Pt 3: Fields. Review of Core topics (Cont.)

Characteristic: 0 or a prime p, means F contains $\mathbb{Q}$ or $\mathbb{F}_p = \mathbb{Z}/p$.
ideals in fields are trivial or whole field $\Rightarrow$ homs are 0 or injective.
So we usually study field ext^{ns}.

Given $\overset{K}{|}_{F}$, i.e. $K \supseteq F$, K is an F-vector space. this dim^{n} is called the degree of K/F.

Key example: $p(x) \in F[x]$ irreducible $\rightsquigarrow K = F[x]/(p(x))$
($p(x)$ irred. $\Rightarrow$ prime $\Rightarrow$ max^{al} (PID) $\Rightarrow$ field quotient.)
If p has degree n, $[K:F] = n$, an F-basis of K is $\{1, \theta, \cdots, \theta^{n-1}\}$, $\theta := \overline{x}$.
Can do field arithmetic in K by polynomial division.
Further $K = F[x]/(p) \cong F(\alpha)$ for a root α of p.

Special ext^{ns}: Algebraic: all elts satisfy poly^{ls} over F.
If $\alpha \in L/K$ is alg., $\{p(x) \in K[x] \mid p(\alpha) = 0\} = (\min_K(\alpha))$ (ideal gen. by min. poly.)
If α is alg. of degree n, $K(\alpha)/K$ has degree n, basis $\{1, \alpha, \cdots \alpha^{n-1}\}$
If $\alpha \in L$, α alg/$K \Leftrightarrow [K(\alpha):K] < \infty$
Algebraic/algebraic = alg: L/F, F/K alg. $\Rightarrow L/K$ alg
Can take algebraic closures.

Towers: $\overset{L}{|}_{F}\ \overset{F}{|}_{K}$ $[L:K] = [L:F] \cdot [F:K]$ as a basis of L/K is $\{\alpha_i \beta_j\}$, $\{\alpha_i\}$ basis of L/F, $\{\beta_i\}$ basis of F/K.

Constructible: Ex: $\sqrt[3]{2}$ not constructible as $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, can't live in a power of 2-ext^{n} of $\mathbb{Q}$ by degree.

Splitting fields: splitting field of $g(x) \in F[x]$ is an ext^{n} L/F s.t. g factors into linear terms over L, but not over a proper subfield of L.

Fact: They exist and are unique up to isomorphism

Key: Extension of isomorphisms:

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\sim} & F(\Delta) \\ | & & | \\ F & \xrightarrow{\sim} & F' \end{array}$$

deg. of splitting field $\leq n!$.

Ex: • $x^n - 1 / \mathbb{Q}$ ⇝ Cyclotomic field $\mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$.

min poly $= \Phi_n(x) = \prod_{1 \leq a \leq n, (a,n)=1} (x - \zeta_n^a) \in \mathbb{Z}[x]$ & deg $= \varphi(n)$.

• finite fields: ∀ primes p, $n \in \mathbb{N}$, ∃! (up to ≅) field $\mathbb{F}_{p^n}$ of size p^n, the splitting field $/ \mathbb{F}_p$ of $x^{p^n} - x$. Frobenius map: $x \to x^p$. [Also $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ ⟺ $m | n$.] are simple.

Normal ext^n: Def^n 1: Every irred poly $/K$ splits $/L$.
L/K alg: Def^n 2: L is a splitting field of a family of polys$/K$.

Normal closure: throw in missing roots!

Ex: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not normal, adjoin $\zeta_3 = \omega$
⇝ $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal.

Separable: poly $/F$ sep. if all roots (over a splitting field) are simple!
test: $(f(x), f'(x)) = 1$.

perfect field: char$(F) = 0$ or char$(F) = p$, Frob$_p$ is surjective
⇒ irred. polys / perfect fields are sep.

if $f(x)$ is inseparable, irred., ∃! irred. sep. poly $f_{sep.} \in F[x]$; $k \geq 0$
$f(x) = f_{sep}(x^{p^k})$, p = char(F).

Sep. ext^n: all elts are roots of sep. polys / base (⟺ min polys of all elts are sep).

Fact: finite ext^{ns} of perfect fields are sep.

Pt. 4: Galois theory: field aut. of K fixing F: Aut(K/F).

Idea: Aut(K/F) permute roots of irred. polys.

