BILINEAR FORMS:

Def: (V a finite dimensional vectorspace over F) A bilinear form on V is a function $f: V \times V \to F$ Satisfying
① $\langle v_1 + v_2 | w \rangle = \langle v_1 | w \rangle + \langle v_2 | w \rangle$
② $\langle v | w_1 + w_2 \rangle = \langle v | w_1 \rangle + \langle v | w_2 \rangle$ } hence "bilinear"
③ $\langle cv | w \rangle = c \langle v | w \rangle = \langle v | cw \rangle$, $c \in F$

Def: A bilinear form is
symmetric if $\langle v|w \rangle = \langle w|v \rangle \Leftrightarrow A^T = A$ for any basis
skew-symmetric if $\langle v|w \rangle = -\langle w|v \rangle \Leftrightarrow A^T = -A$ " " "
positive definite if $\langle v|v \rangle \geq 0$ only 0 if $v = \vec{0}$
non-degenerate $\Leftrightarrow$ A is invertible for any basis

With respect to some basis $\langle v|w \rangle_A = v^T A w$

Prop: Let A be the matrix of a bilinear form w.r.t. some basis. Then the matrices A' of the same form w.r.t. other bases are of the form $A' = P^T A P$ w/ P invertible

Theorem: Let $A \in M_{n \times n}(\mathbb{R})$, then TFAE
i) A is the dot product w.r.t. some basis
ii) $A = P^T P$ where P is invertible
iii) $A^T = A$ (symmetric) and $x^T A x \geq 0$ ($=0$ iff $x = \vec{0}$) (positive definite)

Theorem: (Gram-Schmidt): (V a vector space over $\mathbb{R}$) Let $\langle \cdot | \cdot \rangle$ be a positive definite symmetric bilinear form on V. Then there exists an "orthonormal" bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ with respect to the form (i.e. $\langle v_i | v_j \rangle = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$

Def: Let V be a vector space with symmetric bilinear form $\langle \cdot | \cdot \rangle$. If W is a subspace of V, then the orthogonal complement of W is defined as $W^\perp = \{v \in V \mid \langle v|w \rangle = 0 \ \forall w \in W\}$. In particular, $V^\perp = \{v \in V \mid \langle v|v' \rangle = 0 \ \forall v' \in V\}$

Def: Then $V^\perp$ is the nullspace of the form.

Basic Properties of Orthogonal Complements:
i) $W^\perp$ is a subspace of V
ii) $W \subseteq (W^\perp)^\perp$
iii) $W_1 \subseteq W_2 \Rightarrow W_2^\perp \subseteq W_1^\perp$
iv) $(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$

Proposition (Spectral Theorem for Real Symmetric Forms):

Let V be a vector space over $\mathbb{R}$, $\langle \cdot | \cdot \rangle$ a symmetric bilinear form. Then there exists an orthogonal basis $\{u_1, \ldots, u_n\}$ for V (i.e. $\langle u_i | u_j \rangle = 0$ if $i \neq j$, $\langle u_i | u_j \rangle \in \{-1, 0, 1\}$ if $i = j$)

Corollary: Let A be a symmetric real $n \times n$ matrix. then there is an invertible matrix Q such that $Q^T A Q = \begin{bmatrix} I_p & & \\ & -I_m & \\ & & 0_z \end{bmatrix}$, where $p + m = \operatorname{rank} A$, $z = \dim V^\perp$ (independent of basis for A)

Note: $\operatorname{rank} A + \dim V^\perp = \dim V$, regardless of choice of basis for A

Def: Let $x^* = \overline{x}^T$ (conjugate transpose, x a vector over $\mathbb{C}$) Then the standard hermitian form is $\langle x|y \rangle = x^* y = (x^* I y)$. The standard hermitian satisfies $x^* x = |x|^2$ and i, ii, iii, iv

A General Hermition Form $\langle \cdot | \cdot \rangle$ satisfies: (for any basis, $A^* = A$) (then $A = P^* P$ for some invertible matrix P)

i) $\langle x | y_1 + y_2 \rangle = \langle x | y_1 \rangle + \langle x | y_2 \rangle$, $\langle x | cy \rangle = c \langle x | y \rangle$ "linear in 2nd argument"

ii) $\langle x_1 + x_2 | y \rangle = \langle x_1 | y \rangle + \langle x_2 | y \rangle$, $\langle cx | y \rangle = \overline{c} \langle x | y \rangle$ "conjugate linear in first"

iii) $\langle x | y \rangle = \overline{\langle y | x \rangle}$ "conjugate symmetric" (iv) $\langle x|x \rangle \geq 0 \ \forall x$, $\langle x|x \rangle = 0$ iff $x = 0$ Positive Definite

GALOIS PREREQUISITES: Definitions

Def: (F a field) The prime subfield is the subfield (as a ring) generated by 1 (Products and quotients of Sums and differences of 1)

Def: ($F \subseteq K$ a subfield) We say K is a field extension of F, write K/F, say "K over F".

Def: The characteristic of a field F is char F = smallest n such that $n \cdot 1 = 0$ (Char F = 0 if no such n exists)

Def: If K/F is a field extension, then K is an F-module (since K a ring, $F \subseteq K$

Def: If K is a vector space over F, define the degree or index $[K:F] := \dim_F K$
We call the extension finite if $[K:F] < \infty$, otherwise infinite

Def: ($F \subseteq K$ fields) Let $\{\alpha_j\}_{j \in \Gamma}$ be a collection of elements in K. The field generated by $\{\alpha_j\}_{j\in\Gamma}$ is $F(\alpha_j \mid j \in \Gamma) :=$ the smallest subfield of K containing F and $\{\alpha_j\}_{j\in\Gamma}$ which turns out to be equal to $\left\{\frac{p(\alpha_j\text{'s})}{q(\alpha_j\text{'s})} \text{ where } p(x), q(x) \text{ polys in } F[x_j \mid j \in \Gamma]\right\}$

Def: If $K = F(\{\alpha_j\}_{j\in\Gamma})$, then we say K is generated by α_j's over F.

