Jumpstart

Jim Davis

Examples are the heart of mathematics. Abstract algebra can unify and conceptualize the examples.

1 Group Theory

Definition. A *group* $(G, \cdot)$ is a set G and a function $\cdot : G \times G \to G$ so that

i) $\forall x, y, z \in G, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ Associativity
ii) $\exists e \in G, \forall x \in G, e \cdot x = x = x \cdot e$ Identity
iii) $\forall x \in G, \exists y \in G, x \cdot y = e = y \cdot x$ Inverses
Remarks a) e is unique
b) $\forall x \in G, \exists! y \in G, x \cdot y = e$. Write $y = x^{-1}$.
c) cancellation $x \cdot y = x \cdot z \Rightarrow x = z$
d) notation: $x^3 = x \cdot x \cdot x$.

1.1 Examples

1. symmetric group S_n

   $S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ bijection } \}$
   $\cdot$ = composition $\circ$. Three sorts of notation for elements of symmetric group: function, cycle, matrix

2. permutation group $\mathrm{Aut}(X)$

   X set $\qquad \mathrm{Aut}(X) = \{$ bijections $\sigma : X \to X\}$
   e.g. $X = \{1, 2, \ldots, n\}$, then $\mathrm{Aut}(X) = S_n$.

3. dihedral group D_n = isometries of regular n-gon

   D_3 = e, two rotations, three reflections
   let g be rotation by $2\pi/n$; let T be reflection thru y-axis

$D_n = \{e, g, g^2, \ldots, g^{n-1}, T, gT, \ldots, g^{n-1}T\}$
Note $g^n = e$, $T^2 = e$ and $TgT^{-1} = g^{-1}$.

4. cyclic groups $\mathbb{Z}$ and $\mathbb{Z}/n$
5. $GL_n(F)$ for F a field. $F^\times = GL_1(F)$

1.2 Basic Definitions

Definitions:

- abelian group

  $x \cdot y = y \cdot x$.

- subgroup

  $H \subset G$ is *subgroup* if $H \cdot H \subset H$ and $(H, \cdot)$ is a group $\Leftrightarrow$ (i) $x, y \in H \Rightarrow x \cdot y \in H$, (ii) $h \in H \Rightarrow h^{-1} \in H$, (iii) H is nonempty.
  write $H < G$

- generators

  set $S \subset G$
  $\langle S \rangle$ = intersection of all subgroups containing S
  = minimal subgroup containing S.
  S generates G
  cyclic group
  $D_n = \langle g, T \rangle$.

- cyclic group
- order of group and element
- isomorphism, classify cyclic groups
- direct product ($\oplus$ for abelian groups)

  e.g $\mathbb{Q}^\times \cong$?

- finitely generated abelian groups
- groups of order 10 or less.

- normal subgroup $N \triangleleft G$
- conjugation, automorphism group
- homomorphism

  Lemma: kernel is normal

1.3 Group Actions

Definitions:

- A left action of a group G on a set X; written $G \curvearrowright X$

  Definiton, equivalently $G \to \mathrm{Aut}(X)$
  Examples S_n $GL_n(F)$ D_4 C_n, $\mathbb{Z}_2 \curvearrowright \{a, b, c\}$
  Cayley's theorem: G subgroup of permutation groups
  exercise define an isomorphism of G-sets.

- transitive action
- free
- effective

  $\forall g \neq e, \exists x \in X, gx \neq x \Leftrightarrow G \to \mathrm{Aut}(X)$ is a mono
- orbit Gx
- orbit decomposition of X

  do action of S_n on $\{1, 2, \ldots, n\}$ and get disjoint cycle notation., e.g (1 3 4)(5 2)
- isotropy subgroup (or stabilizer) G_x
- orbit space

  $G\backslash X$

$$X = \coprod_{[x] \in G\backslash X} Gx$$

1.3.1 Action of a Subgroup on a Group by Right Translation

- (left) cosets
- index
- Lagrange's theorem $|G| = |H||G : H|$.
- quotient groups $H \triangleleft G \Longrightarrow (gH)(g'H) = gg'H$
- exact sequence, short exact sequence, canonical example

$$1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$$

  exact is equivalent to α a mono, β epi, and $B/\alpha(A) \cong C$.

$$1 \to N \to G \to G/N \to 1$$

- first isomorphism theorem him $\phi : G \to H$ then $G/\ker\phi \xrightarrow{\cong} \phi(G)$.

1.3.2 Action of a Group on Itself by Conjugation

revisit orbits and orbit decomposition

$$X \cong \coprod_{[x] \in G\backslash X} G/G_x$$

Note $|G| = |Gx||G_x|$.

$G \curvearrowright G$ by conjugation
$(h, g) \mapsto hgh^{-1}$
orbits are *conjugacy classes*

$$(g) = \{hgh^{-1} \mid h \in G\}$$

isotropy group $G_g = \{h \mid hgh^{-1} = g\} = Z(g)$, the *centralizer* of g. Thus $|G| = |(g)||Z(g)|$.