For splitting fields $K = $ split$_F(f(x))$, $|\text{Aut}(K/F)| \leq [K:F]$,
$=$ if $f(x)$ is F-separable.

Def^n 1: K/F is finite. It's Galois if $|\text{Aut}(K/F)| = [K:F]$

Def^n 2: K/F is Galois if its normal + separable.

Ex: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not Galois as its missing aut: only 1 as gen. $\sqrt[3]{2}$ has to be sent to $\sqrt[3]{2}$

Ex: $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle Frob_p \rangle \cong \mathbb{Z}_n$ Explains simple structure of lattice of subfields.

Ex: $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$: Explicitly, given $a \in \mathbb{Z}_n^\times$, the Galois elt. maps $\zeta \mapsto \zeta^a$ another primitive n^{th} r.o.u.

Fundamental Th^m of Galois Theory K/F finite Galois, $G = Gal(K/F)$.

$\exists$ bijection

$\{ K \supseteq E \supseteq F \}$ $\leftrightarrow$ $\{ H \subseteq G \}$

n^{th} fields subgps of G.

$E \longmapsto \{$elts of G fixing $E\}$

K^H = fixed field of H $\longmapsto$ H

+ a ton number of properties.

- Be familiar with these! Review examples!

Further properties: • K/F Galois, $F \subseteq F' \Rightarrow KF'/F'$ Galois, (KF' composite.)
$Gal(KF'/F') \cong Gal(K/K \cap F')$.

• K_1, K_2 Galois/$F \Rightarrow K_1 \cap K_2$, $K_1 K_2$ Galois/F,
and $Gal(K_1K_2/F) \cong \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$
$\subseteq Gal(K_1/F) \times Gal(K_2/F)$

Cor: If K_1, K_2 Gal/F, $K_1 \cap K_2 = F$, $Gal(K_1K_2/F) \cong Gal(K_1/F) \times Gal(K_2/F)$.
$\rightsquigarrow$ Cor: Galois closures.

Primitive elt. Theorem: K/F simple $\Leftrightarrow$ $\exists$ finitely many intermediate fields

So K/F finite + separable $\Rightarrow$ K/F simple

Examples: Just take linear comb. of generators, "most" combs work.

Galois groups of polys: (splitting field of polys).

Gal(irred. poly of deg n / F) is a transitive subgp of S_n.

Discriminant: $D = \prod_{i<j} (x_i - x_j)^2$, $x_1, \dots, x_n$

$D \neq 0$ ((poly) = disc(roots)

$D = 0 \Leftrightarrow f$ is insep., over perfect fields $\Rightarrow f$ is reducible.

Fact: $Gal(f) \leq A_n \Leftrightarrow D$ is a square in F.

Small degree polys: Flowchart in book: know up to deg 4.

For deg. 4, use resolvent cubic, know formula for deg. 3 disc.

Over $\mathbb{Q}$: (also over field of fractions of a UFD...)

Pick any prime p not dividing disc(f). The degrees in factorization into irred. polys mod p gives the cycle type of an elt. in $Gal_{\mathbb{Q}}(f)$.

Guaranteed to find all elts' cycle types in $Gal_{\mathbb{Q}}(f)$ eventually. (enough primes chosen)

Tricks: One example (see notes):

Transitive subgps of S_n cont. a transposition & $(n-1)$ cycle are S_n.

Pt 5: Modules: Most recent, so quicker overview

Basis = free: not all modules are free

problem: torsion, and weirder stuff

Over commutative rings, $R^m \cong R^n \Rightarrow m = n$ ($\neq 0$) (idea: descend to vector spaces)

hom., isomorphism theorems, etc. Similar to ring theory

Cyclic module: $M = R \cdot a$, gen. by one elt.

Recognizing direct products $\mathbb{Z}/2\mathbb{Z}$ for gps.

Nicest case: R = PID $\Rightarrow$ R Noetherian (a.c.c.)
inc. Chain terminate

$\mathrm{Tor}(M) = \{x \in M \mid rx = 0 \text{ some } r \in R \setminus \{0\}\}$
torsion (annihilator) $\mathrm{Ann}(N) = \{r \in R \mid rn = 0 \ \forall n \in N\}$
$N \leq M$

module over a domain: rank = max $\#$ of R-lin. ind. elts.

