Groups

- **def**: Φ is an isomorphism if it is a homo. and $\exists \psi : G' \to G$ s.t. $\phi \circ \psi = id_{G'}$, $\psi \circ \phi = id_G$
  - ↳ bijective homomorphism (lemma)
- **def**: $H \leq G$, left cosets are gH ($g_1 \sim g_2$ iff $g_1^{-1} g_2 \in H$)
- **lemma**: all left cosets have the same cardinality

  PF: bijection $H \to gH$ by $h \mapsto gh$. obv surjective (gH is by def. the elts of the form gh), and $gh = gh' \Rightarrow h = h'$ so injective $\square$
- **Cor**: $|G| = |H| \cdot |G/H|$
- **Lagrange's thm**: $H \leq G$ then $|H| \mid |G|$
- **Fermat's little thm**: p prime, $(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod p$

  PF: $G = (\mathbb{Z}_p^*, \cdot)$ is a group, if $a \in G$, then $a^{|G|} = (a^{|a|})^{|G|/|a|} = 1$, $|G| = p-1$ $\square$
- **def**: $H \leq G$ normal iff $g^{-1} H g = H$ $\forall g \in G$ ($H \trianglelefteq G$)
  - ▷ G is extension of G/H by H
- **lemma**: If $\Phi : G \to G$ is a homomorphism then $\ker \phi \trianglelefteq G$
- **thm** (first isomorphism): $G / \ker \phi \simeq im(\phi)$

$$\begin{tikzcd} G \arrow[r, "\Phi"] \arrow[d] & im(\phi) \\ G/\ker\phi \arrow[ur, "\sim"'] & \end{tikzcd}$$

- **thm**: $H \leq G$, then $H \trianglelefteq G$ iff $\exists$ homo $\phi : G \to G'$ for some group G' with $\ker \phi = H$

  pf: ($\Leftarrow$): lemma ($\Rightarrow$): If $H \trianglelefteq G$, define $\Phi : G \to G/H$ by $g \mapsto gH$, homomorphism with $\ker \phi = H$ ($G' := G/H$)
- **lemm**: $H \trianglelefteq G \Leftrightarrow gH = Hg$ $\forall g \in G$
- **def**: index of H in G is $[G:H]$ # of left or right cosets ($= |G/H|$ if normal)
- **def**: G group, $S \subseteq G$ (subset) $\langle S \rangle :=$ smallest subgroup containing $S = \bigcap_{S \subseteq H \leq G} H$ ($\leq G$)
- **lemma**: $|G|$ prime $\Rightarrow$ G cyclic

  Pf: take $g \in G$, $g \neq e$, $|g| \mid |G|$ so $|g| = 1$ or $|G|$ but $g \neq e$ so $G = \langle g \rangle$. $\square$
- **lemma**: any cyclic group is $\simeq$ to $\mathbb{Z}$ or $(\mathbb{Z}_n, +)$ for $n \in \mathbb{Z}$. (Pf: $G = \langle g \rangle$, $g \mapsto 1$)
- **thm**: subgroup or quotient of cyclic groups is cyclic
- **def**: G group, X set, an action of G on X is a function $G \times X \to X$ $(g,x) \mapsto g \cdot x$ s.t.

  1) $e \cdot x = x$ $\forall x$ 2) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
  - ▷ G acts on itself by left multiplication
  - ▷ G acts on itself by left conjugation ($g \cdot x = g x g^{-1}$)

- group actions of G on X is equivalent to some homomorphism $G \to \mathrm{Sym}(X)$, called <u>permutation representation</u>
- <u>def</u>: for $x \in X$, $G_x := \{g \in G \mid g \cdot x = x\} = \mathrm{Stab}(x)$
  - <u>Lemma</u>: $G_x \leq G$
- <u>def</u>: for $x \in X$, $G \cdot x := \{g \cdot x \mid g \in G\} = \mathrm{Orb}(x) \subseteq X$
- <u>Orbit-Stabilizer thm</u>: If G acts on X then $\forall x \in X$, $|G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$.

<u>Pf</u>: define $\Phi : G/G_x \to G \cdot x$ by $g \cdot G_x \mapsto g \cdot x$
[it's well def & bijection, $|G/G_x| = |G \cdot x| \Rightarrow |G| = |G_x| \cdot |G \cdot x|$.] $\square$

- <u>Cauchy's thm</u>: $|G| < \infty$ and $p \mid |G|$ then $\exists g \in G$ s.t. $|g| = p$
- <u>Lemma</u>: p prime, G a <u>p-group</u> ($|G| = p^k$ for some $k \geq 1$). G acts on finite X. Let $F = \{x \in X \mid g \cdot x = x \ \forall g \in G\} = \{\text{fixed pts of action}\}$. Then $|F| \equiv |X| \pmod p$

<u>Pf</u>: Let $G \cdot x_1, \dots, G \cdot x_d$ be the diff orbits so that X is a disj union of these orbits, so $|X| = \sum_{i=1}^{d} |G \cdot x_i|$, but $|G \cdot x_i| = 1 \Leftrightarrow x_i \in F$ and so $|X| = |F| + (\text{sum of all } |G \cdot x_i| \text{ nontrivial})$, but the second term is a multiple of p by Orbit-Stab thm since $|G| = p^k$, so $|X| \equiv |F| \bmod p$. $\square$

<u>Pf</u>: Let $X = \{(x_1, \dots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = e\}$, $\mathbb{Z}_p$ acts on X by cyclic right shift: $1 \cdot (x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1})$.
$F = \{(x, \dots, x) \mid x \in G, x^p = e\}$ (fixed pts are those w/ all same entries i.e. elts with order dividing p.), so goal is to show $|F| > 1$ ($(e, e, \dots, e) \in F$)
But $|X| = |G|^{p-1}$ - we can choose $p-1$ elts freely but the final coord is determined by the restriction. $p \mid |G|$, so $p \mid |X|$ hence $p \mid |F|$ by Lemma. $\square$

- <u>Cor</u>: If $p \mid |G|$ then G has a subgroup of order p.
- <u>Lemma</u>: $H \leq G$. Then $H \trianglelefteq G$ iff natural action of H on G/H is trivial.
  - ↳ natural action: G acts on G/H by $g \cdot (g_1 H) = (g g_1) H$, restrict G to H.
  - ↳ trivial action: $g \cdot x = x \ \forall g, x$.

<u>Pf</u>: $h \cdot (gH) = gH \ \forall g, h \Leftrightarrow g^{-1} h g H = H \Leftrightarrow g^{-1} h g \in H \Leftrightarrow H \trianglelefteq G$ $\square$

- <u>thm</u>: G finite, p prime smallest dividing $|G|$. Then any subgroup index p is normal

<u>Pf</u>: $H \leq G$, $[G : H] = p$ as in thm. Consider H acting on G/H.
$\mathrm{Orb}_H(eH) = H \cdot (eH) = eH$, so any other orbit $\mathrm{Orb}_H(gH)$ has size at most $p-1$ (there are p many cosets, one is used in trivial, G/H is disj union of orbits)

★ p smallest prime
↓ dividing |G|.

every orbit size divides |G| so is either size 1 or ≥ p. second not possible by before, so every orbit has size 1 ⇒ trivial action □

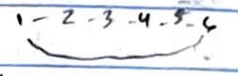
— Polya's Counting Method —

- lemma: (Burnside): G finite acting on finite X. for $g \in G$, $Fix(g)$ = # of fixed pts $:= |\{x \in X : g \cdot x = x\}|$. Then #orbits $= \frac{1}{|G|}\sum_{g\in G} Fix(g)$

Pf: $\frac{1}{|G|}\sum_{g\in G} Fix(g) = \frac{1}{|G|}\sum_{g\in G}\sum_{\substack{x\in X\\ g\cdot x = x}} 1 = \frac{1}{|G|}\sum_{x\in X}\sum_{\substack{g\in G\\ g\cdot x = x}} 1 = \frac{1}{|G|}\sum_{x\in X}|G_x| = \frac{1}{|G|}\sum_{\text{orbits}}\sum_{x\in\sigma}|G_x|$
$= \frac{1}{|G|}\sum_{\sigma \text{ orbits}}\sum_{x\in\sigma}\frac{|G|}{|G\cdot x|} = \sum_{\sigma\text{ orbit}}\sum_{x\in\sigma}\frac{1}{|\sigma|} = \sum_{\sigma \text{ orbit}} 1 =$ # orbits □

- ex: How many different circular necklaces can be made with 6 beads, each one of 4 colors?
↳ rotations and flips are same necklace

Ans: X = set of 4 colored labelled hexagons, $|X| = 4^6$



D_{12} acts on X - want to count # of orbits (things in same orbit are the same necklace)

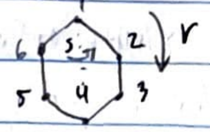
Let X^* = set of uncolored labelled hexagons, D_{12} acts on X^* also

let g^* be the permutation of [6] induced by $g \in D_{12}$

r rotation : $r^* = (1\,2\,3\,4\,5\,6)$ 6-cycle

s flip : $s^* = (2\,6)(3\,5)(1)(4)$ $1^2 \cdot 2^2$-cycle

e : $e^* = (1)(2)\ldots(6)$ 1^6-cycle



elt	cycle type	# cycles	# k-colorings fixed by elt
1	1^6	6	K^6
r^5, r	6^1	1	K^1
r^4, r^2	3^2	2	K^2
r^3	2^3	3	K^3
s	$1^2 \cdot 2^2$	4	K^4
sr^5, sr	2^3	3	K^3
sr^4, sr^2	$1^2 \cdot 2^2$	4	K^4
sr^3	2^3	3	K^3

