1 Groups

1.1 Definitions and Properties

A **permutation** of a set X is a bijective function whose domain and range are X. In other words, it is a bijective function:

$$\pi : X \to X$$

A **group** consists of a set G and a composition law:

$$G \times G \to G \quad (g_1, g_2) \to g_1 \cdot g_2$$

Satisfying the following axioms:

Identity Axiom: There exists an element $e \in G$ such that, for all $g \in G$:

$$e \cdot g = g \cdot e = g$$

Inverse Axiom: For all $g \in G$ there is an element $g^{-1} \in G$ such that:

$$g \cdot g^{-1} = g^{-1} \cdot g = e$$

Associative Law: For all $g_1, g_2, g_3 \in G$, we have that:

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$$

Commutative Law: While this is not necessary for G to be a group, if for all $g_1, g_2 \in G$ we have the following, G is **commutative** or **abelian**:

$$g_1 \cdot g_2 = g_2 \cdot g_1$$

Let G be a group. Then:

(a): G has exactly one identity element.
(b): Each element of G has exactly one inverse.
(c): Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.
(d): Let $g \in G$. Then $(g^{-1})^{-1} = g$.

The **order of a group** G, denoted $\#G$, is the cardinality of the set of elements of G.

The **order of an element** $g \in G$ is the smallest integer $n \geq 1$ such that $g^n = e$. If no n exists, then g has infinite order.

Let G be a group, let $g \in G$. The order of g divides the order of G.

1.2 Examples of Groups

The set of integers modulo m, denoted $\mathbb{Z}/m\mathbb{Z}$, form the **group of integers modulo** m with addition as the group law.

The set of real numbers $\mathbb{R}$, the set of rational numbers $\mathbb{Q}$, and the set of complex numbers $\mathbb{C}$ all form groups with addition as the group law. The set of positive or non-zero real numbers also form groups with multiplcation as the group law.

A group G is a **cyclic group** if there is an element $g \in G$ such that $G = \{...g^{-1}, e, g, g^2, ...\}$. In other words, all other elements are generated by g, and g is called the **generator of** G. We denote the cyclic groups of the integers up to n as $\mathcal{C}_n$.

The **symmetric group of** X, denoted S_X, is the collection of all permutations of X, with the group law being the composition of permuations.

The group of $n \times n$ matrices, A, such that $det(A) \neq 0$ is the **general linear group**, denoted $GL_n(X)$, where X is the group where the entries live in.

The group of symmetries of a regular n-gon is the **n'th dihedral group**, denoted $\mathcal{D}_n$. There are exactly n rotations and n flips in this group.

The **quaternion group** $\mathcal{Q}$ is a non-commutative group with eight elements with operations you can look up:

$$\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$$

1.3 Group Homomorphisms

Let G and G' be groups. A **group homomorphism from G to G'** is a function $\phi : G \to G'$ such that, for all $g_1, g_2 \in G$:

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$

The above is sufficient to prove the following two properties:

(a): Let $e \in G$ be the identity element of G. Then $\phi(e)$ is the identity element of G'.
(b): Let $g \in G$. Then $\phi(g^{-1}) = \phi(g)^{-1}$.

Let G_1 and G_2 be groups. These groups are **isomorphic** if there exists a bijective homomorphism $\phi : G_1 \to G_2$, which we call an **isomorphism**. In this case, G_1 and G_2 are the same group, just relabelled.

1.4 Subgroups, Cosets, and Lagrange's Theorem

Let G be a group. A **subgroup of** G is a subset $H \subset G$ that is also a group under G's group law. That is, H satisfies:

(a): For all $h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$.
(b): $e \in H$.
(c): For all $h \in H$, $h^{-1} \in H$.

We note that all groups have two trivial subgroups, $\{e\}$ and G itself.

Let G be a group, let $g \in G$ have order n. The **cyclic subgroup of G generated by** g is:

$$\langle g \rangle = \{...g^{-1}, e, g, g^2...\}$$

It is isomorphic to the cyclic group $\mathcal{C}_n$.

