PMATH 347 (Groups & Rings)[-0.4em]

Group Theory

Operations, identity, inverses

- Binary op on X: $\star : X \times X \to X$. k-ary op: $X^k \to X$.
- Associative: $x\star(y\star z) = (x\star y)\star z$. If associative, all bracketings of $a_1 \star \cdots \star a_n$ agree.
- Commutative/abelian: $a \star b = b \star a$.
- Identity e: $e \star x = x \star e = x$ (unique).
- Left inverse of x: $y_L \star x = e$; right inverse: $x \star y_R = e$. If associative & e exists and both exist, then $y_L = y_R =: x^{-1}$.
- Inverses: $(ab)^{-1} = b^{-1}a^{-1}$; $(x^{-1})^{-1} = x$; $e^{-1} = e$.
- Cancellation: if a has left inverse and $au = av$ then $u = v$ (sim. right).

Groups, notation, order

Group $(G, \cdot)$: associative, identity e, every g invertible. Abelian $\iff gh = hg$.

- Powers: $g^0 = e$, $g^n = g\cdots g$ $(n \geq 1)$, $g^{-n} = (g^{-1})^n$, and $g^m g^n = g^{m+n}$.
- Order: $|g| = \min k \geq 1 : g^k = e$ (else ∞). If $g^n = e$ then $|g| \mid n$.
- Examples: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$; $R^\times$ (units) under $\cdot$; S_X bijections $X \to X$ under $\circ$; $S_n := S_{1,\ldots,n}$, $|S_n| = n!$.
- $GL_n(R)$ invertible matrices, identity I_n; $SL_n(R) = \ker(\det : GL_n(R) \to R^\times)$.

Dihedral group

Regular n-gon symmetries: D_{2n} (order $2n$).

$$D_{2n} = \{s^i : 0 \leq i < n\} \cup \{s^i r : 0 \leq i < n\}, \quad s^n = e,\ r^2 = e,\ rs = s^{-1}r.$$

Hence any element is $s^i r^j$ with $0 \leq i < n$, $j \in \{0, 1\}$; $|s| = n$, $|r| = 2$.

Subgroups & generation

$H \leq G$ iff (i) $H \neq \emptyset$ and (ii) $gh^{-1} \in H$ for all $g, h \in H$.

- Intersections: if $\{H_\alpha\}$ is a nonempty family of subgroups, $\bigcap_\alpha H_\alpha \leq G$.
- Generated subgroup: $\langle S\rangle = \bigcap\{H \leq G : S \subseteq H\} = \{s_1 \cdots s_k : s_i \in S \cup S^{-1},\ k \geq 0\}$.
- Cyclic: $G = \langle a\rangle$; then $\langle a\rangle = \{a^i : i \in \mathbb{Z}\}$ and if $|a| = n < \infty$ then $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$.
- Subgroups of cyclic groups are cyclic; $|\langle a\rangle| = |a|$.
- $\mathbb{Z}/n\mathbb{Z}$: $|[a]| = \dfrac{n}{\gcd(a,n)}$; $\langle[a]\rangle = \mathbb{Z}/n\mathbb{Z} \iff \gcd(a, n) = 1$.
- For each $d \mid n$, unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d: $\langle[n/d]\rangle$.

Homomorphisms & isomorphisms

Homomorphism $\varphi : G \to H$: $\varphi(gh) = \varphi(g)\varphi(h)$.

- $\varphi(e) = e$, $\varphi(g^{-1}) = \varphi(g)^{-1}$, $\varphi(g^n) = \varphi(g)^n$.
- $\operatorname{Im}\varphi := \varphi(G) \leq H$; $\ker\varphi := \varphi^{-1}(e) \trianglelefteq G$.
- Preimage: if $K \leq H$ then $\varphi^{-1}(K) \leq G$. Image: if $L \leq G$ then $\varphi(L) \leq H$.
- $\varphi(\langle S\rangle) = \langle\varphi(S)\rangle$.
- Isomorphism: bijective homomorphism. If $G \cong H$ then $|G| = |H|$ (finite), abelian preserved, and $|g| = |\varphi(g)|$.
- Cyclic classification: cyclic G isomorphic to $\mathbb{Z}$ (if $|G| = \infty$) or $\mathbb{Z}/n\mathbb{Z}$ (if $|G| = n$).