- Conjugacy classes

$$G = \coprod (g) \cong \coprod_{(g)} G/Z(g)$$

- Class equation

  $|G| = \sum_{(g)} |(g)|$, noting that $|(g)||Z(g)| = |G|$.
  e.g. $|\mathbb{Z}/3| = 1 + 1 + 1$
  $|D_3| = 1 + 2 + 3$ (cor: no normal subgroups of order 2).
  Do some examples, e.g. S_5; conjugacy class are

  $(e), ((12)), ((12)(34)), ((123)), ((123)(45)), ((1234)), ((12345))$.

  Corollary Center of p-group is non-trivial Proof:

$$|G| = \sum_{(g)|g \in Z(G)} |(g)| + \sum_{(g)|g \notin Z(G)} |(g)| \equiv |Z(G)| \pmod{p}$$

  Corollary (Cauchy's Theorem) If $p \mid |G|$ then G has an element of order p.

2 Linear Algebra, Part 1

Definitions

- Ring $(R, + : R \times R \to R, \cdot : R \times R \to R)$
  satisfies (i) (R,+) abelian group,
  (ii) $(R, \cdot)$ associative
  (iii) distributive prop,
  (iv) multiplicative identity

  e.g. $R = \mathbb{Z}, \mathbb{Z}/n = \{0, 1, \cdots, n-1\}, \mathbb{Q}, \mathbb{R}$

  commutative ring

- new rings from old: ring R
  $M_n R$ $n \times n$ matrices
  $R[x]$ polynomials with coeff in R
  $R \times S$
  R/I where I is an two-sided ideal.

- unit group $R^\times = \{r \in R \mid \exists s, rs = 1 = sr\}$,
  e.g. $\mathbb{R}^\times$, $\mathbb{Z}^\times$, $(\mathbb{Z}/p)^\times$, $(M_n R)^\times$, $R[x]^\times$

- Field

  a commutative ring $(F, +, \times)$ so that $(F - 0, \times)$ is ab. group.
  e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \{0, 1, \ldots, p-1\}$
  note $ab = 0 \Rightarrow a = 0$ or $b = 0$. *no divisors of zero*
  Thus if $n1 = 1 + 1 + \cdots + 1 = 0$ then $p1 = 0$ for a unique prime divisor of n. Say Char $F = p$; otherwise Char $F = 0$.
  Char $F = p \Rightarrow \mathbb{F}_p \subset F$
  Char $F = 0 \Rightarrow \mathbb{Q} \subset F$
  F finite implies Char $F = p$. Converse?

- Algebraic Closure

  A field F is *algebraically closed* if every non-constant poly $f(x) \in F[x]$ has a root α ($\Leftrightarrow$ every $f(x)$ factors as a product of linear polys).
  e.g. $\mathbb{C}$, not $\mathbb{R}$ e.g. x^2+1, not $\mathbb{F}_2$ e.g. x^2+x+1, not $\mathbb{F}_p$ e.g. $x^{p-1}+x-1$.

  Fields $E \subset F$
  E is a subfield of F or
  F is an extension of E
  $\alpha \in F$ is *algebraic* over E if $\exists 0 \neq f(x) \in E[x]$ s.t. $f(\alpha) = 0$.
  e.g. $\pi \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$.
  $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$.
  Def: $F \subset \bar{F}$ is an *algebraic closure of F* if

  - $\bar{F}$ is algebraically closed
  - every element of $\bar{F}$ is algebraic over F

  Every field has an alg. closure, unique up to iso.
  $\bar{\mathbb{R}} = \mathbb{C}$
  $\bar{\mathbb{F}}_p = \cup \mathbb{F}_{p^n}$
  $\mathbb{Q} \subsetneq \overline{\mathbb{Q}} \subsetneq \mathbb{C}$
  $\overline{\mathbb{Q}}$ field of alg. numbers

- Module over a ring R is an abelian group M and $R \times M \to M$ which is associative, distributive, respects identity.

- Vector Space = module over a field

  e.g. F^n, $F[x]$, $\mathbb{R}$. $\mathbb{Q}[\sqrt{2}]$ are v.s. over $\mathbb{Q}$.

Dimension Theory
set $\mathcal{B} \subset V$

- Span

  $\mathcal{B}$ *spans* V if $\forall v \in V$,

  $$v = a_1 v_1 + \cdots + a_n v_n$$

  with $a_i \in F$ and $v_i \in \mathcal{B}$.

- Linear independence

  $\mathcal{B}$ is *linearly independent* if

  $$a_1 v_1 + \cdots + a_n v_n = 0 \Rightarrow \forall i, a_i = 0$$

- Basis

  $\mathcal{B}$ is a *basis* if it spans and is lin. ind.

Existence and Uniqueness Theorem:

1. Every v.s. has a basis
2. If $\mathcal{B}, \mathcal{B}'$ are bases, than $\exists$ bijection $\mathcal{B} \to \mathcal{B}'$.

A max'l lin. ind. set is a basis.
1. requires Zorn's Lemma
e.g. $\mathbb{R}$ has a basis over $\mathbb{Q}$
$\mathbb{Q}[x]$ has basis $\{1, x, x^2, \dots\}$
If $\#\mathcal{B} < \infty$, write $\dim V = \#\mathcal{B}$.
Cor of 2.: If V is f.d, then $V \cong F^n$.

