# DEFINITIONS...

1. Group: A group is a set $G$ together with a function $G \times G \to G$ $\ni$ $(a,b) \to a*b$ $\ni$
   1) $*$ is associative ie $a*(b*c) = (a*b)*c$ $\forall a,b,c \in G$
   2) $\exists$ e identity element $\ni$ $e*a = a*e = a$ $\forall a \in G$
   3) every element has an inverse ie $\forall a \in G$ $\exists b \in G \ni a*b = e = b*a$
2. Abelian: A group is Abelian if $a*b = b*a$ $\forall a,b \in G$
3. Subgroup: A subgroup of a group $G$ is a nonempty subset $H$ which is closed under $*$ and under inverses ie if $h \in H$, then $h^{-1} \in H$
4. Order: The order of $a \in G$ is the smallest positive integer $n$ $\ni$ $a^n = 1$. Denoted, $|a| = n$. If no such $n$ exists, $|a| = \infty$
5. Dihedral Group: The dihedral group, $D_{2n}$, is the group of symmetries of a regular $n$-gon
6. Generates: Let $G$ be a group and $S$ a subset. Then $S$ generates $G$ if every element of $G$ can be written as a finite product of elements of $S$ and their inverses, denoted $G = \langle S \rangle$
7. Symmetric Group: The symmetric group on $n$ letters, $S_n$ is the set of all permutations of $\{1, \dots, n\}$ which is a group under composition
8. Homomorphism: Let $G, H$ be groups. A function $\varphi: G \to H$ is a homomorphism if $\varphi(a*b) = \varphi(a) * \varphi(b)$
9. $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \mid \gcd(a,n) = 1\}$
10. Group Action: Let $G$ be a group and $X$ a set. $G$ acts on $X$ if $\exists$ function $G \times X \to X$ $\ni$ $(g,x) \to g \cdot x$ satisfying $\forall x \in X$, $g_1, g_2 \in G$
    (i) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
    (ii) $1 \cdot x = x$
    In this case, $X$ is a left $G$-set
11. Kernel: The kernel of a group action is $\{g \mid g \cdot x = x \ \forall x \in X\}$
12. Faithful: An action is faithful if the kernel $= \{1\}$
13. Center: Let $G$ be a group. $Z(G) = \{g \in G \mid hg = gh \ \forall h \in G\}$ is the center of $G$
14. Centralizer: Let $G$ be a group and $S \subseteq G$. The centralizer of $S$ is $C_G(S) = \{g \in G \mid gs = sg \ \forall s \in S\}$
15. Cyclic Subgroup: Let $a \in G$. The cyclic subgroup generated by $a$ is $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$

16. Cyclic: A group $G$ is cyclic if $G = \langle a \rangle$ for some $a \in G$

17. Kernel: Let $\varphi: G \to H$ be a group homomorphism. The kernel of $\varphi$ is $\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = 1_H\}$

18. Image: The image of $\varphi$ is $\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$

19. Coset: Let $H$ be a subgroup of $G$. A left coset of $H$ is $aH = \{ah \mid h \in H\}$

20. Normal: $H$ is a normal subgroup of $G$ if $g^{-1}Hg = H \ \forall g \in G$

21. Index: The number of cosets of $H$ in $G$ is called the index of $H$ in $G$ denoted $|G:H|$

22. Simple: A group $G$ is simple if it has no nontrivial proper normal subgroups

23. Even Permutation: A permutation $\sigma \in S_n$ is even if it can be written as an even number of two cycles and odd otherwise

24. Alternating Group: $A_n$ is the subgroup of $S_n$ consisting of all even permutations called the alternating group

25. $HK = \{hk \mid h \in H, k \in K\}$

26. Vector Space: A vector space $V$ over a field $F$ is a set with two operations $+, \cdot$ (scalar multiplication) $\ni$
 1) $V$ abelian group under $+$
 2) $(ab)v = a(bv) \quad \forall a,b \in F, v \in V$
 3) $1_F \cdot v = v \quad \forall v \in V$
 4) $a(v+w) = av + aw$
 5) $(a+b)v = av + bv$

27. Linear Transformation: A function $T: V \to W$ is a linear transformation if $T(v_1+v_2) = T(v_1) + T(v_2)$ and $T(av) = aT(v) \ \forall a \in F, \forall v, v_1, v_2 \in V$

28. Linearly Independent: $S \subseteq V$ is linearly independent if $a_1v_1 + \dots + a_nv_n = 0 \Rightarrow a_1 = \dots = a_n = 0$ for $a_i \in F$, $v_i \in S$

29. Span: The span of $S \subseteq V$ is $\operatorname{span} S = \{a_1v_1 + \dots + a_nv_n \mid a_i \in F, v_i \in S\}$ and $S$ spans $V$ if $\operatorname{span} S = V$

30. Basis: $S$ is a basis for $V$ if $S$ spans $V$, is linearly independent, and is ordered

31. Dimension: The dimension of $V$ is the number of elements in any basis

32. Subspace: A subspace of a vector space is a subset $W \subseteq V$ which is a

vectorspace under the same operations ie W closed under +, ·

33. Matrix of a Linear Map: Let $V, W$ be finite dimensional vectorspaces $B = \{v_1, \dots, v_n\}$, $C = \{w_1, \dots, w_m\}$ bases for $V, W$ respectively, $T: V \to W$ linear map. Then $\underline{T(v_j)} = \sum_{i=1}^{m} \alpha_{i,j} w_i$ for $\alpha_{i,j} \in F$ and $\underline{M_B^C(T)} = (\alpha_{ij})_{i,j}$. In this case, the coordinate vector of $T(v_j)$ wrt $C$, denoted $[T(v_j)]_C$, is the jth column of $M_B^C(T)$

34. $\underline{Hom_F(V,W)} = \{T: V \to W \mid T \text{ is } F\text{-linear}\}$

35. Linear Operator: A linear operator is a linear transformation $T: V \to V$

36. Change of Basis Matrix: The change of basis matrix $P$ from $C$ to $B$ is $P = M_C^B(I)$ where $I: V \to V$ identity operator

37. Similar: Two matrices $A, B$ are similar if $\exists P$ invertible $\ni B = P^{-1}AP$

38. Equivalent: Two matrices $A, B$ are equivalent if $B = Q^{-1}AP$ for invertible $Q, P$

39. Independent: Subspaces $W_1, \dots, W_n$ are independent if the only way to write $w_1 + \dots + w_n = 0$ for $w_i \in W_i$ is to take all $w_i = 0$

40. Direct Sum: If $W_1, \dots, W_n$ are subspaces of $V \ni W_1 + \dots + W_n = V$ and $W_1, \dots, W_n$ are independent then $V$ is the direct sum of $W_1, \dots, W_n$

41. T-Invariant: Let $T: V \to V$ be a linear operator and $W$ a subspace of $V$. $W$ is T-invariant if $T(W) \subseteq W$

42. Direct Sum: The direct sum of two matrices $A, B$ is $\left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]$

43. Eigenvector: Let $T: V \to V$ be a linear operator. An eigenvector for $T$ is a nonzero $v \in V \ni T(v) = cv$ where $c$ is the eigenvalue for $v$. If $A \in M_n(F)$ a nonzero column vector $x \in F^n$ is an eigenvector with eigenvalue $c$ if $Ax = cx$

44. Determinant: A determinant is a function $d: M_n(F) \to F \ni$

(i) $d(\| {R \atop S} \|) = d(\|R\|) + d(\|S\|)$ and $d(\|cR\|) = c\,d(\|R\|)$ ie is linear in the columns of a matrix

(ii) $d$ vanishes if 2 adjacent columns are equal

(iii) $d(I) = 1$

45. Characteristic Polynomial: The characteristic polynomial of $T$ is $p(t) = \det(tI - T) = \det(tI - A)$ for any $A$ representing $T$

46. Upper Triangular: A matrix $A$ is upper triangular if $a_{ij} = 0$ for $i > j$

50. Stabilizer: Let $G$ act on $X$. The stabilizer of $x \in X$ is $G_x = \{g \in G \mid g \cdot x = x\}$

51. Orbit: Let $G$ act on $X$. The orbit of $x \in X$ is $O_x = \{g \cdot x \mid g \in G\}$

52. Transitive: An action is transitive if $\exists$ exactly one orbit ie $\forall x, y \in X$ $\exists g \in G \ni g \cdot x = y$

53. Left Regular Action: The action of $G$ on itself by left multiplication is the left regular action and the resulting homomorphism $G \to S_G$ is the left regular representation

54. Conjugate: Two elements $x, y \in G$ are conjugate if $y = gxg^{-1}$ for some $g \in G$

55. Class Equation: $|G| = |Z(G)| + |O_{a_1}| + \dots + |O_{a_s}|$ where $a_1, \dots, a_s$ are representatives for the conjugacy classes of size $> 1$

56. p-Group: $G$ is a p-Group if $|G| = p^m$ for some $m \geq 1$ and $p$ prime

57. Cycle Type: Let $\sigma \in S_n$ be written as a product of disjoint cycles $\sigma = \sigma_1 \dots \sigma_r$ of lengths $\ell_1 \geq \dots \geq \ell_r$. The cycle type of $\sigma$ is $(\ell_1, \dots, \ell_r)$

58. Partition: A partition of $n \in \mathbb{N}$ is an expression of $n$ as a sum $n = \lambda_1 + \dots + \lambda_r$ where $\lambda_1 \geq \dots \geq \lambda_r \geq 1$ are integers

59. Sylow p-subgroup: Let $G$ be a group $\ni |G| = p^r m$ where $p \nmid m$ and $p$ prime. A subgroup $H$ of order $p^r$ is a Sylow p-subgroup

60. Characteristic Subgroup: $H$ is a characteristic subgroup if $\varphi(H) \subseteq H$ $\forall \varphi \in Aut(G)$

61. Automorphism: $\varphi: G \to G$ is an automorphism if $\varphi$ is an isomorphism

62. Free Semigroup: Let $S = \{a, b, c, \dots\}$ be a set of symbols. The free semigroup on $S$ consists of all finite words in the alphabet of $S$, denoted $W_S$

63. Free Semigroup: Let $\tilde{S} = S \cup \{a^{-1} \mid a \in S\}$ where $a^{-1}$ is another symbol, then $\tilde{W} = W_{\tilde{S}}$ is free semigroup on $\tilde{S}$

64. Reduced: A word in $\tilde{W}$ is reduced if it contains no subword of the form $zz^{-1}$ or $z^{-1}z$ for $z \in S$. If $w$ is not reduced, a reduction of $w \in \tilde{W}$ is any word obtained by deleting one or more occurences of $zz^{-1}$ or $z^{-1}z$

65. Equivalent: $w, w' \in \tilde{W}$ are equivalent if they have the same reduced form, denoted $w \sim w'$

66. Free Group: $F_S = \tilde{W}/\sim$, the set of equivalence classes of $\tilde{W}$, is the free group on $S$.

67. Set of Defining Relations: Let $G$ be a group, $F$ free group, $\varphi: F \to G$ surjective group homomorphism. Then $R \subseteq \ker\varphi$ is a set of defining relations for $G$ if $\ker\varphi$ is the smallest normal subgroup of $F$ containing $R$, in this case $G = \langle S | R \rangle$

68. Bilinear Form: Let $V$ be a vector space over $F$. A bilinear form on $V$ is a function $f: V \times V \to F \ni (v, w) \to f(v, w) = \langle v | w \rangle \ni$

1) $f(v_1 + v_2, w) = f(v_1, w) + f(v_2, w)$, $f(v, w_1 + w_2) = f(v, w_1) + f(v, w_2)$

2) $f(cv, w) = cf(v, w) = f(v, cw)$ $\forall v, w, v_1, v_2, w_1, w_2 \in V$, $c \in F$

69. Symmetric: A bilinear form $f$ is symmetric if $f(v, w) = f(w, v)$ $\forall v, w$

70. Skew Symmetric: A bilinear form $f$ is skew-symmetric if $f(v, w) = -f(w, v)$ $\forall v, w \in V$

71. Orthogonal Complement: Let $W$ be a subspace of $V$, $\langle\ |\ \rangle$ symmetric bilinear form. The orthogonal complement of $W$ is $W^{\perp} = \{v \in V | \langle v | w \rangle = 0 \ \forall w \in W\}$

72. Null Space: The nullspace of $V$ is the orthogonal complement of $V$
$V^{\perp} = \{v \in V | \langle v | w \rangle = 0 \ \forall w \in V\}$

73. Nondegenerate: If $V^{\perp} = \{0\}$, $\langle\ |\ \rangle$ is a nondegenerate form

74. Functional: A functional on $V$ is a linear map $\varphi: V \to F$ and
$V^* = \{\text{functionals on } V\} = \{\varphi: V \to F \mid \varphi \text{ linear}\}$

75. Length: The length of $z = x + iy \in \mathbb{C}$ is $|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$. The length of a vector $(z_1, \dots, z_n)^T \in \mathbb{C}^n$ is $\sqrt{z_1\bar{z}_1 + \dots + z_n\bar{z}_n}$

76. Standard Hermitian Product: If $x = (x_1, \dots, x_n)^T$, $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)^T$, the standard Hermitian product is $\langle x | y \rangle = \bar{x}^T y = x^* y$

77. Hermitian Product: A hermitian product on a complex vector space $V$ is $\langle\ |\ \rangle: V \times V \to \mathbb{C}$ which satisfies

1) $\langle z | \alpha w \rangle = \alpha \langle z | w \rangle$ and $\langle z | w_1 + w_2 \rangle = \langle z | w_1 \rangle + \langle z | w_2 \rangle$

2) $\langle \alpha z | w \rangle = \bar{\alpha} \langle z | w \rangle$ and $\langle z_1 + z_2 | w \rangle = \langle z_1 | w \rangle + \langle z_2 | w \rangle$

3) $\langle z | w \rangle = \overline{\langle w | z \rangle}$ ie $\langle z | z \rangle \in \mathbb{R}$

78. Positive Definite: A hermitian product is positive definite if $\langle z | z \rangle \geq 0$ equality iff $z = 0$

79. $A^* = \overline{A}^T$ ie $ij$ entry $A^*$ is $\overline{a_{ji}}$

80. Hermitian/Self Adjoint: A complex matrix $A$ is hermitian or self adjoint if $A^* = A$ $(T^* = T)$

81. Orthogonal: A $n \times n$ matrix $A$ over field $F$ is orthogonal if its columns form an orthonormal basis for $F^n$ wrt the dot product ie $A^T A = I$

82. Unitary: $A \in M_n(\mathbb{C})$ is unitary if $A^* A = I$ $(T^* T = I)$

83. Hermitian Space: A hermitian space is a finite dimensional complex vector space $V$ with a positive definite hermitian form

84. Normal: A linear operator $T: V \to V$ on a hermitian space $V$ is norma
if $T$ commutes with its adjoint ie $T^* T = T T^*$

85. Adjoint: The function $T^* : V \to V \ni v \to T^* v$ is a linear operator called the adjoint of $T \ni \langle T^* v | w \rangle = \langle v | Tw \rangle$

86. Unitarily Diagonalizable: A is unitarily diagonalizable if $\exists P$ unitary, invertible $\ni P^* A P = D$ diagonal

87. Ring: A ring is a nonempty set $R$ together with two binary operations $+, \cdot \ni$
   1) $(R, +)$ is an abelian group
   2) $(ab)c = a(bc)$ $\forall a, b, c \in R$
   3) $(a+b)c = ac + bc$ and $a(b+c) = ab + ac$ $\forall a, b, c \in R$

88. Commutative Ring: A ring $R$ is commutative if $ab = ba$ $\forall a, b \in R$

89. Zero Divisor: $0 \neq a \in R$ is a zero divisor if $\exists\, 0 \neq b \in R \ni ab = 0$ or $ba = 0$

90. Unit: $a \in R$ is a unit if $\exists b \in R \ni ab = ba = 1$

91. Division Ring: A division ring is a ring in which every nonzero element is a unit

92. Field: A commutative division ring is a field

93. Integral Domain: A commutative ring is an integral domain if it has no zero divisors

94. Polynomial Ring: A polynomial ring is $R[x] = \{a_0 + \dots + a_n x^n \mid a_0, \dots, a_n \in R, n \geq$
where $R$ is a ring

95. Subring: Let $R$ be a ring. A subring of $R$ is $\emptyset \neq S \subseteq R \ni S$ is a ring under $+, \cdot$

96. Left Ideal: Let $R$ be a ring. A left ideal of $R$ is $\emptyset \neq I \subseteq R \ni$

a) $\forall a,b \in I$, $a+b \in I$

b) $\forall a \in I, \forall r \in R$, $ra \in I$

97. Ring Homomorphism: Let $R,S$ rings. A ring homomorphism $\varphi: R \to S \ni$

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ $\forall a,b \in R$

2) $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a,b \in R$

98. Maximal: Let $R$ be a ring with 1. An ideal $I \neq R$ is maximal if whenever $I \subsetneq J \triangleleft R$ then $J = R$

99. Prime: Let $R$ be a commutative ring with 1. An ideal $I$ is prime if whenever $ab \in I$ then $a \in I$ or $b \in I$

100. Multiplicative: $S \subseteq R$ is multiplicative if $0 \notin S$, $1 \in S$, and $s,t \in S \Rightarrow st \in S$

101. Nilpotent: $0 \neq r \in R$ is nilpotent if $r^n = 0$ for some $n > 1$

102. Comaximal: $R$ commutative with 1. $I, J \triangleleft R$ proper are comaximal if $I + J = R$

103. Prime: $0 \neq p \in R$ nonunit is prime if $p | ab \Rightarrow p|a$ or $p|b$

104. Irreducible: $R$ integral domain. $0 \neq p \in R$ nonunit is irreducible if whenever $p = ab$, then $a$ or $b$ is a unit

105. Associates: $a,b \in R$ are associates if $\exists u \in R$ unit $\ni a = bu$

106. PID: An integral domain $R$ is a PID if every ideal is generated by one element ie $\forall I \triangleleft R$, $\exists a \in R \ni I = \langle a \rangle$

107. Norm: Let $R$ be an integral domain. $N: R \to \mathbb{N} \cup \{0\}$ is a norm if $N(0) = 0$. If $N(z) > 0$ $\forall z \neq 0$, $N$ is a positive norm

108. Euclidean Domain: An integral domain $R$ is a Euclidean Domain if $\exists N$ a norm $\ni \forall a,b \in R$ with $b \neq 0$ $\exists q,r \in R \ni a = bq + r$ with $r = 0$ or $N(r) < N(b)$

109. UFD: An integral domain $R$ is a UFD if $\forall 0 \neq a \in R \ni a$ nonunit

1) $a = \prod$ irreducibles

2) If $a = p_1 \dots p_n = q_1 \dots q_m$, $q_i, p_i$ irreducible $\Rightarrow n = m$ and $\exists \sigma \in S_n \ni \forall i$ $p_i, q_{\sigma(i)}$ associates

110. ACC: A ring $R$ satisfies the ascending chain condition on left ideals if every chain of left ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes ie $\exists r \ni I_n = I_{n+1} = \dots$

111. Noetherian: A ring that satisfies the ACC is Noetherian

112. Primitive: A polynomial $f \in R[x]$ is primitive if the coefficients of $f$ are

relatively prime

113. Algebraically closed: Let $F$ be a field. $F$ is algebraically closed if every nonconstant polynomial $f \in F[x]$ has a root in $F$ ie $f$ factors as a product of degree 1 polynomials

114. Module: Let $R$ be a ring with 1. A left $R$-module $M$, $_RM$, is an abelian group $(M, +)$ with an operation of $R$ on $M$, $R \times M \to M \ni (r, m) \to rm \ni$
1) $\forall r_1, r_2 \in R, m \in M, \ (r_1 + r_2)m = r_1 m + r_2 m$
2) $\forall r \in R, m_1, m_2 \in M, \ r(m_1 + m_2) = rm_1 + rm_2$
3) $\forall r, s \in R, \forall m \in M, \ r(sm) = (rs)m$
4) $1 \cdot m = m \ \forall m \in M$

115. Submodule: Let $M$ be a left $R$-module. A submodule $N$ of $M$ is a nonempty subset of $M$ that is an $R$-module wrt the same operations

116. Finitely Generated: A module $M$ is finitely generated if $\exists S \subseteq M \ni M = \langle S \rangle$

117. Cyclic: A module is cyclic if it is generated by one element

118. Annihilator: Let $R$ be a ring and $M$ a left $R$-module. Let $m \in M$. The annihilator of $m$ is $ann_R(m) = \{r \in R \mid rm = 0\}$

119. Annihilator: The annihilator of $M$ in $R$ is $ann_R M = \{r \in R \mid rm = 0 \ \forall m \in M$

120. Faithful: A module is faithful if $ann_R M = 0$

121. Module Homomorphism: Let $M, N$ be $R$-modules. A module homomorphism is $f: M \to N \ni$
i) $f(x+y) = f(x) + f(y) \ \forall x, y \in M$
ii) $f(rx) = rf(x) \ \forall r \in R, \forall x \in M$

122. Kernel: Let $f: M \to N$. The kernel of $f$ is $\ker f = \{x \in M \mid f(x) = 0\}$

123. $Hom_R(M, N) = \{f: M \to N \mid f \text{ homomorphism}\}$ where $M, N$ modules

124. Direct Sum: Let $L, N$ be submodules of $M$. The sum $L + N$ is a direct sum if $L \cap N = 0$, denoted $L \oplus N$. If $L_1, \ldots, L_k$ are submodules of $M$, $L_1 + \ldots + L_k$ is direct if $L_i \cap (L_1 + \ldots + L_{i-1} + L_{i+1} + \ldots + L_k) = 0$

125. Indecomposible: A module $M$ is indecomposible if it cannot be written as $M = A \oplus B$ where $A, B$ nontrivial submodules

126. External Direct Sum: Let $\{M_i\}_{i \in I}$ be a family of $R$-modules.

The external direct sum is $\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} \mid x_i \in M_i$ where only finitely many entries are nonzero$\}$

127. Basis: Let $0 \neq F$ be a left $R$-module. Let $\phi \neq S \subseteq F$. $S$ is a basis of $F$ if
① every element of $F$ can be written as a finite sum $\sum a_i e_i$ where $a_i \in R$, $e_i \in S$ ie $F = \langle S \rangle$
② The above representations are unique