Cosets, Lagrange, index

For $H \leq G$, left coset $gH = \{gh : h \in H\}$, right coset Hg.

- Coset criteria (equivalent): $gH = kH \iff g^{-1}k \in H \iff gH \cap kH \neq \emptyset$; cosets partition G.
- Index: $[G : H] = |G/H|$ (number of left cosets).
- **Lagrange:** if G finite and $H \leq G$, then $|G| = |H|\,[G : H]$; hence $|H| \mid |G|$ and $|g| \mid |G|$ for all $g \in G$.

Quotient groups & universal property

Normal $N \trianglelefteq G$: $gNg^{-1} = N$ (equiv. $gN = Ng$ for all g).

- Product of subsets: $S\cdot T = \{st : s \in S, t \in T\}$. If $N \trianglelefteq G$, then $(gN)(hN) = (gh)N$ (well-defined).
- **Quotient:** if $N \trianglelefteq G$, then G/N is a group with identity N, inverse $(gN)^{-1} = g^{-1}N$, and quotient map $q : G \to G/N$, $q(g) = gN$ is a homomorphism with $\ker q = N$.
- $N \trianglelefteq G \iff N = \ker(\varphi)$ for some homomorphism $\varphi : G \to K$.
- **Universal property:** if $\phi : G \to K$ and $N \subseteq \ker\phi$, then $\exists!\ \psi : G/N \to K$ with $\phi = \psi \circ q$.

Isomorphism theorems (groups)

1st: $\phi : G \to K$ hom. $\Rightarrow G/\ker\phi \cong \operatorname{Im}\phi$ via $g\ker\phi \mapsto \phi(g)$. **Correspondence:** $\phi : G \twoheadrightarrow K$ gives bijection $\{H' \leq G : \ker\phi \leq H'\} \leftrightarrow \{H \leq K\}$ by $H' \mapsto \phi(H')$ and $H \mapsto \phi^{-1}(H)$. Normality and inclusion preserved. **2nd:** if $H, K \leq G$ and $H \leq \mathrm{N}_G(K)$, then $HK \leq G$, $K \trianglelefteq HK$, $H\cap K \trianglelefteq H$, and $H/(H\cap K) \cong HK/K$ via $h(H\cap K) \mapsto hK$. **3rd:** $N \trianglelefteq G$, $N \leq K \trianglelefteq G \Rightarrow (G/N)/(K/N) \cong G/K$.

Group actions

Action (left): $G \times X \to X$, $(g, x) \mapsto g \cdot x$ with $(gh)\cdot x = g\cdot(h\cdot x)$ and $e \cdot x = x$. Right action: $X \times G \to X$, $(x, g) \mapsto x \cdot g$; convert to left via $g \cdot x := x \cdot g^{-1}$.

- Invariant $Y \subseteq X$: $g \cdot y \in Y$ for all g, y; then action restricts to Y.
- Induced actions: on 2^X by $g \cdot S = g \cdot s : s \in S$; on $Fun(X, Y)$ by $(g \cdot f)(x) = g \cdot f(g^{-1} \cdot x)$ (often Y trivial: $(g \cdot f)(x) = f(g^{-1} \cdot x)$).
- Regular action of G on itself: left mult. $g\cdot h = gh$; also G acts on G/H by $g \cdot (kH) = (gk)H$.
- Permutation representation: action on finite $|X| = n$ gives hom. $\phi : G \to S_X \cong S_n$ by $\phi(g) = \ell_g$ where $\ell_g(x) = g \cdot x$; conversely any $\phi : G \to S_X$ defines $g \cdot x = \phi(g)(x)$.
- Kernel of action: $\ker\phi = g : \ell_g = \mathrm{id}_X = \bigcap_{x\in X} G_x$. Faithful $\iff \ker\phi = e$.
- **Cayley:** left regular action is faithful $\Rightarrow G \hookrightarrow S_G$; if $|G| = n$ then $G \leq S_n$.