Def: ($F \subseteq K$ fields) If $\exists$ a single element α s.t. $K = F(\alpha)$, the K is a simple extension (α is a primitive element for K/F)

Def: α is algebraic over F if it is a root of some nonzero $f(x) \in F[x]$, otherwise trancendental

Def: An extension K over F is algebraic if every element of K is algebraic over F

Def: (Let α be algebraic over F) The (unique) minimum polynomial $m_{\alpha,F}(x) = m(x) \in F[x]$ is the monic polynomial of least degree in $F[x]$ that has α as a root.

Def: The degree of α is both $[F(\alpha):F]$, and the number of elements in a basis for $F(\alpha) = \frac{F[x]}{m_\alpha(x)}$ which has basis $1, \alpha, \dots, \alpha^{n-1}$ over F.

Def: K/F is finitely generated if $K = F(\alpha_1, \dots, \alpha_n)$, some n, and some $\alpha_i \in K$.

Def: ($K_1 \subseteq K$, $K_2 \subseteq K$ fields) There composite is $K_1K_2 :=$ smallest subfield of K containing K_1 and K_2.

Def: (F a field, $p(x) \in F(x)$ any poly) The splitting field of $p(x)$ is the minimal field extension over F in which $p(x)$ splits completely into linear factors. "Normal Extension" := Splitting field of a set of polys

Def: The cyclotomic field of n^{th} roots of unity is the splitting field of $x^n - 1$ over $\mathbb{Q}$.
Any generator of this group is called a primitive n^{th} root of unity, denoted ζ_n. (Then $\mathbb{Q}(\zeta)$ contains all roots)

Def: The multiplicative group of n^{th} roots of unity is: $\mu_n = \{1, \zeta, \dots, \zeta^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$, $\zeta^i \mapsto \bar{i}$

this function gives the degree of the ext/$\mathbb{Q}$, so $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$

The Euler Phi Function, $\phi(n) := \left|\{a \mid 1 \le a \le n \text{ and } \gcd(a,n) = 1\}\right|$, these $\bar{a}$ are generators of $\mathbb{Z}/n\mathbb{Z}$ (then ζ^a generates μ_n)

Def: The n^{th} cyclotomic polynomial is $\phi_n(x) := \prod(x - \zeta)$, product over all primitive roots (i.e. ζ^a s.t. $\gcd(a,n)=1$)

Def: A field K is algebraically closed if every poly w/ coefficients in K has a root in K.

Def: The field $\bar{F}$ is called an algebraic closure of F if $\bar{F}$ is algebraic over F, and every poly $p(x) \in F[x]$ splits completely (into linear factors) over $\bar{F}$. (K algebraically closed) $\Leftrightarrow$ (Every p(x) splits completely over K) $\Leftrightarrow$ (No alg ext.) $\Leftrightarrow$ ($K = \bar{K}$)

Def: $p(x)$ is seperable if it has no multiple roots (all distinct (in splitting field)), inseperable otherwise

Def: (Char $F = p > 0$; p prime since F domain) F is perfect if $F^p := \{a^p \mid a \in F\} = F$. Every elt a p^{th} power of some elt in F.

Def: (Char F = p) The map $f: F \to F$, $r \mapsto r^p$ is called the Frobenius Endomorphism of F. Identity in $\mathbb{F}_p$

Def: Any irreducible poly $p(x)$ can be written uniquely as $p(x) = P_{sep}(x^{p^k})$, $(k \ge 0)$ for a unique polynomial $P_{sep}(x)$, which is seperable.

Def: Seperable degree of $p(x)$ is defined as $\deg_s p(x) := \deg P_{sep}(x)$

Def: K is a seperable field extension over F if every $\alpha \in K$ is a root of a seperable polynomial over F (equivilently, its (α) minimal poly is seperable), otherwise K is inseperable over F.

GALOIS PREREQUISITES: Results

so $\mathbb{Z}/p\mathbb{Z} \cong$ sub(ring?) of F

Cor: If Char $F = p > 0$ (p prime since F domain), then the prime subfield contains $1, \dots, p-1$ and $F_p = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Thm: (F a field, $p(x)$ irreducible in $F[x]$) then $\exists$ a field extension K of F in which $p(x)$ has a root, call it α. Then $K = F(\alpha) = \frac{F[x]}{p(x)}$.

Note: $F(x)$ think quotients, $F[x]$ no quotients

Cor1: $\frac{F[x]}{p(x)}$ is really the smallest field extension of F containing a root of $p(x)$.

Cor2: (Let $n = \deg p$) $F(\alpha) = \{F\text{-linear combinations of } 1, \alpha, \dots, \alpha^{n-1}\}$ and $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis of $F(\alpha)$ (as an F-vector space)

Cor3: ($p(x)$ still irreducible in $F[x]$) If α_1 and α_2 are roots in a field extension K, $F(\alpha_1) \cong F(\alpha_2)$ via an iso which fixes F, swaps α_1/α_2

Thm: (Generalizing Cor 3) Let $\varphi: F \to \tilde{F}$ be any isomorphism of fields, $p(x) \in F(x)$ irreducible. Let $\tilde{p}(x)$ be the poly obtained by applying φ to the coeff-s of $p(x)$. Let α be a root of $p(x)$ in some field K (splitting perhaps) and β a root of $\tilde{p}(x)$ in $\tilde{K}$. Then $\exists \sigma: F(\alpha) \to \tilde{F}(\beta)$ (isomorphism), $\sigma|_F = \varphi$.