★ coloring is fixed by elt in D_{12} iff within each cycle, all colors are same for label

k-colorings $= \frac{1}{12}(K^6 + 2k + 2k^2 + k^3 + + k^3$
$= \frac{1}{12}(K^6 + 3k^4 + 4k^3 + 2k^2 + 2k)$
↑ plug in k = 4 for original (430)

□

- ex: how many diff ways are there to k-color faces of cube?
group of sym of cube is ≅ S_4 ! (4 pairs of opposite vertices)

– Groups acting on themselves by conjugation –

- G group, $X = G$, $g, h \in G$: $g \cdot h = ghg^{-1}$
- orbit of elt h = conjugacy class $= Cl_G(h) = \{ghg^{-1} : g \in G\}$
- stabilizer of h = centralizer of $h = C_G(h) = \{g : gh = hg\}$
- kernel of action $= \{g \in G : g \cdot h = h \ \forall h\} = \{g \in G : gh = hg \ \forall h\} = Z(G)$ = centr
- e.g. ① $\sigma \in S_n$: $Cl_{S_n}(\sigma) = \{$perm. w/ same cycle type$\}$

  b/c $\sigma, \tau \in S_n$, $\sigma = (a_1 a_2 \ldots)(b_1 b_2)\ldots$, then $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2) \ldots)(\tau(b_1) \ldots) \ldots$

  # of conjugacy classes of S_n = # partitions of n
- Lemma: $H \trianglelefteq G$ iff H can be written as a union of conjugacy classes
- $G = \bigcup(\text{conjugacy class}) = Z(G) \cup (\bigcup \text{nontrivial conjugacy classes})$

  let $y_1, \ldots, y_r$ be reps for conjugacy classes

  $x_1, \ldots, x_s$ be reps for nontrivial conjugacy class

  $|G| = \sum_{i=1}^{r} |Cl(y_i)| = \sum_{i=1}^{s} |Cl(x_i)| + |Z(G)|$

  $\boxed{|G| = |Z(G)| + \sum_{i=1}^{s} [G : C_G(x_i)]}$ ← orbit stabilizer

  ★ class equation ↳ over nontrivial conjugacy classes
- Thm: If G is a p-group then $|Z(G)| > 1$

  Pf: $|G| = p^k$ $(k \geq 1)$ and $p \mid [G : C_G(x_i)]$ (because $[G : C_G(x_i)] > 1$)

  nontrivial ↓

  so by class eq, $p \mid |Z(G)|$ □
- Cor. If $|G| = p^2$ then G abelian (p prime)

  Pf: $Z(G) \neq 1 \Rightarrow G/Z(G)$ has order p or 1, so $G/Z(G)$ is cyclic $\Rightarrow G$ abl. □

– Conjugate Subgroups –

- G acting on $X = \{H \leq G\}$ by $g \cdot H \mapsto gHg^{-1}$ → always a subgroup
- orbit of H = set of conjugates of H
- stabilizer of H = normalizer of $H = N_G(H)$
  - ▷ $N_G(H) = G$ iff $H \trianglelefteq G$
  - ▷ Lemma: $N_G(H)$ is the largest subgroup H' of G containing H s.t. $H \trianglelefteq H'$
  - * $N_G(H)$ is not necessarily normal in G.
  - ↳ $H \trianglelefteq H' \Rightarrow H' \leq N_G(H)$ (show that)

– Sylow Theorems –

- **def**: G group, a <u>p-Sylow subgp</u> of G (p prime) is a subgroup of order p^k where $|G| = p^k \cdot m$ ($p \nmid m$) aka k is maximal
- **thm 1**: If p divides $|G|$, $\exists$ at least 1 p-Sylow subgroup
- **thm 2**: For fixed prime p, all p-Sylow subgps are conjugate to each other
- **thm 3**: Let n_p be the # of p-Sylow subgroups. Then $n_p \mid |G|$ and $n_p \equiv 1 \pmod p$

Pf (1): Induction on $|G|$. $|G| = 1$ ✓

Suppose $\exists H \lneq G$ w/ $p \nmid [G:H]$, then a p-Sylow subgp of H is also a p-Sylow subgp of G. So WLOG, WMA $p \mid [G:H]$ $\forall H \lneq G$.

Class eq: $\underbrace{|G|}_{\text{divs by } p} = |Z(G)| + \underbrace{\sum_{i=1} [G : C_G(x_i)]}_{\text{divs by } p} \Rightarrow p \mid |Z(G)|$

↳ x_i: nontrivial conjugacy classes

By Cauchy's thm, $\exists N \leq Z(G)$ with $|N| = p$, and also, $N \trianglelefteq G$!

Let $\bar{G} = G/N$, then $|\bar{G}| = |G|/p = p^k m/p = p^{k-1} \cdot m$, with $p \nmid m$. By induction, $\exists$ p-Sylow subgp $\bar{P}$ of $\bar{G}$ and $|\bar{P}| = p^{k-1}$. Consider $\pi : G \to G/N$

[<u>Lattice Isomorphism Thm</u>: Let G group and $N \trianglelefteq G$. There is a 1-1 correspondance between subgroups of G/N and subgroups of G containg N. Consider $\pi : G \to G/N$. If $N \subseteq H \leq G$, the correspondidg subgp is $\pi(H)$. If $\bar{H} \leq G/N$, then the corresponding is $\pi^{-1}(\bar{H})$, which will contain N.]

Let $P = \pi^{-1}(\bar{P}) \leq G$. We claim $|P| = p^k$. $\pi|_P : P \to \bar{P}$, then $\ker(\pi|_P) = N$. By 1st iso thm, $P/N \cong \bar{P}$, so $|P| = |N| \cdot |\bar{P}| = p^k$. □

- <u>note</u>: conjugate subgroups are isomorphic (Sylow 2)

Pf (2): Let $P \in Syl_p(G)$, let H be any subgp of G which is a p-group. We claim $\exists x \in G$ s.t. $H \leq xPx^{-1}$. If this is true, then if H is a p-Sylow subgp, then $|H| = |xPx^{-1}| = p^k \Rightarrow H = xPx^{-1}$, hence H is conjugate to P.

Now to prove the claim, consider the action of H on G/P by left multiplication. Let $F = \{\text{fixed pts}\}$, then $|F| \equiv |G/P| \pmod p$, but P is a p-Sylow subgp so $p \nmid |G/P| \Rightarrow |F| \geq 1$. So let xP be a coset fixed by the action, i.e., $\forall h \in H$, $h \cdot xP = hxP = xP \Rightarrow x^{-1}hx \in P$. Then $h \in xPx^{-1}$, i.e. $H \leq xPx^{-1}$ □

- **Cor** (of claim): Any subgp of G that is a p-group is contained in a p-Sylow subgp.

Pf (3): Consider G acting on $Syl_p(G)$ by conjugation. By Sylow 2, this action is transitive. So there is only one orbit.
Let $n_p = |Syl_p(G)|$, then $n_p \mid |G|$ (size of orbit divides order of gp).
Now fix some $P \in Syl_p(G)$. Consider P acting on $Syl_p(G)$ by conjugation, if $F = \{\text{fixed pts}\}$, then $n_p \equiv |F| \pmod p$. We have $Q \in F$ iff $P \leq N_G(Q)$.
Obviously $P \in F$. If $Q \in F$, then P and Q are both p-Sylow subgps of $N_G(Q)$.
By Sylow 2, P and Q are conjugate in $N_G(Q)$. But $Q \trianglelefteq N_G(Q)$
so $P = Q$, hence $|F| = 1$ so $n_p \equiv 1 \pmod p$. □

- **Corollary**: TFAE: 1) $n_p = 1$ 2) Every p-Sylow subgroup is normal
3) Some p-Sylow subgp is normal

Pf) ($2 \Rightarrow 3$): Clear
($3 \Rightarrow 2$): By Sylow 2, all p-Sylow subgps are conjugate, so all are normal
($3 \Leftrightarrow 1$): Let $P \in Syl_p(G)$, the stabilizer of P is $N_G(P)$ (with G acting on $Syl_p(G)$ by conjugation). the action is transitive so one orbit and $n_p = [G : N_G(P)]$.
then $n_p = 1$ iff $N_G(P) = G$ iff $P \trianglelefteq G$. □

- **def**: If G, H are groups, then $G \times H$ is the group on the cartesian product
  - (external / direct) product of two groups
- **def**: Let G group and $A, B \leq G$. the internal product of A, B is
$AB = \{ab \mid a \in A, b \in B\}$ (not usually a group, just a set)
  - **Lemma**: If at least one of A, B is normal, then AB is a subgroup of G
    PF: Sps $A \trianglelefteq G$, then $(a_1b_1)\cdot(a_2b_2) = b_1b_1^{-1}a_1b_1a_2b_2 = b_1a_1'a_2b_2$
    $= b_1a_2'b_1^{-1}b_1b_2 = a_3b_1b_2 \in AB$ (also closed under inverses) □
  - **Lemma**: $|A \cdot B| = |A| \cdot |B| / |A \cap B|$ (as sets)
- **Recognition thm for products**: If $A, B \trianglelefteq G$, $A \cap B = \{e\}$, then $A \cdot B \cong A \times B$
  - the converse is also true (If $A \cdot B \cong A \times B$ then $A \cap B = \{e\}$ and A, B are normal)

Pf: $\phi : AB \to A \times B$ by $ab \mapsto (a, b)$ with inverse $(a, b) \mapsto ab$ are both well defined homomorphisms, and so it's an isomorphism. □

$(p \nmid q-1)$

- **thm**: If $|G| = pq$, $p<q$ both prime, $p \not\equiv 1 \bmod q$, then G is cyclic.