Let $\phi : G \to G'$ be a group homomorphism. The **kernel of** ϕ is the set:

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

Let $\phi : G \to G'$ be a group homomorphism. Then:

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

Let G be a group, and let $H \subset G$ be a subgroup of G. For all $g \in G$, the **(left) coset of H attached to g** is the set:

$$gH = \{gh : h \in H\}$$

Let G be a finite group, and let $H \subset G$ be a subgroup of G. Then:

(a): Every element of G is in some coset of H.
(b): Every coset of H has the same number of elements.
(c): Let $g_1, g_2 \in G$. Then either:

$$g_1H = g_2H \quad or \quad g_1H \cap h_2H = \emptyset$$

Lagrange's Theorem: Let G be a finite group, and let $H \subset G$ be a subgroup of G. Then the order of H divides the order of G.

Let G be a group and let $H \subset G$ be a subgroup of G. The **index of H in G**, denoted $(G : H)$, is the number of distinct cosets of H.

Let G be a finite group, and let $g \in G$. Then the order of g divides the order of G.

Let p be a prime and let G be a group of order p. Then G is isomorphic to $\mathcal{C}_p$. In other words, G is a cyclic group.

Let p be a prime and let G be a group of order p^2. Then G is an abelian group.

(Sylow's Theorem): Let G be a finite group, let p be prime, and suppose that $p^n \mid \#G$ for some $n \geq 1$. Then G has a subgroup of order p^n.

1.5 Products of Groups

Let G_1 and G_2 be groups. The **product** of G_1 and G_2 is the group:

$$G_1 \times G_2 = \{(a, b) : a \in G_1, b \in G_2\}$$

Where:

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

(Structure Theorem for Finite Abelian Groups): Let G be a finite abelian group. Then there are integers $m_1 ... m_r$ where each m_i is a prime power such that:

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

2 Rings

A **ring** R is a set with two operations, called **addition** $(a + b)$ and **multiplication** $(a \cdot b)$, satisfying the following axioms:

(a): **Addition Properties:** The set R with addition law $+$ is an abelian group with identity 0_R.
(b): **Multiplication Properties:** The set R with multiplication law $\cdot$ satisfies Identity Law and Associative Law.
(c): **Distributive Law:** For all $a, b, c \in R$ we have:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

(d): While this is not necessary for R to be a ring, if for all $a, b \in R$, $a \cdot b = b \cdot a$, the ring is **commutative**.

Let R be a ring. Then:

(a): For all $a \in R$, $0_R \cdot a = 0_R$.
(b): For all $a, b \in R$, $(-a) \cdot (-b) = a \cdot b$.

Let R and R' be rings. A **ring homomorphism** from R to R' is a function $\phi : R \to R'$ satisfying:

(a): $\phi(1_R) = 1_{R'}$.
(b): $\phi(a + b) = \phi(a) + \phi(b)$.
(c): $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

We say that R and R' are **isomorphic** if there is a bijective ring homomorphism $\phi : R \to R'$, called an **isomorphism**.

The **kernel** of ϕ is the set of elements:

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

2.1 Examples of Rings

The following are rings.

$$\mathbb{Z}/m\mathbb{Z}$$

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

$$R[x] = \{\text{polynomials with coefficients in } R.\}$$

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Let R be a ring. There is a unique homomorphism $\phi : \mathbb{Z} \to R$.

2.2 Properties of Rings

A **field** is a commutative ring R where every non-zero element of R has a multiplicative inverse.

Let R be a commutative ring. R has the **cancellation property** if for all $a, b, c \in R$, the following holds:

$$ab = ac \wedge a \neq 0 \iff b = c$$

Let R be a ring. An element $a \in R$ is called a **zero divisor** if $a \neq 0$ and there exists a non-zero element $b \in R$ such that $ab = 0$. The ring R is an **integral domain** if it has no zero divisors.

2.3 Unit Groups and Product Rings

Let R be a commutative ring. The **group of units of** R is the subset $R^* \subset R$ defined by:

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

Elements of R^* are called **units**.

The set of units R^* is a group with group law being ring multiplication.

Let $m \geq 1$ be an integer. Then:

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \mathrm{mod} m : gcd(a, m) = 1\}$$

If p is a prime, then $\mathbb{Z}/m\mathbb{Z}$ is a field, denoted $\mathbb{F}_p$

Let $R_1 ... R_n$ be rings. The **product** of $R_1 ... R_n$ is the ring:

$$R_1 \times ... \times R_n = \{(a_1, ...a_n) : a_1 \in R_1 ... a_n \in R_n\}$$

Let $R_1 ... R_n$ be rings. Then:

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

2.4 Ideals and Quotient Rings

Let R be a commutative ring. An **ideal** of R is a non-empty subset $I \subseteq R$ such that:

(a): If $a, b \in I$, $a + b \in I$,
(b): If $a \in I$ and $r \in R$, then $ra \in I$.

