in \mathbb{R}^2$. Now for $n \in \mathbb{N}$, choose $x = \frac{1}{n}$ and $y = n$. Then we have

$$p(x,y) = p\left(\frac{1}{n}, n\right) = \left(\frac{1}{n} \cdot n - 1\right)^2 + \left(\frac{1}{n}\right)^2 = \frac{1}{n^2}$$

Now given $\epsilon > 0$, choose $N \in \mathbb{N}$ such that $\frac{1}{N^2} < \epsilon$. Then for $n > N$, we have $p(\frac{1}{n}, n) = \frac{1}{n^2} < \epsilon$. But then clearly, $\inf\{p(x,y) \colon (x,y) \in \mathbb{R}^2\} = 0$. □

6. Suppose f is continuous and greater than 1 on $[0,1]$. Prove that for a positive a

$$\lim_{a \to 0} \left(\int_0^1 |f(x)|^a \, dx \right)^{\frac{1}{a}} = \exp\left(\int_0^1 \ln |f(x)| \, dx \right)$$

Hints: First, establish the limit formally. Then attend to the intermediate results that require justification.

August 1993

1. Given a C^1 function $F : \mathbb{R}^n \to \mathbb{R}^n$ satisfying

$$\|F(x)\| \leq \|x\|^2, \quad x \in \mathbb{R}^n,$$

prove that there is an $\epsilon > 0$ such that the equation $F(x) = x + \alpha$ has a solution x whenever the vector α satisfies $\|\alpha\| < \epsilon$.

2. If $a_n \geq 0$ and $\sum_{n=1}^{\infty} a_n < \infty$, prove that there exists a sequence b_n such that $\lim_{n\to\infty} b_n = \infty$ and $\sum_{n=1}^{\infty} a_n b_n$ converges.

Solution: If $a_n = 0$ for all n, the result is trivial. We assume that $a_n > 0$ for all n (this will be generalized to $a_n \geq 0$ at the end with little modification). As $\sum a_n$ is finite, it is Cauchy. In particular, the tail of the sequence tends to 0. That is,

$$\lim_{m\to\infty} \sum_{n=m}^{\infty} a_n = 0$$

Let $r_n = \sum_{m=n}^{\infty} a_m$. Then it is clear that $r_n \to 0$. We define the sequence $b_n = 1/\sqrt{r_n}$ (which is possible as $r_n > 0$). As $r_n \to 0$, it is clear that $\sqrt{r_n} \to 0$ so that $b_n \to \infty$. We have

$$a_n b_n(\sqrt{r_n} + \sqrt{r_{n+1}}) = \frac{a_n}{\sqrt{r_n}}(\sqrt{r_n} + \sqrt{r_{n+1}}) = a_n + a_n\sqrt{\frac{r_{n+1}}{r_n}}$$

However, $r_n \geq r_{n+1}$ so that this shows

$$a_n b_n(\sqrt{r_n} + \sqrt{r_{n+1}}) = \frac{a_n}{\sqrt{r_n}}(\sqrt{r_n} + \sqrt{r_{n+1}}) = a_n + a_n\sqrt{\frac{r_{n+1}}{r_n}} < 2a_n = 2(r_n - r_{n+1})$$

Dividing by $\sqrt{r_n} + \sqrt{r_{n+1}} > 0$, yields

$$a_n b_n = \frac{a_n}{\sqrt{r_n}} < \frac{2(r_n - r_{n+1})}{\sqrt{r_n} + \sqrt{r_{n+1}}} = \frac{2(r_n - r_{n+1})}{\sqrt{r_n} + \sqrt{r_{n+1}}} \cdot \frac{\sqrt{r_n} - \sqrt{r_{n+1}}}{\sqrt{r_n} - \sqrt{r_{n+1}}} = 2(\sqrt{r_n} - \sqrt{r_{n+1}})$$

But we know that

$$\sum_{n=1}^{\infty} 2(\sqrt{r_n} - \sqrt{r_{n+1}}) = 2\sum_{n=1}^{\infty}(\sqrt{r_n} - \sqrt{r_{n+1}}) = 2\sqrt{r_1}$$

as the series telescopes. Therefore by the Comparison Test, we know that

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} \frac{a_n}{\sqrt{r_n}}$$

converges.

We need now only consider the case where a_n can take on zero values. However, this is now trivial. Let $f \in \mathbb{N}$ be the first value such that $a_n > 0$. Let $b_n = 0$ for $n = 1, 2, \cdots, f$ and then take b_n as before for $n > f$. We still have that $b_n \to \infty$ and observe

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=f+1}^{\infty} a_n b_n$$

to which the arguments above apply. □

3. Assume that the family $\{f_n\}_{n=1}^{\infty}$ of real-valued functions on $[0,1]$ is equicontinuous and pointwise bounded. Also assume $\int_a^b f_n(x)\ dx \to 0$ as $n \to \infty$ for every $0 \leq a < b \leq 1$. Prove that $f_n \to 0$ uniformly.

4. Let P_E denote the set of real-valued polynomials which involve no odd powers of the variable, i.e. the coefficient of each odd power term is zero. Prove that P_E is dense in $C([0,1])$ which the sup norm. For which closed intervals other than $[0,1]$ can the same be proved?

5. For which non-decreasing functions β on $[0,1]$ does the Riemann-Stieltjes integral $\int_0^1 \beta\ d\beta$ exist? Prove your assertion.

6. If f is continuous and $\lim_{s\to\infty} f(s) = a$, prove that $\dfrac{1}{\log t}\displaystyle\int_1^t \frac{f(s)}{s}\ ds \to a$ as $t \to \infty$.

Solution: Since $\lim_{s\to\infty} f(s) = a$, for $\epsilon > 0$, there exists $N_1 \in \mathbb{N}$ such that for $s > N_1$, we have $|f(s) - a| < \epsilon/2$. Since $f(s)$ is continuous on $[1, N_1]$, it is bounded, i.e. there exists $M \in \mathbb{R}$ such that $|f(s)| < M$ for $s \in [1.N_1]$. Now $\log x$ is an increasing function and $\lim_{x\to\infty} \log x = \infty$. Choose then $N_2 \in \mathbb{N}$ so that $\frac{(M+|a|)\log N}{\log N_2} < \frac{\epsilon}{2}$. Finally, observe that

$$\frac{1}{\log t}\int_1^t \frac{a}{s}\ ds = \frac{a}{\log t}\int_1^t \frac{ds}{s} = \frac{a}{\log t}\cdot \log s\Big|_1^t = \frac{a}{\log t}\cdot(\log t - \log 1) = a$$

Now given $\epsilon > 0$, as above, choose $N = \max\{N_1, N_2\}$. Then for $t > N$ (noting that $\log x$ is

increasing so $\frac{\log N}{\log t} < 1$), we have

$$\begin{aligned}
\left|\frac{1}{\log t}\int_1^t \frac{f(s)}{s}\,ds - a\right| &= \left|\frac{1}{\log t}\int_1^t \frac{f(s)}{s}\,ds - \frac{1}{\log t}\int_1^t \frac{a}{s}\,ds\right| \\
&= \left|\frac{1}{\log t}\int_1^t \frac{f(s)-a}{s}\,ds\right| \\
&\le \frac{1}{\log t}\int_1^t \frac{|f(s)-a|}{s}\,ds \\
&= \frac{1}{\log t}\int_1^N \frac{|f(s)-a|}{s}\,ds + \frac{1}{\log t}\int_N^t \frac{|f(s)-a|}{s}\,ds \\
&\le \frac{1}{\log t}\int_1^N \frac{|f(s)|+|a|}{s}\,ds + \frac{1}{\log t}\int_N^t \frac{|f(s)-a|}{s}\,ds \\
&\le \frac{1}{\log t}\int_1^N \frac{M+|a|}{s}\,ds + \frac{1}{\log t}\int_N^t \frac{\epsilon/2}{s}\,ds \\
&= \frac{M+|a|}{\log t}\int_1^N \frac{ds}{s} + \frac{\epsilon/2}{\log t}\int_N^t \frac{ds}{s} \\
&= \frac{M+|a|}{\log t}\cdot \log s\Big|_1^N + \frac{\epsilon/2}{\log t}\cdot \log s\Big|_N^t \\
&= \frac{M+|a|}{\log t}(\log N - \log 1) + \frac{\epsilon/2}{\log t}(\log t - \log N) \\
&= \frac{(M+|a|)\log N}{\log t} + \frac{\epsilon}{2}\cdot\left(1 - \frac{\log N}{\log t}\right) \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.
\end{aligned}$$

Therefore, $\frac{1}{\log t}\int_1^t \frac{f(s)}{s}\,ds \to a$ as $t \to \infty$. □

August 1994

1. For which real x does the series $\displaystyle\sum_{n=1}^{\infty} ne^{-nx}$ converge?

Solution: We know that the series converges if $\limsup \frac{c_{n+1}}{c_n} < 1$, where $c_n = ne^{-nx}$. But

$$\lim_{n\to\infty}\left|\frac{(n+1)e^{-(n+1)x}}{ne^{-nx}}\right| = \lim_{n\to\infty}\left|\frac{n+1}{n}\cdot\frac{e^{-nx}e^{-x}}{e^{-nx}}\right| = |e^{-x}|$$

So we want $|e^{-x}| = e^{-x} < 1$. This implies that $x > 0$. We need now only check the case where $x = 0$. But this is easily done as

$$\sum_{n=1}^{\infty} ne^{-nx}\Big|_{x=0} = \sum_{n=1}^{\infty} n$$

which clearly diverges. So the series $\sum_{n=1}^{\infty} ne^{-nx}$ converges for $x > 0$. □

2. Suppose that f is a differentiable function on $[0,\infty)$, $\lim_{x\to\infty} f(x)/x = 0$, and $\lim_{x\to\infty} f'(x) = a$. Prove that $a = 0$.

3. Find $\lim_{n\to\infty} x_n$ when $x_{n+1} = \sqrt{x_n + a}$, $a > 0$, and $x_1 = \sqrt{a}$.

4. Prove that if a function $f(x)$ is integrable on $[a,b]$ then its absolute value $|f(x)|$ is also integrable on $[a,b]$ and

$$\left|\int_a^b f(x)\,dx\right| \le \int_a^b |f(x)|\,dx.$$

5. Let f be a complex valued function on a set $\mathcal{D}$ and suppose that $|f(x)| < 1$ for each $x \in \mathcal{D}$.

(a) Show that the sequence of powers of f, $\{f, f^2, f^3, \ldots\}$ converges pointwise.

(b) Find necessary and sufficient conditions for the convergence to be uniform.

6. Let $K(x,y)$ be continuous on the rectangle $[a,b]\times[c,d] \subset \mathbb{R}^2$. For integrable functions f on $[c,d]$ define an operator T by

$$(Tf)(x) = \int_c^d K(x,y)f(y)\,dy.$$

(a) Show that $(Tf)(x)$ is a continuous function on $[a,b]$.

(b) Show that $S = \{Tf\colon \int_c^d |f(x)|\, dx \leq 1\}$ is an equicontinuous family of functions on $[a, b]$.

7. Let $U = \{(u, v) \in \mathbb{R}^2\colon u > 0\}$ and define $F : U \to \mathbb{R}^2$ by $F(u, v) = (u \cos v, u \sin v) = (x, y)$.

(a) Show that F is an open mapping on U.

(b) Find $\partial u/\partial x$, $\partial u/\partial y$, $\partial v/\partial x$, $\partial v/\partial y$.

8. Let $f(x, y) = x^2 + y^2 - 5$ be a function on $\mathbb{R}^2$.

(a) Describe thoroughly the results of applying the Implicit Function Theorem in a neighborhood of the point $(2, 1)$.

(b) Describe thoroughly the results of applying the Implicit Function Theorem in a neighborhood of the point $(\sqrt{5}, 0)$.

August 1997

1. Let $K \subset \mathbb{R}^n$ be a compact set and let $\epsilon > 0$. Set $J = \{x \in \mathbb{R}^n : \text{dist}(x, K) \leq \epsilon\}$, where $\text{dist}(x, K) = \inf\{\|x - y\|_2 : y \in K\}$ and $\|t\|_2$ is the usual norm in $\mathbb{R}^n$. Prove that J is compact.

2. Determine the convergence or divergence of the following sequences $\{x_n\}_{n=1}^{\infty}$.

(a) $x_n = \dfrac{1}{n^2+1} + \dfrac{2}{n^2+2} + \cdots + \dfrac{n}{n^2+n}$

(b) $x_n = \left(-\dfrac{1}{2}\right)^n + \sin\left(\dfrac{n\pi}{2}\right)$

(c) $x_n = \dfrac{n^n + (-n)^n}{2} + \left(1 + \dfrac{1}{2n}\right)^n$

Solution:

(a) Observe

$$\begin{aligned}
(1 + 2 + \cdots + n) \cdot \frac{1}{n^2+n} \leq x_n \leq (1 + 2 + \cdots + n) \cdot \frac{1}{n^2+1} \\
\frac{n(n+1)}{2} \cdot \frac{1}{n^2+n} \leq x_n \leq \frac{n(n+1)}{2} \cdot \frac{1}{n^2+1} \\
\frac{1}{2} \leq x_n \leq \frac{n^2+n}{2n^2+2}
\end{aligned}$$

for all $n \in \mathbb{N}$. By Squeeze Theorem, we have

$$\begin{aligned}
\lim_{n\to\infty} \frac{1}{2} \leq \lim_{n\to\infty} x_n \leq \lim_{n\to\infty} \frac{n^2+n}{2n^2+2} \\
\frac{1}{2} \leq \lim_{n\to\infty} x_n \leq \frac{1}{2}
\end{aligned}$$

so that we must have $\lim_{n\to\infty} x_n = \frac{1}{2}$.

(b) Define a sequence $b_n = (-\frac{1}{2})^n$. Clearly, $b_n \to 0$ as $n \to \infty$. If the sequence x_n converged, then so too would the sequence $\{x_n - b_n\} = \{\sin(\frac{n\pi}{2})\}$. But

$$\{x_n - b_n\} = \{0, 1, 0, -1, 0, 1, 0, -1, 0, \ldots\}$$

clearly does not converge. Therefore, $\{x_n\}$ does not converge.

(c) The sequence $c_n = (1 + 1/(2n))^n$ converges as

$$\lim_{n\to\infty}\left(1+\frac{1}{2n}\right)^n = \lim_{n\to\infty}\left[\left(1+\frac{1}{2n}\right)^{2n}\right]^{1/2} = \left[\lim_{n\to\infty}\left(1+\frac{1}{2n}\right)^{2n}\right]^{1/2} = \sqrt{e}.$$

If the sequence x_n converged, then the sequence $\{x_n - c_n\}$ would converge. But $x_n - c_n = \frac{n^n+(-n)^n}{2}$. However,

$$\frac{n^n+(-n)^n}{2} = \begin{cases} n^n, & n \text{ even} \\ 0, & n \text{ odd} \end{cases}$$

so that $\{x_n - c_n\}$ cannot converge. But then neither can $\{x_n\}$ converge.

3. Determine whether or not $\sum_{n=1}^{\infty} u_n(x)$ converges uniformly on I, where $u_n(x)$ and I are given in parts (a) and (b) below

(a) $I = \mathbb{R}$ and $u_n = \begin{cases} 0, & |x| \le n \text{ or } |x| \ge n+1 \\ n\sin(1/n^2), & n < |x| < n+1 \end{cases}$

(b) $I = [1, \infty)$ and $u_n(x) = \int_1^x e^{-nt^2}\, dt$, $x \in I$.

4. Let D^+ and D^- denote the operation of taking derivatives of real functions from the right and left respectively, for example $D^+f(x) = \lim_{y\to x^+} \dfrac{f(y)-f(x)}{y-x}$, D^- is defined similarly.

(a) Give an example of a function for which $D^+f(0)$, $D^-f(0)$ both exist but are not equal.

(b) Prove or disprove: if $D^+f(0)$, $D^-f(0)$ both exist then the function f is continuous at $x = 0$.

5. Suppose that $f(x) = x$ and $g(x) = \begin{cases} 0, & 0 \le x < 1/2 \\ 1/2, & x = 1/2 \\ 1, & 1/2 < x \le 1 \end{cases}$, evaluate:

(a) $\int_0^1 f\, dg$

(b) $\int_0^1 g\, df$

6. For a nonnegative integer l let $P_l(x) = \sum_{k=0}^{l} a_k x^k$ for real numbers a_k and $x \in [-1, 1]$. Given a positive integer n set $\mathcal{F}(n) = \{P_l(x) \colon 0 \le l \le n \text{ and } |a_k| < 1 \text{ for } k = 0, \ldots, l\}$. So $\mathcal{F}(n)$ is the set of polynomials of degree less than or equal n whose coefficients all have absolute value less than 1. Prove or disprove, for each n, the set $\mathcal{F}(n)$ is equicontinuous.

7. Let $f(x, y) = |x|^{1/2}|y|^{1/2} + xy$ be a real function on $\mathbb{R}^2$.

(a) Find the partial derivatives of f at the origin.

(b) Discuss the differentiability of f at the origin.

8. Let $x = r\cos\theta\sin\phi$, $y = r\sin\theta\sin\phi$, and $z = r\cos\phi$. Define the map $F(r,\theta,\phi) = (x,y,z)$ from $(r,\theta,\phi) \in \mathbb{R}^3$ to $(x,y,z) \in \mathbb{R}^3$.

(a) Prove or disprove, F has a global inverse on $\mathbb{R}^3$.

(b) Find $\dfrac{\partial}{\partial x}\theta(0,1,0)$.

August 1998

1. Construct an open set containing every rational number but not every real number. What can be said about the closure of any such set?

Solution: Let I be a finite collection of irrational numbers in $\mathbb{R}$. Clearly, I is bounded. Without loss of generality, assume the finite elements of I are $i_1, i_2, \cdots, i_n$ such that $i_1 < i_2 < \cdots < i_n$. Now let

$$S = \mathbb{R} \setminus I = \bigcup_{j=1}^{n} (i_j, i_{j+1}) \bigcup (-\infty, i_1) \cup (i_n, \infty)$$

It is clear that S is open as it is the union of open sets. Clearly, S contains all rational as $x \in S$ for all $x \in \mathbb{R}$ except for $x \in I$. As a concrete example, take $I = \{\sqrt{2}\}$. Then $S = (-\infty, \sqrt{2}) \cup (\sqrt{2}, \infty) = \mathbb{R} \setminus \{\sqrt{2}\} = \{\sqrt{2}\}^C$.

Now suppose S contains all rational numbers but $S \neq \mathbb{R}$ and that S is open. Consider $\overline{S}$. If $x \in \mathbb{R}$, then every open neighborhood of x contains a rational number distinct from x as $\mathbb{Q}$ is dense in $\mathbb{R}$. But then every open neighborhood of every point $x \in \mathbb{R}$ intersects x at a point distinct from x. Then x is a limit point of S. But then $x \in \overline{S}$. Therefore, $\overline{S} = \mathbb{R}$. Or to see this second part, note that $S \supset \mathbb{Q}$ and $\mathbb{Q}$ is dense in $\mathbb{R}$ so that $\mathbb{R} = \overline{\mathbb{R}} \supset \overline{S} \supset \overline{\mathbb{Q}} = \mathbb{R}$. $\square$

2. Prove the inequalities

$$py^{p-1}(x-y) \leq x^p - y^p \leq px^{p-1}(x-y),$$

where x and y are real numbers satisfying $0 < y < x$, and p is a real number satisfying $1 \leq p < \infty$.[28]

Solution: Consider the function $f(x) = x^p$. Observe that $f(x)$ is smooth on $\mathbb{R}$. In particular, $f(x)$ is differentiable on $[y, x]$, $f''(x)$ exists and is everywhere continuous. By the Mean Value Theorem, there exists $c \in (y, x)$ such that $f'(c) = \frac{f(x)-f(y)}{x-y}$. However, $f'(x) = px^{p-1}$ and $f''(x) = p(p-1)x^{p-2} > 0$. Since $f''(x) \geq 0$ for all $x \in [0, \infty)$, $f'(y) \leq f'(c) \leq f'(x)$. However, this is $py^{p-1} \leq \frac{x^p - y^p}{x-y} \leq x^p$. This is precisely,

$$py^{p-1}(x-y) \leq x^p - y^p \leq px^{p-1}(x-y).$$

OR

[28] The result also holds, with inequalities reversed, for $0 < p < 1$.

Let $r \in (0,1)$ and $0 < p < 1$. Since $r < 1$, we have $r < p$. Observe p is the p-fold sum of 1. Now $r < 1$ so that by induction, $r^n < 1$ and $r^n < r^{n-1}$ for all $n \in \mathbb{N}$. Then we have

$$\begin{aligned} pr^{p-1} &= \underbrace{r^{p-1} + r^{p-1} + \cdots + r^{p-1}}_{p \text{ times}} \\ &< r^{p-1} + r^{p-2} + \cdots + r + 1 \\ &< \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = p \end{aligned}$$

Noting that $\sum_{k=0}^{n-1} r^k = \frac{1-r^n}{1-r}$, multiplication by $1 - r$ yields

$$pr^{p-1}(1-r) \leq 1 - r^p \leq p(1-r)$$

Now $0 < y < x$ so that $y/x < 1$. Setting $r = y/x$ yields

$$p\left(\frac{y}{x}\right)^{p-1}\left(1 - \frac{y}{x}\right) \leq 1 - \left(\frac{y}{x}\right)^p \leq p\left(1 - \frac{y}{x}\right)$$

Now multiplication by $x^p > 0$ gives

$$\begin{aligned} x^p \cdot p\left(\frac{y}{x}\right)^{p-1}\left(1 - \frac{y}{x}\right) &\leq x^p \cdot \left[1 - \left(\frac{y}{x}\right)^p\right] \leq x^p \cdot p\left(1 - \frac{y}{x}\right) \\ p \cdot x^{p-1} \cdot \left(\frac{y}{x}\right)^{p-1}\left(1 - \frac{y}{x}\right) \cdot x &\leq x^p - x^p \cdot \left(\frac{y}{x}\right)^p \leq p \cdot x^p \cdot \left(1 - \frac{y}{x}\right) \\ py^{p-1}(x-y) &\leq x^p - y^p \leq px^{p-1}(x-y). \end{aligned}$$

□

3. Let $F(x,y,u,v) = 3x^2 - y^2 + u^2 + 4uv + v^2$ and $G(x,y,u,v) = x^2 - y^2 + 2uv$.

(a) Show that the equations

$$\begin{aligned} F(x,y,u,v) &= 9, \\ G(x,y,u,v) &= -3 \end{aligned}$$

determine x and y as functions of u and v in a neighborhood of $u = 1$, $v = 1$ with $x(1,1) = 2$ and $y(1,1) = 3$. Also find $\frac{\partial y}{\partial u}$ at $(u,v) = (1,1)$.

(b) If the numbers 9 and -3 on the right-hand sides of the equations above are both replaced by 0, show that there is no open set in the (u,v)-plane on which the resulting equations define x and y as functions of u and v.

4. Let f be a real valued continuous function on $[0,1)$ such that

$$\lim_{x\to 1^-} f(x) = f(0).$$

Prove that f cannot be one-to-one.

5. Suppose f is real-valued continuous on $[0,1]$ and

$$\int_0^1 f(x)\, e^{-\lambda x^2}\, dx = 0, \text{ all } \lambda \geq 0.$$

Show that $f(x) \equiv 0$ on $[0,1]$.

August 1999

1. Use $e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$ to prove that e is irrational.

Solution: Let $s_n = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$. Observe that s_n increases monotically to e. Furthermore, we have

$$\begin{aligned} e - s_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots &< \frac{1}{(n+1)!}\left(1 + \frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots\right) \\ &= \frac{1}{(n+1)!} \cdot \frac{1}{1 - \frac{1}{n+1}} \\ &= \frac{1}{(n+1)!} \cdot \frac{n+1}{n} = \frac{1}{n!\,n} \end{aligned}$$

Now suppose that e were rational and that $e = p/q$, where $p, q \in \mathbb{Z}, q \neq$, and $\gcd(p,q) = 1$. Of course, $p, q > 0$ as $e > 0$. By the work above, we have $0 < e - s_q < \frac{1}{q!\,q}$ so that $0 < q!(e - s_q) < \frac{1}{q}$ which holds if and only if $0 < q!e - q!s_q < \frac{1}{q}$. By assumption, $e = p/q$ so that $q!e = (q-1)!p \in \mathbb{Z}$. Furthermore,

$$q!s = q!\left(\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{q!}\right) \in \mathbb{Z}$$

Therefore, this shows that $q!(e - s_q)$ is an integer. But then as $0 < q!(e - s_q) < \frac{1}{q}$ and $q \geq 1$ this implies there is an integer between 0 and 1, a contradiction. □

2. Let $a_n, b_n \geq 0$. Assume that $\sum a_n$ converges and that $\limsup \frac{b_n}{a_n} \leq M < \infty$. Show that $\sum b_n$ converges.

Solution: As $\limsup \frac{b_n}{a_n} \leq M < \infty$, there is a $n_0 \in \mathbb{N}$ such that $\frac{b_n}{a_n} \leq M$ for all $n > n_0$. But then

$$0 \leq b_n \leq M a_n$$

for all $n > n_0$. As $\sum a_n$ converges, $M \sum a_n$ converges so that $M \sum_{n>n_0} a_n$ converges. But then we have $\sum_{n>n_0} b_n$ converges. But

$$\sum b_n = \sum_{n=0}^{n_0} b_n + \sum_{n>n_0} b_n$$

is the sum of two convergent series. Therefore, $\sum b_n$ converges. □

3. Let f be bounded on the real interval (a, b), show that if addition f is both continuous and monotone then f is uniformly continuous.

4. Define

$$f(x) = \begin{cases} 0, & x \text{ irrational} \\ \frac{1}{n}, & x = \frac{m}{n}, \text{ where } m, n \end{cases}$$

Prove that f is integrable on $[0,1]$.[29]

Solution: Note that by definition, $f(x) \geq 0$ for all $x \in [0,1]$. If $x \in \mathbb{Q}$, we force $x = \frac{m}{n}$, where $m, n \in \mathbb{Z}_+$ to avoid $x = \frac{m}{n} = \frac{-m}{-n}$. Let $P = \{x_0, \ldots, x_n\}$ be a partition of $[0,1]$. Since the irrational numbers are dense in $\mathbb{R}$, there exists an irrational number in each interval $[x_i, x_{i+1}]$ for $i = 0, \ldots, n-1\}$. Thus, we must have $L(P,f) = 0$ for every partition P of $[0,1]$. Hence to show that $f(x)$ is integrable, it is sufficient to show for every $\epsilon > 0$, there exists a partition P with $U(P,f) < \epsilon$.

Let $S_n = \{x \colon f(x) \geq \frac{1}{n}\}$. If $x \in S_n$, then $x = \frac{r}{s}$, where $r, s \leq n$. In particular since $0 \leq r, s \leq n$, the set S_n is finite as it can *at most* contain the elements $\{\frac{r}{s} \colon r = 0, \ldots, n, s = 1, \ldots, n\}$.

Let $\epsilon > 0$ and choose $n \in \mathbb{N}$ such that $\frac{1}{n} < \frac{\epsilon}{2}$. Let $E = \{i \colon S_n \cap [x_i, x_{i+1}] = \emptyset\}$. It is clear that $|E| \leq |S_n|$, where $|\cdot|$ represents the cardinality of the set. If $i \in E$, then $M_i < \frac{1}{n} < \frac{\epsilon}{2}$ and if $i \notin E$ then $M_i = 1$, where $M_i = \sup_{x \in [x_i, x_{i+1}]} f(x)$. Observe $\Delta x_i = x_{i+1} - x_i < \frac{\epsilon}{2|S_n|}$. But then we have

$$\begin{aligned} U(P,f) &= \sum_{i=1}^{n} M_i \Delta x_i \\ &= \sum_{i \in E} M_i \Delta x_i + \sum_{i \notin E} M_i \Delta x_i \\ &< \sum_{i \in E} \frac{\epsilon}{2} \Delta x_i + \sum_{i \notin E} \Delta x_i \\ &< \frac{\epsilon}{2} + |S_n| \cdot \frac{\epsilon}{2|S_n|} \\ &< \epsilon. \end{aligned}$$

But then $U(P,f) = U(P,f) - L(P,f) < \epsilon$. Therefore, $f(x)$ is integrable. Furthermore,

$$0 = L(P,f) \leq \int_0^1 f(x)\, dx \leq U(P,f) < \epsilon.$$

But then $\int_0^1 f(x)\, dx = 0$. □

5. Let $\{f_n\}$ be a sequence of uniformly bounded Riemann integrable function on $[0,1]$, set $F_n(s) = \int_0^s f_n(t)\, dt$ for $0 \leq s \leq 1$. Prove that a subsequence of $\{F_n\}$ converges uniformly

[29] Note: it is assumed $f(x) = \frac{1}{n}$ when $x = \frac{m}{n} \in \mathbb{Q}$. If $x = 0$, the given $f(x)$ is not well defined. We assume $f(x) = 1$ if $x = 0$ so that f is continuous at every irrational number but discontinuous at every rational number, as one can show. However, this value does not affect integrability or the value of the integral.

on $[0,1]$.

Solution: The space $[0,1]$ is compact. We know also that $F_n(s)$ is continuous on $[0,1]$. By assumption, the set $\{f_n\}$ is uniformly bounded. Suppose that $|f_n(x)| \leq M$ for all n and $x \in [0,1]$. Then

$$|F_n(s)| = \left| \int_0^s f_n(t)\, dt \right| \leq \int_0^s |f_n(t)|\, dt \leq \int_0^s M\, dt = Ms \leq M(1-0) = M$$

Therefore, $\{F_n(s)\}$ is uniformly bounded for all n and $s \in [0,1]$. Now we see that $\{F_n\}$ is (uniformly) equicontinuous: suppose that $s > r$, then we have

$$|F_n(s) - F_n(t)| = \left| \int_r^s f_n(t)\, dt \right| \leq \int_r^s |f_n(t)|\, dt \leq \int_r^s M\, dt = M(r-s) \leq M(1-0) = M$$

Then given $\epsilon > 0$, simply choose $\delta = \epsilon/M$. Therefore given $|s-r| < \delta$, we have $|F_n(s) - F_n(t)| \leq M(r-s) < M\delta < \epsilon$ so that $\{F_n\}$ is (uniformly) equicontinuous. But then there is a subsequence of $\{F_n(s)\}$ that converges for each $s \in [0,1]$. □

6. Let $f(x)$ be a differentiable mapping of the connected open subset V of $\mathbb{R}^n$. Suppose that $f'(x) = 0$ on V, prove that f is constant on V.

Solution: Fix $x \in V$ and define $S = \{y \in V : f(y) = f(x)\}$. Note that S is nonempty as $x \in S$. We need show that S is open and closed.

Let $y \in S$, then $y \in V$ so that there exists $r > 0$ such that $N_r(y) \subseteq V$ since V is open. But $N_r(y)$ is a convex, open subset of $\mathbb{R}^n$ and $\|f'(x)\| \leq 0$ for all $x \in N_r(y)$. Then $|f(u) - f(v)| \leq 0|u-v| = 0$ for all $u, v \in N_r(y)$. Then $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $N_r(y) \subseteq S$ so that S is open.

Now let $\{y_n\} \subseteq S$ be a sequence such that $y_n \to y \in V$. Since V is open, there exists $r > 0$ such that $N_r(y) \subseteq V$. Now as $N_r(y)$ is convex, $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $f(y_n) = f(x)$ as $y_n \in S$. But $\lim f(y_n) = f(y)$ since f is continuous. But then $f(x) = f(y)$ so that S is closed.

Now S is both open and closed in V. Since S is nonempty and V is connected, it must be that $S = V$. Therefore, f is constant on V. □

7. Let $f(x,y) = (u,v)$, where $u = x^2 - y^2$ and $v = 2xy$. Describe a map from $\mathbb{R}^2$ to $\mathbb{R}^2$.

(a) What is the range of this map?

(b) Show there is no neighborhood of $(0,0)$ in which f has an inverse.

August 2001

1. Let A be an uncountable set of real numbers. Prove that A has an accumulation point.

Solution: Let $A_n = A \cap [n, n+1]$. As $A = \cup_{n\in\mathbb{Z}} A_n$, if each A_n were countable then A would be the countable union of countable sets, hence countable, a contradiction. Then for some $n_0 \in \mathbb{Z}$, A_{n_0} is uncountable. However, $A_{n_0} \subset [n_0, n_0+1]$. But then A_{n_0} is an infinite subset of a compact set in $\mathbb{R}$ so that A_{n_0} has a limit point in $[n_0, n_0+1]$, say x. But for each $\epsilon > 0$, there is a $y \in A_{n_0}$ such that $B(x, \epsilon)$. But $y \in A$ so that x is a limit points of A. □

2. Let $f(x)$ be a differentiable mapping of the connected open subset V of $\mathbb{R}^n$. Suppose that $f'(x) = 0$ on V. Prove that f is constant on V.

Solution: Fix $x \in V$ and define $S = \{y \in V : f(y) = f(x)\}$. Note that S is nonempty as $x \in S$. We need show that S is open and closed.

Let $y \in S$, then $y \in V$ so that there exists $r > 0$ such that $N_r(y) \subseteq V$ since V is open. But $N_r(y)$ is a convex, open subset of $\mathbb{R}^n$ and $\|f'(x)\| \leq 0$ for all $x \in N_r(y)$. Then $|f(u) - f(v)| \leq 0|u - v| = 0$ for all $u, v \in N_r(y)$. Then $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $N_r(y) \subseteq S$ so that S is open.

Now let $\{y_n\} \subseteq S$ be a sequence such that $y_n \to y \in V$. Since V is open, there exists $r > 0$ such that $N_r(y) \subseteq V$. Now as $N_r(y)$ is convex, $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $f(y_n) = f(x)$ as $y_n \in S$. But $\lim f(y_n) = f(y)$ since f is continuous. But then $f(x) = f(y)$ so that S is closed.

Now S is both open and closed in V. Since S is nonempty and V is connected, it must be that $S = V$. Therefore, f is constant on V. □

3. Prove or disprove: the function $f(x) = x^{3/2} \log x$ is uniformly continuous on the interval $(0, 1)$.

Solution: First, observe that $g(x) = x^{3/2}$ and $h(x) = \log x$ are differentiable on $(0, 1)$. We have $g'(x) = \frac{3}{2}x^{1/2}$ and $h'(x) = \frac{1}{x}$. Now using l'Hôpital's Rule, we have

$$\lim_{x\to 0} x^{3/2} \log x = \lim_{x\to 0} \frac{\log x}{\frac{1}{x^{3/2}}} \overset{\text{L.H.}}{=} \lim_{x\to 0} \frac{\frac{1}{x}}{-\frac{3}{2x^{5/2}}} = \lim_{x\to 0} \left(-\frac{2}{3}x^{3/2}\right) = 0.$$

Furthermore, we have $\lim_{x\to 1} g(x) = 1$ and $\lim_{x\to 1} h(x) = 0$ so that $\lim_{x\to 1} g(x)h(x) = \lim_{x\to 1} g(x) \cdot \lim_{x\to 1} h(x) = 1 \cdot 0 = 0$. Finally, since $g(x)$ and $h(x)$ are differentiable on $(0, 1)$, they are continuous on $(0, 1)$, forcing their product $f(x)$ to be continuous on $(0, 1)$.

Define $F(x)$ via

$$F(x) = \begin{cases} f(x), & x \in (0,1) \\ 0, & \text{otherwise} \end{cases}$$

Now by the work above $F(x)$ is continuous on $[0,1]$. But then F is continuous on a compact interval and is hence uniformly continuous. But then $F(x)$ is uniformly continuous on $(0,1)$. But $F(x) = f(x)$ on $(0,1)$ by construction. Therefore, $f(x)$ is uniformly continuous on $(0,1)$. □

4. Let $f(x,y) = (u,v)$, where $u = x^2 - y^2$ and $v = 2xy$ describe a map from $\mathbb{R}^2$ to $\mathbb{R}^2$.

(a) What is the range of this map?

(b) Show that if $(u,v) \neq (0,0)$ then f has an inverse in a neighborhood of (u,v).

(c) Show that there is no neighborhood of $(0,0)$ in which f has an inverse.

5. Prove that

$$\sum_{n=1}^{\infty} \frac{\sin(n^4 x)}{n^2}$$

defines a continuous function on $\mathbb{R}$.

Solution: Let $f_n(x) = \frac{\sin(n^4 x)}{n^2}$. It is clear that $f_n(x)$ is continuous for each $n \in \mathbb{N}$. It is clear also that

$$\left| \sum_{n=1}^{\infty} \frac{\sin(n^4 x)}{n^2} \right| \leq \sum_{n=1}^{\infty} \left| \frac{\sin(n^4 x)}{n^2} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$$

so that by the Weierstrass M-test, $\sum_{n=1}^{\infty} f_n(x) = \sum_{n=1}^{\infty} \frac{\sin(n^4 x)}{n^2}$ converges uniformly on $\mathbb{R}$. That is, $g_m(x) = \sum_{n=1}^{m} f_n(x)$ converges uniformly. Each $g_m(x)$ is continuous as it is the finite sum of continuous functions. But then g_m is a sequence of continuous functions that converges uniformly so that the limit, namely $\sum_{n=1}^{\infty} \frac{\sin(n^4 x)}{n^2}$ is continuous. □

6.

(a) Find the limit

$$\lim_{\lambda \to \infty} \lambda \int_{-1}^{1} e^{-\lambda |y|} \, dy.$$

(b) Let $g : \mathbb{R} \to \mathbb{R}$ be a bounded, continuous function. For $x \in \mathbb{R}$, find the limit

$$\lim_{\lambda \to \infty} \lambda \int_{-1}^{1} g(x+y) e^{-\lambda |y|} \, dy.$$

Hint: Try a "nice" g first, formulate a guess, and then try to prove your guess is correct.

January 2002

1. Let A and B be subsets of a metric space. Prove that $\overline{A \cap B} \subset \overline{A} \cap \overline{B}$ and given an example when $\overline{A \cap B} \neq \overline{A} \cap \overline{B}$.

Solution: Let $x \in \overline{A \cap B}$. If $x \in A \cap B$, then $x \in A \subset \overline{A}$ and $x \in B \subset \overline{B}$. But then $x \in \overline{A} \cap \overline{B}$. Now if $x \in (A \cap B)'$ then all neighborhoods of x intersect $A \cap B$ at a point y distinct from x. But observe that $y \in A$ and $y \in B$. But then $x \in A'$ and $x \in B'$ so that $x \in \overline{A}$ and $x \in \overline{B}$. Therefore, $x \in \overline{A} \cap \overline{B}$. This shows that $\overline{A \cap B} \subset \overline{A} \cap \overline{B}$.

To see strict inclusion, take $A = (-1, 0)$ and $B = (0, 1)$. Then we have $\overline{A} = [-1, 0]$ and $\overline{B} = [0, 1]$ so that $\overline{A \cap B} = \emptyset$ and $\overline{A} \cap \overline{B} = \{0\}$. As another example we have $A = (0, 1) \cup \mathbb{N}$ and $B = (-1, 0) \cup \mathbb{N}$. Then we have $\overline{A} = [0, 1] \cup \mathbb{N}$ and $\overline{B} = [-1, 0] \cup \mathbb{N}$ so that $\overline{A \cap B} = \mathbb{N}$ and $\overline{A} \cap \overline{B} = \mathbb{N} \cup \{0\}$. As a final example, take $A = \mathbb{Q}$ and $B = \mathbb{Q}^C$. Then we have $\overline{A} = \mathbb{R}$ and $\overline{B} = \mathbb{R}$ so that $\overline{A \cap B} = \emptyset$ and $\overline{A} \cap \overline{B} = \mathbb{R}$. □

2. Let f and f' be continuous functions on $\mathbb{R}$. Prove that the sequence of functions

$$g_n(x) = \frac{f(x + 1/n) - f(x)}{1/n}$$

converges to $f'(x)$ uniformly on every interval $[a, b]$, $-\infty < a < b < \infty$.

3. Let f be a Riemann integrable function on $[0, 1]$ and

$$F(x) = \int_0^x f(t)\, dt$$

(a) Show that there is a constant C such that $|F(x) - F(y)| \leq C|x - y|$ for every $x, y \in [0, 1]$.

(b) Given an example of f such that F is not differentiable at some point.

Solution:

(a) Since $f(t)$ is Riemann integrable on $[0, 1]$, we know that $f(t)$ is bounded on $[0, 1]$. Suppose that $|f(t)| \leq M$ for all $t \in [0, 1]$. Without loss of generality, suppose that $x > y$, then

$$\begin{aligned} |F(x) - F(x)| &= \left| \int_0^x f(t)\, dt - \int_0^y f(t)\, dt \right| \\ &= \left| \int_y^x f(t)\, dt \right| \\ &\leq \int_y^x |f(t)|\, dt \\ &\leq \int_y^x M\, dt = M(x - y) = M|x - y| \end{aligned}$$

(b) If $f(t)$ is continuous on $[0,1]$, then we know that $F(x)$ is differentiable on $[0,1]$. Our example must need then be not continuous at some point. Let

$$f(t) = \begin{cases} 0, & t \in [0, \frac{1}{2}) \\ 1, & t \in [\frac{1}{2}, 1] \end{cases}$$

Then we have

$$\frac{F(1/2+h) - F(1/2)}{h} = \frac{\int_0^{\frac{1}{2}+h} f(t)\, dt - 0}{h} = \frac{1}{h}\int_0^{\frac{1}{2}+h} f(t)\, dt = \frac{1}{h}\int_{\frac{1}{2}}^{\frac{1}{2}+h} 1\, dt = \frac{h}{h} = 1$$

so that $F(x)$ clearly cannot be differentiable at $x = \frac{1}{2}$.

□

4. Show that the sequence

$$f_n(x) = \frac{\tan^{-1}(nx)}{\sqrt{n}}$$

is equicontinuous on $\mathbb{R}$ and converges uniformly to $f(x) = \lim_{n\to\infty} f_n(x)$.

Solution:

5. Determine the values of α for which f is differentiable at $(0,0)$ when

$$f(x,y) = \begin{cases} (x^2+y^2)^\alpha \sin\left(\dfrac{1}{x^2+y^2}\right), & (x,y) \neq (0,0) \\ 0, & (x,y) = (0,0) \end{cases}$$

6. Show that if $\phi(y)$ is a continuously differentiable function on $(-a,a)$, $a > 0$, such that $\phi(0) = 0$ and $|\phi'(y)| \leq k < 1$ on $(-a,a)$, then there is $\epsilon > 0$ and a unique differentiable function g on $(-\epsilon,\epsilon)$ satisfying the equation $x = g(x) + \phi(g(x))$.

August 2002

1. Let $f : (0,1) \to \mathbb{R}$ be continuous, bounded, and decreasing. Prove that f is uniformly continuous on $(0,1)$.

Solution: We show that $f(x)$ has a continuous extension $g(x)$ on $[0,1]$. That is, there is a continuous function $g(x) : [0,1] \to \mathbb{R}$ such that $g(x) = f(x)$ on $(0,1)$. But as $g(x)$ is continuous on a compact set so that it is uniformly continuous and as $g(x) = f(x)$ on $(0,1)$, we know that $f(x)$ is uniformly continuous on $(0,1)$.

As $f(x)$ is decreasing, $f(x) < f(y)$ if $x > y$. Let $L = \inf\{f(x) \mid x \in (0,1)\}$. As $f(x)$ is bounded, it is clear that L is finite. Let $\epsilon > 0$ be given. By the properties of the infimum, there is a $y_0 = f(x_0)$ such that $L \leq y_0 \leq L + \epsilon$. Choose $\delta = 1 - x_0 > 0$ so that $0 < 1 - x < \delta$ for $x \in (x_0, 1)$. But then $L \leq f(x) < f(x_0) < L + \epsilon$. But this shows for $x \in (x_0, 1)$, we have $|f(x) - L| < \epsilon$. As $f(x)$ is continuous, this shows that $f(x) \to L$ as $x \to 1$. If $L' = \sup\{f(x) \mid x \in (0,1)\}$, a similar argument shows that $\lim_{x\to 0} f(x) = L'$. Define

$$g(x) = \begin{cases} L', & x = 0 \\ f(x), & 0 < x < 1 \\ L, & x = 1 \end{cases}$$

The work above shows that $g(x)$ is continuous then the comments above show that $f(x)$ is uniformly continuous. □

2. Consider the function $f : \mathbb{R}^n \to \mathbb{R}$ given by $f(x) = \frac{\sum_{j=1}^n x_j^3}{\|x\|^2}$ if $x \neq 0$ and $f(0) = 0$, where $x = (x_1, x_2, \cdots, x_n)$ and $\|x\|$ is the Euclidean norm of x. Prove that f is continuous on $\mathbb{R}^n$.