Pf: Let P, Q be p-Sylow and a q-Sylow subgroup respectively.
By Sylow 3, $n_p | q$ and $n_p \equiv 1 \pmod p$ so $n_p = 1 \Rightarrow P \trianglelefteq G$.
Since $p<q$, $p \not\equiv 1 \pmod q$ so $n_q = 1 \Rightarrow Q \trianglelefteq G$.
$P \cap Q = \{e\}$ because $P \cap Q$ is a subgroup of P and Q ($|P\cap Q|$ divides p and q).
then $|P| \cdot |Q| = pq = |G|$ so by Recognition thm, $G \cong P \times Q$. Note
$\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, so G is cyclic. $\square$

- **thm**: If $|G| = 30$ then $\exists H \trianglelefteq G$ s.t. $H \cong \mathbb{Z}_{15}$

Pf: It suffices to show $\exists H \leq G$ with $|H| = 15$. Let $P_3 \in Syl_3(G)$ and $P_5 \in Syl_5(G)$, if either is normal then P_3P_5 is a subgroup of order 15 in G. By Sylow 3, $n_3 = 1$ or 10 and $n_5 = 1$ or 6. For contradiction, assume $n_3 = 10$ and $n_5 = 6$. Each 3-Sylow subgp intersects trivially, and likewise w/ 5-Sylow subgps, so there are 20 elts of order 3 and 24 elts of order 5, then $|G| \geq 20 + 24 + 1 = 45$ ↯ $\square$

- **thm**: If $|G| = 60$ either G is simple or G has a normal subgp of order 5.
  - ↳ **Note**: A_5 does not have a normal subgp of order 5 ($\Rightarrow A_5$ simple)
    Pf: $\langle (12345) \rangle$ and $\langle (13245) \rangle$ are distinct 5-Sylow subgps $\square$

Pf: For contradiction, assume $n_5 \neq 1$, then $n_5 = 6$. Also assume there is a nontrivial normal subgp H of G. If $5 \mid |H|$, then H contains a 5-Sylow subgroup. But $H \trianglelefteq G \Rightarrow H$ contains all six 5-Sylow subgroups (they are all conjugate to each other inside H). They intersect trivially, so counting orders gives $|H| \geq 1 + 4 \cdot 6 = 27$. Since $|H| / 60$, $|H| = 30$. Then H has a normal subgp N of order 15, so N has all six 5-Sylow subgps, contradiction. Thus $5 \nmid |H|$. So $|H| \in \{2, 3, 4, 6, 12\} \Rightarrow |G/H| \in \{30, 20, 15, 10, 5\}$. In every case G/H has a normal subgroup $\bar{N}$ of order 5 (for 30, see prev argument). Defining $\pi: G \to G/H$, $N := \pi^{-1}(N) \trianglelefteq G$, so $|N| = |\bar{N}| \cdot |H| \Rightarrow 5 \mid |N|$

- **thm**: A_5 is the unique simple group of order 60.

- Semidirect Products -

- def: an automorphism of G is an isomorphism $\phi : G \to G$
  ↳ $\mathrm{Aut}(G)$ is a group with composition.
- ex: conjugation by a fixed elt. $g \in G$: $\phi_g : G \to G : x \mapsto gxg^{-1}$ is an automorphism
  $\underbrace{\{\phi_g : g \in G\}}_{\mathrm{Inn}(G)} \leq \mathrm{Aut}(G)$ $\quad \phi_g \circ \phi_h = \phi_{gh}$, $\phi_g^{-1} = \phi_{g^{-1}}$
  , the group of inner automorphisms
  $\Psi : G \to \mathrm{Inn}(G)$ is a surjective homomorphism
  $\ker(\Psi) = Z(G)$ $\Rightarrow$ first iso says $\mathrm{Inn}(G) \cong G/Z(G)$
- ex: Fix $n \geq 3$, so $Z(S_n) = \{e\}$. Then $\mathrm{Inn}(S_n) \cong S_n$.
  $\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n)$ for all n except 6; $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_n)] = 2$
- ex: $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ for each $a \in \mathbb{Z}_n^*$, $\phi_a(x) = a \cdot x$ is the automorphism
- ex: $\mathrm{Aut}(\mathbb{Z}_p^m) \cong GL_2(\mathbb{F}_p)$
- note: let $H, K \leq G$, $H \trianglelefteq G$, $H \cap K = \{e\}$
  - Recall $HK \leq G$: $(h_1k_1)(h_2k_2) = h_1 \underline{k_1 h_2 (k_1^{-1}} k_1) k_2 = h_3 k_3$ $(h_3 = h_1k_1h_2k_1^{-1}, k_3 = k_1k_2)$
  - for fixed $k \in K$, let $\phi_k : H \circlearrowleft : h \mapsto khk^{-1}$, then $K \to \mathrm{Aut}(H) : k \mapsto \phi_k$ is a homomorphism
- def: let H, K be groups, $\phi : K \to \mathrm{Aut}(H)$ homomorphism. The semidirect product of H and K is
  $G = H \rtimes_\phi K = H \times K$ with rule $(h_1, k_1) * (h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1k_2)$ which is a group.
  ↳ if $\phi = \mathrm{id}$ then G is just the normal direct product $H \times K$.
- ex: $H = \mathbb{Z}_n$, $K = \mathbb{Z}_2 = \langle x \rangle$, $\phi : K \to \mathrm{Aut}(H) : 0 \mapsto (h \mapsto h)$, $x \mapsto (h \mapsto h^{-1})$
  then $H \rtimes_\phi K \cong D_{2n}$
- thm: If p, q prime, $q \equiv 1 \pmod{p}$. then there is a (unique) nonabelian group of order pq.
  Pf: $H = \mathbb{Z}_q$, $K = \mathbb{Z}_p$, $\mathrm{Aut}(H) \cong (\mathbb{Z}_q^*, \cdot) \cong (\mathbb{Z}_{q-1}, +)$
  We need a homomorphism $\phi : \mathbb{Z}_p \to \mathbb{Z}_{q-1}$, but $p \mid q-1$ so $\exists$ elt $y \in \mathbb{Z}_{q-1}$ of order p,
  so send $\phi(x) = y$ (where x generates $\mathbb{Z}_p$)
  [thm: Let H, K abelian. then $H \rtimes_\varphi K$ is abelian iff φ is trivial]
  this homomorphism is nontrivial so $H \rtimes_\phi K$ is nonabelian of order pq. □
- Recognition Thm for Semidirect Products: let G group, $H, K \leq G$, $H \trianglelefteq G$, $H \cap K = \{e\}$, $HK = G$.
  Then $H \rtimes_\varphi K \cong G$, where $\varphi : K \to \mathrm{Aut}(H) : k \mapsto (h \mapsto khk^{-1})$
- thm: If p prime, there are exactly 5 group (up to $\cong$) of order p^3

- def: G is finitely generated if $\exists g_1, \dots, g_k \in G$ st. $G = \langle g_1, \dots, g_k \rangle$
  - ↳ if G is abel, any $g \in G$ can be written $g = g_1^{a_1} g_2^{a_2} \cdots g_k^{a_k}$, $a_i \in \mathbb{Z}$.
- thm: Every f.g. abelian group is $\cong$ to $\mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_t}$ (direct product of cyclic groups) for some $r \geq 0$, $n_1 | n_2 | \dots | n_t$. Further, $r, n_1, \dots, n_t$ are uniquely determined.
  - ↳ r = rank, n_i are invariant factors.
- ex: find all abelian groups of order 16 : $r = 0$, need $n_1 | n_2 | \dots | n_t$, $n_1 n_2 \dots n_t = 16$
  $\mathbb{Z}_{16}$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $(\mathbb{Z}_2)^4$
- def: a group G is solvable if there is a chain $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$ such that G_{i+1}/G_i is abelian for all i
  - ↳ $s = 1 \iff$ abelian
  - ↳ $|G| < 60 \Rightarrow$ solvable
- thm: Sps $N \trianglelefteq G$. Then G is solvable iff N and G/N are solvable
- note: simple group is solvable iff abelian
- thm: every finite group of odd order is solvable (very hard)
- thm (Burnside): every finite grp st. $|G|$ has at most 2 prime factors is solvable
- Classification of finite simple groups : 18 infinite families, 26 sporadic groups
- def: G finite, a composition series for G is a chain $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$ such that G_{i+1}/G_i (the composition factors) is simple $\forall i$.
- thm: composition series always exist, the comp factors for two series agree (up to permutation)
  - ↳ can have nonisomorphic groups with same comp factors

Rings

- def: a ring R is a set with two associative binary operations $+, \cdot$ s.t.
  1) $(R,+)$ is an abelian group
  2) $\cdot$ is left and right distributive
- def: R is commutative if $\cdot$ is commutative
- def: R is unital / has identity if $\exists\, 1 \in R$ st. $1 \cdot r = r \cdot 1 = r \quad \forall r \in R$
- def: a division ring or skew field is a nonzero ring w/ 1 st. every nonzero elt has mult. inv.
- def: a commutative division ring is a field
- e.g.: $\mathbb{Z}$, $\mathbb{Z}_n$ rings, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ prime fields. $M_n(R)$ non-commutative ring $(R \neq 0,\ n \geq 2)$
- def: a zero divisor is a nonzero elt a in a ring R st. $\exists\, b \in R$, $b \neq 0$ with $ab = 0$ (or $ba = 0$)
- def: an integral domain is a nonzero commutative unital ring w/o. zero divisors
- Cancellation Lemma: If R is an integral domain, $ac = bc \Rightarrow a = b$ (if $c \neq 0$)
- def: a unit in a ring R is an elt $a \in R$ st. $\exists b \in R$ with $ab = ba = 1$
- def: $R^* = \{\text{units of } R\}$, $(R^*, \cdot)$ is a group, called unit group of R
- Lemma: a finite integral domain is a field.

