Groups

Group: a set with a composition law satisfying

$$\begin{aligned} g_1g_2 \in G &\quad \forall g_1, g_2 \in G && \text{(closure)} \\ eg = ge = g &\quad \forall g \in G && \text{(identity)} \\ gh = hg = e &\quad \exists h \forall g \in G && \text{(inverse)} \\ g_1(g_2g_3) = (g_1g_2)g_3 &\quad \forall g_1, g_2, g_2 \in G && \text{(associativity)} \end{aligned}$$

Properties:

- G has exactly one identity
- Each element has exactly one inverse
- $(gh)^{-1} = h^{-1}g^{-1}$
- $(g^{-1})^{-1} = g$
- If $g_1g_2 = g_2g_1 \quad \forall g_1, g_2 \in G$ then G is *abelian*
- *Cancellation:* If $gh = gk$ then $h = k$

Order:

1. the cardinality of the set of elements of an infinite group
2. the number of elements in a finite group
3. the smallest integer $n \geq 1$ such that $g^n = e$ with $g \in G$
4. the order of a group is also the order of its generator

Common groups:

- Cyclic group: $\mathcal{C}_n = \{e, g, g^2, \ldots, g^{n-1}\} \cong \langle g \rangle$ using $g^i \cdot g^j = g^{i+j \mod n}$
- Symmetric group: $\mathcal{S}_n$ the set of all permutations of $\{1, 2, \ldots, n\}$
- General Linear Group $GL_2(\mathbb{R})$: the group of 2×2 matrices with $\det A \neq 0$
- Dihedral groups $\mathcal{D}_n$: the group of rotations and reflections of an n-gon
- Quaternion group $\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$

Group homomorphism:

$$\phi : G \to G' \text{ such that } \phi(g_1 g_2) = \phi(g_1)\phi(g_2) \quad \forall g_1, g_2 \in G$$

Bijection: a surjective and injective mapping

1. Surjective (onto) - every element is the image of an element in the domain, $\forall y \in Y, \exists x \in X : f(x) = y$
2. Injective (one-to-one) - $f(x_1) = f(x_2) \implies x_1 = x_2$

Isomorphism: a bijective homomorphism

- $\mathcal{C}_2 \cong \mathcal{S}_2$
- $\mathcal{D}_3 \cong \mathcal{S}_3$
- Every group of prime order is isomorphic to $\mathcal{C}_p$

Isomorphic group share structural properties (both are finite, both are abelian, both share elements of the same order if one of them does)

To prove to groups are not isomorphic, show they have a structural difference.

Subgroup: a subset $H \subset G$ that is closed, has the identity element, and has an inverse for every element (it automatically satisfies the associative law)

To show H is a subgroup, prove that $H \neq \emptyset$ and $h_1 h_2^{-1} \in H \forall h_1, h_2 \in H$

Kernel: the kernel of a group homomorphism $\phi : G \to G'$ is

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

- $\ker(\phi)$ is a subgroup of G
- ϕ is injective if and only if $\ker(\phi) = \{e\}$

Cosets: For $H \subset G$, the coset for each $g \in G$ is $gH = \{gh : h \in H\}$

- Every element of G is in some coset of H
- Every coset of H has the same number of elements
- Two cosets of H are either equal or disjoint

Lagrange's Theorem: the order of a subgroup divides the order of a group

$$\#G = (G : H)\#H$$

where $(G : H)$, the *index of H in G*, is the number of distinct cosets of H.

Corollary: the order of an element $g \in G$ divides the order of the group

Product Group: $G_1 \times G_2 = \{(a, b) : a \in G_1 \text{ and } b \in G_2\}$ with multiplication defined by

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$$

Unproven but useful assertions of Group Theory:

- For p prime and G of order p^2, G is abelian
- Sylow's theorem: for G finite, p prime, with $p^n \Big| \#G$ $(n \geq 1)$, G has a subgroup of order p^n (but not the converse!)
- Structure theorem for Finite Abelian Groups: with G finite abelian, there are prime powers (integers) so that

$$G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})$$

Rings

Ring: set R with two operations such that

1. $(R, +)$ is an abelian group with identity 0
2. $(R, \cdot)$ is closed, has associativity, and has an identity (1)
3. $a(bc) = (ab)c \quad \forall a, b, c \in R$

Properties:

- $0a = 0 \quad \forall a \in R$
- $(-a)(-b) = ab \quad \forall a, b \in R$

Ring homomorphism: $\phi : R \to R'$ satisfying

1. $\phi(1) = 1$

2. $\phi(a + b) = \phi(a) + \phi(b)$

3. $\phi(ab) = \phi(a)\phi(b)$

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

Important rings:

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- $\mathbb{Z}/m\mathbb{Z}$ (not a subring of $\mathbb{C}$ but with homomorphism $\phi(a) = a \mod m, \phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$)
- Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- Polynomial Rings $R[x] = \sum a_k x^k$
- Quaternions $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ (non-commutative)
- $M_2(\mathbb{R})$ (two-by-two matrices with real entries)
- $\mathbb{Z}/p\mathbb{Z}$ with prime p is a field

Important Homomorphisms:

- Evaluation map $E_c : R[x] \to R$ with $E_c(f) = f(c)$ (kernel is polynomials with factor $x - c$)
- For every ring, there is a *unique* homomorphism $\phi : \mathbb{Z} \to R$

Field: a commutative ring with every non-zero element having an inverse

Integral Domain: a ring where $ab = 0$ implies $a = 0$ or $b = 0$

Examples: $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}[i]$

Every field is an integral domain but not every integral domain is a field.

Cancellation Property: $ab = ac \iff b = c$ or $a = 0$. A commutative ring has this property if and only if it is an integral domain.

Unit Groups: the subset $R^* \subset R$ where

$$R^* = \{a \in R : \exists b \in R, ab = 1\}$$

forms a group under multiplication.

Examples:

- $\mathbb{Z}^* = \{\pm 1\}$
- $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

- $\mathbb{R}[x]^* = \mathbb{R}^*$
- $(Z/m\mathbb{Z})^* = \{a \mod m : \gcd(a, m) = 1\}$
- $(\mathbb{Z}/p\mathbb{Z})^* = \{1, \ldots, p-1\}$ (and $\mathbb{Z}/p\mathbb{Z}$ is a field)

A ring is a field if and only if $R^* = R - \{0\}$

Product of Unit Groups: With $R_1, \ldots, R_n$ commutative,

$$(R_1 \times \cdots \times R_n)^* \cong R_1^* \times \cdots \times R_n^*$$

Ideals: a non-empty subset $I \subseteq R$ with

1. $a, b \in I \implies a + b \in I$
2. $a \in I, r \in R \implies ra \in I$

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

Every ring has at least two ideals: $(0) = 0R = \{0\}$ and $(1) = 1R = R$

Coset: $a \in R$,

$$a + I = \{a + c : c \in I\}$$

Note that $a \in a + I$ because $0 \in I$ so $a + 0 \in I$.

If $b - a \in I$ then $b \equiv a \mod I$

Quotient: R/I is the collection of distinct cosets of I and is governed by the group operations

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I$$

Properties:

1. $a' + I = a + I \iff a' - a \in I$
2. Addition and multiplication of cosets is well defined
3. R/I is a commutative ring

Isomorphism Theorem:

1. With $I \subset R$, $\phi : R \to R/I$, $\ker(\phi) = I$

2. With $\phi : R \to R'$, $\ker(\phi) = \{a \in R : \phi(a) = 0\}$ is an ideal of R, ϕ is injective iff $\ker(\phi) = (0) = I$

Homework Results

Generator: If G is a finite cyclic group of order n, and g is a generator of G. g^k is a generator of G if and only if $\gcd(k, n) = 1$

Lemma: $g \in G$ with $o(g) = n, k \geq 1$. $o(g^k) = n/\gcd(n, k)$

Homomorphism: If ϕ is a bijective homomorphism, ϕ^{-1} is a homomorphism

Center: $Z(G) = \{g \in G : gh = hg \quad \forall h \in G\}$

- $Z(G)$ is the set of elements in G that commute with every other element
- It is a subgroup
- $Z(G) = G$ when G is abelian
- The center of S_n is trivial $n \geq 3$
- The center of D_n is trivial for odd $n \geq 3$ and consists of identity and 180 degree rotations for even $n \geq 3$
- The center of Q is $\{1, -1\}$

Subgroups: If G is a finite group whose only subgroups are $\{e\}$ and G, then $G = \{e\}$ or it is cyclic of prime order.

Gaussian integers: $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$ If $D \geq 0$ then it is a subring of $\mathbb{R}$. Otherwise it is a subring of $\mathbb{C}$

Fermat's Little Theorem: with p prime, $a \in \mathbb{Z}$ and $p \nmid a$

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

Ideals:

- R is a field if and only if its only ideals are the zero ideal (0) and the entire ring R
- every ideal in $\mathbb{Z}$ is a principal ideal.