Solution: Observe that $\sum_{j=1}^n x_j^3 = x_1^3 + x_2^3 + \cdots + x_n^3$ and $\|x\|^2 = x_1^2 + x_2^2 + \cdots + x_n^2$ are both polynomial functions in n variables, which are continuous. If $f(x), g(x)$ are continuous, then $\frac{f(x)}{g(x)}$ is continuous at x if $g(x) \neq 0$ at x. It follows immediately that $f(x)$ is continuous if $\|x\|^2 \neq 0$. But as $\|\cdot\|$ is a norm, $\|x\| = 0$ if and only if $\boldsymbol{x} = \mathbf{0}$. We then only need consider continuity at the origin. That is, given $\epsilon > 0$, we need produce a $\delta > 0$ such that

$$|f(x) - f(0)| = \left| \frac{\sum_{j=1}^n x_j^3}{\|x\|^2} - 0 \right| = \left| \frac{\sum_{j=1}^n x_j^3}{\|x\|^2} \right| < \epsilon$$

We do this by induction. If $n = 1$, we have $f_1(x) = \frac{x^3}{x^2} = x$ and $f(0) = 0$. But this is trivially

continuous at the origin. Now assume that $f_n(x)$ is continuous for $n = 1, 2, \cdots, k$. Then

$$\begin{aligned}
|f_{k+1}(x) - f(0)| &= \left| \frac{\sum_{j=1}^{k+1} x_j^3}{\|x\|^2} - 0 \right| \\
&= \left| \frac{\sum_{j=1}^{k+1} x_j^3}{\|x\|^2} \right| \\
&= \left| \frac{x_1^3 + x_2^3 + \cdots + x_k^3 + x_{k+1}^3}{x_1^2 + x_2^2 + \cdots + x_k^2 + x_{k+1}^2} \right| \\
&\leq \left| \frac{x_1^3 + x_2^3 + \cdots + x_k^3 + x_{k+1}^3}{x_1^2 + x_2^2 + \cdots + x_k^2} \right| \\
&= \left| \frac{x_1^3 + x_2^3 + \cdots + x_k^3}{x_1^2 + x_2^2 + \cdots + x_k^2} + \frac{x_{k+1}^3}{x_1^2 + x_2^2 + \cdots + x_k^2} \right| \\
&= \left| f_k(x) + \frac{x_{k+1}^3}{x_1^2 + x_2^2 + \cdots + x_k^2} \right|
\end{aligned}$$

3. Prove that the system

$$\begin{aligned}
xy^5 + yu^5 + zv^5 &= 1 \\
x^5y + y^5u + z^5v &= 1
\end{aligned}$$

has a unique solution $u = f(x, y, z)$, $v = g(x, y, z)$ in a neighborhood of the point $(u, v, x, y, z) = (1, 0, 0, 1, 1)$. Find $\frac{\partial u}{\partial x}(0, 1, 1)$.

Solution: Let $F(u, v, x, y, z) = (xy^5 + yu^5 + zv^5 - 1, x^5y + y^5u + z^5v - 1)$. It is routine to check that $F(1, 0, 0, 1, 1) = (0, 0)$. $F(u, v, x, y, z)$ has Jacobian

$$\begin{pmatrix} 5yu^4 & 5zv^4 & y^5 & 5xy^4 + u^5 & v^5 \\ y^5 & z^5 & 5x^4y & x^5 + 5y^4u & 5z^4v \end{pmatrix}$$

Since each of these partials exist and are continuous, we know that $F(u, v, x, y, z)$ is continuously differentiable on $\mathbb{R}^5$. At the point $(u, v, x, y, z) = (1, 0, 0, 1, 1)$, this Jacobian is

$$\begin{pmatrix} 5 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 5 & 0 \end{pmatrix}$$

We also have $F_{u,v}$

$$\begin{vmatrix} 5 & 0 \\ 1 & 1 \end{vmatrix} = 5 \neq 0$$

Then by the Implicit Function Theorem, there are unique functions $f(x,y,z)$ and $g(x,y,z)$ such that $u = f(x,y,z)$ and $v = g(x,y,z)$ on some open set about $(1,0,0,1,1)$. Furthermore by the Implicit Function Theorem, we have

$$\frac{\partial u}{\partial x}(0,1,1) = -\frac{\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}}{\begin{vmatrix} 5 & 0 \\ 1 & 1 \end{vmatrix}} = -\frac{1}{5}$$

□

4. Let $\mathbb{Q}_0$ be the set of rationals in the interval $[0,1]$. For a bounded function $f : \mathbb{Q}_0 \to \mathbb{R}$ and $n = 1, 2, \cdots$, define

$$S_n(f) = \frac{1}{n}\sum_{k=1}^{n} f(k/n)$$

If $\lim_{n\to\infty} S_n(f)$ exists, we say that f is S-summable and let $S(f) = \lim_{n\to\infty} S_n(f)$ denote this limit. Let $f_1, f_2, \cdots$ be bounded functions on $\mathbb{Q}_0$ which are S-summable and suppose that $f_k \to f$ uniformly on $\mathbb{Q}_0$ as $k \to \infty$. Prove that f is S-summable and that $\lim_{k\to\infty} S(f_k) = S(f)$.

5. Let $a_1, a_2, \cdots$ be a sequence of real numbers such that $\lim_{k\to\infty} a_k = L \in \mathbb{R}$ exists. For $0 < p < 1$, define

$$A(p) = \sum_{k=1}^{\infty} p(1-p)^{k-1} a_k$$

Prove that this sum converges and that $\lim_{p\to 0} A(p) = L$.

6. Prove that

$$\lim_{n\to\infty} \frac{1}{n^{5/2}} \sum_{k=1}^{n} k^{3/2} = \frac{2}{5}$$

January 2003

1. Prove that a continuous function on $\mathbb{R}$ has a finite or countable number of strict local maxima.

Solution: Let $S = \{x_0 \colon \exists \delta > 0 \ni |x - x_0| < \delta \Rightarrow f(x) < f(x_0)\}$. We must show that S is at most countable. We look at $N_{\delta_0}(x_0)$ for each $x_0 \in S$ such that δ is as small as possible. Note that since f is continuous, each open neighborhood contains only one point of S. Then choose a rational number in each open neighborhood (since $\mathbb{Q}$ is dense in $\mathbb{R}$, this is possible). But note that $\mathbb{Q}$ is at most countable. Therefore, the number of open neighborhoods is at most countable. Therefore, S is at most countable.

OR

Let M be the set of strict local maxima of a function f. For each $x \in M$, there is a $\delta_x > 0$ such that $|f(x)| > y$ for all $|x - y| < \delta$ as x is a strict maxima. Let $\delta_0 = \min \delta_x/2$ for all $x \in M$. It is clear that $\delta_0 > 0$ for otherwise there is a maxima with no neighborhood about it so as to be the only maxima. But one can cover $\mathbb{R}$ with intervals of length δ_0, each containing at most one maxima. We can also choose a single rational for each of these intervals so that the number of strict maxima are at most countable. □

2. Proof or counterexample: Let f be a continuous function on $[0, 1]$ that is differentiable on a dense subset. Also, $f' > 0$ wherever it is defined. Then f is increasing. (Hint: think about the Cantor function.)

Solution:

3. Find

$$\lim_{n\to\infty} n^2 \int_0^1 e^{x^2} x^n (1 - x)\, dx.$$

Hint: $\lim_{n\to\infty} n^2 \int_0^1 x^n (1 - x)\, dx = 1$.

Solution: First, recall that $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ so that

$$e^{x^2} = \sum_{k=0}^{\infty} \frac{x^{2k}}{k!}.$$

and the convergence of the summation to e^{x^2} is uniform on $[0,1]$. But then

$$\begin{aligned}\lim_{n\to\infty} n^2 \int_0^1 e^{x^2} x^n (1-x)\, dx &= \lim_{n\to\infty} n^2 \int_0^1 \sum_{k=0}^{n} \frac{x^{2k}}{k!} x^n (1-x)\, dx \\ &= \lim_{n\to\infty} n^2 \int_0^1 \sum k = 0^n \frac{x^{2k+n}}{k!} (1-x)\, dx \\ &= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} \int_0^1 x^{2k+n} (1-x)\, dx\end{aligned}$$

Now

$$\begin{aligned}\lim_{n\to\infty} n^2 \int_0^1 x^{2k+n} (1-x)\, dx &= \lim_{n\to\infty} n^2 \int_0^1 x^n (1-x)\, dx \\ &= \lim_{n\to\infty} n^2 \int_0^1 x^n - x^{n+1}\, dx \\ &= \lim_{n\to\infty} n^2 \left[\frac{x^{n+1}}{n+1} - \frac{x^{n+2}}{n+2} \right]_0^1 \\ &= \lim_{n\to\infty} n^2 \left[\frac{1}{n+1} - \frac{1}{n+2} \right] \\ &= \lim_{n\to\infty} \frac{n^2}{(n+1)(n+2)} \\ &= 1\end{aligned}$$

Therefore,

$$\begin{aligned}\lim_{n\to\infty} n^2 \int_0^1 e^{x^2} x^n (1-x)\, dx &= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} \int_0^1 x^{2k+n} (1-x)\, dx \\ &= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \\ &= e\end{aligned}$$

□

4. Let $a_n, b_n \geq 0$. Assume that $\sum a_n$ converges and that $\limsup \frac{b_n}{a_n} \leq M < \infty$. Show that $\sum b_n$ converges.

Solution: As $\limsup \frac{b_n}{a_n} \leq M < \infty$, there is a $n_0 \in \mathbb{N}$ such that $\frac{b_n}{a_n} \leq M$ for all $n > n_0$. But then

$$0 \leq b_n \leq M a_n$$

for all $n > n_0$. As $\sum a_n$ converges, $M\sum a_n$ converges so that $M\sum_{n>n_0} a_n$ converges. But then we have $\sum_{n>n_0} b_n$ converges. But

$$\sum b_n = \sum_{n=0}^{n_0} b_n + \sum_{n>n_0} b_n$$

is the sum of two convergent series. Therefore, $\sum b_n$ converges. □

5. Let $f(x)$ be a differentiable mapping of the connected open subset V of $\mathbb{R}^n$ to $\mathbb{R}^m$. Suppose that $f'(x) = 0$ on V. Prove that f is constant on V.

Solution: Fix $x \in V$ and define $S = \{y \in V : f(y) = f(x)\}$. Note that S is nonempty as $x \in S$. We need show that S is open and closed.

Let $y \in S$, then $y \in V$ so that there exists $r > 0$ such that $N_r(y) \subseteq V$ since V is open. But $N_r(y)$ is a convex, open subset of $\mathbb{R}^n$ and $\|f'(x)\| \leq 0$ for all $x \in N_r(y)$. Then $|f(u) - f(v)| \leq 0|u - v| = 0$ for all $u, v \in N_r(y)$. Then $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $N_r(y) \subseteq S$ so that S is open.

Now let $\{y_n\} \subseteq S$ be a sequence such that $y_n \to y \in V$. Since V is open, there exists $r > 0$ such that $N_r(y) \subseteq V$. Now as $N_r(y)$ is convex, $f(u) = f(v)$ for all $u, v \in N_r(y)$. But then $f(y_n) = f(x)$ as $y_n \in S$. But $\lim f(y_n) = f(y)$ since f is continuous. But then $f(x) = f(y)$ so that S is closed.

Now S is both open and closed in V. Since S is nonempty and V is connected, it must be that $S = V$. Therefore, f is constant on V. □

6. Let $f(x, y) = (u, v)$, where $u = x^4 - y^4$ and $v = 2xy$, be a map from $\mathbb{R}^2$ to $\mathbb{R}^2$.

(a) Show that if $(u, v) \neq (0, 0)$ then f has an inverse in a neighborhood of (u, v).

(b) Show that there is no neighborhood of $(0, 0)$ in which f has an inverse.

Solution:

(a) We have

$$J_f(x, y) = \det \begin{pmatrix} 4x^3 & -4y^3 \\ 2y & 2x \end{pmatrix} = 8x^4 + 8y^4$$

Then $(u, v) = (0, 0)$ if and only if $x^4 - y^4 = 0$ and $2xy = 0$ if and only if $x = \pm y$ and $x = 0$ or $y = 0$ if and only if $(x, y) = (0, 0)$. So if $(u, v) \neq (0, 0)$, then $(x, y) \neq (0, 0)$ and $J_f(x, y) \neq 0$. Clearly, $f \in C'(\mathbb{R}^2)$ since all the partial derivatives for f exist and are continuos. By the Inverse Function Theorem, f has an inverse in a neighborhood of (u, v).

(b) Let $N_r(0,0)$ be a neighborhood of $(0,0)$. Let $(x,y) \in N_r(0,0)$, then $(-x,-y) \in N_r(0,0)$. But $f(x,y) = (x^4 - y^4, 2xy) = ((-x)^4 - (-y)^4, 2(-x)(-y)) = f(-x,-y)$. But then f cannot be injective in a neighborhood of $(0,0)$. But then f is not injective in any neighborhood of $(0,0)$ so that there can exist no neighborhood of $(0,0)$ in which f has an inverse.

□

August 2003

1. If f is continuous on $[a,b]$ and

$$F(x) = \int_a^x f(t)\,dt$$

for $x \in [a,b]$, show that $F' = f$ on (a,b).

Solution: Let $x \in [a,b]$, $\epsilon > 0$, and h be such that $x+h < b$ and $0 < h < \delta$ (δ given by the continuity of f below). Observe that

$$\frac{F(x+h)-F(x)}{h} = \frac{\int_a^{x+h} f(t)\,dt - \int_a^x f(t)\,dt}{h} = \frac{\int_x^{x+h} f(t)\,dt}{h} = \frac{1}{h}\int_x^{x+h} f(t)\,dt$$

As f is continuous at x, there is a $\delta > 0$ such that when $|f(t)-f(x)| < \epsilon$ whenever $|t-x| < \delta$. Now if $t \in [x, x+h]$, $x \le t \le x+h$ so that $0 < t-x \le h < \delta$. But then $|t-x| < \delta$ so that $|f(t)-f(x)| < \epsilon$. Then $f(x)-\epsilon < f(t) < f(x)+\epsilon$ and

$$\begin{aligned}
f(x)-\epsilon < & f(t) < f(x)+\epsilon \\
\int_x^{x+h} (f(x)-\epsilon)\,dt < & \int_x^{x+h} f(t)\,dt < \int_x^{x+h} (f(x)+\epsilon)\,dt \\
(f(x)-\epsilon)\int_x^{x+h} dt < & \int_x^{x+h} f(t)\,dt < (f(x)+\epsilon)\int_x^{x+h} dt \\
(f(x)-\epsilon)\,h < & \int_x^{x+h} f(t)\,dt < (f(x)+\epsilon)\,h \\
f(x)-\epsilon < & \frac{1}{h}\int_x^{x+h} f(t)\,dt < f(x)+\epsilon \\
-\epsilon < & \frac{1}{h}\int_x^{x+h} f(t)\,dt - f(x) < \epsilon
\end{aligned}$$

so that $\left|\frac{F(x+h)-F(x)}{h} - f(x)\right| < \epsilon$. But then $F'(x)$ exists for $x \in (a,b)$ and $F' = f$ on (a,b).

OR

Consider $x \in (a,b)$. Let $h > 0$ sufficiently small so that $x+h \in [a,b]$. [For instance, take $h = (b-a)/n$ for some $n \in \mathbb{N}_{>1}$.]

$$\begin{aligned}
\frac{F(x+h)-F(x)}{(x+h)-x} &= \frac{\int_a^{x+h} f(t)\,dt - \int_a^x f(t)\,dt}{h} \\
&= \frac{1}{h}\int_x^{x+h} f(t)\,dt
\end{aligned}$$

As $f(x)$ is continuous on $[a,b]$, the Extreme Value Theorem says that there are $r,s \in [a,b]$ such that $f(r) = m$ and $f(s) = M$, where m, M are the minimum and maximum of $f(x)$ on $[a,b]$, respectively. But then we have

$$\frac{1}{h}\int_x^{x+h} m\ dt \leq \frac{1}{h}\int_x^{x+h} f(t)\ dt \leq \frac{1}{h}\int_x^{x+h} M\ dt$$

But simple calculation shows that

$$\frac{1}{h}\int_x^{x+h} m\ dt = \frac{hm}{h} = m$$
$$\frac{1}{h}\int_x^{x+h} M\ dt = \frac{hM}{h} = M$$

Therefore, we have

$$f(r) = m \leq \frac{1}{h}\int_x^{x+h} f(t)\ dt \leq M = f(s)$$
$$f(r) = m \leq \frac{F(x+h) - F(x)}{(x+h) - x} \leq M = f(s).$$

We obtain the same inequality considering $h < 0$ such that $x + h \in [a,b]$ (again, one can take $h = (a-x)/n$ for some $n \in \mathbb{N}_{>1}$), mutatis mutandis. Given $\epsilon > 0$, we can find a $N \in \mathbb{N}$ such that $N > (b-a)/\epsilon$, implying $(b-a)/N < \epsilon$. But then taking h as above with $n > N$, we have $|h| < \epsilon$. Furthermore, $r, s \in (x - |h|, x + |h|) \subset B_\epsilon(x)$. As $r \to x$ and $s \to x$ as $n \to \infty$ and f is continuous, $\lim_{|h|\to 0} f(r) = \lim_{r\to x} f(r) = f(x)$ and $\lim_{|h|\to 0} f(s) = \lim_{s\to x} f(s) = f(x)$. Then by the Squeeze Theorem,

$$F'(x) := \lim_{h\to 0} \frac{F(x+h) - F(x)}{(x+h) - x} = f(x).$$

□

2. Prove that

$$\left(\sum_{k=1}^{n} \frac{1}{k}\right) - \ln n \to \gamma$$

for some $\gamma \in (1/2, 1)$.

Solution: Let $x_n = \left(\sum_{k=1}^{n} \frac{1}{k}\right) - \log n$. Observe that

$$x_n - x_{n-1} = \frac{1}{n} - \log n + \log(n-1) = \frac{1}{n} + \log\left(1 - \frac{1}{n}\right) < 0,$$

where the inequality follows from the fact that $\log(1-x)$ is a concave function (simply examine its derivative) and hence lies beneath $y = -x$ and this line is tangent to $\log(1-x)$, evaluating this function at $x = \frac{1}{n}$, we have $\log\left(1 - \frac{1}{n}\right) \leq -\frac{1}{n}$.

Moreover, this sequence is bounded below as

$$x_n = \sum_{k=1}^{n} \frac{1}{k} > \int_1^{n+1} \frac{dt}{t} = \log(n+1) > \log n$$

as $\log x$ is an increasing function. But then $x_n > 0$ for all n. Therefore, $\{x_n\}$ is a monotone decreasing sequence which is bounded below. Therefore, $\{x_n\}$ is convergent. Call the limit of this sequence γ. We only need show $\gamma \in (1/2, 1)$.

Observe that

$$\frac{1}{n} - \log\left(\frac{1+n}{n}\right) = \int_0^{1/n} \frac{t}{1+t}\, dt \leq \int_0^{1/n} t\, dt = \frac{1}{2n^2}$$
$$\frac{1}{n} - \log\left(\frac{1+n}{n}\right) = \int_0^{1/n} \frac{t}{1+t}\, dt \geq \int_0^{1/n} \frac{t}{1+\frac{1}{n}}\, dt = \frac{1}{2n(n+1)}.$$

Therefore,

$$\gamma = \sum_{n=1}^{\infty} \left(\frac{1}{n} - \log\left(\frac{1+n}{n}\right)\right) \leq \sum_{n=1}^{\infty} \frac{1}{2n^2} \leq \sum_{n=1}^{\infty} \frac{1}{2n^2 - \frac{1}{2}} = \sum_{n=1}^{\infty} \frac{1}{2}\left(\frac{1}{n-\frac{1}{2}} - \frac{1}{n+\frac{1}{2}}\right) = 1$$

and

$$\gamma = \sum_{n=1}^{\infty} \left(\frac{1}{n} - \log\left(\frac{1+n}{n}\right)\right) = \sum_{n=1}^{\infty} \frac{1}{2n(n+1)} = \sum_{n=1}^{\infty} \frac{1}{2}\left(\frac{1}{n} - \frac{1}{n+1}\right) = \frac{1}{2}.$$

Therefore, $\gamma \in (1/2, 1)$.

OR

Observe that $e^{1/k} < e$ for $k \geq 1$. It is simple to prove by induction that $\prod_{k=1}^{n} e^{1/k} \leq ne$

for $n \in \mathbb{N}$. Then we have

$$\begin{aligned} e^{x_n} &= e^{\left(\sum_{k=1}^{n} \frac{1}{k}\right) - \ln n} \\ &= \frac{e^{\sum_{k=1}^{n} \frac{1}{k}}}{e^{\ln n}} \\ &= \frac{e^{\sum_{k=1}^{n} \frac{1}{k}}}{n} \\ &= \frac{\prod_{k=1}^{n} e^{1/k}}{n} \\ &\leq \frac{ne}{n} \\ &= e \end{aligned}$$

Furthermore, one can show via induction that $\prod_{k=1}^{n} me^{1/k} \geq (n-1)e^{1/n}$ for $n \in \mathbb{N}$. Then

$$\begin{aligned} e^{x_n} &= \frac{\prod_{k=1}^{n} e^{1/k}}{n} \\ &= \frac{e \prod_{k=2}^{n} e^{1/k}}{n} \\ &= \frac{e^{1/2} e^{1/2} \prod_{k=2}^{n} e^{1/k}}{n} \\ &\geq \frac{e^{1/2} \prod_{k=2}^{n} e^{1/k}}{n} \\ &\geq \frac{e^{1/2}(n-1)e^{1/n}}{n} \\ &= e^{1/2} \cdot \frac{n-1}{n} \cdot e^{1/n} \end{aligned}$$

which tends to $e^{1/2}$ as $n \to \infty$. But then $e^{1/2} \leq e^{x_n} \leq e^1$. This implies (as e is monotone increasing) that $\frac{1}{2} \leq x_n \leq 1$ for all n . But then $\gamma \in (1/2, 1)$. □

3. Let $f : \mathbb{R} \to \mathbb{R}$ be given by

$$f(x) = \begin{cases} x, & x \in \mathbb{R} \setminus \mathbb{Q} \text{ or } x = 0 \\ p \sin\left(\frac{1}{q}\right), & x = \frac{p}{q},\ p, q \in \mathbb{Z},\ \gcd(p, q) = 1 \end{cases}$$

Where is f continuous?

Solution: As $\lim_{x\to 0}\frac{\sin x}{x}=1$, we have $\lim_{q\to\infty} q\sin(1/q)=\lim_{q\to\infty}\frac{\sin(1/q)}{1/q}=1$. Then for all $\epsilon>0$, there exists a M such that for $q>M$,

$$\left|\frac{\sin(1/q)}{1/q}-1\right|<\left|\frac{q}{p}\right|\frac{\epsilon}{2}$$

for any fixed p. Let $x\notin\mathbb{Q}$ and $\epsilon>0$ be given. Let $\delta_1=\epsilon/2$, $\delta_2=\lim_{q\leq M}|x-p/q|$, and $\delta=\min\{\delta_1,\delta_2\}$. Then for any y, $y=p/q\in\mathbb{Q}$ with $|x-y|<\delta$, we have

$$\begin{aligned}
|f(x)-f(y)| &= |x-p\sin(1/q)| \\
&= \left|x-\frac{p}{q}+\frac{p}{q}-p\sin(1/q)\right| \\
&\leq \left|x-\frac{p}{q}\right|+\left|\frac{p}{q}-p\sin(1/q)\right| \\
&= |x-y|+\left|\frac{p}{q}\right|\ \left|1-\frac{\sin(1/q)}{1/q}\right| \\
&< \delta+\left|\frac{p}{q}\right|\ \left|\frac{q}{p}\right|\frac{\epsilon}{2}\leq\frac{\epsilon}{2}+\frac{\epsilon}{2}=\epsilon
\end{aligned}$$

Taking $\delta=\epsilon$, we have for any $y\notin\mathbb{Q}$, $|f(x)-f(y)|=|x-y|<\delta=\epsilon$ so that f is continuous for $x\notin\mathbb{Q}$. Moreover using the work above, f is continuous at $x=0$.

Now let $x\in\mathbb{Q}$ with $x=p/q$ as in the definition of f. Suppose f were continuous, then for $\epsilon=\frac{1}{2}\left|p\left(\sin(1/q)-\frac{1}{q}\right)\right|$, there would be $\delta>0$ such that for $y\notin\mathbb{Q}$ with $|x-y|<\delta$, $|f(x)-f(y)|<\epsilon$. But

$$|f(x)-f(y)|=|p\sin(1/q)-y|\geq\left|p\sin(1/q)-\frac{p}{q}\right|+\left|\frac{p}{q}-y\right|>\frac{1}{2}\left|p\left(\sin(1/q)-\frac{1}{q}\right)\right|+\delta>\epsilon,$$

a contradiction. But then f cannot be continuous for $x\in\mathbb{Q}$. Therefore, f is continuous on the irrationals and $x=0$ only.

OR

Note that we need only consider $q>0$ as otherwise we have $\sin(1/q)=-\sin(1/|q|)$ and the result follows mutatis mutandis. Moreover, we only need consider $p\geq 0$ as if $x=p/q$, where p/q is rational written in reduced form and $p,q>0$, we have $-x=(-p)/q$ and $f(-x)=-p\sin(1/q)=-f(x)$.

It is clear that $f(x)$ is discontinuous at each nonzero rational point. Let p/q be a nonzero rational written in reduced form. For each $n\in\mathbb{N}$, one can find an irrational x_n in the interval $(p/q-1/n,p/q+1/n)$ as the irrationals are dense in $\mathbb{R}$. Then we can find a

sequence $\{x_n\}$ of irrational numbers converging to p/q. If $f(x)$ were continuous at p/q, then by the continuity of $f(x)$, we would have

$$\lim_{n\to\infty} f(x_n) = f(\lim_{n\to\infty} x_n) = f(p/q) = p\sin\left(\frac{1}{q}\right)$$

But we know that $\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_n = p/q$ as $f(x_n) = x_n$ for all x_n. Then we must have $p/q = p\sin(1/q)$. If $q =$, then we have $1 = \sin(1)$, which is clearly false. If $q \neq 1$, then we have $\sin(1/q) < 1/q$ as for $0 < x < \pi/2$, we know that $\sin x < x$. But this contradicts the fact that $p/q = p\sin(1/q)$ as it must be that $p/q > p\sin(1/q)$.

To see continuity at 0, observe that $f(0) = 0$ so that $|f(x) - f(0)| = |f(x)|$. However, $|f(x)| \leq x$ so that as $x \to 0$, it must be that $f(x) \to 0$ by Squeeze Theorem. To see continuity of $f(x)$ at each irrational point, observe that $\lim_{x\to\infty} \sin x/x = 1$ so that

$$\lim_{q\to\infty} \frac{\sin(1/q)}{1/q} = 1$$

Then for $\epsilon > 0$, there exists an $N \in \mathbb{N}$ such that $|q\sin(1/q) - 1| \leq \epsilon/2$ for $q > N$. Now let $x \in \mathbb{R}$ be irrational. There exists a $0 < \delta < \epsilon/2$ such that for each rational p/q, written in lowest form, with $|p/q - x| \leq \delta$, then $q > N$.

$$\begin{aligned}
|f(p/q) - f(x)| &= |p\sin(1/q) - x| \\
&= \left|\frac{p}{q}\cdot q\sin(1/q) - x\right| \\
&= \left|\frac{p}{q}\cdot q\sin(1/q) - \frac{p}{q} + \frac{p}{q} - x\right| \\
&\leq \left|\frac{p}{q}\cdot q\sin(1/q) - \frac{p}{q}\right| + \left|\frac{p}{q} - x\right| \\
&= \left|\frac{p}{q}\left(q\sin(1/q) - 1\right)\right| + \left|\frac{p}{q} - x\right| \\
&\leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon
\end{aligned}$$

If y were irrational with $|y - x| \leq \epsilon/2$, then $|f(y) - f(x)| = |y - x| \leq \epsilon/2 < \epsilon$. □

4. For each n, let $f_n : \mathbb{R} \to \mathbb{R}$ be a non-decreasing function, and assume f_n converges pointwise to a continuous function f. Prove that f_n converges uniformly on compact sets to f.

Solution: Let $a = x_0 < \cdots < x_m = b$ and choose δ such that $|x_{k+1} - x_k| < \delta$ for all k. Then for $x \in [a, b]$, we have $x \in [x_k, x_{k+1}]$ for some k so that $|x - x_k| < \delta$. But then

$|f(x) - f(x_k)| < \epsilon/5$ by the uniform continuity of f on $[a,b]$ (since f is continuous on a compact set). Since $f_n \to f$, there exists $N \in \mathbb{N}$ such that for $n > N$, $|f_n(x) - f(x)| < \epsilon/5$. But then

$$|f_n(x) - f(x)| \leq |f_n(x) - f_n(x_k)| + |f_n(x_k) - f(x_k)| + |f(x_k) - f(x)| < |f_n(x) - f_n(x_k)| + \frac{2\epsilon}{5}$$

Now $|f_n(x) - f_n(x_k)| = f_n(x) - f_n(x_k)$ since $x > x_k$ and f_n is non-decreasing,

$$\begin{aligned} |f_n(x) - f_n(x_k)| &\leq f_n(x_{k+1}) - f_n(x_k) = |f_n(x_{k+1}) - f_n(x_k)| \\ &\leq |f_n(x_{k+1}) - f(x_{k+1})| + |f(x_{k+1}) - f(x_k)| + |f(x_k) - f_n(x_k)| \\ &< \frac{\epsilon}{5} + \frac{\epsilon}{5} + \frac{\epsilon}{5} = \frac{3\epsilon}{5} \end{aligned}$$

But then

$$|f_n(x) - f(x)| < |f_n(x_k) - f_n(x_k)| + \frac{2\epsilon}{5} < \epsilon$$

for all $x \in [a,b]$. Therefore, f_n converges uniformly to f on compact sets to f. □

5. Let f be a continuous function on $[0,1]$ such that

$$\int_0^1 e^{-\frac{nx}{1-x}} f(x)\, dx = 0$$

for all $n \geq 0$. Show that f is identically zero.

Solution: Define $\mathcal{A}$ as

$$\mathcal{A} := \{f(x) = a_0 + a_1 e^{\frac{-x}{1-x}} + a_2 e^{\frac{-2x}{1-x}} + \cdots + a_m e^{\frac{-mx}{1-x}} \text{ and } f(1) = 0 \colon x \in [0,1), a_i \in \mathbb{R}\}$$

Let $f, g \in \mathcal{A}$ so that $f(x) = a_0 + a_1 e^{\frac{-x}{1-x}} + a_2 e^{\frac{-2x}{1-x}} + \cdots + a_m e^{\frac{-mx}{1-x}}$ and $g(x) = b_0 + b_1 e^{\frac{-x}{1-x}} + b_2 e^{\frac{-2x}{1-x}} + \cdots + b_p e^{\frac{-mx}{1-x}}$. Without loss of generality, assume $m \leq p$. Then $(f+g)(x) = (a_0 + b_0) + (a_1 + b_1) e^{\frac{-x}{1-x}} + (a_2 + b_2) e^{\frac{-2x}{1-x}} + \cdots + (a_m + b_m) e^{\frac{-mx}{1-x}} + \cdots + b_p e^{\frac{-px}{1-x}} \in \mathcal{A}$. Also, $(fg)(x) \in \mathcal{A}$ since $\left(a_i e^{\frac{-ix}{1-x}}\right)\left(b_j e^{\frac{-jx}{1-x}}\right) = a_i b_j e^{\frac{-(i+j)x}{1-x}} \in \mathcal{A}$. Clearly, if $c \in \mathbb{R}$ then $cf \in \mathcal{A}$. Therefore, $\mathcal{A} \subseteq C([0,1], \mathbb{R})$ is an algebra. Let $x_1, x_2 \in [0,1]$ be distinct points. Then $e^{\frac{-x}{1-x}} \in \mathcal{A}$ and $e^{\frac{-x_1}{1-x_1}} \neq e^{\frac{-x_2}{1-x_2}}$. But then $\mathcal{A}$ separates points. Let $x \in [0,1]$. Then $f(x) = 1 \in \mathcal{A}$ and $f(x) = 1 \neq 0$ and $\mathcal{A}$ vanishes at no point. The interval $[0,1]$ is compact. By Stone-Weierstrass, $\overline{\mathcal{A}} = C([0,1], \mathbb{R})$, i.e. there is a $\{f_n\} \subset \mathcal{A}$ such that $\{f_n\}$ converges uniformly

to f on $[0,1]$. Then

$$\begin{aligned}\int_0^1 f^2(x)\,dx &= \int_0^1 \lim_{n\to\infty} f_n(x)\cdot f(x)\,dx \\ &= \lim_{n\to\infty}\int_0^1 f_n(x)f(x)\,dx \\ &= \lim_{n\to\infty}\left[\int_0^1 a_0 f(x)\,dx + \cdots + \int_0^1 a_m e^{\frac{-mx}{1-x}} f(x)\,dx\right] \\ &= \lim_{n\to\infty} 0 \\ &= 0\end{aligned}$$

But then $\int_0^1 f^2(x)\,dx = 0$. As $f^2 \geq 0$ and f^2 is continuous, it must be that $f^2 = 0$ for all $x \in [0,1]$ so that $f \equiv 0$ on $[0,1]$. □

6. Show that there is an open interval containing 0 and a unique curve $(x(t), y(t))$, $t \in I$ with $(x(0), y(0)) = (1,1)$ satisfying

$$\begin{aligned} x + y^2 + \sin t &= 2 \\ x^2 + ty^2 &= 1.\end{aligned}$$

Find the velocity of the curve at $t = 0$. For a given $t_0 \in I$ is there a unique solution (x,y) to the above with $t = t_0$?

Solution: Let $F = (f_1, f_2) : \mathbb{R}^3 \to \mathbb{R}^2$ such that $f_1(x,y,t) = x + y^2 + \sin t - 2$, $f_2(x,y,t) = x^2 + ty - 1$. Then $F(1,1,0) = (0,0)$.

$$F'(1,1,0) = \begin{pmatrix} 1 & 2y & \cos t \\ 2x & 2ty & y^2 \end{pmatrix}\Big|_{(1,1,0)} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

Define

$$\begin{aligned} A_x &= \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \\ A_y &= \begin{pmatrix} 1 \\ 1 \end{pmatrix}\end{aligned}$$

Now $\det A_x = -4 \neq 0$. Then A_x is invertible. By the Implicit Function Theorem, there exists $U \subseteq \mathbb{R}^3$ open such that $(1,1,0) \in U$ and $I \subseteq \mathbb{R}$ open such that $0 \in I$ and for all $t \in I$, there is a unique (x,y) such that $(x,y,t) \in U$ and $F(x,y,t) = 0$. But then there is a differentiable function h in a neighborhood of $(1,1,0)$ such that $h(0) = (1,1,)$ and

$F(h(t), t) = 0$, i.e. the system has a unique solution $(x, y) = h(t)$ in a neighborhood of $(1, 1, 0)$ and

$$h'(0) = -A_x^{-1} A_y = \frac{1}{4} \begin{pmatrix} 0 & -2 \\ -2 & 1 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} -2 \\ -1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{4} \end{pmatrix}.$$

Finally given $t_0 \in I$, there is a unique solution (x, y) to the system of equations with $t = t_0$. □

January 2004

1. Show that if $E \subseteq \mathbb{R}^k$ is not compact, there is a continuous function $f : E \to \mathbb{R}$ which is unbounded.

Solution: If $E \subseteq \mathbb{R}^k$ is not compact, then by the contrapositive to Heine-Borel it is not bounded or not closed. If E is unbounded, then $f : E \to \mathbb{R}$ given by $f(x) = \|x\|$ is an unbounded function. If E is not closed, then E^C is not open so that there is a $x_0 \in E^C$ such that no neighborhood of x_0 is contained entirely within E^C. That is, all neighborhoods of x_0 intersect E. Then $f : E \to \mathbb{R}$ given by $f(x) = \frac{1}{\|x - x_0\|}$ for $x \in E$ is unbounded. Notice the function is defined at all $x \in E$ as $x_0 \notin E$. But as x_0 is a limit point of E, there is a sequence x_n in E which converges to x. That is, for any $\epsilon > 0$ there is an $N \in \mathbb{N}$ such that $|x_n - x_0| < \epsilon$ for $n > N$. Take $\epsilon = \frac{1}{n}$ and choose such an N. Then we have

$$f(x_n) = \frac{1}{\|x_n - x_0\|} > \frac{1}{\frac{1}{n}} = n$$

for all $n > N$ so that $f(x)$ is an unbounded function. □

2. Let $f : (0, +\infty) \to \mathbb{R}$ be a differentiable function such that $\lim_{x \to +\infty} \frac{f(x)}{x} = 0$. Prove that there is a sequence $x_n \nearrow +\infty$ such that $f'(x_n) \to 0$.

Solution: Consider the sequence $\{x_n\}$, where $x_n = 2^n$. Then $x_{n+1} = 2^{n+1} = 2 \cdot 2^n = 2x_n \geq x_n$. Clearly, $x_n \nearrow \infty$. Since $\lim_{x \to \infty} \frac{f(x)}{x} = 0$, for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for $n > N$, we have $\left| \frac{f(x_n)}{x_n} \right| < \frac{\epsilon}{4}$. But this implies $\left| \frac{f(2x_n)}{2x_n} \right| < \frac{\epsilon}{4}$. As f is differentiable, for all n, there exists $c_n \in (x_n, x_{n+1})$ such that $f'(c_n) = \frac{f(x_{n+1}) - f(x_n)}{x_{n+1} - x_n}$. This implies

$$f'(c_n) = \frac{f(2x_n) - f(x_n)}{2x_n - x_n} = \frac{f(2x_n) - f(x_n)}{x_n}.$$

Therefore for $n > N$, we have $\left| \frac{f(2x_n)}{2x_n} \right| < \frac{\epsilon}{4}$. Then

$$\left| \frac{f(x_n) - f(x_n) + f(2x_n)}{2x_n} \right| < \frac{\epsilon}{2}.$$

Using this for $n > N$, we have

$$\begin{aligned} \left| \frac{f(x_n)}{2x_n} \right| - \left| \frac{f(2x_n) - f(x_n)}{2x_n} \right| &< \frac{\epsilon}{4} \\ \frac{1}{2} \left| \frac{f(x_n)}{x_n} \right| - \frac{1}{2} |f'(c_n)| &< \frac{\epsilon}{4} \\ \left| \frac{f(x_n)}{x_n} \right| - |f'(c_n)| &< \frac{\epsilon}{4} \end{aligned}$$

Therefore, $|f'(c_n)| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. Then for all $n > N$, we have $|f'(c_n)| < \epsilon$ so that $f'(x_n) \to 0$. □

3. Let $f : [x_1, x_2] \to \mathbb{R}$ be a differentiable function, where $0 < x_1 < x_2$. Prove that there exists $c \in (x_1, x_2)$ such that

$$\frac{1}{x_1 - x_2} \begin{vmatrix} x_1 & x_2 \\ f(x_1) & f(x_2) \end{vmatrix} = f(c) - cf'(c).$$

Solution: Let $g(x) = \frac{f(x)}{x}$ and $h(x) = \frac{1}{x}$. By the Mean Value Theorem, there exists $c \in (x_1, x_2)$ such that $g'(c)(h(x_1) - h(x_2)) = h'(c)(g(x_1) - g(x_2))$. Then

$$\begin{aligned} \frac{cf'(c) - f(c)}{c^2} \left(\frac{1}{x_1} - \frac{1}{x_2} \right) &= -\frac{1}{c^2} \left(\frac{f(x_1)}{x_1} - \frac{f(x_2)}{x_2} \right) \\ f(c) - cf'(c) \left(\frac{x_2 - x_1}{x_1 x_2} \right) &= \frac{x_2 f(x_1) - x_1 f(x_2)}{x_1 x_2} \\ f(c) - cf'(c) &= x_2 f(x_1) - x_1 f(x_2) \cdot \frac{1}{x_2 - x_1} \end{aligned}$$

Therefore,

$$\frac{1}{x_1 - x_2} \begin{vmatrix} x_1 & x_2 \\ f(x_1) & f(x_2) \end{vmatrix} = f(c) - cf'(c).$$

□

4. Let $f, \rho : [0, +\infty) \to \mathbb{R}$ be functions which are Riemann integrable on each interval $[0, A]$, $A > 0$. Assume that $\rho(x) \geq 0$ for all $x \geq 0$ and

$$\int_0^{+\infty} \rho(x)\, dx = 1, \quad \lim_{x \to +\infty} f(x) = L \in \mathbb{R}.$$

(i) Calculate $t \int_0^{+\infty} \rho(tx)\, dx$, where $t > 0$.

(ii) Show that $\lim_{t \searrow 0} t \int_0^{+\infty} \rho(tx) f(x)\, dx = L$.

Solution:

(i) Let $u = tv$ so that $du = t\, dx$. Then $\frac{1}{t}\, du = dx$. Then we have

$$t \int_0^{\infty} \rho(tx)\, dx = \int_0^{\infty} \rho(u)\, du = 1$$

(ii) Let $\epsilon > 0$. Using (i), we have

$$\begin{aligned}\left| t\int_0^\infty \rho(tx)f(x)\,dx - L\right| &= \left| t\int_0^\infty \rho(tx)f(x)\,dx - L\cdot t\int_0^\infty \rho(tx)\,dx\right| \\ &= \left| t\int_0^\infty \rho(tx)(f(x)-L)\,dx\right| \\ &\le t\int_0^\infty \rho(tx)|f(x)-L|\,dx\end{aligned}$$

Now as $\lim_{x\to\infty} f(x) = L$, there exists an $N \in \mathbb{N}$ such that for $x > N$, $|f(x) - L| < \epsilon$. But then we have

$$\begin{aligned}\left| t\int_0^\infty \rho(tx)f(x)\,dx - L\right| &\le t\int_0^\infty \rho(tx)|f(x)-L|\,dx \\ &= t\int_0^N \rho(tx)|f(x)-L|\,dx + t\int_N^\infty \rho(tx)|f(x)-L|\,dx \\ &< t\int_0^N \rho(tx)|f(x)-L|\,dx + t\int_N^\infty \rho(tx)\epsilon\,dx\end{aligned}$$

Since $\rho(tx), f(x) \in \mathcal{R}[0,N]$, $\rho(tx), f(x)$ are bounded on $[0,N]$, so

$$\begin{aligned}\left| t\int_0^\infty \rho(tx)f(x)\,dx - L\right| &< t\int_0^N \rho(tx)|f(x)-L|\,dx + t\int_N^\infty \rho(tx)\epsilon\,dx \\ &\le tMN + \epsilon t\int_N^\infty \rho(tx)\,dx \\ &\le tMN + \epsilon\end{aligned}$$

for some $M \in \mathbb{R}$. Choosing $t < \frac{\epsilon}{2MN}$, we have that $\lim_{t\searrow 0} t\int_0^{+\infty} \rho(tx)f(x)\,dx = L$.

□

5. Consider the series $\displaystyle\sum_{n=1}^{\infty} \frac{x^n}{n+x^{2n}}$. Find all the values $x \ge 0$ where the series is convergent. Show that the series converges uniformly on the set $[0, 1/2] \cup [2, +\infty)$. Is the series uniformly convergent on $[0, 1)$? Justify your answer.

Solution: Observe

$$\left|\frac{x^{n+1}}{n+1+x^{2n+2}}\cdot\frac{n+x^{2n}}{x^n}\right| = \left|\frac{nx+x^{2n+1}}{n+1+x^{2n+2}}\right|.$$

If $x = 0$, the series sum is clearly 0. If $0 < x < 1$, we have

$$\lim_{n\to\infty}\left|\frac{nx+x^{2n+1}}{n+1+x^{2n+2}}\right| = \left|\frac{x}{1}\right| = |x| = x < 1$$

so that the series converges absolutely by the Ratio Test as $x < 1$. If $x = 1$, then

$$\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}} = \sum_{n=1}^{\infty} \frac{1}{n+1}$$

which diverges by limit comparison with the series $\sum_{n=1}^{\infty} \frac{1}{n}$ — which diverges by the p-test. [Alternatively, one could use the Integral Test or observe that

$$\sum_{n=1}^{\infty} \frac{1}{n+1} > \sum_{n=1}^{\infty} \frac{1}{n+n} = \frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{n}.$$

so that the series diverges by the Comparison Test.] If $x > 1$, then

$$\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}} \leq \sum_{n=1}^{\infty} \frac{x^n}{x^{2n}} = \sum_{n=1}^{\infty} \left(\frac{1}{x}\right)^n$$

The series $\sum_{n=1}^{\infty} \left(\frac{1}{x}\right)^n$ is geometric with $|r| = |1/x| < 1$ since $x > 1$. Therefore, the series $\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}}$ converges (absolutely as the terms are all nonnegative) by the Comparison Test. Then $\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}}$ converges absolutely for $x \in [0, 1) \cup (1, \infty)$.

Let $f_n(x) = \frac{x^n}{n+x^{2n}}$. We have

$$f_n'(x) = \frac{n^2 x^{n-1} - n x^{3n-1}}{(n + x^{2n})^2}.$$

Observe that $f_n'(x) > 0$ for $x \in [0, 1/2]$ but $f_n'(x) < 0$ for $x \in [2, \infty)$. Therefore, f_n is increasing on $[0, 1/2]$ but decreasing on $[2, \infty)$. Then for $x \in [0, 1/2]$,

$$\frac{x^n}{n + x^{2n}} \leq \frac{\left(\frac{1}{2}\right)^n}{n + \left(\frac{1}{2}\right)^{2n}} \leq \frac{1}{n} \left(\frac{1}{2}\right)^n$$

and $\sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{1}{2}\right)^n$ converges absolutely by the Ratio Test. Therefore, $\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}}$ converges uniformly on $[0, 1/2]$ by the Weierstrass M-test. For $x \in [2, \infty)$,

$$\frac{x^n}{n + x^{2n}} \leq \frac{2^n}{n + 2^{2n}} \leq \frac{2^n}{2^{2n}} = \left(\frac{1}{2}\right)^n$$

and $\sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n$ converges by the Geometric Series Test with $r = 1/2$ (or by the Ratio or Root Test). Therefore, $\sum_{n=1}^{\infty} \frac{x^n}{n + x^{2n}}$ converges uniformly on $[2, \infty)$ by the Weierstrass M-test.

