PART I

GROUP THEORY
Chapter 1

Basic Definitions and Properties

1.1 Groups

Definition 1.1 : Let $G$ be a nonempty set and $*: G \times G \mapsto G$ a function.

1. $(G, *)$ is a group if

   \begin{align*}
   (a) & \quad \forall a, b, c \in G : (a * b) * c = a * (b * c) \quad \text{(associativity)} \\
   (b) & \quad \exists e \in G : \forall a \in G : a * e = e = e * a \quad \text{(identity)} \\
   (c) & \quad \forall a \in G : \exists b \in G : a * b = e = b * a \quad \text{(inverses)}
   \end{align*}

2. $(G, *)$ is an abelian group if in addition to (a), (b) and (c) we also have

   \begin{equation}
   (d) \quad \forall a, b \in G : a * b = b * a
   \end{equation}

Remarks:

1. $*$ is just a binary operation on $G$. For a regular group, we mostly use the multiplicative notation (a dot like $a \cdot b$ or the empty notation $ab$). For an abelian group, we use the additive notation $a + b$.

2. Property (a) ensures us that an expression like $abc$ makes sense.

3. The element $e$ from (b) is unique and is called the identity of $G$. We sometimes write 1 in multiplicative notation and 0 in additive notation.

4. The element $b$ from (c) is unique (and depends on $a$) and is called the inverse of $a$. We denote it by $a^{-1}$ in multiplicative notation and by $-a$ in additive notation.

Definition 1.2 : Let $G$ be a group.

1. For $g \in G$ and $n \in \mathbb{Z}$, we put $g^0 = e$, $g^n = \underbrace{g \cdot g \cdots g}_n$ if $n > 0$ and $g^n = (g^{-1})^{-n}$ if $n < 0$. The standard rules for working with exponents are now valid : $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$.
(2) Let $X \subseteq G$. We denote the number of elements in $X$ by $|X|$.

**Remark:** Let $f : X \mapsto Y$ be a function and $x \in X$. We mostly use the exponential notation for function images: $x^f$ instead of $f(x)$. The advantage of this notation is that it turns composition (right to left) into multiplication (left to right): if $g : Y \mapsto Z$ then $x^{fg} = (x^f)^g$. So we define the 'multiplication' of two functions: $fg := g \circ f$.

**Examples**

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.

(b) $(\mathbb{Q}_0, \cdot), (\mathbb{R}_0, \cdot)$ and $(\mathbb{C}_0, \cdot)$ are abelian groups.

(c) For $n \in \mathbb{N}_0$, we denote by $\mathbb{Z}_n$ the integers modulo $n$ and put $C_n = \{e^{\frac{ik\pi}{n}} | k = 0, 1, \ldots, n - 1\}$. Then $(\mathbb{Z}_n, +)$ and $(C_n, \cdot)$ are abelian groups (in fact, they are cyclic groups).

(d) Let $n \in \mathbb{N}_0$ and $F$ a field (like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}_p$ where $p$ is a prime). Then $GL(n, F)$ is the set of all invertible $n \times n$-matrices with entries over $F$ and $SL(n, F) = \{g \in GL(n, F) | \det(g) = 1\}$. Then $GL(n, F)$ and $SL(n, F)$ are groups where the operation is matrix multiplication.

(e) The *quaternions* are the set $Q_8 := \{1, -1, i, -i, j, -j, k, -k\}$. We define $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$. Then $(Q_8, \cdot)$ is a non-abelian group.

(f) Let $n \in \mathbb{N}_0$. We denote by $S_n$ the set of all permutations of the set $\{1, 2, \ldots, n - 1, n\}$. Then $S_n$ is a group (called a symmetric group) under multiplication. Note that $|S_n| = n!$. We can write $\sigma \in S_n$ in cycle notation as follows:

Pick $1 \leq i \leq n$. Put $i_1 = i$ and define inductively $i_j = i_{j-1}^\sigma$ for all $j \geq 2$ as long as $i_{j-1} \neq i$. Hence we get a list of numbers $(i_1, i_2, \ldots, i_m)$ with $i_m^\sigma = i$. Such a list is called a *cycle*. Note that we can view this cycle as an element of $S_n$ : the image of $i_j$ is $i_{j+1}$ for $1 \leq j \leq m_i - 1$ and the image of $i_m$ is $i_1$. Repeating this for all $1 \leq i \leq n$, we see that we can write $\sigma$ as the product of disjoint cycles. We don’t write down cycles containing only one element.

