Algebra - Theorems & definitions : GROUPS

Permutations :

- Disjoint permutations commute
- Two permutations have same cycle structure $\Leftrightarrow$ they are conjugate
- α, β same parity $\Rightarrow \alpha\beta$ even
  α, β diff. parity $\Rightarrow \alpha\beta$ odd
- an n-cycle & transposition will generate all of S_n
- r-cycle is in $A_n \Leftrightarrow r$ is odd
- if α is a disj. product of r_i-cycles, $\text{ord}(\alpha) = \text{lcm}(r_i)$

General

- there are $\frac{n(n-1)\cdots(n-r+1)}{r}$ r-cycles in S_n
- $\phi(p) = p-1$, $\phi(p^k) = p^k - p^{k-1}$
- (Fermat) : $a^p \equiv a \pmod p$; (Euler) : $\gcd(r,m)=1 \Rightarrow r^{\phi(m)} \equiv 1 \pmod m$
- $H, K \leq G$ and one normal, then $HK \leq G$. (both normal $\Rightarrow HK \trianglelefteq G$)
- Isomorphism Thms : ① $f: G \to H$ hom $\Rightarrow G/\ker f \cong \text{im} f$
  ② $H, K \leq G$, $H \trianglelefteq G \Rightarrow H \cap K \trianglelefteq K$ & $K/(H\cap K) \cong HK/H$
  ③ $H, K \trianglelefteq G$, $K \subseteq H$ $\Rightarrow H/K \trianglelefteq G/K$ & $(G/K)/(H/K) \cong G/H$
- Product formula : $H, K \leq G \Rightarrow |HK| \cdot |H \cap K| = |H| \cdot |K|$
- Correspondence : $K \trianglelefteq G$, $\pi: G \to G/K$. Then: $\text{Sub}(G;K) \longleftrightarrow \text{Sub}(G/K)$
  $S \longmapsto \pi(S) = S/K$
- Rep'n on cosets : $H \leq G$, $[G:H] = n$, then $\exists \varphi: G \to S_n$ with $\ker\varphi \subseteq H$

GROUP ACTIONS

$G \circlearrowright X$ by $(g,x) \mapsto gx$;
orbit: $\mathcal{O}(x) = \{gx : g \in G\} \subseteq X$
stabilizer: $G_x = \{g \in G : gx = x\} \leq G$.

- $|X| = \sum_i |\mathcal{O}(x_i)|$
- $|\mathcal{O}(x)| = [G : G_x]$

$G \circlearrowright G$ by $(g,h) \mapsto ghg^{-1}$ conjugation.
$\mathcal{O}(x) = x^G = \{y \in G : y = gxg^{-1} \text{ for } g \in G\}$ conj class
$C_G(x) = \{g \in G : gxg^{-1} = x\}$ centralizer
$N_G(H) = \{g \in G : gHg^{-1} = H\}$ normalizer $\rightarrow H \trianglelefteq N_G(H)$

- $H \leq G \Rightarrow$ • $C_G(H) \trianglelefteq N_G(H)$
  • $N_G(H)/C_G(H) \hookrightarrow \text{Aut}(H)$
- $|x^G| = [G : C_G(x)]$
- $|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$

* An action is transitive if there is only one orbit
$(\forall x, y \in X \ \exists g \in G \text{ s.t. } gx = y)$

SIMPLE GROUPS :

- abelian G simple $\Leftrightarrow$ finite, prime order
- finite p-group simple $\Leftrightarrow$ order p.

Finite Gen Abel. Groups

$G \cong \mathbb{Z}^N \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{e_k})$ (p_i not nec. distinct)

$G \cong \mathbb{Z}^N \oplus G_{p_1} \oplus \cdots \oplus G_{p_k}$ (p_i distinct here; p-primary parts)

Sylow: $P \leq G$ Sylow p-subgrp. ($|P| = p^k$)

(1) Every Sylow p-subgrp is conj. to P

(2) $r_p = \#$ Sylow p-s.g. $\Rightarrow r_p \equiv 1 \pmod p$ and $r_p \mid \frac{|G|}{p^k}$

(3) $P \trianglelefteq G \iff r_p = 1$

Quotients of subgps of solvables are solvable

Solvable Groups

If G has normal series: $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$, $G_{i+1} \trianglelefteq G_i$; G_i/G_{i+1}