2.1 Maps

- linear maps

  $T : V \to W$ is a *linear map* if

  1. $T(v + w) = T(v) + T(w)$
  2. $T(av) = aT(v)$

e.g. A is $m \times n$-matrix

$$F^n \to F^m$$
$$v \mapsto Av$$

Given finite bases $\mathcal{B}, \mathcal{B}'$ for V, W, there is a 1-1 correspondence

$$\text{linear maps } V \to W \leftrightarrow m \times n\text{-matrices}$$

Theorem: If $T : V \to W$, then $\dim V = \dim \ker T + \dim T(V)$ e.g. can't be an epi $\mathbb{R}^2 \to \mathbb{R}^3$.

- Endomorphisms

  Def: linear map $T : V \to V$ is an *endomorphism*. $\text{End}(V)$ forms a ring. If $V \cong F^n$ then $\text{End}(V) \cong M_n F$.

  ordered basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. If

  $$Tv_j = \sum a_{ij} v_i$$

  then let $A_{T,\mathcal{B}} = (a_{ij})$. Fact: If $\mathcal{B}'$ is different basis then $\exists C$ s.t.

  $$A_{T,\mathcal{B}'} = C A_{T,\mathcal{B}} C^{-1}$$

- Determinants
  $\det : \text{End}(V) \to F$
  $\det(AB) = \det A \det B$
  $\det A \neq 0 \Leftrightarrow$A invertible $\Leftrightarrow \ker A = 0$.

- Eigenvalues

  $Tv = \lambda v$ where $v \neq 0$. Then v is an *eigenvector* and λ is an *eigenvalue*.

  T is *diagonalizable* if V has a basis of evec's.

  $A_{T,\mathcal{B}}$ diagonal

  Fact: $A \in M_n F$ is diag . . . iff $\exists C$ s.t. CAC^{-1} is diagonal

- Characteristic poly

  $$\exists v \neq 0, Tv = \lambda v \Leftrightarrow \exists v \neq 0, 0 = \lambda v - Tv \Leftrightarrow \det(\lambda I - T) = 0$$

  Def: *Characteristic polynomial*

  $$p_T(x) = \det(xI - T) \in F[x]$$

  Roots are the evals of T.

- Lemma: If $v_1, \ldots v_k$ are evec's with distinct e'vals then $v_1, \ldots v_k$ are l. ind.
  Cor: If $p_T(x) = (x - \lambda_1) \cdots (x - \lambda_n)$ with $\lambda_i \neq \lambda_j$ for $i \neq j$, then T is diag . . .

- If A is upper triangular, $p_A(x) = ...$

- interesting examples

  - $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ diag . . .
  - $A = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ diag . . .
  - $A = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}$ diag . . .
  - $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ not diag . . .
  - $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ not diag . . . and nilpotent
  - $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ with $0 < \theta < \pi$ not diag . . . over $\mathbb{R}$, diag . . . over $\mathbb{C}$
  - $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ projection
  - $A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ projection $A^2 = A \Rightarrow V = \ker A \oplus \mathrm{im} A$
  - $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ order 4

– $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ order 3

fact: A matrix of finite order is diag . . . over $\overline{\mathbb{C}}$.

- Cayley-Hamilton Theorem $p_T(T) = 0$.
  e.g. $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $p_T(x) = x^2 + 1$, and $T \circ T + I = 0$
  e.g. $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $p_T(x) = x^2 + x + 1$, and $A^2 + A + I = 0$

3 Ring Theory

- Ring hom

  $f : R \to S$
  $f(r + r') = f(r) + f(r')$
  $f(rr') = f(r)f(r')$
  $f(1) = 1$
  $\forall$ rings R, $\exists! \mathbb{Z} \to R$

- Ideal

  I is a *ideal* in R if
  i) (I,+) is subgroup of $(R, +)$
  ii) $RIR \subset I$
  Notation $I \triangleleft R$

  $n\mathbb{Z} \triangleleft \mathbb{Z}$

  set $S \subset R$, $\langle S \rangle = \{r_1 s_1 t_1 + \cdots r_k s_k t_k \mid r_j, t_j \in R, s_j \in S\} \triangleleft R$ is *ideal generated by* S.
  If $|S| = 1$, then $I = \langle S \rangle$ is a *principal ideal*.

  $\langle x, y \rangle \subset \mathbb{R}[x, y]$ is not principal.

  R/I is a ring: $(r + I)(r' + I) = rr' + I$

  1st Isom theorem:If $f : R \to S$, then $\ker f$ is an ideal and $R/\ker f \to f(R)$ is a ring isomorphism.

- A simple ring has only the ideals 0 and R.

  $M_3(\mathbb{R})$ is a simple ring.

  $\begin{pmatrix} * & 0 & 0 \\ * & 0 & 0 \\ * & 0 & 0 \end{pmatrix}$ is a left ideal

Assume our rings are commutative

- integral domains

  Definition, cancellation, examples (e.g. subrings of fields)

- field of fractions

  $\mathrm{Frac}(R) = R \times (R - 0)/\sim$. $(a, b) \sim (c, d)$ iff $ad = bc$.

- prime and maximal ideals

  Let I be a proper ideal of R

  I is a prime ideal if $ab \in I \Rightarrow a \in I$ or $b \in I$.