Let R be a commutative ring, and let $c \in R$. The **principal ideal generated by** c, denoted cR or (c), is the set of all multiples of c:

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

Let R be a commutative ring and let $I \subseteq R$ be an ideal of R. For each element $a \in R$, the **coset of** a is the set:

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

If $a - b \in I$, we say that a is congruent to b modulo I, denoted:

$$a \equiv b$$

And we define addition and multiplication of cosets as follows:

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

$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

And we denote the collection of distinct cosets by R/I, called a quotient ring.

Let R be a commutative ring, and let $I \subseteq R$ be an ideal of R. Then:

(a): Let $a + I$ and $a' + I$ be two cosets. Then $a' + I = a + I$ if and only if $a' - a \in I$.
(b): Addition and multiplication of cosets is well defined.
(c): Addition and multiplcation of cosets turns R/I into a commutative ring, called a **quotient ring**.

Let R be a commutative ring.

(a): Let $I \subseteq R$ be an ideal of R. Then the following map is a ring homomorphism whose kernel is I:

$$\psi : R \to R/I, a \to a + R$$

(b): Let $\phi : R \to R'$ be a ring homomorphism. Then:
(i): The kernel of ϕ is an ideal of R.
(ii): ϕ is injective if and only if $ker(\phi) = \{0\}$
(iii): There is a well-defined injective ring homomorphism:

$$\overline{\phi} : R/I_\phi \to R', \overline{\phi}(a + I_\phi) = \phi(a)$$

Let R be a ring, and let $\phi : \mathbb{Z} \to R$ be the unique homomorphism deterined by the condition that $\phi(1) = 1_R$. Then, there is a unique integer $m \geq 0$, called the **characteristic** of R, such that:

$$ker(\phi) = m\mathbb{Z}$$

Let p be prime, and let R be a commutative ring of characteristic p. Then the following map is a ring homomorphism, called the **Frobenius homomorphism of** R:

$$f : R \to R, f(a) = a^p$$

We notice also that for all $a, b \in R$ and all $n \geq 0$, we have:

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

2.5 Prime Ideals and Maximal Ideals

Let R be a commutative ring. An ideal $I \subseteq R$ is a **prime ideal** if $I \neq R$ and, if whenever $ab \in I$, either $a \in I$ or $b \in I$. Or, in other words, for two $a, b \notin I$, $ab \notin I$.

Let R be a commutative ring. An ideal I is called a **maximal ideal** if $I \neq R$ and if there is no ideal properly contained between I and R. In other words, if J is an ideal and $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

Let R be a commutative ring, and let I be an ideal with $I \neq R$. Then:

(a): I is a prime ideal if and only if the quotient ring R/I is an integral domain.
(b): I is a maximal ideal if and only if the quotient ring R/I is a field.

Corollary: Every maximal ideal is a prime ideal.

3 Vector Spaces

A **field** is a commutative ring F with the property that for every non-zero $a \in F$, where is an element $b \in F$ such that $ab = 1$.

Let F be a field. A **vector space with field of scalars** F, or, an F**-vector space**, is an abelian group V with a rule for multiplying a vector $v \in V$ by a scalar $c \in F$ to obtain a new vector $cv \in V$. Vector addition and scalar multiplication satisfy the following axioms:

Identity Law: For all $v \in V$:

$$1v = v$$

Distributive Law #1: For all $v_1, v_2 \in V$, $c \in F$:

$$c(v_1 + v_2) = cv_1 + cv_2$$

Distributive Law #2: For all $v \in V$, $c_1, c_2 \in F$:

$$(c_1 + c_2)v = c_1 v + c_2 v$$

Associative Law: For all $v \in V$, $c_1, c_2 \in F$:

$$(c_1 c_2)v = c_1(c_2 v)$$

Let V be an F-vector space. Then:

(a): For all $v \in V$, $0v = 0$.
(b): For all $v \in V$, $(-1)v + v = 0$.

Let F be a field, and let V and W be F-vector spaces. A **linear transformation** from V to W is a function:

$$L : V \to W$$

Satisfying for all $v_1, v_2 \in V$, $c_1, c_2 \in F$:

$$L(c_1 v_1 + c_2 v_2) = c_1 L(v_1) + c_2 L(v_2)$$

3.1 Bases and Dimension

Let V be an F-vector space. A **finite basis for** V is a finite set of vectors $\mathcal{B} = \{v_1, ...v_n\} \subset V$ such that every vector $v \in V$ can be uniquely written as a **linear combination** of elements in $\mathcal{B}$.