However, when we want to multiply two permutations in cycle notation, we have to be careful: cycles that are not disjoint do not commute. We will use the empty multiplication notation. Remember that we read the cycles from left to right! So $(12)(23) = (132)$.

(g) Let $n \in \mathbb{N}_0$. A *transposition* of $S_n$ is an element of the form $(i \ j)$ where $1 \leq i, j \leq n$ and $i \neq j$. Note that every cycle can be written as a product of transpositions:

$$(1 \ 2 \ 3 \ldots k - 1 \ k) = (k \ k - 1)(k - 1 \ k - 2)\ldots(3 \ 2)(2 \ 1)$$

Since every element in $S_n$ can be written as a product of (disjoint) cycles, we see that every element of $S_n$ can be written as a product of transpositions. Although an element of $S_n$ can be written in more than one way as a product of transpositions, it turns out that the number of transpositions used is either always even or always odd (for a specific element of $S_n$). We call a
permutation \( \sigma \in S_n \) even (resp. odd) if we can write \( \sigma \) as the product of an even (resp. odd) number of transpositions. We define the alternating group \( A_n \) as the set of all even permutations. It turns out that \( A_n \) is a group and \( |A_n| = \frac{n!}{2} \). Note that every cycle of odd (resp. even) length is even (resp. odd). So \((123) \in A_3 \) but \((1234) \notin A_4 \).

(h) Let \( n \geq 2 \). The dihedral group of order \( 2n \) (notation : \( D_n \)) is the set of all symmetries of a regular \( n \)-gon. Then \( D_n \) contains \( n \) rotations and \( n \) reflections. It turns out that \( D_n \) is a non-abelian group under multiplication.

We describe one way of performing calculations in \( D_n \). Let \( r \) denote the rotation over \( \frac{2\pi}{n} \) and \( s \) a reflection (whose line of symmetry goes through a vertex of the regular \( n \)-gon). Then

\[
D_n = \{ e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, sr^{n-1} \} = \{ e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1} \}
\]

Note that \((rs)^2 = e\). So \( rs = sr^{-1} = sr^{n-1} \). Hence \( r^k s = sr^{-k} \) for all \( k \in \mathbb{Z} \).

1.2 Direct Products

Definition 1.3 Let \((G, .)\) and \((G', \ast)\) be groups. The direct product of \( G \) and \( G' \) (notation : \( G \times G' \)) is the set \( \{(a, b) | a \in G, b \in G'\} \). We define the following multiplication on \( G \times G' \):

\[
(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2, b_1 \ast b_2)
\]

for all \((a_1, b_1), (a_2, b_2) \in G \times G' \). It turns out that \( G \times G' \) forms a group under this multiplication. We have that \( e_{G \times G'} = (e_G, e_{G'}) \) and \((a, b)^{-1} = (a^{-1}, b^{-1}) \) for all \((a, b) \in G \times G' \).

Remark : We can easily generalize this to the cartesian product of any finite number of groups :

\[
G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) | g_i \in G_i \text{ for } i = 1, 2, \ldots, n\}
\]

where the multiplication is defined componentwise :

\[
(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)
\]

1.3 Subgroups

Definition 1.4 Let \((G, .)\) be a group and \( H \subseteq G \). Then \( H \) is a subgroup of \( G \) (notation : \( H \leq G \)) if \((H, .)\) is a group (so we use the same multiplication on \( H \) as on \( G \)).

The following proposition is quite useful when proving that a subset of a group is a subgroup.

Proposition 1.5 (Subgroup Test) Let \( G \) be a group and \( \emptyset \neq H \subseteq G \). Then \( H \leq G \) if and only if \( ab^{-1} \in H \) for all \( a, b \in H \).
Definition 1.6 Let $G$ be a group.

1. For $X \subseteq G$, we define the subgroup generated by $X$ (notation: $\langle X \rangle$) as the ‘smallest’ subgroup of $G$ containing $X$:
   \[ \langle X \rangle = \cap \{ H \mid X \subseteq H \leq G \} \]

2. $G$ is cyclic if $G = \langle g \rangle$ for some $g \in G$.

3. Let $g \in G$. The order of $g$ (notation: $|g|$) is the smallest $n \in \mathbb{N}_0$ such that $g^n = e$. If no such $n$ exists, then we say that $g$ has infinite order. Note that $|\langle g \rangle| = |g|$.

We list some basic properties about the order of an element.

Proposition 1.7 Let $G$ be a group and $g \in G$ of finite order. Then the following holds:

a. If $g^k = e$ for some $k \in \mathbb{Z}$ then $|g|$ divides $k$.

b. The order of $g^k$ is $\frac{|g|}{\gcd(k, |g|)}$ for all $k \in \mathbb{Z}$.

c. If $|G|$ is finite then $g^{|G|} = e$.