  I is prime iff R/I is domain

  I is max'l iff R/I is field

  Cor: max'l $\Rightarrow$ prime

  Example: $\langle x \rangle \subset \mathbb{R}[x, y]$ is prime, not maximal.

- Chinese Remainder Theorem (CRT)

  Ideals $I, J \triangleleft R$ are *comaximal* if $R = I + J \Leftrightarrow \exists i \in I, j \in J, \boxed{1 = \mathrm{i} + \mathrm{j}}$.

  $23\mathbb{Z}$ and $45\mathbb{Z}$ are comaximal $1 = 2 \times 23 - 45$

  CRT: $R/I \cap J \xrightarrow{\sim} R/I \times R/J$
  Pf:

$$\begin{aligned} \varphi : R/I \cap J &\to R/I \times R/J \\ r + I \cap J &\mapsto (r + I, r + J) \end{aligned}$$

  has inverse $\psi(r + I, s + J) = rj + si + I \cap J$ $\boxed{\text{QED}}$

  Remark: $45\mathbb{Z} \cap 23\mathbb{Z} = 1035\mathbb{Z}$.

$\mathbb{Z}/1035 \cong \mathbb{Z}/45 \times \mathbb{Z}/23$

Corollary: $\exists n \in \mathbb{Z}$ so that $n \equiv 36 \pmod{45}$ and $n \equiv 4 \pmod{23}$.

CRT: If $I_1, I_2, \ldots, I_r \triangleleft R$, pairwise comaximal,

$$R/I_1 \cap \cdots \cap I_r \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_r$$

e.g. $n = p_1^{e_1} \ldots p_r^{e_r}$

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}$$

$$\mathrm{Aut}(\mathbb{Z}/n, +) = (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{e_1})^\times \cdots \times (\mathbb{Z}/p_r^{e_r})^\times$$

Fact: $(\mathbb{Z}/p^e)^\times$ is cyclic for p odd.

$(\mathbb{Z}/2^e)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{e-2}$ for $e > 2$.

3.1 Types of Domains

ED	$\Rightarrow PID$	$\Rightarrow UFD$
Euclidean Domain	Principal Ideal Domain	Unique Factorization Domain
$\mathbb{Z}, F[x]$	$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$	$\mathbb{Z}[x], \mathbb{R}[x, y]$

Note: $\mathbb{Z}[2i]$ is a domain, not a UFD - it is not integrally closed.

- Euclidean domain

$$\exists \sigma : R - 0 \to \mathbb{Z}_{\geq 0}$$

$$\forall a, b \in R, b \neq 0, \exists q, r \in R, a = bq + r, \& \ (r = 0 \text{ or } \sigma(r) < \sigma(b))$$

e.g $R = \mathbb{Z}$ and $\sigma(n) = |n|$
$R = F[x]$, F a field, and $\sigma(f(x)) = \deg f(x)$

- PID

  A domain where all ideals are principal.

Prop: ED $\Rightarrow$ PID.
Pf: $0 \neq I \triangleleft R$
Choose $b \in I$ s.t. $\sigma(b) = \min \sigma(I - 0)$
Then $Rb = I$
$\subset$: ✓
$\supset$: If $a \in I$, then $a = bq + r$ and ($r = 0$ or $\sigma(r) < \sigma(b)$).
But $r = a - bq \in I$, so $\sigma(r) \not< \sigma(b) \Rightarrow r = 0$.

Why study ED's?

- Our two examples are important
- $ED \Rightarrow PID$
- Can do long division
- Euclidean algorithm for computing gcd(a,b)
- Bezout's identity; gcd(a,b) = ra+ sb
- Algorithm for CRT

Why study PID's? There is a structure theorem for f.g. modules over PID's. Can deduce structure theorem for f.g. abelian groups $R = \mathbb{Z}$ or rational canonical form in linear algebra $R = F[x]$.

- UFD

Fundamental Theorem of Arithmetic
Every nonzero integer factors uniquely

$$n = \pm p_1^{e_1} \cdots p_r^{e_r}$$

with p_i distinct primes.

Have to be careful with uniqueness since $21 = (3)(7) = -1(3)(-7)$, etc.
Assume R is a domain.

a *divides* b if $b = ac$ some c.
write $a \mid b$

r is a *unit* if $r \in R^\times$.
r is *irreducible* if $r \neq 0$, r is not a unit, and ($r = ab \Rightarrow a$ or b is a unit).

e.g. $3x + 3y$ is irr in $\mathbb{Q}[x, y]$, not in $\mathbb{Z}[x, y]$.

r, s are *associates* if $\exists u \in R^\times, r = su$.

e.g 3 and -3.

Definition: R is a UFD if

1. Any $r \in R - (R^\times \cup 0)$ is a product of irreducibles

$$r = p_1 p_2 \dots p_n$$

2. The factorization is unique up to reordering and associates: if $r = q_1 q_2 \dots q_m$, then $n = m$ and there exists $\sigma \in S_n$ and $u_j \in R^\times$ so that $p_j = u_j q_{\sigma(j)}$.

