PMATH 347 Groups and Rings - Lecture Notes

Instructor: Yu-Ru Liu
LaTeX'd by Daniel Horton

University of Waterloo - Fall 2023

Contents

1 Groups

1.1 Basic Properties

Definition 1.1 (Groups)**:** Let G be a set and $* : G \times G \to G$. The pair $(G, *)$ is a group if it satisfies the following:

1. *Closure*: If $a, b \in G$, then $a * b \in G$.
2. *Associativity*: If $a, b, c \in G$ then $a * (b * c) = (a * b) * c$.
3. *Identity*: There exists $e \in G$ such that $a * e = a = e * a$ for all $a \in G$. In this case we call this element e an identity of G and it must be unique (see Proposition 1.1).
4. *Inverse*: For all $a \in G$, there exists some $b \in G$ such that $a * b = e = b * a$. We call b the inverse of a and it is also unique (see Proposition 1.1).

Notation 1.2: Normally in an abstract group we denote the group operation by multiplication (i.e. $a \cdot b$) or omit it entirely (i.e. ab).

Definition 1.3 (Abelian Groups)**:** A group G is abelian if $a * b = b * a$ for all $a, b \in G$.

Example 1.1: The pairs $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are all abelian groups but $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are not since they do not contain inverses for 0.

Proposition 1.1 (Uniqueness of the Identity and Inverses)**:** Let G be a group with $a \in G$. There exist unique elements $e, a^{-1} \in G$ satisfying the properties of the identity and the inverse of a respectively.

Proof.

- Let e_1, e_2 be two identities elements of G. Then $e_1 = e_1 * e_2 = e_2$ and so they are the same.
- Let b_1, b_2 be inverses of a in G. Then

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

and so they are the same as well.

□

Definition 1.4 (Units)**:** Let G be a group and $S \subseteq G$. An element $s \in S$ is a unit of S if $s^{-1} \in S$ as well. We denote the set of all units of S by $S^* := \{s \in S : \exists s^{-1} \in S, s * s^{-1} = e\}$.

Definition 1.5 (The General Linear Group)**:** For a field $\mathbb{F}$, we define the set

$$\mathrm{GL}_n(\mathbb{F}) := \{M \in M_n(\mathbb{F}) : \det(M) \neq 0\}.$$

When combined with matrix multiplication this set forms a group called the general linear group (see Proposition 1.2).

Proposition 1.2: $(\mathrm{GL}_n(\mathbb{F}), \cdot)$ is a group for all fields $\mathbb{F}$.

Proof.

1. *Closure:* Note that if $A, B \in \mathrm{GL}_n$ then $\det(AB) = \det(A)\det(B) \neq 0$ since $\det(A) \neq 0$ and $\det(B) \neq 0$.
2. *Associativity:* This follows from the associativity of matrix multiplication.
3. *Identity:* Clearly $I_n \in \mathrm{GL}_n(\mathbb{F})$ since $\det(I_n) = 1 \neq 0$.
4. *Inverse:* Since $\det(A) \neq 0$ for all $A \in \mathrm{GL}_n(\mathbb{F})$, we know that there exists a matrix A^{-1} such that $A^{-1}A = I = AA^{-1}$. Moreover, $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$ since $\det(A) \neq 0$ so $A^{-1} \in \mathrm{GL}_n(\mathbb{F})$ as well.

Note: $\mathrm{GL}_n(\mathbb{F})$ is only abelian in the trivial case when $n = 1$.

Notation 1.6: When dealing with multiple groups we use subscripts to distinguish their respective group operations and identity elements (i.e. $e_G *_G a = a$).

Definition 1.7 (Direct Product Groups)**:** Let $(G, *_G), (H, *_H)$ be groups. Their direct product group is $(G \times H, *)$ where $* : (G \times H) \times (G \times H) \to G \times H$ is defined by

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

This group has the identity $e = (e_G, e_H)$ and the inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1}).

Proposition 1.3 (Basic Group Identities)**:** Let G be a group and $g, g \in G$.

1. $(g^{-1})^{-1} = g$
2. $(gh)^{-1} = h^{-1}g^{-1}$
3. $g^n \cdot g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$
4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

Proof. The proof is left as an exercise. □

Note: In general $(gh)^n \neq g^n h^n$. This requires g and h to commute.

Proposition 1.4 (Algebraic Manipulation of Groups)**:** Let G be a group and $f, g, h \in G$. Then:

1. They satisfy left and right cancellation, namely:
   (a) If $gh = gf$ then $h = f$.
   (b) If $hg = fg$ then $h = f$.
2. The equations $gx = h$ and $yg = h$ have unique solutions for $x, y \in G$.

Proof.

1. (a) By multiplying by g^{-1} on the left we get:

$$gh = gf \implies g^{-1}gh = g^{-1}gf \implies h = f$$

   (b) Same as before but multiply by g^{-1} on the right.

2. Let $x = g^{-1}h$ and $y = hg^{-1}$. Clearly these are valid solutions. Now assume that u, v are additional solutions such that $gu = h$ and $vg = h$. This gives $gu = gx$ and $vg = yg$ and so by (1), $u = x$ and $v = y$.

□

1.2 Symmetric Groups and Cycles

Definition 1.8 (Permutations)**:** Given a non-empty set L, a permutation of L is a bijection from L to L.

Definition 1.9 (Symmetric Groups)**:** Given a non-empty set L, The set of all permutations of L is denoted by S_L and forms a group with function composition called the symmetric group over L.

Note: The identity element $\epsilon \in S_L$ is the identity transformation $\epsilon : L \to L$ with $\epsilon(x) = x$

Notation 1.10: For $n \in \mathbb{N}$ let S_n denote the symmetric group over the set $\{1, \cdots, n\}$.

Proposition 1.5: For all $n \in \mathbb{N}$, $|S_n| = n!$.

Proof. This follows from that fact that there are $n!$ ways to permute n objects. □

Definition 1.11 (Cycle Notation)**:** We can define elements $\sigma \in S_n$ by the cycles they form with the elements of $\{1, 2, \cdots, n\}$.

Example 1.2: Let $\sigma, \tau \in S_4$ with

$$\sigma(x) = \begin{cases} 2 & x = 1 \\ 1 & x = 2 \\ 4 & x = 3 \\ 3 & x = 4 \end{cases} \text{ and } \tau(x)) = x + 1 \mod 4.$$

Then in cycle notation we have:

$$\begin{aligned} \sigma &= (1\,2)(3\,4) \\ \sigma^{-1} &= (2\,1)(4\,3) \\ \tau &= (1\,2\,3\,4) \\ \tau^{-1} &= (4\,3\,2\,1) \\ \sigma\tau &= (2\,4) \\ \tau\sigma &= (1\,3) \end{aligned}$$

Theorem 1.6 (Cycle Decomposition Theorem)**:** If $\sigma \in S_n$ with $\sigma \neq \epsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2 and this factorization is unique up to the order of the factors.

Proof. The proof of Theorem 1.6 is left as an exercise (difficult). □

1.3 Cayley Tables

Definition 1.12 (Cayley Tables)**:** Given a group G and $x, y \in G$, if we write the product xy as the entry of a table in the row corresponding to x and column corresponding to y then such a table is called a Cayley table.

Note: By cancellation the entries in each row (or in each column) of a Cayley table are all distinct.

Example 1.3: Consider the groups $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}^*, \cdot)$ where $\mathbb{Z}^* = \{-1, 1\}$. These groups have the following Cayley tables:

$\mathbb{Z}_2$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$\mathbb{Z}^*$	-1	1
-1	1	-1
1	-1	1

Definition 1.13 (Cyclic Groups)**:** The cyclic group of order n is defined by

$$C_n := (\{1, a, a^2, \cdots, a^{n-1}\}, \cdot)$$

with $a^n = 1$ and $1, a, a^2, \cdots, a^{n-1}$ all distinct.

Example 1.4: The Cayley table for C_n is:

C_n	1	a	a^2	$\cdots$	a_{n-1}
1	1	a	a^2	$\cdots$	a_{n-1}
a	a	a^2	a^3	$\cdots$	1
a^2	a^2	a^3	a^4	$\cdots$	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_{n-1}	a_{n-1}	1	a	$\cdots$	a_{n-2}

Definition 1.14 (Isomorphic Groups)**:** We say that two groups G, H are isomorphic if their Cayley tables are the same (up to the naming and ordering of elements), in which case we write $G \cong H$.

Proposition 1.7 (Classification of Groups up to Order 4)**:** Let G be a group.

1. If $|G| = 1$, then $G \cong \{1\}$.
2. If $|G| = 2$, then $G \cong C_2$.
3. If $|G| = 3$, then $G \cong C_3$.
4. If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4 = C_2 \times C_2$.

Proof.

1. If $|G| = 1$ then trivially $G = \{1\}$ up to isomorphism.
2. If $|G| = 2$, then $G = \{1, g\}$ with $g \neq 1$. We must have a g^{-1} in G with $g^{-1} \neq 1$, so $g^{-1} = g$. This gives the Cayley table for C_2.
3. If $|G| = 3$, then $G = \{1, g, h\}$ with $g \neq 1$, $h \neq 1$ and $g \neq h$. By cancellation, $gh \neq g$ and $gh \neq h$. Thus $gh = 1$. Similarly, $hg = 1$. Since all entries on the same row of a Cayley table need to be distinct, this then gives $g^2 = h$ and $h^2 = g$. By observation of the resulting Cayley table, if we let $g = a$ and $h = a^2$ then we get $G \cong C_3$.
4. See assignment 1.

□

Definition 1.15 (The Klein 4-Group)**:** The group $K_4 \cong C_2 \times C_2$ is called the Klein 4-group.

2 Subgroups

2.1 Subgroups

Definition 2.1 (Subgroups)**:** Let G be a group and $H \subseteq G$ be a subset of G. If H is itself a group (using G's group operation) then we say that H is a subgroup of G.

Theorem 2.1 (The Subgroup Test)**:** Let G be a group and $H \subseteq G$. H is a subgroup if and only if the following are all true.

1. If $h_1, h_2 \in H$ then $h_1 h_2 \in H$.
2. $1_G \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proof.

$\implies$ This follows directly from the properties of a group.

$\impliedby$ By assumption the closure, identity and inverse properties of a group hold for H. As for associativity, since G was a group the group operation was associative over G, and so it must be associative over H as well. Hence H is a group.

□

Remark: Essentially, what the subgroup test is saying is that when determining if a subset is or isn't a subgroup we may ignore the associativity group axiom.

Definition 2.2 (The Special Linear Group)**:** The group $\mathrm{SL}_n(\mathbb{F}) = \{M \in M_n(\mathbb{F}) : \det(M) = 1\}$ is called the special linear group and it is a subgroup of $\mathrm{GL}_n(\mathbb{F})$.

Definition 2.3 (The Center of a Group)**:** The center of a group G is the set

$$Z(G) := \{z \in G : \forall x \in G, zx = xz\}$$

and it is an abelian subgroup of G (see Proposition 2.2).

Proposition 2.2: For all groups G, $Z(G)$ is an abelian subgroup of G.

Proof. Note that $Z(G)$ is by definition abelian, so we just need to show that it is a subgroup. We proceed by using the subgroup test (Theorem 2.1).

1. Let $y, z \in Z(G)$. By associativity and the definition of the center we have:

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

   So $yz \in Z(G)$.

2. Clearly $1_G \in Z(G)$ since by definition $1g = g = g1$.

3. Let $z \in Z(G)$ and $g \in G$. we have:

$$zg = gz \iff z^{-1}(gz)z^{-1} = z^{-1}(zg)z^{-1} \iff z^{-1}g = gz^{-1}$$

   So $z^{-1} \in Z(G)$ as well.

□

Proposition 2.3: Let H, K be subgroups of G. Then $H \cap K$ is a subgroup of G as well.

Proof. This follows easily from the subgroup test (Theorem 2.1). □

Proposition 2.4 (The Finite Subgroup Test)**:** If H is a finite non-empty subset of G, then H is a subgroup of G if and only if H is closed under G's group operation.

Proof.

$\implies$ This follows from the closure of a subgroup.

$\impliedby$ If $H = \emptyset$ then the statement is vacuously true, so assume there exists some $h \in H$. Since H is closed under the group operations, $\{h, h^2, h^3, \cdots\} \subseteq H$. Since h is finite these elements are not all distinct and there exists some $n, m \in N$ such that $h^n = h^{n+m}$. By cancellation this implies that $h^m = 1$ so $1 \in H$. Furthermore, $h \cdot h^{m-1} = h^m = 1$ so $h^{-1} = h^{m-1} \in H$ as well. Thus by the subgroup test (Theorem 2.1) H is a subgroup of G.

□

2.2 Alternating Groups

Recall that by the cycle decomposition theorem (Theorem 1.6) for $\sigma \in S_n$, with $\sigma \neq \epsilon$, σ can be decomposed uniquely (up to the ordering of its factors) as disjoint cycles of length at least 2.

Definition 2.4 (Transpositions)**:** A transposition $\sigma \in S_n$ is a cycle of length 2.

Remark: All larger cycles can be decomposed into transpositions (e.g. $(1\,2\,4\,5) = (1\,2)(2\,4)(4\,5) \in S_5$) however this factorization is not unique.