Orbits, stabilizers, class equation, Cauchy

Orbit: $\mathcal{O}_x = g \cdot x : g \in G$; orbits are equivalence classes ($x \sim y \iff \exists g : g \cdot x = y$). Transitive $\iff$ some (equiv. every) orbit is X. Stabilizer: $G_x = g \in G : g \cdot x = x \leq G$.

- **Orbit–stabilizer:** $\phi : G/G_x \to \mathcal{O}_x$, $gG_x \mapsto g\cdot x$ bijective; hence $|\mathcal{O}_x| = [G : G_x]$ (finite case $|\mathcal{O}x| = \frac{|G|}{|G_x|}$).
- Conjugation action: $g \cdot k = gkg^{-1}$. Conjugacy class $\mathrm{Conj}(k) = gkg^{-1} : g \in G$; centralizer $\mathrm{C}_G(k) = g : gk = kg$; $|\mathrm{Conj}(k)| = [G : \mathrm{C}_G(k)]$.
- Center: $Z(G) = z : zg = gz\ \forall g$; $|\mathrm{Conj}(k)| = 1 \iff k \in Z(G)$.
- **Class equation:** if T reps of conjugacy classes not in $Z(G)$, then $|G| = |Z(G)| + \sum t \in T|\,\mathrm{Conj}(t)|$.
- **Cauchy:** if G finite and prime $p \mid |G|$, then $\exists g \in G$ with $|g| = p$.
- If G finite and $H \leq G$ with $[G : H] = p$ (smallest prime dividing $|G|$), then $H \trianglelefteq G$.

Finite abelian groups & small orders

- $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if $\gcd(m, n) = 1$.
- **Classification (finite abelian):** G finite abelian $\cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$ (prime powers), with invariant factors $a_1 \leq \cdots \leq a_k$ unique up to order.
- Groups of small order: $|G| = 2, 3, 5, 7 \Rightarrow G \cong \mathbb{Z}_{|G|}$; $|G| = 4 \Rightarrow \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$; $|G| = 6 \Rightarrow \mathbb{Z}_6$ or $D_6 \cong S_3$.

Sylow

Automorphism: isomorphism $G \to G$; conjugation map $c_g(h) = ghg^{-1} \in \mathrm{Aut}(G)$. p-group: order p^k; Sylow p-subgroup: subgroup $P \leq G$ with $|P| = p^k$ where $|G| = p^k m$, $p \nmid m$.

Sylow theorems: if $|G| = p^k m$ $(p \nmid m)$: (1) $\mathrm{Syl}_p(G) \neq \emptyset$. (2) Any p-subgroup Q is contained in some Sylow p-subgroup; all Sylow p-subgroups are conjugate. (3) $n_p := |\mathrm{Syl}_p(G)| = [G : \mathrm{N}_G(P)]$ for $P \in \mathrm{Syl}_p(G)$; hence $n_p \mid |G|$ and $n_p \equiv 1 \pmod p$.

Cor.: $n_p = 1 \Rightarrow$ unique Sylow p-subgroup, normal. If $|G| = pq$ with primes $p < q$, then Sylow q-subgroup is normal.

Ring Theory

Rings, subrings, units

Ring $(R, +, \cdot)$: $(R, +)$ abelian group, $\cdot$ associative, distributive laws; *in this course: unital* ($\exists 1$).

- $0a = a0 = 0$; $(-a)b = -(ab) = a(-b)$; $(-a)(-b) = ab$; $-x = (-1)x$. If $1 = 0$ then $R = 0$ (zero ring).
- Commutative ring: $ab = ba$. Center $Z(R) = x : xy = yx\ \forall y$ is a subring.
- Subring $S \subseteq R$: subgroup of $(R, +)$, closed under multiplication, and contains 1 (otherwise *non-unital subring*).
- Unit: $u \in R^\times$ iff $\exists u^{-1}$ with $uu^{-1} = 1$.