  Pf: We must show all nonzero elts have $\cdot$ inverse. Define $f_a : R \to R$ by $f_a(x) = ax$ for $a \in R$, $a \neq 0$. This is injective b/c if $ax = ay$, $x = y$ (cancellation). Since R is finite, f_a is surjective, so $1 \in \text{im}(f_a)$. So $\exists b$ st. $ab = 1$. □
- thm: a finite division ring is a field.
- def: R ring, $R[x]$ is polynomial ring, polys w/ coefts in R.
- Lemma: If R is integral domain, then so is $R[x]$ and $R[x]^* = R^*$.
- def: If R_1, R_2 are rings, $R_1 \times R_2$ is a ring
- def: $\phi : R \to S$ is a ring homomorphism if $\phi(0) = 0$ and $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x) \cdot \phi(y)$. If R, S are rings w/ 1, $\phi(1) = 1$ as well.
- def: an ideal $I \subseteq R$ is an additive subgroup and if $x \in I$, $r \in R$:

  $xr \in I$ right ideal, $rx \in I$ left ideal, both $\Rightarrow$ two-sided ideal
- note: I is an ideal iff it is the kernel of some ring homomorphism
- def: $R/I = \{r + I \mid r \in R\}$, $(r+I) + (s+I) = (r+s) + I$, $(r+I) \cdot (s+I) = (rs) + I$ is a ring iff I is an ideal.

- First Iso. Thm: $\phi: R \to S$ ring homomorphism, then $R/\ker\phi \cong \operatorname{im}\phi$
- Lattice Iso. Thm: I ideal of R, bijection b/w ideals of R/I and ideals of R containing I
- def: I, J ideals of R, $I+J := \{x+y \mid x \in I, y \in J\}$ is an ideal of R.
  $I \cdot J = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J\} = (\{xy : x \in I, y \in J\})$ ideal gen. by these elts
  where (S) is the smallest ideal containing S.
- note: $R = \mathbb{Z}$, $I = m\mathbb{Z}$, $J = n\mathbb{Z}$: $I \cap J \overset{!}{=} \operatorname{lcm}(m,n)\mathbb{Z}$, $IJ = mn\mathbb{Z}$, $I+J = \gcd(m,n)\mathbb{Z}$
- def: a principal ideal is one that is generated by a single elt.
- Chinese Remainder Thm: let I, J ideals in commutative ring R w/ id. We say I, J are comaximal if $I+J = R$ (generalizes rel. prime).
  Let I, J be comaximal ideals. Then $R/IJ = R/I \times R/J$
  Pf: define $\phi: R \to R/I \times R/J$ by $r \mapsto (r+I, r+J)$. Note $\ker\phi = I \cap J$. Since $I+J = R \ni 1 \Rightarrow \exists x \in I, y \in J$ st. $x+y = 1$.
  $\phi(x) = (I, 1+J)$, $\phi(y) = (1+I, J)$. So if $(r_1+I, r_2+J) \in R/I \times R/J$, $\phi(r_1 y + r_2 x) = (r_1+I, r_2+J)$ so ϕ is surjective.
  By First Iso Thm, $R/I \times R/J \cong R/\ker\phi = R/I \cap J$
  Note $IJ \subseteq I \cap J$ by properties of ideals / def. If $r \in I \cap J$, $r = r \cdot 1 = r(x+y)$ $= rx + ry$, each is an elt of IJ so sum is in IJ. □
- def: a principal ideal domain (PID) is an integral domain st. every ideal is principal
  (generated by single elt)
  ↳ e.g. $\mathbb{Z}$, $F[x]$ for a field F.
- def: an ideal M is maximal if $M \neq R$ and if $M \subseteq I \subseteq R$ for some ideal I, then $I = M$ or $I = R$.
  ↳ in $\mathbb{Z}$, the maximal ideals are $p\mathbb{Z}$ for prime p.

R comm w/ 1 ↓

- def: an ideal P in R is prime if $P \neq R$ and $ab \in P$, then $a \in P$ or $b \in P$.
  ↳ (0) is prime iff R is an integral domain
  ↳ every maximal ideal is prime
- Lemma: R is a field iff (0), $(1) = R$ are the only ideals
  Pf: ($\Rightarrow$): If R is a field, I an ideal, then either $(0) = I$ or $\exists x \in I$, $x \neq 0$. Then $\exists y \in R$ st. $xy = 1$, so $1 \in I \Rightarrow I = (1)$.

(⇐): Sps the only ideals are (0),(1). Take $x \in R$, $x \neq 0$. Then $x \in (x) \neq (0)$, so $(x) = (1)$ then $xy = 1$ for some y i.e. x has a mult inverse. □

- Lemma: M is maximal iff R/M is a field.

Pf: Lattice Iso Thm + previous lemma. □

- Lemma: P is a prime ideal iff R/P is an integral domain.
- Lemma: Every proper ideal of R is contained in a maximal ideal (AC)
- Zorn's Lemma: A nonempty poset where every chain has an upper bound has a maximal elt.
- Cor: $\text{Spec}(R) = \{\text{prime ideals of } R\}$ is nonempty

Pf: By lemma, it suffices to find a proper ideal, and $I = (0)$ is a proper ideal. □

- Problem: Solve $x^3 - y^2 = 2$ over $\mathbb{Z}$. $(3,5),(3,-5)$ are sols, any others? no!

1) x, y both have to be odd. Over mod 4, $x^3 \equiv 0,1,3 \pmod 4$ and $y^2 \equiv 0,1 \pmod 4$.

if x even, $x^3 \equiv 0 \pmod 4$ so $y^2 \equiv 2$ ↯

if y even, $y^2 \equiv 0 \pmod 4$ so $x^3 \equiv 2$ ↯.

2) factor equation in $R = \mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$. $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$.

3) $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are comaximal (i.e. $(y + \sqrt{-2}, y - \sqrt{-2}) = R$) (for any sol (x,y) to eq)

Pf: $(y + \sqrt{-2}) + (y - \sqrt{-2}) = 2y$ is even. $(y + \sqrt{-2})(y - \sqrt{-2}) = y^2 + 2 = x^3$ is odd. So since our ideal contains an even and an odd number, it contains 1. □

4) (faith): both $y + \sqrt{-2}$ and $y - \sqrt{-2}$ must be perfect cubes.

5) $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2 b - 2b^3)\sqrt{-2} \Rightarrow y = a^3 - 6ab^2$,

$3a^2 b - 2b^3 = 1 = b(3a^2 - 2b^2)$ so b must be a unit $\Rightarrow b = \pm 1$.

also $b^3 \equiv 1 \pmod 3$ so $b = +1$. $3a^2 = 3 \Rightarrow a \pm 1$, then $y = a(a^2 - 6b^2) = \pm 5$ and $x = 3$. □

- def: a norm on a ring R is a fn $N: R \to \mathbb{N}^0$ s.t. $N(0) = 0$. Usually, N is multiplicative: $N(ab) = N(a) + N(b)$
- def: a Euclidean domain is an integral domain with a norm function N s.t. for any $a, b \in R$, $b \neq 0$, $\exists q, r \in R$ s.t. $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$
- Thm: a Euclidean domain is a PID.

Pf: Let I be an ideal (wts I is principal). If $I = (0)$ it's principal, so otherwise let d be any nonzero elt of I with minimal norm. $(d) \subseteq I$ clearly so sps $a \in I$, then $a = qd + r$ for $q, r \in R$, $r = 0$ or $N(r) < N(d)$. But $r = a - dq \in I$ so $r = 0$ and $a = qd \in (d)$. Then $I = (d)$ is principal □

- $R[x]$ is a PID iff R is a field
- Fact: $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not Euclidean (generally hard to prove PIDs but not Euclidean)
- Lemma: In a PID, every nonzero prime ideal is maximal

  Pf: Let $P \neq (0)$ be a prime ideal, so $P = (p)$. Let M be an ideal containing P. $M = (m)$. Then $m | p$, i.e. $p = rm \in P \Rightarrow r \in P$ or $m \in P$ by P prime.
  If $m \in P$, $(m) \subseteq (p) \Rightarrow (m) = (p)$ ✓
  If $r \in P$, $r = ps \Rightarrow p = rm = psm \Rightarrow 1 = sm$. Then $1 \in (m) \Rightarrow (m) = R$. ✓. □
- Cor: $R[X]$ is a PID iff R is a field

  Pf: $R \subseteq R[x]$ so R is a domain. $R[x]/(x) \cong R \Rightarrow (x)$ is prime $\Rightarrow (x)$ is maximal $\Rightarrow R[x]/(x)$ is a field $\Rightarrow R[x]$ is a field. □
- def: Let R an integral domain, $r \in R$ is irreducible in R if $r \neq 0$, r is not a unit, and if $r = ab$ $(a,b \in R)$, then at least one of a or b is a unit.
- def: a is associate to b $(a \sim b)$ if $a = bu$ for some unit u
- def: R is a unique factorization domain (UFD) if R is an integral domain and for any nonzero $r \in R$ which is not a unit,
  1) $\exists$ irred elts $p_1, \dots, p_n \in R$ st. $r = p_1 \dots p_n$ [if a irred and $a \sim b$, then b irred]
  2) the decomposition is unique up to associates and ordering
- thm: Every PID is a UFD.