Prop: ⓐ monic version of $m_{\alpha,F}$ is unique ⓑ Also the unique monic irreducible in $F[x]$ w/ α as a root ⓒ If $f(x) \in F[x]$ has α as a root, then $m_{\alpha,F} \mid f$ (both in $F[x]$)

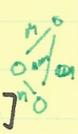
Cor: If F is a field, L a field extension of F, then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ (both in $L[x]$)

Prop: α is algebraic over $F \Leftrightarrow F(\alpha)$ is finite, i.e. $[F(\alpha):F] < \infty$

Stronger: ⓐ α a root of $p(x) \in F[x]$ (and $\deg p = n$) $\Rightarrow [F(\alpha):F] \leq n$

ⓑ $[F(\alpha):F] = n < \infty \Rightarrow \alpha$ algebraic over F w/ $\deg m_{\alpha,F} = n$

Cor: ($F \subseteq K$ a finite extension, i.e. $[K:F] < \infty$) $\Rightarrow K$ is algebraic over F



⊛ **Lemma:** $L \subseteq F \subseteq K$ field extension, then $[K:L] = [K:F][F:L]$

⊛ **Cor:** If $\alpha \in K$ is algebraic over F, then $\deg(m_{\alpha,F}) \mid [K:F]$

$\boxed{x^n - 1 = (x-1)(x^{n-1} + \dots + 1) \text{ never irreducible} / \mathbb{Q}}$

Lemma: $F(\alpha)(\beta) = F(\alpha, \beta)$

Thm: K/F is a finite extension ($\overbrace{[K:F]}^{=\text{dimension of } K \text{ as an } F\text{-vector space}} < \infty$) $\Leftrightarrow K = F(\alpha_1, \dots, \alpha_n)$ w/ each α_i algebraic $/F$

Cor: If α, β algebraic over F, then ① $\alpha \pm \beta \in F(\alpha,\beta)$ ② $\alpha\beta \in F(\alpha,\beta)$ ③ $\frac{\alpha}{\beta} \in F(\alpha,\beta)$ So all are algebraic $/F$!

Cor: K algebraic over F & L algebraic over $K \Rightarrow L$ algebraic over F $\left(\underset{\text{alg}}{F \subseteq} \underset{\text{alg}}{K \subseteq} L \Rightarrow \underset{\text{alg}}{F \subseteq L}\right)$

Prop: If K_1, K_2 are finite field extensions over F, then $[K_1K_2:F] \leq [\underset{n}{K_1}:F][\underset{m}{K_2}:F]$ w/ equality $\Leftrightarrow$ The basis for K_1/F remains indep over K_2

$\Longleftrightarrow$ (Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_m$ be bases for K_1, K_2) $\left\{\alpha_i\beta_j \,\middle|\, \begin{matrix} 1 \leq i \leq n \\ 1 \leq j \leq m \end{matrix}\right\}$ a basis for K_1K_2

$$\begin{tikzcd}
 & K_1K_2 \arrow[dd, dash, "\leq mn"] & \\
K_1 \arrow[dr, dash, "n"'] & & K_2 \arrow[dl, dash, "m"] \\
 & F &
\end{tikzcd}$$

Cor: If $\gcd(n,m) = 1$, then equality holds

Thm: Splitting fields always exist.

Cor: If $\deg p(x) = n$, and K is a splitting field of $p(x)/F$, then $[K:F] \leq n!$

Thm: ($\varphi: F \xrightarrow{\sim} \tilde{F}$, $p(x) \in F[x]$, $\tilde{p}(x) = \varphi(p(x)) \in \tilde{F}(x]$, K & $\tilde{K}$ splitting fields) $\Rightarrow \exists \sigma: K \xleftrightarrow{\sim} \tilde{K}$ s.t. $\sigma|_F = \varphi$

Cor: Splitting fields are unique up to isom.

Thm: The closure of F, $\overline{F}$, is unique up to isom.

Prop/Cor: $p(x)$ has a multiple root $\Leftrightarrow \alpha$ is a root of $p(x)$ and $p'(x) \Leftrightarrow \gcd(p, p') \neq 1 \in F[x]$

Thm: If Char $F = 0$, then every irreducible $p(x) \in F[x]$ is seperable

Thm: If Char $F = p$ and F is perfect, then every irreducible $p(x) \in F[x]$ is seperable

In general: If Char $F = p$, then every irred. $p(x) = P_{sep}(x^{p^K})$ ($K \geq 0$) for a unique seperable $P_{sep}(x)$.

Cor: If $[(\overset{\text{e.g. } \mathbb{Q}}{\text{Char } F = 0}) \vee (\overset{\text{e.g. } \mathbb{F}_p}{\text{Char } F = p \text{ and}}\ F \text{ is perfect})]$ Then any extension K/F is seperable

Theorem: The cyclotomic poly $\Phi_n(x)$ is monic/irred. in $\mathbb{Z}[x]$, and has degree $\phi(n)$. So it is the mimimal polynomial for any primitive n^{th} root of unity ζ_n over $\mathbb{Q}$.