128. Free Module: An $R$-module is a free module if it has a basis

129. Linearly Independent: Let $S \subseteq M$ $R$-module. $S$ is linearly independent if whenever $r_1e_1 + \dots + r_ne_n = 0$ with $e_i \in S$, $r_i \in R \Rightarrow r_1 = \dots = r_n = 0$

130. Simple: An $R$-module $S \neq 0$ is simple if the only submodules of $S$ are $S$ and $0$

131. Idempotent: $e \in R$ is idempotent if $e^2 = e$

132. $End_R(M) = \{f: M \to M \mid f$ homomorphism$\}$

133. Idempotent: An idempotent element of $End_R(M)$ is a homomorphism $\varphi: M \to M \ni \varphi^2 = \varphi$ ie $\varphi \circ \varphi = \varphi$

134. Torsion Free: Let $R$ be an integral domain. An $R$-module $M$ is torsion free if $\forall\, 0 \neq x \in M$, $rx = 0$ for $r \in R \Rightarrow r = 0$

135. Torsion: Let $R$ be integral domain, $0 \neq M$ $R$-module. An element $0 \neq x \in M$ is torsion if $\exists\, 0 \neq r \in R \ni rx = 0$

136 Torsion Submodule: Let $R$ be an integral domain, $M$ $R$-module. The torsion submodule of $M$ is $Tor(M) = \{x \in M \mid \exists\, 0 \neq r \in R \ni rx = 0\}$

137. $\mathfrak{p}$-Primary: Let $R$ be a PID and $M$ a finitely generated $R$-module with $\mathfrak{p} = \langle p \rangle \lhd R$ prime. $M$ is $\mathfrak{p}$-Primary if $\forall\, 0 \neq x \in M$, $\exists\, k \geq 1 \ni p^k x = 0$

138. $M(\mathfrak{p}) = \{x \in M \mid p^k x = 0$ for some $k \geq 1\}$ where $M$ finitely generated, $0 \neq \mathfrak{p} = \langle p \rangle$ prime ideal of $R$

139. Local Ring: A local ring has a unique maximal ideal.

140. $d(M) = \dim_{R/p} M/pM$ where $p = \langle p \rangle$

141. $U_p(n, M) = d(p^n M) - d(p^{n+1} M)$

142. Elementary Divisors: Let $M$ be $\mathfrak{p}$-primary. Its elementary divisors are the ideals $\langle p^{n+1} \rangle$, $n \geq 0$ each taken with multiplicity $U_p(n, M)$

143. Elementary Divisors: Let $M$ be a finitely generated torsion module. Its elementary divisors are the elementary divisors of the primary components

144. Order: The order of $M$ is the ideal $\langle \prod_{i,j} p_i^{r_{i,j}} \rangle$ generated by the product of all the elementary divisors

145. Invariant Factors: Let $M$ be a torsion module over the PID $R$ $\ni$ $M \cong R/\langle a_1 \rangle \oplus \dots \oplus R/\langle a_n \rangle$ with $a_1 | a_2 | \dots | a_n$. The invariant factors of $M$ are $a_1, \dots, a_n$

146. $\det T = \det A$ where $A$ is the matrix of $T$ relative to some basis

147. Eigenspace: $V_\lambda = \{v \in V \mid T(v) = \lambda v\}$ is the eigenspace of $\lambda$

148. Diagonalizable: $T: V \to V$ linear, $\dim V = n < +\infty$. $T$ is diagonalizable if $\exists$ $B = \{e_1, \dots, e_n\}$ basis of $V$ $\ni$ relative to $B$ the matrix of $T$ is $\begin{bmatrix} c_1 & & \\ & \ddots & \\ & & c_n \end{bmatrix}$

149. Minimal Polynomial: $f$ is the minimal polynomial of $V$ if $f$ is the smallest degree monic polynomial annihilating $V$

150. Companion Matrix: If $f(x) = x^t + c_{t-1}x^{t-1} + \dots + c_1 x + c_0$ is a monic polynomial with coefficients in $F$, its companion matrix is the $t \times t$ matrix $\begin{bmatrix} 0 & \dots & 0 & -c_0 \\ 1 & \dots & 0 & -c_1 \\ \vdots & & & \\ 0 & \dots & 1 & -c_{t-1} \end{bmatrix}$

151. Characteristic polynomial: Let $A$ be an $n \times n$ matrix. The characteristic polynomial of $A$ is $\operatorname{char} A = \det(xI - A)$

152. Jordan Block: A Jordan block $J(\lambda, n)$, $\lambda \in F$, is an $n \times n$ matrix $J(\lambda, n) = \begin{bmatrix} \lambda & & \\ 1 & \ddots & \\ & 1 & \lambda \end{bmatrix}$ where $\lambda$ is the eigenvalue of $J(\lambda, n)$ with multiplicity $n$

153. Jordan Canonical Form: $T: V \to V$ is in Jordan canonical form if $\exists$ $B$ a basis of $V$ $\ni$ the matrix of $T$ wrt $B$ is of the form $\begin{bmatrix} \boxed{J_1} & & \\ & \ddots & \\ & & \boxed{J_m} \end{bmatrix}$ with $J_i = J(\lambda_i, n_i)$

154. Characteristic: Let $F$ be a field. The characteristic of $F$ denoted $\operatorname{char} F$ is the smallest positive integer $n$ $\ni$ $n \cdot 1 = 0$. If no such $n$ exists, $\operatorname{char} F = 0$

155. Prime subfield: the prime subfield of $F$ is the smallest subfield of $F$ and is the intersection of all subfields of $F$

156. Field Extension: If $F$ is a subfield of a field $E$, then $F \subset E$ is a field extension, also denoted $E/F$

157. Algebraic: Let $F \subset E$ be a field extension. $\alpha \in E$ is algebraic over $F$ if $\exists f(x) \in F[x]$ $\ni$ $f(\alpha) = 0$

158. Transcendental: If $\alpha \in E$ is not algebraic over $F$, it is transcendental over $F$

159. Algebraic: An extension $F \subset E$ is algebraic if every $\alpha \in E$ is algebraic over $F$

160. Minimal Polynomial: The minimal polynomial of $\alpha$ over $F$, denoted $Irr(\alpha, F)$, is the monic polynomial of smallest degree having $\alpha$ as a root

161. $F[\alpha] = \{ f(\alpha) \mid f(x) \in F[x] \}$ is the smallest subfield of $E$ containing $F$ and $\alpha$ where $F \subset E$

162. $F(\alpha) = \{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in F[x], g(\alpha) \neq 0 \}$ is the field of fractions of $F[\alpha]$

163. Algebraic Numbers: $\mathbb{A} = \{ \alpha \in \mathbb{C} \mid \alpha$ algebraic over $\mathbb{Q} \}$ are the algebraic numbers

164. Compositum: Let $E, F \subset L$ be fields. The compositum of $E$ and $F$, denoted $EF$, is the smallest subfield of $L$ containing $E$ and $F$.

165. Finitely Generated: An extension $F \subset E$ is finitely generated if $E = F(\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n \in E$

166. Simple: An extension $F \subset E$ is simple if $\exists \alpha \in E$ with $E = F(\alpha)$

167. Splitting Field: Let $F$ be a field and $f(x) \in F[x]$. An extension $F \subset E$ is a splitting field of $f(x)$ if $f(x)$ factors over $E$ into linear factors or splits over $E$, and is the smallest with this property i.e. if $F \subset L \subset E$ $\ni f$ splits over $L$, then $L = E$

168. Normal: An algebraic extension $F \subset E$ is normal if $\forall \alpha \in E$, $Irr(\alpha, F)$ splits in $E$

169. K-embedding: Let $E, F$ be extensions of $K$. A nonzero homomorphism $\sigma: E \to F$ leaving $K$ fixed pointwise is a K-embedding i.e. $\sigma(a) = a$ $\forall a \in K$

170. Algebraic closure: Let $F$ be a field. An algebraic closure of $F$ is an extension $\bar{F}$ of $F$ $\ni$ $\bar{F}$ algebraic over $K$, $\bar{F}$ is algebraically closed, and $\bar{F}$ is minimal with this property

171. Separable: Let $F$ be a field. A polynomial $f \in F[x]$ is separable if it has no multiple roots in any extension $E$ of $F$ in which it splits

172. Derivative: Let $f = a_n x^n + \dots + a_0 \in F[x]$. Its derivative is $f' = n a_n x^{n-1} + \dots + a_1 \in F[x]$

173. Separable: Let $F \subset E$ be an algebraic extension. An element $\alpha \in E$ is separable over $F$ if $Irr(\alpha, F)$ is separable

174. Separable Extension: Let $F \subset E$ be algebraic. $F \subset E$ is separable if $\forall \alpha \in E$, $\alpha$ is separable over $F$

175. Galois Group: Let $F \subset E$. The Galois group of $E/F$ is $Gal(E/F) = \{ \sigma \in Aut E \mid \sigma(a) = a \ \forall a \in F \}$

176. Galois Extension: Let $F \subset E$ be algebraic. $F \subset E$ is a Galois extension if it is both normal and separable. OR: $F \subset E$ is Galois if $|Gal(E/F)| = [E:F]$

177. Fixed subfield: Let $E$ be a field and $H$ a subgroup of $\text{Aut}\,E$. The fixed subfield of $H$ is $\text{Fix}(H) = \{x \in E \mid \sigma(x) = x \;\; \forall \sigma \in H\}$

178. $\mathcal{H} = \{H \mid H \text{ subgroup of } G\}$ where $F \subset E$ and $G = \text{Gal}(E/F)$

179. $\mathcal{F} = \{K \mid F \subset K \subset E\}$ where $F \subset E$ and $G = \text{Gal}(E/F)$

180. Normalizer: The normalizer of $X \subseteq G$ is $N_G(X) = \{g \in G \mid gXg^{-1} = X\}$

# THEOREMS...

1. $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \mid \gcd(a,n) = 1\}$
2. $G$ group $\Rightarrow$
   1) Identity $e$ unique
   2) For each $a \in G$, $a^{-1}$ is unique
   3) $(a^{-1})^{-1} = a$
   4) $(ab)^{-1} = b^{-1}a^{-1}$
   5) For any $a_1, \dots, a_n \in G$, $a_1 \dots a_n$ is well defined independent of parentheses
3. $G$ group, $a,b,c \in G$, $ac = bc \Rightarrow a = b$
4. $G = \langle S \rangle$, $S$ commutative set $\Rightarrow G$ abelian
5. Cycle decomposition...
   Step 1: Pick smallest element of $\{1, \dots, n\}$, $a$
   Step 2: Write $\{a, \sigma(a), \sigma^2(a), \dots\}$ until you get back to $a$
   Step 3: Return to step 1
6. Inverse of a cycle $(a_1 \dots a_k)^{-1} = (a_k \dots a_1)$
7. Disjoint cycles commute
8. The order of a $k$ cycle is $k$
9. Cycle decomposition unique up to order of cycles
10. every permutation can be written as a product of "two-cycles" not necessarily disjoint
11. $\varphi$ isomorphism $\Rightarrow \varphi^{-1}$ isomorphism
12. $S_3 \cong D_6 \ncong \mathbb{Z}/6\mathbb{Z}$
13. $G \cong H \Rightarrow$
    (i) $|G| = |H|$
    (ii) $G$ abelian $\Leftrightarrow$ $H$ abelian
    (iii) $|x| = |\varphi(x)|$ $\forall x \in G$
14. $G, H$ groups $\ni G = \langle a_1, \dots, a_n \rangle$, $\{b_1, \dots, b_n\} \subseteq H$, $b_i$'s satisfy all relations of $a_i$'s $\Rightarrow \varphi(a_i) = b_i$ $\forall i$ homomorphism
15. All homomorphisms of $\mathbb{Z}$ are given by $\varphi(n) = kn$ for some $k \in \mathbb{Z}$ $\ni \varphi(1) = k$
16. $G$ acts on $X \Rightarrow$ we have homomorphism $\varphi: G \to S_X$ given by $\varphi(g) = \sigma_g$ where $\sigma_g(x) = g \cdot x$
17. $\varphi: G \to S_X$ homomorphism $\Rightarrow$ we can define an action of $G$ on $X$ by $g \cdot x = \varphi(g)(x)$
18. $\varphi$ homomorphism $\Rightarrow \varphi(1) = 1$

19. Subgroup Test $G$ group, $H \subseteq G$. $H$ is a subgroup of $G \Leftrightarrow H \neq \phi$ and $\forall x,y \in H$, $xy^{-1} \in H$
20. $G$ finite group, $H \subseteq G$. $H$ is a subgroup of $G \Leftrightarrow H$ closed under multiplicati
21. $H \leq G, K \leq G \Rightarrow H \cap K \leq G$
22. $\{H_\alpha\}_{\alpha \in I}$ family of subgroups $\Rightarrow \bigcap_{\alpha \in I} H_\alpha \leq G$
23. $H, K \leq G \not\Rightarrow H \cup K \leq G$
24. $Z(G) \leq G$, $C_G(S) \leq G$
25. $Z(G) \subseteq C_G(S)$ $\forall S \subseteq G$
26. $\langle x \rangle \subseteq C_G(x)$ for $x \in G$ but $S \subseteq C_G(S)$ not true $\forall S \subseteq G$
27. kernel of group action is a subgroup
28. stabilizer of group action is a subgroup
29. Generators not unique ie $\langle a \rangle = \langle a^{-1} \rangle = \ldots$
30. $G$ cyclic $\Rightarrow$ $G$ abelian
31. $G = \langle a \rangle$ cyclic $\Rightarrow |G| = |a|$ and:
(i) $|G| = n < \infty \Rightarrow a^n = 1$ and $G = \{1, a, a^2, \ldots, a^{n-1}\}$
(ii) $|G| = \infty \Rightarrow G = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ and each element is distinct
32. $a \in G$, $a^m, a^n = 1 \Rightarrow a^{\gcd(m,n)} = 1$
33. $G, H$ cyclic groups, $|G| = |H| \Rightarrow G \cong H$ and:
1) $G = \langle x \rangle$, $H = \langle y \rangle \Rightarrow$ isomorphism is $\varphi : G \to H \ni \varphi(x^i) = y^i$
34. $\varphi : \mathbb{Z} \to \langle x \rangle \ni \varphi(i) = x^i$ isomorphism if $\langle x \rangle$ infinite
35. Any cyclic group of order $n < \infty$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$
36. $|a| = \infty \Rightarrow |a^i| = \infty$ $\forall i \neq 0$
37. $|a| = \infty$, $\langle a \rangle = \langle a^i \rangle \Leftrightarrow i = \pm 1$
38. $|a| = n < \infty \Rightarrow |a^k| = \frac{n}{\gcd(k,n)}$
39. $|a| = n < \infty$. $\langle a \rangle = \langle a^i \rangle \Leftrightarrow \gcd(i,n) = 1$
40. $C_n$ has $\varphi(n) = \#\{k \in \{1, \ldots, n\} \mid \gcd(k,n) = 1\}$ generators
41. Every nonidentity element of $C_p$, $p$ prime is a generator
42. $G = \langle a \rangle$ cyclic group $\Rightarrow$
1) Every subgroup of $G$ is cyclic ie $H \leq G \Rightarrow H = \langle a^k \rangle$ or $H = \langle 1 \rangle$ where $k$ smallest positive integer $\ni a^k \in H$
2) $|G| = \infty \Rightarrow G$ has exactly one cyclic subgroup for each $k \geq 1$, $\langle a^k \rangle$
3) $|G| = n < \infty \Rightarrow G$ has exactly one cyclic subgroup for each $d \mid n$

and the subgroup has order $d$

43. $\varphi: G \to H$ homomorphism $\Rightarrow \ker\varphi \le G$ and $\operatorname{Im}\varphi \le H$

44. $\ker\varphi$ is a fiber of $\varphi$ ie $\ker\varphi = \varphi^{-1}(1_H)$

45. The fibers of a homomorphism form a group

46. A fiber of a group homomorphism is both a left and right coset ie $\varphi: G \to H$, $K = \ker\varphi \Rightarrow$ for any $x \in H$, $\varphi^{-1}(x) = aK = Ka$ for any $a \ni \varphi(a) = x$

47. $G$ group, $H \le G$, $a, b \in G \Rightarrow$

(i) $a \in Ha, aH$

(ii) $aH = H \Leftrightarrow a \in H$

(iii) $aH = bH \Leftrightarrow a \in bH$

(iv) $aH = bH \Leftrightarrow b^{-1}a \in H$

(v) Either $aH = bH$ or $aH \cap bH = \emptyset$ ie cosets partition $G$

(vi) $|aH| = |bH| = |H|$

(vii) $aH = Ha \Leftrightarrow aHa^{-1} = H$

(viii) $aH \le G \Leftrightarrow aH = H$

48. $aH \cdot bH = abH$ well defined $\Leftrightarrow g^{-1}Hg = H \ \forall g \in G$

49. $G/H = \{\text{cosets of } H \text{ in } G\}$ is a group iff $H$ normal in $G$

50. $H \le G$. TFAE:

(i) $H$ normal in $G$

(ii) $N_G(H) = G$

(iii) $gH = Hg \ \forall g \in G$

(iv) $gHg^{-1} = H \ \forall g \in G$

51. $H \le G$ normal $\Leftrightarrow$ $H$ is the kernel of some group homomorphism namely $\varphi: G \to G/H \ni \varphi(g) = gH$

52. $G$ abelian $\Rightarrow$ all subgroups are normal

53. $N \le Z(G) \Rightarrow N$ normal in $G$ ie $Z(G)$ normal in $G$

54. Lagrange's Theorem $G$ finite group, $H \le G \Rightarrow |H| \mid |G|$

55. $|G| < \infty \Rightarrow |G:H| = |G|/|H|$

56. $a \in G \Rightarrow |a| \mid |G|$

57. $|G| = p$ prime $\Rightarrow G$ cyclic and $G \cong C_p \cong \mathbb{Z}/p\mathbb{Z}$

58. $A_n$ is normal in $S_n$

59. $|A_n| = \frac{n!}{2}$

60. An m-cycle is odd if m is even and even if m is odd

61. $A_4$ non-Abelian

62. $|G|=n$, $d|n \not\Rightarrow \exists H \leq G \ni |H|=d$

63. $A_4 \not\leq D_{12}$

64. G abelian, $|G|=n$, $d|n \Rightarrow \exists H \leq G \ni |H|=d$

65. Cauchy's Theorem $|G|=n$, $p$ prime $\ni p|n \Rightarrow \exists a \in G \ni |a|=p$ ie $\exists H \leq G \ni |H|=p$

66. Sylow's First Theorem G group, $|G|=p^r m$, $p$ prime, $p \nmid m \Rightarrow$ G has a subgroup of order $p^r$

66. Cauchy's Theorem for Abelian Groups G abelian, $|G|=n$, $p$ prime, $p|n \Rightarrow \exists a \in G \ni |a|=p$

67. $|H|, |K| < \infty \Rightarrow |HK| = \frac{|H||K|}{|H \cap K|}$

68. $H, K \leq G$. HK subgroup $\Leftrightarrow HK=KH$

69. 1st Isomorphism Theorem $\varphi: G \to H$ group homomorphism $\Rightarrow G/\ker\varphi \cong \operatorname{Im}\varphi$ via the isomorphism $\pi: aN \to \varphi(a)$

70. 2nd Isomorphism Theorem G group, $H, N \leq G$, N normal $\Rightarrow H \cap N$ is a normal subgroup and $H/H\cap N \cong HN/N$

71. 3rd Isomorphism Theorem $H \leq K \leq G$, $H, K$ normal in G $\Rightarrow$ H is normal in K, $K/H$ is normal subgroup of $G/H$ and $\frac{G/H}{K/H} \cong G/K$

72. 4th Isomorphism Theorem N normal subgroup of G $\Rightarrow \exists$ bijection $\{$subgroups of $G/N\} \longleftrightarrow \{$subgroups of G containing N$\}$ preserving

(i) containment: $H \leq K \Leftrightarrow \pi(H) \leq \pi(K)$ where $\pi: G \to G/N \ni H \to \pi(H)$

(ii) indices: $|K:H| = |\pi(K):\pi(H)|$

(iii) Normality: H normal in G $\Leftrightarrow \pi(H)$ normal in $G/N$

73. F field, V vectorspace over F $\Rightarrow \forall a \in F, v \in V$:

(i) $0_F \cdot v = 0_V$

(ii) $a \cdot 0_V = 0_V$

(iii) $(-1_F) \cdot v = -v$

74. $T: V \to W$ linear transformation, T bijection $\Rightarrow$ T isomorphism of vector spaces

75. span S subspace of V

76. $B$ basis for $V \Rightarrow \forall v \in V \; \exists! \, v_1, \dots, v_n \in B$ and $c_1, \dots, c_n \in F \ni v = c_1v_1 + \dots + c_nv_n$

77. $S$ spans $V$, no proper subset of $S$ spans $V \Rightarrow S$ basis of $V$

78. $V$ has finite spanning set $S \Rightarrow V$ has a finite basis contained in $S$

79. Replacement Theorem $B = \{b_1, \dots, b_n\}$ finite basis for $V$, $I = \{v_1, \dots, v_m\} \subseteq V$ linearly independent $\Rightarrow$ we may reorder $B \ni \forall i = 0, \dots, m$ the set $\{v_1, \dots, v_i, b_{i+1}, b_{i+2}, \dots, b_n\}$ is a basis for $V$ and $m \leq n$

80. $V$ has finite basis with $n$ elements $\Rightarrow$
(i) every linearly independent set in $V$ has at most $n$ elements
(ii) every set that spans $V$ has at least $n$ elements

81. $V$ has finite basis $\Rightarrow$ every basis has the same number of elements

82. $V$ has finite basis $\Rightarrow$ every linearly independent set can be extended to a basis

83. Finite dimensional vector spaces have finite bases

84. Every vector space has a basis

85. Zorn's Lemma $\emptyset \neq S$ partially ordered set $\ni$ every chain in $S$ has an upper bound $\Rightarrow S$ has a maximal element