But then the series converges uniformly on $[0, 1/2] \cup [2, \infty)$. □

6. Consider the function $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = \dfrac{x^2 y}{x^2 + y^2}$ if $(x, y) \neq (0, 0)$ and $f(0, 0) = 0$. Show that f is uniformly convergent on $\{(x, y) \colon x^2 + y^2 \leq 1\}$. Find the first order partial derivatives of f at $(0, 0)$. Is f differentiable at $(0, 0)$? Justify your answer.

Solution: Note that f is continuous for $(x, y) \neq (0, 0)$ as $f(x, y) = \dfrac{x^2 y}{x^2 + y^2}$ is then a quotient of continuous functions. Observe

$$\left| \frac{x^2 y}{x^2 + y^2} \right| \leq \left| \frac{(2xy)x}{x^2 + y^2} \right| \leq \left| \frac{(x^2 + y^2)x}{x^2 + y^2} \right| = |x|$$

and $x \to 0$ as $(x, y) \to (0, 0)$. Therefore by Squeeze Theorem, $\lim_{(x,y)} f(x, y) = 0 = f(0, 0)$. Then $f(x, y)$ is continuous for all $(x, y) \in \mathbb{R}^2$. But then $f(x, y)$ is continuous on the compact set $\{(x, y) \colon x^2 + y^2 \leq 1\}$. Hence, $f(x, y)$ is uniformly continuous on $\{(x, y) \colon x^2 + y^2 \leq 1\}$. Now

$$D_1 f(0, 0) = \lim_{h \to 0} \frac{f(h, 0) - f(0, 0)}{h} = \lim_{h \to 0} 0 = 0$$
$$D_2 f(0, 0) = \lim_{h \to 0} \frac{f(0, h) - f(0, 0)}{h} = \lim_{h \to 0} 0 = 0$$

Suppose $f(x, y)$ were differentiable at $(0, 0)$. Let $u = (u_1, u_2)$ be a unit vector. Then $D_u f(0, 0) = \nabla f(0, 0) \cdot u$. But

$$D_u f(0, 0) = \lim_{t \to 0} \frac{f((0, 0) + tu) - f(0, 0)}{t} = \lim_{t \to 0} \frac{\dfrac{t^3 u_1^2 u_2}{t^2 (u_1^2 + u_2^2)}}{t} = \lim_{t \to 0} u_1^2 u_2 = u_1^2 u_2$$

and $\nabla f(0, 0) \cdot u = (0, 0) \cdot u = 0u_1 + 0u_2 = 0$. But then $u_1 u_2 = 0$ which is not true for *all* unit vectors u, e.g. $u = (1/\sqrt{2}, 1/\sqrt{2})$. Therefore, f is not differentiable at $(0, 0)$. □

August 2005

1. Let g be a continuous function on $[0,1]$ with $g(1) = 0$ and let $h_n(x) = x^n g(x)$ for $n = 1, 2, \cdots$. Prove that h_n converges uniformly.

Solution: Though certainly not the shortest route, we prove this by showing far more general results (these results could be assumed for the exam in which case only the final argument is needed). We have a more general result: if $f_n(x), g_n(x)$ are sequences of bounded functions which converge uniformly on E to functions f, g, respectively, then $f_n(x)g_n(x)$ converges uniformly to fg on E. We know that $\{f_n\}$ and $\{g_n\}$ are uniformly bounded. Then there P, Q such that $|f_n(x)| < P$ and $|g_n(x)| < Q$ for all $n \in \mathbb{N}$ and $x \in E$. Let $M = \max\{P, Q\}$. It is clear that $|f_n(x)| < M$ and $|g_n(x)| < M$ so that $|f(x)| < M$ an $|g(x)| < M$. Using the convergence of $\{f_n\}$ and $\{g_n\}$, given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|f_n(x) - f(x)| < \epsilon/(2M)$ and $|g_n(x) - g(x)| < \epsilon/(2M)$ for all $n > N$. But then

$$\begin{aligned}
|f_n(x)g_n(x) - f(x)g(x)| &= |f_n(x)g_n(x) - f_n(x)g(x) + f_n(x)g(x) - f(x)g(x)| \\
&\leq |f_n(x)g_n(x) - f_n(x)g(x)| + |f_n(x)g(x) - f(x)g(x)| \\
&= |f_n(x)|\,|g_n(x) - g(x)| + |g(x)|\,|f_n(x) - f(x)| \\
&< M\frac{\epsilon}{2M} + M\frac{\epsilon}{2M} \\
&= \epsilon
\end{aligned}$$

so that $f_n(x)g_n(x)$ converges uniformly to $f(x)g(x)$ on E.

Let $\{f_n\}$ and $\{g_n\}$ (not necessarily bounded) converge uniformly to $f(x), g(x)$ on a set E, respectively. Then we know that the sequences $\{f_n\}$ and $\{g_n\}$ are Cauchy. Then given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|f_n(x) - f_m(x)| < \epsilon/2$ and $|g_n(x) - g_m(x)| < \epsilon/2$ for all $n, m > N$ and $x \in E$. But then

$$\begin{aligned}
|(f_n + g_n)(x) - (f_m - g_m)(x)| &= |(f_n(x) - f_m(x)) - (g_n(x) - g_m(x))| \\
&\leq |f_n(x) - f_m(x)| + |g_n(x) - g_m(x)| \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon
\end{aligned}$$

so that $f_n + g_n$ is uniformly convergent on E.

Take $f_n(x) = x^n$ and $g_n(x) = g(x)$. Observe that $g_n(x), g(x)$ are bounded on $[0,1]$ as they are continuous on a compact interval. It is clear that $f_n(x)$ converges uniformly to 0 on $[0,1)$. Then $f_n(x)g_n(x) = x^n g(x) \to 0$ uniformly on $[0,1)$. Now let $f_n'(x) = 1$ at $x = 1$ and 0 elsewhere. It is clear that $f_n'(x) \to 0$ uniformly on $[0,1]$. But then $f_n'(x)g_n(x) \to 0$ uniformly on $[0,1]$. But observe

$$h_n(x) = \begin{cases} f_n(x)g_n(x), & x \in [0,1) \\ f_n'(x)g_n(x), & x = 1 \end{cases}$$

is then uniformly convergent.

OR

Since g is continuous on $[0,1]$, g is uniformly continuous on the compact set $[0,1]$. Since x^n, g are continuous on $[0,1]$, h_n is continuous on $[0,1]$. But then h_n is uniformly continuous on $[0,1]$. Now since $x \in [0,1]$

$$h_{n+1}(x) = x^{n+1}g(x) = x \cdot x^n g(x) = xh_n(x) \leq h_n(x)$$

for all $x \in [0,1]$ and n. But then $\{h_n\}$ is a decreasing sequence. We show that h_n converges to h. Let $\epsilon > 0$ and $x \in [0,1)$. Take $N \in \mathbb{N}$ such that $x^N < \frac{\epsilon}{g(x)}$ (using $x^n \to 0$ as $n \to \infty$ as $x \in [0,1)$). Then for $n > N$,

$$|h_n(x) - h(x)| = |x^n g(x)| \leq |x^N g(x)| < \left| \frac{\epsilon}{g(x)} \cdot g(x) \right| = \epsilon.$$

For $x = 1$, $h_n(1) = g(1) = 0$. But then h_n converges to h on $[0,1]$. But then by Dini's Theorem, $\{h_n\}$ converges uniformly to h on $[0,1]$. □

2. Let $a_n, n = 1, 2, \cdots$ be a sequence of positive numbers such that $\sum_{n=1}^{\infty} a_n$ converges.

(a) Prove that $\liminf_{n\to\infty} na_n = 0$.

(b) Show by example that $\limsup_{n\to\infty} na_n > 0$ is possible.

Solution:

(a) Suppose that $\liminf_{n\to\infty} na_n \neq 0$. Then there exists $\epsilon > 0$ such that $\liminf_{n\to\infty} na_n \geq \epsilon$ since $a_n > 0$. But then $\lim_{n\to\infty}(\liminf_{k\geq n} ka_k) \geq \epsilon$. Then there exists $N \in \mathbb{N}$ such that for $k \geq N$, $ka_k > \epsilon$. But then $a_k > \frac{\epsilon}{k}$. But then $\sum_{k=1}^{\infty} a_k > \sum_{k=1}^{\infty} \frac{\epsilon}{k} = \epsilon \sum_{k=1}^{\infty} \frac{1}{k}$ diverges by the Comparison Test, a contradiction. Therefore, $\liminf_{n\to\infty} na_n = 0$.

(b) Define

$$a_n = \begin{cases} \dfrac{1}{2^l}, & n = 2^l \text{ for some } l \in \mathbb{N} \\ \dfrac{1}{n^2}, & \text{otherwise} \end{cases}$$

Clearly, $a_n > 0$ for a $n \in \mathbb{N}$. Now

$$\sum_{n=1}^{\infty} a_n \leq \sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{n=2^l}^{\infty} \frac{1}{2^n} = \sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{l=0}^{\infty} \frac{1}{2^{2^l}} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{l=0}^{\infty} \frac{1}{2^l} = \frac{\pi^2}{6} + \frac{1}{1-\frac{1}{2}} = \frac{\pi^2}{6} + 2$$

so that $\sum_{n=1}^{\infty} a_n$ converges. But we have taking the sequence $\{2^n\}$, we have

$$\limsup_{n\to\infty} na_n \geq 2^n \cdot \frac{1}{2^n} = 1.$$

□

3. Let $F(x_1, x_2, y_1, y_2) = (x_1x_2 + x_1y_1 + y_2, x_1y_2 + x_2y_1^2)$. Check that $F(1, 1, 1, 1) = (3, 2)$.

(a) Prove that there is a neighborhood U of $(1, 1, 1, 1)$ and a neighborhood W of $(1, 1)$ and a function $g : W \to \mathbb{R}^2$ such that for all $(y_1, y_2) \in W$ there is a unique $(x_1, x_2) \in \mathbb{R}^2$ given by $g(y_1, y_2)$ such that $(x_1, x_2, y_1, y_2) \in U$ and $F(x_1, x_2, y_1, y_2) = (3, 2)$.

(b) Find $g'(1, 1)$.

(c) Find an approximate solution to the equation $F(x_1, x_2, 1.001, 1.003) = (3, 2)$. Assume that $(1.001, 1.003) \in W$.

Solution:

(a) We have $F(1, 1, 1, 1) = (1 + 1 + 1, 1 + 1) = (3, 2)$. Define $\hat{F}(x_1, x_2, y_1, y_2) = (x_1x_2 + x_1y_1 + y_2 - 3, x_1y_2 + x_2y_1^2 - 2)$. Then $\hat{F}(1, 1, 1, 1) = (0, 0)$ and

$$A := \hat{F}(1, 1, 1, 1) = \begin{pmatrix} x_2 + y_1 & x_1 & x_1 & 1 \\ y_2 & y_1^2 & 2x_2y_1 & x_1 \end{pmatrix} \Bigg|_{(1,1,1,1)} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{pmatrix}.$$

Define then

$$A_x = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$
$$A_y = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

We have

$$\det A_x = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} = 2 - 1 = 1 \neq 0.$$

Therefore, A_x is invertible so that the Implicit Function Theorem applies. By the Implicit Function Theorem, there exists a neighborhood U of $(1, 1, 1, 1)$ and a neighborhood of $(1, 1)$ and a function $\hat{g} : W \to \mathbb{R}^2$ such that for all $(y_1, y_2) \in W$, there exists $(x_1, x_2) \in \mathbb{R}^2$ given by $\hat{g}(y_1, y_2)$ such that $(x_1, x_2, y_1, y_2) \in U$ and $\hat{F}(x_1, x_2, y_1, y_2) = (0, 0)$. Define $g : W \to \mathbb{R}^2$ by $g(y_1, y_2) = (\hat{g}(y_1, y_2) + 3, \hat{g}_2(y_1, y_2) + 2)$ so that we have $F(x_1, x_2, y_1, y_2) = (3, 2)$.

(b) We have

$$g'(1, 1) = -A_x^{-1}A_y = -\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -3 & -1 \end{pmatrix}.$$

(c) We need find $g(1.001, 1.003)$.

$$\begin{aligned} x_1 = g_1(1,001, 1.003) &= g_1(1.001, 1.003) - g_1(1,1) + g_1(1,1) \\ &= \frac{\partial g_1}{\partial y_1}(0.001) + \frac{\partial g_1}{\partial y_2}(0.003) + 1 \\ &= 1(0.001) + 0(0.003) + 1 = 1.001 \end{aligned}$$

$$\begin{aligned} x_2 = g_2(1,001, 1.003) &= g_2(1.001, 1.003) - g_2(1,1) + g_1(1,1) \\ &= \frac{\partial g_2}{\partial y_1}(0.001) + \frac{\partial g_2}{\partial y_2}(0.003) + 1 \\ &= -3(0.001) - (0.003) + 1 = 0.994 \end{aligned}$$

Therefore, $(x_1, x_2) = (1.001, 0.994)$.

□

4. Prove that

$$\lim_{n\to\infty} \frac{\ln(2) + \ln(3) + \cdots + \ln(n)}{n \ln n} = 1$$

Solution: We know that

$$\ln(1) + \ln(2) + \cdots + \ln(n) = \ln(n!)$$

By Stirling's formula, we know that $\ln(n!) - n \ln n - n + O(\ln n)$. So we have

$$\frac{\ln(n!)}{n \ln n} = \frac{n \ln n - n + O(\ln n)}{n \ln n} = 1 - \frac{1}{\ln n} + \frac{O(\ln n)}{n \ln n}$$

which clearly tends to 1 as $n \to \infty$.

OR

We know that $\ln n = \int_1^n \frac{1}{x}\,dx$. So we have

$$\begin{aligned}
\frac{\sum_{m=2}^{n}\int_1^m \frac{1}{x}\,dx}{n\int_1^n \frac{1}{d}\,dx} &= \frac{\int_1^2 \frac{1}{x}\,dx + \int_1^2 \frac{1}{x}\,dx + \int_2^3 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx}{n\left(\int_1^2 \frac{1}{x}\,dx + \int_2^3 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx\right)} \\
&= \frac{(n-1)\int_1^2 \frac{1}{x}\,dx + (n-2)\int_2^3 \frac{1}{x}\,dx + \cdots + (n-n+1)\int_{n-1}^n \frac{1}{x}\,dx}{n\left(\int_1^2 \frac{1}{x}\,dx + \int_2^3 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx\right)} \\
&= \frac{n\left(\int_1^2 \frac{1}{x}\,dx + \int_2^3 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx\right) - \int_1^2 \frac{1}{x}\,dx - 2\int_2^3 \frac{1}{x}\,dx - \cdots - (n-1)\int_{n-1}^n \frac{1}{x}\,dx}{n\left(\int_1^2 \frac{1}{x}\,dx + \int_2^3 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx\right)} \\
&= 1 - \frac{\int_1^2 \frac{1}{x}\,dx + 2\int_2^3 \frac{1}{x}\,dx + \cdots + (n-1)\int_{n-1}^n \frac{1}{x}\,dx}{n\left(\int_1^2 \frac{1}{x}\,dx + \cdots + \int_{n-1}^n \frac{1}{x}\,dx\right)}
\end{aligned}$$

and observe the right term tends to 0 as $n \to \infty$, as desired. □

5. Let $f : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function such that

$$f(tx) = t^5 f(x), \forall t > 0, \forall x = (x_1, \ldots, x_n) \in \mathbb{R}^n.$$

Prove that f satisfies the partial differential equation

$$\sum_{j=1}^{n} x_j \frac{\partial f}{\partial x_j}(x) = 5f(x), \forall x \in \mathbb{R}^n.$$

Solution: Let $x \in \mathbb{R}^n$. Define $\gamma_x(t) = tx$ and $g(t) = f \circ \gamma_x(t)$. Then $g'(t) = \nabla f(\gamma_x(t)) \cdot \gamma_x'(t)$. Then $g'(1) = \nabla f(x) \cdot x$. Now

$$\sum_{j=1}^{n} x_j \frac{\partial f}{\partial x_j}(x) = \nabla f(x) \cdot x = g'(1).$$

But $g(t) = f \circ \gamma_x(t) = f(\gamma_x(t)) - f(tx) = t^5 f(x)$. Hence, $g(t) = t^5 f(x)$ so that $g;(t) = 5t^4 f(x)$ and $g'(1) = 5f(x)$. Therefore,

$$\sum_{j=1}^{n} x_j \frac{\partial f}{\partial x_j}(x) = g'(1) = 5f(x).$$

This proves $\sum_{j=1}^{n} x_j \frac{\partial f}{\partial x_j}(x) = 5f(x)$ for $x \in \mathbb{R}^n$. □

6. Prove that if $\{a_n\}$ is a sequence of positive numbers, then

$$\limsup_{n\to\infty}(a_n)^{1/n} \leq \limsup_{n\to\infty} \frac{a_{n+1}}{a_n}$$

Solution: Note that if $\limsup_{n\to\infty} \frac{a_{n+1}}{a_n} = \infty$, we have

$$\limsup_{n\to\infty}(a_n)^{1/n} \leq \limsup_{n\to\infty} \frac{a_{n+1}}{a_n}.$$

So assume $\limsup_{n\to\infty} \frac{a_{n+1}}{a_n} = \alpha < \infty$. Choose $\beta > \alpha$. Then there exists $N \in \mathbb{N}$ such that for $n > N$, $\frac{a_{n+1}}{a_n} \leq \beta$. So $a_{n+1} \leq \beta a_n$. Furthermore, $a_{n+2} \leq \beta a_{n+1} \leq \beta^2 a_n$. Hence by induction, $a_{n+3} \leq \beta^3 a_n$ so that for $p > 0$, we have $a_{N+p} \leq \beta^p a_N$ or $a_n \leq a_N \beta^{-B} \cdot \beta^n$ taking $p = n - N$. Then $(a_n)^{1/n} \leq (a_N \beta^{-N})^{1/n} \cdot \beta$. Then $\limsup_{n\to\infty}(a_n)^{1/n} \leq \beta$ for $\beta > 2$ since $a_N/\beta_N > 0$. Therefore, $\lim_{n\to\infty}(a_n/\beta_n)^{1/n} = 1$. Then $\limsup_{n\to\infty}(a_n)^{1/n} \leq \alpha$ which improves $\limsup_{n\to\infty}(a_n)^{1/n} \leq \limsup_{n\to\infty} \frac{a_{n+1}}{a_n}$. □

January/August 2006

1. Prove the chain rule: if g is differentiable at a, $g(a) = b$, and f is differentiable at b, then $f \circ g$ is differentiable at a and $(f \circ g)'(a) = f'(b)g'(a)$.

Solution: Since g is differentiable at a, $g(x) = g(a) + g'(a)(x-a) + \phi_a(x)(x-a)$, where ϕ_a is continuous at a and $\phi_a(a) = 0$, i.e. $\phi_a(x) \to 0$ as $x \to a$. Similarly since f is differentiable at b, $f(y) = f(b) + f'(b)(y-b) + \phi_b(y)(y-b)$, where ϕ_b is continuous at b and $\phi_b(b) = 0$, i.e. $\phi_b(y) \to 0$ as $y \to b$. Then

$$\begin{aligned} f(g(x)) &= f(g(a)) + f'(g(a))(g(x) - g(a)) + \phi_b(g(x))(g(x) - g(a)) \\ &= f(g(a)) + f'(g(a))(g(a) + g'(a)(x-a) + \phi_a(x)(x-a) - g(a)) \\ &\qquad + \phi_b(g(x))(g'(a)(x-a) + \phi_a(x)(x-a)) \\ &= f(g(a)) + f'(g(a))g'(a)(x-a) + \big[\phi_a(x)f'(g(a))(x-a) + \phi_b(g(x))g'(a)(x-a) \\ &\qquad + \phi_b(g(x))\phi_a(x)(x-a)\big] \end{aligned}$$

and $\phi_a(x)f'(g(a))(x-a) + \phi_b(g(x))g'(a)(x-a) + \phi_b(g(x))\phi_a(x)(x-a) \to 0$ as $x \to a$. Therefore, $f \circ g$ is differentiable at $x = a$ and $(f \circ g)'(a) = f'(g(a))g'(a) = f'(b)g'(a)$. $\square$

2. Let $f(0) = 0$ and $f(t) = t^2 \sin(1/t)$ for $t \neq 0$ and let $\phi(x, y) = f(x) + f(y)$.

(a) Prove that $\frac{\partial \phi}{\partial x}$ exists everywhere in $\mathbb{R}^2$ but is not continuous at $(0, 0)$.

(b) Prove that ϕ is differentiable at $(0, 0)$ and find $\phi'(0, 0)$.

Solution:

(a) We have

$$\lim_{h \to 0} \frac{\phi(x+h, y) - \phi(x, y)}{h} = \lim_{h \to 0} \frac{f(x+h) + f(y) - f(x) - (y)}{h} = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = f'(x)$$

and for $x \neq 0$, $f'(x) = 2x \sin(1/x) - \cos(1/x)$. For $x = 0$,

$$f'(0) = \lim_{h \to 0} \frac{f(h) - f(0)}{h} = \lim_{h \to 0} \frac{h^2 \sin\left(\frac{1}{h}\right)}{h} = \lim_{h \to 0} h \sin\left(\frac{1}{h}\right) = 0$$

where the last inequality follows from the Squeeze Theorem with $-h \leq h \sin(1/h) \leq h$ as $h \to 0$. Therefore,

$$\frac{\partial \phi}{\partial x} = \begin{cases} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

exists for all $(x, y) \in \mathbb{R}^2$. But

$$\lim_{(x,y)\to(0,0)} \frac{\partial \phi}{\partial x} = \lim_{x\to 0} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) = -\lim_{x\to 0} \cos\left(\frac{1}{x}\right)$$

does not exist so that $\frac{\partial \phi}{\partial x}$ is not continuous at $(0, 0)$.

(b) We have

$$\lim_{(h_1,h_2)\to(0,0)} \frac{\phi(h_1, h_2) - \phi(0, 0)}{|h|} = \lim_{(h_1,h_2)\to(0,0)} \frac{h_1^2 \sin(1/h_1) + h_2^2 \sin(1/h_2)}{\sqrt{h_1^2 + h_2^2}}$$

But we also have

$$-\frac{h_1^2 + h_2^2}{\sqrt{h_1^2 + h_2^2}} \leq \frac{h_1^2 \sin(1/h_1) + h_2^2 \sin(1/h_2)}{\sqrt{h_1^2 + h_2^2}} \leq \frac{h_1^2 + h_2^2}{\sqrt{h_1^2 + h_2^2}}$$

Then

$$-\sqrt{h_1^2 + h_2^2} \leq \frac{h_1^2 \sin(1/h_1) + h_2^2 \sin(1/h_2)}{\sqrt{h_1^2 + h_2^2}} \leq \sqrt{h_1^2 + h_2^2}$$

Therefore by Squeeze Theorem, we have

$$\lim_{(h_1,h_2)\to(0,0)} \lim_{(h_1,h_2)\to(0,0)} \frac{\phi(h_1, h_2) - \phi(0, 0)}{|h|} = 0$$

so that $\phi'(0, 0) = 0$.

□

3. Let $f : [0, 1) \to \mathbb{R}$ be differentiable with bounded derivative. Prove that f can be extended to a continuous function on $[0, 1]$.

Solution: We show that $\lim_{x\to 1} f(x)$ exists. Note that $|f'(x)| \leq M$ for some $M > 0$. Note that $\lim_{x\to 1} f(x) = L$ if and only if for all sequences $\{p_n\}$, $p_n \neq 1$ for all n, and $p_n \to 1$, we have $f(p_n) \to L$. Now let $p_n \to 1$. Since $\{p_n\}$ converges, $\{p_n\}$ is Cauchy. Then for all $\epsilon > M > 0$, there exists $N \in \mathbb{N}$ such that for $n, m > N$, $|p_n - p_m| < \frac{\epsilon}{M}$. By the Mean Value Theorem, there exists $\xi \in (p_n, p_m)$ such that

$$|f(p_n) - f(p_m)| = |f'(\xi)|\,|p_n - p_m| < M \cdot \frac{\epsilon}{M} = \epsilon$$

for $n, m > N$. But then $\{f(p_n)\}$ is Cauchy, which implies $\{f(p_n)\}$ converges as every Cauchy sequence in $\mathbb{R}$ converges. Then $\lim_{x\to 1} f(x) = L$ for some L. Then $f(1-) = L = f(1+)$. Define $\hat{f} : [0,1] \to \mathbb{R}$ such that

$$\hat{f}(x) = \begin{cases} f(x), & x \in [0,1) \\ L, & x = 1 \end{cases}$$

Clearly, $\hat{f}$ is continuous and $\hat{f} \equiv f$ on $[0,1)$. □

4. If $\sum_{k=0}^{n} \frac{a_k}{k+1} = 0$, prove that the polynomial $\sum_{k=0}^{n} a_k x^k$ has at least one root in the interval $(0,1)$.

Solution: Consider the polynomial $F(x) = \sum_{k=0}^{n} \frac{a_k}{k+1} x^{k+1}$. Clearly, this function is differentiable (hence continuous) on $[0,1]$. Observe that $F(0) = 0$ and $F(1) = \sum_{k=0}^{n} \frac{a_k}{k+1} = 0$ by assumption. By Rolle's Theorem, there must be a point $c \in (0,1)$ such that $F'(c) = 0$. However, $F'(x) = \sum_{k=0}^{n} a_k x^k$ so that there is a point c such that $\sum_{k=0}^{n} a_k c^k = 0$. That is, $\sum_{k=0}^{n} a_k x^k$ has a root in $(0,1)$.

OR

Note that the polynomial $\sum_{k=0}^{n} a_k x^k$ is continuous on $[0,1]$. Then by the Mean Value Theorem for integrals, there exists $\xi \in (0,1)$ such that

$$\sum_{k=0}^{n} a_k \xi^k = \int_0^1 \sum_{k=0}^{n} a_k x^k \, dx = \sum_{k=0}^{n} \int_0^1 a_k x^k \, dx = \sum_{k=0}^{n} \left[\frac{a_k}{k+1} x^{k+1} \right]_0^1 = \sum_{k=0}^{n} \frac{a_k}{k+1} = 0.$$

But then $\sum_{k=0}^{n} a_k x^k$ has at least one root in the interval $(0,1)$. □

5. Assume $f : [0,\infty) \to \mathbb{R}$ is nonnegative, Riemann integrable on $[0,b]$ for every $b > 0$, and

$$\lim_{b\to\infty} \int_0^b f(t) \, dt < \infty$$

Prove or give a counterexample;

(a) $\lim_{x\to\infty} f(x) = 0$,

(b) f is continuous implies $\lim_{x\to\infty} f(x) = 0$,

(c) f is uniformly continuous implies $\lim_{x\to\infty} f(x) = 0$.

Solution:

(a)

(b)

(c)

6. Let $f, f_n : [0,1] \to \mathbb{R}$ and $\phi : \mathbb{R} \to \mathbb{R}$. Prove or give a counterexample to each of the following statements;

(a) If $f_n \to f$ uniformly on $[0,1]$ and ϕ is continuous, then $\phi \circ f_n \to \phi \circ f$ uniformly.

(b) If $f_n \to f$ uniformly on $[0,1]$ and ϕ is uniformly continuous, then $\phi \circ f_n \to \phi \circ f$ uniformly.

(c) If $f_n \to f$ uniformly on $[0,1]$ and f and ϕ are continuous, then $\phi \circ f_n \to \phi \circ f$ uniformly.

Solution:

(a) Let $f_n = x + \frac{1}{n}$ and $f(x) = x$. Clearly, f_n converges pointwise to $f(x)$. Let $\epsilon > 0$ and take $N \in \mathbb{N}$ such that $\frac{1}{N} < \epsilon$, i.e. $N > \frac{1}{\epsilon}$. Then for $n > N$, we have

$$|f_n(x) - f(x)| = \left| x + \frac{1}{n} - x \right| = \frac{1}{n} \leq \frac{1}{N} < \epsilon$$

for $x \in [0,1]$ so that $\{f_n\}$ converges uniformly to f. Take $\phi(x) = x^2$. Clearly, ϕ is continuous. If $\phi \circ f_n$ were to converge uniformly to $\phi \circ f$, for $\epsilon > 0$, there would exist $N \in \mathbb{N}$ such that for $n > N$, $|\phi \circ f_n - \phi \circ f| < \epsilon$ for all $x \in [0,1]$. Take $\epsilon = 2$. Observe for $x = 1$ and $n > N$,

$$|\phi \circ f_n - \phi \circ f| = \left| \left(x + \frac{1}{n} \right)^2 - x^2 \right| = \left| \frac{2x}{n} + \frac{1}{n^2} \right| = \left| 2 + \frac{1}{n^2} \right| > 2 = \epsilon,$$

a contradiction. Therefore, $\phi \circ f_n$ does not converge to $\phi \circ f$ uniformly.

(b) Suppose that f_n converges to f uniformly on $[0,1]$ and that ϕ is uniformly continuous. Then given $\epsilon > 0$, there exists $\delta > 0$ such that for $|x - y| < \delta$, $|\phi(x) - \phi(y)| < \epsilon$> Since f_n converges to f uniformly, there exists $N \in \mathbb{N}$ such that for $n > N$, $|f_n(x) - f(x)| < \delta$. But then for $n > N$, $|f_n(x) - f(x)|\delta$ which implies $|\phi(f_n(x)) - \phi(f(x))| < \epsilon$ for all x, y with $|x - y| < \delta$. But then $\phi \circ f_n$ converges to $\phi \circ f$ uniformly.

(c) The statement is false by (a).

□

January 2007

1. Let X be a metric space and let A_j be subsets of X, $j = 1, 2, \ldots$. For each of the following statements, prove it or give a counterexample (the $'$ means limit points):

(i) $(A_1 \cup A_2)' \subseteq A_1' \cup A_2'$

(ii) $\overline{\bigcup_{j=1}^{\infty} A_j} \subseteq \bigcup_{j=1}^{\infty} \overline{A}_j$

Solution:

(i) If A_1, A_2 are empty, then the result is trivial. Let $x \in (A_1 \cup A_2)'$. Then every neighborhood of x intersects $A_1 \cup A_2$ of some point distinct from x. Without loss of generality, assume the neighborhoods intersect A_1. But then $x \in A_1'$. But then $x \in A_1' \cup A_2'$ so that $(A_1 \cup A_2)' \subseteq A_1' \cup A_2'$.

(ii) The statement is false. We give three counterexamples. First as the rationals are countable, enumerate them $a_1, a_2, a_3, \cdots$. Let $A_j = \{a_j\}$. Then $\overline{A_j} = A_j$ for all j. But $\cup A_j = \mathbb{Q}$ and $\overline{\mathbb{Q}} = \mathbb{R}$. So $\mathbb{R} = \overline{\cup_{j=1}^{\infty} A_j} \not\subseteq \cup_{j=1}^{\infty} A_j = \mathbb{Q}$. As a second example, take $A_j = \{1/j\}$ for $j \in \mathbb{N}$. Then $A_j' = \emptyset$. Then

$$\{1/j\}_{j=1}^{\infty} \cup \{0\} = \overline{\bigcup_{j=1}^{\infty} A_j} \not\subseteq \bigcup_{j=1}^{\infty} \overline{A_j} = \{1/j\}_{j=1}^{\infty}$$

As a final counterexample, take $A_j = [1/j, 1]$. We have $\overline{A_j} = A_j$ but

$$[0,1] = \overline{\bigcup_{j=1}^{\infty} A_j} \not\subseteq \bigcup_{j=1}^{\infty} \overline{A_j} = (0,1]$$

□

2. Prove that the series $\displaystyle\sum_{n=1}^{\infty} \frac{n^2}{n!}$ is convergent and find its sum.

Solution: Observe

$$\begin{aligned}
\lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| &= \lim_{n\to\infty} \left| \frac{(n+1)^2}{(n+1)!} \cdot \frac{n!}{n^2} \right| \\
&= \lim_{n\to\infty} \left| \left(\frac{n+1}{n} \right)^2 \frac{n!}{(n+1)!} \right| \\
&= \lim_{n\to\infty} \left| \left(1 + \frac{1}{n} \right) \frac{1}{n+1} \right| \\
&= 0 < 1
\end{aligned}$$

So the series converges by the Ratio Test. Observe also $e^x \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} \frac{x^n}{n!}$. So

$$\frac{d}{dx} e^x = \sum_{n=0}^{\infty} \frac{nx^{n-1}}{n!} = e^x$$

$$\frac{d^2}{dx^2} e^x = \sum_{n=0}^{\infty} \frac{n(n-1)x^{n-2}}{n!} = e^x$$

So

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{nx^{n-1}}{n!} &= e^1 \\ + \sum_{n=0}^{\infty} \frac{n(n-1)x^{n-2}}{n!} &= e^1 \\ \hline \sum_{n=0}^{\infty} \frac{n^2}{n!} &= 2e \end{aligned}$$

One could also do this by shifting index

$$\sum_{n=1}^{\infty} \frac{n^2}{n!} = \sum_{n=1}^{\infty} \frac{n}{(n-1)!} = \sum_{n=0}^{\infty} \frac{n+1}{n!} = \sum_{n=0}^{\infty} \frac{n}{n!} + \sum_{n=0}^{\infty} \frac{1}{n!} = e + e = 2e$$

□

3. Let $f : (-1, 1) \to \mathbb{R}$ be a differentiable function such that $f(0) = 0$ and $f''(0) \in \mathbb{R}$ exists. Prove that the limit $\lim_{x \to 0} \frac{f(2x) - 2f(x)}{x^2}$ exists.

Solution: Observe that $f(2x) - 2f(x)$ is differentiable as $f(x)$ is and that x^2 is differentiable. As $x \to 0$, we know that $f(2x) - 2f(x) \to 0$ and $x^2 \to 0$. Furthermore, $\frac{d}{dx} x^2 = 2x \neq 0$ on all of $(-1, 1)$. Therefore by L'Hôpitals, we know that

$$\lim_{x \to 0} \frac{f(2x) - 2f(x)}{x^2} = \lim_{x \to 0} \frac{2f'(2x) - 2f'(x)}{2x} = \lim_{x \to 0} \frac{f'(2x) - f'(x)}{x}$$

Again, $f'(2x) - f'(x)$ is differentiable as $f'(x)$ is and x is differentiable and $\frac{d}{dx} x = 1 \neq 0$ on all of $(-1, 1)$. Therefore by L'Hôpitals, we know that

$$\lim_{x \to 0} \frac{f'(2x) - f'(x)}{x} = \lim_{x \to 0} \frac{2f''(2x) - f''(x)}{1} = 2f''(0) - f''(0) = f''(0)$$

□

4.

(a) Let $f^4 \in \mathcal{R}$ (this means f^4 is integrable dx on some closed interval) prove or disprove, $f \in \mathcal{R}$.

(b) Let $f^5 \in \mathcal{R}$ prove or disprove, $f \in \mathcal{R}$.

Solution:

(a) The statement is false. Take $f(x)$ to be the

$$f(x) = \begin{cases} 0, & x \notin \mathbb{Q} \\ 1, & \text{otherwise} \end{cases}$$

This function is not Riemann integrable ($\inf U(P,f) = b-a$ while $\sup L(P,f) = 0$ on any compact interval $[a,b]$). However, $f(x)^{2n} = 1$ for all $n \in \mathbb{N}$ is clearly Riemann integral.

(b) If f happens to be bounded on $[a,b]$, then the statement is true. Suppose $f^{2n-1}(x) \in R$ for $n \in \mathbb{N}$. As $f(x)$ is bounded on $[a,b]$, $m \leq f(x) \leq M$ for some $m, M \in \mathbb{R}$. Then $m^3 \leq f^5(x) \leq M^5$ on $[a,b]$. We know that $\phi(x) = x^{1/(2n-1)}$ is continuous on $\mathbb{R}$, in particular $[m^3, M^3]$. But then $\phi(f^{1/(2n-1)}) = f(x)$ is integrable on $[a,b]$.

□

5. Let $f(x,y)$ be a real continuous function on the rectangle $[0,1] \times [0,2]$. Given $\epsilon > 0$ show that there exists n and real continuous functions $g_i(x)$ on $[0,1]$ and $h_i(y)$ on $[0,2]$ for $i = 1, \ldots, n$ so that

$$|f(x,y) - \sum_{i=1}^{n} g_i(x)h_i(y)| < \epsilon$$

for all (x,y) in the rectangle.

Solution: Define

$$\mathcal{A} = \left\{ \sum_{i=1}^{n} g_i(x)h_i(y) \colon n \in \mathbb{N}, g_i : [0,1] \to \mathbb{R}, h_i : [0,2] \to \mathbb{R} \text{ both continuous} \right\}.$$

Note that $[0,1] \times [0,2]$ compact and $\mathcal{A} \subseteq C([0,1] \times [0,2], \mathbb{R})$. Let $\sum_{i=1}^{n} g_i(x)h_i(y), \sum_{i=1}^{m} \tilde{g}_i(x)\tilde{h}_i(y) \in \mathcal{A}$. Without loss of generality, assume $n \leq m$. Then

$$\sum_{i=1}^{n} g_i(x)h_i(y) + \sum_{i=1}^{m} \tilde{g}_i(x)\tilde{h}_i(y) = \sum_{i=1}^{m} f_i(x) \cdot 1 \in \mathcal{A},$$

where $f_i(x) = g_i(x)h_i(y) + \tilde{g}_i(x)\tilde{h}_i(y)$ for $i = 1, \ldots, n$ and $f_i(x) = \tilde{g}_i(x)\tilde{h}_i(y)$ for $i = n+1, \ldots, m$. [Note that $1 \in \mathcal{A}$ and $f_i(x) \in \mathcal{A}$ for $i = 1, \ldots, m$.] Moreover, $\sum_{i=1}^{n} g_i(x)h_i(y) \cdot$

$\sum_{i=1}^{m} \tilde{g}_i(x)\tilde{h}_i(y) \in \mathcal{A}$. Finally, $c\sum_{i=1}^{n} g_i(x)h_i(y) = \sum_{i=1}^{n} cg_i(x)h_i(y) \in \mathcal{A}$ since cg_i is continuous, where $c \in \mathbb{R}$. Therefore, $\mathcal{A}$ is an algebra.

Choose distinct $(x_1, y_1), (x_2, y_2) \in [0,1] \times [0,2]$. Then either $x_1 \neq x_2$ or $y_1 \neq y_2$. Define $p_1(x) = x$, $p_2(y) = y$, $h_1(x) = 1$, and $h_2(y) = 1$. Clearly, $p_1(x)h_2(y), p_2(y)h_1(x) \in \mathcal{A}$. If $x_1 \neq x_2$, then $p_1(x_1)h_2(y_1) = x_1 \neq x_2 = p_1(x_2)h_2(y_2)$. If $y_1 \neq y_2$, then $p_2(y_1)h_1(x_1) = y_1 \neq y_2 = p_2(y_2)h_1(x_2)$. Therefore, $\mathcal{A}$ separates points. Moreover, choosing $g(x) = h(y) = 1$, then $0 \neq g(x)h(y) = 1 \in \mathcal{A}$ so that $\mathcal{A}$ vanishes at no point of $[0,1] \times [0,2]$. By Stone-Weierstrass, $\overline{\mathcal{A}} = C([0,1] \times [0,2], \mathbb{R})$. Then for all $f(x,y) \in C([0,1] \times [0,2], \mathbb{R})$, there exists a sequence of elements of $\mathcal{A}$ that converges uniformly to f. Therefore given $\epsilon > 0$, there exists $n \in \mathbb{N}$, $g_i(x) : [0,1] \to \mathbb{R}$, $h_i(y) : [0,2] \to \mathbb{R}$, both continuous, such that

$$|f(x,y) - \sum_{i=1}^{n} g_i(x)h_i(y)| < \epsilon$$

□

6. Given the equations $x - f(u,v) = 0$ and $y - g(u,v) = 0$ **(a)** give conditions that assure you can solve for (x,y) in terms of (u,v) and **(b)** similarly that you can solve for (u,v) in terms of (x,y). **(c)** Assuming these conditions are satisfied prove that

$$\frac{\partial x(u,v)}{\partial u}\frac{\partial u(x,y)}{\partial x} = \frac{\partial y(u,v)}{\partial v}\frac{\partial v(x,y)}{\partial y}$$

Solution:

(a) Define $F = (F_1, F_2) : \mathbb{R}^4 \to \mathbb{R}^2$, where $F_1(x,y,u,v) = x - f(u,v)$ and $F_2(x,y,u,v) = y - g(u,v)$. Suppose $F \in C^1$ and there exists (a,b,c,d) such that $F(a,b,c,d) = (0,0)$. Then

$$\left.\begin{vmatrix} \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} \end{vmatrix}\right|_{(a,b,c,d)} = \left.\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}\right|_{(a,b,c,d)} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \neq 0$$

Then by the Implicit Function Theorem, there exists h, differentiable in a neighborhood of (a,b,c,d), such that $h(c,d) = (a,b)$ and $F(h(u,v),u,v) = 0$, i.e. the system has a unique solution $(x,y) = h(u,v)$ in a neighborhood of (a,b,c,d). Therefore, it is sufficient that $F \in C^1$ and $F(a,b,c,d) = (0,0)$.

(b) Note that if $F \in C^1$ and there is (a,b,c,d) such that $F(a,b,c,d) = 0$,

$$B := \begin{vmatrix} \frac{\partial F_1}{\partial u} & \frac{\partial F_1}{\partial v} \\ \frac{\partial F_2}{\partial u} & \frac{\partial F_2}{\partial v} \end{vmatrix} \neq 0.$$

Then by the Implicit Function Theorem, there exists a $\hat{h}$, differentiable in a neighborhood of (a,b,c,d), such that $\hat{h}(a,b) = (c,d)$ and $F(x,y,\hat{h}(x,y)) = 0$, i.e. the system has a unique solution $(u,v) = \hat{h}(x,y)$ in a neighborhood of (a,b,c,d). Then it is sufficient that $F \in C^1$ and there is (a,b,c,d) such that $F(a,b,c,d) = 0$.

(c) Assuming the conditions in (a) and (b) hold, the Implicit Function Theorem gives

$$h'(u,v) = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{\partial F_1}{\partial u} & \frac{\partial F_1}{\partial v} \\ \frac{\partial F_2}{\partial u} & \frac{\partial F_2}{\partial v} \end{pmatrix} = \begin{pmatrix} -\frac{\partial F_1}{\partial u} & -\frac{\partial F_1}{\partial v} \\ -\frac{\partial F_2}{\partial u} & -\frac{\partial F_2}{\partial v} \end{pmatrix}$$

and $\frac{\partial x(u,v)}{\partial u} = -\frac{\partial F_1}{\partial u}$, $\frac{\partial y(u,v)}{\partial v} = -\frac{\partial F_2}{\partial v}$. Furthermore, the Implicit Function Theorem gives

$$\hat{h}(x,y) = -\frac{1}{\det B}\begin{pmatrix} \frac{\partial F_2}{\partial v} & -\frac{\partial F_1}{\partial v} \\ -\frac{\partial F_2}{\partial u} & \frac{\partial F_1}{\partial u} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -\frac{1}{\det B}\begin{pmatrix} \frac{\partial F_2}{\partial v} & -\frac{\partial F_1}{\partial v} \\ -\frac{\partial F_2}{\partial u} & \frac{\partial F_1}{\partial u} \end{pmatrix}$$

and $\frac{\partial u(x,y)}{\partial x} = -\frac{1}{\det B}\frac{\partial F_2}{\partial v}$, $\frac{\partial v(x,y)}{\partial y} = -\frac{1}{\det B}\frac{\partial F_1}{\partial u}$. Therefore,

$$\begin{aligned} \frac{\partial x(u,v)}{\partial u}\frac{\partial u(x,y)}{\partial x} &= -\frac{\partial F_1}{\partial u}\cdot -\frac{1}{\det B}\frac{\partial F_2}{\partial v} = \frac{1}{\det B}\frac{\partial F_1}{\partial u}\frac{\partial F_2}{\partial v} \\ \frac{\partial y(u,v)}{\partial v}\frac{\partial v(x,y)}{\partial y} &= -\frac{\partial F_2}{\partial v}\cdot -\frac{1}{\det B}\frac{\partial F_1}{\partial u} = \frac{1}{\det B}\frac{\partial F_1}{\partial u}\frac{\partial F_2}{\partial v} \end{aligned}$$

But then

$$\frac{\partial x(u,v)}{\partial u}\frac{\partial u(x,y)}{\partial x} = \frac{\partial y(u,v)}{\partial v}\frac{\partial v(x,y)}{\partial y}.$$

□

August 2007

1. Show that any set E in a connected metric space X with no boundary in X is either X or empty. Note: if we denote the closure of E by $\overline{E}$ and the complement of E by E^c then the boundary of E is given by $\overline{E} \cap \overline{E}^c$.