Galois Theory

Def: $\mathrm{Aut}(K)$:= all automorphisms of K, $\mathrm{Aut}(K/F) := \{\sigma \in \mathrm{Aut}(K)$ that fix $F\}$. $\mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$

FACT: If $\sigma \in \mathrm{Aut}(K)$, then $\sigma(1)=1$ and σ fixes the prime subfield (usually $\mathbb{Q}$ or $\mathbb{F}_p$)

Prop: (Let K/F be a field extension, α algebraic over F with minimal poly $m(x)$)

① For all $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(a)$ is again a root of $m(x)$

② (K splitting field over F for $m(x)$, α, β roots) There exists a $\sigma \in \mathrm{Aut}(K/F)$: $\sigma(\alpha)=\beta$

so $\mathrm{Aut}(K/F) \leq$ Symmetric group on roots

③ (K splitting field over F for $m(x)$, $\sigma \in \mathrm{Aut}(K/F)$) Then σ is determined by its values on the roots of $m(x)$

Def: If $|\mathrm{Aut}(K/F)| = [K:F]$, we call K/F Galois, and write $\mathrm{Gal}(K/F)$ instead of $\mathrm{Aut}(K/F)$

Def: The fixed field of H ($H < \mathrm{Aut}(K)$) is $K^H := \{k \in K \mid \forall \sigma \in H, \sigma(k)=k\}$

Prop: The association of groups to fields ($H \rightsquigarrow K^H$) and fields to groups is inclusion reversing

① If $F_1 \subseteq F_2 \subseteq K$ are two subfields of K, then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$

$H \rightsquigarrow K^H$
$K^H \rightsquigarrow H$

② If $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups, then $K^{H_2} \subseteq K^{H_1}$

But not necessarily 1 to 1 unless galois

Thm: (Let $G < \mathrm{Aut}(K)$, G finite) Then $|G| = [K:K^G]$

Cor 1: (Let K/F be a finite extension) Then $|\mathrm{Aut}(K/F)| \leq [K:F]$ and they are equal (i.e. K/F Galois) $\Leftrightarrow$ F is the fixed field of $\mathrm{Aut}(K/F)$ (i.e. $F = K^{\mathrm{Aut}(K/F)}$)

Cor 2: (K a field, $G \leq \mathrm{Aut}(K)$, G finite) Then $\mathrm{Aut}(K/K^G) = G$, so K/K^G is Galois w/ Galois group G

Cor 3: If $G_1 \neq G_2$ are finite subgroups of $\mathrm{Aut}(K)$, then their fixed fields are different (i.e. $K^{G_1} \neq K^{G_2}$)

Summary: K/F Galois $\Leftrightarrow |\mathrm{Aut}(K/F)| = [K:F] \Leftrightarrow$ K splitting field of a seperable polynomial $\Leftrightarrow$ K/F is a normal, seperable extension $\Leftrightarrow F = K^{\mathrm{Aut}(K/F)}$

Thm: Fundamental Theorem of Galois Theory: Let K/F be a finite Galois extension, then there is a bijection between subfields E s.t. $F \subseteq E \subseteq K$, and subgroups H of G ($G = \mathrm{Gal}(K/F)$) given by the correspondances $E \longmapsto \{\sigma \in G$ fixing $E\}$ and $K^H \longleftarrow H$ which is: ① Inclusion Reversing ($E_1 \subseteq E_2 \Rightarrow \mathrm{Aut}(K/E_2) \leq \mathrm{Aut}(K/E_1)$ and $H_1 \leq H_2 \Rightarrow K^{H_2} \subseteq K^{H_1}$) ② $\overset{\text{fields}}{[K:E]} = \overset{\text{groups}}{[H:1]} = |H|$ and $[E:F] = [G:H]$

③ K/E is always Galois, and $\mathrm{Gal}(K/E) = H$ ④ E/F is Galois $\Leftrightarrow H \trianglelefteq G$

Then $\overset{\text{quotient}}{G/H} \cong \mathrm{Gal}(E/F)$

⑤

$$\begin{tikzcd}
 & E_1E_2 \arrow[rrr, leftrightarrow, "get"] \arrow[dl, dash] \arrow[dr, dash] & & & H_1\cap H_2 \arrow[dl, dash] \arrow[dr, dash] & \\
E_1 \arrow[dr, dash] & & E_2 \arrow[r, leftrightarrow, "given"] \arrow[dl, dash] & H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
 & E_1\cap E_2 \arrow[rrr, leftrightarrow, "get"] & & & \langle H_1, H_2\rangle &
\end{tikzcd}$$

If E_1, E_2 correspond to H_1, H_2, then $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$ and $E_1E_2 \longleftrightarrow H_1 \cap H_2$

Def: Any finite field has char $=p$, order p^n, and containg $\mathbb{F}_p$ as its prime subfield.

Thm: Each finite field (w/ order p^n) is the splitting field of $x^{p^n} - x$, so unique.

Thm: $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois Ext, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) =$ "cyclic of order n" $= \langle f \rangle =$ group generated by frobenius map

Thm 3: Given $\mathbb{F}_{p^n}/\mathbb{F}_p$, for every d/n, $\frac{n}{d}/n$ and $\exists!$ subgroup of order $\frac{n}{d}$ ($\langle f^d \rangle$) since $\langle f \rangle$ cyclic

$$\begin{tikzcd}
\mathbb{F}_{p^n} \arrow[r, leftrightarrow] \arrow[d, dash, "n/d"'] \arrow[dd, bend right, dash, "n"'] & 1 \arrow[d, dash, "n/d"] \\
E \arrow[r, leftrightarrow] \arrow[d, dash, "d"'] & \langle f^d \rangle \arrow[d, dash, "d"] \\
\mathbb{F}_p \arrow[r, leftrightarrow] & \langle f \rangle
\end{tikzcd}$$

Cor: Given any $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}}$, both in $\mathbb{F}_{p^{n_1 n_2}}$.