86. Universal Mapping Property $B$ basis for vector space $V$. Then for any vector space $W$ and any function $f: B \to W$ $\exists! T: V \to W$ linear transformation $\ni T|_B = f$ ie

$$\begin{tikzcd} B \arrow[r, hook] \arrow[dr, "f"'] & V \arrow[d, dashed, "\exists! T"] \\ & W \end{tikzcd}$$

87. $V$ finite dimensional vector space over field $F \Rightarrow V \cong F^n$ for some $n$

88. $W$ subspace of $V \Rightarrow V/W$ vector space

89. $\dim V = \dim W + \dim V/W$

90. Coordinate vector of $T(v)$ wrt basis $C$ is obtained from the coordinate vector of $v$ wrt $B$ by left multiplication by matrix $M_B^C(T)$ ie $[T(v)]_C = M_B^C(T)[v]_B$ ($j$th column of $M_B^C(T)$ is $[T(v_j)]_C$)

91. $\mathrm{Hom}_F(V, W)$ vector space

92. $\mathrm{Hom}_F(V, W) \cong M_{m \times n}(F)$ where $B = \{v_1, \dots, v_n\}$, $C = \{w_1, \dots, w_m\}$ bases for $V, W$ respectively via isomorphism $\Phi: \mathrm{Hom}_F(V, W) - M_{m \times n}(F) \ni \Phi(T) = M_B^C(T)$

93. $\dim \mathrm{Hom}_F(V, W) = (\dim V)(\dim W)$

94. $U, V, W$ vector spaces, $B, C, D$ bases, $S: U \to V$, $T: V \to W$ linear transformations $\Rightarrow T \circ S: U \to W$ linear

95. $M_B^D(T\circ S) = M_C^D(T)\, M_B^C(S)$

96. Matrix multiplication associative + distributive since function composition is

97. $P = M_C^B(I) \Rightarrow [v]_B = P[v]_C$ ie $P^{-1}[v]_B = [v]_C$

98. $M_C^C(T) = [T(c_j)]_C = P^{-1} M_B^B(T) P = (M_C^B(I))^{-1} M_B^B(T) M_C^B(I)$

99. Two matrices for the same linear operator are similar and similar matrices have the same linear operator

100. $T: V \to W$ linear transformation, $B, B'$ bases for $V$, $C, C'$ bases for $W$
$\Rightarrow M_B^C(T)[v]_B = [T(v)]_C$ and $M_{B'}^{C'}(T)[v]_{B'} = [T(v)]_{C'}$
$P[v]_{B'} = [v]_B$, $Q[w]_{C'} = [w]_C \Rightarrow Q^{-1} M_B^C(T) P = M_{B'}^{C'}(T)$

101. Matrices of a linear map wrt different bases are equivalent and equivalent matrices define the same linear map

102. $W_1, W_2$ subspaces of $V \Rightarrow W_1 + W_2$ smallest subspace of $V$ containing $W_1, W_2$

103. $V$ is the direct sum of $W_1, \dots, W_n$ if every $v \in V$ can be written as $v = w_1 + \dots + w_n$ with $w_i \in W_i$ uniquely

104. $V$ finite dimensional, $W_1, \dots, W_n$ subspaces with bases $B_1, \dots, B_n$.
$B = B_1 \cup \dots \cup B_n$ basis for $W_1 + \dots + W_n \iff W_1, \dots, W_n$ independent
(but $B$ always spans $W_1 + \dots + W_n$)

105. $W$ subspace of $V$ finite dimensional $\Rightarrow \exists W'$ a subspace $\ni V = W \oplus W'$

106. $V = W_1 \oplus W_2$, $W_1, W_2$ T-invariant, $B_1, B_2$ bases, $B = B_1 \cup B_2 \Rightarrow$
$$M_B^B(T) = \left[\begin{array}{c|c} M_{B_1}^{B_1}(T|W_1) & 0 \\ \hline 0 & M_{B_2}^{B_2}(T|W_2) \end{array}\right]$$ ie $M_B^B(T) = M_{B_1}^{B_1}(T|W_1) \oplus M_{B_2}^{B_2}(T|W_2)$

107. $V = W_1 \oplus W_2$, $W_1$ T-invariant, $B_1, B_2$ bases, $B = B_1 \cup B_2 \Rightarrow$
$$M_B^B(T) = \left[\begin{array}{c|c} M_{B_1}^{B_1}(T|W_1) & \sim \\ \hline 0 & \sim \end{array}\right]$$ ie block upper triangular

108. Similar matrices have the same eigenvalues

109. $B = \{v_1, \dots, v_n\}$ basis for $V$. Each $v_i$ is an eigenvector for $T \iff M_B^B(T)$ is diagonal

110. $A \in M_n(F)$, $A = M_C^C(T)$ for some basis $C$ of $V$. $A$ similar to diagonal matrix $\iff \exists$ basis for $V$ consisting of eigenvectors for $T$

111. Determinant Unique

112. $\det(AB) = \det(A)\det(B)$

113. $A$ invertible $\Leftrightarrow \det(A) \neq 0$

114. $T: V \to V$ linear operator, $V$ finite dimensional vector space, $B$ basis for $V$, $A = M_B^B(T)$, TFAE:
1) $T$ not invertible
2) $T$ not injective
3) $T$ not surjective
4) columns of $A$ are linearly dependent
5) columns of $A$ are not a basis
6) $\det A = 0$
7) $0$ eigenvalue of $T$

115. Eigenvalues of $T$ are the scalars $c \ni \det(cI - T) = 0$

116. $F$ field, $V$ finite dimensional vector space over $F$, $T: V \to V$ linear operator, $p(t)$ characteristic polynomial of $T$, $p(t)$ factors into distinct monic linear factors: $p(t) = (t - c_1)\dots(t - c_n) \Rightarrow V$ has a basis of eigenvectors for $T$: $B = \{v_1, \dots, v_n\}$ with $T(v_i) = c_i v_i$ and $M_B^B(T) = \begin{bmatrix} c_1 & & \\ & \ddots & \\ & & c_n \end{bmatrix}$

117. $V$ finite dimensional, $T$ linear operator, $p(t)$ factors into linear factors $\Rightarrow \exists B = \{v_1, \dots, v_n\}$ basis for $V \ni M_B^B(T)$ upper triangular ie $a_{ij} = 0$ for $i > j$

118. Orbit-Stabilizer Theorem $G$ acts on $X$, fix $x \in X$, $\exists$ bijection $\{\text{left cosets of } G_x \text{ in } G\} \longleftrightarrow \{\text{elements of the orbit } O_x\}$ given by $h \cdot G_x \longleftrightarrow h \cdot x$. ie $|O_x| = |G : G_x|$

119. $G$ acts on itself by left multiplication ie $g \cdot h = gh \Rightarrow$ action is transitive ie $xy^{-1} \cdot y = x$, faithful ie $g \cdot h = h \ \forall h \Rightarrow g = 1$, stabilizer free ie $g \cdot h = h$ for some $h \in H \Rightarrow g = 1$

120. Cayley's Theorem $|G| = n \Rightarrow G \cong$ subgroup of $S_n$

121. $G$ group, $H$ subgroup, $G$ acts on left cosets of $H$ in $G$ by left multiplication ie $g \cdot aH = gaH \Rightarrow$ we get homomorphism $G \to S_{G/H}$ and this action is transitive ie $ba^{-1} \cdot aH = bH$, stabilizer of $H \in G/H$ is $H$, stabilizer of $aH \in G/H$ is $aHa^{-1}$, kernel is $\bigcap_{a \in G} aHa^{-1}$

122. Largest normal subgroup of $G$ contained in $H$ is $K = \bigcap_{a \in G} aHa^{-1}$

123. $G$ acts on itself by conjugation ie $g \cdot a = gag^{-1} \Rightarrow$ the orbit of $a \in G$

is the conjugacy class $O_a = \{gag^{-1} \mid g \in G\}$ and the stabilizer of a is $G_a = C_G(a)$

124. G finite group, $a \in G \Rightarrow |O_a| = |G : C_G(a)|$

125. $|G| = |Z(G)| + |O_{a_1}| + \dots + |O_{a_s}|$ where $a_1, \dots, a_s$ are representatives for the conjugacy classes of size $> 1$

126. G p-group $\Rightarrow Z(G) \neq \{1\}$

127. A group of order $p^2$ is abelian and either $G \cong C_{p^2}$ or $G \cong C_p \times C_p$

128. All k-cycles are conjugate in $S_n$

129. Two permutations are conjugate in $S_n \Leftrightarrow$ they have the same cycle type

130. The conjugacy classes in $S_n$ are in a 1-1 correspondence with the partitions of n

131. $A_5$ is simple

132. $A_n$ simple $\forall n \geq 5$

133. Sylow's Theorem $|G| = p^r m$ where $p \nmid m$

(i) $Syl_p(G) \neq \phi$ ie Sylow p-subgroups exist

(ii) $P \in Syl_p(G)$, Q p-subgroup $\Rightarrow$ Q conjugate to a subgroup of P ie $\exists g \in G \ni gQg^{-1} \subseteq P$. And any two Sylow p-subgroups are conjugates to each other

(iii) $n_p(G) \equiv 1 \pmod p$. And $P \in Syl_p(G) \Rightarrow n_p(G) = |G : N_G(P)|$ ie $n_p(G) \mid |G|$ and so $n_p(G) \mid m$

134. A sylow p-subgroup is unique $\Leftrightarrow$ it is normal

135. $P \in Syl_p(G)$, Q p-subgroup $\Rightarrow Q \cap N_G(P) = Q \cap P$

136. $P \in Syl_p(G)$. TFAE:

(1) P unique ie $Syl_p(G) = \{P\}$ ie $n_p(G) = 1$

(2) P normal in G

(3) P characteristic subgroup

137. G simple group, $|G| = 60 \Rightarrow G \cong A_5$

138. $F = \tilde{W}/\sim$ is set of equivalence classes of $\tilde{W}$ (free group on S) is a group under $[v][w] = [vw]$, identity $[\_]$, $[a]^{-1} = [a^{-1}]$

139. $[abc\dots]^{-1} = [\dots c^{-1} b^{-1} a^{-1}]$

140. $F'$ commutator subgroup generated by all words of form $[w, w'] = ww'w^{-1}w'^{-1}$

$\Rightarrow F'$ isomorphic to the free group on infinitely letters. And $\forall n$ $\exists$ injective group homomorphism $F_n \hookrightarrow F_2$ where $F_n = \{a_1, \dots, a_n\}$ and $F_2 = \{a, b\}$

141. Neilson-Schrier Thm subgroups of free groups are free

142. Universal Mapping Property of Free Group $S$ set, $F = F_S$ free group on $S$, $G$ group, $f : S \to G$ function $\Rightarrow \exists!\, \varphi : F \to G$ group homomorphism $\ni \varphi([a]) = f(a)\ \forall a \in S$

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d] & G \\ F \arrow[ur, dashed, "\exists!\varphi"'] & \end{tikzcd} \qquad a \mapsto [a]$$

143. Every group is a homomorphic image of a free group

144. $\langle x|y \rangle = x^T A y \Rightarrow A$ can be recovered from the form, ie $a_{ij} = \langle e_i | e_j \rangle$

145. $\langle x|y \rangle = x^T A y$. The form is (skew-) symmetric $\Leftrightarrow A$ is

146. $A$ symmetric $\Leftrightarrow a_{ji} = a_{ij}\ \forall i,j$

147. $A$ skew symmetric $\Leftrightarrow a_{ji} = -a_{ij}\ \forall i,j$

148. $\langle v|w \rangle = [v]_B^T A [w]_B$, $\langle v|w \rangle = [v]_{B'} A' [w]_{B'}$

149. $\langle | \rangle$ bilinear form, $A$ matrix of the form wrt some basis $\Rightarrow$ the matrices of the form wrt other bases are of the form $P^TAP$ for invertible $P$

150. Any matrix representing the dot product must be symmetric and positive definite

151. $A \in M_n(\mathbb{R})$. TFAE:

(i) $A$ represents dot product on $\mathbb{R}^n$ wrt some basis

(ii) $A = P^TP$ for some $P \in GL_n(\mathbb{R})$

(iii) $A^T = A$ and $x^TAx \geq 0\ \forall x \in \mathbb{R}^n$ with equality iff $x = 0$

152. $\langle | \rangle$ symmetric, positive definite bilinear form on real finite dimensional vector space $V \Rightarrow \exists$ basis $u_1, \dots, u_n$ for $V$ which is orthonormal for $\langle | \rangle$ ie $\langle u_i | u_j \rangle = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$

153. $A$ represents the dot product $\Leftrightarrow A$ symmetric, positive definite

154. Spectral Theorem for Real Symmetric Matrices

155. $A \in M_n(\mathbb{R})$ symmetric $\Rightarrow \exists\, Q \in GL_n(\mathbb{R}) \ni Q^TAQ = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$

156. $\langle | \rangle$ symmetric bilinear form on $\mathbb{R}^n \Rightarrow \exists$ basis $u_1, \dots, u_n$ for $\mathbb{R}^n$ which is orthogonal wrt $\langle | \rangle$ and $\langle u_i | u_i \rangle = 1, -1,$ or $0$

157. $\langle\,|\,\rangle$ symmetric bilinear form not identically zero $\Rightarrow \exists u \in \mathbb{R}^n$ $\ni \langle u|u\rangle \neq 0$

158. $W^\perp$ subspace of $V$ where $W$ is a subspace of $V$

159. $W \subseteq W^{\perp\perp}$

160. $(W_1+W_2)^\perp = W_1^\perp \cap W_2^\perp$

161. $V^\perp \subseteq W^\perp$ $\forall$ $W$ subspace of $V$

160. $V^* = \{\varphi : V \to F \mid \varphi \text{ linear}\}$, $f^\# : V \to V^* \ni f^\#(v)(w) = f(v,w) \Rightarrow$ $\ker f^\# = N = V^\perp$

161. $f^\#$ injective $\Leftrightarrow f$ nondegenerate

162. $f$ symmetric bilinear form on $V$, $B = \{u_1, \dots, u_n\}$ basis for $V$, $A$ matrix of $f$ wrt $B$, $C = \{\lambda_1, \dots, \lambda_n\}$ dual basis $\Rightarrow M_B^C(f^\#) = A$ ie the matrix of the form is the same as the matrix of the linear transformation

163. $f$ symmetric bilinear form. $f$ nondegenerate $\Leftrightarrow$ its matrix $A$ is nonsingular (invertible)

164. $\langle\,|\,\rangle$ symmetric bilinear form on $V$, $u_1, \dots, u_n$ basis, $A$ matrix of $\langle\,|\,\rangle$ wrt $u_i$'s, $N = V^\perp \Rightarrow \dim N = n - \operatorname{rank} A$ ie rank $A$ independent of choice of basis

165. Sylvester's Law $p, m, z$ uniquely determined by $A$ (or $\langle\,|\,\rangle$) independent of choice of $Q$ (or of $u_1, \dots, u_n$) where
$$Q^T A Q = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix} = \begin{bmatrix} I_p & & \\ & -I_m & \\ & & 0_z \end{bmatrix}$$

166. $(A+B)^* = A^* + B^*$

167. $(AB)^* = B^* A^*$

168. $(A^{-1})^* = (A^*)^{-1}$

169. $A^{**} = A$

170. $A^* = A \Rightarrow$ diagonal entries are real

171. all entries of a matrix real. hermitian $\Leftrightarrow$ symmetric

172. $\langle z|w\rangle = [z]_B^* A [w]_B$ where $A$ hermitian

173. $A, A'$ represent same hermitian form wrt two bases $\Leftrightarrow A' = Q^* A Q$ for some invertible $Q$

174. Matrices representing the standard hermitian product on $\mathbb{C}^n$ are

of the form $A = Q^* Q$ for $Q$ invertible ie $A$ is hermitian and positive definite

175. $A$ orthogonal $\Leftrightarrow$ $A$ preserves dot product ie $(Ax)\cdot(Ay) = x \cdot y$

176. A product of orthogonal matrices is orthogonal

177. Inverse of an orthogonal matrix is orthogonal too ie true for transpose

178. $O(n) = \{A \in M_n(\mathbb{R}) \mid A \text{ orthogonal}\}$ is a group

179. $A \in O(n) \Rightarrow \det A = \pm 1$

180. $SO(n) = O(n) \cap SL_n(\mathbb{R}) = \{A \in O(n) \mid \det A = 1\}$ special orthogonal group is normal subgroup of $O(n)$

181. $A$ unitary $\Leftrightarrow$ $A$ preserves standard hermitian product $\langle x | y \rangle = x^* y$

182. $A$ unitary $\Leftrightarrow$ columns of $A$ are orthonormal wrt standard hermitian product

183. $A$ unitary $\Leftrightarrow$ $A$ preserves length ie $|Az| = |z|$ $\forall z \in \mathbb{C}^n$

184. $U(n) = \{A \in M_n(\mathbb{C}) \mid A \text{ unitary}\}$ is a group

185. $SU(n) = \{A \in U(n) \mid \det A = 1\}$ normal subgroup of $U(n)$

186. $B = \{u_1, \ldots, u_n\}$, $B' = \{u_1', \ldots, u_n'\}$ orthonormal bases, change of basis matrix $P = M_{B'}^{B}(I) \Rightarrow P$ unitary ie $P^* P = I$

187. Change of basis matrix between orthonormal bases wrt symmetric bilinear forms is orthogonal

188. $V$ hermitian space, $T: V \to V$ linear operator, $\forall v \in V$ $\exists! \, T^*(v) \ni$ $\langle T^* v | w \rangle = \langle v | Tw \rangle$ $\forall w \in V$

189. $\langle - | - \rangle$ symmetric bilinear or hermitian form on $V$ vector space, positive definite. $\langle v_1 | w \rangle = \langle v_2 | w \rangle$ $\forall w \in V \Rightarrow v_1 = v_2$

190. matrix of the adjoint of $T$ is the congugate transpose of the matrix of $T$

191. $(T^*)^* = T$ ie $\langle v | T^* w \rangle = \langle Tv | w \rangle$ $\forall v, w \in V$

192. $T: V \to V$ unitary $\Leftrightarrow$ $\langle Tv | Tw \rangle = \langle v | w \rangle$ $\forall v, w \in T$

193. $T$ self adjoint $\Rightarrow T$ normal

194. $T$ unitary $\Rightarrow T$ normal

195. $V$ hermitian space, $T: V \to V$ normal linear operator, $u \in V$ eigenvector with eigenvalue $\lambda \in \mathbb{C} \Rightarrow u$ eigenvector of $T^*$ with eigenvalue $\overline{\lambda}$

and span$(u)^\perp$ is an invariant subspace of $T$ and $T^*$

196. Spectral Theorem for Normal Operators $V$ hermitian space, $T: V \to V$ linear operator. TFAE:
(i) $T$ normal ie $T^*T = TT^*$
(ii) $\exists$ basis for $V$ consisting of eigenvectors for $T$ which are orthonormal wrt the form ie $V$ has an orthonormal eigenbasis

197. Spectral Theorem for Normal Matrices $A \in M_n(\mathbb{C})$. TFAE:
(i) $A$ normal ie $AA^* = A^*A$
(ii) $\exists P$ unitary, invertible matrix $\ni P^*AP = D$ diagonal ie $A$ unitarily diagonalizable

198. Spectral Theorem for Hermitian Operators $T: V \to V$ hermitian $\Rightarrow$
a) $\exists$ orthonormal eigenbasis
b) the eigenvalues are real

199. Spectral Theorem for Unitary Matrices $A$ unitary matrix $\Rightarrow$ $A$ unitarily diagonalizable

200. Spectral Theorem for Real Symmetric Matrices $V$ real vector space with a positive definite symmetric bilinear form, $T: V \to V$ symmetric ie $T^* = T$ $\Rightarrow$
(i) $\exists$ an orthonormal eigenbasis for $V$
(ii) eigenvalues of $T$ are real
ie $A \in M_n(\mathbb{R})$ symmetric is orthogonally diagonalizable:
$P^TAP = D$ diagonal for orthogonal $P$

201. $R$ commutative ring $\Rightarrow U(R) = \{u \in R \mid u \text{ unit}\}$ is an abelian group
202. $R$ division ring, $a \neq 0$, $ba = 1$, $ac = 1$ $\Rightarrow b = c$
203. $R$ field $\Rightarrow R$ integral domain
204. $\mathbb{Z}/n\mathbb{Z}$ integral domain $\Leftrightarrow n$ prime $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ field
205. Every finite integral domain is a field
206. $R[x]$ ring (with 1 if $1 \in R$)
207. $R$ integral domain $\Rightarrow R[x]$ integral domain
208. $R$ integral domain, $f, g \in R[x] \ni f, g \neq 0 \Rightarrow \deg(fg) = \deg f + \deg g$ and $\deg(f+g) \leq \max\{\deg f, \deg g\}$
209. $R$ integral domain, the units of $R[x]$ are the units of $R$

210. I left ideal $\Rightarrow$

(1) I closed under multiplication

(2) $0 \in I$

(3) $a \in I \Rightarrow -a \in I$

(4) $(I, +)$ abelian group

(5) I subring

211. $R/I$ ring with zero: $I$ (and $1 : 1+I$ if $1 \in R$)

212. R commutative $\Rightarrow R/I$ commutative

213. R commutative ring. R field $\Leftrightarrow$ only ideals of R are $(0)$ and R

214. $I_1, I_2 \lhd R \Rightarrow I_1 + I_2 \lhd R$

215. $\{I_k\}_{k \in A} \ni I_k \lhd R \ \forall k \Rightarrow \bigcap_{k \in A} I_k$

216. $I_1 + I_2$ smallest ideal of R containing both $I_1, I_2$, $I_1 + I_2 = \bigcap_{I_1, I_2 \subseteq I} I$

217. $I, J \lhd R \Rightarrow IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\} \lhd R$

218. $IJ \subseteq I \cap J$

219. $\varphi : R \to S$ ring homomorphism $\Rightarrow \varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, and
$\varphi : (R, +) \to (S, +)$ group homomorphism

220. $\varphi : R \to S$ ring homomorphism, $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$

221. $\varphi : R \to S$ ring homomorphism $\Rightarrow \ker\varphi \lhd R$

222. Every ideal I of R is the kernel of some homomorphism, namely
$I = \ker\begin{pmatrix} R \to R/I \\ r \mapsto r+I \end{pmatrix}$

223. <u>1st Isomorphism Theorem</u> $\varphi : R \to S$ ring homomorphism $\Rightarrow \varphi(R)$ subring of S and $R/\ker\varphi \cong \operatorname{Im}\varphi$ via the isomorphism $r + \ker\varphi \to \varphi(r)$

224. <u>2nd Isomorphism Theorem</u> R ring, S, T subrings of R, $T \lhd R \Rightarrow S+T$ subring of R and $S/S \cap T \cong S+T/T$ and $T \lhd S+T$

225. <u>3rd Isomorphism Theorem</u> R ring, $I, J \lhd R$, $I \subseteq J \Rightarrow J/I \lhd R/I$ and
$R/I \big/ J/I \cong R/J$

226. <u>4th Isomorphism Theorem</u> R ring, $I \lhd R \Rightarrow \exists$ bijection preserving inclusions between ideals of $R/I$ and ideals of R containing I

227. R ring with 1, $J \neq R$ ideal $\Rightarrow \exists M$ maximal ideal containing I

228. R commutative, $M \lhd R$. M maximal $\Leftrightarrow R/M$ field

229. R commutative, $I \lhd R$. I prime $\Leftrightarrow R/I$ integral domain

230. R integral $\Rightarrow (0)$ prime

231. R commutative. $M \triangleleft R$ maximal $\Rightarrow$ M prime

232. R commutative, $r \in R$ not nilpotent $\Rightarrow S = \{1, r, r^2, \dots\}$ multiplicative

233. R commutative, $S \subseteq R$ multiplicative. On $R \times S$: $(a,s) \sim (b,t) \Leftrightarrow$ $(at - bs)u = 0$ for some $u \in S$ is an equivalence relation.