R int. domain ⤳ def: $p \in R$ is prime if $p \neq 0$, p is a nonunit, and $p | ab \Rightarrow p | a$ or $p | b \Leftrightarrow (p)$ is prime nonzero

- Lemma: In any integral domain, prime $\Rightarrow$ irreducible

  Pf: let p prime, $p = ab$. Then $p | a$ or $p | b$, WLOG assume $p | a$, then $a = pr = abr$ so $br = 1$ and b is a unit. □
- Lemma: In a PID, irred $\Rightarrow$ prime

  pf: Let f be irreducible. We will show (f) is maximal. Sp. $M = (m) \supseteq (f)$ $\Rightarrow m | f$ so $f = mr$. If m is a unit, $1 \in (m) \Rightarrow (m) = R$. If r is a unit, $f \sim m$ so $(f) = (m)$. So (f) is maximal $\Rightarrow (f)$ prime $\Rightarrow f$ prime. □
  $\therefore$ In PID, maximal ideal $\Leftrightarrow$ prime ideal
- Lemma: If R is a UFD, irred $\Rightarrow$ prime

field ⇒ Euc. domain ⇒ PID ⇒ UFD ⇒ Integral Domain

Pf (PID ⇒ UFD): existence: follows from PID is Noetherian.

Uniqueness: Sps $r = p_1 \dots p_m = q_1 \dots q_n$ all irreducible. WLOG $m \geq n$. Induction on n □

- **def**: R is Noetherian if it satisfies the ascending chain condition: if $I_0 \subseteq I_1 \subseteq \dots$ then $\exists N$ st $I_k = I_{k+1}$ $\forall k \geq N$ (the chain stabilizes)
- **Prop**: R is Noetherian iff every ideal is finitely generated

pf: ($\Leftarrow$): Let $I_0 \subseteq \dots$ be an ascending chain. Let $I = \bigcup_k I_k$ is an ideal hence finitely generated by $(a_1, \dots, a_m)$. Then $\exists N$ st. $a_i \in I_N$ $\forall i$, so $I = I_N$ ✓.

($\Rightarrow$): Sps R is Noetherian, and suppose an ideal I is not f.g. We can inductively choose generators $a_1, a_2, \dots$, each $a_i \in I \setminus (\bigcup_{k<i} (a_k))$. Then $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \dots$ is an infinite ascending chain, a contradiction to Noetherian. ✓ □

- **Prop**: In a Noetherian ring, every nonzero nonunit is a product of finitely many irred. elts

Pf: Let r be a nonzero nonunit. If r irred, done, else let $r = r_1 r_2$ w/ both nonzero, nonunits, Note $(r) \subsetneq (r_1)$. Repeat process on r_1, r_2 and this terminates.

- **Note**: Every PID is Noetherian (every ideal gen by 1 elt)
- **def**: Let R be a PID, for $a, b \in R$, $(a,b) = (c)$ for some c (it's a PID) define $\gcd(a,b) = c$ (only up to mult. by units)
- **Lemma**: $\gcd(a,b) \mid a$ and b. If $d \mid a$ and $d \mid b$ then $d \mid \gcd(a,b)$

PF: $a, b \in (c)$ so a and b are mults of c, that is, $c \mid a$, $c \mid b$.

For the second, c is a lin combination of a, b (b/c $c \in (a,b)$), $c = ax + by$. $x, y \in R$

Since $d \mid a$, $d \mid b$, then $d \mid c$. □

- **def**: Let R be a UFD, for $a, b \in R$, $a = u \cdot p_1^{e_1} \cdots p_r^{e_r}$ $b = v \cdot p_1^{f_1} \cdots p_r^{f_r}$ (allow $e_i, f_i \geq 0$) define $\gcd(a,b) = p_1^{\min(e_1, f_1)} \cdots p_r^{\min(e_r, f_r)}$

  ↳ this is the same property as previous def

- **Cor**: In a PID, comaximal ⇔ relatively prime (no common irred factors) ($\gcd = 1$)
- **def**: a poly $p \in R[x]$ (R UFD) is **primitive** if gcd of coeffs of p is a unit
- **thm** (Gauss's Lemma): R UFD, k fraction field, $p \in R[x]$ nonzero.

1) If p is reducible in $k[x]$ then its reducible in $R[x]$
2) If p primitive, then p reducible in $k[x]$ ⇔ reducible in $R[x]$

K field, R UFD (e.g. $R=\mathbb{Z}$, $K=\mathbb{Q}$)

- $x^4-72x+4$ is irred /$\mathbb{Q}$ but reducible mod every prime
- Thm (Rational Root Thm): Let R UFD, K fraction field of R. Let $p(x) \in R[x]$
  $p(x) = a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$. Then every root of $p(x)$ in K has the form r/s where $r \mid a_0$, $s \mid a_n$.

  Pf: Sps $\alpha = r/s \in K$ is a root, WLOG $\gcd(r,s)=1$.

  $a_n(r/s)^n + \dots + a_1(r/s) + a_0 = 0$

  $a_n r^n + \underbrace{a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n}_{} = 0$ (mult by s^n)

  ↳ is a multiple of $s \Rightarrow s \mid a_n r^n$. But by UFD since $\gcd(r,s)=1$, $s \mid a_n$.
  the first $n-1$ terms is a multiple of $r \Rightarrow r \mid a_0 s^n \Rightarrow r \mid a_0$. □
- Prop: R int. domain, M maximal ideal in R. $p(x) \in R[x]$ monic gives poly $\bar{p}(x) \in (R/M)[x]$, If $\bar{p}$ irred in $(R/M)[x]$ then p irred in $R[x]$
- Thm (Eisenstein's Criterion): R int domain, P prime ideal.
  $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1 x^1 + c_0$ monic in $R[x]$. Assume $\forall i$
  $c_i \in P$ and $c_0 \notin P^2$. Then f irred over R.
  - e.g.: $x^7+25x^2-10x-15$ is irred /$\mathbb{Q}$ (Eisenstein at (5)).
  - e.g.: $f(x) = x^4+1$, $g(x) = f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x^2+2$
    is Eisenstein at 2 ⇒ g irred over $\mathbb{Q}$ ⇒ f irred over $\mathbb{Q}$.
  - e.g.: let p prime, define $\Phi_p(x) = (x^p-1)/(x-1) = x^{p-1} + \dots + x + 1$
    $\Phi_p(x+1) = ((x+1)^p - 1)/x = x^{p-1} \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k-1}$ is Eisenstein @ p, so irred
  - e.g.: $f(x,y) = x^n - x^2y^3 + y \in \mathbb{Z}[x,y] = R, = (\mathbb{Z}[y])[x]$
    then (y) is a prime ideal in $\mathbb{Z}[y]$, so f irred, Eisenstein
- Thm: If R Noetherian, $R[x]$ Noetherian
  ↳ $R[x_1, \dots, x_n]/I$ is also Noetherian ((lattice 110)

Pf: Suppose I ideal in $R[x]$ not f.g. $I \neq 0$ so $\exists f_1 \in I$ nonzero which has minimal degree. Choose $f_2 \in I - (f_1)$ minimal degree, $f_3 \in I - (f_1, f_2)$ min degree, ..., get inf. sequence since I is not f.g.

let $n_k = \deg(f_k)$, $n_1 \leq n_2 \leq \dots$ (minimality)

let a_k = leading coeff of f_k

R Noetherian : $(a_1) \subseteq (a_1, a_2) \subseteq \dots$ stabilizes : $\exists K$ s.t. $(a_1, \dots, a_k) = (a_1, \dots, a_{k+1})$.