- $PID \Rightarrow UFD$
  R UFD $\Rightarrow R[x]$ UFD

  e.g. $\mathbb{Z}[x]$ UFD, $\mathbb{Q}[x, y, z]$ UFD

- primes vs. irreducibles
  Def: $p \in R - (R^\times \cup 0)$ is *prime* if $\langle p \rangle$ is prime.
  $\Leftrightarrow (ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p)$
  $\Leftrightarrow (p|ab \Rightarrow p|a$ or $p|b)$

  Lemma: If R is a domain, prime $\Rightarrow$ irr.
  Pf: p prime. Suppose $p = ab$.
  Then $p|a$ or $p|b$, say $p|a$.
  Then $p = ab = pcb \Rightarrow 1 = cb \Rightarrow b \in R^\times$.

  In a UFD, irr. $\Rightarrow$ prime.

4 Linear Algebra, Part II

4.1 Minimal Polynomial

4.1.1 Examples

$$A = \begin{pmatrix} 0 & & \\ & 1 & \\ & & 2 \end{pmatrix} \qquad m_A(x) = p_A(x) = x(x-1)(x-2)$$

$$A = \begin{pmatrix} 2 & \\ & 2 \end{pmatrix} \qquad m_A(x) = x-2 \qquad p_A(x) = (x-2)^2$$

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \qquad m_A(x) = p_A(x) = (x-2)^2$$

$$A = \begin{pmatrix} 2 & 1 & \\ & 2 & \\ & & 2 \end{pmatrix} \qquad m_A(x) = (x-2)^2 \qquad p_A(x) = (x-2)^3$$

$$A = \begin{pmatrix} 2 & 1 & \\ & 2 & \\ & & 3 \end{pmatrix} \qquad m_A(x) = p_A(x) = (x-2)^2(x-3)$$

4.1.2 Minimal Polynomials and PID's

V f.d.v.s. / field F
$T : V \to V$ makes V an $F[x]$-module

$$F[x] \times V \to V$$
$$(f(x), v) \mapsto f(T)v$$

(Conversely: If V is an $F[x]$-module $(\cdot x : V \to V) \in End(V)$)

Lemma. *Let $A \in M_n F$. $\exists f(x) \neq 0$ s.t. $f(T) = 0$*

1st proof. $\dim_F M_n F = n^2$ so
$I, A, A^2, \ldots, A^{n^2}$ are dependent: $a_{n^2}A^{n^2} + \cdots + a_1 A + a_0 = 0$ □

2nd proof. Take $f(x) = p_A(x) = \det(xI - A)$ characteristic poly. □

Ideal: $\mathrm{Ann}(V,T) = \{f(x) \mid f(T) = 0\} \lhd F[x]$ PID
Any non-zero ideal in $F[x]$ has a unique *monic* generator
$x^k + a_{k-1}x^{k-1} + \cdots + a_0$.

Def: $m_T(x)$, the *minimal poly for* T is the unique monic generator for $\mathrm{Ann}(V,T)$.

Properties:

1. $m_T(T) = 0$
2. $f(T) = 0 \iff m_T \mid f$
3. $m_T \mid p_T, \qquad \deg m_T \leq \dim V$
4. $$\{ \text{ roots of } m_T(x)\} = \{ \text{ roots of } p_T(x)\}$$

   Pr of 5.: $\subset$: $m_T \mid p_T$
   $\supset$:

   $$\begin{aligned} p(\lambda) = 0 &\Rightarrow Tv = \lambda v \text{ some } v \neq 0 \\ &\Rightarrow m(T)v = m(\lambda)v \\ &\Rightarrow 0 = m(\lambda)v \\ &\Rightarrow 0 = m(\lambda) \end{aligned}$$

   e.g.

   $$p(x) = (x-1)^2(x-2)$$

   $$m(x) = \begin{cases} (x-1)(x-2) & \begin{pmatrix} 1 & & \\ & 1 & \\ & & 2 \end{pmatrix} \\ \text{or} & \\ (x-1)^2(x-2) & \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 2 \end{pmatrix} \end{cases}$$

5. Can show $\{$ irr factors of $m_T(x)\} = \{$ irr factors of $p_T(x)\}$ by using $F \subset \overline{F}$.

6. Recall the eq. rel. on M_nF

$$A \sim B \iff B = CAC^{-1}, \text{ some } C$$

A is *similar* to B. Note

$$\begin{aligned}(CAC^{-1})^n &= CAC^{-1}\ CAC^{-1} \cdots CAC^{-1} \\ &= CA^nC^{-1}\end{aligned}$$

$\boxed{A \sim B \Rightarrow m_A(x) = m_B(x)}$

4.2 Jordan Canonical Form

- an example

$$A = \begin{pmatrix} 3 & 1 & & & & & \\ & 3 & 1 & & & & \\ & & 3 & & & & \\ & & & 0 & & & \\ & & & & 0 & & \\ & & & & & 0 & 1 \\ & & & & & & 0 \end{pmatrix} \qquad p(x) = (x-3)^3x^4 \qquad m(x) = ?$$

- statement

  A $k \times k$ *Jordan block*

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

  A matrix is in *Jordan Canonical Form* (JCF) if

$$A = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_l \end{pmatrix}$$

  where B_i is a Jordan block.