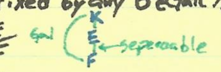
$\overline{\mathbb{F}_p} := \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

Thm: (Primitive Element Thm) Given a seperable finite extension K/F, K/F is a simple extension.

Rmk: Any finite extension of $\mathbb{Q}, \mathbb{R}, \mathbb{F}_p$ is automatically seperable, so theorem above applies.

Rmk: If K is Galois, and θ is an F-linear combo of basis elt not fixed by any $\sigma \in \mathrm{Gal}(K/F)$ except identity, $K = F(\theta)$

Cor/Thm: If E/F is a seperable finite extension, then $\exists$ a Galois closure of E/F



Main Lemma: (K/F finite) then, K/F simple $\Leftrightarrow$ Only finitely many fields between K and F.

MODULE THEORY: Free, Noetherian, etc. [DEFINITIONS]

Def: A left R-module M is an Abelian group under addition together w/a ring action of R on M ($R\times M\to M$, $(r,m)\mapsto r\cdot m$) s.t.: $\forall r,s\in R$ and $\forall\, m,n\in M$
(a) $(r+s)m = rm+sm$ (b) $(rs)m = r(sm)$ (c) $r(m+n) = rm+rn$ (d) $\overset{\text{unitary}}{1m=m}$

Def: A submodule $N\subset M$ is an additive subgroup closed under the R-action

Def: The (left) R-module R acts on itself via left multiplication (submodules $\equiv$ (left) ideals)

Def: The module R^n is the free module of rank n over R. Addition componentwise; $\alpha(a_1,a_2)=(\alpha a_1,\alpha a_2)$

Def: Module homomorphism: $\overset{\text{both R-modules}}{\varphi:M\to N}$; ⓐ $\varphi(m+n)=\varphi(m)+\varphi(n)$ ⓑ $\varphi(rm)=r\varphi(m)$

Def: (M, N R-modules) $\mathrm{Hom}_R(M,N)=\{\forall\varphi:M\to N\}$, $\mathrm{END}_R(M)=\{\forall\varphi:M\to M\}$

Def: ($N\subseteq M$ R-modules) Then M/N is an R-module w/ $r\cdot\overline{m}=\overline{rm}$

Def: (Given an R-module M) Let $X\subseteq M$ be an arbitrary subset. The submodule generated by X is $RX := \{\sum' r_i x_i \mid r_i\in R, x_i\in X\}\subseteq M$. If $N=RX$, we say x generates N, or X is a set of generators for N. (RX is the smallest submodule of M containing X.)
N is finitely generated if $|X|<\infty$, N is cyclic if $|X|=1$, then $N=\{rx \mid r\in R\}$

Def: If $M_1,\dots,M_K$ is a finite collection of R-modules; then the direct product or external direct sum is $\underset{}{\overset{\text{(dir product)}}{M_1\times\cdots\times M_K}} = \overset{\text{(ext dir sum)}}{M_1\oplus\cdots\oplus M_K} = \{(m_1,\dots,m_K) \mid m_i\in M_i\}$ addition/scalar mult defined componentwise

The internal direct sum is $M_1+\cdots+M_K=\{m_1+\cdots+m_K \mid m_i\in M_i\}$ all finite sum of elements in $\cup M_i$ the submodule generated by $\cup M_i$

Def: (F an R-mod) F is free over R (as an R-mod) if it has a basis X such that for every $m\in F$, m $\overset{\text{span}}{\text{can be written}}$ $\overset{\text{independent}}{\text{uniquely}}$ as $m=r_1x_1+\cdots+r_nx_n$ for some $x_1,\dots,x_n \in X$
That is, $m=\sum_{x\in X} r_x x$, r_x's in R, only finitely many r_x non zero, r_x's unique. we say "F is free on the set X"

Def: If X is independent, then $r_1x_1+\cdots+r_nx_n=0 \Rightarrow r_1=\cdots=r_n=0$.

Def: (R a dom, M an R-mod) $\mathrm{Rank}(M)$ = max number of independent elements of M
Rank(M) can be ∞

Def: An R-mod M is Noetherian if any chain $M_1\subseteq M_2\subseteq\cdots$ stabilizes ($\exists N: n\geq N \Rightarrow M_n=M_N$)
A ring R is Noetherian if it is Noeth as a left R-mod R (i.e. if every chain of left ideals stabilizes)

MODULE THEORY: Free, Noetherian, etc. [Results]

Note: (M an R-mod, $I \subset M$ ideal) If I annihilates M, M is naturally an R/I module.

1st Iso Thm: $\varphi: M \to N$ (a homom of submodules) induces $\tilde{\varphi}: M/\ker\varphi \to \operatorname{im}\varphi$ via $\varphi(\bar{m}) \overset{def}{=} \varphi(m)$

2nd Iso Thm: ($A, B \subseteq M$ submodules) Than $\frac{A+B}{B} \cong \frac{A}{A \cap B}$

3rd Iso Thm: ($A, B \subseteq M$ submodules) If $A \subseteq B \subseteq M$, then $\frac{M/A}{B/A} \cong M/B$

Correspondence: Given the natural projection homom $\pi: M \to M/N$ ($N \subseteq M$ submodule) there is a 1 to 1 correspondence $\left\{\begin{matrix}\text{submodules } T \text{ s.t.} \\ N \subseteq T \subseteq M\end{matrix}\right\} \longleftrightarrow \{\text{Submodules of } M/N\}$ via $T \mapsto \pi(T) = T/N$

TFAE: i) The natural R homom $N_1 \oplus \cdots \oplus N_K \xrightarrow{(n_1, \ldots, n_K) \mapsto n_1 + \cdots + n_K} N_1 + \cdots + N_K$ is an isomorphism

ii) Every $x \in N_1 + \cdots + N_K$ can be written uniquely as $n_1 + \cdots + n_K$ w/ $n_i \in N_i$

iii) For each $i \in \{1, \ldots, K\}$, $N_i \cap (N_1 + \cdots + \widehat{N_i} + \cdots + N_K) = 0$.