So $a_{k+1} \in (a_1, \dots, a_k)$ so we can write $a_{k+1} = c_1 a_1 + \dots + c_k a_k$, $c_i \in R$.

define $g = f_{k+1} - \sum_{i=1}^{k} c_i x^{n_{k+1} - n_i} f_k$ ← each term has degree n_{k+1}

degree n_{k+1} ↗ ↖ leading term is a_{k+1} ↖ leading term is $c_i a_i$ $\deg(g) < n_{k+1}$

But $g \in I \setminus (f_1, \dots, f_k)$ (right sum in $(f_1, \dots, f_k)$, f_{k+1} is not in)

So n_{k+1} wasn't minimal. □

Fields

- def: a field is a commutative division ring (every non-0 elt has mult inverse, has 1)
- note: there is a unique homomorphism $\varphi : \mathbb{Z} \to F$ for any field ($n \mapsto 1+1+\dots+1$)
  $\mathbb{Z}/\ker\varphi \cong \text{Im}(\varphi) \subseteq F$ so $\text{im}\,\varphi$ is an integral domain (subring of field).
  Then $\ker\varphi$ is a prime ideal. So $\ker\varphi = p\mathbb{Z}$ where p is prime or zero
- def: the characteristic of F is this number p.
- Lemma: If $\text{char} F = p$ prime then F has a subfield isomorphic to $\mathbb{F}_p$.
  If $\text{char} F = 0$ then F has a subfield isomorphic to $\mathbb{Q}$.
  ↳ the subfield is the prime field of F.
- Lemma: Any homomorphism between fields is injective
  pf: $\varphi(1) = 1$ so $\ker\varphi \neq F$. $\ker\varphi$ is an ideal of F but the only ideals of F are (0) and F. □
- def: A field extension (denoted K/F or $\begin{smallmatrix} K \\ | \\ F \end{smallmatrix}$) is a field K and subfield F
  ↳ tower of fields: $L/K/F$
- sps K/F is an extension, then K can be thought of as a vector space over F:
  $(K, +)$ is an abelian gp, can multiply elts of K by elts of F. forget $\cdot$ of K.
  Write $\dim_F K = [K:F]$ as the degree of the field extension (cardinality of basis)
- Prop: If F field, $g(x) \in F[x]$ non constant poly, then $\exists\, F'/F$ extension st. F' contains a root of g.
  Moreover, if $\deg(g) = n$, then we can choose F' st. $[F':F] \leq n$.
  Pf: Let f be an irred factor of g. Then (f) is maximal in $F[X]$ (irred $\Rightarrow$ prime ideal $\Rightarrow$ maximal ideal). Then $F[x]/(f)$ is a field. There is a natural map $\varphi : F \to F[X]/(f)$ by $c \mapsto \bar{c}$ (the constant poly) which is injective (lemma).
  So F is a subfield of $F[X]/(f) =: F'$. Let $\alpha = \bar{x} \in F'$. Then
  ★ $f(\alpha) = \bar{f}(\alpha) = \bar{f}(\bar{\alpha}) = \overline{f(x)} = \bar{0}$, and so α is a root of f so $g(\alpha) = 0$ also in F'. □
- thm: Let K/F splitting field, $\alpha \in K$. Sps α satisfies an irred poly $g \in F[x]$, of degree n.
  Then $[F(\alpha):F] = n$. Further, $1, \alpha, \dots, \alpha^{n-1}$ is a basis for K/F.
- def: If K/F is extension, $\alpha \in K$ is algebraic over F if α is a root of a nonzero poly $g \in F[x]$.
  K/F is algebraic if every elt of K is algebraic over F. Elts that aren't are transcendental
- Prop: If K/F is an extension and $\alpha \in K$ is algebraic over F, there is a unique monic irred poly $m(x)$ having α as its root. Further, m divides any nonzero poly $g \in F[x]$ with $g(\alpha) = 0$.
  ↳ this $m(x)$ is the minimal poly of α over F ($m_{\alpha,F}(X)$)

- **Cor**: If $\alpha \in K$ is algebraic over F, the degree of $m_{\alpha,F}$ is equal to $[F(\alpha):F]$
- **Prop**: If K/F is a field ext $\alpha \in K$ algebraic over F iff $F(\alpha)/F$ is finite extension.
- **Cor**: Any finite extension of F is algebraic
  - ↳ conv false: $\exists$ algebraic infinite extensions
- **thm**: $F \subseteq K \subseteq L$ fields, then $[L:F] = [L:K][K:F]$
  - ↳ **Cor**: L/F finite iff L/K and K/F finite
- **thm**: K/F is a finite extension iff K is generated by finitely many algebraic elts.
- **Cor**: If K/F extension, $K^{alg} = \{\alpha \in K : \alpha \text{ algebraic over } F\}$ is a subfield of K containing F
- **thm**: If $L/K/F$ tower, L/F algebraic iff L/K and K/F both algebraic
- Let K field, $g \in K[x]$ nonzero poly deg n. We know $\exists$ extension L/K w/ degree at most n st. g has a root in L.
- **def**: a *splitting field* for g over K is an extension L/K st.
  1) g factors as a product of linear polys in $L[x]$
  2) L is minimal wrt. (1) (i.e., g won't linearly factor in any proper subfield of L containing K)
  - ↳ when g factors linear polys in $L[x]$ for some extension L/K, say g *splits over L*
- **thm**: Splitting fields exist and are unique up to $\cong$
- **thm**: Let $\sigma : K \to K'$ be an $\cong$ of fields, $g \in K[x]$ deg n, L splitting field of g over K, L' splitting field of $\sigma(g)$ over K', then σ extends to $\cong$ of $L \to L'$.

$$\begin{tikzcd} L \arrow[r, dashed, "\sim"] \arrow[d, dash] & L' \arrow[d, dash] \\ K \arrow[r, "\sim", "\sigma"'] & K' \end{tikzcd}$$

- **def**: K field, $g \in K[x]$ nonzero. g is *separable* if it has distinct roots in a splitting field L for K. If g has multiple roots in L then g is *inseparable*
- **def**: L/K extension. If $\alpha \in L$ is algebraic over K, it is *separable* over K if its minimal poly over K is separable in $K[x]$. *Inseparable* otherwise
- **thm**: a nonzero poly $g \in K[x]$ is separable iff it's rel prime to its derivative in $K[x]$ i.e., $\gcd(g, g') = 1$.
- **thm**: K field, $g \in K[x]$ irred, then g separable iff derivative is nonzero. In particular: $\text{char}(K) = 0 \Rightarrow g$ separable, $\text{char}(K) = p > 0$ then g separable iff it cannot be written as a poly in x^p.

- Cor: irreducible polys in $\mathbb{Q}[x]$ are separable.
- def: L/K separable if every elt is separable. inseparable else.
- lemma: $\sigma: k \to k'$ $\cong$, $g \in k[x]$ separable, then $\sigma(g) \in k'[x]$ separable.
- thm: $\sigma: k \to k'$ $\cong$, $g \in k[x]$ deg n, L splitting field of g over k, L' — of $\sigma(g)$ over k'. Then σ extends to $\cong$ $L \to L'$, and # of such extensions is at most $[L:k]$. If g separable, # extensions is precisely $[L:k]$.
- thm: L/k finite extension, write $L = K(\alpha_1, \dots, \alpha_m)$. Then L/k separable iff each α_i is separable over k
- thm: (Primitive Elt Thm): every finite separable extension of a field k is in the form $k(\alpha)$ for some $\alpha \in k$.
- thm: If $L/K/F$ tower of fields, L/F separable iff L/k and k/F separable.
- theorem: $\exists$ unique field of p^n elts (splitting field for $x^q - x$ over F_p)
- Lemma: $\text{char}(k) = p > 0$, then $\varphi(x) = x^p$ is injective field homo $k \circlearrowleft$
  - ↳ this is a field automorphism called <u>Frobenius automorphism</u>
- Cor: For every finite field F_q of order $q = p^n$, F_q / F_p is separable
- thm: p prime, $m, n > 0$. $\mathbb{F}_{p^n}$ has a subfield $\cong F_{p^m}$ iff $m | n$
- def: $\varphi(n)$ is Euler totient fn, # of coprime integers $\leq n$. $\varphi(n) = |\mathbb{Z}_n^*|$
- lemma: If G cyclic order n, G has exactly $\varphi(n)$ elts of order d for each $d | n$
  - ↳ $n = \sum_{d|n} \varphi(d)$
- thm: a finite subgp G of the multiplicative gp of a field k is cyclic
- Cor: If p prime, $\mathbb{Z}_p^*$ cyclic
- def: cyclotomic poly: $\Phi_n(x) = \prod_{1 \leq a \leq n, \gcd(a,n)=1} (x - \zeta_n^a) \in \mathbb{C}[x]$ (roots are all nth primitive roots of unity)
- lemma: $\Phi_n(x) \in \mathbb{Z}[x]$ (the coeffs are in $\mathbb{Z}$!)
- note: $x^n - 1 = \prod_{d|n} \Phi_d(x)$
- thm: $\Phi_n(x)$ is irred over $\mathbb{Q}$ $\forall n$.
- thm (Wedderburn): Every finite division ring is a field.

Galois Theory

- def: K/F field extension. $\mathrm{Aut}(K) = \{$field isomorphisms $\sigma : K \to K\}$

  $\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) : \sigma(x) = x \ \forall x \in F\} \leq \mathrm{Aut}(K)$

  ↳ ex: $K = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$. $\mathrm{Aut}(K/F) = \{id, \sigma\}$ where $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$

  ★ any automorphism $\tau \in \mathrm{Aut}(K)$ must have $\tau(\sqrt{2}) = \pm\sqrt{2}$

  Pf: $f(x) = x^2 - 2$, $f(\alpha) = 0$. then $0 = \tau(0) = \tau(f(\alpha)) = \tau(\alpha^2 - 2) = \tau(\alpha)^2 - \overset{2}{\tau(2)}$

- lemma: If $\sigma \in \mathrm{Aut}(K/F)$ and $g \in F[x]$ and α is a root of g, then $\sigma(\alpha)$ is a root of g also. More generally, $\mathrm{Aut}(K/F)$ acts on the set of roots of g in K by $\sigma \cdot \alpha = \sigma(\alpha)$

  ↳ only when automorphisms fix coeffs, i.e. fix F!

  ↳ $\mathrm{Aut}(K/F)$ induces a permutation on roots of g in K

- ex: $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. $g(x) = x^3 - 2$ has a unique root in K so any aut. in $\mathrm{Aut}(K/F)$ is trivial. ☹

- ex: $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ $\omega =$ primitive 3^{rd} root of unity in $\mathbb{C}$

  $\mathbb{Q}(\sqrt[3]{2})$ | deg 6 K is a splitting field for $x^3 - 2$

  $\mathbb{Q} = F$ $\sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \omega \mapsto \omega$ $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega \mapsto \omega^2$

  need to check these extend to automorphisms!