Solution: Recall bd $E = \overline{E} \cap \overline{E^C}$. It is clear that $X = E \cup E^C$. We show that E is clopen. Suppose that E were not open. Then there is an $x \in E$ such that all neighborhoods of x intersect E^C. But then $x \in E^{C\,\prime} \subset \overline{E^C}$. But then $x \in E \subset \overline{E}$ and $x \in \overline{E^C}$ so that $x \in$ bd E, contradicting the fact that E has no boundary. To see that E is closed, suppose it is not. Then there is an $x \in X$ such that all neighborhoods of x intersect E but $x \notin E$. So $x \in E' \subset \overline{E}$. As $x \notin E$ then $x \in E^C \subset \overline{E^C}$. But then $x \in$ bd E, a contradiction. This shows that E is clopen. As X is a connected metric space, one of E, E^C must be empty forcing the other to be X. □

2. Suppose that a function f is defined on $[0, \infty)$, bounded on any interval $[0, a]$, $a < \infty$, and $\lim_{x\to\infty}(f(x+1) - f(x))$ exists. Show that

$$\lim_{x\to\infty} \frac{f(x)}{x} = \lim_{x\to\infty} (f(x+1) - f(x)).$$

Solution: By the Stolz-Cesáro Theorem[30], if $y_n \nearrow \infty$, then $\lim_{n\to\infty} \frac{x_n}{y_n} = \lim_{n\to\infty} \frac{x_{n+1}-x_n}{y_{n+1}-y_n}$ if the limit exists. Now that $x \nearrow \infty$. Then by Stolz-Cesáro Theorem,

$$\lim_{x\to\infty} \frac{f(x)}{x} = \lim_{x\to\infty} \frac{f(x+1) - f(x)}{(x+1) - x} = \lim_{x\to\infty} [f(x+1) - f(x)]\,.$$

Therefore, $\lim_{x\to\infty} \frac{f(x)}{x} = \lim_{x\to\infty} [f(x+1) - f(x)]$. □

3. Suppose that $\sum a_n$ and $\sum b_n$ are series with non-negative terms and the series $\sum b_n$ converges. Show that if

$$\frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n}$$

for all $n \geq n_0$, then the series $\sum a_n$ also converges. Derive that $\sum a_n$ converges if $a_n > 0$ and if there is a $p > 1$ so that $\frac{a_{n+1}}{a_n} < 1 - \frac{p}{n}$ for all n. [Hint: Use $b_n = n^{-p}$.]

Solution: Note that $\frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n}$ so that $a_{n+1} \leq \frac{b_{n+1}}{b_n} a_n$. But then

$$a_{n+2} \leq \frac{b_{n+2}}{b_{n+1}} a_{n+1} \leq \frac{b_{n+2}}{b_{n+1}} \cdot \frac{b_{n+1}}{b_n} a_n = \frac{b_{n+2}}{b_n} a_n.$$

[30] Stolz-Cesáro Theorem: if $\{a_n\}$ and $\{b_n\}$ are sequences of real numbers with $\{b_n\}$ strictly monotone and divergence, if $\lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n} = l$ exists, then $\lim_{n\to\infty} \frac{a_n}{b_n} = l$.

Assume that $a_{n+k-1} \leq \frac{b_{n+k-1}}{b_n} a_n$. Then

$$a_{n+k} \leq \frac{b_{n+k}}{b_{n+k-1}} a_{n+k-1} \leq \frac{b_{n+k}}{b_{n+k-1}} \cdot \frac{b_{n+k-1}}{b_n} a_n = \frac{b_{n+k}}{b_n} a_n.$$

Therefore, $a_{n+k} \leq \frac{b_{n+k}}{b_n} a_n$ for all $k \geq n_0 - n$. Note that $\sum_{n=1}^{\infty} a_n$ converges if and only if $\sum_{n=1}^{\infty} a_{n+k}$ converges for $k \geq n_0 - n$ (since the series differ by finitely many terms). Then

$$\sum_{n=1}^{\infty} a_{n+k} \leq \sum_{n=1}^{\infty} \frac{b_{n+k}}{b_k} a_k = \frac{a_k}{b_k} \sum_{n=1}^{\infty} b_{n+k} < \infty$$

since $\sum_{n=1}^{\infty} b_n$ converges. Therefore, $\sum_{n=1}^{\infty} a_n$ converges. Assume that there exists $p > 1$ such that $\frac{a_{n+1}}{a_n} < 1 - \frac{p}{n}$. Take $b_n = n^{-p}$. Note that $\sum_{n=1}^{\infty} b_n = \sum_{n=1}^{\infty} \frac{1}{n^p}$ converges since $p > 1$. Now $b_n > 0$ and $\frac{a_{n+1}}{a_n} < 1 - \frac{p}{n}$. Note that by the Binomial Theorem, we have

$$(1+c)^k = \sum_{i=0}^{k} \binom{k}{c} c^i = 1 + kc + \cdots + kc^{k-1} + c^k \geq 1 + kc.$$

Then

$$\frac{a_{n+1}}{a_n} < 1 - \frac{p}{n} \leq \left(1 + \frac{1}{n}\right)^{-p} = \left(\frac{n+1}{n}\right)^{-p} = \frac{(n+1)^{-p}}{n^{-p}} = \frac{b_{n+1}}{b_n}.$$

By our original work, $\sum a_n$ converges. □

4. Let $f(x)$ be continuous on $[0,1]$ and suppose that

$$\int_0^1 f(x)\, x^n \, dx = \frac{1}{n+1}$$

for all $n = 0, 1, 2, \ldots$. What can you say about the function $f(x)$? Prove your answer.

Solution: If $n = 0$, then we have $\int_0^1 f(x)\, dx = \frac{1}{0+1} = 1$. Note that

$$\begin{aligned}
\int_0^1 f(x)p(x)\, dx &= \int_0^1 f(x)(a_n x^n + \cdots + a_0)\, dx \\
&= a_n \int_0^1 f(x) x^n \, dx + \cdots + a_0 \int_0^1 f(x)\, dx \\
&= \frac{a_n}{n+1} + \frac{a_{n-1}}{n} + \cdots + \frac{a_1}{2} + a_0 \\
&= \int_0^1 p(x)\, dx.
\end{aligned}$$

Now since f is continuous on $[0,1]$, by Weierstrass' Theorem, there exists a sequence $\{p_n\}$ of polynomials such that $\{p_n\}$ converges uniformly to f on $[0,1]$. Then using uniform convergence,

$$\begin{aligned}
\int_0^1 (f(x))^2\,dx &= \int_0^1 f(x) \lim_{n\to\infty} p_n(x)\,dx \\
&= \lim_{n\to\infty} \int_0^1 f(x)p_n(x)\,dx \\
&= \lim_{n\to\infty} \int_0^1 p_n(x)\,dx \\
&= \int_0^1 \lim_{n\to\infty} p_n(x)\,dx \\
&= \int_0^1 f(x)\,dx \\
&= 1.
\end{aligned}$$

Therefore, $\int_0^1 (f(x))^2\,dx = \int_0^1 f(x)\,dx = 1$. Now as $f(x)$ is continuous, $(f(x)-1)^2$ is continuous and nonnegative on $[0,1]$. Finally,

$$\begin{aligned}
\int_0^1 (f(x)-1)^2\,dx &= \int_0^1 f(x)^2 - 2f(x) + 1\,dx \\
&= \int_0^1 f(x)^2\,dx - 2\int_0^1 f(x)\,dx + \int_0^1 1\,dx \\
&= 1 - 2\cdot 1 + 1 \\
&= 0
\end{aligned}$$

Therefore, $(f(x)-1)^2 = 0$ on $[0,1]$. This implies that $f(x) = 1$ on $[0,1]$. □

5. Prove that the only function $f(x)$ satisfying $f^2(x)$ is Riemann integrable on $[0,1]$ and

$$f(x) = \int_0^x f^2(t)\,dt \text{ for } x \in [0,1]$$

is the function $f(x) \equiv 0$.

6. Consider the map $(u,v) = \boldsymbol{f}(x,y)$ from $\mathbb{R}^2$ to $\mathbb{R}^2$ given by $u = x^2 + y^2$, $v = x^2 + y^2 - y$.

(a) Find all the points (x,y) so that $\boldsymbol{f}(x,y) = (1,1/2)$.

(b) Choose one of the points you found in (a) and call it $\boldsymbol{a} = (x_0,y_0)$. What does the Inverse Function Theorem say about $\boldsymbol{f}$ near $\boldsymbol{a}$? State your answer carefully.

(c) Why is (a) not a contradiction to (b)?

Solution:

(a) Observe $v = x^2 + y^2 - y = u - v$ so that $y = u - v$. Furthermore, $u = x^2 + y^2$ so that $x^2 = u - y^2 = u - (u - v)^2$. Then $x = \pm\sqrt{u - (u - v)^2}$. Now $y = 1 - \frac{1}{2} = \frac{1}{2}$. Then $x = \pm\sqrt{1 - (1 - \frac{1}{2})^2} = \pm\sqrt{\frac{3}{4}} = \pm\frac{\sqrt{3}}{2}$. Therefore,

$$X := \{(x, y) \colon f(x, y) = (1, \frac{1}{2})\} = \{(\frac{\sqrt{3}}{2}, \frac{1}{2}), (-\frac{\sqrt{3}}{2}, \frac{1}{2})\}.$$

(b) Clearly, $f \in C^1(\mathbb{R}^2)$ since f has continuous partial derivatives. Moreover,

$$J_f(x, y) = \begin{vmatrix} 2x & 2y \\ 2x & 2y - 1 \end{vmatrix} = 2x(2y - 1) - 4xy = -2x.$$

Now $J_f(\pm\sqrt{32}, \frac{1}{2}) = \mp\sqrt{3} \neq 0$. Therefore, the Inverse Function Theorem applies to all points $p \in X$. But then there exist neighborhoods of $p \in X$ such that $f^{-1} \in C^1$ exists and $f^{-1}(f(p)) = p$ for $p \in X$.

(c) The statement of (b) holds only for some neighborhood of $p \in X$ and does not imply that f has an inverse outside of that neighborhood.

□

August 2008

1. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be given by the formula

$$f(x,y) = \begin{cases} \dfrac{x^2 y}{x^2+y^2}, & \text{if } (x,y) \neq (0,0) \\ 0, & \text{if } (x,y) = (0,0) \end{cases}$$

(a) Show that f is continuous at $(0,0)$.

(b) Prove that the first order partial derivatives of f at (0,0) exist.

(c) Prove that f is not differentiable at (0,0).

Solution:

(a) Using polar coordinates, we have

$$\lim_{(x,y)\to(0,0)} \left| \frac{x^2 y}{x^2+y^2} \right| = \lim_{r\to 0} \left| \frac{r^3 \sin\theta \cos^2\theta}{r^2} \right| = \lim_{r\to 0} \left| r \sin\theta \cos^2\theta \right| \leq \lim_{r\to 0} |r| = 0$$

so that $f(x,y)$ is continuous at the origin.

OR

Observe that

$$\lim_{(x,y)\to(0,0)} \left| \frac{x^2 y}{x^2+y^2} \right| \leq \lim_{(x,y)\to(0,0)} \left| \frac{x^2 y}{x^2} \right| = \lim_{(x,y)\to(0,0)} |y| = 0$$

so that $f(x,y)$ is continuous at the origin.

OR

Note that

$$|f(x,y)| = \left| \frac{x^2 y}{x^2+y^2} \right| = \left| x \cdot \frac{xy}{x^2+y^2} \right| \leq \left| x \cdot \frac{2xy}{x^2+y^2} \right|$$

Now $(x-y)^2 \geq 0$ for all x, y. But then $x^2 - 2xy + y^2 \geq 0$, showing $x^2 + y^2 \geq 2xy$. Then

$$|f(x,y)| \leq \left| x \cdot \frac{2xy}{x^2+y^2} \right| \leq \left| x \cdot \frac{x^2+y^2}{x^2+y^2} \right| = |x|$$

Then as $\lim_{(x,y)\to(0,0)} |x| = 0$, we must have $\lim_{(x,y)\to(0,0)} f(x,y) = 0$. Therefore, $f(x,y)$ is continuous at $(0,0)$.

(b) We have

$$f_x(0,0) = \lim_{h\to 0} \frac{f(0+h,0) - f(0,0)}{h} = \lim_{h\to 0} \frac{0-0}{h} = 0$$
$$f_y(0,0) = \lim_{h\to 0} \frac{f(0,0+h) - f(0,0)}{h} = \lim_{h\to 0} \frac{0-0}{h} = 0$$

(c) If $f(x,y)$ were differentiable at $(0,0)$, then the following limit exists and is 0:

$$\lim_{(x,y)\to(0,0)} \frac{f(x,y) - \left[f(0,0) + f_x(0,0)(x-0) + f_y(0,0)(y-0)\right]}{\sqrt{x^2+y^2}}$$

But this is precisely

$$\lim_{(x,y)\to(0,0)} \frac{x^2 y}{(x^2+y^2)^{3/2}}$$

Taking $x = y = 1/n$ for $n \in \mathbb{N}$, we have

$$\lim_{(x,y)\to(0,0)} \frac{x^2 y}{(x^2+y^2)^{3/2}} = \lim_{n\to\infty} \frac{(1/n)^2(1/n)}{(1/n^2+1/n^2)^{3/2}} = \lim_{n\to\infty} \frac{1}{\sqrt{8}} \neq 0$$

a contradiction so that the limit does not exist and therefore $f(x,y)$ is not differentiable at the origin.

OR

Let $u = (u_1, u_2)$ be a unit vector, i.e. $u_1^2 + u_2^2 = 1$. Suppose f were differentiable at $(0,0)$. Then $D_u f(0,0) = \nabla f(0) \cdot u$. But

$$D_u f(0,0) = \lim_{t\to 0} \frac{f((0,0)+tu) - f(0,0)}{t} = \lim_{t\to 0} \frac{f(tu_1, tu_2)}{t} = \frac{\frac{t^3 u_1^2 u_2}{t^2(u_1^2+u_2^2)}}{t} = \frac{u_1^2 u_2}{u_1^2+u_2^2} = u_1^2 u_2.$$

Now $\nabla f(0,0) = (0,0) \cdot (u_1, u_2) = 0$. But if neither u_1, u_2 are zero, then $u_1^2 u_2 \neq 0$, a contradiction. Therefore, f is not differentiable at $(0,0)$.

□

2. Suppose $f : \mathbb{R} \to \mathbb{R}$ is a continuous function satisfying the equation

$$|f(x) - f(y)| \geq |x - y| \text{ for all } x, y \in \mathbb{R}$$

Prove that $f(\mathbb{R}) = \mathbb{R}$.

Solution: Suppose that $f(x) = f(y)$. Then $|f(x) - f(y)| \geq |x - y|$ so that $0 \geq |x - y|$, implying $|x - y| = 0$. But then $x = y$ so that f is necessarily injective. Suppose that there exists $x < y < z$ such that $f(x) < f(y)$ and $f(y) > f(z)$. Since $x \neq z$, it must be that $f(x) \neq f(z)$ since that f is injective. Without loss of generality, $f(x) < f(z)$. But then $f(x) < f(z)$ and $f(z) < f(y)$. Since f is continuous, there exists $a \in (x, y)$ such that $f(a) = f(z)$ by the Intermediate Value Theorem. But since f is injective, $a = z$, a contradiction as $z \notin (x, y)$. Similarly, it cannot be possible $f(x) > f(y)$ and $f(y) < f(z)$. This shows that f is strictly monotone. But then f monotonic and injective so that f is a bijection (f is then surjective). Let $x \in \mathbb{R}$, then $x = f(y)$ for some $y \in \mathbb{R}$ as f is surjective. Therefore, $\mathbb{R} \subseteq f(\mathbb{R})$. Clearly, $f(\mathbb{R}) \subseteq$ so that we must have $f(\mathbb{R}) = \mathbb{R}$. □

3. Suppose the boundary of a set in $\mathbb{R}^2$ is a graph of a bounded function. Prove that the function is continuous.

Solution: Let $E \subseteq \mathbb{R}^2$ and $f : \mathbb{R} \to \mathbb{R}$ be bounded, i.e. $|f(x)| \leq M$ for all $x \in \mathbb{R}$. Let G be the graph of f. Then G is the boundary of E by assumption, i.e. $G = \overline{E} \setminus E^\circ = \overline{E} \cap \overline{E^C}$. Then G is closed as $G = \overline{E} \cap \overline{E^C}$ is the intersection of closed sets. Let $\{x_n\}$ be a sequence in $\mathbb{R}$ such that $x_n \to x$. We show that $f(x_n) \to f(x)$. Then we have $(x_n, f(x_n))$ be a sequence in G. Now $(x_n, f(x_n)) \in K := (\{x_n\} \cup \{x\}) \times [-M, M]$. Now $\{x_n\} \cup \{x\}$ is compact (it is the union of compact sets) and $[-M, M]$ is compact. Therefore, K is compact. Therefore for any subsequence $\{(x_{n_k}, f(x_{n_k}))\}$ of $\{(x_n, f(x_n)\}$, there exists a convergent subsequence $\{(x_{n_{k_l}}, f(x_{n_{k_l}}))\}$ so that $(x_{n_{k_l}}, f(x_{n_{k_l}})) \to (x, y)$ for some x, y with $x_n \to x$. Now as G is closed, we must have $(x, y) \in G$. But then $(x, y) = (x, f(x))$ for some x. Then $(x_{n_{k_l}}, f(x_{n_{k_l}})) \to (x, f(x))$ so that $(x_n, f(x_n)) \to (x, f(x))$. This proves that $f(x_n) \to f(x)$. Therefore, $f(x)$ is continuous. □

4. Prove or give a counterexample: Let $f : (0, 1) \to \mathbb{R}$ and $g : (0, 1) \to \mathbb{R}$ be continuously differentiable; that is, $f, g \in C^1(0, 1)$. Suppose that

$$\lim_{x \to 0+} f(x) = \lim_{x \to 0+} g(x) = 0$$

and g and g' never vanish on $(0, 1)$. If

$$\lim_{x \to 0+} \frac{f(x)}{g(x)} = c \quad \text{for some } c \in \mathbb{R},$$

then

$$\lim_{x \to 0+} \frac{f'(x)}{g'(x)} = c.$$[31]

[31] This is essentially l'Hôpital's Rule. The little remembered condition is that if one has a limit which results in an indeterminate form, $\lim_{x \to 0} \frac{f(x)}{g(x)} = \lim_{x \to 0} \frac{f'(x)}{g'(x)}$ assuming that $\lim_{x \to 0} \frac{f'(x)}{g'(x)}$ exists.

Solution: Take $f, g : (0,1) \to \mathbb{R}$ be given by $f(x) = x^2 \sin\left(\frac{1}{x}\right)$ and $g(x) = x$. Then $f'(x) = 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right)$ and $g'(x) = 1$. It is then clear that $f, g \in C'(0,1)$. We have

$$-x^2 \leq \left| x^2 \sin\left(\frac{1}{x}\right) \right| \leq x^2$$

so that $\lim_{x\to 0} f(x) = 0$ by Squeeze Theorem. It is clear that $\lim_{x\to 0} g(x) = 0$. Now g, g' never vanish on $(0,1)$. We have

$$\lim_{x\to 0} \frac{f(x)}{g(x)} = \lim_{x\to 0} x \sin\left(\frac{1}{x}\right)$$

and

$$-x \leq \left| x \sin\left(\frac{1}{x}\right) \right| \leq x$$

so that $\lim_{x\to 0} \dfrac{f(x)}{g(x)} = 0$ by the Squeeze Theorem. [Note that to this point, the limits existed so that in particular the right and left limits exist and are equal to the limit value.] But

$$\lim_{x\to 0^+} \frac{f'(x)}{g'(x)} = \lim_{x\to 0^+} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right),$$

If this limit existed, as

$$\lim_{x\to 0^+} -|2x| \leq \lim_{x\to 0^+} \left| 2x \sin\left(\frac{1}{x}\right) \right| \leq \lim_{x\to 0^+} |2x| = 0,$$

this would imply

$$\lim_{x\to 0^+} 2x \sin\left(\frac{1}{x}\right) - \lim_{x\to 0^+} \frac{f'(x)}{g'(x)} = \lim_{x\to 0^+} \cos\left(\frac{1}{x}\right)$$

exists, a clear contradiction. Therefore, $\lim_{x\to 0^+} \dfrac{f'(x)}{g'(x)} = 0$ does not exist. □

5. Let $\{\varphi_n\}_{n=1}^{\infty}$ be a sequence of non-negative Riemann integrable functions on $[0,1]$ such that

$$\lim_{n\to\infty} \int_0^1 x^k \varphi_n(x)\, dx$$

exists for $k = 0, 1, 2, \ldots$. Show that the limit

$$\lim_{n\to\infty} \int_0^1 f(x) \varphi_n(x)\, dx$$

exists for every continuous function f on $[0,1]$.

Solution: Let f be a continuous function on $[0,1]$. By Weierstrass' Theorem, there exists a sequence $\{p_m\}$ of polynomials such that $\{p_m\}$ converges uniformly to f on $[0,1]$. Then

$$\lim_{n\to\infty}\int_0^1 f(x)\phi_n(x)\,dt = \lim_{n\to\infty}\int_0^1 \lim_{m\to\infty} p_m(x)\phi_n(x)\,dt = \lim_{n\to\infty}\lim_{m\to\infty}\int_0^1 p_m(x)\phi_n(x)\,dx,$$

where we have made use of uniform convergence to exchange the limit and the integral. We show that $\int_0^1 p_m(x)\phi_n(x)\,dx$ converges uniformly to $\int_0^1 f(x)\phi_n(x)\,dx$ as $m\to\infty$. Now for all $n\in\mathbb{N}$, we have $\phi_n(x)\in\mathcal{R}$ so that $\{\phi_n(x)\}$ is pointwise bounded, i.e. $|\phi_n(x)|\le|\phi(x)|$ for some $\phi(x)$. Since $\{p_m\}$ converges uniformly to f, there exists a M such that for $m\ge M$, $|p_m-f|<\xi := \frac{\epsilon}{\int_0^1|\phi(x)|\,dx}$. Then for $m>M$

$$\begin{aligned}\left|\int_0^1 p_m(x)\phi_n(x)\,dt - \int_0^1 f(x)\phi_n(x)\,dt\right| &\le \int_0^1 |p_m(x)-f(x)|\,|\phi_n(x)|\,dx\\ &\le \int_0^1 \xi|\phi(x)|\,dx\\ &= \xi\int_0^1|\phi(x)|\,dx\\ &= \frac{\epsilon}{\int_0^1|\phi(x)|\,dx}\cdot\int_0^1|\phi(x)|\,dx\\ &= \epsilon.\end{aligned}$$

Then $\int_0^1 p_m(x)\phi_n(x)\,dx$ converges uniformly to $\int_0^1 f(x)\phi_n(x)\,dx$ as $m\to\infty$. Now show $\lim_{n\to\infty}\int_0^1 p_m(x)\phi_n(x)\,dx$ exists. Therefore,

$$\begin{aligned}\lim_{n\to\infty}\int_0^1 p_m(x)\phi_n(x)\,dx &= \lim_{n\to\infty}\int_0^1 (a_m x^m+\cdots+a_0)\phi_n(x)\,dx\\ &= \lim_{n\to\infty}\int_0^1 a_m x^m\phi_n(x)\,dx+\cdots+\lim_{n\to\infty}\int_0^1 a_0\phi_n(x)\,dx\end{aligned}$$

exists. But then

$$\lim_{n\to\infty}\int_0^1 f(x)\phi_n(x)\,dx = \lim_{n\to\infty}\lim_{m\to\infty}\int_0^1 p_m(x)\phi_n(x)\,dx = \lim_{m\to\infty}\lim_{n\to\infty}\int_0^1 p_m(x)\phi_n(x)\,dx$$

exists. □

6. For $n=1,2,3,\ldots$, let

$$f_n(x)=\begin{cases}1, & \text{if } x\in\{1,\frac{1}{2},\ldots,\frac{1}{n}\}\\ 0, & \text{otherwise}\end{cases}$$

(a) Does the sequence $\{f_n\}_{n=1}^{\infty}$ converge uniformly on $\mathbb{R}$? Justify your answer.

(b) Assume that $\alpha : \mathbb{R} \to \mathbb{R}$ is an increasing continuous function, prove or disprove the following identity

$$\lim_{n\to\infty} \int_{-1}^{1} f_n(x)\, d\alpha(x) = \int_{-1}^{1} \lim_{n\to\infty} f_n(x)\, d\alpha(x).$$

Solution:

(a)

(b)

January 2009

1. Let C be the standard Cantor set on the interval $[0,1]$ and let $A = C^c$ be its complement on the real line. Identify the set of all limit points A' of A, explaining your answer.[32]

Solution: Since C is closed, $A = C^c$ is open. Then A is the union of disjoint open intervals removed from $[0,1]$ to form the Cantor Set. Note that the endpoints of those intervals are the same endpoints as the nonexcluded intervals in the Cantor Set. Call this set of endpoints B. Let $x \in C$. Then $x \in I_n$ for some n, where I_n a interval in the n^{th} stage of the construction of the Cantor Set. The length of I_n is 3^{-n}. Let $y \in B \cap I_n$ so that y is an endpoint of I_n. Without loss of generality, assume $y \neq x$. Then $d(x,y) < 3^{-n}$ so that $y \in B_{3^{-n}}(x) \cap B$ and $y \neq x$. But then $x \in B'$ so that $x \in A'$. Therefore, $C \subseteq A'$. Now suppose $x \in A'$. Suppose $x \notin C$. Then $x \in B$ so that $x \in C'$. But this is a contradiction since C is closed and hence must contain all its limit points. But then $x \in C$. Therefore, $C = A'$. □

2.

(a) Prove

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

(b) Let $\{a_n\}$ be a sequence with limit L. Define a sequence

$$b_n = \frac{1}{n^2} \sum_{k=1}^{n} k a_k$$

Prove $\lim_{n\to\infty} b_n = L/2$.

Solution:

(a) We proceed by induction. First, we check the first few cases by hand

$$n = 1: \quad \sum_{i=1}^{1} i = 1; \qquad \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

$$n = 2: \quad \sum_{i=1}^{2} i = 1+2 = 3; \qquad \frac{2(2+1)}{2} = \frac{6}{2} = 3$$

$$n = 3: \quad \sum_{i=1}^{3} i = 1+2+3 = 6; \qquad \frac{3(3+1)}{2} = \frac{12}{2} = 6$$

[32] The solution will assume that the complement is meant to be taken in $[0,1]$ not the whole real line. Otherwise since $C \subseteq [0,1]$, $(\infty,0) \cup (1,\infty) \subseteq A$ and clearly every point in these intervals is a limit point. Then in the given solution, we must have $A' = C \cup (\infty,0) \cup (1,\infty)$.

Now assume the result is true for $n = 1, 2, 3, \ldots, k$. We need to show that the formula holds for $n = k + 1$.

$$\sum_{i=1}^{k+1} i = (k+1) + \sum_{i=1}^{k} i \overset{*}{=} (k+1) + \frac{k(k+1)}{2} = \frac{2(k+1)}{2} + \frac{k(k+1)}{2} = \frac{2k+2}{2} + \frac{k^2+k}{2}$$
$$= \frac{2k+k^2+k+2}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2} = \frac{(k+1)\left((k+1)+1\right)}{2}$$

where the starred equality follows from the induction hypothesis: $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. But then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ follows by induction.

OR

Write out the sum in 'increasing' order and again directly beneath it in 'decreasing' order.

$$\begin{array}{ccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & n \\ n & + & (n-1) & + & (n-2) & + & \cdots & + & 1 \end{array}$$

Adding these two rows yields

$$\begin{array}{ccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & n \\ n & + & (n-1) & + & (n-2) & + & \cdots & + & 1 \\ \hline (n+1) & + & (n+1) & + & (n+1) & + & \cdots & + & (n+1) \end{array}$$

This result is the n-fold sum of $(n+1)$'s. But then we have $2(1+2+\cdots+n) = n(n+1)$ so that $\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

OR

We want to find $1 + 2 + \cdots + n = \sum_{i=1}^{n} i$. Observe this is the same as finding $n + (n-1) + \cdots + 2 + 1 = \sum_{i=1}^{n} n - i + 1$, the sum written in reverse. But then we have

$$\begin{aligned} 2\sum_{i=1}^{n} i &= \sum_{i=1}^{n} i + \sum_{i=1}^{n} n - i + 1 \\ &= \sum_{i=1}^{n} i + (n - i + 1) \\ &= \sum_{i=1}^{n} n + 1 \\ &= n(n+1) \end{aligned}$$

But then we have $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

OR

Let $S(n) := \sum_{i=0}^{n} i$. Observe that $S(n) - S(n-1) = n$ for $n = 1, 2, \cdots$. But then $S(n)$ is a polynomial of degree two.[33] Suppose that $S(n) = an^2 + bn + c$. We must have $c = 0$ as $S(0) = 0$. Furthermore, $S(n) - S(n-1) = n$ and

$$n = S(n) - S(n-1) = (an^2 + bn) - (a(n-1)^2 + b(n-1)) = (2a)n + (b-a)$$

Relating the polynomials in n on the far left and right, we have $2a = 1$ and $b - a = 0$. But then $a = 1/2$ and $b = a$. Therefore, $S(n) = \sum_{i=1}^{n} i = \frac{1}{2}n^2 + \frac{1}{2}n = \frac{n(n+1)}{2}$. Alternatively, once one knows that $S(n)$ is a polynomial of degree two, we could use the points $(0,0)$, $(1,1)$, and $(2,3)$ (coming from the fact that $S(0) = 0$, $S(1) = 1$, and $S(2) = 3$) and use Lagrange Interpolation to find that

$$S(n) = 0 \cdot \frac{(n-1)(n-2)}{(1-0)(2-0)} + 1 \cdot \frac{(n-0)(n-2)}{(1-0)(1-2)} + 3 \cdot \frac{(n-0)(n-1)}{(2-0)(2-1)} = \frac{n(n+1)}{2}$$

OR

Let S denote the n-element set $\{1, 2, \ldots, n\}$. We count the number of ways to choose a two–element subset from S. First, we can choose the first element in n ways and the second element in $(n-1)$ ways. However, choosing i and then j produces the same two–element subset as choosing j then i. So the number of ways of choosing a two–element subset from S is $\frac{n(n-1)}{2}$.

Alternatively, suppose the larger of the two numbers chosen is i. Then for $i = 2, 3, \ldots, n$, there are $i - 1$ choices for the second number j. That is for $i = 2, 3, \ldots, n$, there are $1, 2, \cdots, n-1$ possible two–element subsets of S. Then in total there are $1 + 2 + \cdots + (n-1)$ total two–element subsets of S. But then $\sum_{i=1}^{n-1} i = 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}$.

OR

First, we prove Pascal's Identity: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. We count the number of ways to choose a k–element subset from the set $\{1, 2, \ldots, n+1\}$ in two different ways. Since

[33] This actually takes a bit more work to show. Let V be the space of all polynomials defined over $\mathbb{N} \cup \{0\}$ over a field $\mathbb{F}$ of characteristic 0. Define the forward difference operator $Dp(n) := p(n+1) - p(n)$. If $p(n)$ has degree $d+1$, then $Dp(n)$ has degree at most d. Let V_d denote the subspace of V consisting of polynomials of degree at most d. Then we have $\dim_{\mathbb{F}} V_d = d + 1$. Choosing the standard basis, observe that matrix for the forward difference operator is upper triangular and defines an operator $D : V_{d+1} \to V_d$. Then the result is clear.

they count the same thing, they must be equal. First, we do this 'directly'. The number of k–element subsets one can choose from this set is exactly $\binom{n+1}{k}$. Second, each k–element subset either contains $n+1$ or does not. The number of k–element subsets containing $n+1$ is $\binom{n}{k-1}$ while the number of k–element subsets not containing $n+1$ is $\binom{n}{k}$. But then the number of k–element subsets is $\binom{n}{k} + \binom{n}{k-1}$. Therefore, $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. We will need this identity for the starred equality below.

Now we show $\sum_{i=1}^{n} i = \binom{n+1}{2}$ using induction. The case where $n = 1$ is simple: $\sum_{i=1}^{1} i = 1$ and $\binom{2}{2} = 1$. Assume the result is true for $n = 1, 2, \ldots, k-1$. Then

$$\begin{aligned}\sum_{i=1}^{k} i &= k + \sum_{i=1}^{k-1} i \\ &= \binom{k}{1} + \binom{k}{2} \\ &\overset{*}{=} \binom{k+1}{2} \\ &= \frac{k(k+1)}{2}\end{aligned}$$

Then $\sum_{i=1}^{n} i = \binom{n+1}{2} = \frac{n(n+1)}{2}$ follows by induction.

OR

Consider the complete graph K_n. Label the vertices $v_1, v_2, \ldots, v_n$. Associate to vertex v_1 the $(n-1)$-edges connecting it to all the other vertices in K_n. Associate to vertex v_2 the $(n-2)$-edges connecting it to all the other vertices in K_n *except* for v_1. Continue this process for $v_3, v_4, \ldots, v_n$. Notice that for each i, the association for v_{i+1} contributes no *new* edges and this process never duplicates an edge. Let $|v_i|$ denote the number of edges associated with v_i. Then the number of edges in K_n is…

$$\text{\# of edges} = \sum_{i=1}^{n} |v_i| = |v_1| + |v_2| + \cdots + |v_{n-1}| + |v_n| = (n-1) + (n-2) + \cdots + 2 + 1$$

But then we have $\sum_{i=1}^{n} |v_i| = \sum_{i=1}^{n-1} i$. The result will follow if we can show that the number of edges, $\sum_{i=1}^{n} |v_i|$, is $\frac{n(n-1)}{2}$. But every edge in K_n connects two vertices. The number of edges must then be the number of ways one can select two vertices to connect. But this is precisely $\binom{n}{2} = \frac{n(n-1)}{2}$. Therefore, we have

$$\sum_{i=1}^{n-1} i = \sum_{i=1}^{n} |v_i| = \binom{n}{2} = \frac{n(n-1)}{2}$$

But this is exactly what was to be shown.

OR

We want to show that $1+2+\cdots+(n-1)=\frac{n(n-1)}{2}$. Represent the sum $1+2+\cdots+(n-1)$ as a triangular array of yellow circles. Place a row of n blue dots beneath this array to create larger a triangular array of dots. The case when $n=5$ is illustrated in Figure 3. Observe that if one chooses any two *distinct* blue dots, there is a unique

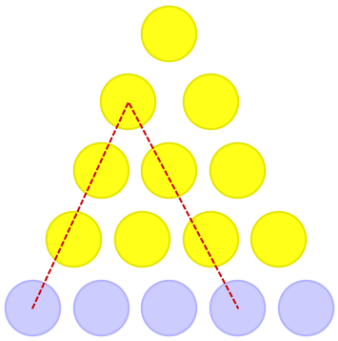


Figure 3: An illustration for the triangular array for $n=5$.

yellow dot in the upper portion of the triangular array 'associated' to the pair of dots as illustrated in Figure 3. Vise versa for each yellow dot, there is a unique pair of blue dots associated to it. That is, there is a one-to-one correspondence between yellow dots and pairs of blue dots. But then the number of yellow dots, $1+2+\cdots+(n-1)$, must be the same as the number of ways of choosing two distinct blue dots, $\binom{n}{2}$. Then we must have

$$\sum_{i=1}^{n-1} i = 1+2+\cdots+(n-1) = \binom{n}{2} = \frac{n(n-1)}{2}$$

But this was exactly what was to be shown.[34]

OR

Observe that $(i+1)^2-i^2=(i^2+2i+1)-i^2=2i+1$. The series

$$\begin{aligned}\sum_{i=1}^{n}(i+1)^2-i^2 &= (2^2-1^2)+(3^2-2^2)+(4^2-3^2)+\cdots+((n+1)^2-n^2)\\ &= -1^2+(n+1)^2\\ &= -1+(n^2+2n+1)\\ &= n^2+2n\end{aligned}$$

[34] L. Larson. A Discrete Look at $1+2+\cdots+n$. *College Mathematics Journal*, 16:369–382, 1985.

Take note also that $\sum_{i=1}^{n} 1 = n$. We also have...

$$\sum_{i=1}^{n}(2i+1) = \sum_{i=1}^{n} 2i + \sum_{i=1}^{n} 1 = 2\sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 = n + 2\sum_{i=1}^{n} i$$

so that $2\sum_{i=1}^{n} i = -n + \sum_{i=1}^{n}(2i+1)$. Putting these results together, we have...

$$\begin{aligned} 2\sum_{i=1}^{n} i &= -n + \sum_{i=1}^{n} 2i + 1 \\ &= -n + \sum_{i=1}^{n}(i+1)^2 - i^2 \\ &= -n + (n^2 + 2n) \\ &= n^2 + n \\ &= n(n+1) \end{aligned}$$

Therefore, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

OR

Consider the finite geometric series

$$1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$$

Differentiating both sides of the equality yields

$$\frac{d}{dr}\left(1 + r + r^2 + \cdots + r^n\right) = 1 + 2r + 3r^2 + \cdots + nr^{n-1}$$
$$\frac{d}{dr}\left(\frac{1 - r^{n+1}}{1 - r}\right) = \frac{-(1-r)(n+1)r^n - (-1)(1 - r^{n+1})}{(1-r)^2} = \frac{nr^{n+1} - (n+1)r^n + 1}{(1-r)^2}$$

We obtain the sum $1 + 2 + \cdots + n$ by taking the limit as r tends to 1:

$$\begin{aligned} \lim_{r\to 1} \frac{nr^{n+1} - (n+1)r^n + 1}{(1-r)^2} &\overset{\text{L.H.}}{=} \lim_{r\to 1} \frac{n(n+1)(r-1)r^{n-1}}{2(1-r)} \\ &\overset{\text{L.H.}}{=} -\lim_{r\to 1} \frac{n(n+1)(n(r-1)+1)r^{n-2}}{2} \\ &= \frac{n(n+1)}{2} \end{aligned}$$

where $\overset{\text{L.H.}}{=}$ denotes that the equality follows by application of l'Hôpital's Rule. But it then follows that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

(b) Note that

$$\left|b_n - \frac{\sum_{k=1}^n k}{n^2}L\right| = \left|\frac{1}{n^2}\sum_{k=1}^n ka_k - \frac{1}{n^2}\sum_{k=1}^n kL\right| \leq \frac{1}{n^2}\sum_{k=1}^n k|a_k - L|.$$

Moreover,

$$\left|b_n - \frac{\sum_{k=1}^n k}{n^2}L\right| = \left|b_n - \frac{\frac{n(n+1)}{2}}{n^2}L\right| = \left|b_n - \frac{n+1}{2n}L\right|.$$

Now since $a_n \to L$, given $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for $n > N$, $|a_n - L| < \epsilon$. Furthermore a_k is convergent, the sequence $\{a_k\}$ is bounded. But then so too is $\{|a_k - L|\}$ bounded. Suppose $|a_k - L| < M$ for all k. Now given $m \in \mathbb{N}$, there exists $P \in \mathbb{N}$ such that $\frac{4Mm(m+1)}{2P^2} = \frac{2Mm(m+1)}{P^2}$, i.e. $\frac{Mm(m+1)}{2P^2} < \frac{\epsilon}{4}$. Notice also that for $n \geq 2$, $1 + \frac{1}{n} \leq 1 + \frac{1}{2} = \frac{3}{2}$.

We are now in a position to prove $\lim_{n\to\infty} b_n = L/2$. Let $\epsilon > 0$ be given. As above, find $N \in \mathbb{N}$ so $n > N$, $|a_n - L| < \epsilon$. Find as above $P \in \mathbb{N}$ so that $\frac{MN(N+1)}{2P^2} < \frac{\epsilon}{4}$. Let $M = \max\{2, N, P\}$. Then for $n > M$, we have

$$\begin{aligned}
\left|b_n - \frac{\sum_{k=1}^n k}{n^2}L\right| &= \left|b_n - \frac{n+1}{2n}L\right| \\
&\leq \frac{1}{n^2}\sum_{k=1}^n k|a_k - L| \\
&= \frac{1}{n^2}\sum_{k=1}^{N-1} k|a_k - L| + \frac{1}{n^2}\sum_{k=N}^n k|a_k - L| \\
&< \frac{1}{n^2}\sum_{k=1}^{N-1} kM + \frac{1}{n^2}\sum_{k=N}^n k\epsilon \\
&= \frac{M}{n^2}\sum_{k=1}^{N-1} k + \frac{\epsilon}{n^2}\sum_{k=N}^n k \\
&< \frac{M}{n^2}\sum_{k=1}^{N} k + \frac{\epsilon}{n^2}\sum_{k=1}^n k \\
&= \frac{M}{n^2}\cdot\frac{N(N+1)}{2} + \frac{\epsilon}{n^2}\cdot\frac{n(n+1)}{2} \\
&= \frac{MN(N+1)}{2n^2} + \frac{n+1}{n}\cdot\frac{\epsilon}{2} \\
&= \frac{MN(N+1)}{2n^2} + \left(1 + \frac{1}{n}\right)\cdot\frac{\epsilon}{2} \\
&< \frac{\epsilon}{4} + \frac{3}{2}\cdot\frac{\epsilon}{2} = \epsilon
\end{aligned}$$

Therefore, $b_n \to L/2$.

□

3. Let f be a continuous real valued function on $[a,b]$ and differentiable on (a,b). Prove

$$\max_{a\le x\le b} |f(x)| \le \frac{1}{b-a}\int_a^b |f(x)|\,dx + (b-a)\sup_{a<x<b}|f'(x)|$$

Solution: Since f is continuous on $[a,b]$, f is integrable so that the Mean Value Theorem for Integrals applies. Then there exists $\xi \in (a,b)$ so that

$$f(\xi) = \frac{1}{b-a}\int_a^b f(x)\,dx.$$

But then we must have

$$|f(\xi)| = \left|\frac{1}{b-a}\int_a^b f(x)\,dx\right| \le \frac{1}{b-a}\int_a^b |f(x)|\,dx.$$

Let $|f(y)| = \max_{a\le x\le b}|f(x)|$. But then for some $c \in (\xi, y)$

$$\begin{aligned} |f(y)| - |f(\xi)| &\le |f(y) - f(\xi)| \\ &= |f'(c)|\,|y-\xi| \\ &\le |f'(c)|\,|b-a| \\ &\le (b-a)\sup_{a<x<b}|f'(x)| \end{aligned}$$

Therefore, we have

$$\begin{aligned} |f(y)| &\le |f(\xi)| + (b-a)\sup_{a<x<b}|f'(x)| \\ &= \frac{1}{b-a}\int_a^b |f(x)|\,dx + (b-a)\sup_{a<x<b}|f'(x)| \end{aligned}$$

Therefore, $\max_{a\le x\le b}|f(x)| \le \frac{1}{b-a}\int_a^b |f(x)|\,dx + (b-a)\sup_{a<x<b}|f'(x)|$. □

4. Suppose $f(x+1) = f(x)$ for all real x, f is real valued, f is Riemann integrable on every compact interval, and $\int_0^1 f(x)\,dx = 0$.

(a) Prove there exists x_0 such that $F(x) = \int_{x_0}^x f(t)\,dt \ge 0$ for all x.

(b) Show by example that $F'(x_0) = 0$ need not be true.

Solution:

(a) Note that since $\int_0^1 f(x)\,dx = 0$, that $\int_0^x f(t)\,dt + \int_x^1 f(t)\,dt = 0$. This implies

$$\int_0^x f(t)\,dt = -\int_x^1 f(t)\,dt$$

for all $x \in \mathbb{R}$. But

$$\int_0^1 f(t)\,dt = \int_0^1 f(t+1)\,dt = \int_1^2 f(t)\,dt = \cdots$$

so that $\int_{\lfloor x \rfloor}^{\lfloor x \rfloor + 1} f(t)\,dt = \int_0^1 f(t)\,dt = 0$ for all $x \in \mathbb{R}$. Then for all $y \in \mathbb{R}$, there exists $x \in [0,1]$ such that

$$\int_{\lfloor y \rfloor}^{y} f(t)\,dt = \int_0^x f(t)\,dt$$
$$\int_{y}^{\lfloor y \rfloor + 1} f(t)\,dt = \int_x^1 f(t)\,dt$$

Define $G(x) : [0,1] \to \mathbb{R}$ by $G(x) = \int_0^x f(t)\,dt$. Note taht G is well-defined since $f \in \mathcal{R}$ and that G is continuous by the Fundamental Theorem of Calculus.

Since G is continuous on $[0,1]$, there exists $x_0 \in [0,1]$ such that $G(x) \geq G(x_0)$ for all $x \in [0,1]$. Let $y \in \mathbb{R}$ and let $F(x) = \int_{x_0}^x f(t)\,dt$. If $y < 0$, then

$$\begin{aligned}
F(y) &= \int_{x_0}^{y} f(t)\,dt \\
&= -\int_{y}^{x_0} f(t)\,dt \\
&= -\left[\int_{y}^{\lfloor y \rfloor + 1} f(t)\,dt + \int_{\lfloor y \rfloor + 1}^{\lfloor y \rfloor + 2} f(t)\,dt + \cdots + \int_0^{x_0} f(t)\,dt\right] \\
&= -\left[\int_{y}^{\lfloor y \rfloor + 1} f(t)\,dt + \int_0^{x_0} f(t)\,dt\right] \\
&= -\left[\int_x^1 f(t)\,dt + \int_0^{x_0} f(t)\,dt\right] \\
&= -\left[\int_0^{x_0} f(t)\,dt - \int_0^x f(t)\,dt\right] \\
&= -(G(x_0) - G(x)) \\
&= G(x) - G(x_0) \geq 0
\end{aligned}$$

This shows that $F(y) \geq 0$ for all $y < 0$. If $y \geq 0$, we have

$$\begin{aligned} F(y) &= \int_{x_0}^{y} f(t)\, dt \\ &= \int_{x_0}^{1} f(t)\, dt + \int_{1}^{2} f(t)\, dt + \cdots + \int_{\lfloor y \rfloor}^{y} f(t)\, dt \\ &= \int_{x_0}^{1} f(t)\, dt + \int_{\lfloor y \rfloor}^{y} f(t)\, dt \\ &= \int_{x_0}^{1} f(t)\, dt + \int_{0}^{x} f(t)\, dt \\ &= \int_{0}^{x} f(t)\, dt - \int_{0}^{x_0} f(t)\, dt \\ &= G(x) - G(x_0) \geq 0 \end{aligned}$$

This shows that $F(y) \geq 0$ for all $y \geq 0$. But then we must have $F(y) \geq 0$ for all $y \in \mathbb{R}$.