G solvable if $G_i/G_{i+1} \cong \mathbb{Z}_{p_i}$ (only for G finite)

BURNSIDE: Every grp order $p^a q^b$ solvable

- Every finite p-group is solvable
- Commutator: $G' = \{xyx^{-1}y^{-1} : x, y \in G\}$

  Derived series: $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots$ where $G^{(1)} = G'$ and $G^{(i+1)} = (G^{(i)})'$

  FACTS: (1) Finite grp solvable $\iff \exists n$ with $G^{(n)} = 1$

  (2) — " — $\iff$ has normal series w/ abelian factors
- G/H & H solvable $\Rightarrow G$ solvable

Semidirect product

If $G = N \rtimes H$ ($N \trianglelefteq G$), have hom. $\phi: H \to \mathrm{Aut}(N)$

$h \mapsto \sigma_h(n) = hnh^{-1}$

$G = N \rtimes H$ if $G = NH$, $N \cap H = \{1\}$

Facts:

- Group order p^2 is abelian
- Group order pq ($q < p$), $q \nmid p-1$ is cyclic
- Subgroup index smallest prime dividing order of grp is normal.

$(\mathbb{Z}_{p^2})^\times \cong \mathbb{Z}_{p(p-1)}$

ZORN'S LEMMA: If every chain in a poset has an upper bound then $\exists$ a maximal elt

$\varphi: G \to S_{|G|}$, $g \mapsto \gamma_g(h) = gh$

γ_g has fixed pt $\iff g = e$. Hence γ_g is $\frac{|G|}{\mathrm{ord}(g)}$ cycles of length $\mathrm{ord}(g)$

$\mathrm{ord}(g)$ — $m = \mathrm{ord}(g)$

$\gamma_g : (e\ g\ g^2 \cdots g^{m-1})(h\ gh\ g^2h \cdots g^{m-1}h) \cdots (\cdots)$

$|G|$

(regular rep'n)

RINGS and MODULES

- k field ⇒ k[x] P.I.D.

irreducibility:
- f(x) ∈ k[x], deg f = 2 or 3 ; f(x) irred ⟺ f(x) has no roots
- Rational roots: $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, then every rational root $\frac{b}{c}$ of f has $b \mid a_0$ and $c \mid a_n$. (monic ⇒ all rational roots are integers)
- For f(x) ∈ ℤ[x], If f(x) irred over $\mathbb{F}_p[x]$, then f(x) irred in ℚ[x].
- For f(x) ∈ ℤ[x], If ∃c∈ℤ with g(x+c) irred in ℤ[x] ⇒ g(x) irred in ℚ[x]
- Eisenstein: $f(x) = a_0 + a_1x + \cdots + a_nx^n$. If ∃p with $p \mid a_i$, $i<n$; $p \nmid a_n$; $p^2 \nmid a_0$ ⇒ f(x) irreducible in ℚ[x].

Correspondence: Ideals in R containing I ⟷ Ideals in R/I : $J \longmapsto J/I$

- I ⊆ R prime ⟺ R/I domain
- I ⊆ R maximal ⟺ R/I field
- maximal ideals are prime.
- R PID: I prime ⟺ I = (p), p irred.
- f: R → S ring hom. If P ⊆ S prime, then $f^{-1}(P)$ prime.
- R PID : Every prime ideal is maximal.
- PID ⇒ UFD ; R UFD ⇒ R[x] UFD

(fin-gen R-algebra for R noeth is itself noeth)

(I max, then I^k / I^{k+1} is fin-dim ∀k≥1)

(ACC) $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stops ⟺ Every ideal fin gen ⟺ NOETHERIAN

(DCC) $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ stops ⟺ ARTINIAN

- R noeth.: for I ⊆ R, ∃M max s.t. I ⊆ M.
- R noeth, I ⊆ R ⇒ R/I noeth.
- HILBERT BASIS : R comm, noeth ⇒ R[x] noeth
- R noeth ⇒ R has finitely many minimal ideals

ARTIN-WEDDERBURN: R s.s. ⇒ $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$

Maximal ideal M has M/Mk fin-dim for some k.