Let V be an F-vector space, and let $\mathcal{A} = \{v_1, ...v_n\}$ be a set of vectors in V. Then:

(a): The set $\mathcal{A}$ **spans** V is every vector in V is a linear combination of the vectors in $\mathcal{A}$. The set of linear combinations of vectors in $\mathcal{A}$ is called the **span** of $\mathcal{A}$, denoted $Span(\mathcal{A})$.

(b): The set $\mathcal{A}$ is **linearly independent** if the only solution to the following is the trivial solution:

$$a_1 v_2 + ... + a_n v_n = \vec{0}$$

Let v be an F-vector space, and let $\mathcal{A} = \{v_1, ...v_n\}$ be a set of vectors in V. Then $\mathcal{A}$ is a basis for V if and only if $\mathcal{A}$ spans V and is linearly independent.

Let V be an F-vector space, let $\mathcal{A}$ be a finite set of vectors in V that spans V, and let $\mathcal{L} \subseteq \mathcal{S}$ be a subset of $\mathcal{S}$ that is linearly independent. Then there is a basis for V satisfying:

$$\mathcal{L} \subseteq \mathcal{B} \subseteq \mathcal{S}$$

Let V be a vector space with a finite basis. Then every basis for V has the same number of elements.

Let V be a vector space with a finite basis. The **dimension** of V is the number of vectors in a basis of V, denoted $dim_F(V)$. We know that this is well defined.

Let V be an F-vector space, let $\mathcal{S}$ be a finite set of vectors in V that span V, and let $\mathcal{L}$ be a set of vectors that is linearly independent. Then, given any vectors $v \in \mathcal{L} - \mathcal{S}$, we can find a vector $w \in \mathcal{S} - \mathcal{L}$ so that the following is still a spanning set:

$$(S - \{w\}) \cup \{v\}$$

Let V be an F-vector space, let $\mathcal{S} \subset V$ be a finite set that spans V, and let $\mathcal{L} \subset V$ be a linearly independent set. Then:

$$\#\mathcal{L} \leq \#\mathcal{S}$$

4 Fields

A **field** is a commutative ring F with the property that for every non-zero $a \in F$ there is an element $b \in F$ such that $ab = 1$.

Let R be a commutative ring. The **unit group of** R is the group:

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

We can use this define a field as:

$$F^* = \{a \in F : a \neq 0\} = F - \{0\}$$

Let F and K be fields, and let $\phi : F \to K$ be a ring homomorphism. Then:

(a): ϕ is injective.
(b): Let $a \in F^*$. Then $\phi(a^{-1}) = \phi(a)^{-1}$.

A **skew field**, also called a **division ring**, is a ring where all non-zero elements have multiplicative inverses, but the ring is not necessarily commutative.

A famous result of Wedderburn says that all finite skew fields are fields.

4.1 Subfields and Extension Fields

Let K be a field. A **subfield** of K is a subset $F \subset K$ that it itself a field using the addition and multiplication operations from K.

Let F be a field. An **extension field** of F is a field K such that F is a subfield of K. We write K/F to indicate that K is an extension field of F.

Let L/F be an extension of fields, and let $\alpha_1, ...\alpha_n \in L$. Then there is a unique field K such that:

(a): $F \subset K \subseteq L$.
(b): $\alpha_1, ...\alpha_n \in K$.
(c): If K' is a field satisfying $F \subseteq K' \subseteq L$, $K \subseteq K'$.

Let K/F be an extension of fields. The **degree of** K **over** F, denoted $[K : F]$, is the dimension of K when viewed as an F-vector space. If $[K : F]$ is finite, then K/F is a **finite extension** - otherwise, K/F is an **infinite extension**.

Let $L/K/F$ be extensions of fields. Then:

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

As long as all of $[L : F], [L : K], [K : F]$ are finite, or if $[L : F]$ is infinite, then either $[L : K]$ or $[K : F]$ is infinite.

4.2 Polynomial Rings

Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial, written as:

$$f(x) = a_0 + a_1x + ... + a_dx^d$$

The **degree** of f is:

$$deg(f) = d$$

Moreover, if $a_d = 1$, then f is a **monic polynomial**.