Theorem 2.5 (Parity Theorem)**:** If a permutation σ has two factorizations

$$\sigma = \gamma_1 \cdots \gamma_r = \mu_1 \cdots \mu_s$$

where each γ_i and μ_j is a transposition, then $r \equiv s \pmod 2$.

Proof. The proof of the parity theorem is left as a (difficult) exercise.

Definition 2.5 (Even and Odd Permutations)**:** A permutation σ is even or odd if it can be written as a product of an even or odd number of transpositions. By the parity theorem (Theorem 2.5) a permutation is either even or odd but not both.

Definition 2.6 (Alternating Groups)**:** For $n \geq 2$, the alternating group A_n is the set of all even permutations of S_n.

Note:

1. It follows from the next proposition (Proposition 2.6) and the subgroup test (Theorem 2.1) that this set is a group.
2. By construction, A_n is a subgroup of S_n.

Proposition 2.6 (Properties of Alternating Groups)**:** For $n \geq 2$ let A_n denote the set of all even permutations of S_n.

1. $\epsilon \in A_n$.
2. If $\sigma, \tau \in A_n$, then $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$.
3. $|A_n| = \frac{1}{2}n! = \frac{1}{2}|S_n|$.

Proof.

1. We can write $\epsilon = (1\,2)(1\,2)$ so ϵ is even and thus $\epsilon \in A_n$.
2. If $\sigma, \tau \in A_n$ we have
$$\sigma = \sigma_1 \cdots \sigma_{2r}, \tau = \tau_1 \cdots \tau_{2s}$$
where $r, s \in \mathbb{N}$. This gives
$$\sigma\tau = \sigma_1 \cdots \sigma_{2r}\tau_1 \cdots \tau_{2s}$$
so clearly $\sigma\tau \in A_n$ as well.
As for σ^{-1}, we note that since each σ_i is a transposition, $\sigma_i^{-1} = \sigma_i$. This gives
$$\sigma^{-1} = (\sigma_1 \cdots \sigma_{2r})^{-1} = \sigma_{2r}^{-1} \cdots \sigma_1^{-1} = \sigma_{2r} \cdots \sigma_1$$
so $\sigma^{-1} \in A_n$ as well.

3. Let O_n denote the set of odd permutations in S_n. By the parity theorem we have $S_n = A_n \cup O_n$ and $A_n \cap O_n = \emptyset$. Since $|S_n| = n!$, it now suffices to show that $|O_n| = |A_n|$. Let $\gamma = (1\,2)$ and define $f : A_n \to O_n$ by $f(\sigma) = \gamma\sigma$. Since $\sigma \in A_n$, $\gamma\sigma \in O_n$ and so f is well defined. Also, if $\gamma\sigma_1 = \gamma\sigma_2$ then $\sigma_1 = \sigma_2$ so f is 1 to 1. Finally, observe that
$$f(f(\sigma)) = (1\,2)(1\,2)\sigma = \sigma$$
so $f^{-1} = f$ and thus f is a bijection from A_n to O_n. We conclude $|A_n| = |O_n|$ and so $|A_n| = \frac{1}{2}n!$.

□

2.3 Orders of Elements

Definition 2.7 (Cyclic Subgroups)**:** Let G is a group and $g \in G$. We define
$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\cdots, g^{-2}, g^{-1}, 1, g, g^2, \cdots\}.$$
This set is called the cyclic subgroup generated by g (see Proposition 2.7).

Proposition 2.7: If G is a group then for all $g \in G$, $\langle g \rangle$ is a subgroup of G.

Proof. This follows from the subgroup test (Theorem 2.1). □

Definition 2.8 (Orders of Elements)**:** Let G be a group and $g \in G$. If n is the smallest positive integer such that $g^n = 1$, then we say the order of g is n (denoted $o(g) = n$). If no such n exists then we say that the order of g is infinite ($o(g) = \infty$).

Proposition 2.8 (Properties of Elements with Finite Order)**:** Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$, we have:

1. $g^k = 1 \iff n|k$
2. $g^k = g^m \iff k \equiv m \pmod{n}$
3. $\langle g \rangle = \{1, g, g^2, \cdots, g^{n-1}\}$

Proof.

1. $\Longleftarrow$ If $n|k$ then $k = nq$ for some $q \in \mathbb{Z}$. Thus
$$g^k = g^{nq} = (g^n)^q = 1^q = 1.$$
$\Longrightarrow$ By the division algorithm we can write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Since $g^k = 1$ and $g^n = 1$ we have,
$$g^r = g^{k-nq} = g^k(g^n)^{-q} = 1(1)^{-q} = 1.$$
Since $0 \leq r < n$ and $o(g) = n$, it follows that $r = 0$ and hence $n|k$.
2. Note that $g^k = g^m \iff g^{k-m} = 1$. By (1) this follows if and only if we have $n|(k-m)$.
3. It follows from (2) that $1, g, \cdots, g^{n-1}$ are all distinct. Clearly, we have $\{1, g, \cdots, g^{n-1}\} \subseteq \langle g \rangle$. To prove that other inclusion, let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then
$$x = g^k = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, \cdots, g^{n-1}\}.$$

□

Proposition 2.9 (Properties of Elements with Infinite Order)**:** Let G be a group and $g \in G$ satisfying $o(g) = \infty$. For $k \in \mathbb{Z}$, we have:

1. $g^k = 1 \iff k = 0$.
2. $g^k = g^m \iff k = m$.
3. $\langle g \rangle = \{\cdots, g^{-2}, g^{-1}, 1, g, g^2, \cdots\}$ are all distinct.

Proof.

1. $\implies$ $g^0 = 1$ by definition.
   $\impliedby$ If $g^k = 1$ for some $k \neq 0$, then $g^{-k} = (g^k)^{-1} = 1$ as well. Thus we can assume $k \geq 1$. However, this implies that $o(g)$ is finite.
2. Note that $g^k = g^m \iff g^{k-m} = 1$. By (1) this is equivalent to $k - m = 0$, i.e. $k = m$.
3. This follows directly from (2).

□

Proposition 2.10: Let G be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. For all $d \in \mathbb{N}$, $o(g^d) = \frac{n}{\gcd(n,d)}$. In particular, if $d|n$ then $\gcd(n, d) = d$ and $o(g^d) = \frac{n}{d}$.

Proof. Let $n_1 = \frac{n}{\gcd(n,d)}$ and $d_1 = \frac{d}{\gcd(n,d)}$. By a result from MATH135, we have $\gcd(n_1, d_1) = 1$. Note that

$$(g^d)^{n_1} = (g^d)^{\frac{n}{\gcd(n,d)}} = (g^n)^{\frac{d}{\gcd(n,d)}} = 1.$$

Thus it remains to show that n_1 is the smallest such positive integer.

Now suppose $(g^d)^r = 1$ with $r \in \mathbb{N}$. Since $o(g) = n$, by theorem 2.8 we have $n|dr$. Thus there exists $q \in \mathbb{Z}$ such that $dr = nq$. Dividing both sides by $\gcd(n, d)$ gives

$$d_1 r = \frac{d}{\gcd(n,d)} r = \frac{n}{\gcd(n,d)} q = n_1 q.$$

Since $n_1|d_1 r$ and $\gcd(n_1, d_1) = 1$, by another result from MATH135 we get $n_1|r_1$, i.e. $r = n_1 \ell$ for some $\ell \in \mathbb{Z}$.

Since $r_1, n_1 \in \mathbb{N}$ it follows that $\ell \in \mathbb{N}$. Since $\ell \geq 1$, we get $r \geq n$. □

2.4 Cyclic Groups

Proposition 2.11: Every cyclic group is abelian.

Proof. Let C_n be a cyclic group and $g, h \in C_n$. By the definition of a cyclic group $g = a^{k_1}$ and $h = a^{k_2}$ for some $k_1, k_2 \in \mathbb{Z}$. Thus

$$gh = a^{k_1} a^{k_2} = a^{k_1 + k_2} = a^{k_2} a^{k_1} = hg$$

so C_n is abelian. □

Proposition 2.12: Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle g \rangle$ be cyclic and let H be a subgroup of G. If $H = \{1\}$ then we are done so we may assume there exists a $g^k \in H$ with $k \neq 0$. Since H is group, $g^{-k} \in H$ as well so we may also assume $k \in \mathbb{N}$.

Let m be the smallest positive integer such that $g^m \in H$. Note that this means $\langle g^m \rangle \subseteq H$. To prove $H \subseteq \langle g^m \rangle$ we note that for all $h \in H$, $h = g^k$ for some $k \in \mathbb{N}$. By the division algorithm $k = mq + r$ with $0 \leq r < m$. Thus

$$g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$$

so $r = 0$, $m|k$ and $H \subseteq \langle g^m \rangle$. □

Proposition 2.13: Let $G = \langle g \rangle$ be cyclic with $o(g) = n \in \mathbb{N}$. Then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.

Proof. This follows directly from Proposition 2.10 and Proposition 2.8.

Theorem 2.14 (Fundamental Theorem of Finite Cyclic Groups)**:** Let $G = \langle g \rangle$ be a cyclic group of order n. Then:

1. If H is a subgroup of G then $H = \langle g^d \rangle$ for some $d|n$. Note it follows that $|H||n$.
2. Conversely, if $k|n$ then $\langle g^{n/k} \rangle$ is a subgroup of G of order k.

Proof.

1. By theorem 2.12 H is cyclic so we have $H = \langle g^m \rangle$ for some $m \in \mathbb{N}$. Let $d = \gcd(m, n)$, by a theorem from MATH135 there exist $x, y \in \mathbb{Z}$ such that $d = mx + ny$.
$$g^d = (g^m)^x (g^n)^y = (g^m)^x 1^y = (g^m)^x \in \langle g^m \rangle$$
2. By theorem 2.10 $o(g^{n/k}) = \frac{n}{\gcd(n,k)} = \frac{n}{\frac{n}{k}} = k$. Now suppose K is any subgroup of G of order k. By (1) $K = \langle g^d \rangle$ for some $d|n$. By theorem 2.8 we have $|K| = o(g^d)$. By theorem 2.10 we have $o(g^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d}$. Since $k = |K|$ we conclude $k = \frac{n}{d}$. It follows that $d = \frac{n}{k}$ and $K = \langle g^{\frac{n}{k}} \rangle$.

□

2.5 Non-Cyclic Groups

Definition 2.9 (Group Generators)**:** Given a group G and a nonempty subset $X \subseteq G$, the subgroup generated by X is the set

$$\langle X \rangle = \{x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} : k_i \in \mathbb{Z}\}.$$

Note: $\langle X \rangle$ is clearly a group by the subgroup test.

Definition 2.10 (Dihedral Groups)**:** For $n \geq 2$ the dihedral group of order $2n$ is defined by the set

$$D_{2n} = \{1, a, \cdots, a^{n-1}, b, ba, \cdots, ba^{n-1}\}$$

where $a^n = b^2 = 1$ and $aba = b$. Thus

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

Remark: In the cases $n = 2$ and $n = 3$ we have $D_4 \cong K_4$ and $D_6 \cong S_3$.

3 Normal Subgroups

3.1 Homomorphisms and Isomorphisms

Definition 3.1 (Group Homomorphisms)**:** Let G and H be groups. A mapping $\alpha : G \to H$ is a group homomorphism if

$$\alpha(a *_G b) = \alpha(a) *_H \alpha(b)$$

for all $a, b \in G$.

Example 3.1: Given a field $\mathbb{F}$, the map $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$ is a group homomorphism where $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Proposition 3.1 (Properties of Group Homomorphisms)**:** Let $\alpha : G \to H$ be a group homomorphism. Then:

1. $\alpha(1_G) = 1_H$
2. For all $g \in G, \alpha(g^{-1}) = \alpha(g)^{-1}$
3. For all $g \in G$ and $k \in \mathbb{Z}, \alpha(g^k) = \alpha(g)^k$

Proof. The proof is left as an exercise. □

Definition 3.2 (Group Isomorphisms)**:** Let G and H be groups. Consider $\alpha : G \to H$. If α is a bijective homomorphism then it is a group isomorphism.

Proposition 3.2: For all groups G, H,

$$G \cong H \iff \text{there exists a group isomorphism } \alpha : G \to H.$$

Remark: Recall that we defined $G \cong H$ in-terms of Cayley tables in Definition 1.14

Proof. The proof is left as an exercise. □

Proposition 3.3 (Properties of Group Isomorphisms)**:** Let G, H and K be groups.

1. The identity map $G \to G$ is a group isomorphism.
2. If $\sigma : G \to H$ is a group isomorphism then so is $\sigma^{-1} : H \to G$.
3. If $\sigma : G \to H$ and $\tau : H \to K$ are both group isomorphisms then $\sigma\tau = \sigma \circ \tau : G \to K$ is also a group isomorphism.

Proof. The proof is left as an exercise. □

Example 3.2: $(\mathbb{R}, +) \cong (\mathbb{R}_{++}, \times)$ where $\mathbb{R}_{++} = \{r \in \mathbb{R} : r > 0\}$ since the function $\sigma(x) = e^x$ is a group isomorphism from $\mathbb{R} \to \mathbb{R}_{++}$.