(b) Let $f : \mathbb{R} \to \mathbb{R}$ be given by

$$f(x) = \begin{cases} -1, & x \in [0, 1/4] \\ 1, & x \in (1/4, 3/4] \\ -1, & x \in (3/4, 1] \end{cases}$$

Extend $f(x)$ to $\mathbb{R}$ as follows: for $x \in \mathbb{R}$, let $n \in \mathbb{Z}$ be the largest element of $\mathbb{Z}$ such that $n \leq x$. Then $x - n \in [0, 1)$. Define $f(x) := f(x - n)$. By construction, it is clear that $f(x + 1) = f(x)$ for all $x \in \mathbb{R}$. On any compact interval $f(x)$ is bounded (since it is bounded on $[0, 1]$) and has only finitely many discontinuities. Therefore, $f \in \mathcal{R}$ and $\int_0^1 f(x)\, dx = 1$. Then $G(x) = \int_0^x f(t)\, dt$ has a minimum at $x_0 = \frac{1}{4}$. Now $F(x) = \int_{1/4}^{x} f(t)\, dt \geq 0$ for all $x \geq 1/4$. But $F'(1/4) \neq 0$ because F is not differentiable at $1/4$ since f is not continuous there.

□

5. Let $f_n(x) = n(e^{x^2/n} - 1)$ for all real x.

(a) Prove $\lim_{n\to\infty} f_n(x) = x^2$ for each x.

(b) Prove $\{f_n\}$ is equicontinuous on $[0, M]$ for all positive M.

(c) Prove that $\lim_{n\to\infty} \int_0^1 (f_n(x))^{1/3}\, dx$ exists and equals $\frac{3}{5}$.

Solution:

(a) Using l'Hôpital's Rule (with $\frac{0}{0}$), we have

$$\lim_{n\to\infty} f_n(x) = \lim_{n\to\infty} n(e^{x^2/n} - 1) = \lim_{n\to\infty} \frac{e^{x^2/n} - 1}{\frac{1}{n}} \overset{\text{L.H.}}{=} \lim_{n\to\infty} \frac{-\frac{x^2}{n^2} e^{\frac{x^2}{n^2}}}{-\frac{1}{n^2}} = \lim_{n\to\infty} x^2 e^{\frac{x^2}{n^2}} = x^2$$

Therefore for all $x \in \mathbb{R}$, we have $\lim_{n\to\infty} f_n(x) = x^2$.

(b) Observe $[0,1]$ is a compact metric space and $f_n'(x) = 2xe^{\frac{x^2}{n}}$. Clearly, $f_n'(x)$ is continuous for all x and $f_n'(x) = 0$ if and only if $x = 0$ for all n. [In fact, f_n' converges uniformly to $f' = 2x$ on $[0, M]$, giving another approach to the proof of equicontinuity below.] Now $f_n'(x) > 0$ on the interval $[0, M]$ for all n. Each f_n is continuous on $[0,1]$, monotone (increasing) on the compact metric space $[0, M]$, and $f_n(x)$ converges pointwise to $f(x) := x^2$ for all $x \in [0, M]$. Finally, observe $f_n(0) = 0$ for all n and $f_n'(x) = 2xe^{x^2/n}$ so that

$$f_{n+1}'(x) = 2xe^{x^2/(n+1)} \leq 2xe^{x^2/n} = f_n'(x)$$

for $x \in [0, M]$ and all n. Therefore, $f_{n+1}(x) \leq f_n(x)$ for all $x \in [0,1]$ and $n \in \mathbb{N}$. Therefore by Dini's Theorem, $f_n \to f$ uniformly on $[0, M]$.[35] Now $[0,1]$ is a compact metric space, $f_n \in C([0,1])$ for all n, and $\{f_n\}$ converges pointwise to f on $[0,1]$ by (a). Therefore, $\{f_n\}$ is equicontinuous on $[0,1]$.

(c) By the work in (a) and (b), $f_n \to f$ uniformly on $[0,1]$. Since $f, f_n \in \mathcal{R}([0,1])$, using the continuity of $\sqrt[3]{x}$ and uniform convergence, we have

$$\begin{aligned}
\lim_{n\to\infty} \int_0^1 (f_n(x))^{1/3}\, dx &= \int_0^1 \lim_{n\to\infty} (f_n(x))^{1/3}\, dx \\
&= \int_0^1 (\lim_{n\to\infty} f_n(x))^{1/3}\, dx \\
&= \int_0^1 (x^2)^{1/3}\, dx \\
&= \int_0^1 x^{2/3}\, dx = \frac{x^{5/3}}{5/3}\Big|_0^1 = \frac{3}{5}
\end{aligned}$$

□

[35] Dini's Theorem: if X is a compact metric space, $\{f_n\}$ is a monotone sequence of continuous functions on X which converges pointwise to a continuous function f, then the convergence is uniform. *Proof.* Let $\epsilon > 0$ and define $g_n = f - f_n$. Without loss of generality, assume $\{f_n\}$ is monotone increasing, i.e. $f_n(x) \leq f_{n+1}(x)$. Let $E_n = \{x \in X : g_n(x) < \epsilon\}$. Each g_n is continuous and hence E_n is open (E_n is the preimage of an open set under g_n). Since $\{f_n\}$ is monotone increasing, $\{g_n\}$ is monotone decreasing, we have $E_n \subseteq E_{n+1}$ for all n. Since f_n converges pointwise to f, $\{E_n\}$ is an open covering of X. By compactness, there is a finite subcovering $\{E_n\}_{n=1,\ldots,N}$. But as $E_n \subseteq E_{n+1}$, we must have $E_N = X$. Then if $n > N$ and $x \in X$, then $|f_n(x) - f(x)| < \epsilon$.

6. The map $(x, y) \mapsto (e^x \sin x - x^2 y, y \cos x - e^x + 1)$ maps the *origin* to the *origin*. Show that the inverse map G exists in a neighborhood of the *origin* and compute

$$\frac{d}{dt}\bigg|_{t=0} f \circ G(-t, t^2) \quad \text{and} \quad \frac{d}{dt}\bigg|_{t=0} f \circ G(-t, t)$$

when $f(x, y) = x + 2y$.

Solution: Let $F(x, y) = (f_1, f_2)$, where $f_1(x, y) = e^x \sin x - x^2 y$ and $f_2(x, y) = y \cos x - e^x + 1$. Now

$$J_f(0,0) = \begin{vmatrix} e^x \cos x + e^x \sin x - 2xy & -x^2 \\ -y \sin x - e^x & \cos x \end{vmatrix}\bigg|_{(0,0)} = \begin{vmatrix} 1 & 0 \\ -1 & 1 \end{vmatrix} = 1$$

Therefore, the Inverse Function Theorem applies to $F(x, y)$ at $(0, 0)$. Then $G := F^{-1}$ exists in a neighborhood of $(0, 0)$. Now

$$DG = DF^{-1} = \frac{1}{J_f(x, y)} \begin{pmatrix} \cos x & x^2 \\ 4 \sin x + e^x & e^x \cos x + e^x \sin x - 2xy \end{pmatrix}$$

Let $g : \mathbb{R} \to \mathbb{R}^2$ be given by $g(t) = (-t, t^2)$. So $g'(t) = \begin{pmatrix} -1 \\ 2t \end{pmatrix}$. Therefore, $f \circ G(-t, t^2) = f \circ G \circ g$. Note that

$$f'(G(g(0))) = f'(G(0,0)) = f'(0,0) = \begin{pmatrix} 1 & 2 \end{pmatrix}\bigg|_{(0,0)} = \begin{pmatrix} 1 & 2 \end{pmatrix}$$

Furthermore, $G'(g(0)) = G'(0,0) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $g'(0) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$. Finally,

$$\frac{d}{dt}\left(f \circ G \circ g\right)\bigg|_{t=0} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 0 \end{pmatrix} = -3.$$

Now let $g : \mathbb{R} \to \mathbb{R}^2$ be given by $g(t) = (-t, t)$ so that $g'(t) = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Then as above, using the fact that $g'(t) = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$,

$$\frac{d}{dt}\left(f \circ G \circ g\right)\bigg|_{t=0} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = -1.$$

□

August 2009

1. If F_1 and F_2 are closed subsets of R^1 and $\text{dist}(F_1, F_2) = 0$ then $F_1 \cap F_2 \neq \emptyset$. Prove or give a counterexample.[36]

Solution: Let $F_1 = \mathbb{N}$ and $F_2 = \{n + \frac{1}{n} : n \in \mathbb{N}\}$. We have $F_1^C = \cup_{n=1}^{\infty} B_{1/2}(n/2)$ is open since each $B_{1/2}(n/2)$ is open. Therefore, F_1 is open. We know also

$$F_2^C = \bigcup_{n=1}^{\infty} B_d\left(\frac{n + \frac{1}{2n} + n + 1 + \frac{1}{2(n+1)}}{2}\right),$$

where $d = \frac{\text{lcm}(2n,2n+2)-1}{\text{lcm}(2n,2n+2)}$. This is clearly open being the union of open sets. Therefore, F_2 is closed. Now

$$\text{dist}(F_1, F_2) = \inf\{d(f_1, f_2) : f_1 \in F_1, f_2 \in F_2\} = \inf\left\{\frac{1}{2n} : n \in \mathbb{N}\right\} = 0$$

Therefore, $\text{dist}(F_1, F_2) = 0$. However, $F_1 \cap F_2 = \emptyset$. □

2. Newton's method for finding zeroes of a function $f : R^1 \to R^1$ is based on the recursion formula

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \quad n \geq 1.$$

Show that if $f \in C^1$, $f(a) = 0$ and $f'(a) \neq 0$, then there exists a $\delta > 0$ such that if $|x_1 - a| < \delta$ then $x_n \to a$. (Suggestion: Use the Mean Value Theorem.)

Solution:
3. Let $f : [0, \infty) \to [0, \infty)$ and for $h > 0$ and $k \geq 1$ set

$$M_k(h) = \sup_{(k-1)h \leq x < kh} f(x), \quad m_k(h) = \inf_{(k-1)h \leq x < kh} f(x).$$

Let

$$U(h) = \sum_{k=1}^{\infty} M_k(h)\, h, \quad L(h) = \sum_{k=1}^{\infty} m_k(h) h.$$

We say that f is *directly Riemann integrable* if $U(h) < \infty$ for all $h > 0$ and

$$\lim_{h \downarrow 0} (U(h) - L(h)) = 0.$$

[36] The statement is true if one of F_1, F_2 is compact. To shows this, use contradiction. We know there are sequences x_n, y_n so that $d(x_n, y_n) \to 0$ (using the fact that $d(F_1, F_2) = 0$. But then $x_n \to x \in F_1$. Use the triangle inequality to show that $d(x, F_2) = 0$ so $x \in F_2$ and $x \in F_1$.

Recall f is *improperly Riemann integrable on* $[0,\infty)$ if f is Riemann integrable on $[0,a]$ for every $a > 0$, and

$$\lim_{a\to\infty}\int_0^a f(t)\,dt < \infty$$

(a) Show that if f is continuous and nonincreasing, then f is directly Riemann integrable whenever f is improperly Riemann integral on $[0,\infty)$.[37]

(b) Give an example of a continuous function f which is improperly Riemann integrable on $[0,\infty)$ but not directly Riemann integrable.

Solution:

(a) If f is improperly Riemann integrable, then given $\epsilon > 0$, there is an $A > 0$ such that $\lim_{a\to\infty}\int_A^a f(t)\,dt < \frac{\epsilon}{2}$. Now partition $[0,A]$ into intervals $[x_{i-1},x_i]$ for $i = 1,\dots,n$. Since f is nonincreasing, $M_i = f(x_{i-1})$ and $m_i = f(x_i)$ for each i. Furthermore since f is continuous, there exists $\delta_1 > 0$ such that for $|x_i - x_{i-1}| < \delta_1$, we have $|f(x_i) - f(x_{i-1})| < \epsilon$. Let $\delta = \min\{\delta_1, 1/(2A)\}$. Then for $|x_i - x_{i-1}| < \delta$,

$$\begin{aligned}
\sum_{i=1}^{\infty}(M_i - m_i)\Delta x_i &< \sum_{i=1}^{n}(M_i - m_i)\Delta x_i + \frac{\epsilon}{2}\\
&= \sum_{i=1}^{n}(f(x_{i-1}) - f(x_i))\Delta x_i + \frac{\epsilon}{2}\\
&< \sum_{i=1}^{n}(f(x_{i-1}) - f(x_i))\delta + \frac{\epsilon}{2}\\
&< \sum_{i=1}^{n}(f(x_{i-1} - f(x_i))\frac{1}{2A} + \frac{\epsilon}{2}\\
&= \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon
\end{aligned}$$

Therefore, $\lim_{h\to 0}(U(h) - L(h)) = 0$ so that f is directly integrable.

(b) Let $f(x)$ be the function given by

$$f(x) = \begin{cases} \sum_{n=1}^{\infty} 1, & x \in \left[n - \frac{1}{2n^2}, n + \frac{1}{2n^2}\right] \\ 0, \text{ otherwise} \end{cases}$$

[37] This notion appears in Renewal Theory.

4. Suppose $f : [0, \infty) \to [0, \infty)$ is such that for any sequence a_n of nonnegative terms we have

$$\sum_{n=1}^{\infty} a_n < \infty \longrightarrow \sum_{n=1}^{\infty} f(a_n) < \infty$$

Prove that

$$\limsup_{x \to 0+} \frac{f(x)}{x} < \infty$$

Solution: Suppose $\lim\limits_{x \to 0^+} \sup \frac{f(x)}{x} = \infty$, then $\lim\limits_{\delta \to 0} \left(\sup\limits_{0 < x < \delta} \frac{f(x)}{x} \right) = \infty$. Therefore for all $n \in \mathbb{N}$, there exists $x_n < \frac{1}{n^2}$ such that $\frac{f(x_n)}{x_n} > n$. But then $f(x_n) > nx_n$, implying that $f(x_n) > n \cdot \frac{1}{n^2} = \frac{1}{n}$. But as $\sum \frac{1}{n}$ diverges, by the Comparison Test $\sum f(x_n)$ diverges. But this contradicts the fact taht $\sum x_n < \sum \frac{1}{n^2}$, since $\sum \frac{1}{n^2}$ converges. Therefore, $\lim\limits_{x \to 0^+} \sup \frac{f(x)}{x} < \infty$. □

5. Let f be continuous real valued function defined on the unit square and for each $0 \leq x \leq 1$ let f_x be function on the unit interval defined by $f_x(y) = f(x, y)$. Prove that for any sequence x_n in $[0, 1]$ there is a subsequence n_k such that $f_{x_{n_k}}$ converges uniformly on $[0, 1]$.

Solution: Note that f is continuous on the set $[0, 1] \times [0, 1]$, which is compact, so that f is bounded. But then it must be that $\{f(x_n)\}$ is pointwise bounded. Let $\epsilon > 0$ be given. Since f is continuous, there exists $\delta_x > 0$ such that for $|y_1 - y_2| < \delta_x$, we have $|f(x, y_1) - f(x, y_2)| < \epsilon$. Choose $\delta = \min_n\{\delta_{x_n}\}$. [Note only finitely many are required since $[0, 1]$ is compact.] Then

$$|y_1 - y_2| < \delta \Rightarrow |f_{x_n}(y_1) - f_{x_n}(y_2)| = f(x_n, y_1) - f(x_n, y_2)| < \epsilon$$

for all $n \in \mathbb{N}$. But then $\{f_{x_n}\}$ is equicontinuous. But since $[0, 1]$ is compact, by the Arzelá-Ascoli Theorem, there exists a uniformly convergent subsequence of $\{f_{x_n}\}$. □

6. If c is a real parameter prove that $x^7 + x + c = 0$ has a unique real root and that this root is a differentiable function of c.

Solution: The function $x^7 + x + c$ is odd so it has at least one real root by the Intermediate Value Theorem. Note also that $\frac{d}{dx}(x^7 + x + c) = 7x^6 + 1 > 0$, implying $x^7 + x + c$ is increasing. But then this root must be unique. Define

$$F(x) = [\underbrace{x}_{A}, \quad \underbrace{x^7 + x + c}_{B}]$$

We have $\det A = 1 > 0, \det B = 7x^6 + 1 > 0$ so that $\det A, \det B$ are invertible. Therefore by the Implicit Function Theorem, we can solve for x in terms of c, i.e. we can find $g \in C^1$ with $F = [g(c), c]$. Therefore, $x^7 + x + c$ has a unique real root which is a differentiable function of c. $\square$

January 2010

1. Let X be a connected metric space. Given two points $p, q \in X$ and a number $\epsilon > 0$, prove that there exist an integer $n \geq 0$ and points $a_0, a_1, \ldots, a_n \in X$ such that $a_0 = p$, $a_n = q$, and

$$d(a_j, a_{j-1}) < \epsilon \quad \text{for all } j = 1, 2, \ldots, n.$$

Solution: Since X is a connected metric space, the only set which is both open and closed in X is X itself. Let $C_{a,\epsilon}$ denote the set of elements $x \in X$ such that there is an $n \in \mathbb{N} \cup \{0\}$ and a sequence $\{p_n\}$ such that $p_0 = a$, $p_n = x$, and $d(p_i, p_{i-1}) < \epsilon$ for $i = 1, 2, \ldots, n$. Let $\epsilon > 0$ be given and choose $a \in X$. We show that $C_{a,\epsilon}$ is nonempty: $a \in C_{a,\epsilon}$ as choosing $n = 1$ and $p_0 = a$ and $p_1 = a$ certainly satisfies the condition. We need only show that $C_{a,\epsilon}$ is clopen so that $X = C_{a,\epsilon}$.

To see that $C_{a,\epsilon}$ is open, we need find a $\epsilon' > 0$ such that $B(t, \epsilon') \subset C_{a,\epsilon}$. In fact, we show that the same ϵ as assumed above suffices. That is for any $y \in B(t, \epsilon)$, we need show that $y \in C_{a,\epsilon}$. As $t \in C_{a,\epsilon}$, there is a sequence $\{p_n\}$ such that $p_0 = a$, $p_n = t$, and $d(p_i, p_{i-1}) < \epsilon$ for $i = 1, 2, \cdots, n$. But then the sequence $\{a, p_1, p_2, \ldots, p_n = t, y\}$ is a sequence meeting the condition so that $y \in C_{a,\epsilon}$. Therefore, $C_{a,\epsilon}$ is open.

To see that $C_{a,\epsilon}$ is closed, let t be a limit point of $C_{a,\epsilon}$. Then for each $\epsilon > 0$, there is a $c \in C_{a,\epsilon}$ such that $d(c, t) < \epsilon$. As $c \in C_{a,\epsilon}$, there is a sequence $\{p_n\}$ such that $p_0 = a$, $p_n = c$, and $d(p_i, p_{i-1}) < \epsilon$ for $i = 1, 2, \cdots, n$. Then it is immediate that the sequence $\{a, p_1, p_2, \ldots, p_n = c, t\}$ is a sequence "connecting" a and t satisfying the condition. This shows that $t \in C_{a,\epsilon}$.

Therefore, $C_{a,\epsilon}$ is clopen so that $C_{a,\epsilon} = X$. This holds for all $a \in X$ so there is a path satisfying the condition of problem statement for any two points $x, y \in X$. □

2. Suppose that $f : (0, 1] \to \mathbb{R}$ is a bounded continuous function such that for every $t \in \mathbb{R}$ the set $\{x \in (0, 1] : f(x) = t\}$ is finite. Prove that f is uniformly continuous on $(0, 1]$.

Solution: We show that $\lim_{x \searrow 0} f(x) = l < \infty$ for some l. Suppose that $\lim_{x \searrow 0} f(x)$ does not exist. Since f is bounded, there exist sequences $\{x_n\}, \{y_n\}$, tending to 0, such that $f(x_n) \to \alpha$ and $f(y_n) \to \beta$ with $\alpha \neq \beta$. Without loss of generality, assume that $\alpha < \beta$. There exists $\epsilon > 0$ such that $|f(y_n) - \alpha| \geq \epsilon$ as $y_n \to 0$. Since between any two real numbers, there is another real number, we know there is a t such that $\alpha < t < \beta$. So there is a $N \in \mathbb{N}$ such that for $n > N$, $f(x_n) < t < f(y_n)$. By the Intermediate Value Theorem, for each $n \geq N$, there exists w_n such that $f(w_n) = t$. Using this, define a sequence $\{w_n\}$ such that $f(w_i) = t$. But this is a contradiction since $\{x \in (0, 1] : f(x) = t\}$ is finite. Then $\lim_{x \searrow 0} f(x) = l < \infty$ for some l. Define

$$g(x) = \begin{cases} f(x), & x \in (0, 1] \\ l, & x = 0 \end{cases}$$

By the work above, $g(x)$ is continuous on $[0,1]$. However as $g(x)$ is continuous on the compact set $[0,1]$, it must be that $g(x)$ is uniformly continuous. But then $f(x)$ is uniformly continuous on $(0,1]$. $\square$

3. Prove or disprove the following: if a function $f : (-1,1) \to \mathbb{R}$ is differentiable on $(-1,1)$ and $f'(0) = 0$, then for every $\delta > 0$ there exists $\epsilon > 0$ such that

$$\left|\frac{f(t) - f(s)}{t - s}\right| < \delta \quad \text{whenever } -\epsilon < s < t < \epsilon.$$

Solution: Define

$$f(x) = \begin{cases} x^2 \sin\left(\dfrac{1}{x}\right), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

We have

$$f'(0) := \lim_{x\to 0} \frac{f(x) - f(0)}{x - 0} = \lim_{x\to 0} \frac{x^2 \sin(1/x)}{x} = \lim_{x\to 0} x \cdot \frac{\sin x}{x} = 0 \cdot 1 = 0$$

[For the last limit, either use the fact that $\lim_{x\to 0} \frac{\sin x}{x} = 1$ and $\lim_{x\to 0} x = 0$, or prove directly using the Squeeze Theorem: since $|\sin x| \leq 1$, $-x \leq x \sin(1/x) \leq x$ which gives

$$\lim_{x\to 0}(-x) \leq \lim_{x\to 0} x \sin(1/x) \leq \lim_{x\to 0} x$$

which gives the required limit.]

This shows $f'(0) = 0$. For nonzero x, we can compute this directly. Putting this together gives

$$f'(x) = \begin{cases} 2x \sin\left(\dfrac{1}{x}\right) - \cos\left(\dfrac{1}{x}\right), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Then f is differentiable and $f'(0) = 0$.

Now define $\delta = 1/2$, $t_n = \dfrac{1}{2\pi n + \frac{1}{n}}$, and $s_n = \dfrac{1}{2\pi n}$. We then have

$$\left|\frac{f(t)-f(s)}{t-s}\right| = \left|\frac{\left(\frac{1}{2\pi n+\frac{1}{n}}\right)^2 \sin\left(2\pi n+\frac{1}{n}\right) - \left(\frac{1}{2\pi n}\right)^2 \sin(2\pi n)}{\frac{1}{2\pi n+\frac{1}{n}} - \frac{1}{2\pi n}}\right|$$

$$= \left|\frac{\sin\left(\frac{1}{n}\right)}{\left(2\pi n+\frac{1}{n}\right)^2 \cdot \frac{\frac{-1}{n}}{\left(2\pi n+\frac{1}{n}\right)2\pi n}}\right|$$

$$= \left|\frac{\sin\left(\frac{1}{n}\right)}{\frac{1}{n}} \cdot \frac{2\pi n}{2\pi n+\frac{1}{n}}\right| = \left|\frac{\sin(1/n)}{1/n} \cdot \frac{2\pi n^2}{2\pi n^2+1}\right|$$

which converges to 1 as n tends to infinity. [The left limit is equivalent to $\lim_{x\to 0}\frac{\sin x}{x} = 1$ and the right limit is a rational function in n whose limit as $n \to \infty$ is obvious.] But then for large enough n, $-\epsilon < s < t < \epsilon$, but $\left|\dfrac{f(t)-f(s)}{t-s}\right| > \delta = 1/2$. □

4. Let f be a bounded real-valued function on $[a,b]$ with a discontinuity at $c \in (a,b)$. Let $\alpha(x)$ be monotonically increasing on $[a,b]$ with $\alpha(c-) < \alpha(c) < \alpha(c+)$. Prove that f is not Riemann-Stieltjes integrable with respect to α on $[a,b]$.

Solution: Suppose $f \in R(\alpha)$. Then given $\epsilon > 0$, there exists a partition $\mathcal{P}$ such that $U(\mathcal{P},f,\alpha) - L(\mathcal{P},f,\alpha) < \epsilon$. Let $\mathcal{P}^* = \mathcal{P} \cup \{c\}$, a refinement of $\mathcal{P}$ by adding the value c. Since this is a refinement, $U(\mathcal{P}^*,f,\alpha) - L(\mathcal{P}^*,f,\alpha) < \epsilon$. Since f is discontinuous at c, choose $\epsilon_f > 0$ such that for all $\delta_f > 0$, there is a x_f such that $|x_f - c| < \delta_F$ but $|f(x_f) - f(c)| \geq \sqrt{\epsilon_f}$. As $\alpha(c-) < \alpha(c) < \alpha(c+)$, we know α is discontinuous at c. Using discontinuity again, choose $\epsilon_\alpha > 0$ such that for all $\delta_\alpha > 0$, there is x_α such that $|x_\alpha - c| < \delta_\alpha$ but $|\alpha(x_\alpha) - \alpha(c)| \geq \sqrt{\epsilon_\alpha}$. Since $a < c < b$, there exist $k \in \{1,2,\ldots,n\}$ such that $x_{k-1} < c < x_k$. Choose $\epsilon = \min\{\epsilon_f, \epsilon_\alpha\}$. Then for $\delta^* = \min\{x_n - c, c - x_{n-1}\}$, there exists x^* such that $|x^* - c| < \delta^*$ and so $|f(x^*) - f(c)| \geq \sqrt{\epsilon}$ and $|\alpha(x^*) - \alpha(c)| \geq \sqrt{\epsilon}$. Therefore,

$$U(\mathcal{P}^*,f,\alpha) - L(\mathcal{P}^*,f,\alpha) = \sum_{i=1}^{n}(M_i - m_i)\Delta\alpha_i \geq M_k\Delta\alpha_k - m_k\Delta\alpha_k = (M_k - m_k)\Delta\alpha_k \geq \sqrt{\epsilon}\,\sqrt{\epsilon} = \epsilon,$$

a contradiction. Therefore, $f \notin \mathcal{R}(\alpha)$ on $[a,b]$. □

5. Give examples of sequences of functions $\{f_n\}$ and $\{g_n\}$ on $\mathbb{R}$ such that $\{f_n\}$ converges uniformly, $\{g_n\}$ converges uniformly but $\{f_n g_n\}$ does not converge uniformly on $\mathbb{R}$.

Solution: Let $f_n(x) = g_n(x) = x + \frac{1}{n}$. Clearly, $\{f_n(x)\}$ converges uniformly to the function $f(x) = x$: given $\epsilon > 0$, choose $N > 1/\epsilon$ and then for $n \geq N$,

$$|f_n(x) - f(x)| = \frac{1}{n} < \epsilon$$

for all $x \in \mathbb{R}$. Then $\{g_n(x)\}$ converges uniformly to $g(x) = x$ as well. Now $\{f_n g_n\} = \{(x + 1/n)^2\}$. If this were to converge uniformly, it must necessarily converge to $f(x)g(x) = x^2$. But take $\epsilon = 1$ and $x = n$. Then

$$|f_n(x)g_n(x) - f(x)g(x)| = \left| x^2 + \frac{2x}{n} + \frac{1}{n^2} - x^2 \right| = \left| \frac{2n^2 + 1}{n^2} \right| > 1,$$

so that $\{f_n g_n\}$ cannot converge uniformly to fg. □

6. Let $\phi, \psi : \mathbb{R}^3 \to \mathbb{R}$ be continuously differentiable functions and define $F : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$F(x, y, z) = (\phi(x, y, z), \psi(x, y, z), \phi^2(x, y, z) + \psi^2(x, y, z))$$

(a) Check whether or not the Inverse Function Theorem applies to F at any point (x_0, y_0, z_0), i.e., check if F satisfies the hypothesis of the Inverse Function Theorem at any point (x_0, y_0, z_0).

(b) Suppose that $F(\vec{a}) = \vec{b}$ for some points $\vec{a}, \vec{b} \in \mathbb{R}^3$. Explain geometrically why F does not have an inverse function from an open set $V \subset \mathbb{R}^3$ containing $\vec{b}$ to an open set $U \subset \mathbb{R}^3$ containing $\vec{a}$.

Solution:

(a) Cleary, $F \in C^1(\mathbb{R}^3)$ since ϕ, ψ are continuously differentiable. We have

$$\begin{aligned} J_F(x, y, z) &= \det \begin{pmatrix} \phi_x & \phi_y & \phi_z \\ \psi_x & \psi_y & \psi_z \\ 2(\phi\phi_x + \psi\psi_x) & 2(\phi\phi_y + \psi\psi_y) & 2(\phi\phi_z + \psi\psi_z) \end{pmatrix} \\ &= 2\phi_x\psi_y\phi\phi_z + 2\phi\psi_y\psi\psi_z + 2\phi_y\psi_z\phi\phi_x + 2\phi_y\psi_z\psi\psi_x + 2\phi_z\psi_x\phi\phi_y \\ &\quad + 2\phi_z\psi_x\psi\psi_y - 2\phi_z\psi_y\phi\phi_x - 2\phi_z\phi_y\psi\psi_x - 2\phi_x\psi_z\phi\phi_y \\ &\quad - 2\phi_x\psi_z\psi\psi_y - 2\phi_Y\psi_x\phi\phi_z - 2\phi_y\psi_x\psi\psi_z \\ &= 0 \end{aligned}$$

Then $J_F(x, y, z) = 0$ for all $(x, y, z) \in \mathbb{R}^3$. But the the Inverse Function Theorem does not apply to F at any point in $\mathbb{R}^3$.

(b) The Inverse Function Theorem requires that for a sufficiently small neighborhood U of $\vec{a} \in \mathbb{R}^3$, $F(U)$ is an open ball about $F(\vec{a}) = \vec{b}$. Suppose $\vec{x} \in \operatorname{im} F$ with $\vec{x} = (x, y, g(x, y))$. For $(x, y) \in \mathbb{R}^2$, there is at most one z with $(x, y, z) \in \operatorname{im} F$ because $z = g(x, y)$. But then for $\epsilon > 0$, $(x, y, z + \epsilon/2) \in B_\epsilon(\vec{x})$ but is not in $\operatorname{im} F$. But then F contains no open ball, contrary to the Inverse Function Theorem.

□

August 2010

1. Suppose that $f : \mathbb{R} \to \mathbb{R}$ is a function such that $f(f(x)) = x$ for all $x \in \mathbb{R}$. Prove that there exists an irrational number such t that $f(t)$ is also irrational.

Solution: Suppose that $f(x) = f(y)$. Then as f is a function we know

$$x = f(f(x)) = f(f(y)) = y$$

so that $x = y$ and f is an injective function. Suppose $f(x)$ were never irrational, then f is an injection from $\mathbb{R}$ (uncountable) to a countable set $\mathbb{Q}$ (countable), a contradiction.

OR

As $f(f(x)) = x$, we know that $f(x)$ is invertible; in fact, $f(x)$ is its own inverse. So $f(x)$ is a bijection. If f never took an irrational value, then there is a bijection from $\mathbb{R}$ (uncountable) to a countable set $\mathbb{Q}$, a clear contradiction. □

2. Find three subsets A, B, C of the real line $\mathbb{R}$ such that $A \cap B = A \cap C = B \cap C = \emptyset$ and $\overline{A} = \overline{B} = \overline{C} = \mathbb{R}$. Prove that your sets satisfy these properties.[38]

Solution: We use a lemma: If p, q are distinct primes, then $\sqrt{pq}$ is irrational. Suppose it were rational, then there are $m, n \in \mathbb{Z}$ with $n \neq 0$ and $(m, n) = 1$ such that

$$\sqrt{pq} = \frac{m}{n}$$

But then $pq = \frac{m^2}{n^2}$. This occurs if and only if $n^2pq = m^2$. As $p \mid n^2pq$ then $p \mid m^2$ so that $p \mid m$. But then $p \mid m^2$. Now as $p^2 \mid n^2pq$ it must be that $p \mid n^2q$ so as $p \nmid q$, we know $p \mid n^2$ so that $p \mid n$, a contradiction as $(m, n) = 1$. Now let

$$A = \{a + \sqrt{p} \mid a \in \mathbb{Q}\}$$
$$B = \{b + \sqrt{q} \mid b \in \mathbb{Q}\}$$
$$C = \{c + \sqrt{r} \mid c \in \mathbb{Q}\}$$

for distinct primes p, q, r. It suffices to show that A, B are disjoint. Suppose they were non disjoint, then there are $a, b \in \mathbb{Q}$ such that $a + \sqrt{p} = b + \sqrt{q}$. But then

$$a + \sqrt{p} = b + \sqrt{q}$$
$$a - b = \sqrt{q} - \sqrt{p}$$
$$(a - b)^2 = q + p - 2\sqrt{pq}$$
$$-\frac{(a - b)^2 - q + p}{2} = \sqrt{pq}$$

[38] You can even be more 'extreme'. For example, it is possible to partition $[0, 1]$ into uncountably many, uncountable sets.

But then $\sqrt{pq}$ would be rational, a contradiction. Therefore, the sets are pairwise disjoint. We need see that these sets are dense in $\mathbb{R}$. This is obvious as they are an invertible linear transformation on $\mathbb{Q}$ given by $q \mapsto q + \sqrt{p}, q + \sqrt{q}, q + \sqrt{r}$, respectively, and $\mathbb{Q}$ is dense in $\mathbb{R}$. Another way of seeing this fact is to note that there is a rational sequence in $\mathbb{R}$, s_n, converging to the point $x_0 - \sqrt{p}$ for all $x_0 \in \mathbb{R}$. But then $s_n + \sqrt{p} \in A$ and this sequence converges to $(x_0 - \sqrt{p}) + \sqrt{p} = x_0 \in \mathbb{R}$. But then every point of $\mathbb{R}$ is a limit point of A so that $\overline{A} = \mathbb{R}$. The density follows mutatis mutandis for B and C. □

3. Let X and Y be metric spaces. Suppose that $f : X \to Y$ has the following property: for any continuous function $g : Y \to \mathbb{R}$ the composition $g \circ f$ is a continuous function from X to $\mathbb{R}$. Prove that f is continuous.

Solution: We show f is continuous by showing the preimage of closed sets are closed, i.e. find a continuous function g such that $f^{-1}(E) = (g \circ f)^{-1}(0)$ (which is closed since $g \circ f$ is continuous and $\{0\}$ is closed), where $E \subseteq Y$ is a closed set. Let $E \subseteq Y$ be closed. We want $f^{-1}(E) = (g \circ f)^{-1}(0)$, i.e. $f^{-1}(E) = (f^{-1} \circ g^{-1})(0)$. This is exactly $f^{-1}(E) = f^{-1}(g^{-1}(0))$, i.e. $g^{-1}(0) = E$. Define $g(y) := \inf\{d(z, y) : z \in E\}$. Then $g(y) = 0$ if and only if $y \in \overline{E} = E$. [Either $y \in E$ and hence $g(y) = 0$, or y is a limit point of E so that $y \in E' \subseteq \overline{E}$ and $g(y) = 0$. In either case, $y \in \overline{E}$.] But E is closed so that $E = \overline{E}$. Therefore, $g(E) = 0$ so that $g^{-1}(0) = E$ and g is continuous. But then $f^{-1}(E) = (g \circ f)^{-1}(0)$ is closed so that f is continuous.

OR

Let $g : Y \to \mathbb{R}$ be the function given by $g(y) = d(y, f(x))$, where $x \in X$ and d is the metric on Y. We need show that g is continuous. Let $\epsilon > 0$ and $y \in Y$. Choose $\delta = \epsilon/2$ so that for $|y - a| < \delta$, we have

$$|g(y) - g(a)| = |d(y, f(x)) - d(a, f(x))| \leq d(y, a) < \epsilon$$

But then g is continuous on Y.

By assumption, we know that $g \circ f$ is continuous. Let $\epsilon > 0$, then we get a $\delta_0 > 0$ such that $|gf(y) - gf(x)| < \epsilon$ for $y \in B_{\delta_0}(x)$. But

$$|gf(y) - gf(x)| = |d(f(y), f(x)) - d(f(x), f(x))| = |d(f(y), f(x))|$$

Taking $\delta = \min(\epsilon, \delta_0)$, we know $d(f(y), f(x)) < \epsilon$. But then $f(x)$ is continuous at x. But the choice of $x \in X$ was arbitrary so that $f(x)$ is continuous on all of X. □

4. Suppose that $f : \mathbb{R} \to \mathbb{R}$ is a function such that $f'(x)$ exists for all $x \in \mathbb{R}$ and $f'(-x) = -f'(x)$ for all $x \in \mathbb{R}$. Prove that $f(-x) = f(x)$ for all $x \in \mathbb{R}$.

Solution: Let $g(x) = f(x) - f(-x)$. Then g is differentiable since f is. Furthermore, $g'(x) = f'(x) + f'(-x) = 0$ since $f'(-x) = -f'(x)$ for all $x \in \mathbb{R}$. But then g is constant.

Now $g(0) = f(0) - f(0) = 0$. Then $g(x) \equiv 0$ for all $x \in \mathbb{R}$. But $g(x) := f(x) - f(-x)$ so that $f(x) = f(-x)$ for all $x \in \mathbb{R}$. □

5. Give an example of a bounded function $f : [0,1] \to \mathbb{R}$ such that

- f is not Riemann integrable on $[0,1]$
- The function g defined by $g(x) = \sin f(x)$ is Riemann integrable on $[0,1]$

Prove your claims using the definition of the Riemann integral.

Solution: Define the function

$$f(x) = \begin{cases} \dfrac{1}{x}, & x \in (0,1] \\ 0, & x = 0 \end{cases}$$

Then $g(x) = \sin f(x)$ is

$$g(x) = \sin f(x) = \begin{cases} \sin\left(\dfrac{1}{x}\right), & x \in (0,1] \\ 0, & x = 0 \end{cases}$$

Clearly, $f \notin \mathcal{R}$ on $[0,1]$ since f is not bounded. We show that $g \in \mathcal{R}$ on $[0,1]$. Let $\epsilon > 0$. Now $g(x)$ is continuous on $[\epsilon, 1]$, so there exists a partition, say $\mathcal{P}_1$, of $[\epsilon, 1]$ such that $U(\mathcal{P}_1, g) - L(\mathcal{P}_1, g) < \epsilon$. Let $\mathcal{P}_2$ be any partition of $[0, \epsilon$. We know $U(\mathcal{P}_2, g) - L(\mathcal{P}_2, g) = \sum(M_i - m_i)\Delta x_i < 2\epsilon$ since $|g(x)| \leq 1$ and the length of the interval is ϵ. Now $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ is a partition of $[0,1]$. But we have $U(\mathcal{P}, g) - L(\mathcal{P}, g) < \epsilon + 2\epsilon = 3\epsilon$. Then $g \in \mathcal{R}[0,1]$. □

6. Let $\boldsymbol{f} : \mathbb{R}^3 \to \mathbb{R}^3$ be a mapping defined by

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_2 - x_1 \\ y_3 &= x_3^5 \end{aligned}$$

(a) Determine all points $\boldsymbol{a} \in \mathbb{R}^3$ at which $\boldsymbol{f}$ satisfies the assumptions of the Inverse Function Theorem.

(b) Is $\boldsymbol{f}$ an open mapping? Prove or disprove.

Reminder: A mapping $\boldsymbol{f} : \mathbb{R}^3 \to \mathbb{R}^3$ is open if $\boldsymbol{f}(W)$ is an open subset of $\mathbb{R}^3$ for every open set $W \subset \mathbb{R}^3$.

Solution:

(a) Clearly, $f \in C^1(\mathbb{R}^3)$ since all partials exist and are continuous. We have

$$J_f(x_1, x_2, x_3) = \det \begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 5x_3^4 \end{pmatrix} = 5x_3^4 \cdot \det \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = 10x_3^4$$

Therefore, the Inverse Function Theorem applies for all $(x_1, x_2, x_3) \in \mathbb{R}^3$ such that $x_3 \neq 0$.

(b) The map f is an open mapping. Set $x_1 + x_2 = y_1$. Then we have

$$\begin{aligned} x_1 + x_2 &= y_1 \\ x_1 &= y_1 - x_2 \\ x_1 &= y_1 - y_2 - x_1 \\ x_1 &= \frac{y_1 - y_2}{2} \end{aligned}$$

Repeating this process for $x_2 - x_1 = y_2$ gives $x_2 = \dfrac{y_2 + y_1}{2}$. We know also that $x_3^5 = y_3$ so that $x_3 = y_3^{1/5}$. But then $f(x_1, x_2, x_3) = (y_1, y_2, y_3)$ has a unique solution $(x_1, x_2, x_3) = f^{-1}(y_1, y_2, y_3)$. This shows that f has a continuous inverse f^{-1}. Since f^{-1} is continuous, $f(U)$ is open in $\mathbb{R}^3$ whenever U is open in $\mathbb{R}^3$. But then f is an open map.

□

January 2011

1. Let X, Y be metric spaces and $f : X \to Y$ be a function. Prove that f is continuous on X if and only if $\overline{f^{-1}(E)} \subset f^{-1}(\overline{E})$ for every $E \subset Y$.

Solution: Assume that f is continuous on X. Let $x \in \overline{f^{-1}(E)} = f^{-1}(E) \cup (f^{-1}(E))'$, where $(f^{-1}(E))'$ denotes the set of limit points of $f^{-1}(E)$. If $x \in f^{-1}(E)$, then $x \in (f^{-1}(E))'$ so that $\overline{f^{-1}(E)} \subseteq f^{-1}(E) \subseteq f^{-1}(\overline{E})$ as $E \subseteq \overline{E}$. But then $\overline{f^{-1}(E)} \subseteq f^{-1}(\overline{E})$. If $x \notin f^{-1}(E)$, then $x \in (f^{-1}(E))'$. Then for each $r > 0$, there exists $y \in B_r(x) \cap f^{-1}(E)$ such that $y \neq x$. Since f is continuous, for every $\epsilon > 0$, there exists $\delta > 0$ such that if $d(z, w) < \delta$, then $d(f(z), f(w)) < \epsilon$. Then there is $y \in B_\delta(x) \cap f^{-1}(E)$ such that $y \neq x$ and $d(x, y) < \delta$. But it must then be that $d(f(x), f(y)) < \epsilon$. Then $f(x) \in B_\epsilon(f(x)) \cap E$ with $f(y) \neq f(x)$ (since f is a function). But this shows that $f(y) \in E' \subseteq \overline{E}$ implying $\overline{f^{-1}(E)} \subseteq f^{-1}(\overline{E})$.

Now assume that $\overline{f^{-1}(E)} \subseteq f^{-1}(\overline{E})$ for all $E \subseteq Y$. To show f is continuous, we show that the preimage of closed sets are closed. Let $C \subseteq Y$ be closed. Note that $\overline{f^{-1}(E)} \subseteq f^{-1}(\overline{C}) = f^{-1}(C)$ ($\overline{C} = C$ since C is closed). But then $\overline{f^{-1}(C)} \subseteq f^{-1}(C)$ so that $f^{-1}(C) = \overline{f^{-1}(C)}$. But then $f^{-1}(C)$ is closed so that f must be continuous.

OR

Suppose that f is continuous. Let $x \in \overline{f^{-1}(E)}$, i.e. $x \in f^{-1}(E)$ or $x \in f^{-1}(E)'$. If $x \in f^{-1}(E)$ then observe $f(x) \in E$ so $f(x) \in E \subset \overline{E}$. Therefore, $f^{-1}(E) \subset f^{-1}(\overline{E})$. Now suppose that $x \in f^{-1}(E)'$. Then all neighborhoods of x intersect $f^{-1}(E)$ at a point y distinct from x. But $f^{-1}(E) \subset f^{-1}(\overline{E})$ so that all neighborhoods of x intersect $f^{-1}(\overline{E})$ at a point distinct from x so that $x \in f^{-1}(\overline{E})'$. But as f is continuous and $\overline{E}$ is closed, $f^{-1}(\overline{E})$ is closed. Hence, $f^{-1}(\overline{E})$ contains all of its limit points. Therefore, $x \in f^{-1}(\overline{E})$. This shows that $\overline{f^{-1}(E)} \subset f^{-1}(\overline{E})$. Note that we are in a metric space so one could produce a sequence $y_n \to x$ as x is a limit point. Then $\lim_{n\to\infty} f(y_n) = f(\lim_{n\to\infty} y_n) = f(x)$ (here we have used the continuity of f) so that $x \in f^{-1}(\overline{E})$.