If these hold, $N = N_1 + \cdots + N_K \cong N_1 \oplus \cdots \oplus N_K$, and we write $N_1 \oplus \cdots \oplus N_K$ for both.

Rmk: F is free on $X \leftrightarrow X$ generates F and X is independent (F an R-module)

Rmk: If R is commutative, then any two bases of an R-mod F have the same cardinality, then we define $\operatorname{rank}(F) = |X|$ for any basis X of F.

UMP for free modules: (R any ring, M any R-module, X any set, $\varphi: X \to M$ map of sets)

① There exists (unique) an R-module F ($F(X)$) that is free on X

② $\exists!$ R-mod homom $\tilde{\varphi}: F \to M$ extending φ (i.e. $\tilde{\varphi}|_X = \varphi$)

$$\begin{tikzcd} X \arrow[r, "\forall\varphi"] \arrow[dr, hook, "\text{inclusion}"'] & M \\ & F \arrow[u, dotted, "\exists!\tilde{\varphi}"'] \end{tikzcd}$$

Cor: The free R-mod on X is unique up to isom. (i.e. If F, G free on X, then $F \cong G$)

Cor: If $|X| < \infty$, say $X = \{x_1, \ldots, x_n\}$ and F free on X ($X \subseteq F$), then $F = Rx_1 \oplus \cdots \oplus Rx_n$ ← internal direct sum of those submodules of F

and $F \cong Rx_1 \oplus \cdots \oplus Rx_n$ ← external direct sum of submods and each $Rx_i \cong R$ as submods, so $F \cong R \oplus \cdots \oplus R = R^n$

Every basis has the same cardinality if R comm, otherwise who knows

Prop: (R a domain, M a free R module of rank $n < \infty$) Any $n+1$ elements are dependent.

Thm: M a left R-module, then TFAE:

i) M is Noetherian

ii) Every nonempty set of submodules of M contains a maximal element.

iii) Every submodule $N \subseteq M$ is finitely generated (in particular, M is finitely generated)

Cor:
R a PID $\Rightarrow$ R Noetherian

RESULTS FROM HOMEWORK ASSIGNMENTS

FACT: (M an R-mod) If M generated by $\{m_\alpha\}$ and M is finitely generated, then M is generated by a finite subset of $\{m_\alpha\}$

Fact: $\mathbb{Q}$ is not a free $\mathbb{Z}$-module

FACT: If F is free on X, G is free on Y, $|X| = |Y|$, then $F \cong G$ as R-modules

FACT: Any cyclic R-module M is isomorphic to an R-module R/I for some ideal I.

FACT: ($N \subseteq M$ submodule) If N and M/N are finitely generated (as R mod), then M is f.g too

FACT: ($N \subseteq M$ submodule) If N and M/N are Noetherian, then M is Noetherian too.

FACT: If N_1 and N_2 are Noetherian R-modules, then so is $N_1 \oplus N_2$

MODULE-S OVER PID-S: RCF & JCF

Structure Theorem for Modules over PID-s: (R a PID, M a free R-module of rank n) Then any submodule N is free of rank $m \le n$. Furthermore, there exists a basis $y_1, \dots, y_m$ of M, and nonzero elt $r_1, \dots, r_m$ of R (w/ $r_1 | r_2 | \cdots | r_m$) s.t. $\overset{\text{w/ some renumbering of } y_i\text{'s}}{r_1 y_1, \dots, r_m y_m}$ basis for N

Fundamental Theorem of F.G. Modules/PIDs: (R PID, M f.g. R-mod) then there exist unique $r, m, \overbrace{r_1, \dots, r_m}^{\text{up to associates}}$ (w/ $r_1 | r_2 | \cdots | r_m$) such that $M \cong R^r \oplus R/(r_1) \oplus \cdots \oplus R/(r_m)$ (Same decomp $\leftrightarrow M_1 \cong M_2$ / Diff decomp $\leftrightarrow M_1 \not\cong M_2$)

Def: r is the free rank of M ($\text{rank}(M) = r$) **Def:** $r_1, \dots, r_m$ are the invariant factors of M.

Def: (R a domain, M an R-module) The torsion submodule is $Tor(M) := \overset{\text{"set of killable elements"}}{\{m \in M \mid rm = 0 \text{ for some } r \neq 0\}}$

Def: (R a domain, M an R-module) M is a torsion R-module if $Tor(M) = M$

Def: (R a domain, M an R-module) M is torsion free if $Tor(M) = \{0\}$

(A general R-module doesn't have to be either)

Def: (R a domain, M an R-module) The annihilator of M is $Ann(M) := \{r \in R \mid rm = 0\ \forall m\}$ $\left[\begin{matrix} Tor(M) \subseteq M \\ Ann(M) \subseteq R \end{matrix}\right]$

Cor to F.T.F.G.M./PIDs: M a torsion module $\overset{\text{then } r_m M = \{0\}}{\leftrightarrow r = 0}$; M torsion free $\overset{\text{then } M \cong R^r\text{, so free}}{\leftrightarrow m = 0}$