Example 3.3: $(\mathbb{Q},+) \ncong (\mathbb{Q}^*,\times)$ since if there existed a group isomorphism $\tau : \mathbb{Q} \to \mathbb{Q}^*$ then there would exist a $q \in \mathbb{Q}$ such that $\tau(q) = 2$. Letting $\tau(\frac{q}{2}) = a$ this gives:

$$2 = \tau(q) = \tau\left(\frac{q}{2} + \frac{q}{2}\right) = \tau\left(\frac{q}{2}\right)\tau\left(\frac{q}{2}\right) = a^2$$

So $a \in \mathbb{Q}^*$ with $a^2 = 2$ which is a contradiction.

Corollary 3.3.1: The existence of an isomorphism between two groups forms an equivalence relation.

Proof. The proof is left as an exercise (hint, use part 3 of Proposition 3.3). □

3.2 Cosets and Lagrange's Theorem

Definition 3.3 (Cosets)**:** Let H be a subgroup of G and $a \in G$. The right coset of H generated by a is the set

$$Ha := \{ha : h \in H\}.$$

Similarly, the left coset of H generated by a is

$$aH := \{ah : h \in H\}.$$

Proposition 3.4 (Properties of Cosets)**:** Let H be a subgroup of G, and let $a, b \in G$.

1. $Ha = Hb \iff ab^{-1} \in H$. In particular, $Ha = H \iff a \in H$.
2. If $a \in Hb$, then $Ha = Hb$.
3. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Thus the distinct right cosets of H form a partition of G.

Proof.

1. If $Ha = Hb$ then $a = 1 \cdot a \in Ha = Hb$ and so $a = hb$ for some $h \in H$ so $ab^{-1} = h$. Conversely, if $ab^{-1} \in H$ then for all $h \in H$ we may write $ha = hab^{-1}b = h^2b \in Hb$ so $Ha \subseteq Hb$. On the other hand, if $ab^{-1} = h$ then $ba^{-1} = h^{-1} \in H$. So for all $h \in H$, $hb = hba^{-1}a = hh^{-1}a = a \in Ha$ so $Hb \subseteq Ha$ as well.
2. If $a \in Hb$, then $a = hb \implies ab^{-1} = h$ for some $h \in H$ and so by (1), $Ha = Hb$.
3. If $Ha \cap Hb = \emptyset$ then we are done, so we may assume there exists an $x \in Ha \cap Hb$. Since $x \in Ha$ and $x \in Hb$, by (2) we have $Ha = Hx = Hb$.

□

Definition 3.4 (Indices of Subgroups)**:** Let G be a group and H be a subgroup of G. The index of H in G denoted $[G : H]$ is the number of distinct right (or left) cosets of H in G.

Theorem 3.5 (Lagrange's Theorem)**:** Let H be a subgroup of a finite group G. We have $|H||G|$ and

$$[G : H] = \frac{|G|}{|H|}.$$

Proof. This follows from part 3 of Proposition 3.4. □

Corollary 3.5.1: If G is a finite group and $g \in G$ then $o(g) \big| |G|$.

Proof. Take $H = \langle g \rangle$, notice that $|H| = o(g)$. The result follows from Lagrange's theorem (Theorem 3.5). □

Corollary 3.5.2: If G is a finite group with $|G| = n$, then for all $g \in G$, we have $g^n = 1$.

Proof. This follows from Corollary 3.5.1 and Proposition 2.8. □

Definition 3.5 (Euler's ψ-Function)**:** Euler's ψ-function, $\psi : \mathbb{N} \to \mathbb{N}$ is defined as

$$\psi(n) = \#\{k \in \{0, \cdots, n-1\} : \gcd(k, n) = 1.$$

Example 3.4: For $n \geq 2$ let $\mathbb{Z}_n^*$ be the set of (multiplicatively) invertible elements in $\mathbb{Z}_n$. Then

$$\psi(n) = |\mathbb{Z}_n|.$$

This follows from a result from MATH135.

Theorem 3.6 (Euler's Theorem)**:** If $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ then $a^{\psi(n)} \equiv 1 \pmod{n}$. When $n = p$ is prime this gives Fermat's little theorem.

Proof. This follows from the definition of $\psi(n)$ and Corollary 3.5.1. □

Proposition 3.7: If G is a group with $|G| = p$ for some prime p then $G \cong C_p$.

Proof. Let $g \in G$ with $g \neq 1$. Then by Corollary 3.5.1 we have $o(g) | p$. Since $g \neq 1$ and p is a prime this implies $o(g) = p$. By Proposition 2.8 we have

$$|\langle g \rangle| = o(g) = p.$$

It follows that $G = \langle g \rangle \cong C_p$. □

Proposition 3.8: Let H, K be finite subgroups of a group G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof. By Proposition 2.3, $H \cap K$ is a subgroup of G and H. By Lagrange's Theorem (Theorem 3.5), we have $|H \cap K| \big| |H|$ and $|H \cap K| \big| |K|$. The result follows from $\gcd(|H|, |K|) = 1$. □

3.3 Normal Subgroups

Definition 3.6: Let H be a subgroup of G. If $gH = Hg$ for all $g \in G$, we say H is normal in G, denoted $H \lhd G$.

Theorem 3.9 (The Normality Test)**:** Let H be a subgroup of G. The following are all equivalent.

1. $H \lhd G$
2. For all $g \in G, gHg^{-1} \subseteq H$
3. For all $g \in G, gHg^{-1} = H$

Proof.

- $(1 \implies 2)$**:** Suppose $H \lhd G$ and thus $gH = Hg$. This means for all $g \in G$ and $h \in H$, there exists an $h' \in H$ such that $gh = h'g$. Now suppose $x = ghg \in gHg^{-1}$. We have $x = h'gg^{-1} = h' \in H$ so $gHg^{-1} \subseteq H$.
- $(2 \implies 3)$**:** If $g \in G$ then by (2), $gHg^{-1} \subseteq H$. Taking g^{-1} in place of g gives $g^{-1}Hg \subseteq H$. This implies $H \subseteq gHg^{-1}$. Thus $gHg^{-1} = H$.
- $(3 \implies 1)$**:** If $gHg^{-1} = H$, then $gH = Hg$.

□

Proposition 3.10: If H is a subgroup of G and $[H : G] = 2$, then $H \lhd G$.

Proof. Let $g \in G$. If $g \in H$ then $Hg = H = gH$ and we are done, so we may assume $g \notin H$. Since $[G : H] = 2$, $G = H \cup Hg$ and $H \cap Hg = \emptyset$. Thus $Hg = G \setminus H$. Similarly, $gH = G \setminus H$. Thus $Hg = gH$ for all $g \in G$ and so $H \lhd G$. □

Definition 3.7 (Products of Subgroups)**:** Let H, K be subgroups of G. We define their product HK to be the set

$$HK := \{hk : h \in H \text{ and } k \in k\}.$$

Proposition 3.11: Let H and K be subgroups of G. The following are all equivalent.

1. HK is a subgroup of G.
2. $HK = KH$
3. KH is a subgroup of G

Proof. We'll prove (1) $\iff$ (2), then (2) $\iff$ (3) will follow by interchanging H and K.

- $(2 \implies 1)$**:** We have $1 \cdot 1 \in HK$. Also if $hk \in HK$ then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Additionally, for $hk, h_1k_1 \in HK$, we have $kh_1 \in KH = HK$, say $kh_1 = h_2k_2$. It follows that $(hk)(h_1k_1) = h(kh_1)k_1 = h(h_2k_2)k_1 = (hh_2)(k_2k_1) \in HK$. So by the subgroup test, HK is a subgroup of G.
- $(2 \implies 1)$**:** Let $kh \in KH$. Since H and K are subgroups of G, we have $h^{-1} \in H$ and $k^{-1} \in K$. Since HK is also a subgroup of G, we have $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus we have $KH \subseteq HK$. On the other hand, if $hk \in HK$, since HK is a subgroup of G, we have $(hk)^{-1} = k^{-1}h^{-1} \in HK$, say $k^{-1}h^{-1} = h_1k_1$. Thus $hk = k_1^{-1}h_1^{-1} \in KH$ so $HK \subseteq KH$. It follows that $HK = KH$.

□

Proposition 3.12: Let H and K be subgroups of a group G.

1. If $H \lhd G$ or $K \lhd G$, then $HK = KH$ is a subgroup of G.
2. If $H \lhd G$ and $K \lhd H$ then $HK \lhd G$

Proof.

1. Suppose $H \lhd G$. Then $HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH$. By lemma 3.11, $HK = KH$ is a subgroup of G.
2. If $g \in G$ and $hk \in HK$, since $H \lhd G$ and $K \lhd G$ we have
$$\begin{aligned} g^{-1}(hk)g &= g^{-1}(hgg^{-1}k)g \\ &= (g^{-1}hg)(g^{-1}kg) \in HK \end{aligned}$$
Thus $HK \lhd G$.

□

Definition 3.8 (Normalizers)**:** Let H be a subgroup of G. The normalizer of H, denoted $N_G(H)$ is defined to be
$$N_G(H) := \{g \in G : gH = Hg\}.$$

Note: We see that $H \lhd G \iff N_G(H) = G$. We also note that in the proof of 3.12 we did not need the full assumption $H \lhd G$. We only needed $k \in N_G(H)$ for all $k \in K$.

Corollary 3.12.1: Let H and K be subgroups of G. If $K \subseteq N_G(H)$, then $HK = KH$ is a subgroup of G.

Proof. See the note above. □

Proposition 3.13: If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

Proof. Define $\sigma : H \times K \to HK$ by $\sigma(h, k) = hk$.

Claim 3.13.1: If $H \lhd G$ and $K \lhd G$ such that $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$.

Proof. Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $khk^{-1} \in kHk^{-1} \in H$. Thus $x = h(kh^{-1}k^{-1}) \in H$. Similarly, one can show that $x \in K$. Since $x \in H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, i.e. $hk = kh$. □

Claim 3.13.2: σ is an isomorphism.

Proof. Let $(h, k), (h_1, k_1) \in H \times K$. By claim 1 we have $h_1k = kh_1$. Thus,
$$\sigma((h, k)(h_1, k_1)) = \sigma((hh_1, kk_1)) = hh_1kk_1 = hkh_1k_1 = \sigma((h, k))\sigma((h_1, k_1))$$
and σ is a homomorphism. Note that by the definition of HK, σ is onto. Also, if $\sigma((h, k)) = \sigma((h_1, k_1))$ then we have $hk = h_1k_1$. Thus $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$ implying $h_1^{-1}h = 1 = k_1^{-1}k$ (i.e. $h_1 = h$ and $k_1 = k$). Thus σ is 1-1, and hence it is an isomorphism. □

By Claim 3.13.2, $HK \cong H \times K$. □

Corollary 3.13.3: Let G be a finite group and let H, K be normal subgroups of G such that $H \cap K = \{1\}$ and $|H||K| = |G|$. Then $G \cong H \times K$.

Proof. This follows from Proposition 3.13 and the fact that $|H \times K| = |H||K| = |G|$. □

4 Isomorphism Theorems

4.1 Quotient Groups

Definition 4.1 (Coset Multiplication)**:** Let G be a group with a subgroup K. We define multiplication on the cosets of K as

$$Ka \cdot Kb := Kab$$

for all $a, b \in G$. Note that we could have $Ka = Ka_1$ and $Kb = Kb_1$ for some $a_1 \neq a$ and $b_1 \neq b$. Thus in order for this operation to make sense, a necessary condition is

$$Ka = Ka_1 \text{ and } Kb = Kb_1 \iff aa_1^{-1} \in K \text{ and } bb_1^{-1} \in K \implies Kab = Ka_1b_1.$$

In this case we say that the multiplication is well-defined.

Lemma 4.1: Let K be a subgroup of G. The following are equivalent:

1. $K \lhd G$
2. For all $a, b \in G$, the multiplication $Ka \cdot Kb = Kab$ is well-defined.

Proof.

$\implies$ Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To get $Kab = Ka_1b_1$ it suffices to show $ab(a_1b_1)^{-1} \in K$. Note that since $K \lhd G$, we have $aKa^{-1} \subseteq K$. Thus,

$$ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} = abb_1^{-1}a^{-1}aa_1^{-1} = (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in K$$

since by assumption $K \lhd G$. It follows that $Kab = Ka_1b_1$.

$\impliedby$ It suffices to show that $aka^{-1} \in K$ for all $k \in K$ and $a \in G$. Since $Kk = K1$,

$$Kak = Ka \cdot K1 = Ka$$

by assumption. It follows that $aka^{-1} \in K$. Thus $K \lhd G$.

□

Proposition 4.2 (Properties of Quotient Groups)**:** Let $K \lhd G$ and write $G/K = \{Ka : a \in G\}$.

1. G/K is a group under the operation $Ka \cdot Kb = Kab$.
2. The mapping $\phi : G \to G/K$ given by $\phi(a) = Ka$ is an onto homomorphism.
3. If $[G : K]$ is finite, then $|G/K| = [G : K]$. In-particular, if $|G|$ is finite, then $|G/K| = \frac{|G|}{|K|}$.

Proof.