1.4 Cosets and Transversals

Definition 1.8 : Let $G$ be a group.

1. Let $X, Y \subseteq G$. We define
   \[ XY = \{ xy \mid x \in X, y \in Y \} \]
   If $X$ has only one element, say $X = \{ x \}$, we write $xY$ in stead of $\{ x \}Y$.

2. Let $H \leq G$. A left (resp. right) coset of $H$ in $G$ is a set of the form $gH$ (resp. $Hg$) for some $g \in G$.

Remark : Let $G$ be a group, $H \leq G$ and $g \in G$. Then $gH = aH$ for any $a \in gH$.

Cosets have the following important properties.

Theorem 1.9 Let $G$ be a group and $H \leq G$. Then the following holds:

a. The set of all left (resp. right) cosets of $H$ in $G$ forms a partition of $G$.

b. $|gH| = |Hg| = |H|$ for all $g \in G$.

Corollary 1.10 (Lagrange) Let $G$ be a finite group and $H \leq G$. Then $|H|$ divides $|G|$.
**Definition 1.11**: Let $G$ be a group and $H \leq G$.

1. The *index of $H$ in $G$* (notation: $[G : H]$) is the number of left cosets of $H$ in $G$ (note that this number could be infinite). It follows from the next proposition that $[G : H]$ is also the number of right cosets of $H$ in $G$.

2. A *left (resp. right) transversal to $H$ in $G$* is a subset of $G$ containing exactly one element from each left (resp. right) coset of $H$ in $G$. \[\Box\]

**Remark**: If $\{g_i | i \in I\}$ is a left transversal to $H$ in $G$ and $g \in G$, then there exists a unique $i \in I$ and a unique $h \in H$ with $g = g_i h$.

We prove two important properties about indices.

**Proposition 1.12** Let $G$ be a group and $H \leq G$. Then $[G : H]$ is the number of right cosets of $H$ in $G$.

**Proof**: Let $L$ be a left transversal to $H$ in $G$. We prove that $L^{-1} := \{l^{-1} | l \in L\}$ is a right transversal to $H$ in $G$. Pick $g \in G$. Then $g^{-1} = lh$ for some $l \in L$ and some $h \in H$. So $g = (lh)^{-1} = h^{-1}l^{-1}$ and $Hg = Hhl^{-1}l^{-1} = Hl^{-1}$. Hence every right coset of $H$ in $G$ is of the form $Hl^{-1}$ for some $l \in L$. Suppose that $k, l \in L$ with $Hk^{-1} = Hl^{-1}$. Then $k^{-1} = hl^{-1}$ for some $h \in H$. So $k = (hl^{-1})^{-1} = lh^{-1}$ and $kH = lh^{-1}H = lH$. Hence $k = l$. So $L^{-1}$ is a right transversal to $H$ in $G$.

We get that the number of right cosets of $H$ in $G$ is $|L^{-1}|$. But $|L^{-1}| = |L|$ since the map $G \mapsto G : g \mapsto g^{-1}$ is a bijection. Note that $|L|$ is the number of left cosets of $H$ in $G$, which in turn is $[G : H]$. \[\square\]

**Theorem 1.13** Let $G$ be a group and $A \leq B \leq G$. Then $[G : A] = [G : B][B : A]$.

**Proof**: Let $K$ be a left transversal to $B$ in $G$ and $L$ a left transversal to $A$ in $B$. So $[G : B] = |K|$ and $[B : A] = |L|$. We will prove that $\{kl \mid k \in K, l \in L\}$ is a left transversal to $A$ in $G$ with $|K||L|$ elements. Pick $g \in G$. Then $g = kb$ for some $k \in K$ and some $b \in B$. But $b = la$ for some $l \in L$ and some $a \in A$. Hence $g = kb = kla$ and $gA = klaA = kA$. So every left coset of $A$ in $G$ is of the form $kA$ for some $k \in K$ and some $l \in L$. Suppose that $k, k' \in K$ and $l, l' \in L$ with $klA = k'l'A$. Then $kl = k'l'a$ for some $a \in A$. So $kB = klB = k'l'aB = k'B$. Hence $k = k'$. So $l = l'a$ and $lA = l'A = l'A$. Hence $l = l'$. So every left coset of $A$ in $G$ is of the form $kA$ for some unique $k \in K$ and some unique $l \in L$ and $\{|kl \mid k \in K, l \in L\} = |K||L|$. So $[G : A] = |K||L| = [G : B][B : A]$. \[\square\]

### 1.5 Group Homomorphisms and (Inner) Automorphisms

**Definition 1.14**: Let $(G, \cdot)$ and $(G', \ast)$ be groups and $\theta : G \mapsto G'$ a function.

1. $\theta$ is a *group homomorphism* if $(a \cdot b)^\theta = a^\theta \ast b^\theta$ for all $a, b \in G$.