Let $f_1(x), f_2(x) \in F[x]$ be non-zero polynomials. Then:

$$deg(f_1 f_2) = deg(f_1) + deg(f_2)$$

Let F be a field, and let $f(x), g(x) \in F[x]$ be polynomials with $g(x) \neq 0$. Then there are unique polynomials $q(r), r(x) \in F[x]$ with $deg(r) < deg(g)$ satisfying:

$$f(x) = g(x)q(x) + r(x)$$

Let F be a field and let $I \subseteq F[x]$ be an ideal in the ring $F[x]$. Then I is a principal ideal.

4.3 Building Extension Fields

Let F be a field. A non-constant polynomial $f(x) \in F[x]$ is **reducible (over F)** if there exists non-constant polynomials $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$. An **irreducible** polynomial is a non-constant polynomial that has no such non-trivial factorizations in $F[x]$.

Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. The following are equivalent:

(a): The polynomial $f(x)$ is irreducible.
(b): The principal ideal $f(x)F[x]$ generated by $f(x)$ is a maximal ideal.
(c): The quotient ring $F[x]/f(x)F[x]$ is a field.

Let F be a field, let $f(x) \in F[x]$ be an irreducible polynomial, let $I_f = f(x)F[x]$ be the principal ideal generated by $f(x)$ and let $K_f = F[x]/I_f$ be the indicated quotient ring.

(a): The ring K_f is a field.
(b): The field K_f is a finite extension of the field of F. Its degree is given by:

$$[K_f : F] = deg(f)$$

(c): The polynomial $f(x)$ has a root in K_f.

4.4 Finite Fields

NOTE: We are missing some stuff with regards to counting polynomials, since it is painful. Refer to the textbook for this!

Let F be a finite field. Then,

(a): The characteristic of F is prime.
(b): Let $p = char(F)$. Then the finite field $\mathbb{F}_p$ is a subfield of F, in the sense that there exists a unique injective homomorphism from $\mathbb{F}_p$ to F.
(c): The number of elements of F is given by:

$$\#F = p^{[F:\mathbb{F}_p]}$$

Let p be prime, and let $d \geq 1$. Then the ring $\mathbb{F}_p[x]$ contains an irreducible polynomial of degree d.

Let p be a prime and let $d \geq 1$. Then,

(a): There exists a field F containing exactly p^d elements.
(b): Any two fields containing p^d elements are isomorphic.

5 Groups Continued

5.1 Normal Subgroups and Quotient Groups

Let G be a group and let H be a subgroup of G. We denote the set of (left) cosets of G by:

$$G/H = \{\text{(left) cosets of } H\}$$

Let G be a group, let $H \subseteq G$ be a subgroup of G, and let $\mathcal{C}_1$ and $\mathcal{C}_2$ be cosets of H. We define the **product** of $\mathcal{C}_1$ and $\mathcal{C}_2$ by the rule:

$$\mathcal{C}_1 \cdot \mathcal{C}_2 = g_1 g_2 H$$

For some $g_1 \in \mathcal{C}_1$ and some $g_2 \in \mathcal{C}_2$. Note that this is only well defined if H is a normal subgroup.

Let G be a group, let $H \subseteq G$ be a subgroup of G, and let $g \in G$. The **g-conjugate of** H is the subgroup:

$$g^{-1}Hg = \{g^{-1}hg : g \in G\}$$

Let G be a group, let $H \subseteq G$ be a subgroup of G, and let $g \in G$. H is a **normal subgroup of** G is, for all $g \in G$,

$$g^{-1}Hg = H$$

If G is abelian, than all subgroups are normal. All groups G trivially have two normal subgroups, $\{e\}$ and G. If these are the only two subgroups, then G is called a **simple group**.

Let $\phi : G \to G'$ be a group homomorphism. Then $ker(\phi)$ is a normal subgroup of G.

Let G be a group and let $H \subset G$ be a subgroup. Then:

(a): If $g^{-1}Hg \subseteq H$ for all $g \in G$, then H is a normal subgroup of G.
(b): For all $g \in G$, $g^{-1}Hg$ is a subgroup of G.
(c): For all $g \in G$, the map $H \to g^{-1}Hg$ defined by $h \to g^{-1}hg$ is a group isomorphism.