Now suppose $\overline{f^{-1}(E)} \subset f^{-1}(\overline{E})$ for all $E \subset Y$. Let $E \subset Y$ be closed. Then $\overline{E} = E$. We want to show that f is continuous, which we do by showing the preimage of closed is closed. But $f^{-1}(E) \subset \overline{f^{-1}(E)} \subset f^{-1}(\overline{E}) = f^{-1}(E)$ so $\overline{f^{-1}(E)} = f^{-1}(E)$.

OR

Assume that f is continuous and $U \subseteq X$. We need only show that if $x \in \overline{U}$, then $f(x) \in \overline{f(U)}$. Let V be a neighborhood of $f(x)$. Then $f^{-1}(V)$ is an open neighborhood of X containing x. Then $f^{-1}(V)$ must intersect U at some point y. But then V intersects $f(U)$ at $f(y)$ so that $f(x) \in \overline{f(U)}$.

Now assume that for all $V \subseteq Y$, we have $\overline{f^{-1}(V)} \subseteq f^{-1}(\overline{V})$. We show the preimage of closed sets are closed. Let $V \subseteq Y$ be closed. Now $f^{-1}(V) \subset \overline{f^{-1}(V)} \subset f^{-1}(\overline{V}) = f^{-1}(V)$

so $\overline{f^{-1}(V)} = f^{-1}(V)$. Therefore, f is continuous. $\square$

2. Prove that the sequence $x_n = n\sin(2\pi en!)$, $n \geq 1$, is convergent and find its limit. Hint: Use the fact that $e = \sum_{k=0}^{n} \dfrac{1}{k!} + r_n$, where $r_n < \dfrac{1}{n \cdot n!}$, $n \geq 1$.

Solution: We have $e = \sum_{n=0}^{\infty} \frac{1}{n!}$. Then

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 1+1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\cdots < 1+1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\frac{1}{n!(n+1)}+\frac{1}{n!(n+1)^2}+\cdots$$

We also have

$$\sum_{m=0}^{\infty} \frac{1}{n!}\left(\frac{1}{n+1}\right)^{m+1} = \frac{\frac{1}{n!(n+1)}}{1-\frac{1}{n+1}} = \frac{1}{n!(n+1)}\frac{n+1}{n} = \frac{1}{n!n}$$

so we can write $e = \sum_{k=0}^{n} \frac{1}{k!} + r_n$, where $r_n < \frac{1}{nn!}$ for $n \geq 1$ and $r_n \to 0$ as $n \to \infty$. Therefore,

$$\begin{aligned} n\sin(2\pi n! e_n) &= n\sin\left(2\pi n! \sum_{k=0}^{n} \frac{1}{k!} + r_n\right) \\ &= n\sin\left(2\pi \sum_{k=0}^{n} \frac{n!}{k!} + 2\pi n! r_n\right) \\ &= n\sin\left(2\pi \sum_{k=0}^{n} \frac{n!}{k!}\right)\cos(2\pi n! r_n) + n\cos\left(2\pi \sum_{k=0}^{n} \frac{n!}{k!}\right)\sin(2\pi n! r_n) \end{aligned}$$

Now as $\sum_{k=0}^{n} \frac{n!}{k!}$ is an integer for each value of k, the sum is an integer. Using the fact that $\sin(2\pi m) = 0$ and $\cos(2\pi m) = 1$, we know that the above sum is simply $n\sin(2\pi n! r_n)$. We know that sin is increasing on $\left[0, \frac{2\pi}{n}\right]$ for $n > 2$. Now

$$n\sin\left(\frac{2\pi}{n+1}\right) < n\sin(2\pi n! r_n) < n\sin\left(\frac{2\pi}{n}\right)$$

and then

$$\frac{\sin\left(\frac{2\pi}{n+1}\right)}{\frac{1}{n+1}} < \frac{\sin\left(\frac{2\pi}{n+1}\right)}{\frac{1}{n}} < \frac{\sin(2\pi n! r_n)}{\frac{1}{n}} < \frac{\sin\left(\frac{2\pi}{n}\right)}{\frac{1}{n}}$$

Then taking the limit as $n \to 0$ and using the fact that $\lim_{x\to 0} \frac{\sin x}{x} = 1$, the Squeeze Theorem says that the limit must be 2π. $\square$

3. Let $f : \mathbb{R} \to \mathbb{R}$ be a differentiable function such that $|f'(x)| \geq 1$ for all $x \in \mathbb{R}$. Prove that f is one-to-one and onto $\mathbb{R}$, and that the inverse function $f^{-1} : \mathbb{R} \to \mathbb{R}$ is differentiable.

Solution: Suppose $f'(a) < 0 < f'(b)$ for some $a, b \in \mathbb{R}$. Then by the Intermediate Value Theorem for Derivatives, there exists $x \in (a, b)$ such that $f'(x) = 0$, a contradiction as $|f'(x)| > 1$ for all $x \in \mathbb{R}$. Then $|f'(x)| \neq 0$ for all all $x \in \mathbb{R}$. Since we can replace $f'(x)$ by $-f'(x)$, without loss of generality, assume that $f'(x) > 0$ for all $x \in \mathbb{R}$. Then f must be strictly increasing. Then f is a bijection, i.e. f has an inverse $f^{-1} : \mathbb{R} \to \mathbb{R}$.

$$\lim_{t \to x} \frac{f^{-1}(t) - f^{-1}(x)}{t - x} = \lim_{t \to x} \frac{f^{-1}(t) - f^{-1}(x)}{f(f^{-1}(t)) - f(f^{-1}(x))} = \lim_{u \to y} \frac{u - y}{f(y) - f(y)} = \frac{1}{\lim_{u \to y} \dfrac{f(u) - f(y)}{u - y}} = \frac{1}{f'(y)},$$

which is well defined as $f'(y) \neq 0$. [Note, $u := f^{-1}(y)$ and $y := f^{-1}(x)$.] Therefore, f^{-1} is differentiable. □

4. Suppose $f : \mathbb{R} \to \mathbb{R}$ is continuous. Show that

$$\int_0^1 f(x)x^2 \, dx = \frac{1}{3} f(\xi)$$

for some $\xi \in [0, 1]$.

Solution: We use the following lemma: If $f(x), g(x)$ are continuous functions on $[a, b]$ and $g(x) \geq 0$ on (a, b) then there is a $\xi \in (a, b)$ such that

$$\int_a^b f(x)g(x) \, dx = f(\xi) \int_a^b g(x) \, dx$$

To see this, using the continuity of $f(x), g(x)$ on $[a, b]$, we know that $f(x)g(x)$ is continuous on $[a, b]$. Then $f(x)g(x)$ is integrable on $[a, b]$. As $f(x)$ is continuous on $[a, b]$ (which is a bounded interval), then $f(x)$ is bounded on $[a, b]$. Suppose $m \leq f(x) \leq M$ for all $x \in [a, b]$. So as $g(x) \geq 0$, we know

$$mg(x) \leq f(x)g(x) \leq Mg(x)$$

So that

$$m \int_a^b g(x) \, dx \leq \int_a^b f(x)g(x) \, dx \leq M \int_a^b g(x) \, dx$$

If $\int_a^b g(x) \, dx = 0$, as $g(x) \geq 0$ and is continuous, the result is trivial. Suppose that the integral is nonzero, then

$$m \leq \frac{\int_a^b f(x)g(x) \, dx}{\int_a^n g(x) \, dx} \leq M$$

The continuity of $f(x)$ gives $\xi \in [a, b]$ such that

$$f(\xi) = \frac{\int_a^b f(x)g(x) \, dx}{\int_a^n g(x) \, dx}$$

But then this immediately implies that $\int_a^b f(x)g(x)\,dx = f(\xi)\int_a^b g(x)\,dx$.

To obtain the desired result, simply take $g(x) = x^2$, we have $\xi \in [0,1]$ such that

$$\begin{aligned}\int_0^1 f(x)x^2 &= f(\xi)\int_0^1 x^2\,dx \\ &= f(\xi)\,\frac{x_3}{3}\Big|_0^1 \\ &= \frac{1}{3}f(\xi)\end{aligned}$$

OR

Observe f is continuous on $[0,1]$, a compact set. By the Extreme Value Theorem, there exists $\xi_1, \xi_2 \in [0,1]$ such that $f(\xi_1) \le f(x) \le f(\xi_2)$ for all $x \in [0,1]$. Say $m = f(\xi_1)$ and $f(\xi_2) = M$, so that $m \le f(x) \le M$ for all $x \in [0,1]$. Then

$$\frac{m}{3} = \int_0^1 mx^2\,dx \le \int_0^1 f(x)x^2\,dx \le \int_0^1 Mx^2\,dx$$

so that $m \le 3\int_0^1 x^2 f(x)\,dx \le M$. By the Intermediate Value Theorem, there exists $\xi \in (0,1)$ so that $f(\xi) = 3\int_0^1 x^2 f(x)\,dx$. But then

$$\frac{1}{3}f(\xi) = \int_0^1 x^2 f(x)\,dx.$$

□

5. Let $f_1 : [0,1] \to \mathbb{R}$ be a continuous function. Consider the sequence of functions defined on the interval $[0,1]$ as follows: for $n = 1, 2, \ldots$,

$$f_{n+1}(x) = \cos f_n(x).$$

Prove that $\{f_n\}$ contains a uniformly convergent subsequence.

Solution: The set $[0,1]$ is compact. The function $\cos x$ is continuous on $\mathbb{R}$, the function $f(x)$ is continuous on $[0,1]$, therefore the composition $\cos f(x)$ is continuous on $[0,1]$ (hence uniformly so). Hence each $f_{n+1}(x)$ is uniformly continuous. Furthermore as $f_1(x)$ is continuous on $[0,1]$, there is a $M \in \mathbb{R}$ such that $|f(x)| \le M$ for all $x \in [0,1]$. As $\cos x$ is bounded, this shows that $|f_n(x)| \le \max\{M, 1\}$ for all $x \in [0,1]$. Then the sequence $\{f_n(x)\}$ is uniformly bounded. We need only show that $\{f_n(x)\}$ is equicontinuous to see that the sequence contains a uniformly convergent subsequence. However via the Mean Value Theorem for any $[x,y] \subset \mathbb{R}$, we have

$$|\cos x - \cos y| = |g'(c)|\,|x - y| \le |x - y|$$

for some $c \in [a,b]$. However, $g(x) = \cos x$ so that $|g'(x)| = |-\sin x| = |\sin x| \leq 1$ for all $x \in \mathbb{R}$. Let $\epsilon > 0$. As $f_1(x)$ is continuous on $[0,1]$, it is uniformly continuous. So there is a $\delta > 0$ such that $|f_1(x) - f_1(y)| < \epsilon$ for $|x-y| < \delta$. But then observe that via induction

$$|f_n(x) - f_n(y)| \leq |f_{n-1}(x) - f_{n-1}(y)| \leq \cdots \leq |f_1(x) - f_1(y)| < \epsilon$$

for all $x, y \in [0,1]$ such that $|x-y| < \delta$. Therefore, we know that $\{f_n\}$ is equicontinuous and pointwise bounded on the compact interval $[0,1]$. By the Arzelà-Ascoli Theorem, $\{f_n\}$ contains a uniformly convergent subsequence. □

6. Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R}^2 \to \mathbb{R}$ be continuously differentiable. Suppose that none of the derivatives f', $D_1 g$, $D_2 g$ attains the value 0. Define $\boldsymbol{h} = (h_1, h_2)$ by

$$\begin{aligned} h_1(x,y,z) &= f(x) + g(y,z) \\ h_2(x,y,z) &= f(y) - g(x,z) \end{aligned}$$

Prove that $\boldsymbol{h}(W)$ is an open subset of $\mathbb{R}^2$ for every open set $W \subset \mathbb{R}^3$.

Solution: Notice that $h \in C^1(\mathbb{R}^3)$ since f, g are continuously differentiable.

$$\boldsymbol{h}' = \begin{pmatrix} f'(x) & D_1 g(y,z) & D_2 g(y,z) \\ -D_1 g(x,z) & f'(y) & -D_2 g(x,z) \end{pmatrix}$$

Let $\hat{h} = (h_1, h_2, z) : \mathbb{R}^3 \to \mathbb{R}^3$. Then

$$\begin{aligned} J_{\hat{h}}(x,y,z) &= \det \begin{pmatrix} f'(x) & D_1 g(y,z) & D_2 g(y,z) \\ -D_1 g(x,z) & f'(y) & -D_2 g(x,z) \\ 0 & 0 & 1 \end{pmatrix} \\ &= \det \begin{pmatrix} f'(x) & D_1 g(y,z) \\ -D_1 g(x,z) & f'(y) \end{pmatrix} \\ &= f'(x) f'(y) + D_1 g(x,z) D_1 g(y,z) \end{aligned}$$

Since $f_1, D_1 g, D_2$ are never zero, they are always positive or always negative. [If they switched sign they would have to vanish at some point as they are continuous.] If $J_{\hat{h}}$ were to vanish, then it must be that $f'(x)f'(y) = -D_1 g(x,z) D_1 g(y,z)$. But since $f'(x)$ and $f'(y)$ have the same sign, $f'(x)f'(y) > 0$. This holds mutatis mutandis for $D_g(x,z)$ and $D_1 g(y,z)$. But then then $f'(x)f'(y)$ and $-D_1 g(x,z) D_1 g(x,z)$ have opposite signs and cannot be equal. Thus, $J_{\hat{h}}$ never vanishes. In fact, $J_{\hat{h}} > 0$ as $f'(x)f'(y), D_1 g(x,y) D_1(x,z) > 0$. The Inverse Function Theorem then applies to $\hat{h}$ for all $(x,y,z) \in \mathbb{R}^3$. Therefore, $\hat{h}$ is an open mapping. Then it must be that h is open (for if it were not then neither could $\hat{h}$ be open). Then $h(W)$ is open for all $W \subseteq \mathbb{R}^3$ open subsets. □

August 2011

1. Suppose A is an infinite bounded subset of the real line $\mathbb{R}$. Prove that there exists a set $B \subset A$ which is neither open nor closed in $\mathbb{R}$.

Solution: Since A is infinite and bounded, by Weierstrass Theorem, A has a limit point $x \in \mathbb{R}$. Choose a sequence $\{s_n\}$ of elements of A such that $s_n \to x$. Define $B := \{s_n\}$. Clearly, $B \subseteq A$. Now B cannot be closed since $x \notin B$ and x is a limit point of B. But B cannot be open since it consists solely of singletons. □

2. Let X be a metric space. Suppose that $f : [0,1] \to X$ is continuous. prove that there exists an integer n such that for any choice of the partition $0 = t_0 < t_1 < \cdots < t_n = 1$ we have

$$\min_{1 \le i \le n} \operatorname{diam} f([t_{i-1}, t_i]) \le 1$$

Reminder: $\operatorname{diam} E = \sup\{d(a,b) \colon a, b \in E\}$.

Solution: Note that $f(x)$ is uniformly continuous since it is continuous on a compact set. Then for $\epsilon = 1$, there exists $\delta > 0$ such that for all $x, y \in [0,1]$ with $|x - y| < \delta$, we have $d(f(x), f(y)) < 1$. Choose $n \in \mathbb{N}$ such that $1/n < \delta$. We have $\sum_{i=1}^{n}(t_i - t_{i-1}) = 1 - 0 = 1$ (note this series telescopes). Then there exists a i such that $t_i - t_{i-1} \le 1/n < \delta$. Therefore if $x, y \in [t_{i-1}, t_i]$, we have $d(f(x), f(y)) < 1$. This shows that $\min_{1 \le i \le n} \operatorname{diam} f([t_{i-1}, t_i]) \le 1$. □

3. Let $f : [1, e] \to \mathbb{R}$ be a continuous function. Prove that

$$\left(\int_1^e f(x)\, dx \right)^2 \le \int_1^e x f(x)^2\, dx$$

Solution: Observe

$$\begin{aligned}
\left| \int_1^e f(x)\, dx \right| &\le \left(\int_1^e \left| \frac{1}{\sqrt{x}} \right|\, dx \right)^{1/2} \left(\int_1^e \left| \sqrt{x} f(x) \right|^2\, dx \right)^{1/2} \\
&= \left(\int_1^e \frac{dx}{x} \right)^{1/2} \left(\int_1^e x f(x)^2\, dx \right)^2 \\
&= (\log e - \log 1)^{1/2} \left(\int_1^e x f(x)^2\, dx \right)^{1/2} \\
&= \left(\int_1^e x f(x)^2\, dx \right)^{1/2}
\end{aligned}$$

where the first inequality is Hölder's Inequality. Taking squares yields the result.

OR

Define $\langle f, g\rangle := \int_1^e f(x)g(x)\,dx$. For $r \in \mathbb{R}$, we have

$$\begin{aligned}
\langle rf, g\rangle &= \int_1^e rf(x)g(x)\,dx = r\int_1^e f(x)g(x)\,dx = r\langle f, g\rangle \\
\langle f, g\rangle &= \int_1^e f(x)g(x)\,dx = \int_1^e g(x)f(x)\,dx = \langle g, f\rangle \\
\langle f+h, g\rangle &= \int_1^e (f(x)+h(x))g(x)\,dx = \int_1^e f(x)g(x)\,dx + \int_1^e h(x)g(x)\,dx = \langle f, g\rangle + \langle h, g\rangle \\
\langle f, f\rangle &= \int_1^e f(x)^2\,dx \geq 0
\end{aligned}$$

Since $f(x)$ is continuous on $[1, e]$, so too is $f(x)^2$ continuous on $[1, e]$. Then $\langle f, f\rangle = 0$ if and only if $f^2(x) = 0$ if and only if $f(x) = 0$ on $[1, e]$. Therefore, $\langle \cdot, \cdot \rangle$ is an inner product. By Cauchy-Schwartz, $|\langle f, g\rangle|^2 \leq \langle f, f\rangle \cdot \langle g, g\rangle$. Now if $h(x)$ is any positive function,

$$\begin{aligned}
\left(\int_1^e f(x)\,dx\right)^2 = |\langle f/h, h\rangle|^2 \leq \langle f/h, f/h\rangle \cdot \langle h, h\rangle &= \int_1^e \frac{f(x)^2}{h(x)^2}\,dx \cdot \int_1^e h(x)^2\,dx \\
&= \int_1^e \left[\frac{\int_1^e h(y)^2\,dy}{h(x)^2}\right] f(x)^2\,dx.
\end{aligned}$$

Taking $h(x) = \frac{1}{\sqrt{x}}$, we have

$$\frac{\int_1^e h(y)^2\,dy}{h(x)^2} = \frac{\int_1^e \frac{dy}{y}}{1/x} = x \cdot (\log y)\Big|_0^e = x$$

The result then follows. □

4. Let $\{f_n\}$ be a sequence of Riemann integrable (with respect to dx) real-valued functions defined on $[0, 1]$. Suppose that the functions $g_n(x) = \sqrt{x} f_n(x)$ form a uniformly convergent sequence. Prove that the limit

$$\lim_{n\to\infty} \int_0^1 f_n(x)\,dx$$

exists.

Solution: We show that $\left\{\int_0^1 f_n(x)\,dx\right\}$ is Cauchy. Since $\{g_n\}$ is uniformly convergent, for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for $n, m > N <$ $|g_n(x) - g_m(x)| < \epsilon/2$, i.e.

$$\left|\sqrt{x}(f_n(x) - f_m(y))\right| < \frac{\epsilon}{2}.$$

Then

$$\begin{aligned}\left|\int_0^1 f_n(x)\,dx - \int_0^1 f_m(x)\,dx\right| &= \left|\int_0^1 (f_n(x) - f_m(x))\,dx\right| \\ &= \left|\int_0^1 \frac{\sqrt{x}(f_n(x) - f_m(x))}{\sqrt{x}}\,dx\right| \\ &< \left|\int_0^1 \frac{\epsilon}{2\sqrt{x}}\,dx\right| \\ &= \left|\epsilon\left(\sqrt{x}\Big|_0^1\right)\right| = \epsilon\end{aligned}$$

Therefore, $\left\{\int_0^1 f_n(x)\,dx\right\}$ is Cauchy in $\mathbb{R}$. But this shows that $\lim_{n\to\infty}\int_0^1 f_n(x)\;dx$ exists. □

5. Let $f : (0,\infty) \to \mathbb{R}$ be everywhere differentiable with $|f'(x)| \leq \frac{1}{x^2}$, $0 < x < \infty$. Prove that the improper integrals

$$\int_{2y}^{\infty}(f(x) - f(x-y))\,dx, \quad 0 < y < \infty$$

are well defined and in absolute value not greater than 1.

Solution: First, observe

$$\left|\int_{2y}^{\infty} f(x) - f(x-y)\,dx\right| \leq \int_{2y}^{\infty} |f(x) - f(x-y)|\,dx$$

But since f is differentiable on $(x-y,x)$ and continuous on $[x-y,x]$, there exists $\xi \in (x-y,x)$ such that $f(x) - f(x-y) = yf'(\xi)$ by the Mean Value Theorem. So

$$\begin{aligned}\left|\int_{2y}^{\infty} f(x) - f(x-y)\,dx\right| &\leq \int_{2y}^{\infty} |y|\,|f'(\xi)|\,dx \\ &\leq \int_{2y}^{\infty} y\cdot\frac{1}{\xi^2}\,dx \\ &\leq y\int_{2y}^{\infty}\frac{dx}{(x-y)^2} \\ &y\left(-\frac{1}{x-y}\right)\Big|_{2y}^{\infty} \\ &= y\cdot\frac{1}{2y-y} = 1\end{aligned}$$

Therefore, $\left|\int_{2y}^{\infty}(f(x)-f(x-y))\,dx\right| \leq 1$. We need now show that these are well defined, i.e. to show that $\int_{2y}^{\infty}(f(x)-f(x-y))\,dx$ are absolutely convergent. Now

$$|f(x)-f(x-y)| = y\,|f'(\xi)| \leq y\frac{1}{\xi^2} \leq y\frac{1}{(x-y)^2}$$

and $\int_{2y}^{\infty}\frac{y}{(x-y)^2}\,dx = 1$ by the work above. Therefore, $\int_{2y}^{\infty}(f(x)-f(x-y))\,dx$ converges absolutely so that the integral is well defined. □

6. Let $g:\mathbb{R}\to\mathbb{R}$ be a strictly increasing differentiable function. Define $\boldsymbol{f}:\mathbb{R}^2\to\mathbb{R}^2$ by

$$\boldsymbol{f}(x_1,x_2) = (x_1+g(x_1-x_2), x_2+\sin x_2 - g(x_1-x_2)).$$

Does it follow that $\boldsymbol{f}$ satisfies the conditions of the Inverse Function Theorem at every point of $\mathbb{R}^2$? Prove or give a counterexample.

Solution: Take $g(x)=x^3$. Clearly, $g(x)$ is strictly increasing and differentiable. Then

$$f(x_1,x_2) = (x_1+(x_1-x_2)^3, x_2+\sin x_2-(x_1-x_2)^3).$$

Clearly, $f\in C^1(\mathbb{R}^2)$ since all the partials exist and are continuous.

$$\begin{aligned}
J_f(x_1,x_2) &= \det\begin{bmatrix} 1+3(x_1-x_2)^2 & -3(x_1-x_2)^2 \\ -3(x_1-x_2)^2 & 1+\cos x_2+3(x_1-x_2)^2\end{bmatrix}\\
&= (1+3(x_1-x_2)^2)(1+\cos x_2+3(x_1-x_2)^2) - 9(x_1-x_2)^4\\
&= 1+\cos x_2+3(x_1-x_2)^2+3(x_1-x_2)^2+3\cos x_2(x_1-x_2)^2\\
&= 1+\cos x_2+6(x_1-x_2)^2+3\cos x^2(x_1-x_2)^2
\end{aligned}$$

Take $(x_1,x_2)=(\pi,\pi)\in\mathbb{R}^2$. Then $J_f(\pi,\pi)=0$. Therefore, the Inverse Function Theorem does not apply for all $(x_1,x_2)\in\mathbb{R}^2$. □

January 2012

1. Let $\{c_n\}$ be a sequence so that $c_n > 0$ for all $n \geq 1$ and $\lim_{n\to+\infty} c_n = 0$. Show that there exists a sequence $\{a_n\}$ so that $a_n > 0$ for all $n \geq 1$, $\sum_{n=1}^{\infty} a_n$ is divergent and $\sum_{n=1}^{\infty} c_n a_n$ is convergent.

Solution: Since $\lim_{n\to\infty} c_n = 0$, there is a subsequence $\{c_{n_k}\}$ such that $c_{n_k} < 1/2^k$ for $k \in \mathbb{N}$. Define

$$a_n = \begin{cases} 1, & n = n_k \text{ for some } k \\ \dfrac{1}{n^2 c_n}, & n \neq n_k \text{ for all } k. \end{cases}$$

Clearly, $\sum a_n$ diverges since $\lim_{n\to\infty} a_n \neq 0$. But

$$\sum_{n=1}^{N} c_n a_n = \sum_{n_k \leq N} c_{n_k} a_{n_k} + \sum_{\substack{n=1 \\ n\neq n_k}} c_n a_n \leq \sum_{n_k \leq N} \frac{1}{2^k} + \sum_{\substack{n=1 \\ n\neq n_k}} \frac{1}{n^2} < 1 + \frac{\pi^2}{6}.$$

Therefore, $\sum c_n a_n$ is bounded and $c_n a_n > 0$. But then it must be that $\sum c_n a_n$ converges. □

2. Let $f : \mathbb{R} \to \mathbb{R}$ be a uniformly continuous function. Show that there exist positive constants A, B so that $|f(x)| \leq A|x| + B$ for every $x \in \mathbb{R}$.

Solution: Since f is uniformly continuous, there is a $\delta > 0$ such that for all x, y such that $|x - y| < \delta$, we have $|f(x) - f(y)| \leq 1$. If $x \in [0, \delta]$, we have $|f(x) - f(0)| \leq 1$. Then $|f(x)| \leq 1 + |f(0)|$. If $x \in [\delta, 2\delta]$, then $|f(x) - f(\delta)| \leq 1$. Therefore, $|f(x)| \leq 1 + |f(\delta)| \leq 2 + |f(0)|$. Now assume $x \in [(n-2)\delta, (n-1)\delta]$. This implies $|f(x)| \leq n - 1 + |f(0)|$. This shows that for $x \in [(n-2)\delta, n\delta]$, that $|f(x)| \leq n + |f(0)|$. Then for $x \in [(n-1)\delta, n\delta]$, $|f(x) - f((n-1)\delta)| \leq 1$ so that $|f(x)| \leq 1 + |f((n-1)\delta)| \leq n + |f(0)|$. Similarly, $|f(x)| \leq n + |f(0)|$ for all $x < 0$. Therefore, $|f(x)| \leq n + |f(0)|$ for all $x \in \mathbb{R}$ for some n. But then $|f(x)| \leq \frac{1}{\delta}|x| + 1 + |f(0)|$. Define $A = \frac{1}{\delta} > 0$ and $B = 1 + |f(0)| > 0$. Then there exist $A, B > 0$ such that $|f(x)| \leq A|x| + B$ for all $x \in \mathbb{R}$. □

3. Let $f : \mathbb{R} \to \mathbb{R}$ be a function which is differentiable at 0 and so that $f(0) = 0$. Show that the following limit exists and find it:

$$\lim_{x\to 0} \frac{f(x) - \sin f(x)}{x^3}.$$

Solution: Observe that since $f(x)$ is differentiable at 0, we have

$$\lim_{x\to 0} \frac{f(x)}{x} = \lim_{x\to 0} \frac{f(x) - 0}{x - 0} = \lim_{x\to 0} \frac{f(x) - f(0)}{x - 0} = f'(0)$$

This shows that

$$f'(0)^3 = \lim_{x\to 0}\frac{f(x)}{x}\cdot\lim_{x\to 0}\frac{f(x)}{x}\cdot\lim_{x\to 0}\frac{f(x)}{x} = \lim_{x\to 0}\left(\frac{f(x)}{x}\right)^3$$

Now using the Taylor Series for $\sin x$, we have

$$\begin{aligned}
\sin x &= \sum_{n=0}^{\infty}(-1)^n\frac{x^{2n+1}}{(2n+1)!}\\
x-\sin x &= \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^{2n+1}}{(2n+1)!}\\
\frac{x-\sin x}{x^3} &= \sum_{n=0}^{\infty}(-1)^n\frac{x^{2(n-1)}}{(2n+1)!}
\end{aligned}$$

The convergence of this series is uniform (a power series converges uniformly to its function within the interval of convergence). Hence,

$$\begin{aligned}
\lim_{x\to 0}\frac{x-\sin x}{x^3} &= \lim_{x\to 0}\sum_{n=0}^{\infty}(-1)^n\frac{x^{2(n-1)}}{(2n+1)!}\\
&= \lim_{x\to 0}\left[\frac{1}{3!}+\sum_{n=1}^{\infty}(-1)^n\frac{x^{2(n-1)}}{(2n+1)!}\right]\\
&= \frac{1}{3!}+\sum_{n=0}^{\infty}\lim_{x\to 0}\left[(-1)^n\frac{x^{2(n-1)}}{(2n+1)!}\right]\\
&= \frac{1}{3!}
\end{aligned}$$

where we have used uniform convergence to exchange limits and summations. But as $f(x)$ is differentiable at 0, it is continuous at 0. Further as $f(x)$ is differentiable at 0, $\sin f(x)$ is differentiable at 0, hence continuous there. But then $x^3, f(x), \sin f(x)$ are all continuous at 0. But then using the work from above, this shows

$$\lim_{x\to 0}\frac{f(x)-\sin f(x)}{f(x)^3} = \frac{1}{3!} = \frac{1}{6}.$$

But then

$$\begin{aligned}
\frac{1}{6}\cdot f'(0)^3 &= \lim_{x\to 0}\frac{f(x)-\sin f(x)}{f(x)^3}\cdot\lim_{x\to 0}\left(\frac{f(x)}{x}\right)^3\\
&= \lim_{x\to 0}\left[\frac{f(x)-\sin f(x)}{f(x)^3}\cdot\frac{f(x)^3}{x^3}\right]\\
&= \lim_{x\to 0}\frac{f(x)-\sin f(x)}{x^3}
\end{aligned}$$

□

4. Does the improper integral $\int_0^\infty \cos(x^2)\ dx$ converge or diverge? Prove your answer.[39]

Solution: First, note that $|\cos x| \leq 1$ so that $\int_0^\infty \cos x^2\ dx \leq \int_0^1\ dx + \int_1^\infty \cos x^2\ dx$. So we need only show that $\int_1^\infty \cos x^2\ dx$ coverages.

Make the u-substitution $u = x^2$. Note that this is injective over $[1, \infty)$. Then we have $du = 2x\ dx$ so that $dx = \frac{du}{2x} = \frac{du}{2\sqrt{u}}$. This gives us the integral

$$\int_1^n \cos(x^2)\ dx = \int_1^{n^2} \frac{\cos u}{\sqrt{u}}\ du$$

Integration by parts with $u' = u^{-1/2}$ yields

$$\frac{\sin u}{\sqrt{u}}\bigg|_1^{n^2} + \frac{1}{2}\int_1^{n^2} \frac{\sin u}{\sqrt{u^3}}\ du = \frac{\sin n^2}{n} - \sin 1 + \frac{1}{2}\int_1^{n^2} \frac{\sin u}{\sqrt{u^3}}\ du$$

Clearly, $\lim_{n\to\infty} \frac{\sin n^2}{n} = 0$ by Squeeze Theorem with comparison to the function $1/n$ (making use of $|\sin x| \leq 1$). It then only remains to show that the integral on the right converges. But observe that

$$\left|\int_1^{n^2} \frac{\sin u}{\sqrt{u^3}}\ du\right| \leq \int_1^{n^2} \left|\frac{\sin u}{\sqrt{u^3}}\right|\ du \leq \int_1^{n^2} \frac{du}{\sqrt{u^3}},$$

which clearly converges as $n \to \infty$. □

5. Given that

$$(1+t)^{-1/2} = 1 - \frac{1}{2}t + \frac{1\cdot 3}{2\cdot 4}t^2 - \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}t^3 + \cdots$$

has a radius of convergence of 1 about $t = 0$, and that

$$\frac{d}{dx}\arcsin(x) = \frac{1}{\sqrt{1-x^2}} \text{ for } |x| < 1$$

find the Taylor series expansion for $\arcsin(x)$ at 0 and its radius of convergence. Justify your reasoning.

[39] This is one of the Fresnel Integrals and has many uses in Applied Mathematics.

Solution: Note that a power series converges uniformly to its function within the interval of convergence, so that derivatives may be exchanged with summations. Then we have

$$\begin{aligned}
\frac{d}{dx}\arcsin(x) &= \frac{1}{\sqrt{1-x^2}} \text{ for } |x| < 1 \\
\frac{d}{dx}\arcsin(x) &= (1-x^2)^{-1/2} = 1 + \frac{1}{2}x^2 + \frac{1\cdot 3}{2\cdot 4}x^4 + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}x^6 + \cdots \text{ for } |-x^2| < 1 \\
\frac{d}{dx}\arcsin(x) &= (1-x^2)^{-1/2} = 1 + \frac{1}{2}x^2 + \frac{1\cdot 3}{2\cdot 4}x^4 + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}x^6 + \cdots \text{ for } |x| < 1 \\
\arcsin(x) &= (1-x^2)^{-1/2} = x + \frac{1}{2\cdot 3}x^3 + \frac{1\cdot 3}{2\cdot 4\cdot 5}x^5 + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6\cdot 7}x^7 + \cdots \text{ for } |x| < 1
\end{aligned}$$

where for the last equality, we have integrated (hence using uniform convergence exchanging integrals and summations) the previous equality to obtain a power series representation for $\arcsin x$. The radius of convergence is clearly 1. □

6. Give the real valued function $g(x,y,z) = z - x^2 - y^2$ on $\mathbb{R}^3$, find $Dg(0)$. Define the mapping $F(x,y,z) = (x^3, y^3, g(x,y,z))$ from $\mathbb{R}^3$ to $\mathbb{R}^3$ with $F(0) = 0$. What does the Inverse Function Theorem say about F in a neighborhood of the origin? Does F has a continuous inverse in a neighborhood of the origin?

Solution: We have

$$Dg = \begin{pmatrix} -2x & -2y & 1 \end{pmatrix}$$

So that

$$Dg(0) = Dg(0,0,0) = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$$

Observe that the Jacobian of $F(x,y,z)$ is

$$\begin{pmatrix} 3x^2 & 0 & 0 \\ 0 & 3y^2 & 0 \\ -2x & -2y & 1 \end{pmatrix}$$

Notice that each of these partials is continuous on $\mathbb{R}^3$ so that $F(x,y,z)$ is continuously differentiable. This Jacobian has determinant $9x^2y^2$ so that the Inverse Function Theorem guarantees a continuously differentiable inverse for any point of $\mathbb{R}^3$ such that $x \neq 0$ and $y \neq 0$. The Inverse Function Theorem fails to apply at the origin as then $F'(0)$ is not invertible (in fact, it is the zero matrix). The function $F(x,y,z)$ then fails to have a continuous inverse in the neighborhood of the origin. □

August 2012

1. Let X be a metric space. Suppose that A_n, $n = 1, 2, 3, \ldots$ are nonempty compact subsets of X such that $A_{n+2} \subset A_n \cup A_{n+1}$ for every $n \geq 1$. Prove that there exists a point $x \in X$ such that $x \in A_n$ for infinitely many values of n.

Solution: Define $B_n := A_n \cup A_{n+1}$ for $n = 1, 2, \ldots$. Then $B_{n+1} = A_{n+1} \cup A_{n+2} \subseteq A_{n+1} \cup (A_n \cup A_{n+1}) = B_n$ so that $B_{n+1} \subseteq B_n$. Note that since each A_n is nonempty, each B_n is nonempty for all $n \in \mathbb{N}$. Each B_n is compact as each B_n is a finite union of compact sets. Therefore, $\bigcap_{n=1}^{\infty} B_n \neq \emptyset$. Then there is a $x \in \bigcap_{n=1}^{\infty} B_n$; that is, there is a $x_0 \in B_n$ for infinitely many n. As $B_n = A_n \cup A_{n+1}$, $x_0 \in A_n$ for infinitely many n. □

2. Suppose that $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to (0, \infty)$ are continuous functions. For $x \in \mathbb{R}$ define

$$h(x) = \sup_{0<t<g(x)} f(t)$$

(a) Prove that $h : \mathbb{R} \to \mathbb{R}$ is continuous.

(b) Give an example in which f is uniformly continuous on $\mathbb{R}$ but h is not.

Solution:

(a) Define $F(y) = \sup_{0<t<y} f(t) = \max_{0<t<y} f(t)$ (the latter equality following from the fact that f is continuous on a compact set). Clearly F is non-decreasing. Since F is monotone, F has only discontinuities of the first type. Suppose F is discontinuous at x. Then $F(x-) < F(x)$ or $F(x) < F(x+)$. Assume that $F(x-) < F(x)$. Then for all $s \in (0, x)$, we have $f(s) \leq F(s) \leq F(x-) < F(x)$. Therefore, $f(s) < F(x)$ for all $s \in (0, x)$, a contradiction. Therefore, F is continuous. But then $h = F \circ g$ is a composition of continuous functions, hence continuous.

(b) Let $f(x) = x$ and $g(x) = x^2 + 1$. Then $h(x) = \sup_{0<t<g(x)} f(t) = \sup_{0<t<g(x)} t = g(x)$. But then $h(x) = x^2 + 1$. Suppose that h is uniformly continuous on $\mathbb{R}$. Then for $\epsilon = 1$, there is a $\delta > 0$ such that $|x - y| \leq \delta$ implies $|h(x) - h(y)| < 1$. Choose $y = x + \delta$ for $x > 0$. Then

$$|h(x) - h(y)| = |(x^2 + 1) - ((x + \delta)^2 + 1)| = |-2x\delta - \delta^2| = 2x\delta + \delta^2$$

tends to infinity as $x \to \infty$. But then $|h(x) - h(y)| > 1$, a contradiction. Therefore, h is not uniformly continuous on $\mathbb{R}$.

□

3. Suppose that $f : \mathbb{R} \to \mathbb{R}$ is a differentiable function such that $f'(x+1) = f'(x)$ for all $x \in \mathbb{R}$. Prove that the limit $\lim_{x\to+\infty} \dfrac{f(x)}{x}$ exists and is finite.

Solution: Define $g(x) = f(x+1) - f(x)$. Then $g'(x) = f'(x+1) - f(x) = 0$ since $f'(x+1) = f'(x)$ for all $x \in \mathbb{R}$. But then $g'(x) = 0$ for all $x \in \mathbb{R}$ so that $g(x)$ is constant. Therefore, $f(x+1) = f(x) + c$ for some $c \in \mathbb{R}$. We need show $\lim_{x\to+\infty} \frac{f(x)}{x} = c$. Note that $f(x) = f(x-1) + c = f(x-2) + 2c = \cdots = f(x-n) + nc$ for $x \in [n, n+1]$. Moreover, f is differentiable so that f is continuous on $[0,1]$. Then f is bounded on $[0,1]$, i.e. there is a M such that $|f(y)| \leq M$ for all $y \in [0,1]$. But then $f(x) = f(x-n) + nc \leq M + [x]c$ as $x - n \in [0,1]$. Furthermore, $f(x) = f(x-n) + nc \geq -M + [x]c$. But then we have

$$-\frac{M}{x} + \frac{[x]}{x}c \leq \frac{f(x)}{x} \leq \frac{M}{x} + \frac{[x]}{x}c$$

Taking limits yields $c \leq \lim_{x\to+\infty} \frac{f(x)}{x} \leq c$ so that $\lim_{x\to+\infty} \frac{f(x)}{x} = c$. □

4. Let $f_n : \mathbb{R} \to \mathbb{R}$, $n = 1, 2, \ldots$, be C^1-functions; that is, continuously differentiable functions such that, for all n,

$$|f_n'(x)| \leq \frac{1}{\sqrt{x}} \ \ (0 < x \leq 1) \quad \text{and} \quad \int_0^1 f_n(x)\, dx = 0$$

Prove that the sequence $\{f_n\}$ has a subsequence that converges uniformly on $[0,1]$.

Solution: Consider $|f_n(x) - f_n(y)|$ for $x, y \in [0,1]$ (with $x > y$). Since f is C^1, we have $|f_n(x) - f_n(y)| = |\int_y^x f_n'(t)\, dt|$ by the Fundamental Theorem of Calculus. But

$$|f_n(x) - f_n(y)| = \left|\int_y^x f_n'(t)\, dt\right| \leq \int_y^x |f_n'(t)|\, dt \leq \int_y^x \frac{dt}{\sqrt{t}} = 2|\sqrt{x} - \sqrt{y}| = 2|g(x) - g(y)|$$

where $g(x) = \sqrt{x}$. Since g is uniformly continuous on $[0,1]$, given $\epsilon > 0$, there is $\delta > 0$ such that $|g(x) - g(y)| < \epsilon$ for $|x - y| < \delta$ with $x, y \in [0,1]$. Given $\epsilon > 0$, there is $\delta > 0$ such that for $x, y \in [0,1]$ with $|x - y| < \delta$, we have $|f_n(x) - f_n(y)| < \epsilon$ for all n. But then $\{f_n\}$ is equicontinuous. Since f_n is continuous on $[0,1]$, there is $x_n \in (0,1)$ such that $f_n(x_n) = \int_0^1 f_n(x)\, dx = 0$ by the Mean Value Theorem for Integrals. Then there is $x_n \in (0,1)$ such that $f_n(x_n) = 0$. But then

$$|f_n(x)| = |f_n(x) - 0| = |f_n(x) - f_n(x_n)| \leq 2|\sqrt{x} - \sqrt{x_n}| \leq 4$$

for $x, y \in [0,1]$ and $n \geq 1$. Then $\{f_n\}$ is pointwise bounded. But as $[0,1]$ is compact, $\{f_n\}$ is equicontinuous and pointwise bounded. By the Ascoli-Arzela Theorem, there is a uniformly convergent subsequence $\{f_{n_k}\}$ on $[0,1]$. □

5. Suppose that $\boldsymbol{f} : \mathbb{R}^2 \to \mathbb{R}^2$ is a C^1-mapping with $\det \boldsymbol{f}'(x) > 0$ for all $x \in \mathbb{R}^2$. Assume that $\boldsymbol{f}^{-1}(K)$ is compact whenever $K \subset \mathbb{R}^2$ is compact. Prove that $f(\mathbb{R}^2) = \mathbb{R}^2$.

Solution: Since $\det f'(x) > 0$ for all $\boldsymbol{x} \in \mathbb{R}^2$ and $\boldsymbol{f} \in C^1$, the Inverse Function Theorem applies for all $\boldsymbol{x} \in \mathbb{R}^2$. Then $\boldsymbol{f}$ is an open mapping. But then $U := \boldsymbol{f}(\mathbb{R}^2)$ is open. Suppose that $U \neq \mathbb{R}^2$. Then there is a $y \in \text{Bd } U$ such that $y \notin U$. Then there is a sequence $\{y_n\}$, where $y_n = \boldsymbol{f}(\boldsymbol{x}_n) \in U$, such that $y_n \to y$ for $\boldsymbol{x}_n \in \mathbb{R}^2$. Define $K = \{y_n\} \cup \{y\}$. Now K is compact in $\mathbb{R}^2$ so that $\boldsymbol{f}^{-1}(K)$ is compact. But then $\boldsymbol{x}_n \in \boldsymbol{f}^{-1}(K)$. Then there is a subsequence $\{\boldsymbol{x}_{n_k}\}$ such that $\boldsymbol{x}_{n_k} \to \boldsymbol{x}_0$ as $\boldsymbol{x}_n \in f^{-1}(K)$ is compact. But $\boldsymbol{f}$ is continuous so that $f(\boldsymbol{x}_{n_k}) \to f(\boldsymbol{x}_0)$. Then $y_{n_k} \to y$ showing that $y = f(\boldsymbol{x}_0) \in \boldsymbol{f}(\mathbb{R}^2) = U$. This contradicts the fact that $y \in U$. Therefore, $\boldsymbol{f}(\mathbb{R}^2) = \mathbb{R}^2$. □

6. Let $f : \mathbb{R} \to \mathbb{R}$ be a C^1-function with $f'(x) > 0$ for all $x \in \mathbb{R}$. Suppose that f takes the interval $[0, 1]$ onto itself. Prove that there is a sequence of polynomials $p_n : [0, 1] \to [0, 1]$ such that $p_n \to f$ uniformly on $[0, 1]$ and each p_n is a strictly increasing function on $[0, 1]$.