Elementary Divisors: Since R PID $\Rightarrow$ R UFD, each invariant factor r_i decomposes further into irreducibles uniquely up to associates, so $\frac{R}{(r_i)} \cong R/(q_1^{e_1}) \oplus \cdots \oplus R/(q_t^{e_t})$

Theorem: Elem. Div. version of Fun. Thm/PIDs: (R a PID, M a f.g. R-module) Then for a unique r, and unique p_i's up to associates (but not nec. distinct) $M \cong R^r \oplus \frac{R}{(p_i^{n_i})} \oplus \cdots \oplus \frac{R}{(p_s^{n_s})}$

RATIONAL CANONICAL FORM [canonical form over original field]

Given V an n-dim vector space, F a field, $T: V \to V$ an ~~F~~ $\overset{F \text{ linear map}}{\text{linear map}}$, Then V is isomorphic to an $F[x]$-module w/ $x \cdot \vec{v} := T(v)$; Conversely, given an $F[x]$-module V, we can define $T(v) := xv$

So given V and $T: V \to V$, $V \cong \frac{F[x]}{r_1(x)} \oplus \cdots \oplus \frac{F[x]}{r_m(x)}$ where $m_T(x) = r_m(x)$ and $\prod_{i=1}^{m} r_i(x) = c_T(x)$

Then RCF of T (of A) is $\begin{bmatrix} \boxed{C_{r_1(x)}} & & \\ & \ddots & \\ & & \boxed{C_{r_m(x)}} \end{bmatrix}$ with companion matrix $C_{r_i(x)} = \begin{bmatrix} 0 & & & -b_0 \\ 1 & \ddots & & -b_1 \\ & \ddots & 0 & -b_{n-2} \\ & & 1 & -b_{n-1} \end{bmatrix}$ where $r_i(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$

- $c_T(x) = \prod_{i=1}^{m} r_i(x)$; $m_T(x) = r_m(x)$

Two matrices/transformations are similar iff they have the same RCF (up to block order)

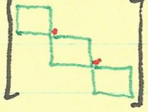
JORDAN CANONICAL FORM [canonical form over extension containing all roots]

Like RCF, start by breaking into invariant factor. Then break those down to elementary divisors: $V \cong \frac{\mathbb{Q}[x]}{r_1(x)} \oplus \cdots \oplus \frac{\mathbb{Q}[x]}{r_m(x)}$

$$V \cong \frac{\mathbb{Q}[x]}{(x-\lambda_i)^{n_i}} \oplus \cdots \oplus \frac{\mathbb{C}[x]}{(x-\lambda_j)^{n_j}} \oplus \cdots \oplus \frac{\mathbb{Q}[x]}{(x-\lambda_k)^{n_k}} \oplus \cdots \oplus \frac{\mathbb{Q}[x]}{(x-\lambda_p)^{n_p}}$$

(λ_j, λ_k) can be the same

Jordan Block for each $(x-\lambda_i)^{n_i}$ has size n_i, of the form $\begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & \ddots \\ & & & \lambda_i \end{bmatrix}_{n_i \times n_i}$

Then JCF =  (order of blocks doesn't matter for JCF or RCF)

POLYNOMIAL RINGS: RESULTS

Cor: $R[x]$ a PID $\rightarrow$ R a field (equivalently) R not a field $\rightarrow$ $R[x]$ not a PID

Prop: R a UFD $\longrightarrow$ $R[x]$ a UFD (also) R a domain $\longrightarrow$ $R[x]$ a domain

Domain not necessary, see p. 30

Prop: (R, $R[x]$ domains) Units of $R[x]$ are the units of R, (also) $\overset{\neq 0}{f,g} \in R[x] \rightarrow \deg(fg) = \deg(f) + \deg(g)$

Note: $a = bx \leftrightarrow b|a \leftrightarrow a \in (b) \leftrightarrow (a) \subseteq (b)$

Prop: (In a domain) an element p is prime $\rightarrow$ p is irreducible

Prop: (In a UFD) an element p is prime $\longleftrightarrow$ p is irreducible

Thm: (R, S comm) Given any ringmap $\varphi: R \to S$ w/ $\varphi(1) = 1$, if we choose any $s \in S$, there exists a unique "evaluation at s" map $\tilde{\varphi}: R[x] \to S$ extending φ s.t. $\tilde{\varphi}|_R = \varphi$ and $\tilde{\varphi}(x) = s$

Prop: "Division Algorithm": Let $f, g \in R[x]$ $(\neq 0)$. If leading coeff of g a unit in R, $\exists! q, r \in R[x]: f = qg + r$ w/ $r = 0$ or $\deg(r) < \deg(g)$

Cor: If F is a field, $F[x]$ is a Euclidean Domain

Cor. of Div. Alg: Let $f \in \overset{\leftarrow \text{E.D.}}{R[x]}$. Then $c \in R$ a root $\longleftrightarrow$ $x - c$ divides f.

Thm: (R, S Domains w/ $R \subseteq S$) $f \in R[x]$ w/ $\deg(f) = n$ $\Rightarrow$ f has at most n distinct roots in S.