1. By Lemma 4.1, the group operation is well defined and G/K is closed under it. The identity element is $K = K1$ since $Ka \cdot K1 = Ka = K1 \cdot Ka$ for all $Ka \in G/K$. Also, since $Ka \cdot Ka^{-1} = K1 = Ka^{-1} \cdot Ka$, the inverse of Ka is Ka^{-1}. Finally, by the associativity of G, we have $Ka(Kb \cdot Kc) = (Ka \cdot Kb)Kc$. It follows that G/K is a group.

2. ϕ is clearly onto. Also, for $a, b \in G$ we have $\phi(a)\phi(b) = Ka \cdot Kb = Kab = \phi(ab)$. Thus ϕ is a homomorphism.

3. If $[G : K]$ is finite, then by the definition of the index $[G : K]$, we have $|G/K| = [G : K]$. Also, if $|G|$ is finite, by Lagrange's theorem (Theorem 3.5)

$$|G/K| = [G : K] = \frac{|G|}{|K|}.$$

□

Definition 4.2 (Quotient Groups)**:** Let $K \lhd G$. The group G/K of all cosets of K in G is called the quotient group of G by K. Also, the mapping $\phi : G \to G/K$ given by $\phi(a) = Ka$ is called the coset map of K in G.

4.2 Isomorphism Theorems

Definition 4.3 (Kernals and Images)**:** Let $\alpha : G \to H$ be a group homomorphism. The kernal of α is

$$\ker(\alpha) := \{g \in G : \alpha(g) = I_H\} \subseteq G$$

and the image of α is

$$\text{Im}(\alpha) = \alpha(G) = \{\alpha(g) : g \in G\} \subseteq G.$$

Proposition 4.3: Let $\alpha : G \to H$ be a group homomorphism.

1. $\text{Im}(\alpha)$ is a subgroup of H.
2. $\ker(\alpha)$ is a normal subgroup of G.

Proof.

1. Note that $1_H = \alpha(1_G) \in \alpha(G)$ and for $h_1 = \alpha(g_1)$, $h_2 = \alpha(g_2)$ in $\alpha(G)$, we have

$$h_1 h_1 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G).$$

   Also, by theorem 3.1, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$. By the subgroup test (Theorem 2.1) $\alpha(G)$ is a subgroup of H.

2. For $\ker(\alpha)$, note that we have $\alpha(1_G) = 1_H$. Also, if $k_1, k_2 \in \ker(\alpha)$, then

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1\dot{1} = 1$$

   and $\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1$. By the subgroup test (Theorem 2.1), $\ker(\alpha)$ is a subgroup of G.

   Now note that if $g \in G$ and $k \in \ker(\alpha)$, then

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)\alpha(g)^{-1} = 1$$

   Thus $g(\ker(\alpha))g^{-1} \subseteq \ker(\alpha)$ and by the normality test (Theorem 3.9) we have $\ker(\alpha) \lhd G$.

□

Theorem 4.4 (First Isomorphism Theorem)**:** Let $\alpha : G \to H$ be a group homomorphism. We have

$$G/\ker(\alpha) \cong \mathrm{Im}(\alpha).$$

Proof. Let $K = \ker(\alpha)$. Since $K \lhd G$, G/K is a group. Define the group map $\overline{\alpha} : G/K \to \mathrm{Im}(\alpha)$ by:

$$\overline{\alpha}(kg) = \alpha(g)$$

for all $kg \in G/K$.

Note that:

$$kg = kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg^{-1}) = 1 \iff \alpha(g) = \alpha(g_1)$$

Thus $\overline{\alpha}$ is well-defined and 1 to 1. Also, $\overline{\alpha}$ is clearly onto. It follows that $\overline{\alpha}$ is a group homomorphism. Thus $\mathrm{Im}(\alpha) \cong G/\ker(\alpha)$. □

Proposition 4.5: Let $\alpha : G \to H$ be a group homomorphism and $K = \ker(\alpha)$. Then α factors uniquely as $\alpha = \overline{\alpha} \circ \phi$, where $\phi : G \to G/K$ is the coset map and $\overline{\alpha} : G/K \to H$ is defined by $\overline{\alpha}(kg) = \alpha(g)$. Note that ϕ is onto and 1 to 1.

Note: By uniquely we mean that $\overline{\alpha}$ is the only homomorphism $G/K \to H$ satisfying $\overline{\alpha} \circ \phi = \alpha$.

Proof. The proof is left as an exercise. □

Proposition 4.6: If G is a cyclic group then either $G \cong \mathbb{Z}_n$ (if G is finite) or $G \cong \mathbb{Z}$ (if G is infinite).

Proof. Let G be a cyclic group and consider the map $\alpha : (\mathbb{Z}, +) \to G$ defined by $\alpha(k) = g^k$ for some $g \in G$ with $g \neq 1$. Note that α is a group homomorphism and since G is cyclic α is onto. Also note that $\ker(\alpha) = \{k \in \mathbb{Z} : g^k = 1\}$.

If $o(g) = \infty$ then by Proposition 2.9 $\ker(\alpha) = \{0\}$ and so by the first isomorphism theorem (Theorem 4.4) $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

On the other hand, if $o(g) = n$ then by Proposition 2.8 $\ker(\alpha) = n\mathbb{Z}$ and so by the first isomorphism theorem (Theorem 4.4) $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. □

Theorem 4.7 (Second Isomorphism Theorem)**:** Let H and K be subgroups of a group G with $K \lhd G$. Then HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$ and

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. Since $K \lhd G$, HK is a subgroup, $HK = KH$ and $K \lhd HK$. Consider the map $\alpha : H \to \frac{HK}{K}$ given by

$$\alpha(h) = Kh.$$

Then α is a homomorphism (exercise).

Now let $x \in HK = KH$. We have $x = kh$ and so $Kx = Kkh = Kh = \alpha(h)$ so α is onto. By a previous theorem,

$$\ker(\alpha) = \{h \in H : Kh = K\} = \{k \in K : Hk = H\} = H \cap K$$

so by the first isomorphism theorem we have:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

□

Theorem 4.8 (Third Isomorphism Theorem)**:** Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then $H/K \subseteq G/K$ and

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Proof. Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$. To see that this map is well-defined, note that if $Kg = Kg_1$ then $gg_1^{-1} \in K \subseteq H$ and thus $Hg = Hg_1$ as well. Clearly α is onto as well.

Next, note that

$$\ker(\alpha) = \{Kg : Hg = H\} = \{Kg : g \in H\} = H \cap K.$$

By the first isomorphism theorem, this means that

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

□

5 Group Actions

5.1 Cayley's Theorem

Theorem 5.1 (Cayley's Theorem)**:** If G is a finite group with $|G| = n$ then G is isomorphic to a subgroup of S_n.

Proof. Let $G = \{g_1, \cdots, g_n\}$ and let S_G be the permutation group of G. By identifying g_i with $1 \leq i \leq n$ we see that $S_G \cong S_n$. Thus, to prove the theorem it suffices to find a 1-1 homomorphism $\sigma : G \to S_G$ (so the kernel will be $\{1\}$ and we can apply the first isomorphism theorem).

For $a \in G$ define $\mu_a : G \to G$ by $\mu_a(g) = ag$. Clearly μ is a 1-1 homomorphism and so by the first isomorphism theorem we have $G \cong G/\{1\} \cong \operatorname{Im}\sigma$, as subgroup of S_n. □

Theorem 5.2 (Extended Cayley's Theorem)**:** Let H be a subgroup of a group G with $[G : H] = m < \infty$. If G has no normal subgroups contained in H except $\{1\}$, then G is isomorphic to a subgroup of S_m.

Proof. Let $X = \{g_1H, \cdots, g_mH\}$ be the set of left cosets of G and $\lambda_a : X \to X$ be defined by

$$\lambda_a(gH) = agH.$$

Now let $\tau : G \to S_X \cong S_m$ be defined by

$$\tau(a) = \lambda_a$$

and defined $K = \ker\tau \subseteq H$. By the first isomorphism theorem we have $G/K \cong \operatorname{Im}\tau$. Since $K \subseteq H$ and $K \lhd G$, by the assumption, $K = \{1\}$. It follows that $G \cong \operatorname{Im}\tau$, a subgroup of $S_X \cong S_m$. □

Corollary 5.2.1: Let G be a finite group and p be the smallest prime divisor of $|G|$. If H is a subgroup of G with $[G : H] = p$, then $H \lhd G$.

Remark: This is a generalization of Proposition 3.10 where we had $p = 2$.

Proof. Let X be the set of all left cosets of $H \subseteq G$ and consider the homomorphism $\tau : G \to S_X$ from the previous proof. Note that if $a \in \ker(\tau)$ then $\lambda_a \epsilon$. Thus

$$H = \lambda_a(H) = aH$$

and hence $a \in H$. Thus $\ker(\tau) \subseteq H$ and so by the first isomorphism theorem (Theorem 4.4) $G/\ker(\tau)$ is isomorphic so some subgroup of S_p. Now let

$$k = [H : \ker(\tau)].$$

By Lagrange's theorem (Theorem 3.5) this gives

$$\left|\frac{G}{K}\right| = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = pk$$

and so $pk|p! \implies k|(p-1)!$.

Since $k\big||H|$, $|H|\big||G|$ and p is the smallest prime divisor of $|G|$, so the only prime divisor k can have is p. However, p cannot be a divisor of k since $k|(p-1)!$. We conclude k has no prime divisors and hence $k = 1$. Therefore $\ker(\tau) = H$ and so $H \lhd G$. □

5.2 Group Actions

Definition 5.1 ((Left) Group Actions)**:** Let G be a group and X be a non-empty subset of G. A (left) group action of G on X is a mapping $G \times X \to X$, denoted $(a, x) \to a \cdot x$ such that

1. $1 \cdot x = x$ for all $x \in X$.
2. $a \cdot (b \cdot x) = (ab) \cdot x$ for all $a, b \in G$ and $x \in X$.

In this case we say G acts on X.

Note: Let G be a group acting on an set $X \neq \emptyset$. For $a, b \in G$ and $x, y \in X$, by (1) and (2), we have

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y.$$

In particular, we have $a \cdot x = a \cdot y \iff x = y$.

Example 5.1: If G is a group, let G act on itself (i.e. $X = G$) by

$$a \cdot x = axa^{-1}$$

for all $a, x \in G$. Note that this satisfies the definition of a group action. In this case we say G acts on itself by conjugation.

Remark: For all $a \in G$, define $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. Then one can show (see assignment 5):

1. $\sigma_a \in S_X$
2. The function $\theta : G \to S_X$ given by $\theta(a) = \sigma(a)$ is a group homomorphism with

$$\ker\theta = \{a \in G : a \cdot x = x \text{ for all } x \in X\}$$

Note that the group homomorphism θ gives an equivalent definition of a group action of G on X. If $X = G$ with $|G| = n$ and $\ker\theta = 1$, the map $\theta : G \to S_G \cong S_n$ show that G is isomorphic to a subgroup of S_n which is Cayley's theorem.

Definition 5.2: Let G be a group acting on a set X and $x \in X$. We denote by

$$G \cdot x := \{g \cdot x : g \in G\} \subseteq X$$

the orbit of x and

$$S(x) := \{g \in G : g \cdot x = x\} \subseteq G$$

the stabilizer of x.

Proposition 5.3: Let G be a group on a set $X \neq \emptyset$ and $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizer of x. Then:

1. $S(x)$ is a subgroup of G.
2. There exists a bijection from $G \cdot x$ to $\{gS(x) : g \in G\}$ and $|G \cdot x| = [G : S(x)]$.

Proof.

1. Since $1 \cdot x = x$ we have $1 \in S(x)$. Also, if $g, h \in S(x)$ then

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

and

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x$$

Thus $gh, g^{-1} \in S(x)$. By the subgroup test (Theorem 2.1, $S(x)$ is a subgroup of G.

2. Write $S(x) = S$ and consider the map

$$\phi : G \cdot x \to \{gS : g \in G\}$$

defined by

$$\phi(g \cdot x) = gS.$$

Note that

$$\begin{aligned} g \cdot x = h \cdot x &\iff (h^{-1}g) \cdot x = x \\ &\iff h^{-1}g \in S \\ &\iff gS = hS \end{aligned}$$

Thus ϕ is well-defined and 1-1. Since ϕ is clearly onto, ϕ is a bijection. It follows that

$$|G \cdot x| = |\{gS : g \in G\}| = [G : S].$$

□

Theorem 5.4 (Orbit Decomposition Theorem)**:** Let G be a group acting on a finite set $X \neq \emptyset$. Let

$$X_f = \{x \in X : a \cdot x = x, \forall a \in G\}.$$

Note that $x \in X_f$ if and only if $|G \cdot x| = 1$. Let $G \cdot x_1, \cdots, G \cdot x_n$ denote the distinct non-singleton orbits (i.e. $|G \cdot x_i| > 1$). Then

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)].$$

Proof. Note that for $a, b \in G$ and $x, y \in X$:

$$\begin{aligned} a \cdot x = b \cdot y &\iff (b^{-1}a) \cdot x = y \\ &\iff y \in G \cdot x \\ &\iff G \cdot x = G \cdot y \end{aligned}$$

Thus two orbits are either disjoint or the same. It follows that the orbits from a disjoint cover of X. Since $x \in X_f$ if and only if $|G \cdot x| = 1$, the set $G \setminus X_f$ contains all non-singleton orbits, which are disjoint. Thus by prop 5.4, we have:

$$|X| = |X_f| + \sum_{i=1}^{n} |G \cdot x_i| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

□

Definition 5.3 (Centralizers)**:** Let G be a group. For $x \in G$ the set

$$C_G(x) = \{g \in G : gx = xg\}$$

is called the centralizer of x in G. Note that $Z(G) \subseteq C_G(x)$ for all $x \in G$.