Let G be a group, and let $H \subset G$ be a normal subgroup of G. Let $g_1, g_1', g_2, g_2' \in G$ be elements such that:

$$g_1'H = g_1H \quad \wedge \quad g_2'H = g_2H$$

Then:

$$g_1'g_2'H = g_1g_2H$$

Let G be a group, and let $H \subset G$ be a normal subgroup of G. Then:

(a): The collection of cosets G/H is a group with the well-defined group operation:

$$g_1 H \cdot g_2 H = g_1 g_2 H$$

(b): The following map is a homomorphism with $ker(\phi) = H$:

$$\phi : G \to G/H, \phi(g) = gH$$

(c): Let $\psi : G \to G'$ be a homomorphism with $H \subseteq ker(\phi)$. Then there is a unique homomorphism:

$$\lambda : G/H \to G' \quad \text{such that} \quad \lambda(gH) = \psi(g)$$

(d): If we take $H = ker(\psi)$ in (c), then λ is injective. In particular, the following is an isomorphism onto the image of λ:

$$\lambda : G/ker(\phi) \to \lambda(G) \subseteq G'$$

5.2 Groups Acting on Sets

Let G be a group, and let X be a set. An **action of G on X** is a rule that assigns each element $g \in G$ and each element $x \in X$ another element $g \cdot x \in X$ such that:

(1): For all $x \in X$, $e \cdot x = x$.
(2): For all $x, \in X$ and all $g_1, g_2 \in G$, $(g_1 g_2)x = g_1(g_2 x)$.

Alternatively, we can define an action of G on X as a group homomorphism:

$$\alpha : G \to \mathcal{S}_X$$

where α returns a permutation of the elements of X, and $g \cdot x = \alpha(g)(x)$.

Given a group G acting on a set X, we get two important quantities.

The **orbit of x** is the set of elements in X that G sends x to:

$$Gx = \{gx : g \in G\}$$

The **stabilizer of x** is the set of elements in X that G leaves unchanged:

$$G_x = \{g \in G : gx = x\}$$

Let G be a group that acts on a set X. Then:

(a): Every element of X is in some orbit.
(b): Let $x \in X$. G_x is a subgroup of G.
(c): Let $x \in X$. Then:

$$\#G_x \cdot \#Gx = \#G$$

(d): Let $x_1, x_2 \in X$. Then the orbits Gx_1 and Gx_2 are either equal or disjoint.

We say that G acts **transitively** on X if, for all $x \in X$, $Gx = X$.

5.3 Orbit-Stabilizer Counting Theorem

(Orbit-Stabilizer Counting Theorem): Let G be a finite group that acts on a finite set X. Then:

$$\#X = \sum_{i=1}^{n} \#Gx_i = \sum_{i=1}^{n} \frac{\#G}{\#G_{x_i}}$$

Let G be a group. The **center** of G, denoted $Z(G)$, is the set of elements in G that commute with every element of G:

$$Z(G) = \{g \in G : gg' = g'g, \forall g' \in G\}$$

For subgroups $H \subseteq G$, the **normalizer** of H is:

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

Let p be a prime, and let G be a finite group with p^n elements for some $n \geq 1$. Then $Z(G) \neq \{e\}$.

Let p be a prime, and let G be a group with p^2 elements. Then G is abelian.

5.4 Sylow's Theorem: Part 1

Sylow's Theorem: Part 1. Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. Then G has a subgroup of order p^n.

Let p be a prime, let $n \geq 0$, and let $m \geq 1$ with $p \nmid m$. Then $\binom{p^n m}{m^n}$ is not divisible by p.

Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. A subgroup $H \subseteq G$ with $\#H = p^n$ is called a p-**Sylow subgrou pof** G. G must have at least one Sylow subgroup.

Sylow's Theorem. Let G be a finite group, and let p be a prime. Then:

(a): G has at least one p-Sylow subgroup.
(b): Let H_1 and H_2 be p-Sylow subgroups of G. Then H_1 and H_2 are conjugate: $H_1 = gH_2g^{-1}$ for some $g \in G$.
(c): Let H be a p-Sylow subgroup of G, and let k be the number of distinct p-Sylow subgroups of G. Then $k \mid \#G$ and $k \equiv 1 \text{mod} p$.

5.5 Two Counting Lemmas

Let G be a finite group and let $H \subseteq G$ be a subgroup. Then H has exactly $\#G/\#N(H)$ distinct conjugates in G.