234. $S^{-1}R$ set of equivalence classes, $\frac{a}{s} \ni \frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ and $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

235. $S^{-1}R$ commutative ring with identity with zero: $\frac{0}{s}$ $\forall s \in S$ and identity: $\frac{1}{1} = \frac{s}{s}$ $\forall s \in S$

236. $\exists$ ring homomorphism $\varphi: R \to S^{-1}R \ni \varphi(r) = \frac{r}{1}$ $\not\Rightarrow \ker\varphi = 0$

237. R integral domain $\Rightarrow \ker\varphi = 0 \Rightarrow \varphi: R \to S^{-1}R$ injective

238. $S \subseteq R$ multiplicative $\Rightarrow$ every element in S is a unit

239. Universal Property of Rings of Fractions $S \subseteq R$ multiplicative, $g: R \to T$ ring homomorphism $\ni g(s)$ unit in T $\forall s \in S \Rightarrow \exists!$ ring homomorphism $h: S^{-1}R \to T \ni h\phi = g$

$$\begin{tikzcd} & R \arrow[dl, "\phi"'] \arrow[dr, "g"] & \\ S^{-1}R \arrow[rr, dashed, "h"'] & & T \end{tikzcd}$$

240. K field, $h: K \to T$ nonzero ring homomorphism $\Rightarrow$ h injective

241. Chinese Remainder Theorem $I_1, \dots, I_n \triangleleft R$, $\varphi: R \to R/I_1 \times \dots \times R/I_n \ni$ $\varphi(r) = (r + I_1, \dots, r + I_n)$ is a ring homomorphism and $\ker\varphi = I_1 \cap \dots \cap I_n$. If $I_1, \dots, I_n$ pairwise comaximal, then $I_1 \cdots I_n = I_1 \cap \dots \cap I_n$ and $\varphi$ surjective so $R/I_1 \cdots I_n \cong R/I_1 \times \dots \times R/I_n$

242. $R \times S$ is never an integral domain

243. $m, n \in \mathbb{Z}^+ \ni (m,n) = 1 \Rightarrow \mathbb{Z}/\langle mn \rangle \cong \mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle$

244. p prime, p' associate of p $\Rightarrow$ p' prime

245. q irreducible, q' associate to q $\Rightarrow$ q' irreducible

246. R integral domain, p prime $\Rightarrow$ p irreducible

247. p prime. $p \mid a_1 \cdots a_n \Rightarrow p \mid a_i$ for some i

248. $p_1 \cdots p_n = q_1 \cdots q_m$ primes $\Rightarrow$ m = n and $\exists \sigma \in S_n \ni \forall i, p_i, q_i$ associates

249. R integral domain $\Rightarrow$

1) $a \mid b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$

2) a, b associates $\Leftrightarrow \langle a \rangle = \langle b \rangle$

3) $a \in R$ irreducible $\Leftrightarrow \langle a \rangle$ maximal among all proper principal ideals

4) $a \in R$ prime $\Leftrightarrow \langle a \rangle$ prime

5) b common multiple of $a_1, \dots, a_n \in R \Rightarrow \langle b \rangle \subseteq \langle a_1 \rangle \cap \dots \cap \langle a_n \rangle$

6) $d$ common divisor of $a_1,\dots,a_n \in R \Leftrightarrow \langle a_1\rangle+\dots+\langle a_n\rangle \subseteq \langle d\rangle$
7) $\langle a_1,\dots,a_n\rangle = \langle d\rangle \Rightarrow d=\gcd(a_1,\dots,a_n)$
250. $R$ PID, $a,b\in R \ni a,b\neq 0$, $d>0 \ni \langle d\rangle = \langle a,b\rangle \Rightarrow$
1) $d=\gcd(a,b)$
2) $\exists x,y\in R$ with $d=ax+by$
3) $d$ unique up to multiplication of a unit
251. In a PID, gcds exist
252. $R$ PID $\Rightarrow$ every nonzero prime ideal is maximal
253. $R$ integral domain $\ni R[x]$ PID $\Rightarrow R$ field
254. $F$ field $\Rightarrow F[x]$ PID
255. $R$ Euclidean domain, $a,b\in R \ni b\neq 0 \Rightarrow \exists$ gcd unique up to multiplication by a unit
256. Every Euclidean domain is a PID
257. $F$ field $\Rightarrow F[x]$ Euclidean domain $\Rightarrow F[x]$ PID
258. $R$ UFD. $p\in R$ irreducible $\Rightarrow p$ prime
259. $R$ ring with 1. TFAE:
1) $R$ left Noetherian
2) Every left ideal is finitely generated
3) Every nonempty set of left ideals of $R$ has a maximal element
260. $R$ PID $\Rightarrow R$ Noetherian
261. fields $\subseteq$ euclidean domains $\subseteq$ PID $\subseteq$ Noetherian
262. $R$ PID $\Rightarrow R$ UFD
263. Gauss lemma $f,g\in R[x]$ primitive $\Leftrightarrow fg$ primitive
264. $f\in R[x]$ nonconstant, irreducible in $R[x] \Rightarrow f$ irreducible in $K[x]$
265. $f$ primitive, irreducible in $K[x] \Rightarrow f$ irreducible in $R[x]$
266. $R$ UFD $\Rightarrow R[x]$ UFD
267. $F$ field. $f\in F[x]$ has a factor of degree 1 $\Leftrightarrow f$ has a root in $F$ i.e. $\exists \alpha\in F \ni f(\alpha)=0$
268. $R$ integral domain, $0\neq f\in R[x]$ primitive, $f=a_nx^n+\dots+a_0 \Rightarrow$
1) $\deg f = 2,3$. $f$ reducible in $R[x] \Leftrightarrow f$ has linear factor in $R[x]$
2) $a,b\in R$, $a$ nonunit. $f$ reducible in $R[x] \Leftrightarrow g(x)=f(ax+b)$ reducible in $R[x]$

3) S commutative ring, $\varphi: R \to S$ ring homomorphism, $\varphi(a_n) \neq 0$
$\hat{f}(x) = \varphi(a_n)x^n + \dots + \varphi(a_0) \in S[x]$. $\hat{f}$ irreducible in $S[x] \Rightarrow f$ irreducible in $R[x]$

269. R integral domain, $0 \neq f \in R[x] \ni f(0) \neq 0$ ie 0 is not a root of $f$. $f$ irreducible in $R[x] \Leftrightarrow$ its reciprocal $\hat{f}(x) = a_0x^n + \dots + a_n$ is irreducible in $R[x]$

270. Eisenstein's Criterion R UFD, K ring of fractions, $f = a_nx^n + \dots + a_0$ primitive, $\exists p \in K$ prime $\ni p \nmid a_n$ but $p \mid a_{n-1}, \dots, p \mid a_0$ and $p^2 \nmid a_0$ $\Rightarrow f$ irreducible in $R[x]$

271. F field, algebraically closed $\Rightarrow$ only irreducible polynomials in $F[x]$ are polynomials of degree 1

272. $\mathbb{C}$ algebraically closed

273. irreducible polynomials over $\mathbb{R}$ are linear polynomials and polynomials $ax^2+bx+c \ni a \neq 0$ and $\Delta = b^2 - 4ac < 0$

274. $f \in \mathbb{C}[x]$, $z$ root $\Rightarrow \bar{z}$ root of $\bar{f}$

275. F field, M module over F $\Rightarrow$ M vector space over F

276. M left R-module, $\varphi \neq N \subseteq M$. N submodule $\Leftrightarrow$
(i) $\forall x, y \in N$, $x+y \in N$
(ii) $\forall x \in N$, $\forall r \in R$, $rx \in N$

278. $\mathrm{Ann}_R(m)$ left ideal of R

279. $f: {}_RM \to {}_RN$ module homomorphism $\Rightarrow f(0) = 0$

280. $f: M \to N$ module homomorphism $\Rightarrow \ker f \leq M$ and $\mathrm{Im} \leq N$ are submodules

281. $\mathrm{Hom}_R(M,N)$ abelian group $\ni f, g \in \mathrm{Hom}_R(M,N) \Rightarrow (f+g)(x) = f(x) + g(x)$

282. R commutative ring. $\mathrm{Hom}_R(M,N)$ R-module $\ni (rf)(x) = rf(x) = f(rx)$

283. M R-module, N submodule of M $\Rightarrow M/N$ R-module

284. $\pi: M \to M/N \ni \pi(x) = x + N$ surjective homomorphism with $\ker \pi = N$

285. 1st Isomorphism Theorem $f: M \to N$ homomorphism $\Rightarrow \exists$ isomorphism $\hat{f}: M/\ker f \to \mathrm{Im} f \ni \hat{f}(x + \ker f) = f(x)$

286. 2nd Isomorphism Theorem $L, N \leq M \Rightarrow L+N/L \cong N/L\cap N$

287. 3rd Isomorphism Theorem $L \leq N \leq M \Rightarrow M/L \,/\, N/L \cong M/N$

288. 4th Isomorphism Theorem $N \leq M \Rightarrow \exists$ bijection preserving inclusions

between submodules of $M/N$ and submodules of $M$ containing

289. $L_1,\dots,L_k$ submodules of $M$. $L_1+\dots+L_k$ direct $\iff \forall x \in L_1+\dots+L_k$, $x$ can be written uniquely as $x = x_1+\dots+x_k$ with $x_i \in L_i$

290. $\bigoplus_{i\in I} M_i$ R-module with $(x_i)_{i\in I}+(y_i)_{i\in I} = (x_i+y_i)_{i\in I}$ and $r(x_i)_{i\in I} = (rx_i)_{i\in I}$

291. $L_1,\dots,L_k$ submodules of $M \ni L_1+\dots+L_k$ direct $\Rightarrow$ their external and internal sums are isomorphic as R-modules $\ni \varphi: \bigoplus L_i \to L_1 \oplus \dots \oplus L_k$ $\ni \varphi(x_1,\dots,x_k) = x_1+\dots+x_k$

292. $\{M_i\}_{i\in I}$ family of R-modules $\Rightarrow \forall j$ we have injective homomorphisms $k_j: M_j \to \bigoplus_{i\in I} M_i \ni k_j(m_j) = (x_i)_{i\in I}$ where $x_i = \begin{cases} m_j & i=j \\ 0 & i\neq j \end{cases}$ ie in $M_1 \oplus M_2$, we have $k_1: M_1 \to M_1 \oplus M_2 \ni x_1 \to (x_1, 0)$ and $k_2: M_2 \to M_1 \oplus M_2 \ni x_2 \to (0, x_2)$

293. $\prod M_i$ R-module $\ni (m_i)_{i\in I} + (m_i')_{i\in I} = (m_i+m_i')_{i\in I}$ and $r(m_i)_{i\in I} = (rm_i)_{i\in I}$

294. $|I| < \infty \Rightarrow \prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$, $|I|$ infinite $\Rightarrow \prod_{i\in I} M_i \neq \bigoplus_{i\in I} M_i$

295. $S \subseteq F$ module, $S$ basis $\iff \langle S \rangle = F$ and $S$ linearly independent

296. $F$ R-module, $\phi \neq S = \{e_i\}_{i\in I} \subseteq F$. $S$ basis of $F \iff F = \bigoplus_{i\in I} Re_i$

297. ${}_R Re_i \cong {}_R R \ni re_i \longleftrightarrow r \iff F \cong \bigoplus_{i\in I} R = R^{(I)}$

298. R-module free $\iff$ it is isomorphic to a direct sum of copies of ${}_R R$

299. Direct sum of free modules is free

300. $R$ ring, $S$ set $\Rightarrow \exists F$ a free R-module having $S$ as a basis

301. Universal Property of Free Modules $S$ set, $F$ R-module. $F$ free with basis $S \iff \forall M$ R-module and map $f: S \to M$ $\exists!$ R-homomorphism $\hat{f}: F \to M$ with $\hat{f}|_S = f$

$$\begin{tikzcd} S \arrow[r, hook] \arrow[d, "f"'] & F \arrow[dl, dotted, "\exists!\,\hat{f}"] \\ M & \end{tikzcd}$$

302. If we want to find a homomorphism from a free module $F$ to a module $M$ it is enough to know where the basis elements go

303. Every module is a quotient of some free module

304. $F$ free module, $\exists g: L \to F$ surjective homomorphism $\Rightarrow \exists f \ni f: F \to L$ homomorphism with $g \circ f = 1_F$ and $L = \ker g \oplus X$ where $X \cong F$

305. $L, N$ modules, $I \triangleleft R$, $M = L \oplus N \Rightarrow IM = IL \oplus IN$

306. $R$ commutative, $R^n \cong R^m$ for some $m, n \in \mathbb{Z}^+ \Rightarrow m = n$

307. $M$ module, $N$ maximal submodule $\Rightarrow M/N$ simple

308. $S$ simple module $\Rightarrow S$ cyclic

309. $S$ simple $R$-module $\Rightarrow S \cong R/I$ where $I$ maximal left ideal

310. Schur's Lemma $_RS$ simple module, $f: S \to S$ nonzero homomorphism $\Rightarrow f$ isomorphism

311. $End_R(M)$ is a ring under $(f+g)(m) = f(m)+g(m)$ and $fg = f \circ g$

312. $M$ $R$-module, $e: M \to M$ idempotent homomorphism $\Rightarrow M = \ker e \oplus \operatorname{Im} e$

313. $R$ ring, $M$ left module. TFAE:
1) Every ascending chain of submodules stabilizes ie $M$ noetherian
2) Every submodule of $M$ is finitely generated
3) Every nonempty set of submodules has a maximal element

314. $M$ $R$-module, $L \leq M$. $L$, $M/L$ finitely generated $\Rightarrow M$ finitely generated

315. $M$ $R$-module, $L \leq M$. $M$ noetherian $\Leftrightarrow L, M/L$ noetherian

316. $M_1, \ldots, M_n$ noetherian $R$-modules $\Rightarrow \bigoplus_{i=1}^{n} M_i$ noetherian

317. $R$ left noetherian $\Rightarrow$ every finitely generated free $R$-module is noetherian

318. $R$ noetherian, $M$ finitely generated over $R \Rightarrow {}_RM$ is noetherian

319. $R$ PID, $M$ finitely generated over $R \Rightarrow M$ noetherian

320. $Tor(M) \leq M$

321. $R$ PID, $F$ finitely generated torsion-free, $M$ submodule of $F \Rightarrow M$ free and $\operatorname{rank} M \leq \operatorname{rank} F$

322. $F$ free, finitely generated over PID, $M \leq F \Rightarrow M$ free

323. $M(p) \leq M$ is a submodule

324. $R$ commutative, $S \subseteq R$ multiplicative, $M$ $R$-module $\Rightarrow M_S$ $R_S$-module

325. $R$ integral domain, $k = R_S$ field of fractions of $R$ ie $S = R \setminus \{0\}$, $M$ $R$-module, $x_1, \ldots, x_n \in M$. $x_1, \ldots, x_n$ linearly independent over $R \Leftrightarrow \frac{x_1}{1}, \ldots, \frac{x_n}{1}$ linearly independent over $K$

326. $R$ commutative, $S \subseteq R$ multiplicative, $M$ $R$-module, $M = \langle A \rangle$ for some $A \subseteq M \Rightarrow M_S = \langle B \rangle$ where $B = \{\frac{a}{1} \mid a \in A\}$

327. $R$ integral domain, $F$ free $R$-module of rank $n \Rightarrow$ any $n+1$ or more elements of $F$ are linearly dependent

328. $M$ finitely generated torsion module over PID $\Rightarrow \operatorname{ann}_R M \neq 0$

329. $M$ finitely generated, $P$-primary $\Rightarrow \exists k \geq 1 \ni p^k x = 0 \ \forall x \in M$

330. $M$ finitely generated torsion module over PID $R \Rightarrow \exists$ prime elements

$p_1,\dots,p_n \in R \ni M = \overset{n}{\underset{i=1}{\oplus}} M(p_i)$ and this decomposition is unique ie if $M = \overset{m}{\underset{i=1}{\oplus}} M(q_i)$ for $q_1,\dots,q_m$ prime then $m=n$ and after rearranging we have $p_i = u_i q_i$ for $u_i$ units

331. F free over R integral domain $\Rightarrow$ rank F = largest # linearly independent elements of F

332. R integral domain, F free of rank n, G free submodule of F $\Rightarrow$ rank $G \le n$

333. R PID, F free of rank n $\Rightarrow$ every submodule of F is free of rank $\le n$

334. R PID, M finitely generated $\Rightarrow$ M is a direct sum of cyclic submodules where each summand is either P-primary for some prime ideal P or free

335. $M \cong \text{Tor} M \oplus M/\text{Tor} M \cong \text{Tor} M \oplus R^k \cong \overset{n}{\underset{i=1}{\oplus}} M(p_i) \oplus R^k$

336. M cyclic $\Leftrightarrow$ $\dim M/pM = 1$ over field $R/\langle p \rangle$

337. M P-primary $\Rightarrow$ M decomposes into $d_p(M)$ cyclic submodules

338. M P-primary $\Rightarrow$ number of cyclic summands whose annihilator is $\langle p^{n+1} \rangle$ is $U_p(n, M)$

339. Two finitely generated torsion modules over a PID are isomorphic $\Leftrightarrow$ they have the same elementary divisors

340. R PID, F free module of rank n, $G \le F$, $y_1, \dots, y_n$ basis of F $\Rightarrow \exists a_1,\dots,a_m \in R$ $\ni a_1 | a_2 | \dots | a_m$ and $a_1 y_1, \dots, a_m y_m$ is a basis of G where rank $G = m \le n$

341. <u>Invariant Factor Thm</u> M finitely generated over PID R $\Rightarrow \exists a_1, \dots, a_m \in R$ with $a_1 | a_2 | \dots | a_m \ni M \cong R/\langle a_1 \rangle \oplus \dots \oplus R/\langle a_m \rangle \oplus R^k$

342. $\text{ann}_R M = \langle a_m \rangle$

343. M, N finitely generated torsion modules. $M \cong N \Leftrightarrow$ they have the same invariant factors

344. M P-primary over PID $\Rightarrow$ elementary factor and invariant factor decompositions are the same

345. M finitely generated torsion module over PID $\Rightarrow$
1) elementary divisors of M are the prime power factors of invariant factors of M
2) largest invariant factor is obtained by multiplying largest of prime powers among the elementary divisors

346. V vector space over F $\Rightarrow \exists$ bijection $\{F[x]\text{-modules } V\} \longleftrightarrow \{\text{Linear maps } V \to V\}$

347. $V^T \cong V^S \iff A, B$ similar where $T, S: V \to V$, $V^S, V^T$ corresponding $F[x]$-modules, $A, B$ are matrices of $T, S$

348. $B = \{e_1, \dots, e_n\}$ basis of $V$ over $F$, $T: V \to V$ linear $\Rightarrow$ if $\forall i$ $Te_i = \sum_{j=1}^{n} a_{ji} e_j$, $a_{ji} \in F$ then $A = (a_{ij})$ is the matrix of $T$ wrt $B$

349. $B'$ another basis of $V$, $A'$ matrix of $T$ wrt $B'$ $\Rightarrow$ $A \sim A'$ and $\det A = \det A'$

350. $\{F[x]\text{-submodules of } V\} \longleftrightarrow \{T \text{ invariant subspaces of } V\}$

351. $V_\lambda$ $T$-invariant subspace of $V$ ie $V_\lambda$ $F[x]$-submodule of $V$

352. $0 \neq v \in V$ eigenvector corresponding to $\lambda \iff \operatorname{ann}_{F[x]} v = \langle \lambda - x \rangle$

353. $\operatorname{ann} V_\lambda = \langle \lambda - x \rangle$

354. $T: V \to V$ diagonalizable $\iff$ $V$ has basis of eigenvectors $\{e_1, \dots, e_n\}$

355. $T: V \to V$ linear, $\dim V = n$. $T$ diagonalizable $\iff$ as an $F[x]$-module $V$ decomposes as $V = F[x]/\langle x - c_1 \rangle \oplus \dots \oplus F[x]/\langle x - c_n \rangle$ for some $c_1, \dots, c_n \in F$

356. Rational Canonical Form $T: V \to V$ linear, $\dim V = n < +\infty \Rightarrow \exists$ basis of $V \ni$ the matrix of $T$ wrt that basis is block diagonal $\begin{bmatrix} C_1 & & \\ & \ddots & \\ & & C_s \end{bmatrix}$ where $\forall i$, $C_i$ is the companion matrix of some monic polynomial $a_i(x)$ and $a_1(x) \mid a_2(x) \mid \dots \mid a_s(x)$. This representation is unique

357. $V$ finite dimensional over $F$, $T: V \to V$ linear, $W \leq V$ $F[x]$-submodule ie $T$-invariant subspace. $W$ cyclic $F[x]$-module $\iff \exists v \in W$ and $n \geq 1$ $\ni \{v, T(v), \dots, T^{m-1}(v)\}$ is a basis of $W$ over $F$.