Ring homomorphisms

Homomorphism $\varphi : R \to S$ (unital): $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(1_R) = 1_S$ (drop last $\Rightarrow$ non-unital hom).

- $\ker\varphi$ is an ideal; $\operatorname{Im}\varphi$ a subring; φ injective $\iff \ker\varphi = 0$.
- If φ surjective and $I \trianglelefteq R$ ideal then $\varphi(I) \trianglelefteq S$.
- Group rings: for group G and ring R, $RG = \sum_{g\in G} a_g g : a_g \in R$, finite support; group hom $\phi : G \to H$ induces ring hom $RG \to RH$, $\sum a_g g \mapsto \sum a_g \phi(g)$.

Polynomial rings

$R[x] = \{\sum_{i=0}^k a_i x^i\}$ with $(a_i) + (b_i) = (a_i + b_i)$ and convolution product: $(a_i) \cdot (b_i) = (c_k)$ where $c_k = \sum_{i=0}^k a_i b_{k-i}$.

- $1_{R[x]} = 1 \cdot x^0$; if R commutative then $R[x]$ commutative.
- $\deg(0) = -\infty$, $\deg(\sum_{i=0}^k a_i x^i) = \max\{i : a_i \neq 0\}$; leading term $a_k x^k$.
- Multivariable: $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.
- Evaluation (commutative R): $\mathrm{ev}_\alpha : R[x] \to R$, $p \mapsto p(\alpha)$ is a ring hom; similarly $\mathrm{ev}_\alpha : R[x_1, \ldots, x_n] \to R$.

Ideals

Ideal $I \subseteq R$: additive subgroup of R with $RI, IR \subseteq I$.

- $\{0\}, R$ ideals; $I = R \iff 1 \in I$.
- Principal ideal: $(x) = Rx = xR$ (commutative: xR).
- Generated ideal: for $S \subseteq R$, $(S) = \bigcap\{I \trianglelefteq R : S \subseteq I\}$. If R commutative and $S = \{f_1, \ldots, f_n\}$ then $(S) = f_1R + \cdots + f_nR$.
- Ideal sum: $I + J$ ideal; also $I \cap J$ ideal; product $IJ = \{\sum i_k j_k\}$ ideal (commutative).
- In $R[x]$ (commutative): $\ker(\mathrm{ev}_c) = (x - c)$; any h with $\deg h \leq n$ can be written $h = \sum_{i=0}^n a_i(x - c)^i$.
- Not all ideals principal: $(x, y) \subseteq \mathbb{Z}[x, y]$.

Quotient rings

If $I \trianglelefteq R$, then R/I with $[a] + [b] = [a + b]$, $[a], [b] = [ab]$, $1 = [1]$ is a ring; quotient map $q : R \to R/I$ is a ring hom with $\ker q = I$.

- $I \trianglelefteq R \iff I = \ker(\varphi)$ for some ring hom $\varphi : R \to S$.
- Example: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(n)$.
- **Universal property:** $\phi : R \to S$ ring hom, $I \trianglelefteq R$, then $\exists!\ \psi : R/I \to S$ with $\phi = \psi \circ q \iff I \subseteq \ker\phi$.
- Construction pattern: $S = R[x_1, \ldots, x_n]/(p_1, \ldots, p_m)$ forces $p_i(\bar{x}_1, \ldots, \bar{x}_n) = 0$. Example: $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$ (send $x \mapsto i$).

Isomorphism theorems (rings)

1st: $\phi : R \to S$ ring hom $\Rightarrow R/\ker\phi \cong \operatorname{Im}\phi$. **Correspondence:** $\phi : R \twoheadrightarrow S$ gives bijection between ideals of S and ideals of R containing $\ker\phi$ via $J \mapsto \phi^{-1}(J)$. **2nd (standard):** if $A \leq R$ subring and $I \trianglelefteq R$ ideal, then $A/(A \cap I) \cong (A + I)/I$. **3rd:** $I \subseteq J \trianglelefteq R$ ideals $\Rightarrow (R/I)/(J/I) \cong R/J$.