Remark: If G is a group acting on itself by conjugation, then $G_f = Z(G)$ and $S(x) = C_G(x)$ for all $x \in G$. In this case, the orbit

$$G \cdot x = \{gxg^{-1} : g \in G\}$$

is called the conjugacy class of x.

Corollary 5.4.1 (The Class Equation)**:** Let G be a finite group and let

$$\{gx_1g^{-1} : g \in G\}, \cdots, \{gx_ng^{-1} : g \in G\}$$

denote the distinct non-singular conjugacy classes. Then:

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

Proof. This follows directly from the orbit decomposition theorem. □

Lemma 5.5: Let p be a prime and $m \in \mathbb{N}$. Let G be a group of order p^m acting on a finite set $X \neq \emptyset$. Let X_f be defined as in the orbit decomposition theorem (Theorem 5.4). Then $|X| \equiv |X_f| \mod p$.

Proof. By the orbit decomposition theorem (Theorem 5.4) we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x)]$$

with $[G : S(x_i)] > 1$ for all i. Since $[G : S(x_i)]$ divides $|G| = p^m$ and $[G : S(x_i)] > 1$, we have $p | [G : S(x_i)]$ for all i. It follows that $|X| = |X_f| \mod p$. □

Theorem 5.6 (Cauchy's Theorem)**:** Let p be a prime and G a finite group. If $p||G|$ then G contains an element of order p.

Proof. Define

$$X := \{(a_1, \cdots, a_p) : a_i \in G, a_1 \cdots a_p = 1\}.$$

Notice that for any $(a_1, \cdots, a_{p-1}) \in G^{p-1}$ we have

$$(a_1, \cdots, a_p) \in X \iff a_p = (a_1 \cdots a_{p-1})^{-1} = a_{p-1}^{-1} \cdots a_1^{-1}.$$

This means that if $|G| = n$ then $|X| = n^{p-1}$. Since $p|n$ this means that $|X| \equiv 0 \bmod p$. Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on X by "cycling" i.e. for $k \in \mathbb{Z}_p$,

$$k \cdots (a_1, \cdots, a_p) = (a_{k+1}, \cdots, a_p, a_1, \cdots, a_k).$$

One can verify this action is well-defined (exercise).

Now let X_f be defined as in the orbit decomposition theorem (Theorem 5.4). Then

$$(a_1, \cdots, a_p) \in X_f \iff a_1 = \cdots = a_p \text{ and } a_i^p = 1.$$

Clearly $(1, \cdots, 1) \in X_f$ so $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, by the previous lemma we have $|X_f| \equiv |X| \bmod p$. Since $|X| \equiv 0 \bmod p$ and $|X_f| \geq 1$ it follows that $|X_f| \geq p$. It follows that there exists an element $a \neq 1$ such that $a^p = 1$. □

6 Sylow Theorems

6.1 p-Groups

Definition 6.1 (p-Groups)**:** Let p be a prime. A group in which every element has an order of a non-negative power of p is called a p-group.

Note: By Cauchy's theorem we have that a finite group G is a p-group if and only if $|G|$ is a power of p.

Lemma 6.1: The center $Z(G)$ of a non-trivial finite p-group G contains more than one element.

Proof. Recall the class equation of G.

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

where $[G : C_G(x_i)] > 1$. Since G is a p-group, by the previous remark we have $|G|$ is a power of p. By Lemma 5.5 we have $|G| \equiv |Z(G)| \bmod p$. It follows that $p|Z(G)$. Since $1 \in Z(G)$, $|Z(G)| \geq 1$ and so $|Z(G)| \geq p$. □

Lemma 6.2: If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \bmod p$.

Proof. Let X be the set of all left cosets of H in G, hence $|X| = [G : H]$. Let H act on X by left multiplication. For $x \in G$ we have:

$$\begin{aligned} xH \in X_f &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hxH = H, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|X_f|$ is the number of cosets xH with $x \in N_G(H)$, and hence $|X_f| = [N_G(H) : H]$. By Lemma 5.5,

$$[N_G(H) : H] = |X_f| \equiv |X| = [G : H] \mod p.$$

□

Corollary 6.2.1: Let H be a p-subgroup of a group G. If $p|[G : H]$ then $p|[N_G(H) : H]$ and $N_G(H) \neq H$.

Proof. Since $p|[G : H]$ by Lemma 6.2 we have $[N_G(H) : H] \equiv 0 \mod p$ and so $p|[N_G(H) : H]$. Since $|N_G(H)| \geq 1$ we have $[N_G(H) : H] \geq p$ and so $N_G(H) \neq H$. □

6.2 Sylow's Three Theorems

Theorem 6.3 (First Sylow Theorem)**:** Let G be a group with $|G| = p^n m$ where p is a prime and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, for $i < n$ all subgroups of order p^i are normal in some other subgroup of order p^{i+1}.

Proof. We proceed by induction on i.

- **Base Case:** $i = 1$.

  When $i = 1$, since $p||G|$ by Cauchy's theorem (Theorem 5.6) there exists $a \in G$ with $o(a) = p$ and hence $\langle a \rangle$ is a subgroup of order p.

- **Inductive Case:** Suppose the for some $1 \leq i < n$, G has a subgroup H of order p^i.

  Since G is finite, by Lagrange's theorem (Theorem 3.5) we have $[G : H] = \frac{|G|}{|H|} = p^{n-i}m$ so $p|[G : H]$. By the previous corollary this means $p|[N_G(H) : H]$ and $[N_G(H) : H] \geq p$. Thus by Cauchy's theorem (Theorem 5.6) $N_G(H)/H$ contains a subgroup of order p. Such a group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$.

  Since $H \lhd N_G(H)$ we have $H \lhd H_1$. Finally, since $|H_1|$ is finite we have

$$p = \left|\frac{H_1}{H}\right| = \frac{|H_1|}{|H|} = \frac{|H_1|}{p^i} \implies |H_1| = p^{i+1}.$$

□

Definition 6.2 (Sylow p-Subgroups)**:** A subgroup P of a group G is a Sylow p-subgroup of G if P is a maximal p-subgroup of G (i.e. if $P \subseteq H \subseteq G$ where H is another p-subgroup of G then $P = H$).

Proposition 6.4 (Properties of Sylow p-Subgroups)**:** Let G be a group of order $p^n m$ for some prime p with $\gcd(p, m) = 1$. The following are true:

1. For all p-subgroups H of G, H is a Sylow p-subgroup if and only if $|H| = p^n$.
2. Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.
3. If G has exactly one Sylow p-subgroup P then $P \lhd G$.

Proof. This follows from the first Sylow theorem. □

Theorem 6.5 (Second Sylow Theorem)**:** If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup of G then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In-particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let X be the set of all left cosets of P in H, and let H act on X by left multiplication. Lemma 5.5 we have $|X| \equiv |X_f| = [G : P] \bmod p$. Since $p \nmid [G : P]$ we have $|X_f| \neq 0$. Thus there exists some $gP \in X_f$ for some $g \in G$. Note that:

$$\begin{aligned} gP \in X_f &\iff hgP = gP, \forall h \in H \\ &\iff g^{-1}hgP = P, \forall h \in H \\ &\iff g^{-1}hg \in P, \forall h \in H \\ &\iff g^{-1}Hg \subseteq P \\ &\iff H \subseteq gPg^{-1} \end{aligned}$$

Also, since H is a Sylow p-subgroup $|H| = |P| = |gPg^{-1}|$ and so $H = gPg^{-1}$. □

Theorem 6.6 (Third Sylow Theorem)**:** Let G be a finite group and p be a prime with $p \big| |G|$. Then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$.

Proof. By the second Sylow theorem (Theorem 6.5), the number of Sylow p-subgroups of G is the number of conjugates of any particular Sylow p-subgroup P. This number is $[G : N_G(P)]$ which divides $|G|$.

Now X be the set of all Sylow p-subgroups of G and let P act on X by conjugation. Then $Q \in X_f \iff gQg^{-1} = Q$ for all $g \in P$. The latter condition holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$. Thus they are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, this can only occur if $Q = P$. Thus $Q = P$ and $X_f = \{P\}$. Since $|X| \equiv |X|_f \equiv 1 \bmod p$ this gives $|X| = kp + 1$ for some $k \in N \cup \{0\}$. □

Note: Suppose that G is a group with $|G| = p^n m$ where $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups of G. By the third Sylow theorem we see that $n_p | p^n m$ and $n_p \equiv 1 \bmod p$. So we have $n_p | m$.

7 Finite Abelian Groups

7.1 Primary Decomposition

Notation 7.1: Let G be a group and $m \in \mathbb{Z}$. We define $G^{(m)} = \{g \in G : g^m = 1\}$.

Proposition 7.1: Let G be an abelian group. Then $G^{(m)}$ is a subgroup of G.

Proof. This follows easily from the subgroup test (Theorem 2.1). □

Proposition 7.2: Let G be a finite abelian group with $|G| = mk$ where $\gcd(m, k) = 1$. Then:

1. $G \cong G^{(m)} \times G^{(k)}$
2. $\left|G^{(m)}\right| = m$ and $\left|G^{(k)}\right| = k$.

Proof.

1. Since G is abelian we have $G^{(m)} \lhd G$ and $G^{(k)} \lhd G$. Also, since $\gcd(m,k) = 1$, there exist $x, y \in \mathbb{Z}$ such that $mx + ky = 1$.

   Claim 7.2.1: $G^{(m)} \cup G^{(k)} = \{1\}$.

   Proof. Suppose that $g \in G^{(m)} \cup G^{(k)}$. Then since $mx + ky = 1$:

   $$\begin{aligned} g &= g^{mx+ky} \\ &= (g^m)^x (g^k)^y \\ &= 1^x 1^y \\ &= 1 \end{aligned}$$

   □

   Claim 7.2.2: $G = G^{(m)} G^{(k)}$.

   Proof. If $g \in G$ then

   $$1 = (g^m)^k = g^{mk} = (g^k)^m.$$

   It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Thus

   $$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}.$$

   □

   Combining Claims 7.2.1 & 7.2.2 gives $G \cong G^{(m)} \times G^{(k)}$.

2. Let $|G^{(m)}| = m'$ and $|G^{(k)}| = k'$. By (1) we have $mk = |G| = m'k'$.

   Claim 7.2.3: $\gcd(m, k') = 1$.

   Proof. Suppose $\gcd(m, k') \neq 1$. Then there exists a prime p such that $p|m$ and $p|k'$ and so by Cauchy's theorem (Theorem 5.6) there exists a $g \in G^{(k)}$ such that $o(g) = p$. Since $p|m$ we have $g^m = 1$ and so $g \in G^{(m)}$ as well. Thus by Claim 7.2.1 $g = 1$, which contradicts $o(g) = p$. □

   Note that since $m|m'k'$ and $\gcd(m, k') = 1$ we have $m|m'$. A similar argument gives $k|k'$. Since $mk = m'k'$ this means $m = m'$ and $k = k'$.

   □

Theorem 7.3 (Primary Decomposition Theorem)**:** Let G be a finite abelian group with $|G| = p_1^{n_1} \cdots p_k^{n_k}$ where $p_1, \cdots, p_k$ are distinct primes and $n_1, \cdots, n_k \in \mathbb{N}$. Then we have:

1. $G \cong G^{(p_1^{n_1})} \times \cdots \times G^{(p_k^{n_k})}$
2. $|G^{(p_i^{n_i})}| = p_i^{n_i}, \forall 1 \leq i \leq k$

Proof. This follows directly from the previous theorem. □

7.2 Structure Theorem for Finite Abelian Groups

Proposition 7.4: If G is a finite abelian p-group that contains only one subgroup of order p, then G is cyclic.

Proof. Let $y \in G$ be of maximal order.

Claim 7.4.1: $G = \langle y \rangle$.

Proof. Suppose $G \neq \langle y \rangle$. Then the quotient group $G/\langle y \rangle$ is a non-trivial p-group, which contains an element z of order p by Cauchy's theorem. In particular, $z \neq 1$. Consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ satisfy $\pi(x) = z$. Since $\pi(x^p) = z^p = 1$ we see that $x^p \in \langle y \rangle$. Thus $x^p = y^m$ for some $m \in \mathbb{Z}$.

- **Case 1:** $p \nmid m$.

  If $p \nmid m$ then since $o(y) = p^r$ for some $r \in \mathbb{N}$ we have $o(y^r) = o(y)$. Since y is of maximal order, we have

  $$o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$$

  which leads to a contradiction.

- **Case 2:** $p|m$.

