Groups

Group: a set with a composition law which satisfies closure, associativity, identity, and inverse.

Order of a Group: the number of elements in the group; also the smallest n such that $a^n = e$

Group homomorphism: a map $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$

Bijection: a surjective and injective mapping

1. Surjective (onto) - every element in H is mapped to by some element in G ($\forall h \in H, \exists g \in G$ such that $\phi(g) = h$)
2. Injective (one-to-one) - every element in H is mapped to by at most one element in G; iff $\ker\phi = \{e\}$. ($\forall g_1, g_2 \in G, \phi(g_1) = \phi(g_2) \implies g_1 = g_2$)

Isomorphism: a bijective homomorphism; two isomorphic groups share exactly the same structure

Kernel: $\ker\phi = \{g \in G \mid \phi(g) = e\}$

Cosets: with $H \subset G$, $gH = \{gh : h \in H\}$

- every $g \in G$ is in a coset of H
- every coset of H has the same size and two cosets of H are either equal or disjoint

Lagrange's Theorem: if G is a finite group and $H \subset G$, then $|H|$ divides $|G|$

- Corollary: if $g \in G$ has order n, then n divides $|G|$

Unit group: $R^* = \{a \in R : \exists b \in R \text{ such that } ab = 1\}$

- $\mathbb{Z}^* = \{\pm 1\}$
- $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$
- $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$
- $\mathbb{R}[x]^* = \mathbb{R}^*$
- $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \ldots, p-1\}$

Subgroups:

- the center of a group is the subgroup of elements that commute with all other elements
- The center of S_n is trivial for $n \geq 3$
- The center of D_n is trivial for odd $n \geq 3$ and is $\{e, r^{\frac{n}{2}}\}$ for even n
- If G is a finite group whose only subgroups are $\{e\}$ and G, then $|G|$ is prime or $G = \{e\}$

Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \mod p$$

Normal Group:

$$H = aHa^{-1} \iff a^{-1}Ha = H \iff a^{-1}Ha \subset H$$

- All subgroups of an abelian group are normal
- Any group is a normal subgroup of itself

Quotient group: $G/N = \{gN : g \in G\}$ and

$$aN \cdot bN = ab \cdot N$$

Cayley's Theorem: Every group is isomorphic to a subgroup of a symmetric/permutation group

Lemma: two orbits are identical or disjoint

Abelian Cauchy: If G abelian and $p \mid G$, G has an element of order p

Cauchy Theorem: Every finite group with $p \mid |G|$ has an element of order p

Proposition: $|H| = p^n$ has a subgroup of order p^m for any $m \leq n$

If G abelian, every subgroup is normal

Every group has at least two normal subgroups: $\{e\}$ and G

Simple group: a group whose only normal subgroups are $\{e\}$ and G

Proposition: any group of prime order is simple

Proposition: $\phi : G_1 \to G_2$ is a group homomorphism, $\ker\phi \trianglelefteq G_1$

Normality:

1. $H \trianglelefteq G$ if $gHg^{-1} \subseteq H, \forall g \in G$
2. $\forall g \in G, \{gHg^{-1}\} \trianglelefteq G$
3. there is an isomorphism $H \to g^{-1}Hg$

Isomorphism theorem: If $\phi : G_1 \to G_2$ is a group homomorphism with $\ker\phi = N$, then $G_1/\ker\phi \cong \mathrm{Im}(\phi)$

Corrolary:

$$\frac{\#G}{\#\ker(\phi)} = \#\mathrm{Im}(\phi)$$

Group action: G group, X set, $\phi : G \times X \to X$ such that

1. *Identity:* $e \cdot x = x \quad \forall x \in X$
2. *Associativity:* $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

Remark: Defining an action G on X is equivalent to a homomorphism $\alpha : G \to S_X$ where S_X is the set of permutations on X and $\alpha(g) : X \to X$ with $g \cdot x = \alpha(g)(x)$

Orbit: $Gx = \{g \cdot x : g \in G\}$

Stabilizer: $G_x = \{g \in G : g \cdot x = x\}$

Proposition:

$$|Gx| = \frac{|G|}{|G_x|}$$

Transitive action: $Gx = X \quad \forall x \in X$

Orbit Stabilizer Counting TheoremL G, X finite $Gx_1, \ldots, Gx_k$ distinct orbits,

$$|X| = \sum_{i=1}^{l} |Gx_i| = \sum_{i=1}^{K} \frac{|G|}{|G_{x_i}|}$$

Theorem: $|G| = p^n$, then $Z(G) \neq \{e\}$

Conjugation action: $g \cdot x = gxg^{-1} \in X$

$$G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

Corollary: $|G| = p^2$, G is abelian

Centralizer: $Z_G(H) = \{g \in G : gh = hg \quad \forall h \in H\}$

Normalizer: $N_G(H) = \{g \in G : g^{-1}Hg = H\}$

Sylow's theorems:

- *p-Sylow subgroup:* $p^n \mid G$, $H \subseteq G$ with $|H| = p^n$
- If $p^r \mid |G|$, G has a subgroup of order p^r
- $|G| = \prod_i |H_{p_i}|$ with H_{p_i} p-Sylow subgroups of distinct p_i
- For any two distinct p-Sylow subgroups, $P_1 \cap P_2 = \{e\}$

1. $|G| = p^n \cdot k$, G has at least one p-Sylow subgroup

2. All p-Sylow subgroups are conjugate: $\exists g \in G$, $H_2 = gH_1g^{-1}$
3. n is the number of distinct p-Sylow subgroups. $p \mid |G|$, $p \mid |k|$, $n \equiv 1 \mod p$

Lemma: $N_G(H) = \{g \in G : g^{-1}Hg = H\}$. If $H \subseteq G$, H has exactly $\#G/\$N_G(H)$ conjugates in G

Lemma: $A, B \subset D$, $AB = \{ab : a \in A, b \in B\}$,

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

Lemma:

$$|HaK| = \frac{|H|\,|K|}{|aHa^{-1} \cap K|}$$

Rings

Ring: a set with two binary operations (addition and multiplication) which satisfy closure, associativity, identity, inverse, and distributivity

- $(R, +)$ is an abelian group with identity 0
- $(R, \times)$ is closed, has assoicativity, and has identity 1
- R is associative under multiplication
- $0a = 0 \quad \forall a \in R$
- $(-a)(-b) = ab \quad \forall a, b \in R$

Ring Homomorphism: a map $\phi : R \to S$ such that

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(1) = 1$

Kernel: $\ker \phi = \{r \in R : \phi(r) = 0\}$

Integral Domain: a ring with no zero divisors ($ab = 0 \implies a = 0$ or $b = 0$)

- A commutative ring has cancellation iff it is an integral domain

Ideal: a subset $I \subset R$ such that

1. $a, b \in I \implies a + b \in I$ (additive closure)
2. $a \in I, r \in R \implies ra \in I$ (multiplicative closure/absorption)

Principal ideal: $(c) = cR = \{rc : r \in R\}$

- Every ring has at least two ideals: (0) and R

Quotient Ring: R/I is the set of cosets of I in R (a commutative ring) with addition and multiplication defined as

1. $(a + I) + (b + I) = (a + b) + I$
2. $(a + I)(b + I) = ab + I$

Isomorphism Theorem: if $\phi : R \to S$ is a surjective ring homomorphism with kernel I, then $R/I \cong \phi(R)$ iff ϕ is injective; the map $R \to R/I$ has kernel I

Characteristic of a Ring: the integer generating the kernel of $\phi : \mathbb{Z} \to R$. If ϕ not injective, the smallest m such that $m\alpha = 0$ for all $\alpha \in R$.

Principal Ideal Domain: R is a PID (principal ideal domain) if all ideals are principal. (We also assume it is an integral domain ($ab = 0 \implies a = 0 orb = 0$))

Unit: $u \in R : uv = 1$ for some $v \in R$

Reducible: a non-unit p is reducible if $p = ab$, where a, b are non-units.

Associates: $a, b \in R$ are associates if $a = ub$ for some unit $u \in R$ (this is an equivalence relation)

Unique Factorization Domain:

1. Every non-unit factors into finitely many irreducibles
2. The factoring is unique up to units and reordering

Euclidean Domain: an integral domain with a size function $\sigma : R \to \{0, 1, 2, \dots\}$ such that

1. $\sigma(mn) \geq \sigma(m)$
2. $a = kb + r$ where $r = 0$ or $\sigma(r) < \sigma(b)$

Theorem: $ED \implies PID \implies UFD$

Lemma: In a PID, if p irreducible and $p \mid ab$, then $p \mid a$ or $p \mid b$

Fields

Field: a commutative ring with identity where every nonzero element has a multiplicative inverse

- Every field is an integral domain but not every integral domain is a field
- Corollary of integral domain: all fields have cancellation
- A ring is a field iff $R^* = R \setminus \{0\}$
- A ring is a field iff its only ideals are (0) and R
- A ring is a field iff it has division and commutativity

Theorem: R/I integral domain $\iff$ I is prime. R/I is a field $\iff$ I is maximal.

Vector space: an abelian group under addition V over a field F with

Theorem: all ideals in $F[x]$ are principal

Irreducibility: $p(x) = a(x)b(x) \implies a(x)$ or $b(x)$ is a constant

Theorem: if $p(x) \in F[x]$ is irreducible, $I = p(x)F[x]$ is maximal

Theorem: if $F/p(x)F[x]$ is a field and contains a root of $p(x)$

Theorem: if $F \subset K \subset L$ then

$$[L : F] = [L : K][K : F]$$

Proposition: the order of a finite field of Characteristic p is some power of p.

Theorem: p prime and $d \geq 1$, $\mathbb{F}_p[x]$ contains an irreducible polynomial of degree d

Theorem: There exists a field F containing exactly p^d elements ($d \geq 1$) and any two fields containing p^d elements are isomorphic.

Fundamental Theorem of Algebra: $p(z) \in \mathbb{C}[z]$ has a root in $\mathbb{C}$.