358. $T: W \to W$ linear, $W$ cyclic $F[x]$-module with generator $v$, $g(x) \in F[x]$ monic $\ni \langle g(x) \rangle = \operatorname{ann}_{F[x]} v$, $g(x) = x^s + c_{s-1}x^{s-1} + \dots + c_1 x + c_0$ $\Rightarrow B = \{v, Tv, \dots, T^{s-1}v\}$ $F$-basis of $W$ and matrix of $T$ wrt $B$ is the companion matrix of $g(x)$

359. $T, S: V \to V$, $V$ finite dimensional over $F$. TFAE:
1) $T, S$ similar
2) $F[x]$-modules obtained from $S, T$ are isomorphic
3) $S, T$ have same rational canonical form

360. $a(x)$ monic polynomial in $F[x]$, $C$ its companion matrix $\Rightarrow$ $a(x)$ characteristic polynomial of $C$

361. $\operatorname{char} A$ is monic of degree $n$

362. $\lambda \in F$ eigenvalue of $T \iff \lambda$ root of $\operatorname{char} T$ (or matrix $A$)

363. Cayley Hamilton $T: V \to V$ linear, $\dim V = n \Rightarrow \operatorname{char} T$ annihilates $T$

364. $m(x) \mid \text{char}\, T$

365. The minimal polynomial and the characteristic polynomial have the same roots

366. Diagonalization over Euclidean Domains $R = F[x]$ with $F$ field, ie $R$ Euclidean domain, $A \in M_n(R)$. Allowable operations
1) Interchange rows/columns
2) multiply row/column by units in $R$
3) add scalar multiple of a row/column to another row/column

$\exists$ sequence of operations $\ni A \sim \begin{bmatrix} u_1 & & & & & \\ & \ddots & & & & \\ & & u_t & & & \\ & & & a_1 & & \\ & & & & \ddots & \\ & & & & & a_s \end{bmatrix}$ where $u_1, \dots, u_t$ units, $a_1 \mid a_2 \mid \dots \mid a_s$. If $R$ field, $A \sim \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$

367. $xI - A \sim \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & a_1 & & \\ & & & & \ddots & \\ & & & & & a_s \end{bmatrix} \Rightarrow a_1(x) \mid \dots \mid a_s(x)$ invariant factors

368. $W \cong F[x]/\langle (x-\lambda)^n \rangle$, $v$ generator of cyclic $F[x]$-module $W \Rightarrow$ $\{v, (T-\lambda I)v, \dots, (T-\lambda I)^{n-1}v\}$ basis of $W$ over $F$

369. $T: V \to V$ linear, $V$ finite dimensional over $F$. $\exists B$ basis of $V \ni$ the matrix of $T$ wrt $B$ is in Jordan Canonical Form $\Leftrightarrow$ characteristic polynomial of $T$ is a product of linear polynomials

370. $F$ algebraically closed $\Rightarrow$ every linear transformation has a Jordan Canonical form in some basis

371. $T$ diagonalizable $\Leftrightarrow$ minimal polynomial of $T$ is a product of distinct monic linear polynomials

372. $F$ field $\Rightarrow$ either $\text{char}\, F = 0$ or $\exists p$ prime $\ni \text{char}\, F = p$

373. $F$ field, $\text{char}\, F = 0 \Rightarrow$ prime subfield of $F$ is isomorphic to $\mathbb{Q}$

374. $h: K \to F$ nonzero homomorphism, $K, F$ fields $\Rightarrow h$ injective

375. $F \subset E$ field extension $\Rightarrow E$ vector space over $F$ and $[E:F] = \dim_F E$

376. $F$ finite, $\text{char}\, F = p \Rightarrow |F| = p^n$

377. $p(x)$ irreducible with coefficients in $F$ field $\Rightarrow \exists K$ a field extension of $F$ in which $p(x)$ has a root

378. $p(x) \in F[x]$ irreducible of degree $n$, $\alpha \in K = F[x]/\langle p(x) \rangle$ root of $p(x) \in K[x] \Rightarrow 1, \alpha, \dots, \alpha^{n-1}$ basis of $K$ over $F$

379. $F[\alpha] \subseteq F(\alpha)$

380. $F \subset E$, $\alpha \in E$ algebraic over $F \Rightarrow F(\alpha) = F[\alpha]$ and $[F(\alpha):F] = \deg \text{Irr}(\alpha, F) < \infty$

381. $F \subset E$, $\alpha \in E$, $F[\alpha] = F(\alpha) \Rightarrow \alpha$ algebraic over $F$

382. $F \subset E \subset K \Rightarrow [K:F] = [K:E][E:F]$

383. $F \subset E$ finite $\Rightarrow F \subset E$ algebraic

384. $F \subset E$, $K = \{\alpha \in E \mid \alpha$ algebraic over $F\} \Rightarrow K$ contains $F$ and is a subfield of $E$

385. $\mathbb{Q} \subset \mathbb{A}$ algebraic

386. $F \subset E$, $\alpha_1, \ldots, \alpha_n \in E \Rightarrow F(\alpha_1, \ldots, \alpha_n)$ is the compositum of $F(\alpha_1), \ldots, F(\alpha_n)$ and $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1) \ldots (\alpha_n)$

387. $F \subset E$ finite $\rightarrow F \subset E$ finitely generated

388. $\begin{tikzcd}[column sep=small, row sep=small] & EK \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash] & & E \arrow[dl, dash] \\ & F & \end{tikzcd}$ finite extensions $\Rightarrow [EK:F] \leq [K:F][E:F]$ with equality $\Leftrightarrow$ a basis of $E$ or $K$ over $F$ is linearly independent over the other

389. $\begin{tikzcd}[column sep=small, row sep=small] & EK \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash, "n"'] & & E \arrow[dl, dash, "m"] \\ & F & \end{tikzcd}$ but $\gcd(m,n) = 1 \Rightarrow [EK:F] = mn$

390. $F \subset E$ simple extension $\Rightarrow F \subset E$ finitely generated

391. $F$ field, $f \in F[x]$ nonconstant $\Rightarrow \exists$ splitting field of $f$

392. $E$ splitting field of $f(x) \in F[x]$, $\alpha_1, \ldots, \alpha_n$ roots of $f$ in $E \Rightarrow E = F(\alpha_1, \ldots, \alpha_n)$

393. $E$ splitting field of $\mathcal{F} \subset F[x] \Rightarrow E = F(R)$ where $R = \bigcup_{f \in \mathcal{F}} R_f$ with $R_f = \{$roots of $f$ in $E\}$

394. $E$ splitting field over $F \Rightarrow E$ algebraic over $F$

395. Every family $\mathcal{F} \subseteq K[x]$ has a splitting field

396. Any two splitting fields of a family $\mathcal{F} \subseteq K[x]$ are isomorphic over $F$

397. $E$ splitting field of $f(x) \in K[x]$ and $\deg f = n \Rightarrow [E:K] \mid n!$

398. Every field $K$ has an algebraic closure $E$ unique up to $K$ isomorphism

399. $K$ field. TFAE:

1) $K$ algebraically closed
2) every nonconstant $f \in K[x]$ splits in $K$
3) $K \subset F$ algebraic $\Rightarrow F = K$

400. algebraic closure of $K$ is a splitting field of $K[x]$ over $K$

401. $K = \overline{K} \Rightarrow K$ algebraically closed

402. $F \subset E$ algebraic $\Rightarrow |E| \leq |F[x]|$

403. Every algebraically closed field is infinite

404. $G$ finite abelian group. TFAE:

1) G has a cyclic sylow p-subgroup $\forall p$ prime $\ni p \mid |G|$
2) G cyclic
3) $\forall$ prime $p \ni p \mid |G|$, G has a unique subgroup of order p
405. F field, G finite subgroup of multiplicative group $F^* = F \setminus \{0\} \Rightarrow$ G cyclic
406. F finite field $\Rightarrow F^*$ cyclic
407. F finite field, $x \in F \Rightarrow x = x^{p^n}$
408. $K \subset E$ finite, $E = K(\alpha)$ for some $\alpha \in E \Leftrightarrow \exists$ finitely many intermediate fields
409. K perfect $\Rightarrow$ every finite extension is simple
410. $K \subset E$ algebraic. TFAE:
1) E splitting field of some family $\mathcal{F} \subseteq K[x]$
2) Every irreducible polynomial $f(x) \in K[x]$ having a root in E splits in E ie $K \subset E$ normal
3) Every K-embedding $\sigma: E \to \overline{E}$ maps E to E
4) Every K-isomorphism $\sigma: \overline{E} \to \overline{E}$ maps E to E
411. $K \subset E$ finite. $K \subset E$ normal $\Leftrightarrow$ E splitting field of a polynomial $f \in K[x]$
412. $K \subset F \subset E$, $K \subset E$ algebraic $\Leftrightarrow F \subset E$ algebraic and $K \subset F$ algebraic
413. $F \subset E$, E splitting field of $f \in F[x]$, $f(x) = c(x-\alpha_1)^{n_1} \dots (x-\alpha_t)^{n_t}$, $\alpha_i$ distinct in E. f separable $\Leftrightarrow n_1 = \dots = n_t = 1$
414. $(f+g)' = f' + g'$, $(cf)' = cf'$ $\forall c \in F$, $(fg)' = f'g + g'f$
415. $f \in F[x]$ has a multiple root $\alpha$ in some extension field $\Leftrightarrow \alpha$ is also a root of $f'$
416. f separable $\Leftrightarrow \gcd(f, f') = 1$ in $F[x]$
417. char $F = 0$, $f \in F[x]$ irreducible $\Rightarrow$ f separable
418. char $F = 0$, $F \subset E$ algebraic $\Rightarrow F \subset E$ separable
419. $f \in F[x]$ separable $\Leftrightarrow$ f has distinct roots in its splitting field
420. $K \subset F \subset E$. $E/K$ separable $\Leftrightarrow E/F$ and $F/K$ separable
421. F field, $\exists f \in F[x]$ inseparable $\Rightarrow$ char $F = p > 0$ and F infinite
422. over a finite field or field of char 0, every polynomial is separable
423. $F \subset E$ finite, algebraic, char $F = 0$ or $|F| < \infty \Rightarrow F \subset E$ separable
424. char $F = 0$, E splitting field of some $f \in F[x] \Rightarrow E/F$ is Galois
425. Fix(H) is a subfield of E
426. $F \subset E \Rightarrow F \subset \mathrm{Fix}(\mathrm{Gal}(E/F))$

427. $f(H) = Fix(H)$, $g(K) = Gal(E/K) \Rightarrow$

1) $\forall H \in \mathcal{G}$, $H \subseteq g(f(H))$

2) $\forall K \in \mathcal{F}$, $K \subseteq f(g(K))$

3) $H_1 \leq H_2 \in \mathcal{G} \Rightarrow f(H_2) \subset f(H_1)$

4) $K_1, K_2 \in \mathcal{F} \Rightarrow g(K_2) \leq g(K_1)$

428. Fundamental Theorem of Galois Theory $E/F$ Galois extension with Galois group $G$ $\Rightarrow$

1) $f: \mathcal{G} \to \mathcal{F}$ and $g: \mathcal{F} \to \mathcal{G}$ are bijections, inverse to each other

2) $g(K) = H \Rightarrow [E:K] = |H|$ and $[K:F] = |G:H|$

3) $g(K) = H$, $\sigma \in G \Rightarrow g(\sigma(K)) = H^{\sigma} = \sigma^{-1} H \sigma$

Then $H \trianglelefteq G \Leftrightarrow K/F$ is a Galois extension

In this case $Gal(K/F) = G/H$

**Algebra Preliminary Examination, August 22, 2005**

Print name: Score:

**Show your work, provide all necessary proofs and counterexamples. There are 10 problems on 20 pages worth the total of 100 points. Check that you have a complete exam.**

1. (a) (5 points) How many elements of order 6 are there in the symmetric group $S_7$?

| Partition/Cycle Type | Representative | order | Number/Size |
|---|---|---|---|
| 7 | (1234567) | 7 | |
| 6+1 | (123456) | 6 | $\binom{7}{6}5! = 7\cdot120 = 840$ |
| 5+2 | (12345)(67) | lcm(5,2) = 10 | |
| 5+1+1 | (12345) | 5 | |
| 4+3 | (1234)(567) | lcm(4,3) = 12 | |
| 4+2+1 | (1234)(56) | lcm(4,2) = 4 | |
| 4+1+1+1 | (1234) | 4 | |
| 3+3+1 | (123)(456) | lcm(3,3) = 3 | |
| 3+2+2 | (123)(45)(67) | lcm(3,2) = 6 | $\binom{7}{3}\binom{4}{2}2! = 35\cdot6\cdot2 = 60$ |
| 3+2+1+1 | (123)(45) | lcm(3,2) = 6 | $\binom{7}{3}\binom{4}{2}2! = 60$ |
| 3+1+1+1+1 | (123) | 3 | |
| 2+2+2+1 | (12)(34)(56) | lcm(2,2) = 2 | |
| 2+2+1+1+1 | (12)(34) | lcm(2,2) = 2 | |
| 2+1+1+1+1+1 | (12) | 2 | |
| 1+1+1+1+1+1+1 | 1 | 1 | |

∴ There are 840+60+60 = 960 elements of order 6 in $S_7$

X

1470

1. (continued)
(b) (5 points) How many conjugacy classes in $S_7$ consist of elements of order 6?

by (a) there are 3 conjugacy classes in $S_7$ consisting of elements of order 6 since in $S_n$ elements are conjugate iff they have the same cycle type

2. (10 points) Show that a group of order 48 cannot be simple.

$|G| = 48 = 2^4 \cdot 3$

Then $n_3(G) \equiv 1 \pmod 3$ and divides 16

So $n_3(G) = 1, \cancel{2}, 4, \cancel{8}, 16$

$\therefore n_3(G) = 1, 4, 16$

And $n_2(G) \equiv 1 \pmod 2$ and divides 3

So $n_2(G) = 1, 3$

Now suppose that $n_3(G) = 4$ and let $P \in Syl_3(G)$

Then $|G : N_G(P)| = 4$

Consider action of $G$ on $G/N_G(P)$

Then we have homomorphism $\varphi : G \to S_{G/N_G(P)} \cong S_4$

If $\varphi$ is injective, then $|\varphi(G)| = 48$

But also $\varphi(G) \leq S_4 \Rightarrow |\varphi(G)| \mid 4! = 24$

But $48 \nmid 24$

$\therefore \varphi$ not injective

$\therefore \ker\varphi \neq \{1\}$

But also $\ker\varphi \neq G$ since action of $G$ on $G/N_G(P)$ is not trivial since $N_G(P) \neq G$

$\therefore G$ has a nontrivial, proper normal subgroup, namely $\ker\varphi$

$\therefore G$ not simple

So assume that $n_3(G) = 16$ and $n_2(G) = 3$

Let $P, P' \in Syl_3(G)$

Then $|P \cap P'| = 1, 3$ by lagrange since $P \cap P' \leq P, P'$

so $P \cap P' = \{1\}$ or $P = P'$

Then $G$ has 16 cyclic subgroups of order 3 each having 2 elements of order 3

That is $16 \cdot 2 = 32$ elements

And let $Q, Q' \in Syl_2(G)$

Then $|Q \cup Q'| = |Q| + |Q'| - |Q \cap Q'| = 32 - |Q \cap Q'|$

But $|Q \cap Q'| \mid 16$ by lagrange but $Q \neq Q' \Rightarrow |Q \cap Q'| \neq 16$

so $|Q \cap Q'| \leq 8$

Then $|Q \cup Q'| = 32 - |Q \cap Q'| \geq 32 - 8 = 24$

so we have $32 + 24 = 56$ elements

Contradiction since $|G| = 48$

$\therefore$ At least one of $n_3(G), n_2(G)$ must be 1

Then $G$ has a unique sylow 3 or 2-subgroup

$\therefore G$ has a normal nontrivial, proper subgroup

$\therefore G$ not simple

4

(continued)

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

The stabilizer in K of H is $K_H = \{k \in K \mid k \cdot H = H\}$

$= \{k \in K \mid kH = H\}$

$= \{k \in K \mid k \in H\}$

$= H \cap K$

(b) (3 points) Show that $[K : H \cap K] \leq [G : H]$.

Note that $|O_H|_K| = |K : K_H|$ by Orbit Stabilizer Thm

$= |K : H \cap K|$ by (a)

And $|O_H|_K| \leq |O_H| = |G : G_H|$ Again by orbit Stabilizer

And $G_H = \{g \in G \mid g \cdot H = H\} = \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} = H$

So $|O_H|_K| \leq |O_H| = |G : G_H| = |G : H|$

$\therefore |K : H \cap K| \leq |G : H|$

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

$|G:H\cap K| = |G:K||K:H\cap K| \leq |G:K||G:H|$ by (b)

$\therefore |G:H\cap K| \leq |G:K||G:H|$

4. Let $A$ be a real, symmetric $m \times m$ matrix.
(a) (5 points) Show that the eigenvalues of $A$ are real.

Let v be eigenvector of A associated with eigen value $\lambda$
Then $Av = \lambda v$

Consider $(v^*Av)^* = v^*A^*v = v^*\bar{A}^Tv = v^*A^Tv$ since A real
$= v^*Av$ since A symmetric

$\therefore (v^*Av)^* = v^*Av$

So $(v^*\lambda v)^* = v^*\lambda v \Rightarrow (\lambda v^*v)^* = \lambda v^*v \Rightarrow \bar{\lambda} v^*v = \lambda v^*v$

$\therefore \bar{\lambda} = \lambda$

$\therefore \lambda$ real

$\therefore$ The eigenvalues of A are real

4. (continued)

(b) (5 points) Show that eigenvectors corresponding to distinct eigenvalues are orthogonal.

Let $\lambda_1, \lambda_2$ be distinct eigenvalues
And let $v_1, v_2$ be their corresponding eigenvectors
Then show $v_1 \cdot v_2 = 0$

$Av_1 \cdot v_2 = \lambda_1 v_1 \cdot v_2 = \lambda(v_1 \cdot v_2)$

But since A symmetric, $Av_1 \cdot v_2 = (Av_1)^T v_2 = v_1^T A^T v_2 = v_1^T A v_2$
$= v_1 \cdot A v_2$

So $Av_1 \cdot v_2 = v_1 \cdot Av_2 = v_1 \cdot \lambda_2 v_2 = \lambda_2(v_1 \cdot v_2)$

$\therefore \lambda_1(v_1 \cdot v_2) = \lambda_2(v_1 \cdot v_2)$

$\therefore \lambda_1(v_1 \cdot v_2) - \lambda_2(v_1 \cdot v_2) = 0$

$\therefore (\lambda_1 - \lambda_2)(v_1 \cdot v_2) = 0$

But $\lambda_1 - \lambda_2 \neq 0$ since $\lambda_1, \lambda_2$ distinct

so $v_1 \cdot v_2 = 0$

$\therefore v_1, v_2$ 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 the 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) (2 points) Prove that $B(f,g)$ is a bilinear form on $V$; first define a bilinear form.

Let $V$ be a vector space over $F$. A bilinear form on $V$ is a function $f: V \times V \to F \ni (v,w) \to f(v,w)$ and

1) $f(v_1+v_2, w) = f(v_1,w) + f(v_2,w)$, $f(v, w_1+w_2) = f(v,w_1) + f(v,w_2)$

2) $f(cv,w) = cf(v,w)$, $f(v,cw) = cf(v,w)$ $\forall v, w, v_1, v_2, w_1, w_2 \in V, c \in F$

$B(f_1+f_2, g) = \int_0^\pi (t+1)(f_1(t)+f_2(t))g(t)dt = \int_0^\pi (t+1)(f_1(t)g(t) + f_2(t)g(t))dt$

$= \int_0^\pi (t+1)f_1(t)g(t)dt + \int_0^\pi (t+1)f_2(t)g(t)dt = B(f_1,g) + B(f_2,g)$

Similarly $B(f, g_1+g_2) = B(f,g_1) + B(f,g_2)$

And $B(cf,g) = \int_0^\pi (t+1)cf(t)g(t)dt = c\int_0^\pi (t+1)f(t)g(t)dt = cB(f,g)$

Similarly $B(f,cg) = cB(f,g)$

$\therefore B(f,g)$ bilinear form on $V$

(b) (2 points) Give the definition of a symmetric bilinear form. Is $B(f,g)$ symmetric?

A bilinear form is symmetric if $f(v,w) = f(w,v)$ $\forall v, w \in V$

Clearly $B(f,g) = B(g,f)$ $\forall g, f \in V$

$\therefore B(f,g)$ symmetric

5. (continued)

(c) (3 points) Give the definition of a positive definite real quadratic form and determine whether the quadratic form associated to $B(f,g)$ is positive definite.

The quadratic form associated to a symmetric bilinear form $\langle \cdot | \cdot \rangle$ on $V$ over $F$ is the function $q: V \to F$ $\ni q(v) = \langle v | v \rangle$. $q$ is positive definite if $q(v) = 0$ iff $v = 0$

$q(f) = B(f,f) = \int_0^{\pi} (t+1) f^2(t)\,dt$

Note since $f^2 \geq 0$, $\int_0^{\pi} (t+1) f^2(t)\,dt \geq 0$

So $\int_0^{\pi} (t+1) f^2(t)\,dt = 0$ iff $(t+1) f^2(t) = 0$ iff $t = -1$ or $f^2(t) = 0$

But $t \in [0, \pi]$ so iff $f^2(t) = 0$ iff $f = 0$

$\therefore B(f,f) \geq 0$ and $B(f,f) = 0$ iff $f = 0$

$\therefore B(f,f)$ positive definite

(d) (3 points) Is there a basis $e_1, \ldots, e_m$ for $V$, for some $m > 0$, with respect to which the $m \times m$ identity matrix $I_m$ is the matrix of $B(f,g)$?