2. Suppose that $\theta$ is a homomorphism. If $\theta$ is one-to-one (resp. onto or bijective), then we call $\theta$ a *group monomorphism* (resp. epimorphism or isomorphism). If $\theta$ is an isomorphism, we say that $G$ is *isomorphic* to $G'$ (notation: $G \cong G'$).
Suppose that \( G' = G \) and that \( \theta \) is a homomorphism (resp. isomorphism). Then \( \theta \) is called an (group) endomorphism (resp. automorphism).

Homomorphisms have the following properties.

**Proposition 1.15** Let \( \theta : G \to G' \) be a homomorphism. Then the following holds:

(a) \( \theta(e_G) = e_{G'} \)

(b) \( \theta(g^{-1}) = (\theta(g))^{-1} \) for all \( g \in G \)

(c) \( \theta(g^n) = (\theta(g))^n \) for all \( g \in G \) and all \( n \in \mathbb{Z} \).

**Definition 1.16**: Let \( G \) be a group.

(1) The set of all automorphisms of \( G \) is denoted by \( \text{Aut}(G) \). Note that \( \text{Aut}(G) \) forms a group where the binary operation is the multiplication of bijections.

(2) Let \( g \in G \). We define the following function

\[
\theta_g : G \mapsto G : a \mapsto g^{-1}ag
\]

It turns out that \( \theta_g \in \text{Aut}(G) \). This map is called the *conjugation under* \( g \). We write \( a^g \) in stead of \( \theta_g(a) \).

(3) An automorphism of the form \( \theta_g \) with \( g \in G \) is called an *inner automorphism* of \( G \). The set of all inner automorphisms of \( G \) is denoted by \( \text{Inn}(G) \).

**Theorem 1.17** Let \( G \) be a group. Then \( \text{Inn}(G) \) is a group.

**Proof**: Let \( g, h \in G \). Then for all \( x \in G \), we have that

\[
(x^g)^h = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = x^{gh}
\]

So \( \theta_g \theta_h = \theta_{gh} \in \text{Inn}(G) \).

The multiplication of inner automorphisms is clearly associative.

Note that \( \theta_e \) is indeed the identity map on \( G \).

Let \( g \in G \). From above, we get that \( \theta_g \theta_{g^{-1}} = \theta_{gg^{-1}} = \theta_e \). So \( \theta_g^{-1} = \theta_{g^{-1}} \).

**Example**: There is an easy way to perform conjugation in \( S_n \) without calculating any inverses if the elements involved are written in cycle notation. Let \( \sigma = (i_1i_2\ldots i_k) \) be a cycle and \( g \in S_n \). For \( 1 \leq i \leq n \), we have that

\[
i^\sigma g = i^{g^{-1}\sigma g} = i^{g^{-1}g} = i
\]

if \( i^{g^{-1}} \notin \{i_1, i_2, \ldots, i_k\} \) (or equivalently, if \( i \notin \{i_1^g, i_2^g, \ldots, i_k^g\} \)). We easily get that

\[
(i_{j+1}^g)^\sigma = i_1^{g^{-1}\sigma g} = i_j^g = \begin{cases} i_{j+1}^g & \text{for } j = 1, 2, \ldots, k - 1 \\ i_1^g & \text{if } j = k
\end{cases}
\]

Hence we get that

\[
(i_1i_2\ldots i_k)^g = (i_1^g i_2^g \ldots i_k^g)
\]

So \((1234)^{(12)(34)} = (2143) = (1432)\).
1.6 Normal and Characteristic Subgroups

Definition 1.18 : Let \((G,\cdot)\) be a group and \(H \leq G\).

1. \(H\) is a normal subgroup of \(G\) (notation : \(H \trianglelefteq G\)) if \(H^g := g^{-1}Hg = H\) for all \(g \in G\).

2. \(H\) is a characteristic subgroup of \(G\) (notation : \(H^{\text{char}} \trianglelefteq G\)) if \(H^\theta := \{h^\theta \mid h \in H\} = H\) for all \(\theta \in \text{Aut}(G)\).