Theorem. *If F is alg. closed, then any matrix is similar to a matrix in JCF, unique up to reordering of the blocks.*

- poly $f(x)$, then
$$f(A) = \begin{pmatrix} f(B_1) & & \\ & \ddots & \\ & & f(B_l) \end{pmatrix}$$
Thus $m_A(x) = lcm(m_{B_1}(x), \ldots, m_{B_l}(x))$ and $p_A(x) = \prod p_{B_i}(x)$
- e.g. minimal poly of $\begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{pmatrix}$ is x^4
-
Lemma. *The minimal poly of a $k \times k$* Jordan block $A = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$
is $\boxed{m_A(x) = (x-\lambda)^k}$

Proof. It suffices to show $(A-\lambda I)^k = 0$ but $(A-\lambda I)^{k-1} \neq 0$. In general
$(A-\lambda I)e_1 = 0, (A-\lambda I)e_2 = e_1, \ldots, (A-\lambda I)e_k = e_{k-1}$
$(A-\lambda I)^{k-1}e_k = e_1$, but
$(A-\lambda I)^k e_i = 0$ for all i. □

Now go back and do the minimal and char poly for "an example"

- Applications
  - Cayley-Hamilton Theorem: $p_A(A) = 0$.

    Pf: Replace F by $\overline{F}$ and A by its JCF: $A = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_m \end{pmatrix}$
$$m_A(x) \mid \prod m_{B_i}(x) = \prod p_{B_i}(x) = p_A(x)$$

– If F is algebraically closed,

$$\prod \lambda_i = \det A$$
$$\sum \lambda_i = \operatorname{Tr} A$$

(Here $\operatorname{Tr} A = \sum a_{ii}$)

Proof. $A \sim B = \begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}$ □

Remark. Suppose $p_A(x) = (x-\lambda_1)\cdots(x-\lambda_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then

$$(-1)^n a_0 = \prod \lambda_i$$
$$-a_{n-1} = \sum \lambda_i$$

– A tier problem
Suppose $A_1, A_2 \in M_3\mathbb{C}$ and $\deg m_{A_i}(x) \leq 2$. Show they have a common evec.

- Generalized Eigenspaces

λ is eval for T

Eigenspace $E_\lambda(T) = \ker(\lambda I - T)$

Generalized Eigenspaces

$$E_\lambda(T) \subset GE_\lambda(T) := \bigcup_k \ker(\lambda I - T)^k$$

Thm: If $p_T(x) = (x-\lambda_1)\cdots(x-\lambda_n)$, then

$$V = \bigoplus_\lambda GE_\lambda(T)$$

Do "an example"

- toward an algorithm

  Remark: The evals $\{\lambda_i\}$ and the numbers $\dim\ker(A-\lambda_i I)^j$ for $j = 1, 2, 3, \ldots$ determine the JCF.

  Make a table for "an example" and work out JCF for $\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

- toward a proof

  In fact, we give a full proof assuming the structure theorem for finitely generated modules over PID's.

  Thm: Let M be a f.g. module over a PID R. Then

  $$M \cong R^k \oplus R/\langle p_1^{e_1}\rangle \oplus \cdots \oplus R/\langle p_l^{e_l}\rangle$$

  where p_i are primes in R. Furthermore, this decomposition is unique up to reordering.

  When $R = \mathbb{Z}$ this gives a version of the structure theorem for f.g. abelian groups.
  When $k = 0$ we say M is a *torsion* module: $\forall m \in M, \exists r \in R - 0, rm = 0$.

  Now let $T : V \to V$ be an endomorphism (with $\dim_F V < \infty$). Then
  V is an $F[x]$-module $f(x)v := f(T)v$
  V is torsion by the CH Thm.
  $F[x]$ is a PID since it is a ED. Thus

  $$V \cong F[x]/\langle p_1(x)^{e_1}\rangle \oplus \cdots \oplus F[x]/\langle p_l(x)^{e_l}\rangle$$

  Now assume $p_T(x)$ factors as a product of linear factors, e.g. F is alg. closed.

  $$V \cong F[x]/\langle (x-\lambda_1)^{e_1}\rangle \oplus \cdots \oplus F[x]/\langle (x-\lambda_l)^{e_l}\rangle$$

  Finally note that if

  $$V = \frac{F[x]}{(\langle x-\lambda)^k\rangle}$$

  and $T = \cdot x : V \to V$, then have a basis

  $$\left\{[(x-\lambda)^{k-1}], [(x-\lambda)^{k-2}], \ldots, [(x-\lambda)^0]\right\}$$

with matrix a Jordon Block

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

5 Number Theory

Example.

$$F = \frac{\mathbb{F}_2[x]}{\langle x^2 + x + 1 \rangle}$$

The polynomial is irr since it has no roots. Let $\varepsilon = [x] = x + \langle x^2 + x + 1 \rangle$. Then $\varepsilon^2 + \varepsilon + 1 = 0$.
F is a $\mathbb{F}_2$-vector space with basis $\{1, \varepsilon\}$. Hence F is a field with 4 elements.

$+$	0	1	ε	$1+\varepsilon$
0	0	1	ε	$1+\varepsilon$
1		0	$1+\varepsilon$	ε
ε			0	1
$1+\varepsilon$				0

$\times$	0	1	ε	$1+\varepsilon$
0	0	0	0	0
1		1	ε	$1+\varepsilon$
ε			$1+\varepsilon$	1
$1+\varepsilon$				ε

- $F[\alpha]$ versus $F(\alpha)$
  - Rings $R \subset S$, $\quad \alpha \in S$. Define $R \subset R[\alpha] \subset S$.