  If $p|m$ then $m = pk$ for some $k \in \mathbb{Z}$. Thus we have $x^p = y^m = y^{pk}$. Since G is abelian, we have $(xy^{-k})^p = 1$. Thus xy^{-k} belongs to the one and only subgroup of order p, say H. On the other hand, the cyclic group $\langle y \rangle$ contains a subgroup of order p, which must be the one and only H. Thus $xy^{-k} \in \langle y \rangle$, which implies that $x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$ which is a contradiction.

  By combining the above two cases we have $G = \langle y \rangle$.

□

Since $G = \langle y \rangle$, it is cyclic and the proof is complete. □

Proposition 7.5: Let $G \neq \{1\}$ be a finite abelian p-group. Let C be a cyclic subgroup of maximal order. Then G contains a subgroup B such that $G = CB$ and $C \cap B = \{1\}$. Thus by Proposition 3.13 $G \cong C \times B$.

Proof. We proceed by induction.
Base Case: If $|G| = p$ then we take $C = G$ and $B = \{1\}$ and the result follows.
Inductive Case: Suppose that the result holds for all abelian groups of order p^{n-1} for some $n \in N$, $n \geq 2$. Consider $|G| = p^n$. We have two cases:

- **Case 1:** If $C = G$ then by taking $B = \{1\}$ the result follows.

- **Case 2:** If $G \neq C$ then G is not cyclic. By theorem 7.4, there exist at least two subgroups of order p. Since C is cyclic, it contains exactly one subgroup of order p. Thus there exists a subgroup D of G with $|D| = p$ and $D \subsetneq C$. Since $|D| = p$ and $D \subsetneq C$ we have $C \cap D = \{1\}$. Consider the coset map $\pi : G \to G/D$. If we consider $\pi|_{C_1}$, the restriction of π onto C, then $\ker(\pi|_{C_1}) = C \cap D = \{1\}$. Thus by the first isomorphism theorem, $\pi(C) = C$.

  Let y be a generator of the cyclic group C. Since $\pi(C) \cong C$, $\pi(C) \cong \langle \pi(y) \rangle$. By the assumption on C, $\pi(C)$ is a cyclic subgroup of G/D of maximal order. Since $|G/D| = p^{n-1}$, by the inductive hypothesis G/D contains a subgroup E such that $G/D = \pi(C)E$ and $\pi(C) \cap E = \{1\}$. Let $B = \pi^{-1}(E)$ i.e. $\pi(B) = E$.

Claim 7.5.1: $G = CB$

Proof. Note that E is a subgroup containing $\{1\}$. We have $\pi^{-1}(\{1\}) = D \subseteq B$. If $x \in G$, since $\pi(C)\pi(B) = \pi(C)E = G/D$, there exist $u \in C$ and $v \in B$ such that $\pi(x) = \pi(u)\pi(v)$. Since $\pi(xu^{-1}v^{-1}) = 1$ we have $xu^{-1}v^{-1} \in D \subseteq B$. Since G is abelian, we have $x = uxu^{-1} \in CB$. □

Claim 7.5.2: $C \cap B = \{1\}$

Proof. Let $x \in C \cap B$. Then

$$\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}.$$

Since $\pi(x) = 1 \in G/D$, we have $x \in D$. Since $x \in C \cap D = \{1\}$ we see $x = 1$. □

By Claims 7.5.1 and 7.5.2, the result follows by induction.

□

Proposition 7.6: Let G be a finite abelian p-group. Then G is isomorphic to a direct product of cyclic groups.

Proof. By the previous theorem there exists a cyclic group C_1 and a subgroup B_1 of G such that $G \cong C_1 \times B_1$. Since $|B_1|$ divides $|G|$ by Lagrange's theorem, the group B_1 is also a p-group. Thus if $B_1 \neq \{1\}$, then by the previous theorem these exists groups C_2 and B_2 such that $B_1 \cong C_2 \times B_2$... Repeat until we get $B_k = \{1\}$. Thus

$$G \cong C_1 \times \cdots \times C_k.$$

□

Theorem 7.7 (Structure Theorem for Finite Abelian Groups)**:** If G is a finite abelian group then

$$G \cong C_{p_1^{n_1}} \times \cdots \times C_{p_k^{n_k}}$$

where each $C_{p_i^{n_i}}$ is a cyclic group of order $p_i^{n_i}$. The numbers $p_i^{n_i}$ are uniquely determined up to order, but the p_i need not be unique.

Note: If $p_1, \cdots, p_k$ are distinct primes then

$$C_{p_1^{n_1}} \times \cdots \times C_{p_k^{n_k}} \cong C_{p_1^{n_1} \cdots p_k^{n_k}}.$$

Proposition 7.8 (Invariant Factor Decomposition of Finite Abelian Groups)**:** Let G be a finite abelian group. Then

$$G \cong C_{n_1} \times \cdots \times C_{n_r}$$

where $n_i \in \mathbb{N}$, $n_1 > 1$ and $n_1 | n_2 | \cdots | n_r$.

8 Rings

8.1 Basic Properties

Definition 8.1 (Rings)**:** A ring is a set R equipped with two binary operations called addition and multiplication (which are denoted $+$ and $\cdot$) such that $(R, +)$ is an abelian group, $(R, \cdot)$ satisfies the closure, associativity and identity properties of a group and multiplication distributes over addition.

More precisely, a set R is a ring if for all $a, b, c \in R$:

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. There exists $0 \in R$ such that $a + 0 = a = 0 + a$ (0 is called the zero of R)
5. There exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$ ($-a$ is called the negative of a in R and we define $a - b := a + (-b)$, $(-a) + b := -a + b$)
6. $ab := a \cdot b \in R$
7. $a(bc) = (ab)c$
8. There exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a$ (1 is called the unity of R)
9. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

Furthermore, if R also has the property

10. $ab = ba$

then it is a commutative ring.

Note: Since $(R, +)$ forms a group, it follows that $-(-a) = a$.

Example 8.1: $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all commutative rings, while $M_n(\mathbb{R})$ is a non-commutative ring (for $n \geq 2$).

Definition 8.2 (Repeated Multiplication and Addition)**:** Given a ring R and $n \in \mathbb{Z}$, we define n-times repeated addition as:

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}}, & n > 0 \\ 0, & n = 0 \\ \underbrace{-a - \cdots - a}_{n \text{ times}}, & n < 0 \end{cases}$$

Similarly, for $n \in \mathbb{N} \cup \{0\}$ we define n-times repeated multiplication as:

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n \text{ times}}, & n \in \mathbb{N} \\ 1, & n = 0 \end{cases}$$

Furthermore, if there exists $a^{-1} \in R$ such that $a^{-1}a = 1 = aa^{-1}$ then for $n \in \mathbb{N} \cup \{0\}$ we also define

$$a^{-n} = (a^{-1})^n.$$

Note: Be careful of the difference between na for $n \in \mathbb{Z}$ and ba for $b \in R$. One is repeated ring addition and the other is ring multiplication. We often write $0_R, 1_R \in R$ to distinguish the identity and unity of R with those of $\mathbb{Z}$.

Proposition 8.1 (Algebraic Identities of Rings)**:** Let R be a ring, $r, s \in R$ and $n, m \in \mathbb{Z}$.

1. $na + ma = (n + m)a$
2. $n(ma) = (nm)a$
3. $n(a + b) = na + nb$
4. $0_R r = 0_R = r0_R$
5. $(-r)s = r(-s) = -(rs)$
6. $(-r)(-s) = rs$
7. $(mr)(ns) = (mn)(rs)$

Proof. 1,2 and 3 follow from the corresponding group identities of $(R, +)$. The rest are left as an exercise. □

Definition 8.3 (Trivial Rings)**:** A ring R is a trivial ring if $|R| = 1$.

Remark: In a trivial ring we have $0_R = 1_R$.

Definition 8.4 (Direct Products of Rings)**:** Let $R_1, \cdots, R_n$ be rings. Their direct product is the set $R_1 \times \cdots \times R_n$ and we define addition and multiplication on this set (using the addition and multiplication functions of $R_1, \cdots, R_n$) as

$$(r_1, \cdots, r_n) + (s_1, \cdots, s_n) = (r_1 + s_1, \cdots, r_n + s_n)$$

and

$$(r_1, \cdots, r_n) \cdots (s_1, \cdots, s_n) = (r_1 s_1, \cdots, r_n s_n).$$

Note: One can easily show that the set $R_1 \times \cdots \times R_n$ forms a ring when equipped with the addition and multiplication operations defined above.

Definition 8.5 (Characteristics of Rings)**:** Given a ring R, the characteristic of R (denoted $\text{ch}(R)$ using the order of $1 \in R$ in the additive group $(R, +)$ as

$$\text{ch}(R) = \begin{cases} n, & o(1) = n \text{ in } (R,+) \\ 0, & o(1) = \infty \text{ in } (R,+) \end{cases}$$

Example 8.2: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ all have characteristic 0, while $\mathbb{Z}_n$ has characteristic n.

Definition 8.6: For $k \in \mathbb{Z}$ we write $kR = 0$ to mean $kr = 0_R$ for all $r \in R$.

Note: By Proposition 8.1 we have $kr = k(1_R r) = (k1_R)r$ so $kR = 0 \iff k1_R R = 0$.

Theorem 8.2: Let R be a ring and $k \in \mathbb{Z}$.

1. If $\text{ch}(R) = n \in \mathbb{N}$ then $kR = 0 \iff k|n$.
2. If $\text{ch}(R) = 0$ then $kR = 0 \iff k = 0$.

Proof. This follows from results in chapter 2 applied to the group $(R, +)$. □

8.2 Subrings

Definition 8.7 (Subrings)**:** A subset S of a ring R is a subring if S is itself a ring under R's addition and multiplication operations.

Proposition 8.3 (The Subring Test)**:** A subset S of a ring R is a subring if it satisfies the following properties:

1. $1_R \in S$
2. If $s, t \in S$, then $s - t, st$ are all in S (note that if this is true then $s - s = 0 \in S$ and $0 - t = -t \in S$ as well)

Proof. The properties 2,3,7 and 9 of a ring are automatically satisfied in any subset of R. The two requirements of the subring test clearly satisfy the remaining properties. □

Example 8.3: We have a chain of subrings: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Definition 8.8 (Centers of Rings)**:** Given a ring R the center of R is

$$Z(R) = \{z \in R : zr = rz, \forall r \in R\}.$$

Note: We have $1_R \in Z(R)$ and if $s, t \in Z(R)$ then for all $r \in R$,

$$(s-t)r = sr - tr = rs - rt = r(s-r)$$

and

$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

so by the subring test $Z(R)$ is a subring of R.

Example 8.4: Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$. Then one can show (exercise) that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ called the Gaussian integers.

8.3 Ideals

Definition 8.9 (Ring Cosets and Quotients)**:** Let R be a ring and A be a subgroup of R under addition. Note that since $(R, +)$ is an abelian group, $A \triangleleft R$. For $r \in R$, we define the r-coset of A as:

$$r + A = \{r + a : a \in A\}$$

Similarly to quotient groups, we also define:

$$R/A = \{r + A : r \in R\}$$

Theorem 8.4 (Ring Coset Identities)**:** Let R be a ring and A an additive subgroup of R. For all $r, s \in R$ we have:

1. $r + A = s + A \iff r - s \in A$
2. $(r + A) + (s + A) = (r + s) + A$
3. $0 + A = A$ is the additive identity of R/A
4. $-(r + A) = -r + A$ is the additive inverse of $r + A$
5. $k(r + A) = kr + A, \forall k \in \mathbb{Z}$

Proof. This follow from known properties of cossets and quotient groups. □

Remark: Given $r, r_1, s, s_1 \in R$, if

$$r + A = r_1 + A, s + A = s_1 + A \implies rs + A = r_1 s_1 + A$$

then

$$(r + A)(s + A) = rs + A$$

is a well defined multiplication operation on R/A making it into a ring. This is characterized in the following proposition.

Proposition 8.5: Let A be a an additive subgroup of a ring R. For $a \in A$ define

$$Ra = \{ra : r \in R\} \text{ and } aR = \{ar : r \in R\}.$$

The following are all equivalent:

1. $Ra \subseteq A$ and $aR \subseteq A$ for every $a \in A$.
2. For $r, s \in R$, the multiplication $(r + A)(s + A) = rs + A$ is well-defined.

Proof.

$\Longrightarrow$ If $r + A = r_1 + A$ and $s + A = s_1 + A$ then we need to show $rs + A = r_1 s_1 + A$. Since $(r - r_1 \in A)$ and $(s - s_1) \in A$ by (1) we have:

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

So $rs + A = r_1 s_1 + A$.

$\Longleftarrow$ Let $r \in R$ and $a \in A$. We have:

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = r0 + A = 0 + A = A$$

Thus $ra \in A$ and we have $Ra \subseteq A$. Similarly, $aR \subseteq A$.

□

Definition 8.10 (Ideal)**:** An additive subgroup A of a ring R is an ideal of R if $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$. Thus a subset A of R is an ideal if $0 \in A$ and for all $a, b \in A$ and $r \in R$ we have $ra, ar \in A$ and $a - b \in A$.

Example 8.5: For all rings R, $\{0\}$ and R are both ideals.

Note: If A is an ideal of a ring R with $1_R \in A$, then $A = R$.