A a k-module. $k \subseteq k'$. Then $A \otimes_k k'$ extension of scalars of A (now k'-module)

VARIETIES & NULLSTELLENSATZ

- $Var(I) = \{\alpha \in k^n : f(\alpha) = 0 \ \forall f \in I\}$
- $Id(A) = \{f(x) \in k[x] : f(a) = 0 \ \forall a \in A\}$ $(A \subseteq k^n)$
- $\sqrt{I} = \{r \in R : r^m \in I \text{ for some } m \geq 1\}$
- $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$; I, J radical $\Rightarrow I \cap J$ radical.

Max ideals R ↕ # pts in variety of I

- **Nullstellensatz**: $k = \bar{k}$, $I \subseteq k[x]$. Then $Id(Var(I)) = \sqrt{I}$.
- Every maximal ideal in $\mathbb{C}[x_1, \dots, x_n]$ has form $(x_1 - a_1, \dots, x_n - a_n) = Id(a)$
- $\mathbb{C}[x_1, \dots, x_n]/\sqrt{I} \cong \mathbb{C}^{|Var I|}$ when $|Var I| < \infty$

PRIME ideals are radical

$Var I \cap Var J = Var I + J$

MODULES

- R-mod M simple $\Leftrightarrow M \cong R/I$ some maximal $I \subseteq R$.
- $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ short exact ($\operatorname{im}\alpha = \ker\beta$)
  $\Rightarrow A \cong \operatorname{im}\alpha$ & $B/\operatorname{im}\alpha \cong C$; If split, $B \cong A \oplus C$
- R noeth $\Leftrightarrow$ every submod of R-mod is fin-gen.

Art ⇓ Noeth

- Free mod: R-mod free of $\cong \bigoplus_{i \in I} R$
  - $\mathbb{Z}/p_i \, e_i \otimes \mathbb{Z}/q_j \, f_j \cong \mathbb{Z}/\gcd(p_i, q_j)$
- Tensor products: • Distributive: $A \otimes (\bigoplus B_i) = \bigoplus A \otimes B_i$
  • $\dim(V \otimes W) = \dim V \cdot \dim W$ • $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ • $R \otimes_R M \cong M$ (M R-mod)
- R-mod M has comp series $\Leftrightarrow M$ has both ACC & DCC
- A k-algebra is fin-gen of $\exists$ surj. $k[x_1, \dots, x_n] \twoheadrightarrow A$
- JACOBSON radical: $J(R) = \bigcap_{I \subseteq R \text{ max}} I$
- NAKAYAMA lemma: A fin-gen R-mod & $J(R) \cdot A = A \Rightarrow A = \{0\}$.
  - $I \subseteq J(R)$ $\forall$ nilpotent $I \subseteq R$.
  - R artinian $\Rightarrow J(R)$ nilpotent
  - M R-mod s.s. $\Leftrightarrow$ every submod of M is direct summand
- R semisimple $\Leftrightarrow$ artinian & Jacobson s.s.
- **Maschke**: if $\operatorname{char} k \nmid |G|$ then kG semisimple

GALOIS THEORY

- $[E:k] = |Gal(E/k)|$
- $f \in k[x]$, $\deg f = n \Rightarrow Gal(E_f/k) \leq S_n$
- All polynomials in char 0 have no repeated roots (sep.)

* E/k spl. fld for $\deg f = n$. If f irred $\Rightarrow n \mid |Gal(E/k)|$

- $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n \cong \langle \sigma(u) = u^p \rangle = \langle Frob \rangle$
- E/k spl. fld for sep. f. f irred $\Leftrightarrow Gal(E/k)$ C roots of f trans. freely

---

Normal extensions: $k \subseteq B \subseteq E$; B/k, E/k normal. Then: $\begin{cases} Gal(E/B) \trianglelefteq Gal(E/k) \\ Gal(E/k)/Gal(E/B) \cong Gal(B/k) \end{cases}$

(splitting field for some poly)

$f(x)$ solvable $\Rightarrow Gal(E/k)$ is solvable. ($\Leftarrow$ true in char 0)

Fundamental Theorem of Galois Theory:

E/k finite, Galois. $G = Gal(E/k)$.