    $R[\alpha]$ = smallest subring of S containing α and R
    $= \{a_n\alpha^n + \cdots + a_1\alpha + a_0 \mid a_i \in R\}$

e.g. $\mathbb{Z} \subset \mathbb{C} \ni \sqrt{2}$

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

field $F \subset S$ ring
degree $|S : F| = \dim_F S$
$|\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| = 2$.

– Fields $F \subset K$, $\quad \alpha \in K$. Define $F \subset F(\alpha) \subset K$.

$F(\alpha)$ = smallest subfield of K containing α and F
$F[\alpha] \subset F(\alpha)$

Definition. α is *algebraic/F* if $\exists f(x) \in F[x] - 0$, $f(\alpha) = 0$.

Theorem. *$F[\alpha]$ is a field $\iff$ α alg. /K.*

Proof. $\Longrightarrow$: $\alpha^{-1} \in F[\alpha]$
$\Rightarrow 1/\alpha = g(\alpha)$
$\Rightarrow 0 = \alpha g(\alpha) - 1$

$\Longleftarrow$: $f(\alpha) = 0 \Rightarrow a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$

Claim. $F[\alpha] = F\alpha^{n-1} + \cdots + F1$

Proof.

$$(*) \qquad \alpha^n = -\frac{a_{n-1}}{a_n}\alpha^{n-1} - \cdots - \frac{a_0}{a_n}$$
$$\alpha^{n+1} = -\frac{a_{n-1}}{a_n}\alpha^n - \cdots - \frac{a_0}{a_n}\alpha$$

Now plug in $(*)$ and continue inductively $\square$

Thus $|F[\alpha] : F| \leq n < \infty$
Let $k \in F[\alpha] - 0$. Then

$$\cdot k : F[\alpha] \to F[\alpha]$$

is injective (since $F[\alpha] \subset K$ is a domain) hence surjective (since $F[\alpha]$ is f.dim'l). Thus $1/k \in F[\alpha]$. Thus $F[\alpha]$ is a field. $\square$

Cor: α alg/$F \Leftrightarrow F[\alpha] = F(\alpha)$

Def: α *transcendental* over F if α is not alg. $\Leftrightarrow F[\alpha] \cong F[x]$
eg $F = \mathbb{Q}, \qquad \alpha = \pi.$

- alg. numbers $\rightleftarrows$ polynomials
  - alg. numbers $\to$ polynomials
    $F \subset K \ni \alpha$
    Def: *minimal poly* $m_\alpha(x) \in F[x]$ is the irr, monic poly with α as a root.
    e.g. $\alpha = \sqrt{2} \qquad m(x) = x^2 - 2.$
    1. $f(x) \in F[x], f(\alpha) = 0 \Rightarrow m_\alpha \mid f$
    2. $m_\alpha(x) = m_T(x), \qquad T = \cdot\,\alpha : F[\alpha] \to F[\alpha]$
    3. $F[x]/\langle m_\alpha(x)\rangle \xrightarrow{\cong} F[\alpha]$

    e.g. (w/o proof) $m_{\sqrt[3]{2}}(x) = x^3 - 2$ (use Gauss' Lemma or Eisenstein criterion to prove irr)
    $\alpha = \sqrt{2} + \sqrt{3}$

    $$m_\alpha(x) =$$
    $$\Big(x - (\sqrt{2} + \sqrt{3})\Big)\Big(x - (-\sqrt{2} + \sqrt{3})\Big)\Big(x - (\sqrt{2} - \sqrt{3})\Big)\Big(x - (-\sqrt{2} - \sqrt{3})\Big)$$
    $$= x^4 - 10x + 1$$

    "conjugates"

    $$x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$$

    where $\zeta_3 = \exp 2\pi/3 \qquad \zeta_3^3 = 1$

    Theorem. *1. For fields $F \subset K \subset L$, $\quad |L : F| = |L : K||K : F|$*
    2. α, β alg over $F \Rightarrow \alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$ alg over F.

    Proof. 1.$L - K - F$
    $\{\alpha_i\}$ basis $L/K, \{\beta_j\}$ basis $K/F \Rightarrow \{\alpha_i\beta_j\}$ basis L/F.
    2. $K(\alpha)/K$ is finite since α is alg.
    β alg/ $K \Rightarrow \beta$ alg over $K(\alpha) \Rightarrow K(\alpha, \beta)/K(\alpha)$ finite. Thus $K(\alpha, \beta)/K$ is finite, hence alg. $\square$

Corollary. *Let $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ be the set of complex numbers alg over $\mathbb{Q}$. Then $\overline{\mathbb{Q}}$ is a field.*

e.g. $\sqrt{2} + \zeta_{29} \in \overline{\mathbb{Q}}, e^{\pi} \notin \overline{\mathbb{Q}}$.