6. (10 points) 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.

$\operatorname{rank}(A+5I) = 7 \Rightarrow \operatorname{nullity}(A+5I) = 1$

So the JCF has 1 Jordan block of size 4 for the eigenvalue $-5$

So $m(x) = (x^2+3)^2(x+5)^4$ or $m(x) = (x^2+3)(x+5)^4$

And the invariant factors are $(x^2+3)^2(x+5)^4$ or $(x^2+3), (x^2+3)(x+5)^4$

$\therefore$ JCF's:

$$\begin{bmatrix} i\sqrt{3} & 0 & & & & & & \\ 1 & i\sqrt{3} & & & & & & \\ & & -i\sqrt{3} & 0 & & & & \\ & & 1 & -i\sqrt{3} & & & & \\ & & & & -5 & 0 & 0 & 0 \\ & & & & 1 & -5 & 0 & 0 \\ & & & & 0 & 1 & -5 & 0 \\ & & & & 0 & 0 & 1 & -5 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} i\sqrt{3} & & & & & & & \\ & i\sqrt{3} & & & & & & \\ & & -i\sqrt{3} & & & & & \\ & & & -i\sqrt{3} & & & & \\ & & & & -5 & 0 & 0 & 0 \\ & & & & 1 & -5 & 0 & 0 \\ & & & & 0 & 1 & -5 & 0 \\ & & & & 0 & 0 & 1 & -5 \end{bmatrix}$$

6. (continued)

7. (a) (7 points) 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 $y^2 - x^3$.

$\ker\phi = \{ f(x,y) \in \mathbb{C}[x,y] \mid \phi(f(x,y)) = 0_{\mathbb{C}[t]} \}$

show $\ker\phi = \langle y^2 - x^3 \rangle$

Let $f \in \langle y^2 - x^3 \rangle \Rightarrow f(x,y) = c(x)(y^2 - x^3)$

Then $\phi(f(x,y)) = \phi(c(x)(y^2 - x^3)) = \phi(c(x))[\phi(y^2) - \phi(x^3)] = \phi(c(x))(t^6 - t^6) =($

$\therefore f \in \ker\phi$

$\therefore \langle y^2 - x^3 \rangle \subseteq \ker\phi$

Let $f \in \ker\phi \Rightarrow \phi(f(x,y)) = 0$

So $\phi(\sum_{i,j} a_{i,j} x^i y^j) = 0 \Rightarrow \sum_{i,j} \phi(a_{i,j} x^i)\phi(y^j) = 0$

$\Rightarrow \sum_{i,j} a_{i,j} t^{2i} t^{3j} = 0 \Rightarrow \sum_{i,j} a_{i,j} t^{2i+3j} = 0$

7. (continued)
(b) (3 points) Determine the image of $\phi$ explicitly.

By (a) $\operatorname{Im} \phi = \{ \sum_{i,j} a_{i,j} t^{2i+3j} \mid a_{i,j} \in \mathbb{C} \}$

8. (a) (2 points) Give the definition of an integral domain.

A commutative ring is an integral domain if it has no zero divisors, ie if $a, b \in R \ni ab = 0$ then $a = 0$ or $b = 0$

(b) (2 points) Give the definition of the characteristic of a nonntrivial commutative ring.

The characteristic of R is the smallest integer n $\ni n \cdot 1 = 0$. If no such n exists then the ring has characteristic 0.

8. (continued)

(c) (3 points) Is there an integral domain of characteristic 6? Explain.

Let R integral domain
Suppose char $R = 6$

$6 \cdot 1 = 0 \Rightarrow (2 \cdot 3) \cdot 1 = 0 \Rightarrow (2 \cdot 1)(3 \cdot 1) = 0$

$\Rightarrow 2 \cdot 1 = 0$ or $3 \cdot 1 = 0$ since R integral domain

But this contradicts minimality of 6

$\therefore \nexists$ integral domain of char 6

(d) (3 points) Is there an integral domain with 12 elements? Explain.

Suppose R integral domain with 12 elements
Then R field since R finite

But $12 = 2^2 \cdot 3 \neq p^n$ for $p$ prime, $n > 0$

contradiction

$\therefore \nexists$ R integral domain of order 12

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

(a) (3 points) $\mathbb{Q}(\sqrt{7})$.

$x = \sqrt{2} + \sqrt{7}$

$x - \sqrt{7} = \sqrt{2}$

$(x - \sqrt{7})^2 = \sqrt{2}^2$

$x^2 - 2\sqrt{7}x + 7 = 2$

$x^2 - 2\sqrt{7}x + 5 = 0$

And $\sqrt{2} + \sqrt{7} \in \mathbb{Q}(\sqrt{2}+\sqrt{7}) \Rightarrow 9 + 2\sqrt{14} \in \mathbb{Q}(\sqrt{2}+\sqrt{7}) \Rightarrow \sqrt{14} \in \mathbb{Q}(\sqrt{2}+\sqrt{7})$

$\Rightarrow 2\sqrt{7} + 7\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{7}) \Rightarrow 5\sqrt{7} \in \mathbb{Q}(\sqrt{2}+\sqrt{7}) \Rightarrow \sqrt{7} \in \mathbb{Q}(\sqrt{2}+\sqrt{7})$

$\therefore \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{7}$

$\therefore \mathbb{Q}(\sqrt{2}+\sqrt{7}) = \mathbb{Q}(\sqrt{2},\sqrt{7})$

And we have $\sqrt{2} \notin \mathbb{Q}(\sqrt{7})$

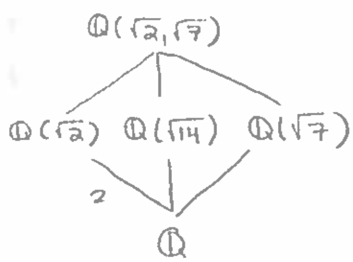
If $\sqrt{2} \in \mathbb{Q}(\sqrt{7})$, $\sqrt{2} = a + b\sqrt{7}$ $a, b \in \mathbb{Q} \Rightarrow 2 = a^2 + 2ab\sqrt{7} + 7b^2$

$\Rightarrow \sqrt{7} = \dfrac{2 - a^2 - 7b^2}{2ab} \in \mathbb{Q}$ impossible

So $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}(\sqrt{7})) = x^2 - 2 \Rightarrow [\mathbb{Q}(\sqrt{2},\sqrt{7}) : \mathbb{Q}(\sqrt{7})] = 2$

$\therefore [\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}(\sqrt{7})] = 2$ and so $\mathrm{Irr}(\sqrt{2}+\sqrt{7}, \mathbb{Q}(\sqrt{7})) = x^2 - 2\sqrt{7}x + 5$

(b) (3 points) $\mathbb{Q}(\sqrt{14})$.




Note that $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \Rightarrow [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Then $[\mathbb{Q}(\sqrt{2},\sqrt{7}) : \mathbb{Q}] = 4$

And $\mathrm{Irr}(\sqrt{14}, \mathbb{Q}) = x^2 - 14 \Rightarrow [\mathbb{Q}(\sqrt{14}) : \mathbb{Q}] = 2$

$\therefore [\mathbb{Q}(\sqrt{2},\sqrt{7}) : \mathbb{Q}(\sqrt{14})] = 2$

So $[\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}(\sqrt{14})] = 2$

$x = \sqrt{2} + \sqrt{7}$

$x^2 = 9 + 2\sqrt{14}$

$x^2 - 2\sqrt{14} - 9 = 0$

$\therefore \mathrm{Irr}(\sqrt{2}+\sqrt{7}, \mathbb{Q}(\sqrt{14})) = x^2 - 2\sqrt{14} - 9$

9. (continued)
(c) (4 points) $\mathbb{Q}$.

$x = \sqrt{2}+\sqrt{7}$

$x^2 = 9 + 2\sqrt{14}$

$\frac{x^2-9}{2} = \sqrt{14}$

$\left(\frac{x^2-9}{2}\right)^2 - 14 = 0$

$\frac{1}{4}x^4 + \frac{81}{4} - \frac{9x^2}{2} - 14 = 0$

$x^4 - 18x^2 + 25 = 0$

Note that by rational root test, only possible roots are $\pm 1, \pm 5, \pm 25$

And none of these are roots

$\therefore x^4 - 18x^2 + 25$ has no roots in $\mathbb{Q}$

Suppose $x^4 - 18x^2 + 25 = (x^2 + ax + b)(x^2 + cx + d)$, $a, b, c, d \in \mathbb{Q}$

$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$

Then $a + c = 0 \Rightarrow c = -a$

$ac + b + d = -18 \Rightarrow a^2 = 18 + b + d$

$ad + bc = 0 \Rightarrow a(d-b) = 0 \Rightarrow a = 0$ or $d - b = 0$

$bd = 25 \Rightarrow d = \frac{25}{b}$

If $a = 0$, $b + d = -18 \Rightarrow b + \frac{25}{b} = -18 \Rightarrow b^2 + 18b + 25 = 0 \Rightarrow b = \frac{-18 \pm 4\sqrt{14}}{2} \notin \mathbb{Q}$

$\therefore a \neq 0$

$\therefore d = b$

$\therefore d = b = \pm 5$

If $d = b = 5$, then $a^2 = 28$ impossible

If $d = b = -5$, then $a^2 = 8$ impossible

$\therefore x^4 - 18x^2 + 25$ irreducible over $\mathbb{Q}$

$\therefore \operatorname{Irr}(\sqrt{2}+\sqrt{7}, \mathbb{Q}) = x^4 - 18x^2 + 25$

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

(a) (5 points) 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 $\mathbb{Q}$.

Note that the roots of $x^5-1$ are $\zeta^i$ for $0 \le i < 5$

And the splitting field of $x^5-1$ is the smallest extension of $\mathbb{Q}$ containing each of the above roots

Then $K = \mathbb{Q}(\zeta)$ splitting field for $x^5-1$ since $\zeta^i \in K$ $\forall i$

and $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta^i)$ $\forall i$

And $[K:\mathbb{Q}] = \phi(5) = 4$

$\therefore [K:\mathbb{Q}] = 4$

10. (continued)

(b) (5 points) Determine the Galois group $G(K/\mathbb{Q})$ explicitly and up to isomorphism.

Let $\sigma \in Gal(K/\mathbb{Q})$

Then $\sigma(\zeta) = \zeta^{i}$ for some $0 < i < 5$

So we have $\sigma_1 = 1$, $\sigma_2 : \zeta \to \zeta^2$, $\sigma_3 : \zeta \to \zeta^3$, $\sigma_4 : \zeta \to \zeta^4$

$\therefore Gal(K/\mathbb{Q}) \cong C_4$

Artin

Chapter 2

2.2

16. a. Let G be a cyclic group of order 6. How many elements generate G?

Let $g$ be a generator of G since G cyclic

Then $|g^r| = \frac{|g|}{\gcd(|g|,r)} = \frac{6}{\gcd(6,r)}$ $\forall r = 1,\dots,6$

We want to find each element of order 6 ie we want each element

$g^r \ni \gcd(6,r) = 1$

So the generators of G are $g, g^5$

$\therefore$ G has 2 generators

b. Answer the same question for cyclic groups of order 5, 8, and 10

If $|G| = 5$ and $g$ generator

The generators are $g^r \ni \gcd(5,r) = 1$ ie $g, g^2, g^3, g^4$

$\therefore$ G has 4 generators

If $|G| = 8$ and $g$ generator

The generators are $g^r \ni \gcd(8,r) = 1$ ie $g, g^3, g^5, g^7$

$\therefore$ G has 4 generators

If $|G| = 10$ and $g$ generator

The generators are $g^r \ni \gcd(10,r) = 1$ ie $g, g^3, g^7, g^9$

$\therefore$ G has 4 generators

c. How many elements of a cyclic group of order n are generators of G?

If $|G| = n$ and $g$ generator

The generators are $g^r \ni \gcd(n,r) = 1$

$\therefore$ G has $\Phi(n)$ generators

2.3

5. Let $\varphi: G \to G'$ be a group isomorphism. Prove that $\varphi^{-1}$ is also an isomorphism.

Clearly since $\varphi$ bijective, $\varphi^{-1}$ also bijective

So show $\varphi^{-1}$ homomorphism

Let $x, y \in G'$

since $\varphi$ surjective $\exists a,b \in G \ni x = \varphi(a)$ and $y = \varphi(b) \Rightarrow a = \varphi^{-1}(x), b = \varphi^{-1}(y)$
Then $\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$
$\therefore \varphi^{-1}$ homomorphism
$\therefore \varphi^{-1}$ isomorphism

10. Prove that $\varphi: GL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \ni \varphi(A) = (A^T)^{-1}$ is an automorphism
Let $A, B \in GL_n(\mathbb{R})$
Then $\varphi(AB) = ((AB)^T)^{-1} = (B^T A^T)^{-1} = (A^T)^{-1}(B^T)^{-1} = \varphi(A)\varphi(B)$
$\therefore \varphi$ homomorphism
Let $\varphi(A) = \varphi(B)$
Then $(A^T)^{-1} = (B^T)^{-1} \Rightarrow A^T = B^T \Rightarrow A = B$
$\therefore \varphi$ injective
Let $A \in GL_n(\mathbb{R})$
Then $A = (((A^{-1})^T)^T)^{-1} = \varphi((A^{-1})^T)$
$\therefore \varphi$ surjective
$\therefore \varphi$ automorphism

2.4

17. Prove that $Z(G)$ is a normal subgroup of $G$
Let $g^{-1}zg \in g^{-1}Z(G)g$ and let $h \in G$
Then $g^{-1}zgh = g^{-1}gzh$ since $z \in Z(G)$
$= zh = hz = hzg^{-1}g = hg^{-1}zg$
$\therefore g^{-1}zg \in Z(G)$
$\therefore g^{-1}Z(G)g \subseteq Z(G)$
$\therefore Z(G)$ normal in $G$

22. Let $\varphi: G \to G'$ be a surjective homomorphism.
a. Assume that $G$ is cyclic. Prove that $G'$ is cyclic
$G$ cyclic $\Rightarrow G = \langle g \rangle$ for some $g \in G$
Now let $g' \in G'$
since $\varphi$ surjective $g' = \varphi(x)$ for some $x \in G$
But $G$ cyclic $\Rightarrow x = g^n$ for some $n \in \mathbb{Z}$

so $g' = \varphi(x) = \varphi(g^n) = (\varphi(g))^n$ since $\varphi$ homomorphism

$\therefore G = \langle \varphi(g) \rangle$

$\therefore G$ cyclic

b. Assume that G abelian. Prove that G' abelian.

Let $a, b \in G'$

since $\varphi$ surjective $a = \varphi(x)$ and $b = \varphi(y)$ for some $x, y \in G$

Then $ab = \varphi(x)\varphi(y) = \varphi(xy)$ since $\varphi$ homomorphism

$= \varphi(yx)$ since G abelian

$= \varphi(y)\varphi(x) = ba$

$\therefore G'$ abelian

2.5

6. a. Prove that the relation x conjugate to y in a group G is an equivalence relation on G.

Say $x \sim y$ iff $\exists g \in G \ni g^{-1}xg = y$

Note $\sim$ reflexive since $1^{-1}x1 = x$

Let $x \sim y \Rightarrow g^{-1}xg = y$ for some $g \in G \Rightarrow x = gyg^{-1} = (g^{-1})^{-1}yg^{-1}$ for some $g^{-1} \in G$

so $y \sim x$

$\therefore \sim$ symmetric

Finally let $x \sim y$ and $y \sim z$

Then $g^{-1}xg = y$ and $h^{-1}yh = z$ for some $g, h \in G$

Then $z = h^{-1}yh = h^{-1}g^{-1}xgh = (gh)^{-1}xgh$

$\therefore x \sim z$

$\therefore \sim$ transitive

$\therefore \sim$ equivalence relation

b. Describe the elements a whose conjugacy class consist of a alone

Then $g^{-1}ag = a \ \forall g \in G$

$\therefore ag = ga \ \forall g \in G$

$\therefore a \in Z(G)$

2.8

10. Let $x \in G \ni |x| = m$ and $y \in G' \ni |y| = n$. What is the order of $(x,y)$ in $G \times G'$?

Let $l = \text{lcm}(m,n) \Rightarrow l = mp = nq$ for some $p,q \in \mathbb{Z}$

Then $(x,y)^l = (x^l, y^l) = (x^{mp}, y^{nq}) = ((x^m)^p, (y^n)^q) = (1,1)$

$\therefore |(x,y)| \mid l$

Suppose $|(x,y)| < l$, say $|(x,y)| = r$

Then $r$ is not a common multiple of $m,n$

WLOG say $r$ not a multiple of $m$

Then $(1,1) = (x,y)^r = (x^r, y^r)$

so $x^r = 1$

Contradiction since $r$ not multiple of $m$

$\therefore |(x,y)| = l = \text{lcm}(m,n)$

Misc

2. Compute $\text{Aut}(G)$ for $Q_8$ (the quaternion group)

Note that $Q_8 = \langle i, j \rangle$ so it suffices to define where $i,j$ are sent to determine an automorphism

Then we have $i \longrightarrow \pm i, \pm j, \pm k$, $j \longrightarrow \pm i, \pm j, \pm k$

Now note that $i \longrightarrow a \Rightarrow j \not\longrightarrow a$ $\forall a \in Q_8$ since automorphisms are injective

And also if $i \longrightarrow k$ and $j \longrightarrow -k$, then $i \cdot j \rightarrow -k \cdot k \Rightarrow k \rightarrow 1$ impossible since $|k| \neq |1|$

So we have 6 choices of where to send $i$ and then only 4 choices of where to send $j$ and each of these is clearly an automorphism

$\therefore |\text{Aut}(G)| = 6 \cdot 4 = 24$

And $\sigma_1 : \begin{cases} i \rightarrow j \\ j \rightarrow i \end{cases}$, $\sigma_2 : \begin{cases} i \rightarrow -i \\ j \rightarrow k \end{cases}$ $\Rightarrow \sigma_1\sigma_2(j) = \sigma_1(k) = \sigma_1(ij) = \sigma_1(i)\sigma_1(j) = ji = -k$

But $\sigma_2\sigma_1(j) = \sigma_2(i) = -i$

$\therefore \text{Aut}(G)$ non-Abelian group of order 24

11. Let $H \leq G$. Show that the double cosets $HgH$ are the left cosets $gH$ if $H$ is normal, but if $H$ is not normal then there is a double coset which properly contains a left coset.

Assume $H$ normal and show $HgH = gH$ $\forall g \in G$

$HgH = (gH)H$ since $H$ normal

$\quad = gH$

$\therefore HgH = gH$

But take $G = S_3$ and $H = \langle (12) \rangle$

Note that $H$ not normal since $g^{-1}Hg = (23)H(23) = \{1, (13)\} \notin H$

And $(23)H = \{(23), (132)\}$ while $H(23)H = \{(23), (132), (123), (13)\}$

$\therefore (23)H \subsetneq H(23)H$

Artin

## Chapter 3

3.3

5. Find a basis for the space of symmetric $n\times n$ matrices.

Let $B_{ij}$ be $n\times n$ matrix $\ni b_{ij} = b_{ji} = 1$ and all other entries are 0

Then let $\mathcal{B} = \{B_{ij} \mid i \geq j\}$

Show that $\mathcal{B}$ is a basis for the space above

Let $\sum_i c_i B_{ij} = 0$

Then $\begin{bmatrix} c_1 & c_2 & \cdots \\ c_2 & \ddots & \\ \vdots & & \end{bmatrix} = 0 \Rightarrow c_i = 0 \ \forall i$

$\therefore \mathcal{B}$ linearly independent

Now let $A$ be a symmetric $n\times n$ matrix

Then $A = \sum_{i,j} a_{ij} B_{ij}$ since $a_{ij} = a_{ji}$

$\therefore A \in \operatorname{span} \mathcal{B}$

$\therefore \mathcal{B}$ basis

3.4

1. Compute the matrix $P$ of change of basis of $F^2$ from $E$ the standard basis to $B = \left\{\begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\right\}$.

$$\left[\begin{array}{cc|c} 1 & 2 & 1 \\ 3 & 2 & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & 1 \\ 0 & -4 & -3 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 2 & 1 \\ 0 & 1 & 3/4 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & -1/2 \\ 0 & 1 & 3/4 \end{array}\right]$$

$$\left[\begin{array}{cc|c} 1 & 2 & 0 \\ 3 & 2 & 1 \end{array}\right] \to \left[\begin{array}{cc|c} -2 & 0 & -1 \\ 3 & 2 & 1 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 1/2 \\ 0 & 2 & -1/2 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 1/2 \\ 0 & 1 & -1/4 \end{array}\right]$$

$\therefore P = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix}$

Check: Let $v = \begin{pmatrix}1\\2\end{pmatrix}$

$[v]_B = [B]^{-1} v = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/4 \end{bmatrix}$

And $P[v]_E = P[E]^{-1} v = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/4 \end{bmatrix}$

$\therefore P[v]_E = [v]_B$

$\therefore P = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix}$ is change of basis matrix from $E$ to $B$

6. Let $B$ and $B'$ bases for $F^n$. Prove that the change of basis matrix from $B$ to $B'$ is $P = [B']^{-1}[B]$

Let $P$ be the change of matrix from $B$ to $B'$

Then $P[v]_B = [v]_{B'} \quad \forall v \in F^n$

So $P[B]^{-1} = [B']^{-1}$

$\therefore P = [B']^{-1}[B]^{-1}$

Misc

2. Let $V$ be a vector space over an infinite field $F$. Prove that $V$ is not the union of finitely many proper subspaces.