The following proposition might be useful when proving that a subgroup is normal or characteristic.

**Proposition 1.19** Let \(G\) be a group and \(H \leq G\). Then the following holds:

(a) \(H \trianglelefteq G\) if and only if \(h^g \in H\) for all \(h \in H\) and all \(g \in G\) (so if and only if \(H^g \subseteq H\) for all \(g \in G\)).

(b) \(H^{\text{char}} \trianglelefteq G\) if and only if \(h^\theta \in H\) for all \(h \in H\) and all \(\theta \in \text{Aut}(G)\) (so if and only if \(H^\theta \subseteq H\) for all \(\theta \in \text{Aut}(G)\)).

**Proof** : We only prove (a). The proof of (b) is similar. If \(H \trianglelefteq G\) then \(H^g = H\) for all \(g \in G\) and so \(h^g \in H\) for all \(h \in H\) and all \(g \in G\). So suppose that \(h^g \in H\) for all \(h \in H\) and all \(g \in G\). Pick \(g \in G\). Then \(H^g \subseteq H\) and \(H^{g^{-1}} \subseteq H\). Hence \(H = H^e = (H^{g^{-1}})^g \subseteq H^g\). So \(H^g = H\) and \(H \trianglelefteq G\).

**Definition 1.20** Let \(G\) be a group. The center of \(G\) (notation : \(Z(G)\)) is the set

\[ Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\} \]

**Proposition 1.21** Let \(G\) be a group. Then \(Z(G)^{\text{char}} \trianglelefteq G\).

1.7 Quotient Groups

**Proposition 1.22** Let \(G\) be a group and \(N \leq G\). Then the following holds:

(a) \(N \trianglelefteq G\) if and only if every left coset of \(N\) is also a right coset of \(N\).

(b) If \(N \trianglelefteq G\) then the set of all cosets of \(N\) forms a group under multiplication.

**Proof** : (a) Suppose first that \(N \trianglelefteq G\). For all \(g \in G\), we have that \(g^{-1}Ng = N\) and so \(Ng = gN\). Hence every left coset of \(N\) is a right coset of \(N\). Suppose next that every left coset of \(N\) is also a right coset of \(N\). Pick \(g \in G\). So \(gN\) is some right coset of \(N\), say \(gN = Na\) where \(a \in G\). Then \(g \in Na\). But clearly \(Ng\) is a right coset of \(N\) that contains \(g\). Since the set of all right cosets of \(N\) forms a partition of \(G\) (by Theorem 1.9), we get that \(gN = Na = Ng\). So \(N = g^{-1}Ng\). Hence \(N \trianglelefteq G\).

(b) Note that \(HH = H\) for any \(H \leq G\). Suppose that \(N \trianglelefteq G\). So \(gN = Ng\) for any \(g \in G\). For all \(a, b \in G\), we have that \((aN)(bN) = aNNb = aNb = abN\). The multiplication of cosets is clearly associative. For all \(a \in G\), we get that \((aN)(eN) = aN = (eN)(aN)\) and \((aN)(a^{-1}N) = eN = (a^{-1}N)(aN)\). \(\square\)
**Definition 1.23** : Let $G$ be a group and $N \trianglelefteq G$. Then the group of all cosets of $N$ in $G$ (notation : $G/N$) is called the quotient group (or factor group) of $G$ by $N$.

There is a bijection between the (normal) subgroups of the quotient group of $G$ by $N$ and the (normal) subgroups of $G$ containing $N$.

**Proposition 1.24** Let $G$ be a group, $N \trianglelefteq G$ and $H^* \subseteq G/N$. Put $H = \{ g \in G \mid gN \in H^* \}$. Then $H^* \trianglelefteq G/N$ (resp. $H^* \trianglelefteq G$) if and only if $H \trianglelefteq G$ (resp. $H \trianglelefteq G$). In this case, $N \trianglelefteq H$ and $H^* = H/N$.

**Proof** : If $x, y \in H^*$, then there exist $a, b \in H$ with $x = aN$ and $y = bN$; if $a, b \in H$ then $x := aN \in H^*$ and $y := bN \in H^*$. We easily get that

$$xy^{-1} \in H^* \iff (aN)(bN)^{-1} \in H^* \iff ab^{-1}N \in H^* \iff ab^{-1} \in H$$

So $H^* \trianglelefteq G/N$ if and only if $H \trianglelefteq G$. In this case, we have that $N \trianglelefteq H$ since $N \trianglelefteq H^*$ and $nN = N$ for all $n \in N$. Also, $H^* = H/N$.