Let G be a finite group, let A and B be subgroups of G, and let $AB = \{ab : a \in A, b \in B\}$. Then:

$$\#(AB) = \frac{\#A \cdot \#B}{\#(A \cap B)}$$

5.6 Double Cosets and Sylow's Theorem

Let H_1, H_2 be subgroups of G. The **double coset** associated to g is the set:

$$H_1 g H_2 = \{h_1 g h_2 : h_1 \in H_1, h_2 \in H_2\}$$

We can define a **double coset equivalence relation on** G by saying $g\ g'$ if $g' = h_1 g h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$.

Let H_1, H_2 be subgroups of G, and let $g \in G$. Then:

$$\#H_1 g H_2 = \frac{\#H_1 \cdot \#H_2}{\#(g^{-1} G_1 g \cap H_2}$$

6 Rings Continued

6.1 Irreducible Elements and Unique Factorization Domains

Let R be a ring, and let $a \in R$ be a **unit** if it has a multiplicative inverse. The set of units of R, denoted R^*, is a group with group law multiplication.

Let R be a ring. A non-zero element $a \in R$ is **irreducible** if a is not a unit and the only way to factor $a = bc$ is for either b or c to be a unit.

Let R be an integral domain. Then R is a **unique factorization domain (UFD)** if:

(a): For all $a \in R$, we can write $a = b_1 \cdot b_2 \cdots b_n$ for irreducible $b_1, b_2, \dots b_n \in R$.
(b): Suppose $b_1, b_2, \dots b_n \in R$ and $c_1, c_2, \dots c_m \in R$ are all irreducible, and that their products are equal. Then $n = m$ and each $c_i = u_i b_i$, after relabelling.

Let F be a field. Then the ring $F[x_1, \dots, x_n]$ is a UFD.

6.2 Euclidean Domains and Principal Ideal Domains

A ring R is a **principal ideal domain (PID)** if it is an integral domain in which every ideal of R is principal.

A ring R is a **Euclidean domain** if it is an integral and there is a size function:

$$\sigma : R \to \{0, 1, 2, \dots\}$$

Such that:

(a): $\sigma(a) = 0 \iff a = 0$.
(b): For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that:

$$a = bq + r, \sigma(r) < \sigma(b)$$

(3): For all $a, b \in R$ we have $\sigma(ab) = \sigma(a)\sigma(b)$.

Every Euclidean domain is a PID.

The ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain with size function:

$$\sigma(a + bi) = a^2 + b^2$$

Let R be a PID and let $c \in R$. The following are equivalent:

(a): c is irreducible.
(b): The principal ideal cR is maximal.
(c): The quotient ring R/cR is a field.

Let R be an integral domain, and let $a, b \in R$. We say that b **divides** a is we can write $a = bc$ for some $c \in R$, and we denote this $b \mid a$. We note that this is equivalent to the assertion $a \in bR$, as well as $aR \subseteq bR$.

Let R be a PID and let $a, b, c \in R$. Suppose a is irreducible and $a \mid bc$. Then either $a \mid b$ or $a \mid c$ or both.

Let R be a PID and let $a, b_1, \dots b_n \in R$. Suppose that a is irreducible and divides the product of b_i's. Then a divides at least one b_i.

Let R be a Euclidean domian with size function σ, and let $u \in R$. Then $u \in R^*$ if and only if $\sigma(u) = 1$.

Let R be a PID. Then R is a UFD.

The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$ for a field F and UFDs.

6.3 Field of Fractions

Note: this part isn't easily summarizable. I recommend looking at the book.

Let R be an integral domain. There exists a field F, called the **field of fractions of** R, with the following properties:

(a): R is a subring of F.
(b): If R is a subring of some other field K, then there is a unique injective homomorphism $F \to K$ that takes R to itself by the identity map.

7 Fields Continued

7.1 Algebriac Numbers and Transcendental Numbers

Let L/F be an extension of fields, and let $\alpha \in L$. We say α is **algebraic over** F is α is the root of a non-zero polynomial in $F[x]$. Otherwise, α is **transcendental over** F.

Let L/F be an extension of fields, and let $\alpha \in L$. $F[\alpha]$ is the subring of L given by:

$$F[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \geq 0, a_0 \dots a_n \in F\} \tag{1}$$

We can also define $F[\alpha]$ as the image of the evaluation map:

$$E_\alpha : F[x] \to F, E_\alpha(f(x)) = f(\alpha) \tag{2}$$

$F(\alpha)$ is the smallest subfield of L containing both F and α.

$F[\alpha]$ is the smallest subring of L containing both F and α.