Solution: Since $'f$ is continuous on $[0, 1]$ by Weierstrass' Theorem, there is a sequence $\{g_n\}$ of polynomials such that the sequence converges uniformly to f' on $[0, 1]$. SO for $\epsilon = c/2$, there is a n_0 such that for $n \geq n_0$, $|g_n(x) - f'(x)| < c/2$. But then for $n \geq n_0$, $g_n(x) \geq f'(x) - c/2 \geq c/2$ since $f'(x) \geq c > 0$ (f is increasing implies $f' > 0$). This shows for $n \geq n_0 g_n(x) \geq c/2 > 0$. Define $h_n(x) = \int_0^x g_n(t)\, dt$. Now $h_n(x)$ is a polynomial such that $h_n(0) = 0$ and $h_n'(x) = g_n(x) > 0$. But then $h_n(x)$ is increasing on $[0, 1]$. Now $f(x) = \int_0^x f'(t)\, dt$.

$$|h_n(x) - f(x)| = \left| \int_0^x g_n(t) - f'(t)\, dt \right| \leq \int_0^x |g_n(t) - f'(t)|\, dt \leq \|g_n - f'\|$$

But then $\|h_n(x) - f(x)\| \leq \|g_n - f'\| \to 0$ as $n \to \infty$ since $\{g_n\}$ converges uniformly to f'. But then $\{h_n\}$ converges uniformly to f on $[0, 1]$. Since f is increasing and onto, $h_n(1) \to f(1) = 1$. Let $P_n(x) = \frac{h_n(x)}{h_n(1)} : [0, 1] \to [0, 1]$. Now $P_n(x)$ is a strictly increasing function. We have

$$P_n(x) - f(x) = \frac{h_n(x) - f(x)}{h_n(1)} + \frac{f(x)}{h_n(1)} - f(x)$$

Now $\left\| \frac{h_n - f}{h_n(1)} \right\| = \frac{\|h_n - f\|}{h_n(1)} \to 0$ as $n \to \infty$.

$$\left\| \frac{f}{h_n(1)} - f \right\| = \left\| \frac{1 - h_n(1)}{h_n(1)}\, f \right\| = \frac{|1 - h_n(1)|}{h_n(1)}\, \|f\| \to 0$$

since $h_n(1) \to 1$. Therefore, $\|P_n(x) - f(x)\| \to 0$ as $n \to \infty$. But then $\{P_n\}$ converges uniformly to f on $[0, 1]$, is strictly increasing on $[0, 1]$, and such that $P_n([0, 1]) = [0, 1]$. □

January 2013

1. Let f_n be a non-negative differentiable functions on $[0,1]$ such that for every x the sequence $f_n'(x)$ is non-increasing, and such that $f_n(0)$ is also non-increasing. Prove that the f_n converge point-wise on $[0,1]$.

Solution: Since f_n is nonnegative, we have f_n is bounded below by 0. We show f_n is decreasing. Define $g(x) := f_n - f_{n+1}$. We have $g'(x) = f_n' - f_{n+1}' \geq 0$ since $\{f_n'\}$ is non-increasing so that g is increasing. Now $g(x) \geq g(0)$ and $g(x) \geq g(0) = f_n(0) - f_{n+1}(0) \geq 0$ as $\{f_n(0)\}$ is non-increasing. But then $f_n(x) \geq f_{n+1}(x)$ for all $x \in [0,1]$. Therefore, $\{f_n\}$ is decreasing and bounded below so that $\{f_n\}$ converges pointwise on $[0,1]$. □

2. Let $(\mathcal{M}, d)$ be a non-empty compact metric space and $f : M \to M$ a continuous mapping such that $d(f^{(n)}(x), f^{(n)}(y)) \to 0$ uniformly in x, y, where $f^{(n)}(x)$ denotes n-fold composition of f with itself (for example, $f^{(3)}(x) = f(f(f(x)))$). Prove that f has a fixed point x, i.e. there exists an $x \in \mathcal{M}$ such that $f(x) = x$.

Solution: First, $d(f^{(n)}(x), f^{(n)}(y)) \to 0$ uniformly implies for all $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that for $n > N$, $d(f^{(n)}(x), f^{(n)}(y)) < \epsilon$ for all $x, y \in M$. Define $x := x_0$ and $y = f^{(p)}(x_0)$. If $n > N$, then $d(f^{(n)}(x_0), f^{(n+p)}(x_0)) < \epsilon$. Then the sequence $\{f^{(n)}(x_0)\}$ is Cauchy. However, M is compact so that it is a complete metric space. Therefore, there exists $x \in M$ such that $f^{(n)}(x_0) \to x$ for some x. As f is continuous, $f(f^{(n)}(x_0)) \to f(x)$ so that $f^{(n+1)}(x_0) \to f(x)$ and $f^{(n+1)}(x_0) \to x$. Therefore, $f(x) = x$, i.e. f has a fixed point. □

3. Let f be a continuous function such that $\lim_{x\to\infty} f(x) = c \in \mathbb{R}$. Prove that for any $\alpha > 0$ we have

$$\lim_{N\to\infty} \frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha f(x)\, dx = c$$

Solution: First, observe

$$\frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha c\, dx = c\, \frac{\alpha+1}{N^{\alpha+1}} \left[\frac{x^{\alpha+1}}{\alpha+1}\right]_0^N = c$$

Therefore, $c = \frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha c\, dx$. Furthermore,

$$\begin{aligned}
\left|\frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha f(x)\, dx - c\right| &= \left|\frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha f(x)\, dx - \frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha c\, dx\right| \\
&= \left|\frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha (f(x) - c)\, dx\right| \\
&\leq \frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha |f(x) - c|\, dx
\end{aligned}$$

Now given $\epsilon > 0$, there is a $N_0 \in \mathbb{N}$ such that if $x > N_0$, $|f(x) - c| < \frac{\epsilon}{2}$. Then

$$\begin{aligned}\left|\frac{\alpha+1}{N^{\alpha+1}}\int_0^N x^\alpha f(x)\,dx - c\right| &\le \frac{\alpha+1}{N^{\alpha+1}}\int_0^N x^\alpha |f(x)-c|\,dx \\ &= \frac{\alpha+1}{N^{\alpha+1}}\int_0^{N_0} x^\alpha |f(x)-c|\,dx + \frac{\alpha+1}{N^{\alpha+1}}\int_{N_0}^N x^\alpha |f(x)-c|\,dx\end{aligned}$$

Now f is continuous on $[0, N_0]$, which is compact, f is bounded on $[0, N_0]$. Suppose $|f(x)| < M$ on $[0, N_0]$. Then

$$\begin{aligned}\left|\frac{\alpha+1}{N^{\alpha+1}}\int_0^N x^\alpha f(x)\,dx - c\right| &\le \frac{\alpha+1}{N^{\alpha+1}}\int_0^{N_0} x^\alpha |f(x)-c|\,dx + \frac{\alpha+1}{N^{\alpha+1}}\int_{N_0}^N x^\alpha |f(x)-c|\,dx \\ &\le \frac{\alpha+1}{N^{\alpha+1}}\,(M+|c|)\,\frac{N_0^{\alpha+1}}{\alpha+1} + \frac{\alpha+1}{N^{\alpha+1}}\,\frac{\epsilon}{2}\,\frac{N^{\alpha+1}}{\alpha+1} \\ &= \frac{(M+|c|)N_0^{\alpha+1}}{N^{\alpha+1}} + \frac{\epsilon}{2}\end{aligned}$$

For $N > (M+|c|)^{1/(\alpha+1)} N_0$, we have

$$\left|\frac{\alpha+1}{N^{\alpha+1}}\int_0^N x^\alpha f(x)\,dx - c\right| \le \frac{\epsilon}{2} + \frac{(M+|c|)\,N_0^{\alpha+1}}{N^{\alpha+1}} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

Therefore, $\lim_{N\to\infty} \frac{\alpha+1}{N^{\alpha+1}} \int_0^N x^\alpha f(x)\,dx = c$. □

4. The Dirichlet function $D(x)$ on $[0,1]$ is the function equal to 1 when x is rational and 0 when x is irrational. Show that $D(x) \notin \mathcal{R}(\alpha)$ for any monotonically increasing non-constant function α. (Recall that $\mathcal{R}(\alpha)$ is the space of functions on $[0,1]$ integrable with respect to α in the Riemann sense.)

Solution: Let $P = \{0 = x_0 < \cdots < x_n = 1\}$ be a partition of $[0,1]$. Note that between any two real numbers there is a rational and irrational number. Every interval of the partition contains a rational and an irrational number so that $M_i = \sup_{x_{i-1}\le x\le x_i} D(x) = 1$ and $m_i = \inf_{x_{i-1}\le x\le x_i} D(x) = 0$ for $1 \le i \le n$. Therefore using the fact that α is nonconstant and monotonically increasing

$$\begin{aligned}U(P, D, \alpha) &= \sum M_i \Delta\alpha_i = \sum \Delta\alpha_i = \alpha(1) - \alpha(0) > 0 \\ L(P, D, \alpha) &= \sum m_i \Delta\alpha_i = 0\end{aligned}$$

Therefore, $\overline{\int} D\,d\alpha = \alpha(1) - \alpha(0) \neq 0 = \underline{\int} D\,d\alpha$. Then $\overline{\int} D\,d\alpha \neq \underline{\int} D\,d\alpha$. Therefore, $D \notin \mathcal{R}(\alpha)$ on $[0,1]$. □

5. Let f be a differentiable function on $\mathbb{R}$ and its derivative f' is continuous there. Show that the functions

$$f_n(x) = n\left(f(x+\frac{1}{n}) - f(x)\right)$$

converge uniformly to f' on any interval $[a,b]$, $-\infty < a < b < \infty$.

Solution: Observe that f is continuous on $[x, x+\frac{1}{n}]$ and differentiable on $(x, x+\frac{1}{n})$. By the Mean Value Theorem, there is a $c \in (x, x+\frac{1}{n})$ such that $f(x+\frac{1}{n}) - f(x) = f'(c)\,\frac{1}{n}$. Then $f_n(x) = n(f(x+\frac{1}{n}) - f(x)) = nf'(c)\,\frac{1}{n} = f'(c)$. Therefore, $f_n(x) = f'(c)$. As f' is uniformly continuous on $[a, b+1]$; that is, given $\epsilon > 0$, there is a $\delta > 0$ such that $|f'(x) - f'(y)| < \epsilon$ for $|x-y| < \delta$ and $x, y \in [a, b+1]$. There is N_0 such that $1/N_0 < \delta$. For $n > N$, $x \in [a,b]$, $c \in [a, b+1]$, we have $|c - x| < \frac{1}{n} < \delta$. Then $|f_n(x) - f'(x)| = |f'(c) - f'(x)| < \epsilon$ for all $x \in [a,b]$ so that f_n converges uniformly to f'. □

6. Is the function $f(x,y) = (x^3 + y^3)^{1/3}$ differentiable at $(0,0)$?

Solution: Suppose f is differentiable at $(0,0)$. Then $D_u f(0,0) = \nabla f(0,0) \cdot u$, where u is a unit vector. Define $u = (u_1, u_2)$, a unit vector. We have

$$D_u f(0,0) = \lim_{t\to 0} \frac{f(tu) - f(0)}{t} = \lim_{t\to 0} \frac{f(tu_1, tu_2)}{t} = \lim_{t\to 0} \frac{t(u_1^3 + u_2^3)^{1/3}}{t} = (u_1^3 + u_2^3)^{1/3}$$

Now we have also

$$\frac{\partial f}{\partial x}(0,0) = \frac{d}{dx} f(x,0)\Big|_{x=0} = 1$$
$$\frac{\partial f}{\partial y}(0,0) = \frac{d}{dy} f(0,y)\Big|_{y=0} = 1$$

But $\nabla f(0,0) \cdot u = f_x(0,0)u_1 + f_y(0,0)u_2 = u_1 + u_2$. Therefore, $D_u f(0,0) \neq \nabla f(0,0) \cdot u$ for all unit vectors u. Therefore, f is not differentiable at $(0,0)$. □

August 2013

1. Let f be a real valued function on $\mathbb{R}$ and suppose that f has three derivatives in an open interval containing the point a. Show

$$\lim_{h\to 0} \frac{f(a+2h) - 2f(a+h) + f(a)}{h^2} = f''(a)$$

and

$$\lim_{h\to 0} \frac{f(a+3h) - 3f(a+2h) + 3f(a+h) - f(a)}{h^3} = f'''(a)$$

Solution: For notational ease, let $f_h = f(a+h)$. Now choose h sufficiently small so that $a+3h$ is in a neighborhood of $f(a)$ that f is differentiable. We apply L'Hôpital's rule.

$$\begin{aligned}
\lim_{h\to 0} \frac{f_{2h} - 2f_h + f_0}{h^2} &\overset{\text{L.H.}}{=} \lim_{h\to 0} \frac{2f'_{2h} - 2f'_h}{2h} \\
&= \lim_{h\to 0} \frac{f'_{2h} - f'_h}{h} \\
&\overset{\text{L.H.}}{=} \lim_{h\to 0} 2f''_{2h} - f''_h \\
&= f''_0
\end{aligned}$$

By the same method,

$$\begin{aligned}
\lim_{h\to 0} \frac{f_{3h} - 3f_{2h} + 3f_h - f_0}{h^3} &\overset{\text{L.H.}}{=} \lim_{h\to 0} \frac{3f'_{3h} - 6f'_{2h} + f'_h}{3h^2} \\
&= \lim_{h\to 0} \frac{f'_{3h} - 2f'_{2h} + f'_h}{h^2} \\
&\overset{\text{L.H.}}{=} \lim_{h\to 0} \frac{3f''_{3h} - 4f''_{2h} + f''_h}{2h} \\
&\overset{\text{L.H.}}{=} \lim_{h\to 0} \frac{9f''_{3h} - 8f''_{2h} + f''_h}{2} \\
&= \frac{2f'''_0}{2} \\
&= f'''_0
\end{aligned}$$

□

2. Let the sequence x_n be given by

$$x_n = \prod_{k=1}^{n} \left(1 - \frac{1}{2^k}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right) \cdots \left(1 - \frac{1}{2^n}\right)$$

Prove that the sequence x_n converges and that the limit is **not** 0.

Solution: To see convergence, we know that $0 < 1 - \frac{1}{2^k} < 1$ for $k \in \mathbb{N}$, so that $0 < x_n < 1$ for all $n \in \mathbb{N}$. This shows that the sequence is bounded. Furthermore, $x_1 = 1/2$, $x_2 = 3/8$, so $x_2 < x_1$. Now assume that the sequence is decreasing for $n = 1, 2, 3, \cdots, N$. Now

$$x_{N+1} = \prod_{k=1}^{N+1} 1 - \frac{1}{2^k} = \left(1 - \frac{1}{2^{N+1}}\right) \prod_{k=1}^{N} 1 - \frac{1}{2^k} < \prod_{k=1}^{N} 1 - \frac{1}{2^k} = x_N$$

as $0 < \left(1 - \frac{1}{2^{N+1}}\right) < 1$. Therefore, the sequence x_n is decreasing. By the Monotone Convergence Theorem, the sequence x_n converges.

To see the limit is nonzero, consider

$$\ln(x_n) = \ln\left(\prod_{k=1}^{n} 1 - \frac{1}{2^k}\right) = \sum_{k=1}^{n} \ln(1 - 1/2^k)$$

note that $1 - 1/2^k > 0$. Now we consider the series $\sum_{k=1}^{\infty} \ln(1 - 1/2^k)$. The series $\sum_{k=1}^{\infty} \frac{-1}{2^k}$ converges. Furthermore, $\ln(1 - 1/2^k) < 0$ for all k as $1 - 1/2^k < 1 < e$. Observe

$$\lim_{k\to\infty} \frac{\ln(1 - 1/2^k)}{\frac{-1}{2^k}} \overset{\text{L.H.}}{=} \lim_{k\to\infty} \frac{\frac{\ln 2 \cdot 2^{-k}}{1 - \frac{1}{2^k}}}{\ln 2 \cdot 2^{-k}} = \lim_{k\to\infty} \frac{1}{1 - \frac{1}{2^k}} = 1$$

so by the Limit Comparison Test, $\sum_{k=1}^{\infty} \ln(1 - 1/2^k)$ converges, say to x. Then we have

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} e^{\ln(x_n)} = \lim_{n\to\infty} e^{\sum_{k=1}^{n} \ln(1-1/2^k)} = e^{\lim_{n\to\infty} \sum_{k=1}^{n} \ln(1-1/2^k)} = e^x > 0$$

for all $x \in \mathbb{R}$. □

3. Let f be a real valued function on $\mathbb{R}$ that satisfies $\{x\colon |f(x)| \geq \epsilon\}$ is compact for all $\epsilon > 0$. Prove or provide a counterexample to the statement: f has a limit as $|x| \to \infty$.

Solution: Let $M_n = \{x \mid |f(x)| \geq \frac{1}{n}\}$. By assumption, this set is compact for all $n \in \mathbb{N}$ with $\epsilon = 1/n$. As $M_n \subset \mathbb{R}$ is compact, it is closed and bounded by Heine-Borel. So there exists a $t_n \in \mathbb{R}$ such that $|x| \leq t_n$ for all $x \in M_n$. But this implies that $|f(x)| < \frac{1}{n}$ for all $|x| > t_n$. As this holds for all $n \in \mathbb{N}$, it must be that $\lim_{|x|\to\infty} f(x) = 0$. □

4. Let $f : [0, 1] \to \mathbb{R}$ be a continuous function. For $n = 1, 2, \ldots$. Let $\alpha_n(x) = x^n$. Prove that the limit

$$\lim_{n\to\infty} \int_0^1 f \, d\alpha_n$$

exists and determine its value.

Solution: Observe for all n, α_n is monotonic increasing on $[0,1]$ and $\alpha_n'(x) = nx^{n-1}$ is continuous and hence integrable on $[0,1]$. As $f(x)$ is continuous on $[0,1]$, it is bounded. Furthermore as $f(x)$ is continuous on $[0,1]$, it is integrable on $[0,1]$. Therefore, we know that for each $n \in \mathbb{N}$

$$\int_0^1 f(x)\ d\alpha_n(x) = \int_0^1 f(x)\alpha_n'(x)\ dx = n\int_0^1 x^{n-1}f(x)\ dx$$

For convenience, we shall work with

$$\int_0^1 f(x)\ d\alpha_{n+1}(x) = \int_0^1 f(x)\alpha_{n+1}'(x)\ dx = (n+1)\int_0^1 x^n f(x)\ dx$$

Let $p_n(x)$ be a polynomial, i.e. $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Observe that

$$\begin{aligned}
\int_0^1 x^n p_{n_0}(x)\ dx &= \int_0^1 a_{n_0}x^{n+n_0} + a_{n_0-1}x^{n+n_0-1} + \cdots + a_1 x^{n+1} + a_0 x^n\ dx \\
&= a_{n_0}\frac{x^{n+n_0+1}}{n+n_0+1} + a_{n_0-1}\frac{x^{n+n_0}}{n+n_0} + \cdots + a_0\frac{x^{n+1}}{n+1}\Bigg|_0^1 \\
&= \frac{a_{n_0}}{n+n_0+1} + \frac{a_{n_0-1}}{n+n_0} + \cdots + \frac{a_0}{n+1}
\end{aligned}$$

But then this shows that

$$\begin{aligned}
\lim_{n\to\infty}(n+1)\int_0^1 x^n f(x)\ dx &= \lim_{n\to\infty}(n+1)\left(\frac{a_{n_0}}{n+n_0+1} + \frac{a_{n_0-1}}{n+n_0} + \cdots + \frac{a_0}{n+1}\right) \\
&= \lim_{n\to\infty} a_{n_0}\frac{n+1}{n+n_0+1} + a_{n_0-1}\frac{n+1}{n+n_0} + \cdots + a_0\frac{n+1}{n+1} \\
&= a_{n_0} + a_{n_0-1} + \cdots + a_1 + a_0 \\
&= \sum_{i=0}^{n_0} a_i \\
&= p_{n_0}(1)
\end{aligned}$$

So that the result holds for any polynomial. Now as $f(x)$ is continuous on the compact interval $[0,1]$, the Stone-Weierstrass Theorem gives a sequence of polynomials $\{p_n(x)\}$ such that $\{p_n(x)\}$ converges to $f(x)$ on $[0,1]$ uniformly. Then given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|p_n(x) - f(x)| < \epsilon$ for all $n > N$ and $x \in [0,1]$. But the above shows

$\lim_{n\to\infty}(n+1)\int_0^1 x^n p_n(x)\,dx = p_n(1)$ for all $p_n(x) \in \{p_m(x)\}$. Then

$$\begin{aligned}\left|(n+1)\int_0^1 x^n f(x)\,dx - (n+1)\int_0^1 x^n p_{n_0}(x)\,dx\right| &= \left|(n+1)\int_0^1 x^n(f(x)-p_{n_0}(x))\,dx\right| \\ &< \left|(n+1)\int_0^1 x^n\epsilon\,dx\right| \\ &= \left|\epsilon(n+1)\int_0^1 x^n\,dx\right| \\ &= \left|\epsilon\frac{n+1}{n+1}\right| \\ &= \epsilon\end{aligned}$$

for all $n_0 > N$. But then $\lim_{n\to\infty}(n+1)\int_0^1 x^n f(x)\,dx = \lim_{n\to\infty}(n+1)\int_0^1 x^n p_{n_0}(x)\,dx$. However, we have shown this converges to $p_n(1)$ for all n. But we know also that $\lim_{n\to\infty} p_n(x) = f(x)$. Then $\lim_{n\to\infty} p_n(1) = f(1)$, as desired. This shows that

$$\lim_{n\to\infty}\int_0^1 f\,d\alpha_n = f(1)$$

□

5. Let $f : [1,\infty) \to \mathbb{R}$ be a continuous function such that $\lim_{x\to\infty} f(x) = 0$. Prove that for every $\epsilon > 0$ there exists an integer n and real numbers $c_0, \ldots, c_n$ such that

$$\left|f(x) - \sum_{k=0}^{n} c_k e^{-kx}\right| < \epsilon \text{ for all } x \in [1,\infty)$$

Solution: Let $t = e^{-x}$ for $x \geq 1$. Observe $t \in (0, \frac{1}{e}]$. Now $x = -\log t$. Define

$$g(t) = \begin{cases} f(-\log t), & 0 < t \leq \dfrac{1}{e} \\ 0, & t = 0 \end{cases}$$

Clearly, g is continuous on $[0, 1/e]$ since f is continuous, $-\log t$ is continuous, and $\lim_{t\downarrow 0} g(t) = \lim_{x\to+\infty} f(x) = 0 = g(0)$. Therefore by Weierstrass' Theorem, there is a sequence $\{p_n(t)\}$ is a sequence of polynomials converging uniformly to $g(t)$. That is, there are c_k such that

$$\left|g(t) - \sum_{k=0}^{n} c_k t^k\right| < \epsilon$$

for all $t \in [0, 1/e]$. But then

$$\left|f(x) - \sum_{k=0}^{n} c_k e^{-kx}\right| < \epsilon$$

for all $x \in [1, \infty)$. □

6. Consider the mapping $\boldsymbol{f} = (f_1, f_2, f_3)$ of $\mathbb{R}^3$ into $\mathbb{R}^3$ given by

$$\begin{aligned} f_1(x_1, x_2, x_3) &= x_1 \\ f_2(x_1, x_2, x_3) &= x_1^2 + x_2 \\ f_3(x_1, x_2, x_3) &= x_1 + x_2^2 + x_3^3 \end{aligned}$$

(a) Is $\boldsymbol{f}$ continuously differentiable? Why or why not?

(b) Find all points at which $\boldsymbol{f}$ satisfies the assumptions of the Inverse Function Theorem.

(c) Is $\boldsymbol{f}$ injective?

Solution:

(a) The function $f(x_1, x_2, x_3)$ has Jacobian

$$\begin{pmatrix} 1 & 0 & 0 \\ 2x_1 & 1 & 0 \\ 1 & 2x_2 & 3x_3^2 \end{pmatrix}$$

each of the partials of f are continuously on all of $\mathbb{R}^3$ as they are given by polynomials. Therefore, $f(x_1, x_2, x_3)$ is continuously differentiable.

(b) The above Jacobian has determinant $3x_3^2$ which is zero only when $x_3 = 0$. Therefore, the above determinant above is invertible for all (x_1, x_2, x_3) for which $x_3 \neq 0$.

(c) Suppose that $f(a, b, c) = f(x, y, z)$. Then the first coordinate gives $a = x$. Using this in the second coordinate, we have $a^2 + b = a^2 + y$ so that $b = y$. Using $a = x$ and $b = y$ in the third coordinate yields $a + b^2 + c^3 = a + b^2 + z^3$ so that $c^3 = z^3$ which implies $c = z$. Therefore, f must be an injective function.

□

January 2014

1. Show that the following limit exists and find it:

$$\lim_{n\to+\infty}\left(\frac{(3n)!}{(n!)^3}\right)^{1/n}.$$

Solution: Let $c_n = \frac{(3n)!}{(n!)^3}$. It is clear that $c_n > 0$. We know that

$$\liminf \frac{c_{n+1}}{c_n} \leq \liminf \sqrt[n]{c_n}$$
$$\limsup \sqrt[n]{c_n} \leq \limsup \frac{c_{n+1}}{c_n}$$

But

$$\begin{aligned}\lim_{n\to\infty}\frac{c_{n+1}}{c_n} &= \lim_{n\to\infty}\frac{(3n+3)!}{((n+1)!)^3}\cdot\frac{(n!)^3}{(3n)!}\\ &= \lim_{n\to\infty}\frac{(3n+3)(3n+2)(3n+1)}{(n+1)^3}\\ &= 27\end{aligned}$$

But then $\liminf \frac{c_{n+1}}{c_n} = 27$ and $\limsup \frac{c_{n+1}}{c_n} = 27$. But then

$$27 = \liminf \frac{c_{n+1}}{c_n} \leq \liminf c_n^{1/n} \leq \left(\frac{(3n)!}{(n!)^3}\right)^{1/n} \leq \limsup c_n^{1/n} \leq \limsup \frac{c_{n+1}}{c_n} = 27$$

<u>OR</u>

We know from Stirling's formula

$$\lim_{n\to\infty}\frac{\ln(an)!}{n\ln n} = 1$$

so that

$$\lim_{n\to\infty}\frac{\ln(3n)!}{3n\ln n} = 1$$

Then

$$\left(\frac{(3n)!}{(n!)^3}\right)^{1/n}$$
$$e^{\ln\left(\frac{(3n)!}{(n!)^3}\right)^{1/n}}$$
$$e^{\frac{1}{n}\left(\frac{(3n)!}{(n!)^3}\right)}$$
$$e^{\frac{1}{n}(\ln(3n)!-\ln(n!)^3)}$$
$$e^{\frac{\ln(3n)!}{n}-\frac{\ln(n!)^3}{n}}$$

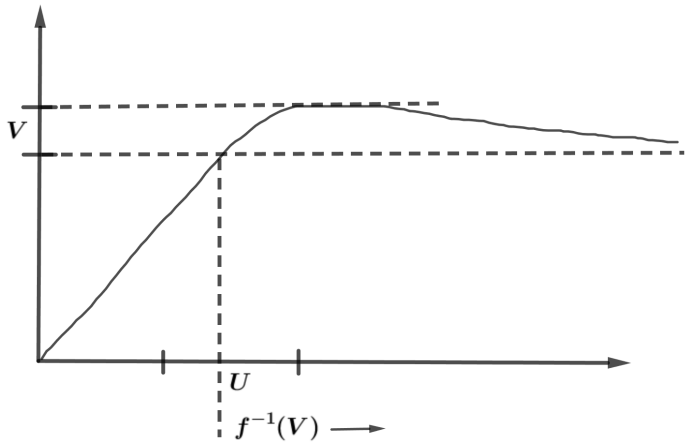
Then from the continuity of e^x, we know

$$\begin{aligned}
\lim_{n\to\infty}\left(\frac{(3n)!}{(n!)^3}\right)^{1/n} &= \lim_{n\to\infty} e^{\frac{\ln(3n)!}{n}-\frac{\ln(n!)^3}{n}} \\
&= e^{\lim_{n\to\infty}\frac{\ln(3n)!}{n}-\frac{\ln(n!)^3}{n}} \\
&= e^{3\ln(3n)-3\ln 3} \\
&= e^{3(\ln 3n-\ln n)} \\
&= e^{3\ln\frac{3n}{n}} \\
&= e^{3\ln 3} \\
&= e^{\ln 27} \\
&= 27
\end{aligned}$$

□

2. Let $f : X \to Y$ be a continuous function, where X, Y are metric spaces and X is compact. Assume that $y_0 \in Y$ is a point which has a unique preimage $x_0 \in X$, i.e. $f^{-1}(y_0) = \{x_0\}$. Prove that for every open neighborhood U of x_0 in X there exists an open neighborhood V of y_0 in Y such that $f^{-1}(V) \subset U$. Give an example to show that this conclusion is false if X is not compact.

Solution: Suppose there is a $U \subseteq X$ is open with $x_0 \in U$ such that for all $V \subseteq Y$ with $y_0 \in V$, we have $f^{-1}(V) \not\subseteq U$. Take $V = B_{1/n}(y_0)$. Since $f^{-1}(V) \not\subseteq U$, there is a sequence $\{x_n\}$ such that $x_n \notin U$ for all n. Since $x_n \in f^{-1}(V)$, $f(x_n) \in V = B_{1/n}(y_0)$. Therefore, $f(x_n) \to y_0$. Now $x_n \in X \setminus U$ and $X \setminus U$ is closed since U is open. But $X \setminus U$ is compact since it is a closed subset of the compact set X. But $\{x_n\} \in X \setminus U$ is compact so that there is a subsequence $\{x_{n_k}\}$ such that $x_{n_k} \to z \in X \setminus U$. Then $f(x_{n_k}) \to f(z) = y_0$ since f is continuous. Therefore, $x_{n_k} \to f^{-1}(y_0) = x_0$. But then $x_{n_k} \to x_0 \in U$, a contradiction as $x_{n_k} \to z \in Z \setminus U$. Then for all $U \subseteq X$ such that $x_0 \in U$, there is a $V \subseteq Y$ with $y_0 \in V$ with $f^{-1}(V) \subseteq U$. To see this is false if X is not compact, consider the following:



□

3. Let $f : \mathbb{R} \to \mathbb{R}$ be a differentiable function such that $\lim_{x\to+\infty} f'(x) = 1$, and let $a \in \mathbb{R}$. Prove that the following limit exist and find it:

$$\lim_{x\to+\infty} \frac{e^{f(x+a)}}{e^{f(x)}}$$

Solution: If $a = 0$, the limit is trivially 1. Assume $a \neq 0$.

$$\begin{aligned}\frac{e^{f(x+a)}}{e^{f(x)}} &= e^{f(x+a)-f(x)} \\ &= \left(e^{f(x+a)-f(x)}\right)^{a/a} \\ &= \left(e^{\frac{f(x+a)-f(x)}{a}}\right)^{a}\end{aligned}$$

Then using the continuity of e^x, we know

$$\lim_{x\to\infty} \frac{e^{f(x+a)}}{e^{f(x)}} = \lim_{x\to\infty} \left(e^{\frac{f(x+a)-f(x)}{a}}\right)^{a} = \left(e^{\lim_{x\to\infty} \frac{f(x+a)-f(x)}{a}}\right)^{a}$$

Let $L = \lim_{x\to\infty} f'(x)$. Then for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that for $x \geq N$, $|f'(x) - L| < \epsilon$. Then for $x > N$,

$$\begin{aligned}\left|\frac{f(x+a)-f(x)}{a} - L\right| &= \left|\frac{1}{a}\int_x^{x+a} f'(t) - L\, dt\right| \\ &\leq \frac{1}{a}\int_x^{x+a} |f'(t) - L|\, dt \\ &\leq \frac{1}{a}\int_x^{x+a} \epsilon = \epsilon\end{aligned}$$

So $\lim_{x\to\infty} \frac{f(x+a)-f(x)}{a} = L$ (in our case $L = 1$). Then

$$\lim_{x\to\infty} \frac{e^{f(x+a)}}{e^{f(x)}} = \left(e^{\lim_{x\to\infty} \frac{f(x+a)-f(x)}{a}}\right)^a = e^{a\lim_{x\to\infty} f'(x)} = e^{aL} = e^a$$

OR

By the Mean Value Theorem on $[x, x+a]$, there is a $c_a \in (x, x+a)$ such that $f(x+a) - f(x) = af'(c_a)$. But then $f'(c_a) = \frac{f(x+a)-f(x)}{a}$. But then $L = \lim_{x\to\infty} f'(c_a) = \lim_{x\to\infty} \frac{f(x+a)-f(x)}{a}$. Therefore, $aL = \lim_{x\to\infty} f(x+a) - f(x)$. Therefore by the continuity of e^x, we have $\lim_{x\to+\infty} \frac{e^{f(x+a)}}{e^{f(x)}} = e^{aL}$.

OR

As f is continuous on $[x, x+a]$ and differentiable on $(x, x+a)$ by the Mean Value Theorem, there is a $c_x \in (x, x+a)$ such that $f(x+a) - f(x) = af'(c_x)$. As $c_x \to +\infty$ as $x \to +\infty$,

$$\lim_{x\to+\infty} \frac{e^{f(x+a)}}{e^{f(x)}} = \lim_{c_x\to+\infty} e^{af'(c_x)} = e^a$$

as $\lim_{x\to+\infty} f'(x) = 1$. Therefore, $\lim_{x\to+\infty} \frac{e^{f(x+a)}}{e^{f(x)}} = e^a$ exists. □

4. For each $s \in [0,1]$ there is a function $f_s(x)$ defined for $x \in [a,b]$ and $f_s \in \mathcal{R}(\alpha)$ on $[a,b]$, where α is a monotonically increasing function on $[a,b]$. Suppose that

$$f_{s_j} \to f_{\frac{1}{2}} \text{ uniformly on } [a,b] \text{ as } j \to \infty$$

for any sequence $\{s_j\}_{j=1}^{\infty}$ from $[0,1]$ that converges to $\frac{1}{2}$. Show that

$$\lim_{s\to\frac{1}{2}} \int_a^b f_s(x)\, d\alpha(x) = \int_a^b f_{\frac{1}{2}}(x)\, d\alpha(x).$$

Solution: Define $F(s) = \int_a^b f_s(x)\, d\alpha(x)$, $s \in [0,1]$. We need show that $\lim_{s\to 1/2} F(s) = F(\frac{1}{2})$. Suppose that $\lim_{s\to 1/2} F(s) \neq F(\frac{1}{2})$. Then there is $s_j \in [0,1] \setminus \{\frac{1}{2}\}$ such that $s_j \to \frac{1}{2}$ but $F(s_j) \not\to F(\frac{1}{2})$. But as $f_{s_j} \to f_{1/2}$ and $f_{s_j} \in \mathcal{R}(\alpha)$, we have $\lim_{j\to\infty} \int_a^b f_{s_j}\, d\alpha = \int_a^b f_{1/2}\, d\alpha$, i.e. $F(s_j) \to F(1/2)$, a contradiction. Therefore, $\lim_{s\to 1/2} F(s) = F(1/2)$. Then $\lim_{s\to 1/2} \int_a^b f_s(x)\, d\alpha(x) = \int_a^b f_{1/2}(x)\, d\alpha(x)$. □

5. Let f be a real valued continuous function on $[0,1]$, with $\|f\| \leq 1$ (sup norm less than or equal 1) and $f(0) = 0$. Show that the sequence of powers of f, $\{f^n\}_{n=1}^{\infty}$ is equicontinuous

if and only if $\|f\| < 1$.

Solution:
$\Longleftarrow$: Assume $\|f\| < 1$. We need show $\{f^n\}$ is equicontinuous. Now $\|f\| < 1$ so that $\sup_{x\in[0,1]}\{|f(x)|\} < 1$ so that $|f(x)| \leq A < 1$ for some A. Therefore, $|f^n(x)| \leq A^n \to 0$ as $A \in [0,1)$. But then $f^n(x)$ converges to 0 on $[0,1]$ (a compact interval). Now as f is continuous, f^n is continuous. But then $\{f^n\}$ is equicontinuous.

$\Longrightarrow$: Assume $\{f^n\}$ is equicontinuous. We need show $\|f\| < 1$. Suppose that $\|f\| = 1$. Then $\sup_{x\in[0,1]}\{|f(x)|\} = 1$. So there exists $x_0 \in [0,1]$ such that $|f(x_0)| = 1$. Moreover, $|f^n(x)| \leq 1$ for all $x \in [0,1]$ and for all n. Since $\{f^n\}$ is uniformly bounded (hence pointwise bounded), $[0,1]$ is compact, and $\{f^n\}$ is equicontinuous, by the Ascoli-Arzela Theorem, there exists a subsequence f^{n_k} converging to g for some function $g(x)$ on $[0,1]$. But as f^{n_k} are continuous and $f^n \to g$, g is continuous. Now $|f^{n_k}| \to |g|$ and

$$|g| = \begin{cases} 0, & |f(x)| < 1 \\ 1, & |f(x)| = 1 \end{cases}$$

But then $|g|$ is not continuous, a contradiction. Therefore, $\|f\| < 1$. □

6. Let $\boldsymbol{f} = (f_1, f_2)$ from $\mathbb{R}^2$ to $\mathbb{R}^2$ be given by $f_1(x,y) = 2x + |x| - |x+1|$, $f_2(x,y) = (y-1)^3$.

(a) At which points (x,y) does the Inverse Function Theorem provide the existence of a C^1 inverse in a neighborhood? Check the conditions of the theorem!

(b) At which points is $\boldsymbol{f}$ not invertible?

Solution:

(a) If $x \leq -1$, $f_1(x,y) = 2x - x + x + 1 = 2x + 1$. If $-1 < x \leq 0$, then $f_1(x,y) = 2x - x - (x+1) = -1$. If $x > 0$, $f_1(x,y) = 2x + x - (x = 1) = 2x - 1$. Therefore,

$$f_1(x,y) = \begin{cases} 2x+1, & x \leq -1 \\ -1, & -1 < x \leq 0 \\ 2x-1, & x > 0 \end{cases}$$

Then f_1 is continuous but clearly not differentiable at $x = -1, 0$. Furthermore, $f_2 \in C^1$ for all x. Then $f \in C'(U)$, where $u \in \mathbb{R}^2 \setminus \{(x,y) \colon x = -1, 0\}$. We have

$$J_f(x,y) = \det \begin{bmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} \end{bmatrix} = \det \begin{bmatrix} \frac{\partial f_1}{\partial x} & 0 \\ 0 & 3(y-1)^2 \end{bmatrix} = 3(y-1)^2 \frac{\partial f_1}{\partial x} = \begin{cases} 6(y-1)^2, & x \leq -1 \\ 0, & -1 < x \leq 0 \\ 6(y-1)^2, & x > 0 \end{cases}$$

Therefore, the Inverse Function Theorem applies for all (x, y) with $x < -1$ or $x > 0$, and $y \neq 1$.

(b) f is not invertible at $(x, y) \in \mathbb{R}^2$ such that $-1 \leq x \leq 0$ or $y = 1$.

□

August 2014

1. Suppose f is positive, twice differentiable, and log-concave, i.e., the graph of the composite function $\ln(f)$ is everywhere concave down. Prove that the function

$$g(x) = f(x)\left(\frac{1}{f(x)}\right)'$$

is non-decreasing.

Solution: As $f(x) > 0$ is differentiable, we know $\frac{1}{f(x)}$ is differentiable.

$$\left(\frac{1}{f(x)}\right)' = \frac{-f'(x)}{f(x)^2}$$

So

$$g(x) = f(x)\left(\frac{1}{f(x)}\right)' = \frac{-f'(x)}{f(x)}$$

As $f(x) > 0$ and $f(x)$ is twice-differentiable, since the quotient of differentiable functions is differentiable, $g(x)$ is differentiable. It suffices to show that $g'(x) > 0$.

$$g'(x) = \left(\frac{-f'(x)}{f(x)}\right)' = \frac{-f''(x)f(x) + f'(x)^2}{f(x)^2}$$

As $f(x)^2 > 0$, it suffices to show $-f''(x)f(x) + f'(x)^2 > 0$. We know $\ln f$ is concave down as $f(x)$ is log concave. So

$$(\ln f(x))' = \frac{f'(x)}{f(x)}$$
$$(\ln f(x))'' = \left(\frac{f'(x)}{f(x)}\right)' = \frac{f''(x)f(x) - f(x)^2}{f(x)^2} < 0$$

so $f''(x)f(x) - f'(x)^2 < 0$ so $f'(x)^2 - f''(x)f(x) > 0$. □

2. Let X be a compact metric space with metric d, and let $x_0 \in X$. Prove that $K = \{d(x_0, x) \colon x \in X\}$ is a closed subset of the real numbers.

Solution: First, we prove a lemma.

Lemma: If $d : X \times X \to \mathbb{R}$ is a metric then d is continuous.

Proof: Let (a,b) be an open set in $\mathbb{R}$. Let $(x,y) \in d^{-1}((a,b))$ (if this is empty it is trivial but this cannot be so for a metric). Then $a < d(x,y) < b$. Choose $\epsilon > 0$ such that $B_{2\epsilon}(d(x,y)) \subset (a,b)$. We look at $B_\epsilon(x) \times B_\epsilon(y)$. Suppose $(\overline{x},\overline{y}) \in B_\epsilon(x) \times B_\epsilon(y)$. Then

$$d(\overline{x},\overline{y}) \leq d(\overline{x},x) + d(x,y) + d(y,\overline{y}) < d(x,y) + 2\epsilon$$
$$d(x,y) \leq d(x,\overline{x}) + d(\overline{x},\overline{y}) + d(\overline{y},y) < d(\overline{x},\overline{y}) + 2\epsilon$$

So

$$d(\overline{x},\overline{y}) < d(x,y) + 2\epsilon$$
$$d(x,y) < d(\overline{x},\overline{y}) + 2\epsilon$$

But then the choice of ϵ shows

$$a < d(x,y) - 2\epsilon < d(\overline{x},\overline{y}) < d(x,y) + 2\epsilon < b$$

So $B_\epsilon(x) \times B_\epsilon(y) \subset d^{-1}((a,b))$, so d is continuous.

Now $X \times X$ is compact, as it is the finite product of compact spaces. Indeed, $\{x_0\} \times X$ is compact as it is the finite product of compact spaces. But then K is the image of a compact set under a continuous map, hence compact. But then K is a compact set in a Hausdorff space. Therefore, K is closed. □

3. Let A be a subset of the natural numbers whose elements have been arranged into a sequence $a_1, a_2, \ldots$. Call the set *petite* if it is finite, or if it is infinite and

$$\sum_{j=1}^{\infty} \frac{1}{a_j} < \infty.$$

A set which is not petite is called *husky*. Prove that the complement of a petite set is husky, but that the complement of a husky set is not necessarily petite.

Solution: Note that as $a_n \in \mathbb{N}$ for all n, then $a_n > 0$. So if $\sum a_n$ converges it does so absolutely and any arrangement of its terms converges. Note also that $\sum \frac{1}{n}$ diverges and that this also implies that $\sum_{n \geq m} \frac{1}{n}$ diverges for all $m \in \mathbb{N}$. If A is finite, let $n_0 \in \mathbb{N}$ such that $a_n < n_0$ for all $n \in N$. Then A^C is infinite for it must contain all $n \in N$ such that $n > n_0$. We know

$$\sum_{a \in A} \frac{1}{a} + \sum_{a \in A^C} \frac{1}{a} = \sum_{n=1}^{\infty} \frac{1}{n}$$

Now as $\sum_{a \in A} \frac{1}{a}$ converges (being a finite sum), it must be that $\sum_{a \in A^C} \frac{1}{a}$ diverges for otherwise the above equality would then show that the harmonic series converges. Therefore,

A^C is husky. Now suppose that A is infinite and petite. Suppose A^C were finite, then $\sum_{a\in A^C}\frac{1}{a}$ converges as it is a finite sum but then once again

$$\sum_{a\in A}\frac{1}{a}+\sum_{a\in A^C}\frac{1}{a}=\sum_{n=1}^{\infty}\frac{1}{n}$$

show that the harmonic series converges, impossible. Therefore, it must be that A^C is infinite. Assume to the contrary that $\sum_{a\in A^C}\frac{1}{a}$ converges. But then yet again,

$$\sum_{a\in A}\frac{1}{a}+\sum_{a\in A^C}\frac{1}{a}=\sum_{n=1}^{\infty}\frac{1}{n}$$

yields a contradiction for the same reason. Therefore, A^C is husky. To see that the complement of a husky set need not be petite, take $A=\{2,4,6,\cdots\}$. We know that A is infinite and $\sum_{a\in A}\frac{1}{a}$ diverges as

$$\sum_{a\in A}\frac{1}{a}=\frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{n}$$

However, $A^C=\{1,3,5,\cdots\}$ and

$$\sum_{a\in A^C}\frac{1}{a}=\frac{1}{1}+\frac{1}{3}+\frac{1}{5}+\cdots=\frac{1}{1}+\frac{1}{2(1)+1}+\frac{1}{2(2)+1}+\cdots>\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots=\sum_{a\in A}\frac{1}{a}$$

so that $\sum_{a\in A^C}\frac{1}{a}$ diverges. Therefore, A^C is not petite. □

4. Suppose that $\{f_n\}$, $n=1,2,\ldots$, are continuous functions defined on the interval $[0,1]$, and

$$\lim_{n\to\infty}\int_0^1 f_n(x)\,dx=0$$

Suppose also that for each n, the function f_n is increasing, and $f_n(0)=0$. Prove that f_n converges to 0 uniformly on the interval $[0,1/2]$.