Example 8.6: Let R be a commutative ring and $a_1, \cdots, a_n \in R$. Consider the set I generated by $a_1, \cdots, a_n$, i.e.

$$I = \langle a_1, \cdots, a_r \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}.$$

Then one can show that I is an ideal (exercise).

Proposition 8.6: Let A be an ideal of a ring R. Then the additive quotient group R/A is a ring with multiplication $(r + A)(s + A) = rs + A$. The unity of this group is $1 + A$.

Proof. The proof is left as an exercise. □

Definition 8.11 (Quotient Rings)**:** Let A be an ideal of a ring R. The ring R/A is called the quotient ring of R by A.

Definition 8.12 (Principal Ideals)**:** Let R be a commutative ring and A be an ideal of R. If $A = aR = Ra$ for some $a \in R$ then we say A is a principal ideal generated by a and we write $A = \langle a \rangle$.

Proposition 8.7: All ideals of $\mathbb{Z}$ are of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$. Moreover, if $\langle n \rangle \neq \langle 0 \rangle$ and then n is unique in $\mathbb{N}$.

Proof. Let A be an ideal of $\mathbb{Z}$. If $A = \{0\}$ then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ and $|a|$ minimal. Clearly $\langle a \rangle \subseteq A$. To prove the other includes, let $b \in A$. By the division algorithm we have $b = qa + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < |a|$. If $r \neq 0$, since A is an ideal and $a, b \in A$ we have $r = b - qa \in A$ with $|r| < |a|$, which contradicts our choice of a. Thus $r = 0$ and $b = qa \in \langle a \rangle$. □

8.4 Ring Isomorphism Theorems

Definition 8.13 (Ring Homomorphisms)**:** Let R and S be rings. A mapping $\theta : R \to S$ is a ring homomorphism if for all $a, b \in R$:

1. $\theta(a + b) = \theta(a) + \theta(b)$
2. $\theta(ab) = \theta(a)\theta(b)$
3. $\theta(1_R) = 1_S$

Remark: (2) does not imply (3) since $\theta(1_R)$ does not necessarily have a multiplicative inverse in S.

Proposition 8.8 (Properties of Ring Homomorphisms)**:** Let $\theta : R \to S$ be a ring homomorphism and let $r \in R$.

1. $\theta(1_R) = 0_S$
2. $\theta(-r) = -\theta(r)$
3. $\theta(kr) = k\theta(r), \forall k \in \mathbb{Z}$
4. $\theta(r^n) = \theta(r)^n, \forall n \in N \cup \{0\}$
5. If $u \in R^*$ (the set elements of R that have multiplicative inverses) then $\theta(u^k) = \theta(u)^k$ for all $k \in \mathbb{Z}$. We call such u a unit of R.

Definition 8.14 (Ring Isomorphisms)**:** A ring homomorphism is a ring isomorphism if it is bijective. If there exists a ring isomorphism from R to S then we say R and S are isomorphic and we write $R \cong S$.

Definition 8.15 (Ring Kernals and Images)**:** Let $\theta : R \to S$ be a ring homomorphism. The kernal of θ is

$$\ker \theta = \{r \in R : \theta(r) = 0\} \subseteq R$$

and the image is

$$\operatorname{Im} \theta = \theta(R) = \{\theta(r) : r \in R\} \subseteq S.$$

Proposition 8.9: Let $\theta : R \to S$ be a ring homomorphism. Then:

1. $\operatorname{Im}\theta$ is a subring of S
2. $\ker\theta$ is an ideal of R

Proof.

1. Since $\operatorname{Im}\theta = \theta(R)$ is an additive subgroup of S, it suffices to show that $\theta(R)$ is closed under multiplication and $1_S \in \theta(R)$. Note that $1_S = \theta(1_R) \in \theta(R)$. Also, if $s_1 = \theta(r_1)$ and $s_2 = \theta(r_2)$ are in $\theta(R)$ then
$$s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R).$$
2. Since $\ker(\theta)$ is an additive subgroup of R it suffices to show that $ra, ar \in \ker\theta$ for all $r \in R$ and $a \in \ker(\theta)$. If $r \in R$ and $a \in \ker\theta$ then:
$$\theta(ra) = \theta(r)\theta(a) = \theta(r) \cdot 0 = 0$$
Thus $ra \in \ker\theta$. Similarly, $ar \in \ker\theta$.

□

Theorem 8.10 (First Ring Isomorphism Theorem)**:** Let $\theta : R \to S$ be a ring homomorphism. We have
$$R/\ker\theta \cong \operatorname{Im}\theta.$$

Proof. Let $A = \ker\theta$. Since A is an ideal of R, R/A is a ring. Define the ring map
$$\overline{\theta} : R/A \to \operatorname{Im}\theta, \quad \overline{\theta}(r + A) = \theta(r)$$
for all $r + A \in R/A$. Note that
$$r + A = s + A \iff r - a \in A \iff \theta(r - s) = 0 \iff \theta(r) = \theta(s).$$
Thus $\overline{\theta}$ is well-defined and 1-1. Also $\overline{\theta}$ is clearly onto. Moreover, $\overline{\theta}$ is a ring homomorphism (exercise). Thus $\overline{\theta}$ is a ring isomorphism and $R/\ker\theta \cong \operatorname{Im}\theta$. □

Remark: If A, B are subrings of a ring R, then $A \cap B$ is also a subring. Moreover, it is the largest subring contained in both A and B.

Definition 8.16 (Sums of Ring Subsets)**:** To consider the smallest subring of R containing two subsets (not necessarily subrings) A and B, we define
$$A + B := \{a + b : a \in A, b \in B\}.$$

Proposition 8.11: Let R be a ring an let A, B be subsets of R.

1. If A and B are two subrings of R with $1_A = 1_B = 1_R$, then $A \cap B$ is a subring of R.
2. If A is a subring and B is an ideal of R then $A + B$ is a subring of R.
3. If A and B are ideals of R, then $A + B$ is an ideal of R as well.

Proof. The proof is left as an exercise. □

Theorem 8.12 (Second Ring Isomorphism Theorem)**:** Let A be a subring and B an ideal of a ring R. Then $A+B$ is a subring of B, B is an ideal of $A+B$, $A\cap B$ is an ideal of A and

$$\frac{A+B}{B}\cong\frac{A}{A\cap B}.$$

Proof. See assignment 8. □

Theorem 8.13 (Third Ring Isomorphism Theorem)**:** Let A and B be ideal of a ring R with $A\subseteq B$. Then B/A is an ideal of R/A and

$$\frac{R/A}{B/A}\cong R/B.$$

Proof. See assignment 8. □

Example 8.7: Combining the third isomorphism theorem and the fact that all ideals of $\mathbb{Z}$ are principal, it follows that all ideals of $\mathbb{Z}_n$ are principal.

Theorem 8.14 (Chinese Remainder Theorem)**:** Let A and B be ideals of R, then:

1. If $A+B=R$ then $\frac{R}{A\cap B}\cong\frac{R}{A}\times\frac{R}{B}$.
2. If $A+B=R$ and $A\cap B=\{0\}$ then $R\cong\frac{R}{A}\times\frac{R}{B}$.

Proof. (2) is a direct consequence of (1), so it suffices to prove (1). Define $\theta:R\to\frac{R}{A}\times\frac{R}{A}$ by

$$\theta(r)=(r+A,r+B$$

for all $r\in R$. Then θ is a ring homomorphism (exercise).

To show θ is onto, let $(s+A,t+B)\in\frac{R}{A}\times\frac{R}{B}$ with $s,t\in R$. Since $A+B=R$, there exists $a\in A$ and $b\in B$ such that $a+b=1$.

Let $r=sb+ta$. Then

$$s-r=s-sb-ta=s(1-b)-ta=sa-ta=(s-t)a\in A.$$

Thus $s+A=r+A$. Similarly, we have $t+B=r+B$. Thus

$$\theta(r)=(r+A,r+B)=(s+A,t+B).$$

So $\operatorname{Im}\theta=\frac{R}{A}\times\frac{R}{B}$. Since $\ker\theta=A\cap B$, by the first isomorphism theorem, we have $R/(A\cap B)\cong\frac{R}{A}\times\frac{R}{B}$. □

Corollary 8.14.1:

1. If $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$, then $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$.
2. If $m,n\in\mathbb{N}$ with $m,n\geq 2$ and $\gcd(m,n)=1$ then $\psi(mn)=\psi(m)\psi(n)$ where $\psi(m)=|\mathbb{Z}_m^*|$ is the Euler ψ function.

Remark: Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. For $a, b \in \mathbb{Z}$, by the previous corollary, for $[a] \in \mathbb{Z}_m$ and $[b] \in \mathbb{Z}_n$ there exists a unique $[c] \in \mathbb{Z}_{mn}$ such that $[c] = [a]$ in $\mathbb{Z}_m$ and $[c] = [b]$ in $\mathbb{Z}_n$. In other words, the simultaneous congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a unique solution of the form $x \equiv c \pmod{mn}$, which is the Chinese remainder theorem from MATH135.

Proposition 8.15: If R is a ring with $|R| = p$ for some prime p then $R \cong \mathbb{Z}_p$.

Proof. Define $\theta : \mathbb{Z}_p \to R$ by $\theta([k]) = k1_R$. Note that since R is an additive subgroup of itself and $|R| = p$, by Lagrange's theorem $o(1_R) \in \{1, p\}$. Since $1_R \neq 0$ we have $o(1_R) = p$. Thus

$$[k] = [m] \iff p|(k-m) \iff (k-m)1_R = 0 \iff k1_R = m1_R.$$

So θ is well-defined and 1-1. Also θ is a ring homomorphism (exercise). Since $|\mathbb{Z}_p| = |R| = p$, θ is also onto. We conclude $R \cong \mathbb{Z}_p$. □

Example 8.8: What are all the possible rings of order $|R| = p^2$ (exercise)?

9 Commutative Rings

9.1 Integral Domains and Fields

Definition 9.1 (Units)**:** Let R be a ring. We say $u \in R$ is a unit if it has a multiplicative inverse in R, denoted by u^{-1}. We have $uu^{-1} = u^{-1}u$ and we write

$$R^* = \{u \in R : u \text{ is a unit}\}$$

Note: If u is a unit in R and $r, s \in R$, we have

$$ur = ur \iff r = s \iff ru = su.$$

Remark: One can show that R^* forms a group under multiplication called the group of units of R.

Definition 9.2 (Division Rings)**:** A non-trivial ring R is a division ring if $R^* = R \setminus \{0_R\}$.

Definition 9.3 (Fields)**:** A field is a commutative division ring.

Remark: Recall that in MATH135 we saw that $\mathbb{Z}_n$ is a field if and only if n is prime.

Theorem 9.1 (Wedderburn's Little Theorem)**:** Every finite division ring is a field.

Proof. The proof is left as an exercise (hard). □

Definition 9.4 (Zero Divisors)**:** Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$ we say that a is a zero divisor if there exists $0 \neq b \in R$ such that $ab = 0$.

Proposition 9.2: Given a ring R, the following are equivalent.

1. If $ab = 0$ in R, then $a = 0$ or $b = 0$.
2. If $ab = ac$ in R and $a \neq 0$, then $b = c$.
3. If $ba = ca$ in R and $a \neq 0$, then $b = c$.

Proof. We prove (1) $\iff$ (2). (1) $\iff$ (3) is similar.

$\implies$ Let $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$ by (1). Since $a \neq 0$ we have $b - c = 0 \implies b = c$.

$\impliedby$ Let $ab = 0$ in R. We have two cases:

1. If $a = 0$ then we are done.
2. If $a \neq 0$ then $ab = 0 = a \cdot 0$. By (2) we have $b = 0$.

□

Definition 9.5 (Integral Domains)**:** A non-trivial commutative ring is an integral domain if it has no zero divisor (i.e. if $ab = 0$ in R then $a = 0$ or $b = 0$).

Proposition 9.3: Every field is an integral domain.

Proof. Let $ab = 0$ in a field R. We want to show $a = 0$ or $b = 0$. If $a = 0$ we are done so suppose $a \neq 0$. Since R is a field this means $a \in R^*$ and so

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

thus $b = 0$ as desired. □

Remark:

- This proof also shows that every subring of a field is an integral domain.
- The converse of this theorem is not true. However, we do have the following proposition which is similar.

Proposition 9.4: Every finite integral domain is a field.

Proof. Let R be a finite integral domain and $a \in R$ with $a \neq 0$. Let $\theta : R \to R$ be defined by $\theta(r) = ar$. Since R is an integral domain and $a \neq 0$, θ is injective. In-particular, there exists a $b \in R$ such that $\theta(b) = ab = 1$. Since R is finite θ is also surjective. Since R is commutative we have $ab = ba = 1$ so a is a unit. Thus R is a field. □

Proposition 9.5: The characteristic of an integral domain is either zero or p for some prime p.