  [↳ e.g. $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$ is the same field K, don't always extend to automorphism]

  $\mathrm{Aut}(K/F) = \langle \sigma, \tau \rangle = S_3$ (order 6 ($\sigma^3 = id$, $\tau^2 = id$) and $\sigma\tau \neq \tau\sigma$)

- def: K/F is Galois if $|\mathrm{Aut}(K/F)| = [K:F]$. Write $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$

- note: $K/L/F$ tower $\Rightarrow \mathrm{Aut}(K/L) \leq \mathrm{Aut}(K/F)$ | ↳ generally, $|\mathrm{Aut}(K/F)| \leq [K:F]$

  converse also true! Sps K/F and $H \leq \mathrm{Aut}(K/F)$, define:

  def: $K^H = \{x \in K : \sigma(x) = x \ \forall \sigma \in H\}$ the fixed field of H (is a subfield of K)

- lemma: $K^{\mathrm{Aut}(K/F)} = F$ iff K/F is Galois

- Fundamental Thm of Galois Theory: K/F finite extension and is Galois. Then there is a bijection $\{$subgps of $\mathrm{Aut}(K/F)\} \leftrightarrow \{$intermediate fields L, $K/L/F\}$ (by $H \mapsto K^H$, $\mathrm{Aut}(K/L) \leftarrow L$). this is inclusion reversing. $[K:K^H] = |H|$

- thm: K/F is Galois iff K is the splitting field of a separable polynomial over F

  ↳ also K/K^H is Galois and $\mathrm{Gal}(K/K^H) \cong H$

- ex: back to $\mathbb{Q}(\sqrt[3]{2}, \omega) = k$, $\mathbb{Q} = F$

$G: \mathrm{Aut}(k/F) \cong \langle \sigma, \tau \rangle \cong S_3 \cong D_6$

Subgroups of G: $\overset{\text{ord }1}{\langle 1 \rangle}$, $\overset{\text{ord }2}{\langle \tau \rangle}$, $\overset{\text{ord }2}{\langle \tau\sigma \rangle}$, $\overset{\text{ord }2}{\langle \sigma\tau \rangle}$, $\overset{\text{ord }3}{\langle \sigma \rangle}$, $\overset{\text{ord }6}{\langle \tau, \sigma \rangle} = G$

$$\begin{tikzcd}
 & & K = \mathbb{Q}(\sqrt[3]{2}, \omega) = K^{\langle 1 \rangle} \arrow[lld, dash, "2"'] \arrow[ld, dash, "2"] \arrow[rd, dash, "2"] \arrow[rrd, dash, "3"] \arrow[dd, dash, "6"] & & \\
K^{\langle \tau \rangle} = \mathbb{Q}(\sqrt[3]{2}) \arrow[rrd, dash, "3"'] & K^{\langle \tau\sigma \rangle} = \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[rd, dash, "3"] & & K^{\langle \sigma\tau \rangle} = \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[ld, dash, "3"'] & K^{\langle \sigma \rangle} = \mathbb{Q}(\omega) \arrow[lld, dash, "2 \hookrightarrow \text{this is Galois extension}"] \\
 & & F = \mathbb{Q} = K^G & &
\end{tikzcd}$$

— Pf of Galois Correspondence —

L/K finite extension, M intermediate field

- **Lemma**: L is not a finite union of intermediate subfields
- **Cor**: $\exists \theta \in L$ st. $\mathrm{Stab}(\theta)$ in $\mathrm{Aut}(L/k)$ is only $\{id\}$

Pf: $\forall 1 \neq \sigma \in \mathrm{Aut}(L/k)$, $L^\sigma = \{x \in L : \sigma(x) = x\}$ is a proper intermediate field

But $\bigcup_{\sigma \neq 1} L^\sigma \neq L$ by lemma, choose $\theta \in L \setminus \bigcup_{\sigma \neq 1} L^\sigma$. □

- **thm**: 1) $|\mathrm{Aut}(L/k)| \leq [L:k]$

2) If $=$ in (1) (L/k is Galois), $\exists \theta \in L$ st. $L = k(\theta)$, min poly f for θ is separable, and L is a splitting field for f.

Pf: Choose $\theta \in L$ by lemma, elts of $\mathrm{Aut}(L/k)$ map θ to other roots of f.

Claim: distinct automorphisms $\mathrm{Aut}(L/k)$ map θ to distinct roots

Pf: $\tau\theta = \sigma\theta \Rightarrow \theta = \tau^{-1}\sigma\theta \Rightarrow \tau^{-1}\sigma = id \Rightarrow \tau = \sigma$ □

$\Rightarrow |\mathrm{Aut}(L/k)| \leq$ # distinct rts of f in $L \leq \deg f = [k(\theta : k] \leq [L:k]$ ✓

If $|\mathrm{Aut}(L/k)| = [L:k]$ then f factors into distinct linear factors in L, so f separable, L splitting field for f, $L = k(\theta)$. □

★ - **thm**: let $G = \mathrm{Aut}(L/k)$. TFAE:

1) L/k is Galois 2) k is fixed field of G 3) L is splitting field of a separable poly over k 4) every irred poly over k with a root in L splits into distinct linear factors over L

Pf: $(1) \Rightarrow (2)$: let $M = L^G$, $G = \mathrm{Aut}(L/k) \overset{*}{=} \mathrm{Aut}(L/M)$. $M \supseteq k$.

$|G| \leq [L:M] \leq [L:k] = |G \Rightarrow M = k$

$(2) \Rightarrow (3)$: generalization of $\alpha \in \mathbb{C}$, $(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$ (not just $\mathbb{Q}[x]$)

$\sigma \in \mathrm{Aut}(L/k)$ are conjugates.

$(3 \Rightarrow 1)$: done previously

trick: fix a basis $\omega_1, \dots, \omega_n$ for L/K $\square$

- **Thm**: L/K Galois, $\mathcal{F} = F(L/K)$ (subfields of L/K), $\mathcal{G} = \{$subgps of $G = \mathrm{Aut}(L/F)\}$
  $\Phi : \mathcal{F} \to \mathcal{G} : M \mapsto \mathrm{Aut}(L/M)$, $\Psi : \mathcal{G} \to \mathcal{F} : H \mapsto L^H$
  Φ, Ψ are $\cong$, inverse to each other, inclusion reversing (smaller field = bigger automorphism set)
  Pf. Show $\Phi \circ \Psi = id_{\mathcal{F}}$, $\Psi \circ \Phi = id_{\mathcal{G}}$ $\square$
- **Thm** (Primitive Elt. Thm): If K/F is separable, $\exists \theta \in K$ s.t. $K = F(\theta)$
  ↳ proved before for Galois extensions
- **Lemma**: If K_1/F, K_2/F is Galois, then $(K_1 \cap K_2)/F$ is Galois
- **thm**: If K/F finite, sep extension, then K is contained in a minimal Galois extension E/F (called the Galois closure)

$$\begin{tikzcd} E \arrow[d, dash, dotted] \\ K \arrow[d, dash, dotted] \\ F \arrow[uu, phantom, bend left=60, "\text{Galois}"'] \end{tikzcd}$$

- Proving Fund. Thm. Alg (need these 2 facts)
- Fact: $\mathbb{R}$ has no finite extension or odd degree
  Pf:

$$\begin{tikzcd} K \ni \alpha \arrow[d, dash, "\text{odd}"'] \arrow[dr, dash] & \\ \mathbb{R} \arrow[r, dash] & \mathbb{R}(\alpha) \end{tikzcd}$$

  Sps not, that $[K : \mathbb{R}]$ odd. then $[\mathbb{R}(\alpha) : \mathbb{R}]$ odd also, which is the deg of min poly of α. But every odd deg poly over $\mathbb{R}$ has a root in $\mathbb{R}$ ↯ $\square$
- Fact: $\mathbb{C}$ has no quadratic extension.
  Pf: If $[K : \mathbb{C}] = 2$ then $K = \mathbb{C}(\alpha)$ for some $\alpha \in K$.
  $m_\alpha(x) = x^2 + bx + c$, $b, c \in \mathbb{C}$, then $\Delta = b^2 - 4c \in \mathbb{C}$ but $\alpha = \frac{-b \pm \sqrt{\Delta}}{2}$
  so $\alpha \in \mathbb{C}$ and $K = \mathbb{C}(\alpha) = \mathbb{C}$ ↯ $\square$
- Recall: $g \in \mathbb{Z}[x]$, g irred if g irred over $\mathbb{F}_p$ for some p (not $\Leftarrow$)
- ex: $x^4 + 1$ is irred over $\mathbb{Z}$ (it is $\Phi_8(x)$) but is reducible mod every p
- **thm**: If K/F is a finite extension of finite fields, then $\mathrm{Gal}(K/F)$ is cyclic and generated by σ_q where $|F| = q$, $\sigma_q(\alpha) = \alpha^q$ for $\alpha \in K$
  ↳ called Frobenius automorphism
  ↳ any extension of a finite field is Galois
- **def**: $g \in F[x]$ monic, K splitting field, $g(x) = (x - \alpha_1) \dots (x - \alpha_n)$ $(\alpha_i \in K)$
  $D_g = \prod_{i<j} (\alpha_i - \alpha_j)^2$ discriminant
- **Lemma**: $D_g \neq 0 \Leftrightarrow g$ is separable
- **Lemma**: $D_g \neq 0 \Rightarrow D_g \in F$ Pf: $\mathrm{Gal}(K/F)$ fixes D_g b/c D_g is symmetric in α_i

- $G = \mathrm{Gal}(K/F)$ acts on $\{\alpha_1, \dots, \alpha_n\}$ (roots, by permutation)
  $\Rightarrow G \subseteq S_n$. when does $G \subseteq A_n$?
- Prop: $G \subseteq A_n \Leftrightarrow D_g$ is a square in F.