Let L/F be an extension of fields, and let $\alpha \in L$. Then:

$$F[\alpha] = F(\alpha) \iff \alpha \text{is algebraic over} F \tag{3}$$

Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. Then:

(a): $dim_F F[x]/f(x)F[x] = deg(f)$
(b): Let α be a root of $f(x)$ in some extension field of F. Then $[F(\alpha) : F] \leq deg(f)$.
(c): Let $f(x)$ be irreducible in $F[x]$ and $f(\alpha) = 0$. Then:

$$F(\alpha) \cong F[x]/f(x)F[x] \text{ and } [F(\alpha) : F] = deg(f)$$

If α and β are algebraic over F, then $\alpha + \beta$ and $\alpha\beta$ are as well.

7.2 Polynomial Roots and Multiplicative Subgroups

Let R be a commutative ring, and let $f(x) \in R[x]$ be a non-zero polynomial.

(a): Let α be a root of $f(x)$. Then there is a polynomial $g(x) \in R[x]$ such that $f(x) = (x - \alpha)g(x)$.
(b): Let R be an integral domain, and let $\alpha_1 \dots \alpha_n \in R$ be distinct roots of $f(x)$. Then there is a polynomial $g(x) \in R[x]$ such that $f(x) = (a - \alpha_1) \cdots (x - \alpha_n)g(x)$.
(c): Let R be an integral domain. A non-zero polynomial $f(x) \in R[x]$ of degree d has at most d distinct roots in R.

Let F be a field, and let $U \subseteq F^*$ be a finite subgroup of the multiplicative group of F. Then U is a cyclic group.

Let A be an abelian group, and let $\alpha\beta \in A$, and suppose that $o(\alpha) = m$ and $o(\beta) = n$.

(a): If $\gcd(m, n)$ is 1, then $\alpha\beta$ has order mn.
(b): If m is the largest order in elemnets of A. Then $n \mid m$.

7.3 Splitting Fields, Separability, and Irreducibility

Let F be a field, L/F an extension field, and let $f(x) \in F[x]$ be a non-zero polynomial. We say that f **splits completely in** L if $f(x)$ factors as:

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (c - \alpha_d)$$

For some $\alpha_1 \ldots \alpha_d \in L$.

We say that L is a **splitting field for** $f(x)$ **over** F if f splits completely in L but does not split completely in any proper subfield of L.

Let F be a field and let $f \in F[x]$ be a non-zero polynomial. Then: (a): There exists an extension field L/F that is a splitting field for $f(x)$ over F,
(b): If L/F is a splitting field for $f(x)$ over F, then the degree of L/F is bounded by:

$$[L : F] \leq deg(f)!$$

Let F be a field, let $f(x) \in F[x]$ be a polynomial, and write $f(x)$ as:

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d$$

Then, the **formal derivative of** $f(x)$ is:

$$f'(x) = a_1 + 2a_1 x + \cdots + d a_d x^{d-1}$$

Let F be a field, let $f(x), g(x) \in F[x]$ be polynomials, and let $a, b \in F$ be constants. Then: (a) Sum Rule: $(af + bg)'(x) = af'(x) + bg'(x)$.
(b) Product Rule: $(fg)'(x) = f(x)g'(x) = f'(x)g(x)$.
(c) Chain Rule: $(f \circ g)'(x) = f'(g(x))g'(x)$.
(d) If F has characteristic 0, then $f'(x) = 0$ if and only if $f(x) \in F$ (f is a constant polynomial).
(e): If F has characteristic $p > 0$, then $f'(x) = 0$ if and only if there is a polynomial $f_1(x) \in F[x]$ such that $f(x) = f_1(x^p)$.

Let F be a field and let $f(x) \in F[x]$ be a non-zero polynomial. f is **separable** if its roots are distinct. If f has one or more repeated roots, it is **inseparable**.

Let F be a field, and let $f(x) \in F[x]$ be a non-constant polynomial. Then:

$$f \text{ is separable} \iff gcd(f(x), f'(x)) = 1$$

Let F be a field. Then: (a): All irreducible $f(x) \in F[x]$ with a non-zero derivative are separable.
(b): If F has characteristic 0, then every irreducible polynomial in $F[x]$ is separable.

7.4 Finite Fields Revisited

Let p be a prime and let $d \geq 1$. Then: (a): There exists a field F containing exactly p^d elements.
(b): Any two fields containing p^d elements are isomorphic.