Prop: (R a domain, $f \in R[x]$, $c \in R$ a root of f) c is a multiple root $\longleftrightarrow$ $f(c) = 0 \wedge f'(c) = 0$

Lemma: (I an ideal of R) ① Ideal in $R[x]$ generated by I is $I[x] := \{$poly's w/ coeff in $I\}$ ② $\frac{R[x]}{I[x]} \cong (R/I)[x]$

Prop: (R a domain, I a proper ideal, $f(x)$ monic, $\deg(f) > 0$)($\varphi: R[x] \to (R/I)[x]$, $f(x) \mapsto \overline{f(x)}$)

If $\overline{f(x)} \in \frac{R}{I}[x]$ cannot be factored into a product of 2 poly of smaller deg, then $f(x) \in R[x]$ is irreducible

Eisenstein Criterion: (R a domain, $P \subseteq R$ prime ideal) If $f(x)$ monic, non-leading coeff's $\in P$, $a_0 \notin P^2 \rightarrow f(x)$ irreducible in $R[x]$

Gauss's Lemma: (R a UFD, F it's ffrac) If $p(x)$ reducible(~~irreducible~~) in $F[x]$, then reducible(~~irreducible~~) in $R[x]$

equivalently If $p(x)$ irreducible in $R[x]$, then $p(x)$ irreducible in $F[x]$.

Corollary (partial converse): (R UFD, F ffrac) $\gcd(a_0, \ldots, a_n) = 1 \longrightarrow$ (p irred in $R[x] \longleftrightarrow p$ irred in $F[x]$)

RING THEORY: RESULTS

- Any finite domain is a field
- Any finite division Ring is a field
- Given ring map $\varphi; R \to S$, and $0 \subseteq I \subseteq \ker\varphi$, $\bar{\varphi}: R/I \to S, \bar{r} \mapsto \varphi(r)$ is a well defined homom.
- (Correspondance) Ideals of R containing I: Ideals of R/I: $\boxed{\begin{array}{cccc} I \subset J & \subset K & \subset R \\ I/I \subset J/I & \subset K/I & \subset R/I \end{array}}$ $R/J \cong \dfrac{R/I}{J/I}$

$\underline{I+J}$: $= \{a + b \mid a \in I, b \in J\}$ } both ideals

$\underline{IJ}$: $= \{\sum_{i=1}^{n} a_i b_j \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$ }

Fact: $X \subseteq I \leftrightarrow (X) \subset I$

Prop: $I = R \longleftrightarrow I$ contains a unit $\longleftrightarrow I = (1_R)$

Cor: (R commutative) R is a field $\longleftrightarrow$ no proper nontrivial ideals

Cor: If K is a field, then any nonzero homom $\varphi: K \to S$ is injective

Prop: Every proper ideal I is contained in a maximal one (R must have 1, i.e. $R \neq \{0\}$)

Prop: (R comm.) A proper ideal M is maximal $\longleftrightarrow R/M$ is a field

Prop: (R comm w/ $1 \neq 0$) An ideal P is prime $\longleftrightarrow R/P$ is a domain

Cor: (R comm w/1) The ideal $(0) = \{0\}$ is prime $\longleftrightarrow R$ is a domain

Cor: (R comm) I is maximal $\Rightarrow I$ is prime

UMP: R a ring (comm), $S^{-1}R$ is the field of fractions of R, T a ring:

$$\begin{tikzcd} & S^{-1}R \arrow[dd, dotted, "\exists! \tilde{\phi}"] \\ R \arrow[ur, hook, "i"] \arrow[dr, "\forall \phi \text{ (homom)}"'] & \\ & T \end{tikzcd}$$

ϕ inj, $S \mapsto$ units

Fact: $\gcd(m,n) = g \longleftrightarrow (m,n) = (g)$

SunTzu: (R comm w/ $1 \neq 0$) $I_1 \ldots I_n$ pairwise comaximal, then $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$ (p. 16, 17)

Cor: If $\gcd(m,n) = 1$ for $m,n \in \mathbb{Z}$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Cor: ($n \in \mathbb{Z}^+$) $n = p_1^{e_1} \cdots p_r^{e_r}$, then $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times = (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \cdots (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$

Prop: (R a PID) Every nonzero prime ideal is maximal

RING THEORY: DEFINITIONS

Division Ring: A ring w/ every nonzero element a unit (finite $\Rightarrow$ field, commutative $\Rightarrow$ field)

Field: A commutative division ring

Integral Domain: A commutative ring w/ no zero divisors (Cancellation holds)

Ideal Generated by X: $RXR = \{rxr' \mid r, r' \in R$ and $x \in X$ after closure under addition$\}$

Principal Ideal (x): RxR (If R is commutative, (x) is prime)

Prime Ideal: $ab \in P \to a \in P \vee b \in P$ p is prime if (p) is a prime ideal

Comaximal Ideals: I, J ideals of commutative ring R comaximal if $I + J = R$

Norm: Measure of size on an integral domain R. $N: R \to \mathbb{N}$, $N(0) = 0$, $\boxed{\overset{\text{positive norm}}{N(a) > 0 \quad \forall a \neq 0}}$

Division Algorithm: An integral domain w/ a division algorithm: $\forall a, b \in R\ (b \neq 0) \exists q, r \in R: a = qb + r$ s.t. $r = 0$ or $N(r) < N(b)$

Euclidean Domain: An integral domain that has a division algorithm (this allows the Euclidean Algorithm to work)

Divisor/Multiple: If $a = bx$ for some x, then b/a and a is a multiple of b

GCD: $d \in R$ is the $\gcd(a,b)$ if d/a and $d|b$, and $(d'|a \wedge d'|b) \to d'|d$ (or equivelently $N(d') \leq N(d)$)

(rephrased in terms of ideals) $(d) = (a,b)$

Irreducible: $r \in R$ (nonzero, nonunit) irreducible if it can't be factored into 2 non-units

Associate Elements: elements that differ multiplicatively by a unit

UFD: Every nonzero nonunit can be factored into finite irreducibles uniquely (up to associates)