Modules

R ring w/ id (not necessarily commutative)

- **def**: a (left) **R-module** is an abelian gp $(M,+)$ w/ an action of R, i.e. $R \times M \to M : (r,m) \mapsto r\cdot m$ such that $\forall m,n \in M$, $r,s \in R$
  1) (identity) $1\cdot m = m$
  2) $r\cdot(s\cdot m) = (rs)\cdot m$
  3) (distributive): $(r+s)\cdot m = r\cdot m + s\cdot m$
  4) (distributive): $r\cdot(m+n) = r\cdot m + r\cdot n$
- **lemma**: $0\cdot m = 0$ $\forall m$

  pf: $0\cdot m = (0+0)\cdot m = 0\cdot m + 0\cdot m \Rightarrow 0\cdot m = 0$ $\square$
- **lemma**: $(-1)\cdot m = -m$ $\forall m$

  pf: $0 = 0\cdot m = (-1+1)\cdot m = (-1)\cdot m + 1\cdot m = (-1)\cdot m + m \Rightarrow (-1)\cdot m = m$ $\square$
- **ex**: If $R=F$ is a field then F-module = F-vector space
- **ex**: If $R = \mathbb{Z}$ then $\mathbb{Z}$-module = abelian gp
- **ex**: R is a R-module
- **def**: a **R-submodule** of M is a subgp N of M st. if $n \in N$, $r \in R$ then $r\cdot n \in N$

  ↳ a R-submodule of R is a left ideal
- **ex**: $R = F[x]$ (F field). $F[x]$-module?

  it's a vector space over F, completely determined by how x acts (e.g. $x^2\cdot m = x\cdot(x\cdot m)$)

  $\{F[x]\text{-modules}\} \overset{1\text{-}1}{\longleftrightarrow} \{(V,T) : V \text{ } F\text{-vector space}, T: V \to V \text{ linear transformation}\}$
- **def**: $f: M \to N$ is a R-module homomorphism if $\forall x,y \in M$, $r \in R$.

  1) $f(rx) = r\cdot f(x)$ 2) $f(x+y) = f(x) + f(y)$

  ↳ **ex**: $R = F \Rightarrow$ linear transformations, $R = \mathbb{Z} \Rightarrow$ group homomorphisms

  ↳ $\ker f$, $\operatorname{im} f$ are submodules of M, N respectively
- **def**: $\mathrm{Hom}_R(M,N) = \{R\text{-module homomorphisms } f: M \to N\}$

  ↳ is an abelian group: $f,g \in \mathrm{Hom}_R(M,N)$, $(f+g)(m) \overset{\text{def}}{=} f(m) + g(m)$

  ↳ If R commutative, this makes $\mathrm{Hom}_R(M,N)$ into a R-module
- **note**: If $M=R$, $\{R\text{-module homos}\} \neq \{\text{ring homos } R \to R\}$

  ↳ $f(rs) = rf(s)$ in 1st, $f(rs) = f(r)f(s)$ in 2nd

- ex: $R=\mathbb{Z}$, $f(x)=2x$ is a $\mathbb{Z}$-module homo, but not ring homo
- ex: $R=F[x]$, $f(p(x))=p(x^2)$ is a ring homo, but not a R-module homo
- def: M R-module, N R-submodule, M/N is a R-module (quotient) $r\cdot(x+N)\overset{\text{def}}{=}rx+N$ (can quotient b/c M abelian). is well defined, natural surjective R-module homo $\pi: M\to M/N$ by $x\mapsto x+N$ with $\ker\pi=N$
- 1st Isomorphism Thm: $f:M\to N$ R-mod. homo, $M/\ker f\simeq \operatorname{Im} f$
- Lattice Isomorphism Thm: $\{\text{submodules of } M/N\}\overset{1-1}{\leftrightarrow}\{\text{submodules of } M \text{ containing } N\}$
- def: M R-mod, $S\subseteq M$ $R\cdot S=$ submodule generated by $S=$ smallest submodule containing $S=\{\text{formal sums } \sum r_i x_i\}$
  - ↳ M finitely generated if there is a finite generating set
    - ↳ $R=F \Rightarrow M$ f.g. means finite dim. vector space
- Structure Thm for Finitely Gen. Modules over a PID: R PID, M f.g. R-module, then $M\cong R^r\oplus R/(d_1)\oplus\dots\oplus R/(d_k)$ where d_i are nonzero non units and $d_1|d_2|\dots|d_k$, and $r, d_1,\dots,d_k$ are unique (d_i up to associates)
  - ↳ $r=$ rank of module
  - ↳ $d_i=$ invariant factors
  - ↳ M is the direct sum of cyclic R-modules
- for $R=F[x]$, V finite dim vector space, F field, T F-linear endomorphism of V $(T:V\to V)$, then $\exists$ T-invariant subspaces of V st. $V\cong V_1\oplus V_2\oplus\dots\oplus V_k$ and vectors $v_1,\dots,v_k$, integer pos $m_1,\dots,m_k$ st. $V_i=\operatorname{span}\{v_i, Tv_i,\dots,T^{m_i}v_i\}$.

T as a matrix: basis $v, Tv,\dots,T^m v$, companion matrix

$$\begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \ddots & 0 & -a_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & 1 & 0 & -a_{m-1} \\ 0 & \dots & 0 & 1 & -a_m \end{bmatrix} =: C_{g(x)}, \quad g(x)=a_0+a_1x+\dots+a_mx^m.$$

$g(x)$ is minimal poly and char poly for $C_{g(x)}$

- **Thm**: (Rational Canonical Form): V finite dim F-vec space, T F-linear endomorphism of V. Then $\exists\, \mathcal{B}$ ordered basis of V s.t. T as a matrix w.r.t. $\mathcal{B}$ is

$$\begin{bmatrix} C_{a_1(x)} & & 0 \\ & \ddots & \\ 0 & & C_{a_m(x)} \end{bmatrix}$$

$a_1, \dots, a_m \in F[x]$ nonconstant monic polys, $a_1 | a_2 | \dots | a_m$ - <u>invariant factors</u>

RCF is uniquely determined by T

- **Thm** (Structure Thm, F.G. mod. over PID, elementary divisors): R PID, M f.g. R-mod. $\exists\, r \geq 0$, $p_1, \dots, p_t \in R$, $e_1, \dots, e_t \geq 0$ s.t. $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \dots \oplus R/(p_t^{e_t})$.
  - ↳ uniquely determined
  - ↳ $(p_1^{e_1}), \dots, (p_t^{e_t})$ are <u>elementary divisors</u>.
- <u>def</u>: <u>free R-module</u> of rank m means $M \cong R^m$.
  - ↳ Prop: R PID, R-submodule of a free R-module is free of rank $\leq m$
- <u>Cor</u>: A, B $n \times n$ matrices over F; TFAE:
  1) A, B similar over F ($A = MBM^{-1}$, M invertible)
  2) A, B have same r.c.f.
  3) A, B have same invariant factors.
- Cor: A, B $n \times n$ over F field, K/F field extension. A, B similar over K iff similar over F
- <u>Thm</u>: (Cayley-Hamilton): the minimal poly of A divides the char poly of A (equiv to char poly annihilates A)
- <u>Thm</u>: char poly divides a power of the minimal polynomial
- **Thm**: A $n \times n$ over F. $xI - A$ in $F[x]$, compute SNF by putting into diagonal:

$$\begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & a_1(x) & \\ & & & & \ddots \\ 0 & & & & a_m(x) \end{bmatrix}$$

$a_1, \dots, a_m \in F[x]$ nonconstant, monic, $a_1 | \dots | a_m$.

$a_1, \dots, a_m$ are invariant factors of A.

- <u>Thm</u>: A $m \times n$ over R PID. $\Delta_0(A) = 1$, $1 \leq k \leq \min(m,n)$, $\Delta_k(A) = \gcd$ of dets of all $k \times k$ submatrices. Then $\Delta_k(A) = d_1 \dots d_k$, d_i's diagonal ents of SNF.
- Cor: A $n \times n$ over F field. Invariant factors of A are Δ_i / Δ_{i-1} for $i = 0, \dots, n$ where $\Delta_0 = 1$, $\Delta_k = \gcd$ of det of all $k \times k$ submats of $xI - A$.

- Thm (Jordan Canonical Form): A $n \times n$ matrix field F, F contains all eigenvalues of A.

1) A is similar to a matrix in JCF: $\exists$ $n \times n$ P invertible over F st
$PAP^{-1} = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{pmatrix}$, each diagonal block
J_i is elementary Jordan matrix: $\longrightarrow$ $\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & \ddots & \lambda \end{pmatrix}$

2) $\{$elementary divisors of $A\}$ $\leftrightarrow$ $\{$Jordan blocks $J_i\}$
$(x-\lambda)^k$ $\leftrightarrow$ $k \times k$ elementary block, e.val λ

3) JCF unique up to ordering Jordan blocks.

- Cor: A $n \times n$, F field, F contains e.vals of A. TFAE:

1) A diagonalizable over F
2) JCF (A) is diagonal
3) minimal poly of A is square free.