If $x \in H^*$ and $y \in G/N$, then there exist $a \in H$ and $g \in G$ with $x = aN$ and $y = gN$; if $a \in H$ and $g \in G$, then $x := aN \in H^*$ and $y := gN \in G/N$. We get that

$$y^{-1}xy \in H^* \iff (gN)^{-1}(aN)(gN) \in H^* \iff g^{-1}agN \in H^* \iff g^{-1}ag \in H$$

So $H^* \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

\[\Box\]

## 1.8 Isomorphism Theorems

**Definition 1.25** : Let $G, G'$ be groups and $\theta : G \mapsto G'$ a homomorphism.

1. The kernel of $\theta$ (notation : $\ker \theta$) is the set $\ker \theta = \{ g \in G \mid g^\theta = e_{G'} \}$
2. The image of $\theta$ (notation : $\im(\theta)$) is the set $\im(\theta) = \{ g^\theta \mid g \in G \}$.

The kernel and the image of a homomorphism are not just sets.

**Theorem 1.26** Let $G, G'$ be groups and $\theta : G \mapsto G'$ a homomorphism. Then the following holds :

1. $\ker \theta \trianglelefteq G$ and $\im(\theta) \subseteq G'$

2. If $H \trianglelefteq G$ (resp. $H \trianglelefteq G$), then $H^\theta \trianglelefteq \im(\theta)$ (resp. $H^\theta \trianglelefteq \im(\theta)$).

The following proposition is useful when proving that a homomorphism is one-to-one.

**Proposition 1.27** Let $G, G'$ be groups and $\theta : G \mapsto G'$ a homomorphism. Then $\theta$ is one-to-one if and only if $\ker \theta = \{ e_G \}$.
Proof: If $\theta$ is one-to-one, then $\text{Ker} \theta = \{e_G\}$ since $e_G' = e_{G'}$. So suppose that $\text{Ker} \theta = \{e_G\}$. Pick $a, b \in G$ with $a^\theta = b^\theta$. Then $(ab^{-1})^\theta = a^\theta(b^{-1})^\theta = e_{G'}$. So $ab^{-1} \in \text{Ker} \theta = \{e_G\}$. Hence $ab^{-1} = e_G$. So $a = b$ and $\theta$ is one-to-one. \hfill \Box

We now prove the three Isomorphism Theorems.

**Theorem 1.28 (First Isomorphism Theorem)** Let $G, G'$ be groups and $\theta : G \to G'$ a homomorphism. Then $G/\text{Ker} \theta \cong \text{Im}(\theta)$.

Proof: Put $N = \text{Ker} \theta$. Consider the map $\phi : G/N \to G' : aN \mapsto a^\theta$.

Note that $\phi$ is well-defined. Indeed, suppose that $aN = bN$ for some $a, b \in G$. Then $b^{-1}aN = N$. So $b^{-1}a \in N$ and $e_{G'} = (b^{-1}a)^\theta = (b^{-1})^{-1}a^\theta$. Hence $a^\theta = b^\theta$.

Pick $a, b \in G$. Then $((aN)(bN))^\phi = (abN)^\phi = (ab)^\theta = a^\theta b^\theta = (aN)^\phi(bN)^\phi$. So $\phi$ is a homomorphism.

Pick $g \in G$ with $(gN)^\phi = e_{G'}$. So $g^\phi = e_{G'}$ and $g \in N$. Hence $gN = N$ (the identity element in $G/N$). So $\text{Ker} \phi = \{N\}$. By Proposition 1.27, we get that $\phi$ is one-to-one.

Pick $y \in \text{Im}(\theta)$. Then $y = x^\theta$ for some $x \in G$. Hence $(xN)^\phi = x^\phi = y$. So $\phi$ is onto.

Hence $\phi$ is an isomorphism. \hfill \Box

**Theorem 1.29 (Second Isomorphism Theorem)** Let $G$ be a group, $H \leq G$ and $N \trianglelefteq G$. Then $HN = NH \leq G$, $H \cap N \trianglelefteq H$ and $HN/N \cong H/H \cap N$.

Proof: It follows from HW2 that $HN = NH \leq G$. Consider the map $\theta : H \to G/N : h \mapsto hN$. For all $a, b \in H$, we have that $(ab)^\theta = abN = (aN)(bN) = a^\theta b^\theta$. So $\theta$ is a homomorphism. Pick $h \in H$. Then we have

$$h^\theta = N \iff hN = N \iff h \in N$$

So $\text{Ker} \theta = H \cap N$. By Theorem 1.26, $H \cap N \trianglelefteq H$. Clearly, $\text{Im}(\theta) \subseteq HN/N$. Pick $y \in HN/N$. Then there exists $x \in HN$ with $y = xN$. Hence there exist $h \in H$ and $n \in N$ with $x = hn$. So $y = xN = hnN = hN = h^\theta$. Hence $HN/N \subseteq \text{Im}(\theta)$ and $\text{Im}(\theta) = HN/N$.