Fund. Th^{m} of f.g. modules / PIDs:

$M \cong R^{\text{free rank}} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ (invariant factors)
free part; torsion part
$a_1 \mid a_2 \mid \cdots \mid a_m$ (non-zero, non-units); inv. factors.
$\mathrm{Ann}(\mathrm{Tor}(M)) = (a_m)$.

$M \cong R^{r} \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$ ($\alpha_i \geq 0$) (elementary divisors)
$p_1, \ldots, p_t$ primes in R.

Moreover, these are unique.

To convert: inv. factors $\longrightarrow$ factor as into prime powers $\longrightarrow$ elem. divisors
elem. divisors $\longrightarrow$ take away highest powers of each prime ("one at a time") $\longrightarrow$ inv. factors.

Cor: Fund. Th^{m} of f.g. abelian gps:
ab. groups are just $\mathbb{Z}$-modules!

15

RCF/JCF:

Given a vector space V/F a field,
$F[x]$-modules extending the v. space structure are just determined by linear transf. $T: V \to V$ by sending: $x \cdot v = T(v)$.
(and submodules are just T-~~invariant~~ stable vector subspaces)

RCF: Apply fund. theorem in invariant factor form

Basis of $F[x]/(a_i(x))$ (monic) $= \{1, x, \ldots, x^{k-1}\}$,

$\rightsquigarrow$ companion matrix $C_{a(x)} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 & \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{pmatrix}$

$RCF(A) = \begin{pmatrix} C_{a_1(x)} & & \\ & \ddots & \\ & & C_{a_m(x)} \end{pmatrix}$

This determines similarity types of matrices.

$\text{Char}(A)$ = prod. of inv. factors; $\min \text{poly} = a_m(x)$ (last inv. factor)

Cor: (Cayley-Hamilton)
$\text{char}(A)$, $\min(A)$ have same roots,
$\text{char}(A) \mid \min(A)^m$, $\min(A) \mid \text{char}(A)$
$\Rightarrow$ $\text{char}(A)$ applied to A gives 0.

Computing: Trick: small (2×2, 3×3 mat.): use char, min
Larger alg: Use row col. ops to diagonalize $(xI - A)$ (Smith normal form) to determine

JCF: Take a field where eigenvalues are contained. (ext^n)

Basis of $F[x]/(x-\lambda)^k$: $\{\overline{(x-\lambda)^{k-1}}, \ldots, \overline{1}\}$.

$\rightsquigarrow$ Jordan blocks: $\begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$

$TCF(A) = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{pmatrix}$

Closest you can get to diagonalizability:

A is diagonalizable $\Leftrightarrow$ all roots of $\min(A)$ are simple.
(over field cont. eigenvalues)

Computing JCF: Compute ~~elem~~ inv. factors first

Suggested problems?

1). Prove that if $K/\mathbb{Q}$ is a finite ext^n, there are only finitely many roots of unity in K.

2). Suppose $K = \mathbb{Q}(\vartheta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, $D_1, D_2 \in \mathbb{Z}$, $\vartheta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}$, $a, b, c, d \in \mathbb{Q}$.
Prove the min. poly for ϑ / $\mathbb{Q}$ is irred., of degree 4, but reducible mod every prime p. In particular, show that $x^4 - 10x^2 + 1$ is irred in $\mathbb{Q}[x]$ but is reducible mod every prime. [Hint: are there any biquadratic ext^{ns} / finite fields?]

7

3). Let α be a root in $\mathbb{C}$ of $f(x) := x^6 + 3$.

Let $K := \mathbb{Q}(\alpha)$.

a). Show K contains a primitive 6^{th} r.o.u.

b). Show $K/\mathbb{Q}$ is Galois.

c). Find, with proof, the number of intermediate fields $\mathbb{Q} \subseteq F \subseteq K$ with $[F:\mathbb{Q}] = 3$.

4). Let F be a field, $f(x) \in F[x]$ irreducible / F, K the splitting field of $f(x)$ over F.

Show that if $Gal(K/F)$ is abelian, then $K = F(\alpha)$, where α is a root of $f(x)$.

5). Use Rational Canonical Form to find representatives for all conjugacy classes in $GL_3(\mathbb{F}_2)$, the group of 3×3 invertible matrices over the field of 2 elements.

6). Let M be an R-module and N an R-submodule of M. Prove that M is Noetherian if and only if N and M/N are Noetherian.