① $H \leq G \longleftrightarrow k \subseteq E^H \subseteq H$

② $\begin{cases} k \subseteq B \subseteq E \Rightarrow E^{Gal(E/B)} = B \\ H \leq G \Rightarrow Gal(E/E^H) = H \end{cases}$

③ $k \subseteq B \subseteq E \Rightarrow [B:k] = [G : Gal(E/B)]$

$H \leq G \Rightarrow [G:H] = [E^H : k]$

④ $k \subseteq B \subseteq E$; B/k Galois ext $\Leftrightarrow Gal(E/B) \trianglelefteq Gal(E/k)$

$$N(u) = \prod_{\sigma \in Gal} \sigma(u)$$

$$T(u) = \sum_{\sigma \in Gal} \sigma(u)$$

- If B/k is finite, sep then $\exists u \in B$ s.t. $B = k(u)$
- In char 0, EVERY finite ext is simple.

IVT: If $f(x)$ cont on $[a,b]$ and N between $f(a)$ & $f(b)$ then $\exists c \in (a,b)$ s.t. $f(c) = N$.

MVT: If $f(x)$ cont on $[a,b]$, diff on (a,b), then $\exists c \in (a,b)$ s.t. $f'(c) = \dfrac{f(b)-f(a)}{b-a}$

$[\mathbb{Q}(w) : \mathbb{Q}] = \deg$ minpoly of w; $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$

MODULES

- **Free**: an R-mod M is free if it is $\cong$ to direct sum of copies of R
- **Projective**: an R-mod P is projective if it is direct summand of a free module (i.e. $\exists Q$ s.t. $Q \oplus P$ is free)

Prop: R-mod A is proj. $\Leftrightarrow \exists (a_i)_{i\in I} \subseteq A$ & R-maps $(\varphi_i : A \to R)_{i\in I}$ s.t. (i) for each $x \in A$, almost all $\varphi_i(x) = 0$
(ii) for each $x \in A$, we have $x = \sum_{i\in I} (\varphi_i x) a_i$

Prop: R-mod P proj $\Leftrightarrow$ every s.e.s. $0 \to A \to B \to P \to 0$ is split.

FT of Mod/PID:
R PID, every fin-gen R-mod M is of form
$M = R^k \oplus R/(c_1) \oplus \cdots \oplus R/(c_t)$, $t \geq 1$, $c_1 | c_2 | \cdots | c_t$.

Irreducible reps of kG: kG s.s. $\Rightarrow kG \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_r}(k)$
r = # of irred. reps (simple mods)
n_i = dim. of simple mods.
Thm: the # of inequiv. simple kG-mods is equal to the # of conjugacy classes in G, and $|G| = n_1^2 + \cdots + n_r^2$

LOCALIZATION $R_M = \{\frac{a}{b} : a \in A, b \in A \setminus M\} / \frac{a}{b} \sim \frac{c}{d} \Leftrightarrow s(ad-bc) = 0$ for some $s \in A \setminus M$.

* **Prop**: M an R-module. TFAE: (1) $M = 0$ (2) $M_p = 0$ $\forall$ prime ideals $P \subseteq R$ (3) $M_m = 0$ $\forall$ max ideals $m \subseteq R$

- M char $N \trianglelefteq G \Rightarrow M \trianglelefteq G$

groups

S an R-mod; then $S \cong S \otimes_R R$

[Flat]: A R-mod. Then A Flat if for all L, M, N R-mod

$0 \to L \to M \to N \to 0$ exact

$\Rightarrow 0 \to A \otimes L \to A \otimes M \to A \otimes N \to 0$ exact.

- PROJECTIVE modules are Flat
- $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

- If $|P| = p^2$; then $P \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \otimes \mathbb{Z}_p$, so: $|Aut(P)| = p(p-1)$ or $p(p-1)^2(p+1)$
- $Aut(\mathbb{Z}_p \oplus \mathbb{Z}_p) \cong GL_2(\mathbb{F}_p)$
- $\mathbb{Z}$ modules: projective $\Leftrightarrow$ free.

$S_n = \langle a, b$ and $a^n = b^2 = 1$, $ab = ba^{n-1} \rangle$

$D_{2n} = \langle a, b : a^2 = b^2 = 1$, $aba = b^{-1} \rangle$

Isomorphism for modules:

(1st) $S, T \subseteq M$ sub R-mods, then $S/S \cap T \cong S+T/T$

(3rd) $(M/T)/(S/T) \cong M/S$