By the First Isomorphism Theorem, we get that $H/\text{Ker} \theta \cong \text{Im}(\theta)$. So $H/H \cap N \cong HN/N$. \hfill \Box

**Theorem 1.30 (Third Isomorphism Theorem)** Let $G$ be a group and $M, N \trianglelefteq G$ with $N \subseteq M$. Then $M/N \leq G/N$ and $(G/N)/(M/N) \cong G/M$.

Proof: Consider the map $\phi : G/N \to G/M : gN \mapsto gM$. Note that $\phi$ is well-defined: if $a, b \in G$ with $aN = bN$, then $b^{-1}aN = N$ and so $b^{-1}a \in N \subseteq M$; hence $b^{-1}aM = M$ and so $aM = bM$. Pick $a, b \in G$. Then $((aN)(bN))^\phi = (abN)^\phi = abM = (aM)(bM) = (aN)^\phi(bN)^\phi$. So $\phi$ is a homomorphism.

For all $g \in G$, we have that $(gN)^\phi = gM$. Hence $\phi$ is onto. Finally, for all $g \in G$, we have that

$$gN \in \text{Ker} \theta \iff (gN)^\phi = M \iff gM = M \iff g \in M$$

So $\text{Ker} \theta = M/N$. By Theorem 1.26, $M/N \leq G/N$. By the First Isomorphism Theorem, we get that $(G/N)/(M/N) \cong G/M$. \hfill \Box
Chapter 2
Commutators, Solvable Groups and the Three Subgroup Lemma

2.1 Commutators and Solvable Groups

Definition 2.1 Let $G$ be a group.
(1) Let $a, b \in G$. The commutator of $a$ and $b$ (notation : $[a, b]$) is the element $a^{-1}b^{-1}ab$.
(2) Let $A, B \leq G$. Then $[A, B] = \langle [a, b] | a \in A, b \in B \rangle$.
(3) We define the following groups inductively :
\[
\begin{align*}
G^{(0)} &= G \\
G^{(n+1)} &= [G^{(n)}, G^{(n)}] \quad \text{for } n = 0, 1, \ldots
\end{align*}
\]
The group $G^{(1)}$ is also denoted by $G'$ and is called the commutator subgroup of $G$ or the derived group of $G$.
(4) $G$ is solvable if $G^{(n)} = \{e\}$ for some $n \geq 0$. We say that $G$ is solvable of length $n$ if $n$ is the smallest integer with $G^{(n)} = \{e\}$ and call $n$ the derived length of $G$ (notation : $\text{der}(G)$).

Remark : Note that $[b, a] = [a, b]^{-1}$ for all $a, b \in G$. Hence $[A, B] = [B, A]$ for all $A, B \leq G$.­

The subgroups $G^{(n)}$ are another example of characteristic subgroups.

Proposition 2.2 Let $G$ be a group. Then $G^{(n)} \leq G$ for all $n \geq 0$.

Proof : The proof is by induction on $n$. The case `$n = 0$' is obvious. Suppose that $G^{(n)} \leq G$ for some $n \geq 0$. Let $\theta \in \text{Aut}(G)$ and $a, b \in G^{(n)}$. Then $[a, b]^{\theta} = [a^{\theta}, b^{\theta}] \in [G^{(n)}, G^{(n)}] = G^{(n+1)}$. So
\[
(G^{(n+1)})^{\theta} = \langle [a, b] | a, b \in G^{(n)} \rangle^{\theta} = \langle [a, b]^{\theta} | a, b \in G^{(n)} \rangle \leq G^{(n+1)}
\]
Hence $G^{(n+1)} \leq G$. \qed

The following theorem tells us when a quotient group is abelian.

**Theorem 2.3** Let $G$ be a group and $N \trianglelefteq G$. Then $G/N$ is abelian if and only if $G' \leq N$.

**Proof**: We easily get that

$G/N$ is abelian $\iff [aN, bN] = N$ for all $a, b \in G$ $\iff [a, b]N = N$ for all $a, b \in G$ $\iff [a, b] \in N$ for all $a, b \in N$

So $G/N$ is abelian if and only if $G' \leq N$. \qed

Solvability is a property that is inherited by subgroups and quotient groups.