Suppose $V = \bigcup_{i=1}^{n} V_i$ where each $V_i$ proper subspace of $V$ and $n \geq 1$ is minimal such that this equality is true

Then $V \neq \bigcup_{i=1}^{n-1} V_i \Rightarrow V_n \notin \bigcup_{i=1}^{n-1} V_i$

Let $v \in V_n \setminus \bigcup_{i=1}^{n-1} V_i$ and $u \notin V_n$

Define $S = \{v + tu \mid t \in F\}$

Since $u \notin V_n$, $u \neq 0$

And since $F$ infinite, $S$ infinite

We have $S \subseteq V = \bigcup_{i=1}^{n} V_n$

So some $V_i$ must contain infinitely elements of $S$

Suppose $\exists$ another element from $S$ in $V_n$ besides $v$

Then $\exists t \in F \ni v + tu \in V_n$

So $tu = v + tu - v \in V_n \Rightarrow u \in V_n$

Contradiction

$\therefore V_n$ does not contain infinitely many elements of $S$

Then some $V_i$ contains infinitely many elements of $S$ for $i < n$

Let $v + t_1 u, v + t_2 u \in V_i \ni t_1 \neq t_2$

But then $t_2(v + t_1 u) - t_1(v + t_2 u) \in V_i \Rightarrow (t_2 - t_1) v \in V_i$

$\therefore v \in V_i$

Contradiction since $v \in V_n \setminus \bigcup_{i=1}^{n-1} V_i$

$\therefore V$ not union of finitely many proper subspaces

7. Let $A \in M_n(\mathbb{R})$. Prove that $\exists f(t)$ polynomial which has $A$ as a root.

Note that by the Cayley-Hamilton theorem, $c(x)$ the characteristic polynomial of $A$ annihilates $A$

$\therefore c(A) = 0$

$\therefore \exists c(x)$ polynomial having $A$ as a root

Artin

## Chapter 4

4.2

8. Prove that $\operatorname{rank}(A) = \operatorname{rank}(A^T)$ where $A \in M_{m \times n}(F)$

$\operatorname{rank}(A^T) = \dim(\operatorname{Col}(A^T)) = \#$ basis vectors for $\operatorname{Col}(A^T)$

$= \#$ basis vectors for $\operatorname{Row}(A)$

And we know $\operatorname{Row}(A) = \operatorname{span}(r_1, \dots, r_m)$ where $r_i$'s are rows of $A$

And note that the nonzero rows in $\operatorname{rref}(A)$ are linearly independent

$\therefore$ The nonzero rows in $\operatorname{rref}(A)$ are a basis for $\operatorname{Row}(A)$

$\therefore \operatorname{rank}(A^T) = \#$ nonzero rows in $\operatorname{rref}(A) = \#$ leading 1's in $\operatorname{rref}(A)$

$\operatorname{rank}(A) = \dim(\operatorname{Col}(A)) = \#$ basis vectors for $\operatorname{Col}(A)$

And $\operatorname{Col}(A) = \operatorname{span}(c_1, \dots, c_n)$ where $c_i$ columns of $A$

And the nonzero columns in $\operatorname{rref}(A)$ are linearly independent

$\therefore$ The nonzero columns in $\operatorname{rref}(A)$ are a basis for $\operatorname{Col}(A)$

$\therefore \operatorname{rank}(A) = \#$ nonzero columns in $\operatorname{rref}(A)$

$\therefore \operatorname{rank}(A) = \#$ leading 1's in $\operatorname{rref}(A)$

$\therefore \operatorname{rank}(A) = \operatorname{rank}(A^T)$

4.4

4. Prove that $A \in M_3(\mathbb{R})$ has at least one real eigenvalue

Consider the characteristic equation of $A$, $c(x)$

Since $A$ is $3 \times 3$, $c(x)$ is a cubic polynomial

And cubic polynomials must have at least one real root

because complex roots must come in pairs

9. Do $A$ and $A^T$ have same eigenvalues? The same eigenvectors?

Note that $A, A^T$ are similar

$\therefore A, A^T$ have same eigenvalues

But they do not necessarily have the same eigenvectors

Take $A = \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}$

$\lambda I - A = \begin{bmatrix} \lambda-1 & 0 \\ -2 & \lambda-3 \end{bmatrix} \Rightarrow c(x) = (\lambda-1)(\lambda-3) \Rightarrow A$ has eigenvalues $\lambda = 1, 3$

Consider $\lambda = 3$

$\left[\begin{array}{cc|c} 2 & 0 & 0 \\ -2 & 0 & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 2 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \Rightarrow x = 0 \to \begin{bmatrix} 0 \\ t \end{bmatrix} = t\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$\therefore A$ has eigenvector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ associated with $\lambda = 3$

But $A^T = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$

$\lambda I - A^T = \begin{bmatrix} \lambda-1 & -2 \\ 0 & \lambda-3 \end{bmatrix} \Rightarrow c(x) = (\lambda-1)(\lambda-3) \Rightarrow A^T$ has eigenvalues $\lambda = 1, 3$

Consider $\lambda = 3$

$\left[\begin{array}{cc|c} 2 & -2 & 0 \\ 0 & 0 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{cc|c} 1 & -1 & 0 \\ 0 & 0 & 0 \end{array}\right] \Rightarrow x - y = 0 \Rightarrow x = y \Rightarrow \begin{bmatrix} t \\ t \end{bmatrix} = t\begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$\therefore A^T$ has eigenvector $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ associated with $\lambda = 3$

$\therefore A, A^T$ have different eigenvectors

14. Let $P \in M_n(\mathbb{R}) \ni P^T = P^2$. What are the possible eigenvalues of $P$?

$P = (P^T)^T = (P^2)^T = (P^T)^2 = (P^2)^2 = P^4$

$\therefore P^4 - P = 0$

$\therefore$ The polynomial $x^4 - x$ annihilates $P$

Then $m(x) \mid x^4 - x$ where $m(x)$ minimal polynomial of $P$

Note that every eigenvalue of $P$ is a root of $c(x)$

Hence every eigenvalue of $P$ is a root of $m(x)$ since $m(x), c(x)$ have the same roots

So every eigenvalue is a root of $x^4 - x$ since $m(x) \mid x^4 - x$

And $x^4 - x = x(x^3 - 1)$ has roots $x = 0, 1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$

$\therefore$ The possible eigenvalues of $P$ are $0, 1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$

4.6 Let $M$ be the block matrix, $M = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & D \end{array}\right]$. Prove that $M$ is diagonalizable iff $A, D$ are diagonalizable.

($\Rightarrow$) Assume $M$ diagonalizable

Then the minimal polynomial, $m(x)$, of $M$ splits into nonrepeated factors

But $m(x) = \text{lcm}(m_A(x), m_D(x))$ which is monic

So $m_A(x), m_D(x) \mid m(x)$

$\therefore m_A(x), m_D(x)$ split into nonrepeated factors

$\therefore A, D$ diagonalizable

($\Leftarrow$) Assume $A, D$ diagonalizable

Then $\exists P, Q \ni P^{-1}AP, \; Q^{-1}DQ$ diagonal

Take $R = \left[\begin{array}{c|c} P & 0 \\ \hline 0 & Q \end{array}\right]$

Then $R^{-1}MR = \left[\begin{array}{c|c} P^{-1} & 0 \\ \hline 0 & Q^{-1} \end{array}\right]\left[\begin{array}{c|c} A & 0 \\ \hline 0 & D \end{array}\right]\left[\begin{array}{c|c} P & 0 \\ \hline 0 & Q \end{array}\right] = \left[\begin{array}{c|c} P^{-1}AP & 0 \\ \hline 0 & Q^{-1}DQ \end{array}\right]$ diagonal

$\therefore$ M diagonalizable

Misc

4. Let $A, B \in M_n(\mathbb{C})$ and let $C = AB - BA$. Prove that if $C$ commutes with $A$ then $C$ is nilpotent.

$trace(C) = trace(AB - BA) = trace(AB) - trace(BA) = 0$

$\therefore trace(C) = 0$

So let $c(x) = (x-\lambda_1)\ldots(x-\lambda_n)$ be the characteristic polynomial of $C$

Then $0 = trace(C) = \sum_{i=1}^{n} \lambda_i$

14. Prove that a linear operator on a vector space of dimension $n$ can have at most $n$ different eigenvalues

Let $\dim V = n$, $T: V \to V$ linear operator

Let $\lambda_1, \ldots, \lambda_m$ be distinct eigenvalues of $T$

And $v_1, \ldots, v_m$ corresponding eigenvectors

Then $v_1, \ldots, v_m$ linearly independent

$\therefore m \leq n$

$\therefore$ there are at most $n$ different eigenvalues

Artin

## Chapter 6

6.1

4. Let $G$ be a p-group and let $S$ be a finite set on which $G$ acts. Assume that $p \nmid |S|$. Prove that there is a fixed point of the action.

Suppose there is no fixed point

Then $|Ox| \neq 1 \quad \forall x \in X$

But $|S| = \sum_{x \in S} |Ox| = \sum_{x \in S} |G:Gx|$ where $x$ are the representatives for distinct orbits

So each term of the sum must be a power of $p$ since none are 1 and the must divide $|G| = p^r$ for some $r$

$\therefore p \mid |S|$

Contradiction since $p \nmid |S|$

$\therefore$ There is a fixed point

9. Let $G$ be a group of order $n$ and let $F$ be a field. Prove that $G$ is isomorphic to a subgroup of $GL_n(F)$

Since $|G| = n$, $G$ isomorphic to a subgroup of $S_n$ by Cayley's Thm

It suffices to show $S_n$ isomorphic to a subgroup of $GL_n(F)$

Define $\varphi : S_n \to GL_n(F) \ni \varphi(\sigma) = A$ where $A_{ij} = \begin{cases} 1 & \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}$

Clearly this is an isomorphism to a subgroup of $GL_n(F)$

$\therefore G$ isomorphic to subgroup of $GL_n(F)$

6.3

7. Let $H \leq G$. Prove or disprove: $N_G(H)$ is a normal subgroup of $G$.

Take $G = S_3$, $H = \langle (12) \rangle$

Then $N_G(H) = \langle (12) \rangle$ which is not normal since $(13)(12)(13) = (23) \notin H$

6.4

2. Prove that no group of order $pq$ where $p, q$ prime is simple

$|G| = pq$

WLOG say $p < q$

Then $n_q(G) \equiv 1 \pmod q$ and divides $p$

So $n_q(G) = 1, p$

But $p<q \Rightarrow p \not\equiv 1 \pmod{q}$

$\therefore n_q(G)=1$

$\therefore$ G has a unique Sylow q-subgroup

$\therefore$ G has a normal subgroup of order q

$\therefore$ G not simple

12. Prove that no group of order 224 is simple.

$|G| = 224 = 2^5 \cdot 7$

$n_2(G) \equiv 1 \pmod 2$ and divides 7

so $n_2(G) = 1, 7$

suppose $n_2(G)=7$ and let $P \in Syl_2(G)$

Then $|G:N_G(P)| = 7$

Consider G acting on $G/N_G(P)$

Then we get homomorphism $\varphi: G \to S_{G/N_G(P)} \cong S_7$

If $\varphi$ injective, then $|\varphi(G)| = 224$

But $\varphi(G) \leq S_7 \Rightarrow |\varphi(G)| \mid 7!$ by lagrange

But $224 \nmid 7!$

$\therefore \varphi$ not injective

$\therefore \ker\varphi \neq \{1\}$

Also $\ker\varphi \neq G$ since action nontrivial since $N_G(P) \neq G$

$\therefore \ker\varphi$ is a nontrivial, proper, normal subgroup of G

$\therefore$ G not simple

And if $n_2(G)=1$

Then G has a unique Sylow 2-subgroup

$\therefore$ G has a normal subgroup of order 32

$\therefore$ G not simple

6.5

3. 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.

$|G| = 30 = 2 \cdot 3 \cdot 5$

$n_3(G) \equiv 1 \pmod 3$ and divides 10

So $n_3(G) = 1, \cancel{2}, \cancel{5}, 10$

$\therefore n_3(G) = 1, 10$

$n_5(G) \equiv 1 \pmod 5$ and divides 6

So $n_5(G) = 1, \cancel{2}, \cancel{3}, 6$

$\therefore n_5(G) = 1, 6$

Suppose $n_3(G) = 10$ and $n_5(G) = 6$

Let $P, P' \in Syl_3(G)$

Then $|P \cap P'| = 1, 3$ by lagrange since $P \cap P' \leq P, P'$

So $P = P'$ or $P \cap P' = \{1\}$

So we have 10 sylow 3-subgroups each having 2 elements of order 3

That is $10 \cdot 2 = 20$ elements

Let $Q, Q' \in Syl_5(G)$

Then $|Q \cap Q'| = 1, 5$ by Lagrange since $Q \cap Q' \leq Q, Q'$

So $Q = Q'$ or $Q \cap Q' = \{1\}$

So we have 6 sylow 5-subgroups each having 4 elements of order 5

So in total we have $20 + 6 \cdot 4 = 44$

Contradiction since $|G| = 30$

$\therefore$ At least one of $n_3(G), n_5(G)$ must be 1

$\therefore$ Either H or K is normal

b. Prove that HK is a cyclic subgroup of G

Note that at least one of H, K is normal by (a)

So $HK \leq G$

And $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{3 \cdot 5}{1} = 15$

So $|HK| = 15 = 3 \cdot 5$

$n_3(HK) \equiv 1 \pmod 3$ and divides 5

So $n_3(HK) = 1, \cancel{5}$

$\therefore n_3(HK) = 1$

$n_5(HK) \equiv 1 \pmod 5$ and divides 3

So $n_5(HK) = 1, \cancel{3}$

$\therefore n_5(HK) = 1$

So HK has 1 Sylow 3-subgroup having 2 elements of order 3

and 1 Sylow 5-subgroup having 4 elements of order 5

That accounts for 6 non-identity elements

But there are still 8 non-identity elements left

Let x be one of them

Suppose $|x| = 3$, then $|\langle x \rangle| = 3$ and thus $\langle x \rangle$ is another

Sylow 3-subgroup

Contradiction since $n_3(HK) = 1$

Similarly $|x| \neq 5$

$\therefore$ There are 8 elements of order 15 by Lagrange

$\therefore$ HK cyclic

6.6

20. Prove that $A_n$ is the only subgroup of $S_n$ of index 2

Let $H \leq S_n \ni |S_n : H| = 2$

Then H normal in $S_n$

So $S_n/H$ group and $|S_n/H| = 2$

So every element $\sigma H \in S_n/H$ has order $|\sigma H| \leq 2$

$\therefore (\sigma H)^2 = 1_{S_n/H} \ \forall \sigma \in S_n$ ie $\sigma^2 H = H \ \forall \sigma \in S_n$

So $\sigma^2 \in H \ \forall \sigma \in S_n$

But then look at $\sigma_3$ any 3cycle in $S_n$

$|\sigma_3| = 3$ so $\sigma_3^4 = \sigma_3^3 \cdot \sigma_3 = 1 \cdot \sigma_3 = \sigma_3$

$\therefore \sigma_3 = \sigma_3^4 = (\sigma_3^2)^2 \ \forall \sigma_3$

$\therefore \sigma_3 \in H \ \forall$ 3cycles $\sigma_3$

But $A_n$ is generated by the 3-cycles

$\therefore A_n \leq H$

But $|A_n| = |H|$ since $|S_n : A_n| = 2$

So $H = A_n$

$\therefore$ The only subgroup of index 2 in $S_n$ is $A_n$

6.8

1. Prove that $a, b \in G$ generate the same group as $bab^2, bab^3$

Show $\langle a, b \rangle = \langle bab^2, bab^3 \rangle$

Clearly $bab^2 = (a^0 b)(ab^2) \in \langle a, b \rangle$ by closure

And $bab^3 = (a^0 b)(ab^3) \in \langle a, b \rangle$ by closure

$\therefore \langle bab^2, bab^3 \rangle \subseteq \langle a, b \rangle$

Now $bab^2 \in \langle bab^2, bab^3 \rangle$ so $(bab^2)^{-1} \in \langle bab^2, bab^3 \rangle$

so $(bab^2)^{-1} bab^3 \in \langle bab^2, bab^3 \rangle$ by closure

$\therefore b^{-2} a^{-1} b^{-1} bab^3 \in \langle bab^2, bab^3 \rangle \Rightarrow b \in \langle bab^2, bab^3 \rangle$

So $b^{-1} \in \langle bab^2, bab^3 \rangle$

$\therefore b^{-1}(bab^2) b^{-2} \in \langle bab^2, bab^3 \rangle \Rightarrow a \in \langle bab^2, bab^3 \rangle$

$\therefore \langle a, b \rangle \subseteq \langle bab^2, bab^3 \rangle$

$\therefore \langle a, b \rangle = \langle bab^2, bab^3 \rangle$

Artin

Chapter 7

7.1

1. Let $A, B \in M_n(\mathbb{R})$. Prove that if $x^T A y = x^T B y \ \forall x,y \in \mathbb{R}^n$ then $A = B$.

$x^T A y = x^T B y \ \forall x,y \in \mathbb{R}^n \Rightarrow x^T A y - x^T B y = 0 \ \forall x,y \in \mathbb{R}^n$

So $x^T(A-B)y = 0 \ \forall x,y \in \mathbb{R}^n$

Let $C = A - B$

So $x^T C y = 0 \ \forall x,y \in \mathbb{R}^n$

Since this is true $\forall x,y \in \mathbb{R}^n$, it must be true for $e_i, e_j \ \forall i,j$

So $e_i^T C e_j = 0 \Rightarrow C_{ij} = 0 \ \forall i,j$

$\therefore C = 0$

$\therefore A - B = 0$

$\therefore A = B$

7.2

2. Prove that $A^T A$ is positive semi-definite for any $A \in M_{m\times n}(\mathbb{R})$.

$x^T A^T A x = (Ax)^T A x = (Ax)\cdot(Ax) = \langle Ax | Ax \rangle \geq 0$ since the standard dot product is positive definite

$\therefore x^T A^T A x \geq 0 \ \forall x \in \mathbb{R}^n$

$\therefore A^T A$ positive semidefinite

7.4

10. Prove that the determinant of a hermitian matrix is real.

Let $A$ be hermitian

So $A^* = A$

$\therefore \det(A) = \det(A^*) = \det(\overline{A^T}) = \det(\overline{A}) = \sum_\sigma \operatorname{sgn}(\sigma)\overline{a}_{\sigma(1),1} \ldots \overline{a}_{\sigma(n),n}$

$= \overline{\sum_\sigma \operatorname{sgn}(\sigma) a_{\sigma(1),1} \ldots a_{\sigma(n),n}} = \overline{\det(A)}$

$\therefore \det(A) = \overline{\det(A)}$

$\therefore \det(A) \in \mathbb{R}$

7.5

5. Let $A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$. Find a real orthogonal matrix $P \ni PAP^T$ diagonal.

Note that since $A$ symmetric, $\exists$ such a $P$ by Spectral Theorem

$\det(\lambda I - A) = \begin{vmatrix} \lambda-1 & -2 \\ -2 & 1 \end{vmatrix} = (\lambda-1)^2 - 4 = \lambda^2 - 2\lambda - 3 = (\lambda+1)(\lambda-3)$

$\therefore$ Eigenvalues of A are $\lambda = -1, 3$

If $\lambda = -1$, $\left[\begin{array}{cc|c} -2 & -2 & 0 \\ -2 & -2 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{cc|c} -2 & -2 & 0 \\ 0 & 0 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right] \Rightarrow \begin{matrix} x+y=0 \\ x=-y \end{matrix} \Rightarrow \begin{matrix} x=-t \\ y=t \end{matrix} \Rightarrow \begin{bmatrix} -t \\ t \end{bmatrix} = t\begin{bmatrix} -1 \\ 1 \end{bmatrix}$

$\therefore$ Eigenvector for $\lambda = -1$ is $v = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$

Take $v/|v| = \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ since $|v| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}$

If $\lambda = 3$, $\left[\begin{array}{cc|c} 2 & -2 & 0 \\ -2 & 2 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{cc|c} 2 & -2 & 0 \\ 0 & 0 & 0 \end{array}\right] \longrightarrow \left[\begin{array}{cc|c} 1 & -1 & 0 \\ 0 & 0 & 0 \end{array}\right] \Rightarrow \begin{matrix} x-y=0 \\ x=y \end{matrix} \Rightarrow \begin{matrix} x=t \\ y=t \end{matrix} \Rightarrow \begin{bmatrix} t \\ t \end{bmatrix} = t\begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$\therefore$ Eigenvector for $\lambda = 3$ is $v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Take $v/|v| = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

Let $P = \begin{bmatrix} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix}$

$\left[\begin{array}{cc|cc} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 1 & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cc|cc} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 1 & 0 \\ 0 & \sqrt{2} & 1 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cc|cc} -\frac{\sqrt{2}}{2} & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \sqrt{2} & 1 & 1 \end{array}\right]$

$\longrightarrow \left[\begin{array}{cc|cc} 1 & 0 & -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ 0 & 1 & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{array}\right]$

$\therefore P^{-1} = \begin{bmatrix} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix} = P^T$

$\therefore$ P orthogonal since $P^{-1} = P^T \Rightarrow P^T P = I$

And $PAP^T = \begin{bmatrix} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 3 \end{bmatrix}$ Diagonal

10. Prove that for any square matrix A, $\ker A = (\operatorname{Im} A^*)^\perp$

Let $x \in \ker A \Rightarrow Ax = 0$

Let $y \in \operatorname{Im} A^* \Rightarrow y = A^* z$ for some z

And $x \cdot y = x \cdot A^* z = x^* A^* z = Ax \cdot z = 0 \cdot z = 0$

$\therefore x \in (\operatorname{Im} A^*)^\perp$

$\therefore \ker A \subseteq (\operatorname{Im} A^*)^\perp$

Now let $x \in (\operatorname{Im} A^*)^\perp$ and let $y \in \operatorname{Im} A^* \Rightarrow y = A^* z$ for some z

Then $0 = x \cdot y = x \cdot A^* z = x^* A^* z = Ax \cdot z$

so $Ax \cdot z = 0 \quad \forall z$

$\therefore Ax \cdot Ax = 0$

$\therefore Ax = 0$ since standard hermitian product positive definite

$\therefore x \in \ker A$

$\therefore (\operatorname{Im} A^*)^\perp \subseteq \ker A$

$\therefore \ker A = (\operatorname{Im} A^*)^\perp$

7.7

1. Show that for any normal matrix $A$, $\ker A = (\operatorname{Im} A)^\perp$

Let $x \in \ker A \Rightarrow Ax = 0$

Let $y \in \operatorname{Im} A \Rightarrow y = Az$ for some $z$

First note that $0 = Ax \cdot Ax = x^* A^* A x = x^* A A^* x$ since $A$ normal

$= A^*x \cdot A^*x$

$\therefore A^*x = 0$ since standard hermitian product positive definite

So $x \cdot y = x \cdot Az = x^* Az = A^*x \cdot z = 0 \cdot z = 0$

$\therefore x \in (\operatorname{Im} A)^\perp$

$\therefore \ker A \subseteq (\operatorname{Im} A)^\perp$

Now let $x \in (\operatorname{Im} A)^\perp \Rightarrow x \cdot y = 0 \quad \forall y \in \operatorname{Im} A$