Fields, maximal ideals, Zorn

Field: commutative ring with $1 \neq 0$ and $R^\times = R \setminus \{0\}$.

- In $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, $[m] \in \mathbb{Z}_n^\times \iff \gcd(m, n) = 1$; $\mathbb{Z}_n$ field $\iff n$ prime.
- R (commutative) is a field $\iff 1 \neq 0$ and the only ideals are $\{0\}, R$.
- Maximal ideal I: $I \neq R$ and only ideals containing I are I, R; equivalently R/I field.
- Prime ideal P: $P \neq R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$; equivalently R/P integral domain.
- Zorn (used): if every chain of proper ideals has an upper bound (union), then R has a maximal ideal. Hence if $1 \neq 0$ then $\exists$ field K and hom $R \to K$ (take $K = R/I$ for maximal I).

Integral domains & fractions

Zero divisor: $x \neq 0$ with $\exists y \neq 0$ s.t. $xy = 0$. Integral domain (domain): commutative, $1 \neq 0$, no zero divisors.

- If R domain and $f, g \in R[x]$, then $\deg(fg) = \deg f + \deg g$; hence $R[x]$ domain.
- In a domain, $x^2 = t^2 \Rightarrow x = \pm t$.
- Field of fractions $\mathrm{Frac}(R)$ for domain R: equivalence on $R \times (R \setminus \{0\})$ by $(a, b) \sim (c, d) \iff ad = bc$; elements $\frac{a}{b}$; yields a field containing an isomorphic copy of R via $a \mapsto \frac{a}{1}$. For field K, $\mathrm{Frac}(K[x]) = K(x)$ (rational functions).

CRT (ring form)
If $I, J \trianglelefteq R$ are comaximal ($I + J = R$), then

$$R/(I\cap J) \cong R/I \times R/J, \qquad r \mapsto (r \bmod I,\ r \bmod J),$$

and (commutative) $I \cap J = IJ$. For pairwise comaximal $I_1, \dots, I_k$, $R/(\cap I_i) \cong \prod R/I_i$. Example: if $\gcd(m, n) = 1$, then $\mathbb{Z}/(mn) \cong \mathbb{Z}/m \times \mathbb{Z}/n$.

PID, gcd, factorization, UFD
PID: commutative domain where every ideal is principal. Divisibility: $f \mid g \iff g \in (f) \iff \exists h : g = fh$; associates $x \sim y \iff y = ux$ with $u \in R^\times$.

- $\sim$ is an equivalence relation; if u unit then any divisor of u is a unit.
- gcd: $d = \gcd(a, b)$ means $d \mid a, b$ and any common divisor divides d (unique up to units). In a commutative ring,

  $$d \text{ is gcd of } (a, b) \iff (a, b) = (d) \iff d = xa+yb \text{ and } d \mid a, b.$$

- If $R[x]$ is a PID, then R is a field (use $\mathrm{ev}_0 : R[x] \to R$, $\ker = (x)$).
- Prime element (R domain): $p \neq 0$, $p \notin R^\times$, and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Irreducible: $p = ab \Rightarrow a$ or b unit. Then prime $\Rightarrow$ irreducible; in a PID, irreducible $\Rightarrow$ prime.
- Prime ideals: p prime element $\iff$ (p) prime ideal; associates preserve prime/irreducible.
- UFD: domain where every nonzero nonunit factors into irreducibles and factorization is unique up to associates/order.
- **UFD criteria:** if every irreducible is prime, then factorization (when it exists) is unique. Also: R is a UFD $\iff$ (i) all irreducibles are prime and (ii) ACC on principal ideals (ACCP).
- In a UFD, if $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$, then $\gcd(a, b) \sim \prod p_i^{\min(a_i, b_i)}$. PID $\Rightarrow$ UFD.
- Non-UFD examples: $\mathbb{Q}[x, y, z, w]/(xy - zw)$; $\mathbb{Z}[i\sqrt{5}]$ with $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.