Solution: We need show that given $\epsilon>0$, there is a $N\in\mathbb{N}$ such that $|f_n(x)-0|=|f_n(x)|<\epsilon$ for all $x\in[0,1/2]$ and $n>N$. As $f_n(0)=0$ and f_n is increasing, we know $f_n\geq 0$ on the interval $[0,1]$ for all n. Moreover, $f_n(1/2)\geq f_n(x)$ for all $x\in[0,1/2]$ and $f_n(1/2)\leq f(x)$ for all $x\in[1/2,1]$. Now $\int f_n\,dx\geq 0$ for all n as $f_n\geq 0$ for all n. We have also

$$\int_0^1 f_n(x)\,dx=\int_0^{1/2} f_n(x)\,dx+\int_{1/2}^1 f_n(x)\,dx\geq\int_{1/2}^1 f_n(x)\,dx\geq 0$$

Now as $\int_0^1 f_n\,dx\to 0$, this implies $\int_{1/2}^1 f_n\,dx\to 0$. But we have

$$\int_{1/2}^1 f_n(x)\,dx\geq f_n(1/2)\left(1-\frac{1}{2}\right)=\frac{f_n(1/2)}{2}\geq 0$$

for all n. This implies that $\lim f_n(1/2) = 0$; that is, given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|f_n(1/2)| < \epsilon$. However, $|f_n(x)| \leq |f_n(1/2)| < \epsilon$ for $n > N$ and all $x \in [0, 1/2]$. □

5. Let $f : [0,1] \to \mathbb{R}$ be a continuous function. Prove that there exists a sequence of polynomials, $\{p_n\}$ such that $p_n \to f$ uniformly on $[0,1]$, and $p_n(x) > p_{n+1}(x)$ for every $x \in [0,1]$. and every $n = 1, 2, \ldots$.

Solution: Let x_n be any nonconstant nonzero increasing sequence converging to 0. It is then clear that $x_n < 0$. Take $A_n = \frac{x_{n-1}+x_n}{2}$ and $B_n = \frac{x_n - x_{n-1}}{2}$. Observe that $A_n < 0$, $B_n > 0$, and both $A_n \to 0, B_n \to 0$ as $n \to \infty$. Furthermore, $A_n + B_n = x_{n-1}$ and $A_n - B_n = x_n$. As $f(x)$ is continuous, so too is $f(x) - A_n$ continuous on the compact interval $[0,1]$. By Stone-Weierstrass, there is a polynomial $p_n(t)$ such that $|p_n(x) - (f(x) - A_n)| < B_n$. Therefore, $f(x) - x_n = f(x) - A_n - B_n < p_n(x) < f(x) - A_n + B_n = f(x) - x_n$. In particular, $f(x) - x_{n+1} < p_n(x) < f(x) - x_n$. Now as $|p_n(x) - f(x)| \leq |p_n(x) - (f(x) - A_n)| + |A_n| \to 0$, we have $p_n(x)$ converges to $f(x)$ uniformly on $[0,1]$. □

6. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuously differentiable nondecreasing function. Define $\boldsymbol{g} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$\boldsymbol{g}(x_1, x_2) = (x_2 + f(2x_1 + x_2), 2x_1 + f(2x_1 + x_2))$$

Show that $\boldsymbol{g}$ satisfies the conditions of the Inverse Function Theorem at every point of $\mathbb{R}^2$.

Solution: The function $g(x_1, x_2)$ has Jacobian

$$\begin{pmatrix} 2f'(2x_1 + x_2) & 1 + f'(2x_1 + x_2) \\ 2 + 2f'(2x_1 + x_2) & f'(2x_1 + x_2) \end{pmatrix}$$

Notice that each of these partials are continuous as f is a continuously differentiable function (meaning that f' is continuous). Therefore, we know that $g(x_1, x_2)$ is C' on $\mathbb{R}^2$. Observe that the above has determinant

$$2f'^2(2x_1 + x_2) - (1 + f'(2x_1 + x_2))(2 + 2f'(2x_1 + x_2)) = -2 - 4f'(2x_1 + x_2)$$

So that the determinant is only zero when $-2 - 4f'(2x_1 + x_2) = 0$ so that $f'(2x_1 + x_2) = \frac{-1}{2}$. However as f is a nondecreasing function, $f'(x) \geq 0$ so that this is impossible. But then g' is invertible for all $(x_1, x_2) \in \mathbb{R}^2$. Therefore, $g(x_1, x_2)$ satisfies the conditions of the Inverse Function Theorem everywhere on $\mathbb{R}^2$. □

January 2015

1.

(i) If $x > 0$ and $y > 0$ show that $x + \dfrac{1}{y^2 x} \geq \dfrac{2}{y}$.

(ii) Suppose that the series $\displaystyle\sum_{n=1}^{\infty} a_n$ converges and $a_n > 0$ for all $n \geq 1$. Show that the series $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2 a_n}$ diverges.

Solution:

(i) This follows from

$$\begin{aligned} (xy-1)^2 &\geq 0 \\ x^2y^2 - 2xy + 1 &\geq 0 \\ x^2y^2 + 1 &\geq 2xy \\ x + \frac{1}{y^2 x} &\geq \frac{2}{y} \end{aligned}$$

where in the last line we divided by xy^2, using the fact that $xy^2 \neq 0$ as $x, y > 0$.

(ii) We know that $a_n > 0$ and $n > 0$ for $n \in \mathbb{N}$. By the previous part, we know that

$$\sum_{n=1}^{\infty} \left(a_n + \frac{1}{n^2 a_n} \right) \geq \sum_{n=1}^{\infty} \frac{2}{n}$$

Suppose that $\sum_{n=1}^{\infty} \frac{1}{n^2 a_n}$ converges. Then the left side can be split as

$$\sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty} \frac{1}{n^2 a_n} \geq 2 \sum_{n=1}^{\infty} \frac{1}{n}$$

But then the left side is a sum of convergent series, hence convergent, greater than a divergent series, a contradiction. Therefore, it must be that $\sum_{n=1}^{\infty} \frac{1}{n^2 a_n}$ converges.

□

2. Let $f : [0, +\infty) \to \mathbb{R}$ be a continuous function such that $\lim_{x \to +\infty} (f(x) - x) = 0$. Prove or provide a counterexample to the statement: f is uniformly continuous on $[0, +\infty)$.

Solution: We know from $\lim_{x\to\infty}(f(x)-x)=0$, given $\epsilon>0$ there is an $N\in\mathbb{N}$ such that $|f(x)-x|<\epsilon$ for $x>N$. As $f(x)$ is continuous on $[0,\infty)$, it is continuous on $[0,N]$. But then $f(x)$ is uniformly continuous on $[0,N]$. Given $\epsilon>0$, there is a $\delta_1>0$ such that $|f(x)-f(y)|<\epsilon$ for $|x-y|<\delta_1$, where $x,y\in[0,N]$. Now given $\epsilon>0$, choose $\delta_2=\epsilon/3$. For $x,y\in(N,\infty)$ with $|x-y|=|y-x|<\delta_2$, we have

$$\begin{aligned}|f(x)-f(y)| &= |f(x)-x+x-f(y)| \le |f(x)-x|+|f(y)-x| \\ &= |f(x)-x|+|f(y)-x+y-y| \le |f(x)-x|+|f(y)-y|+|y-x| \\ &< \frac{\epsilon}{3}+\frac{\epsilon}{3}+\frac{\epsilon}{3}=\epsilon\end{aligned}$$

But then given $\epsilon>0$, taking $\delta=\min\{\delta_1,\delta_2\}$, we have $|f(x)-f(y)|<\epsilon$ for $x,y\in[0,\infty)$ with $|x-y|<\delta$ so that $f(x)$ is uniformly continuous on $[0,\infty)$. □

3. Let $f,g:\mathbb{R}\to\mathbb{R}$ be functions such that f is differentiable and for every $x,h\in\mathbb{R}$ one has $f(x+h)-f(x-h)=2hg(x)$. Prove that f is a polynomial of degree at most 2.

Solution: As $f(x)$ is differentiable with respect to x and $2hg(x)=f(x+h)-f(x-h)$, we know that $g(x)$ is differentiable with respect to x. Moreover, we have

$$\begin{aligned}2hg(x) &= f(x+h)-f(x-h) \\ 2hg(x) &= f(x+h)-f(x)+f(x)-f(x-h) \\ 2g(x) &= \frac{f(x+h)-f(x)}{h}-\frac{f(x-h)-f(x)}{h}\end{aligned}$$

so that as $h\to 0$,

$$2g(x)=\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}-\frac{f(x-h)-f(x)}{h}=f'(x)-(-f'(x))=2f'(x).$$

This shows that $g(x)=f'(x)$. As $g(x)$ is differentiable, this shows that $f(x)$ is twice differentiable and that $g'(x)=f''(x)$. All that remains is to show that $f''(x)=g'(x)$ is constant. Differentiating $f(x+h)-f(x-h)=2hg(x)$ twice with respect to h yields $f''(x+h)-f''(x-h)=0$. But this is true for all x,h so that f'' is constant. Therefore, $f''(x)$ must be a polynomial of at most degree 2. □

4.

(a) Give an example of a differentiable function $f:\mathbb{R}\to\mathbb{R}$ whose derivative f' is not continuous. Prove that your example works.

(b) Let f be as in Part (a). If $f'(0)<2<f'(1)$, prove that $f'(x)=2$ for some $x\in[0,1]$.

Solution:

(a) Let $f(x)$ be given by

$$f(x) = \begin{cases} x^2 \sin\left(\frac{1}{x}\right), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

It is clear this function is continuous as $x^2 \sin(1/x)$ is continuous at all nonzero points and $|x^2 \sin(1/x)| \leq |x^2|$ forces $\lim_{x\to 0} x^2 \sin(1/x)$ to have limit 0 at the origin by the Squeeze Theorem. But then $f(x)$ is continuous. Furthermore, $f(x)$ is clearly differentiable at all nonzero values. In addition,

$$\lim_{h\to 0} \frac{f(0+h) - f(0)}{h} = \lim_{h\to 0} \frac{h^2 \sin\left(\frac{1}{h}\right) - 0}{h} = \lim_{h\to 0} h \sin(1/h) = 0$$

where the last equality follow from the Sequence Theorem with $|h \sin(1/h)| \leq |h|$. Then $f(x)$ is differentiable at 0 - hence everywhere on $\mathbb{R}$ - with $f'(x) = 0$. The derivative of $f(x)$ is given by

$$f(x) = \begin{cases} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) & x \neq 0 \\ 0, & x = 0 \end{cases}$$

We have shown $f'(0) = 0$. But note that $\left|2x \sin\left(\frac{1}{x}\right)\right| \leq |2x|$ has limit 0 as $x \to 0$ by Squeeze Theorem. But then

$$\lim_{|x|\to 0} f(x) = \lim_{|x|\to 0} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) = -\lim_{|x|\to 0} \cos\left(\frac{1}{x}\right)$$

Now $f'(0) = 0$ but taking $x_n = \frac{1}{2\pi n}$ and the above calculation shows that $\lim_{n\to\infty} f'(x_n) = 1$. But then $f'(x)$ is not continuous at $x = 0$. In fact, we can produce a differentiable function whose derivative is discontinuous at $x = x_0, x_1, \cdots, x_n$ via

$$f(x) = \begin{cases} \left(\prod_{i=0}^{n} (x - x_i)^2\right) \sin\left(\frac{1}{\prod_{i=0}^{n}(x-x_i)}\right), & x \notin \{x_0, x_1, \ldots, x_n\} \\ 0, & \text{otherwise} \end{cases}$$

(b) Let $a = f'(0)$ and $b = f'(1)$. By assumption, $a < 2 < b$. Let $g(t) = f(t) - 2t$. Observe that $g(t)$ is differentiable and $g'(t) = f'(t) - 2$. As $g(t)$ is differentiable on $[0,1]$, $g(t)$ is continuous on $[0,1]$. Observe that $g'(0) = f'(0) - 2 = a - 2 < 0$ while $g'(1) = f'(1) - 2 = b - 2 > 0$. But then clearly $g(t)$ has a minimum on $[0,1]$ at some value $t_0 \in [0,1]$. But at t_0, it must be the case that $g'(t_0) = 0$. However, this is $0 = g'(t_0) = f'(t_0) - 2$ so that $f'(t_0) = 2$, as desired.

□

5. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. Show that

$$\lim_{n\to\infty}(n+1)\int_0^1 x^n f(x)\,dx = f(1)$$

Solution: Let $p_n(x)$ be a polynomial, i.e. $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Observe that

$$\begin{aligned}\int_0^1 x^n p_{n_0}(x)\,dx &= \int_0^1 a_{n_0}x^{n+n_0} + a_{n_0-1}x^{n+n_0-1} + \cdots + a_1 x^{n+1} + a_0 x^n\,dx \\ &= a_{n_0}\frac{x^{n+n_0+1}}{n+n_0+1} + a_{n_0-1}\frac{x^{n+n_0}}{n+n_0} + \cdots + a_0\frac{x^{n+1}}{n+1}\Bigg|_0^1 \\ &= \frac{a_{n_0}}{n+n_0+1} + \frac{a_{n_0-1}}{n+n_0} + \cdots + \frac{a_0}{n+1}\end{aligned}$$

But then this shows that

$$\begin{aligned}\lim_{n\to\infty}(n+1)\int_0^1 x^n f(x)\,dx &= \lim_{n\to\infty}(n+1)\left(\frac{a_{n_0}}{n+n_0+1} + \frac{a_{n_0-1}}{n+n_0} + \cdots + \frac{a_0}{n+1}\right) \\ &= \lim_{n\to\infty} a_{n_0}\frac{n+1}{n+n_0+1} + a_{n_0-1}\frac{n+1}{n+n_0} + \cdots + a_0\frac{n+1}{n+1} \\ &= a_{n_0} + a_{n_0-1} + \cdots + a_1 + a_0 \\ &= \sum_{i=0}^{n_0} a_i \\ &= p_{n_0}(1)\end{aligned}$$

So that the result holds for any polynomial. Now as $f(x)$ is continuous on the compact interval $[0,1]$, the Stone-Weierstrass Theorem gives a sequence of polynomials $\{p_n(x)\}$ such that $\{p_n(x)\}$ converges to $f(x)$ on $[0,1]$ uniformly. Then given $\epsilon > 0$, there is a $N \in \mathbb{N}$ such that $|p_n(x) - f(x)| < \epsilon$ for all $n > N$ and $x \in [0,1]$. But the above shows $\lim_{n\to\infty}(n+1)\int_0^1 x^n p_n(x)\,dx = p_n(1)$ for all $p_n(x) \in \{p_m(x)\}$. Then

$$\begin{aligned}\left|(n+1)\int_0^1 x^n f(x)\,dx - (n+1)\int_0^1 x^n p_{n_0}(x)\,dx\right| &= \left|(n+1)\int_0^1 x^n(f(x) - p_{n_0}(x))\,dx\right| \\ &< \left|(n+1)\int_0^1 x^n\epsilon\,dx\right| \\ &= \left|\epsilon(n+1)\int_0^1 x^n\,dx\right| \\ &= \left|\epsilon\frac{n+1}{n+1}\right| \\ &= \epsilon\end{aligned}$$

for all $n_0 > N$. But then $\lim_{n\to\infty}(n+1)\int_0^1 x^n f(x)\ dx = \lim_{n\to\infty}(n+1)\int_0^1 x^n p_{n_0}(x)\ dx$. However, we have shown this converges to $p_n(1)$ for all n. But we know also that $\lim_{n\to\infty} p_n(x) = f(x)$. Then $\lim_{n\to\infty} p_n(1) = f(1)$, as desired. □

6. The Arzelá-Ascoli Theorem asserts that a sequence $\{f_n\}$ of continuous real valued functions on a metric space Ω is precompact (i.e. has a uniformly convergent subsequence) if

(i) Ω is compact.

(ii) $\sup\{|f_n(x)|\colon x \in \Omega \text{ and } n \in \mathbb{N}\} < \infty$,

(iii) the sequence is equicontinuous.

Give examples of sequences which are not precompact such that: (i) and (ii) holds but (iii) fails; (i) and (iii) hold but (ii) fails; (ii) and (iii) hold but (i) fails. Take Ω to be a subset of the real line.

Solution:

(i),(ii) $\not\to$ (iii) Let $\Omega = [0,1]$ and take $f_n(x) = x^n$. It is clear that $\sup_\Omega f_n(x) = 1$ for all n and that Ω is compact. However, the sequence of functions $\{f_n(x)\}$ is not equicontinuous. If the sequence were equicontinuous, there would be a $\delta > 0$ such that $0 < \delta < 1$ and $|x^n - y^n| < \frac{1}{2}$ for all $n \in \mathbb{N}$ and $x, y \in (1-\delta, 1]$. As $t^n \to 0$ as $n \to \infty$ if $0 < t < 1$, we can choose n sufficiently large so that $\left(1 - \frac{\delta}{2}\right)^n < \frac{1}{2}$. Choose $x = 1$ and $y = 1 - \frac{\delta}{2}$. But then

$$|x^n - y^n| = \left|1 - \left(1 - \frac{\delta}{2}\right)^n\right| > 1 - \frac{1}{2} > \frac{1}{2}$$

But this contradicts the equicontinuity of the sequence. Therefore, $\{f_n\}$ is not equicontinuous.

(i),(iii) $\not\to$ (ii) Take $\Omega = [0,1]$ and $f_n(x) = n$ for all $x \in [0,1]$. The series of functions $\{f_n\}$ is clearly equicontinuous but $\sup\{|f_n(x)| \mid x \in \Omega \wedge n \in \mathbb{N}\}$ is clearly infinite.

(ii),(iii) $\not\to$ (i) Take $\Omega = \mathbb{R}$ and choose

$$f_n(x) = \begin{cases} 0, & x \le n \\ x - n, & n < x \le n+1 \\ 1, & x > n+1 \end{cases}$$

Observe that $\sup f_n(x) = 1$ for all $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Furthermore, the sequence of functions $\{f_n(x)\}$ is equicontinuous as $\|f_n(x) - f_m(y)\| = 1$ for $n, m \in \mathbb{N}$, $n \neq m$, and $x, y \in \mathbb{R}$.

□

August 2015

1. Assume f_n is a sequence of functions mapping R into $[0,1]$. Prove there is a subsequence n_k along which $f_{n_k}(q)$ converges for all rational q.

Solution: The collection $\{f_n(q)\}$ is a sequence in a compact metric space $[0,1]$. Then there is a convergent subsequence of this sequence which converges, n_k. But then $f_{n_k}(q)$ converges for all $q \in \mathbb{Q}$. □

2. Prove that

$$\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\ln n\right)$$

exists.

Solution: Let $s_n = \sum_{k=1}^{n}\frac{1}{k} - \ln n$. The sequence s_n is decreasing as

$$s_n - s_{n-1} = \frac{1}{n} + \ln(n-1) - \ln(n) = \frac{1}{n} - \ln\left(1-\frac{1}{n}\right)$$

However, $\frac{d}{dx}\ln(1-x) = \frac{1}{1-x} < 0$ for $x \in \mathbb{N}$ so that $\ln(1-x)$ is concave. But then $\ln(1-x)$ lies below its tangent at $x=0$, which is $-x$. Taking $x = 1/n$ gives $\ln(1-1/n) \leq \frac{-1}{n}$. But then $s_n - s_{n-1} < 0$ for all $n \in \mathbb{N}$. But s_n is bounded below by 0 as

$$\sum_{k=1}^{n}\frac{1}{k} > \int_1^{n+1}\frac{dx}{x}\,dx = \ln(n+1) > \ln n$$

as $\ln n$ is increasing and $\ln n \geq 0$ for $n \in \mathbb{N}$. But then the sequence s_n converges by the Monotone Convergence Theorem. □

3. Is

$$\int_1^{\infty}\frac{\sin x}{x}\,dx$$

a convergent integral?

Solution: Integration by parts yields

$$\int_1^{\infty}\frac{\sin x}{x}\,dx = \frac{-\cos x}{x}\bigg|_1^{\infty} - \int_1^{\infty}\frac{\cos x}{x^2}\,dx = \cos 1 - \int_1^{\infty}\frac{\cos x}{x^2}$$

But observe that

$$\left|\int_1^{\infty}\frac{\cos x}{x^2}\,dx\right| < \int_1^{\infty}\left|\frac{\cos x}{x^2}\right| < \int_1^{\infty}\frac{dx}{x^2} < \infty$$

so that the integral $\int_1^\infty \frac{\cos x}{x}\, dx$ converges. But then the original integral converges. □

4. If $p_k \geq 0$ and $\sum_{k=1}^\infty p_k = 1$, show that

$$\left(\sum_{k=1}^\infty k p_k\right)^2 \leq \sum_{k=1}^\infty k^2 p_k.$$

Let $a_k = k\sqrt{p_k}$ and $b_k = \sqrt{p_k}$. By the Cauchy-Schwartz Inequality (in the case where the sequences are entirely real),

$$\left|\sum_{k=1}^n a_k b_k\right|^2 \leq \sum_{k=1}^n |a_k|^2 \sum_{k=1}^n |b_k|^2$$

But using the fact these sequences are nonnegative and , this is precisely

$$\left(\sum_{k=1}^n k p_k\right)^2 \leq \sum_{k=1}^n k^2 p_k \sum_{k=1}^n p_k$$

Then taking the limit as $n \to \infty$ and using the fact that $\sum_{k=1}^\infty p_k = 1$, we have

$$\left(\sum_{k=1}^\infty k p_k\right)^2 \leq \sum_{k=1}^\infty k^2 p_k \sum_{k=1}^\infty p_k = \sum_{k=1}^\infty k^2 p_k$$

□

5. Let $\{f_n\}$ be equicontinuous on the compact set K. Assume that $\{f_n\}$ converges pointwise. Prove that $\{f_n\}$ converges uniformly on K.

Solution: Suppose that $f_n \to f$ pointwise on K. As the set $\{f_n\}$ is equicontinuous, given $\epsilon_1 > 0$, there is a $\delta > 0$ such that $|f_n(x) - f_n(y)| < \epsilon_1/3$ for all $x, y \in K$ with $|x - y| < \delta$ and all $f_k \in \{f_n\}$. The set $\{B(x, \delta)\}$, where $\delta > 0$, is an open covering of K. Therefore, there is a finite cover of this covering. That is, there are $x_1, x_2, \ldots, x_n$ such that $\{B(x_i, \delta)\}$ is an open covering of K. As f_n converges to f pointwise, given $\epsilon_2 > 0$ and $x \in K$, there is a $N \in \mathbb{N}$ such that $|f_n(x) - f(x)| < \epsilon_2/3$ for all $n > N$. In particular, $|f_n(x_i) - f(x_i)| < \epsilon_2/3$ for all $n > N$. But then given $\epsilon > 0$, choose $\epsilon' = \min\{\epsilon, \epsilon_1, \epsilon_2\}$. Then let δ be as given as above. Note that $|f_n(x) - f(x)| = |f_n(x) - f(x) + f(x_i) - f(x_i)|$ so that

$$|f_n(x) - f(x)| \leq |f_n(x) - f_n(x_i)| + |f_n(x_i) - f(x_i)| + |f(x_i) - f(x)| < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$$

for all $x \in B(x_i, \delta)$. But each $x \in K$ is in some $B(x_i, \delta)$ for some i so that $\{f_n\}$ converges uniformly to f on K. □

6. Let

$$f(x) = \begin{cases} x + 2x^2 \sin(1/x), & x \neq 0 \\ 0, & x = 0 \end{cases}$$

with $f : \mathbb{R} \to \mathbb{R}$.

(a) Show that $f'(0) = 1$. Show that f' is not continuous at $x = 0$.

(b) Write $y = f(x)$, what does the Inverse Function Theorem say or not say about the inverse of f in a neighborhood of $y = 0$? Explain.

(c) Show that f is not 1-1 in any neighborhood of $x = 0$.

Solution:

(a)

$$\frac{f(0+h) - f(0)}{(0+h) - 0} = \frac{f(h) - f(0)}{h} = \frac{h + 2h^2 \sin(1/h) - 0}{h} = 1 + 2h \sin(1/h)$$

But we have

$$\lim_{h \to 0} h \sin(1/h) = \lim_{h \to 0} \frac{\sin(1/h)}{\frac{1}{h}} = \lim_{h \to \infty} \frac{\sin h}{h} = 0$$

Therefore,

$$\lim_{h \to 0} \frac{f(0+h) - f(0)}{(0+h) - 0} = \lim_{h \to 0} 1 + 2h \sin(1/h) = 1$$

However for $x \neq 0$, $f'(x) = 1 + 4x \sin(1/x) - 2\cos(1/x)$. Taken $x_n = \frac{1}{2n\pi}$, observe that $x_n \to 0$ as $n \to \infty$ and we have

$$f'(x_n) = 1 + \frac{2\sin(2n\pi)}{n\pi} - 2\cos(2n\pi) = -1$$

But as $f'(0) = 1$, $f'(x)$ is not continuous at $x = 0$.

(b) The Inverse Function Theorem fails to give any statement about an inverse of $f(x)$ for any open set containing the origin as f need be a C' mapping but $f'(x)$ is not continuous about the origin, despite the fact that $f'(0) \neq 0$. However for any open set not containing the origin, $f'(x) = 1 + 4x \sin(1/x) - 2\cos(1/x)$ is continuous. Therefore for any other open interval, E, containing an x_0 such that $f(x_0) = 0$ and $f'(x_0) \neq 0$, the Inverse Function Theorem gives an inverse $g(x) \in C'(E)$.

(c) In any neighborhood of the origin, E, $x_n = \frac{1}{2n\pi}$ and $x_m = \frac{1}{(2m+1)\pi}$ are in E for some $n, m \in \mathbb{N}$. However, observe that

$$f'(x_n) = 1 + \frac{2\sin(2n\pi)}{n\pi} - 2\cos(2n\pi) = -1 < 0$$
$$f'() = 1 + \frac{2\sin((2m+1)\pi)}{(2m+1)\pi} - 2\cos((2m+1)\pi) = 3 > 0$$

so that $f(x)$ cannot be one-to-one on any neighborhood of the origin.

□

January 2016

1. Let $E \subset \mathbb{R}$ be a nonempty set.

(a) What does it mean to say that E has an upper bound?

(b) When E has an upper bound define $\sup E$, the supremum of E.

(c) Give an example of a bounded set E such that $\sup E \notin E$.

(d) If E has an upper bound prove that there is a sequence $\{x_n\}$, $x_n \in E$, such that $\lim_{n\to\infty} x_n = \sup E$.

Solution:

(a) E has an upper bound if there exists a $x \in \mathbb{R}$ such that $e \leq x$ for all $e \in E$. If $y \in \mathbb{R}$ is such a number such that $e \leq y$ for all $e \in E$, we say that y is an upper bound for E.

(b) Suppose E is bounded above. If $s \in \mathbb{R}$ is an upper bound of E such that if $x < s$ then x is not an upper bound of E, we say that s is the supremum of E and denote it $\sup E$.

(c) Consider $E = (0, 1) \subset \mathbb{R}$. Clearly, $e \leq 1$ for all $e \in E$ so that 1 is an upper bound of E. Clearly, no $s \in \mathbb{R}$ with $s < 0$ is an upper bound for E. If $0 < s < 1$, then $s < \frac{s+1}{2} < 1$ is an element of E and therefore s is not an upper bound of E. Then $\sup E = 1 \notin E$.

(d) Since $E \subset \mathbb{R}$ has an upper bound, $\sup E$ exists. Define $s = \sup E$. Now consider $K_n := E \cap [s - 1/n, s]$ for $n \in \mathbb{N}$. If $K_n = E \cap [s - 1/n, s] = \emptyset$, then $s - 1/n < s$ is an upper bound for E, contradicting the fact that $s = \sup E$. Therefore, there is a $e_n \in K_n$ for every $n \in \mathbb{N}$. The sequence $\{e_n\}_{n\in\mathbb{N}}$ converges to $s = \sup E$ as $|e_n - s| \leq \frac{1}{n} \to 0$ as $n \to \infty$.

□

2. Let f be a real valued function defined on a metric space X with distance $d(x, y)$, $x, y \in X$. Prove or disprove the following assertions.

(a) If f is uniformly continuous on X and if $\{x_n\}$, $x_n \in X$, is a Cauchy sequence, then $\{f(x_n)\}$ is Cauchy.

(b) If f is continuous on X and if $\{x_n\}$, $x_n \in X$, is a Cauchy sequence, then $\{f(x_n)\}$ is Cauchy.

Solution:

(a) The statement is true. Let $\epsilon > 0$ be given. Using the uniform continuity of f, choose $\delta > 0$ such that $|f(x) - f(y)| < |x - y|$ for all $|x - y| < \delta$. Using the fact that $\{x_n\}$ is Cauchy, choose $N \in \mathbb{N}$ such that $|x_n - x_m| < \delta$ for $n, m > N$. Then choosing $\delta = \epsilon$, we have $|f(x_n) - f(x_m)| < |x_n - x_m| < \epsilon$ for $n, m > N$. Therefore, $\{f(x_n)\}$ is Cauchy.

(b) The statement is false. Let $X = (0, 1)$ with the usual metric topology on $\mathbb{R}$ and $f(x) = \frac{1}{x}$. Clearly, f is continuous on X. Consider the sequence $\left\{\frac{1}{n}\right\}_{n\in\mathbb{N}}$. Since $\frac{1}{n} \to 0$ is convergent, the sequence is Cauchy. However, $|f(1/n) - f(1/m)| = |n - m| \geq 1$ for all $n \neq m$, where $n, m \in \mathbb{N}$. But then $\{f(x_n)\}$ cannot be a Cauchy sequence.

□

3. Let f be a real valued continuous function on the interval $[0, 1]$.

(a) If $0 < p < 1$ and $f(x) = x^p \sin(x^{1-p})$, $x \in (0, 1]$, compute (the one-sided derivative) $f'(0)$.

(b) Give an example of an f with $f'(x)$ uniformly bounded on $(0, 1]$ such that $f'(0)$ does not exist.

(c) Suppose $f'(x)$ is uniformly bounded and nondecreasing for $x \in (0, 1]$. Prove $f'(0) = \lim_{x\to 0} f'(x)$.

Solution:

(a) First, observe $f(0) = 0$. Recall $\lim_{x\to 0} \frac{\sin x}{x} = 1$ so that both the left and right hand limits at 0 exist. Now

$$f'(0) := \lim_{h\to 0^+} \frac{f(0+h) - f(0)}{(0+h) - h} = \lim_{h\to 0^+} \frac{h^p \sin(h^{1-p})}{h} = \lim_{h\to 0^+} h^{p-1} \sin(h^{1-p}) = \lim_{h\to 0^+} \frac{\sin(h^{1-p})}{h^{1-p}} = 1$$

(b)

4. Suppose a non-negative function f has maximum equal to 1 and vanishes on a dense set of points in $[0, 1]$. Let β be a nondecreasing continuous function such that $\beta(0) = 0$ and $\beta(1) = 1$. Show that any number $0 < \alpha < 1$ can be obtained as the value of some Riemann sum for the integral $\int_0^1 f \, d\beta$.

5. Let $\mathcal{F}$ be an equicontinuous family of non-negative continuous functions on a metric (M, d). Let S be dense in M and suppose that for each $x \in S$ we have $f(x) = 0$ for some $f \in \mathcal{F}$. Prove that for any $y \in M$ we have $\inf\{f(y) : f \in \mathcal{F}\} = 0$.

6. Let f and g be C^1 real-valued functions such that $f(0) = g(0) = 0$ and $f'(0) = g'(0) = 1$. Show that for any $\epsilon > 0$ there are numbers x, y such that $|x| + |y| < \epsilon$ and $f(x) = g(y) > 0$. Hint: Consider the mapping $F(x, y) = (f(x), g(y))$.

May 2016

1.

(i) Give an example of a sequence of real numbers $\{a_n\}_{n\geq 1}$ such that the series $\displaystyle\sum_{n=1}^{\infty} a_n$ converges, but the series $\displaystyle\sum_{n=1}^{\infty} a_n^2$ diverges.

(ii) If $a_n \geq 0$ for all $n \geq 1$ and the series $\sum_{n=1}^{\infty} a_n$ converges show that the series $\displaystyle\sum_{n=1}^{\infty} a_n^2$ must converge.

Solution:

(i) Consider the sequence $\left\{\dfrac{(-1)^n}{\sqrt{n}}\right\}_{n\in\mathbb{N}}$. The series $\sum_{n=1}^{\infty} \frac{(-1)^n}{\sqrt{n}}$ converges by the Alternating Series Test: $\lim_{n\to\infty} \frac{1}{\sqrt{n}} = 0$ and the sequence $\{1/\sqrt{n}\}$ is decreasing ($\sqrt{x}$ is an increasing function so $\sqrt{n} < \sqrt{n+1}$ so that $\frac{1}{\sqrt{n+1}} < \sqrt{n}$). However, $\left(\frac{(-1)^n}{\sqrt{n}}\right)^2 = \frac{1}{n}$ for all $n \in \mathbb{N}$ and the series $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

(ii) Suppose $\sum_{n=1}^{\infty} a_n$ converges and denote the sum L. Then $L^2 = L \cdot L = \left(\sum_{n=1}^{\infty} a_n\right)\left(\sum_{n=1}^{\infty} a_n\right) = \left(\sum_{n=1}^{\infty} a_n\right)^2$. Moreover, it follows immediately by induction that

$$0 \sum_{n=1}^{N} a_n^2 \leq \left(\sum_{n=1}^{N} a_n\right)^2$$

for all $N \geq 1$ (the left inequality follows from the fact $a_n \geq 0$). Therefore,

$$0 \lim_{N\to\infty} \sum_{n=1}^{N} a_n^2 \leq \lim_{N\to\infty} \left(\sum_{n=1}^{N} a_n\right)^2 = L^2$$

Therefore, $\left\{\sum_{n=1}^{N} a_n^2\right\}_{N\in\mathbb{N}}$ is an increasing sequence which is bounded above. Therefore, $\sum_{n=1}^{\infty} a_n^2$ converges.

□

2. Let X, Y be metric spaces and $f : X \to Y$ be a continuous function such that for every compact $K \subset Y$, $f^{-1}(K)$ is a compact subset of X. If $F \subset X$ is closed, prove that $f(F)$ is closed in Y.

Solution:

3. Let $f, g : \mathbb{R} \to (0, +\infty)$ be differentiable functions such that $g'(x) > 0$ for all x, $\lim_{x\to+\infty} g(x) = +\infty$, and $\lim_{x\to+\infty} \frac{f'(x)}{g'(x)} = L$ for some number $L > 0$. Show that $\lim_{x\to+\infty} \frac{\log f(x)}{\log g(x)} = 1$.

4. Let $f : [0,1] \to \mathbb{R}$ be an integrable function. Prove that there exists $a \in (0,1)$ such that $\int_0^a |f(x)|\, dx \leq \int_a^1 |f(x)|\, dx$.

5. Let K be a compact subset of a metric space X. Given a bounded sequence $\{x_n\}$ in X, define $f_n(x) = d(x, x_n) - d(x, x_1)$ for $n = 1, 2, \ldots$. Prove that there exists a subsequence $\{f_{n_k}\}$ that converges uniformly on K.

6. Suppose $f : \mathbb{R} \to \mathbb{R}$ is a continuously differentiable function such that $f(0) = 0$ and $f(1) = 1$. Prove that there exists a point in $\mathbb{R}^2$ where the map

$$\boldsymbol{F}(x_1, x_2) = (x_1 + x_2^3, f(x_1) + x_2)$$

does not satisfy the assumptions of the Inverse Function Theorem.

August 2016

1. Consider the following proposition: *Every bounded continuous real-valued function f on $\mathbb{R}$ attains its maximum.* The following argument which attempts to prove this has an error. (a) Find where the error occurs and (b) provide a counterexample, with details, to show that the argument indeed fails at that point:

Let $M = \sup\{f(x) : x \in \mathbb{R}\}$, and let $x^*, x_n \in \mathbb{R}$ such that $x_n \to x^*$ and $f(x_n) \to M$. Since f is continuous, $f(x_n) \to f(x^*)$, which implies $f(x^*) = M$. Hence, x^* is where f attains its maximum.

2. Prove: there exists $c > 0$ and continuous functions f, g on $(-c, c)$ such that $f(0) = g(0) = 0$ and

$$\sin(f(z)) + \cos(g(z)) = z^2 + 1, \text{ and}$$
$$(f(z))^2 + 2e^{2g(z)} = 2\cos z$$

3. Let f be continuously differentiable, and suppose that $f(0) < -1$, $f(1) > 0$, and $f(2) < 0$. Prove that for each $c \in [0, 1]$ there exists $x_c \in (0, 2)$ such that $f'(x_c) = c$,

4. Let (X, d) be a metric space. Prove or provide a counterexample:

(a) The intersection of finitely many dense subsets of X is dense.

(b) The intersection of finitely many open dense subsets of X is open and dense.

5. Let f, g be continuous functions on $\mathbb{R}$ such that f is differentiable everywhere and let $f(1) = 0$. Prove that fg is differentiable at 1.

Solution: Since $f(x)$ is differentiable at 1, we know that

$$\lim_{h \to 0} \frac{f(1+h) - f(1)}{h} = f'(1)$$

Moreover since $g(x)$ is continuous at 1, $\lim_{h\to 0} g(1+h) = g(1 + \lim_{h\to 0} h) = g(1)$. Then

we have

$$\begin{aligned}
(fg)'(1) &:= \lim_{h\to 0} \frac{f(1+h)g(1+h) - f(1)g(1)}{h} \\
&= \lim_{h\to 0} \frac{f(1+h)g(1+h) - 0\cdot g(1)}{h} \\
&= \lim_{h\to 0} \frac{f(1+h)g(1+h)}{h} \\
&= \lim_{h\to 0} \frac{f(1+h)g(1+h) - hg(1+h) + hg(1+h)}{h} \\
&= \lim_{h\to 0} \left[\frac{f(1+h)g(1+h) - hg(1+h)}{h} + \frac{hg(1+h)}{h}\right] \\
&= \lim_{h\to 0} \left[g(1+h)\ \frac{f(1+h) - h}{h} + g(1+h)\right] \\
&= \lim_{h\to 0} \left[g(1+h)\ \frac{f(1+h) - 0}{h} - \frac{h}{h} + g(1+h)\right] \\
&= \lim_{h\to 0} \left[g(1+h)\ \frac{f(1+h) - f(1)}{h} - 1 + g(1+h)\right] \\
&= g(1)f'(1) + g(1) - 1 \\
&= g(1)\big(f'(1) + 1\big) - 1
\end{aligned}$$

□

6. Let (f_n) be a sequence of functions on $[0,1]$ with continuous first and second derivatives, such that for all $n \geq 1$,

$$1 \leq f_n(0) \leq 2, \quad 3 \leq f_n'(0) \leq 4, \quad \sup_{0\leq x\leq 1} |f_n''(x)| \leq 12$$

Prove that (f_n) has a subsequence which converges uniformly on $[0,1]$.

May 2017

1. Let $f : \mathbb{Q} \to \mathbb{R}$ where $\mathbb{Q}$ is the set of all rational numbers.

(a) If f is uniformly continuous prove it has an extension to a continuous function $F : \mathbb{R} \to \mathbb{R}$, i.e. there exists a continuous function $F : \mathbb{R} \to \mathbb{R}$ such that $f(q) = F(q)$ for all $q \in \mathbb{Q}$.

(b) Give an example of a continuous $f : \mathbb{Q} \to \mathbb{R}$ that has no continuous extension $F : \mathbb{R} \to \mathbb{R}$.

2. Let X denote the collection of all bounded functions $f : \mathbb{R} \to \mathbb{R}$. For $f, g \in X$ define

$$d(f,g) = \sup\{|f(x) - g(x)| \colon x \in \mathbb{R}\}$$

Then (X, d) is a metric space. Let

$$E = \{f \in X \colon \text{ there exists } K \text{ such that } f(x) = 0 \text{ for all } x > K\}.$$

Find the closure of E in X.

3. For $p \geq 0$, find

$$\lim_{n\to\infty} n^{-(p+1)} \sum_{k=1}^{n} k^p$$

4. Assume $f : \mathbb{R}^2 \to \mathbb{R}$ and $\dfrac{\partial f}{\partial x} : \mathbb{R}^2 \to \mathbb{R}$ are both continuous. Let

$$g(x) = \int_0^1 f(x,t)\, dt.$$

Prove g is differentiable and that

$$g'(x) = \int_0^1 \frac{\partial f}{\partial x}(x,t)\, dt.$$

5. Suppose that $\displaystyle\sum_{n=0}^{\infty} a_n x^n$ converges for all $x \in \mathbb{R}$. Let $f : \mathbb{R} \to \mathbb{R}$ be an indefinitely differentiable function such that

$$|f^{(n)}(x)| \leq n!|a_n|$$

for all n and all $x \in \mathbb{R}$. Prove that the Taylor series about $x = 0$ for f converges uniformly to f on every closed and bounded interval $[-M, M]$.

6. Let $f : \mathbb{R} \to \mathbb{R}$ be a strictly increasing continuous function such that $f(0) = 0$. Let $g : [0,1] \to \mathbb{R}$ be a continuous function such that

$$\int_0^1 f^n(x) g(x)\, dx, \quad n = 0, 1, 2, \ldots$$

Prove that g is identically *zero*.

August 2017

1. Let X be a metric space. Consider a family of subsets of X, denoted $\{E_i : i \in A\}$ where A is an uncountable index set. Suppose that for every finite or countable set $B \subset A$ the intersection

$$\bigcap_{i \in B} E_i$$

is open. Prove that the set

$$E = \bigcap_{i \in A} E_i$$

is also open.

2. Suppose that $f : \mathbb{R} \to \mathbb{R}$ is a function such that for every compact set $K \subset \mathbb{R}$ the inverse image $f^{-1}(K)$ is also compact. Prove that

$$\lim_{x \to +\infty} |f(x)| = +\infty$$

3. Suppose that $f : \mathbb{R} \to \mathbb{R}$ has derivatives of all orders and satisfies $f(0) = f'(0) = f''(0) = 0$. Prove that the function $g(x) = f(x)^{1/3}$ is differentiable at 0.

4. Let f and g be Riemann-Stieltjes integrable on $[a, b]$ with respect to a non-decreasing function α. Suppose that given any partition P of $[a, b]$ there exists a partition Q of $[a, b]$ such that

$$L(f, P, \alpha) \leq L(g, Q, \alpha) \quad \text{and} \quad L(g, P, \alpha) \leq L(f, Q, \alpha)$$

Prove that

$$\int_a^b f \, d\alpha = \int_a^b g \, d\alpha$$

5. Determine all positive continuous functions f on $[1, \infty)$ such that

$$\ln\left(1 + \int_0^\theta f(e^x) \, dx\right) = \theta$$

for all real numbers $\theta > 0$.

6. Prove that the image of any open set containing the unit disk $\{(x, y) : x^2 + y^2 \leq 1\}$ under the mapping $f(x, y) = (x^4 + y^4, 2xy)$ is *not* a subset of the unit disk.

May 2018

1. Let $\{a_n\}$ be the sequence with terms $\{1, 2, 2\frac{1}{2}, 3, 3\frac{1}{3}, 3\frac{2}{3}, 4, \frac{1}{4}, 4\frac{2}{4}, 4\frac{3}{4}, 5, \ldots\}$. Prove that for any positive integer p

$$\lim_{n\to\infty} a_{n+p} - a_n = 0$$

Is the sequence Cauchy? Explain.

2. Give an example of two disjoint nonempty closed sets A and B from $\mathbb{R}$ so that the distance between them is 0, i.e. $\inf\{|a-b| : a \in A \text{ and } b \in B\} = 0$. Show that your example does in fact work.

Solution: Let $F_1 = \mathbb{N}$ and $F_2 = \{n + \frac{1}{n} : n \in \mathbb{N}\}$. We have $F_1^C = \cup_{n=1}^{\infty} B_{1/2}(n/2)$ is open since each $B_{1/2}(n/2)$ is open. Therefore, F_1 is open. We know also

$$F_2^C = \bigcup_{n=1}^{\infty} B_d\left(\frac{n + \frac{1}{2n} + n + 1 + \frac{1}{2(n+1)}}{2}\right),$$

where $d = \frac{\text{lcm}(2n,2n+2)-1}{\text{lcm}(2n,2n+2)}$. This is clearly open being the union of open sets. Therefore, F_2 is closed. Note that $F_1 \cap F_2 = \emptyset$. Now

$$\text{dist}(F_1, F_2) = \inf\{d(f_1, f_2) : f_1 \in F_1, f_2 \in F_2\} = \inf\left\{\frac{1}{2n} : n \in \mathbb{N}\right\} = 0$$

Therefore, $\text{dist}(F_1, F_2) = 0$. □

3. Consider the equation $x^4 - y^2 = 0$. This equation determines y as a function of x, for all $x \in \mathbb{R}$, in many ways. Here are five such examples, $y = x^2$, $y = -x^2$, $y = x|x|$, $y = -x|x|$ or even $y = \begin{cases} x^2, & x \in \mathbb{Q} \\ -x^2, & x \notin \mathbb{Q} \end{cases}$.

(a) What does the Implicit Function Theorem say (or not say) about y as a function of x at the point $(\frac{1}{4}, \frac{1}{16})$?

(b) What does the Implicit Function Theorem say (or not say) about y as a function of x at the point $(0, 0)$?

4. Show that $\sum_{k=2}^{n-1} \frac{1}{\log k} - \int_2^n \frac{1}{\log x}\, dx$ converges as $n \to \infty$ to a positive number no larger than $\log 2$.

5. Let f be a Riemann integrable function on $[0, 1]$ and suppose that

$$\int_0^1 f(x)x^n\, dx = 0 \quad \text{for } n = 0, 1, 2, \ldots$$

Prove that if f is continuous. at a point $x_0 \in [0,1]$ then $f(x_0) = 0$.

6. Let $\{f_1, f_2, \ldots\}$ be a sequence of continuous nonnegative functions on $[0,1]$ such that $f_k(x) \leq f_{k+1}(x)$ for all $k \geq 1$ and all $x \in [0,1]$, and $f_k \to f$ uniformly on $[0,1]$ as $k \to \infty$ for a function f. Prove that

$$\lim_{n\to\infty} \int_0^1 \left(\sum_{k=1}^{n} f_k^n(x) \right)^n \, dx = \int_0^1 f(x) \, dx$$