$Ax \cdot Ax = x^* A^* A x = x^* A A^* x = x \cdot AA^* x = 0$ since $AA^*x \in \operatorname{Im} A$

$\therefore Ax = 0$

$\therefore x \in \ker A$

$\therefore (\operatorname{Im} A)^\perp \subseteq \ker A$

$\therefore \ker A = (\operatorname{Im} A)^\perp$

6. Let $P$ be a real skew-symmetric matrix. Prove that $P$ is normal.

Note that $P$ real $\Rightarrow P^* = \bar{P}^T = P^T$

So show $PP^* = P^*P$ ie $PP^T = P^TP$

$P$ skew symmetric $\Rightarrow P = -P^T$ and hence $-P = P^T$

So $PP^T = -P^TP^T = -P^T(-P) = P^TP$

$\therefore PP^T = P^TP$

$\therefore P$ normal

11. Prove that for any linear operator $T$, $TT^*$ is hermitian

$(TT^*)^* = TT^*$

$\therefore TT^*$ hermitian

7.8

1. Prove or disprove: A matrix $A$ is skew symmetric iff $x^TAx=0$ $\forall x$

($\Rightarrow$) Assume $A$ skew symmetric

Then $A=-A^T$

And $x^TAx = x\cdot Ax$

But also $x^TAx = -x^TA^Tx = -(Ax)^Tx = -Ax\cdot x = x\cdot -Ax = -x\cdot Ax$

$\therefore$ $x\cdot Ax = -x\cdot Ax$

$\therefore$ $x^TAx = -x^TAx$ $\forall x$

$\therefore$ $x^TAx=0$ $\forall x$

($\Leftarrow$) Assume $x^TAx=0$ $\forall x$

Then $e_i^TAe_i = 0 \Rightarrow A_{ii}=0$ $\forall i$

And $(e_i+e_j)^TA(e_i+e_j) = 0 \Rightarrow e_i^TAe_i + e_i^TAe_j + e_j^TAe_i + e_j^TAe_j = 0$

so $e_i^TAe_j + e_j^TAe_i = 0 \Rightarrow A_{ij}+A_{ji}=0 \Rightarrow A_{ij}=-A_{ji}$ $\forall i,j$

$\therefore$ $A=-A^T$

$\therefore$ $A$ skew-symmetric

7.9

1. Determine the symmetry of $AB+BA$ and $AB-BA$ if

a. $A,B$ symmetric

Then $A=A^T$, $B=B^T$

so $(AB+BA)^T = (AB)^T+(BA)^T = B^TA^T + A^TB^T = BA+AB = AB+BA$

$\therefore$ $AB+BA$ symmetric

$(AB-BA)^T = (AB)^T-(BA)^T = B^TA^T - A^TB^T = BA-AB = -(AB-BA)$

$\therefore$ $AB-BA$ skew-symmetric

b. $A,B$ hermitian

Then $A=A^*$, $B=B^*$

so $(AB+BA)^* = (AB)^*+(BA)^* = B^*A^*+A^*B^* = BA+AB = AB+BA$

$\therefore$ $AB+BA$ hermitian

And $(AB-BA)^* = (AB)^*-(BA)^* = B^*A^*-A^*B^* = BA-AB$

$= -(AB-BA)$

$\therefore$ $AB-BA$ not hermitian

c. $A, B$ skew-symmetric

Then $A = -A^T$, $B = -B^T$

So $(AB+BA)^T = (AB)^T + (BA)^T = B^T A^T + A^T B^T = (-B)(-A) + (-A)(-B)$

$= BA + AB = AB + BA$

$\therefore AB+BA$ symmetric

And $(AB-BA)^T = (AB)^T - (BA)^T = B^T A^T - A^T B^T = (-B)(-A) - (-A)(-B)$

$= BA - AB = -(AB-BA)$

$\therefore AB-BA$ skew-symmetric

d. $A$ symmetric, $B$ skew-symmetric

Then $A = A^T$ and $B = -B^T$

So $(AB+BA)^T = (AB)^T + (BA)^T = B^T A^T + A^T B^T = (-B)A + A(-B) = -BA - AB$

$= -(AB+BA)$

$\therefore AB+BA$ skew-symmetric

And $(AB-BA)^T = (AB)^T - (BA)^T = B^T A^T - A^T B^T = (-B)A - A(-B)$

$= -BA + AB = AB - BA$

$\therefore AB-BA$ symmetric

Artin

Chapter 10

10.3

18. a. is $\mathbb{Z}/\langle 10\rangle \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 5\rangle$

$\mathbb{Z}/\langle 10\rangle \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 5\rangle$ by CRT since $\gcd(2,5)=1$

b. is $\mathbb{Z}/\langle 8\rangle \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 4\rangle$

Elementary factor decomposition for $\mathbb{Z}/\langle 8\rangle$ is $2^3$

Elementary factor decomposition for $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 4\rangle$ is $2, 2^2$

$\therefore$ They have different elementary factor decompositions and hence are in different isomorphism classes

$\therefore \mathbb{Z}/\langle 8\rangle \ncong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 4\rangle$

28. Let $R$ be a ring and let $I \triangleleft R[x]$. Suppose the lowest degree of a nonzero element of $I$ is $n$ and that $I$ contains a monic polynomial $f(x)$ of degree $n$. Prove that $I$ is principal.

Note that since $f(x) \in I$, $\langle f(x)\rangle \subseteq I$

Now let $g(x) \in I$

Then $g(x) = q(x)f(x) + r(x)$ with $r(x)=0$ or $\deg r(x) < \deg f(x)$

Note we can write $g$ in this way since $f$ monic and of smallest degree in $I$ ie $\deg f(x) \leq \deg g(x)$

suppose $\deg r(x) < \deg f(x)$

we have that $r(x) = g(x) - q(x)f(x) \in I$ since $g, f \in I$, ideal

contradiction to minimality of $n$

$\therefore r(x) = 0$

$\therefore g(x) = q(x)f(x) \in \langle f(x)\rangle$

$\therefore I \subseteq \langle f(x)\rangle$

$\therefore I = \langle f(x)\rangle$

$\therefore$ I principal

10.4

7. Let $I, J \triangleleft R \ni I+J=R$ (R commutative)

a. Prove that $IJ = I \cap J$

Let $ij \in IJ$

Then $ij \in I, J$ since $I, J$ ideals

$\therefore ij \in I \cap J$

$\therefore IJ \subseteq I \cap J$

Now let $x \in I \cap J \Rightarrow x \in I$ and $x \in J$

Note that $1 \in R = I + J \Rightarrow 1 = i + j$ for some $i \in I, j \in J$

So $x = 1 \cdot x = (i+j)x = ix + jx = ix + xj$

But $ix \in IJ$ since $x \in J$ and $xj \in IJ$ since $x \in I$

$\therefore x \in IJ$ since $IJ$ ideal hence closed under addition

$\therefore I \cap J \subseteq IJ$

$\therefore IJ = I \cap J$

10.6

3. Let $R$ be an integral domain. Prove that $R[x]$ is an integral domain.

Let $f(x), g(x) \in R[x]$

And assume $f(x)g(x) = 0$

Then $\deg f(x)g(x) = 0$

So $\deg f(x) + \deg g(x) = 0$

$\therefore \deg f(x) = \deg g(x) = 0$

$\therefore f, g \in R$

Then since $R$ integral domain, $f = 0$ or $g = 0$

$\therefore R[x]$ has no zero divisors

$\therefore R[x]$ integral domain

MISC

23. Let $f(x), g(x) \in R[x]$ where $R$ ring. Assume $f(x) \neq 0$. Prove that if $f(x)g(x) = 0$ then $\exists\, 0 \neq c \in R \ni cg(x) = 0$.

First note that if $g(x) = 0$, the $cg(x) = 0 \;\forall c \in R$

so assume $g(x) \neq 0$

Then since $f(x) \neq 0$ and $f(x)g(x) = 0$, $g(x)$ zero divisor

Now $\deg f(x)g(x) = 0$, so $\deg f(x) + \deg g(x) = 0$

$\therefore \deg f(x) = \deg g(x) = 0$

so $f \in R$

$\therefore \exists 0 \neq f \in R \ni fg(x) = 0$

Artin

Chapter 11

11.2

5. Prove that every prime element of an integral domain is irreducible

Let $R$ be an integral domain and let $p \in R$ prime

Note that $0 \neq p$ nonunit since prime

Assume $p = ab$

Then $p|ab \Rightarrow p|a$ or $p|b$ since $p$ prime

If $p|a$, then $a = pc \Rightarrow ab = pcb \Rightarrow p = pcb \Rightarrow p - pcb = 0 \Rightarrow p(1-cb) = 0$

$\Rightarrow p = 0$ or $1 - cb = 0$ since $R$ integral domain

But $p \neq 0$, so $1 - cb = 0$

$\therefore 1 = cb$

$\therefore b$ unit

Similarly if $p|b$, then $a$ unit

$\therefore$ Either $a$ unit or $b$ unit

$\therefore p$ irreducible

11.3

4. Prove that two integer polynomials are relatively prime in $\mathbb{Q}[x]$ iff the ideal they generate in $\mathbb{Z}[x]$ contains an integer.

Let $f, g$ be integer polynomials

($\Rightarrow$) Assume $\gcd(f,g) = 1$ in $\mathbb{Q}[x]$

Then $1 = qf + rg$ for some $q, r \in \mathbb{Q}[x]$

Let $s$ be common denominator of all terms in $q$ and $r$

Then $s = sqf + srg \in \langle f, g \rangle$ in $\mathbb{Z}[x]$ since $sq, sr \in \mathbb{Z}[x]$

$\therefore \langle f, g \rangle$ contains an integer, namely $s$

($\Leftarrow$) Assume $\langle f, g \rangle$ in $\mathbb{Z}[x]$ contains an integer

Then $n = af + bg$ for some $n \in \mathbb{Z}$, $a, b \in \mathbb{Z}[x]$

So $1 = \frac{a}{n} f + \frac{b}{n} g$

$\therefore \gcd(f,g) = 1$ in $\mathbb{Q}[x]$

11.4

1. Prove the polynomial is irreducible in $\mathbb{Q}[x]$

a. $x^2 + 27x + 213$

Note that $3 | 27, 213$ but $9 \nmid 213$ and $3 \nmid 1$

Then $x^2+27x+213$ irreducible by eisensteins with $p=3$

b. $x^3+6x+12$

Note that $3 \nmid 1$ but $3 | 6, 12$ and $9 \nmid 12$

Then $x^3+6x+12$ irreducible by eisensteins with $p=3$

c. $8x^3-6x+1$

By RRT, the only possible roots in $\mathbb{Q}$ are: $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$

Routine computation shows that none of these are roots

$\therefore 8x^3-6x+1$ does not have a factor of degree 1

$\therefore 8x^3-6x+1$ irreducible in $\mathbb{Q}[x]$

d. $x^3+6x^2+7$

By RRT, the only possible roots in $\mathbb{Q}$ are: $\pm 1, \pm 7$

Routine computation shows that none of these are roots

$\therefore x^3+6x^2+7$ has no factor of degree 1

$\therefore x^3+6x^2+7$ irreducible in $\mathbb{Q}[x]$

e. $x^5-3x^4+3$

Note that $3 \nmid 1$ but $3 | -3, 3$ and $9 \nmid 3$

$\therefore x^5-3x^4+3$ irreducible by Eisensteins with $p=3$

6. Prove that the polynomial is irreducible

a. $x^2+x+1$ in $\mathbb{F}_2$

Note that $(0)^2+0+1 = 1 \neq 0$

and $(1)^2+(1)+1 = 1 \neq 0$

$\therefore x^2+x+1$ has no roots in $\mathbb{F}_2$

$\therefore x^2+x+1$ irreducible in $\mathbb{F}_2$

b. $x^2+1$ in $\mathbb{F}_7$

Note that $(0)^2+1=1 \neq 0$

$(1)^2+1=2\neq 0$
$(2)^2+1=5\neq 0$
$(3)^2+1=3\neq 0$
$(4)^2+1=3\neq 0$
$(5)^2+1=5\neq 0$
$(6)^2+1=2\neq 0$
$\therefore x^2+1$ has no roots in $\mathbb{F}_7$
$\therefore x^2+1$ irreducible in $\mathbb{F}_7$

11. Let $p$ be prime and let $I\neq A\in M_n(\mathbb{Z}) \ni A^p=I$ but $A\neq I$. Prove that $n\geq p-1$.
$A^p=I \Rightarrow A^p-I=0$
$\therefore f(A)=0$ where $f(x)=x^p-1$
By Cayley-Hamilton, $m(x)\mid f(x)$ where $m(x)$ minimal polynomial of $A$
But $A\neq I \Rightarrow A-I\neq 0$
$\therefore g(A)\neq 0$ where $g(x)=x-1$ so $m(x)\nmid x-1$
But $f(x)=x^p-1=(x-1)(x^{p-1}+x^{p-2}+\dots+1)$
$\therefore m(x)\mid x^{p-1}+x^{p-2}+\dots+1$
But $x^{p-1}+\dots+1$ irreducible since $p$ prime
$\therefore m(x)=x^{p-1}+\dots+1$
But $\deg c(x)\geq \deg m(x)=p-1$ where $c(x)$ characteristic polynomial
$\therefore n\geq p-1$

16. Let $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$ be a monic polynomial in $\mathbb{Z}[x]$, and let $r\in\mathbb{Q}$ be a rational root of $f(x)$. Prove that $r\in\mathbb{Z}$.
RRT $\Rightarrow$ only possible rational roots are $\pm\frac{a_0}{1}=\pm a_0\in\mathbb{Z}$ since $f\in\mathbb{Z}[x]$
$\therefore r\in\mathbb{Z}$

11.6

3. Let $d,d'$ distinct square free integers. Prove that $\mathbb{Q}(\sqrt{d})\neq\mathbb{Q}(\sqrt{d'})$
Suppose $\sqrt{d'}\in\mathbb{Q}(\sqrt{d})$

Then $\sqrt{d'} = a + b\sqrt{d} \Rightarrow d' = a^2 + 2ab\sqrt{d} + b^2$ for $a, b \in \mathbb{Q}$

so $\sqrt{d} = \frac{d' - a^2 - b^2}{2ab} \in \mathbb{Q}$

contradiction since $d$ squarefree

$\therefore \sqrt{d'} \notin \mathbb{Q}(\sqrt{d})$

$\therefore \mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$

Artin

Chapter 12

12.1

7. a. Let $I = \text{ann}_R M$ where $M$ R-module. Prove that $I \triangleleft R$

Note that $0 \in R$ and $0m = 0 \ \forall m \in M$

$\therefore 0 \in \text{ann}_R M$

$\therefore \phi \neq \text{ann}_R M \subseteq R$

Let $x, y \in \text{ann}_R M \Rightarrow xm = ym = 0 \ \forall m \in M$

$(x+y)m = xm + ym = 0 + 0 = 0 \ \forall m \in M$

$\therefore x+y \in \text{ann}_R M$

Let $r \in R$

$(rx)m = r(xm) = r \cdot 0 = 0 \ \forall m \in M$

$\therefore rx \in \text{ann}_R M$

$\therefore \text{ann}_R M \triangleleft R$

$\therefore I \triangleleft R$

b. What is $\text{ann}_{\mathbb{Z}} M$ where $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$? what about $\text{ann}_{\mathbb{Z}} \mathbb{Z}$?

Note that the elementary divisor decomposition of $M$ is: $2, 2^2, 3$

so the invariant factors are $2, 12$

And $\text{ann}_{\mathbb{Z}} M$ is the largest invariant factor

$\therefore \text{ann}_{\mathbb{Z}} M = \langle 12 \rangle$

And $\text{ann}_{\mathbb{Z}} \mathbb{Z} = 0$ since $rm = 0 \ \forall m \in \mathbb{Z} \Rightarrow r = 0$

12.6

8. Let $W_1, \ldots, W_k$ be submodules of an R-module $V \ni V = \sum W_i$. Assume that $W_1 \cap W_2 = 0$, $(W_1 + W_2) \cap W_3 = 0, \ldots, (W_1 + \ldots + W_{k-1}) \cap W_k = 0$. Prove that $V = W_1 \oplus \ldots \oplus W_k$

Show that $w_1 + \ldots + w_k = 0$ for $w_i \in W_i \Rightarrow w_i = 0 \ \forall i$

Go by induction on $k$

Clearly true for $k = 1$

If $k = 2$, we have $w_1 + w_2 = 0 \Rightarrow w_2 = -w_1 \in W_1$

$\therefore w_2 \in W_1 \cap W_2$ and similarly $w_1 \in W_1 \cap W_2$

But $W_1 \cap W_2 = 0$, so $w_1 = w_2 = 0$

Now assume true for $k-1$ ie $w_1 + \dots + w_{k-1} = 0 \Rightarrow w_i = 0 \ \forall i$

Now look at $w_1 + \dots + w_{k-1} + w_k = 0$

Then $w_k = -(w_1 + \dots + w_{k-1}) \in (W_1 + \dots + W_{k-1}) \cap W_k$

But $(W_1 + \dots + W_{k-1}) \cap W_k = 0$

So $w_k = 0$

Then $w_1 + \dots + w_{k-1} = 0 \Rightarrow w_i = 0 \ \forall i$ by induction

$\therefore w_1 + \dots + w_k = 0 \Rightarrow w_i = 0 \ \forall i$

$\therefore V = W_1 \oplus \dots \oplus W_k$

12.7

5. Find all possible Jordan Canonical forms for a matrix whose characteristic polynomial is $c(t) = (t+2)^2 (t-5)^3$

Possible minimal polynomials:
1. $m(t) = (t+2)^2 (t-5)^3$
2. $m(t) = (t+2)^2 (t-5)^2$
3. $m(t) = (t+2)^2 (t-5)$
4. $m(t) = (t+2)(t-5)^3$
5. $m(t) = (t+2)(t-5)^2$
6. $m(t) = (t+2)(t-5)$

JCF's:
1. $J(2,-2) \oplus J(3,5)$
2. $J(2,-2) \oplus J(1,5) \oplus J(2,5)$
3. $J(2,-2) \oplus J(1,5)^3$
4. $J(1,-2)^2 \oplus J(3,5)$
5. $J(1,-2)^2 \oplus J(1,5) \oplus J(2,5)$
6. $J(1,-2)^2 \oplus J(1,5)^3$

3. ie
$$\begin{bmatrix} \begin{smallmatrix} -2 & 0 \\ 1 & -2 \end{smallmatrix} & & & & 0 \\ & \begin{smallmatrix} -2 & 0 \\ 1 & -2 \end{smallmatrix} & & & \\ & & 5 & & \\ & 0 & & 5 & \\ & & & & 5 \end{bmatrix}$$

20. Find all possible Jordan canonical forms for $8 \times 8$ matrices whose minimal polynomial is $x^2(x-1)^3$

Possible invariant factors:
1. $x, x^2, x^2(x-1)^3 \Rightarrow J(1,0) \oplus J(2,0)^2 \oplus J(3,1)$
2. $x, x, x, x^2(x-1)^3 \Rightarrow J(1,0)^3 \oplus J(2,0) \oplus J(3,1)$
3. $x^2(x-1), x^2(x-1)^3 \Rightarrow J(2,0)^2 \oplus J(1,1) \oplus J(3,1)$

4. $x, x(x-1), x^2(x-1)^3 \Rightarrow J(1,0)^2 \oplus J(2,0) \oplus J(1,1) \oplus J(3,1)$

5. $x(x-1)^2, x^2(x-1)^3 \Rightarrow J(1,0) \oplus J(2,0) \oplus J(2,1) \oplus J(3,1)$

6. $(x-1), x(x-1), x^2(x-1)^3 \Rightarrow J(1,0) \oplus J(2,0) \oplus J(1,1)^2 \oplus J(3,1)$

7. $(x-1)^3, x^2(x-1)^3 \Rightarrow J(2,0) \oplus J(3,1)^2$

8. $(x-1), (x-1)^2, x^2(x-1)^3 \Rightarrow J(2,0) \oplus J(1,1) \oplus J(2,1) \oplus J(3,1)$

9. $(x-1), (x-1), (x-1), x^2(x-1)^3 \Rightarrow J(2,0) \oplus J(1,1)^3 \oplus J(3,1)$

Artin

Chapter 13

13.1

3. Let $R$ be an integral domain containing a field $F$ as a subring and which is finite-dimensional when viewed as a vector space over $F$. Prove that $R$ is a field.

Let $\dim_F R = n$

Let $0 \neq r \in R$

Consider $1, a, a^2, \dots, a^n$ which is linearly dependent since there are $n+1$ elements in the list and $\dim_F R = n$

so we have $f_0 + f_1 a + \dots + f_n a^n = 0$ $\ni$ at least one $f_i \neq 0$, $f_i \in F$

choose $k$ to be smallest index $\ni f_k \neq 0$

So we have $f_k a^k \left(1 + \frac{f_{k+1}}{f_k} a + \dots + \frac{f_n}{f_k} a^{n-k}\right) = 0$

But $R$ integral domain and $f_k, a^k \neq 0$, so $1 + \frac{f_{k+1}}{f_k} a + \dots + \frac{f_n}{f_k} a^{n-k} = 0$

$\therefore a\left(-\frac{f_{k+1}}{f_k} - \dots - \frac{f_n}{f_k} a^{n-k-1}\right) = 1$

$\therefore a$ unit

$\therefore R$ field

13.3

4. Let $\zeta_n = e^{\frac{2\pi i}{n}}$. Determine the irreducible polynomial over $\mathbb{Q}(\zeta_3)$ of

a. $\zeta_6$