– polynomials $\to$ alg numbers
irr monic $f(x) \in F[x]$

1. $\exists \alpha, K, s.t.\ \alpha \in K \supset F$, $K = F(\alpha) = F[\alpha]$, α a root of $f(x)$
2. Any two such K are isomorphic
3. $|K : F| = \deg f(x)$
4. $\exists!$ minimal field L, $F \subset L \subset \overline{F}$ s.t.

$$f(x) = \prod (x - \lambda_i), \lambda_i \in L$$

L is the *splitting field of* $f(x)$. $|L : F| \geq \deg n$

Proof. 1. $K = F[x]/\langle f(x) \rangle \qquad \alpha = [x]$.
2. The map $F[x]/\langle f(x) \rangle \xrightarrow{\cong} K$
3. $F[x]/\langle f(x)$ has basis $\{1, [x], [x^2], \ldots, [x^{n-1}]\}$
4. $L = F[\lambda_1, \ldots, \lambda_n]$. □

eg $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ splitting field $|\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| = 2$.
eg $f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3 \sqrt[3]{2})(x - \zeta_3^2 \sqrt[3]{2})$
$\mathbb{Q} \subsetneq K = \mathbb{Q}[\sqrt[3]{2}] \subsetneq L$ and $|L : \mathbb{Q}| = 6$.

5.0.1 Finite Fields

$\mathbb{Z}/n$ field $\iff n$ prime
Let F be a finite field.
$\exists! \phi : \mathbb{Z} \to F$
Let $n\mathbb{Z} = \ker \phi$
$\mathbb{Z}/n\mathbb{Z} \hookrightarrow F$
$\Rightarrow \mathbb{Z}/n\mathbb{Z}$ domain
$\Rightarrow n = p$ prime.
Consequences

- $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p \hookrightarrow F$
- $|F : \mathbb{F}_p| = r \Rightarrow F \cong (\mathbb{F}_p)^r$ (as an $\mathbb{F}_p$-v.s.). Thus $|F| = p^r$.

- $p1 = 0 \Rightarrow pa = p1a = 0$. Thus $pF = 0$.

Fact: A finite ring w/o zero divisors is a field:

Theorem. *Let $q = p^r$ with p prime. Let F be a field of order q.*

1. *$F^\times$ is cyclic (order $q-1$).*
2. *$x^q - x = \prod_{\alpha \in F}(x - \alpha)$. Thus the elements of F are the roots of $x^q - x$.*
3. *Any two fields of order q are iso. Write $\mathbb{F}_q$.*
4. *$\exists$ field of order q.*
5. *$\mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^r}$ if and only if $k \mid r$.*

Proof. 1. $F^\times$ is a group of order $q-1$. Thus $\alpha \in F^\times \Rightarrow \alpha^{q-1} = 1$. Hence $\forall \alpha \in F, \quad \alpha^q - \alpha = 0$. Thus

$$\prod_{\alpha \in F}(x - \alpha) \mid x^q - x$$

Since the degrees are equal, $\prod_{\alpha \in F}(x - \alpha) = x^q - x$.
2. $F^\times$ is abelian group, order $q-1$.

$$n = \exp F^\times := \max_{\alpha \in F^\times}\{\text{order } \alpha\} \mid q - 1$$

Thus there are $q-1$ roots of $x^n - 1 \Rightarrow n \geq q - 1$.
$\therefore n = q - 1$, i.e. $F^\times$ is cyclic.
3. Let F, K be two fields of order q. Let $\alpha \in F^\times$ be a generator. Then α is a root of $f(x) = x^q - x$. Let $m(x)$ be an irreducible factor of $f(x)$ which has α as a root. Then $F = \mathbb{F}_p[\alpha] \cong \mathbb{F}_p[x]/\langle m(x)\rangle$. By 1., there is a root $\beta \in K$ of $m(x)$. Thus $\mathbb{F}_p[x]/\langle m(x)\rangle$ is isomorphic to the subfield $\mathbb{F}_p[\beta]$ of K and by counting orders, the subfield can't be proper.
4. Let $L/\mathbb{F}_p$ be a splitting field of $f(x) = x^q - x$. Let $F \subset L$ be the *set* of roots of $f(x)$. Note that F has order q since f has no multiple roots since the gcd $(f, f') = (x^q - x, -1) = 1$.
Claim: F is a field: $\alpha, \beta \in F \Rightarrow -\alpha, \alpha^{-1}, \alpha\beta, \alpha + \beta \in F$.

Proof of Claim. All assertions are clear except for $\alpha + \beta$. One proves that $(\alpha + \beta)^{p^r} = \alpha^{p^r} + \beta^{p^r}$ by induction on r. □

5. $\Rightarrow$: $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^r}$. Let $l = |\mathbb{F}_{p^r} : \mathbb{F}_{p^k}|$. Then $(p^k)^l = p^r$ so $kl = r$.
$\Leftarrow$: Suppose $kl = r$. Then

$$\begin{aligned} p^k - 1 \mid p^{kl} - 1 &\Rightarrow x^{p^k-1} - 1 \mid x^{p^{kl}-1} - 1 \\ &\Rightarrow x^{p^k} - x \mid x^{p^{kl}} - x \end{aligned}$$

Thus $\mathbb{F}_{p^r}$ contains all the roots of $x^{p^k} - x$, and this set of roots is a field of order p^k.

Example. Lattice of fields $\mathbb{F}_{2^k}$ for $k \leq 6$.

□