Proof. Let R be an integral domain. If $\text{ch}(R) = 0$ then we are done, so assume $\text{ch}(R) = n$ for some positive integer n. Note that $R \neq \{0\}$ so $n \neq 1$. For the sake of contradiction, suppose that n is not prime, then $n = ab$ for some $1 < a, b < n$, $a, b \in \mathbb{N}$. It follows that

$$(a \cdot 1)(b \cdot 1) = (ab)(1 \cdot 1) = n \cdot 1 = 0$$

which (since R is an integral domain) means that either $a \cdot 1 = 0$ or $b \cdot 1 = 0$. This contradicts $o(1) = n$. □

Example 9.1: Let R be an integral domain with $\text{ch}(R) = p$ for some prime p. Then for all $a, b \in R$ we have:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^p b^{p-i}$$

But since p is prime, $p | \binom{p}{i}$ for all $1 < i < p$. Since $\text{ch}(R) = p$ this means that

$$(a+b)^p = a^p + b^p.$$

9.2 Prime and Maximal Ideals

Definition 9.6 (Prime Ideals)**:** Let R be a commutative ring. An ideal $P \neq R$ is a prime ideal if whenever $r, s \in R$ satisfy $rs \in P$, then $r \in P$ or $s \in P$.

Proposition 9.6: If R is a commutative ring then an ideal P of R is a prime ideal if and only if R/P is an integral domain.

Proof. Since R is a commutative ring, so is R/P. Note that

$$R/P \neq \{0\} \iff 0 + P \neq 1 + P \iff 1 \notin P \iff P \neq R.$$

Also, for $r, s \in R$ we have:

$$\begin{aligned} P \text{ is principal} &\iff (rs \in P \implies r \in P \text{ or } s \in P) \\ &\iff ((r+P)(s+P) = 0 + P \implies r + P = 0 + P \text{ or } s + P = 0 + P) \\ &\iff R/P \text{ is an integral domain} \end{aligned}$$

□

Definition 9.7 (Maximal Ideals)**:** Let R be a commutative ring, an ideal $M \neq R$ of R is a maximal ideal if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Proposition 9.7: If R is a commutative ring, then an ideal M of R is a maximal ideal if and only if R/M is a field.

Proof. Since R is a commutative ring, so is R/M. Notice that:

$$R/M \neq \{0\} \iff 0 + M \neq 1 + M \iff 1 \notin M \iff M \neq R$$

Also, for $r \in R$, note that $r \notin M$ if and only if $r + M \neq 0 + M$, so:

$$\begin{aligned} M \text{ is maximal} &\iff \langle r \rangle + M = R, \forall r \notin M \\ &\iff 1 \in \langle r \rangle + M, \forall r \notin M \\ &\iff \forall r \notin M, \exists s + M \in R/M \text{ s.t. } (r + M)(s + M) = 1 + M \\ &\iff R/M \text{ is a field} \end{aligned}$$

□

Proposition 9.8: Every maximal ideal of a commutative ring is a prime ideal.

Proof. This follows directly from Propositions 9.3, 9.6, and 9.7 (see diagram below). □

Remark: The converse of this is not true.

Remark: What we have shown is the following:

I maximal	$\iff$	R/I field
$\Downarrow$		$\Downarrow$
I prime	$\iff$	R/I integral domain

Furthermore, by Proposition 9.4 all four of these statements are equivalent in the case where $|R|$ is finite.

9.3 Fields of Fractions

Recall that every subring of a field is an integral domain. The "converse" also holds: Every integral domain R is isomorphic to a subring of a field F.

Note: Let R be an integral domain and let $D = R \setminus \{0\}$. Consider the set:

$$X = R \times D = \{(r, s) : r \in R, s \in D\}$$

We say $(r, s) \equiv (r_1, s_1)$ on X if and only if $rs_1 = r_1 s$. One can show that this is an equivalence relation (exercise). In particular:

1. $(r, s) \equiv (r, s)$
2. $(r, s) \equiv (r_1, s_1) \implies (r_1, s_1) \equiv (r, s)$
3. $(r, s) \equiv (r_1, s_1)$ and $(r_1, s_1) \equiv (r_2, s_2) \implies (r, s) \equiv (r_2, s_2)$

Motivated by the case $R = \mathbb{Z}$, we now define the following:

Definition 9.8 (Fields of Fractions)**:** Let R be an integral domain, $D = R \setminus \{0\}$ and $X = R \times D$ as before. We define the fraction $\frac{r}{s}$ to be the equivalence class $[(r, s)]$ of the pair $(r, s) \in X$. Let F denote the set of all such fractions we call F the field of fractions of R.

$$F = \left\{ \frac{r}{s} : r \in R, s \in D \right\} = \left\{ \frac{r}{s} : r, s \in R, s \neq 0 \right\}$$

We define addition and multiplication over F by:

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1} \text{ and } \frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

where $ss_1, rs_1 + r_1 s, rr_1$ are elements of R. Note that $ss_1 \neq 0$ since R is an integral domain and $s, s_1 \neq 0$, thus these operations are well defined.

Example 9.2: One can show (exercise) the the above operations make F into a field with the zero $\frac{0}{1}$, the unity $\frac{1}{1}$ and the negation $-\frac{r}{s} = \frac{-r}{s}$. Moreover, if $\frac{r}{s} \neq 0 \in F$ then $r \neq 0$ and thus $\frac{s}{r} \in F$ as well and we have

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = \frac{rs}{rs} = \frac{1}{1} = 1_F$$

so $\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$.

Remark: In addition, we have $R \cong R'$ where

$$R' = \left\{ \frac{r}{1} : r \in R \right\} \subseteq F.$$

Thus we have the following theorem:

Proposition 9.9: Let R be an integral domain and F be its corresponding field of fractions. Then R is isomorphic to the subring

$$R' = \left\{ \frac{r}{1} : r \in R \right\} \subseteq F.$$

Proof. The proof is left as an exercise. □

10 Polynomial Rings

10.1 Polynomials Over Rings

Definition 10.1 (Polynomials)**:** Let R be a ring and x a variable. We define:

$$R[x] = \{f(x) = a_0 + a_1 x + \cdots + a_m x^m : m \in \mathbb{N} \cup \{0\}, a_i \in R\}$$

The $f(x) \in R[x]$ are called polynomials in x over R. If $a_m \neq 0$, we say $f(x)$ has degree m. This value is denoted $\deg(f) = m$ and we call a_m the leading coefficient of $f(x)$. If the leading coefficient is $a_m = 1$ then we say that $f(x)$ is monic. If $\deg(f) = 0$ then $f(x) = a_0$ is a constant polynomial. Note that

$$f(x) = 0 \iff a_1, \cdots, a_m = 0$$

and in this case we define $\deg(0) = -\infty$.

Proposition 10.1: Let R be a ring and x a variable.

1. $R[x]$ is a ring.
2. R is a subring of $R[x]$.
3. If $Z = Z(R)$ is the center of R, then $Z(R[x]) = Z[x]$.

Proof. The proof is left as an exercise. □

Proposition 10.2: Let R be an integral domain, then:

1. $R[x]$ is an integral domain.
2. If $f, g \in R[x] \setminus \{0\}$ then $\deg(fg) = \deg(f) + \deg(g)$.
3. The units in $R[x]$ are R^*.

Proof. Let $f(x) = a_0 + \cdots + a_m x^m$ and $g(x) = b_0 + \cdots + b_n x^n$ with $a_m, b_n \neq 0$. This means that $f(x)g(x) = a_0 b_0 + \cdots + a_m b_n x^{m+n}$. Since R is an integral domain, $a_m b_n \neq 0$ and so $f(x)g(x) \neq 0$ and $\deg(fg) = m + n$, which proves (1) & (2).

As for (3), let $u(x)$ be a unit in $R[x]$ with inverse $v(x)$. Since $u(x)v(x) = 1$, (2) implies that $u(x), v(x) \in R$ and (1) implies $u(x), v(x) \neq 0$. Hence $u(x), v(x) \in R \setminus \{0\} = R^*$ so $R[x]^* \subseteq R^*$. Since $R^* \subseteq R[x]^*$ this means $R[x]^* = R^*$. □

10.2 Polynomials Over Fields

Definition 10.2 (Polynomial Division)**:** Let F be a field and $f(x), g(x) \in F[x]$. We say that $f(x)$ divides $g(x)$ (denoted $f(x)|g(x)$) if there exists a polynomial $q(x) \in F[x]$ such that

$$f(x)q(x) = g(x).$$

Proposition 10.3: Let F be a field and $f(x), g(x), h(x) \in F[x]$.

1. If $f(x)|g(x)$ and $g(x)|h(x)$ then $f(x)|h(x)$.
2. If $f(x)|g(x)$ and $f(x)|h(x)$ then for all $u(x), v(x) \in F[x]$,

$$f(x)|u(x)g(x) + v(x)h(x).$$

Proof. The proof is left as an exercise. □

Proposition 10.4: Let F be a field and $f(x), g(x)$ be monic polynomials. If $f(x)|g(x)$ and $g(x)|f(x)$ then $f(x) = g(x)$.

Proof. Since $f(x)|g(x)$ and $g(x)|f(x)$ we have $f(x)r(x) = g(x)$ and $g(x)s(x) = f(x)$ for some $r, s \in F[x]$. Thus

$$f(x) = g(x)s(x) = f(x)r(x)s(x)$$

and so by Proposition 10.2 we have

$$\deg(f) = \deg(r) + \deg(s) + \deg(f) \implies \deg(r) = \deg(s) = 0.$$

Furthermore, since $f(x)$ and $g(x)$ are both monic, $r(x)$ and $s(x)$ must also be monic. Hence $r(x) = s(x) = 1$ and so $f(x) = g(x)$. □

Remark: Recall that for $a, b \in \mathbb{Z}$, if $a|b$, $b|a$ and a, b are both positive then $a = b$. Thus in a sense the monic polynomials in $F[x]$ play the same role as the positive integers in $\mathbb{Z}$.

Proposition 10.5 (The Division Algorthim for Polynomials)**:** Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(f)$ such that

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

Proof. This result can be derived by induction, however the proof is long and will be omitted (exercise). □

Proposition 10.6: Let F be a field and $f(x), g(x) \in F[x] \setminus \{0\}$. There exists a polynomial $d(x) \in F[x]$ with the following properties:

1. $d(x)$ is monic.
2. $d(x)|f(x)$ and $d(x)|g(x)$.
3. If $e(x)|f(x)$ and $e(x)|g(x)$ then $e(x)|d(x)$.
4. $d(x) = u(x)f(x) + v(x)g(x)$ for some $u(x), v(x) \in F[x]$.

Note that if $d(x)$ and $d_1(x)$ both satisfy the above conditions then since they are both monic by Proposition 10.4 $d(x) = d_1(x)$. Hence $d(x)$ is also unique.

Proof. Consider the set

$$X = \{u(x)f(x) + v(x)g(x) : u(x), v(x) \in F[x]\}.$$

Since $f(x) \in X$, X contains a non-zero polynomial. Furthermore, since F is a field we may divide by the leading coefficient and so X contains a monic polynomial. Now let

$$X' = \{h(x) \in X : h(x) \text{ is monic}\}.$$

We have seen that X' is non-empty, so pick $d(x) \in X'$ with minimal degree. Clearly this choice of $d(x)$ satisfies both (1) and (4), while (3) follows from Proposition 10.3. One can also prove that $d(x)$ satisfies (2) using the division algorithm for polynomials (Proposition 10.5) (exercise). □

Definition 10.3 (Irreducible Polynomials)**:** Let F be a field. A polynomial $\ell(x) \neq 0$ in $F[x]$ is irreducible if $\deg \ell \geq 1$ and whenever $\ell(x) = \ell_1(x)\ell_2(x)$ in $F[x]$, $\deg \ell_1 = 0$ or $\deg \ell_2 = 0$.

Proposition 10.7: Let F be a field and $f(x)$,$g(x) \in F[x]$. If $\ell(x) \in F[x]$ is irreducible and $\ell(x)|f(x)g(x)$, then $\ell(x)|f(x)$ or $\ell(x)|g(x)$.

Proof. The proof is left as an exercise. □

Theorem 10.8 (Unique Factorization Theorem)**:** Let F be a field and let $f(x) \in F[x]$ with $\deg f \geq 1$. Then we can write

$$f(x) = c\ell_1(x) \cdots \ell_m(x)$$

where $c \in F^*$ and $\ell_i(x)$ are monic irreducible polynomials. This factorization is unique up to the order of ℓ_i.

Remark: This theorem implies the existence of infinitely many irreducible polynomials.

Proof. The proof is left as an exercise. □

Proposition 10.9: Let F be a field. Then all ideal of $F[x]$ are of the form $\langle h(x)\rangle = h(x)F[x]$ for some $h(x) \in F[x]$. If $\langle h(x)\rangle \neq \{0\}$ and $h(x)$ is monic then the generator is uniquely determined.

Proposition 10.10: Let F be a field and let $h(x) \in F[x]$ with $\deg h = m \geq 1$. Then the quotient ring $R = F[x]/\langle h(x)\rangle$ is given by

$$R = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} : a_i \in F \text{ and } h(t) = 0\}$$

in which each element of R can be uniquely represented in the above form.

Proposition 10.11: Let F be a field and let $h(x) \in F[x]$ with $\deg h \geq 1$. The following are all equivalent:

1. $F[x]/\langle h(x)\rangle$ is a field.
2. $F[x]/\langle h(x)\rangle$ is an integral domain.
3. $h(x)$ is irreducible in $F[x]$.