**Lemma 2.4** Let $G$ be a group, $H \leq G$ and $N \trianglelefteq G$. Then the following holds:

(a) $H^{(n)} \leq G^{(n)}$ for all $n \geq 0$. In particular, if $G$ is solvable then $H$ is solvable and $\text{der}(H) \leq \text{der}(G)$.

(b) $(HN/N)^{(n)} = H^{(n)}N/N$ for all $n \geq 0$. In particular, if $G$ is solvable then $G/N$ is solvable and $\text{der}(G/N) \leq \text{der}(G)$.

**Proof**:

(a) We use induction on $n$. The case ‘$n = 0’$ is obvious. So suppose that $H^{(n)} \leq G^{(n)}$ for some $n \geq 0$. Then

$$H^{(n+1)} = [H^{(n)}, H^{(n)}] \leq [G^{(n)}, G^{(n)}] = G^{(n+1)}$$

Suppose that $G$ is solvable of length $k$. Then $H^{(k)} \leq G^{(k)} = \{e\}$. Hence $\text{der}(H) \leq k = \text{der}(G)$.

(b) We use induction on $n$. The case ‘$n = 0’$ is obvious. So suppose that $(HN/N)^{(n)} = H^{(n)}N/N$ for some $n \geq 0$. Using induction and HW 3, we get that

$$(HN/N)^{(n+1)} = [(HN/N)^{(n)}, (HN/N)^{(n)}] = [H^{(n)}N/N, H^{(n)}N/N] = [H^{(n)}, H^{(n)}]N/N = H^{(n+1)}N/N$$

Suppose that $G$ is solvable of length $k$. Then $(G/N)^{(k)} = G^{(k)}N/N = N$. Hence $\text{der}(G/N) \leq k = \text{der}(G)$. \qed

We finish this section with two characterizations of solvable groups.

**Theorem 2.5** Let $G$ be a group and $N \trianglelefteq G$. Then $G$ is solvable if and only if $N$ and $G/N$ are both solvable. In this case, $\text{der}(G) \leq \text{der}(N) + \text{der}(G/N)$.

Suppose first that $G$ is solvable. By Lemma 2.4(a)(b), $N$ and $G/N$ are both solvable.

Suppose next that $N$ (resp. $G/N$) is solvable of length $m$ (resp. $n$). By Lemma 2.4(b), $N = (G/N)^{(n)} = G^{(n)}N/N$. Hence $G^{(n)} \leq N$. By Lemma 2.4(a), $G^{(n+m)} = (G^{(n)})^{(m)} \leq N^{(m)} = \{e\}$. So $G$ is solvable and $\text{der}(G) \leq n + m = \text{der}(N) + \text{der}(G/N)$.
Theorem 2.6 Let $G$ be a group. Then $G$ is solvable if and only if there exists a chain

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

such that $G_i/G_{i-1}$ is abelian for $i = 1, \ldots, n$.

Proof : Suppose first that $G$ is solvable of length $n$. For $i = 0, \ldots, n$, put $G_i = G^{(n-i)}$. By Theorem 2.3, $G_i/G_{i-1}$ is abelian for $i = 1, \ldots, n$.

Suppose next that such a chain exists. We use induction on $k$ to prove that $G_k$ is solvable for $k = 0, 1, \ldots, n$. The case ‘$k = 0$’ is obvious. Suppose that $G_k$ is solvable for some $k \in \{0, 1, \ldots, n - 1\}$. Note that $G_{k+1}/G_k$ is solvable since it is abelian. Hence $G_{k+1}$ is solvable by Theorem 2.5.

Hence $G = G_n$ is solvable.

Note that there are several modifications of this last characterization. We can change $G_i \trianglelefteq G_{i+1}$ to $G_i \trianglelefteq G$ and abelian to solvable. Moreover, if $G$ is finite, we can replace abelian by cyclic.

2.2 The Three Subgroup Lemma

Definition 2.7 Let $G$ be a group.

(a) For $a, b, c \in G$, we put $[a, b, c] = [[a, b], c]$ (so we read commutators from the left to right).

(b) For $A, B, C \leq G$, we put $[A, B, C] = [[A, B], C]$. Using Lemma 2.8, one can show that

$$[A, B, C] = \langle [a, b, c] \mid a \in A, b \in B, c \in C \rangle$$

Lemma 2.8 Let $G$ be a group. Then the following holds:

(a) $[x, y]^{-1} = [y, x]$.
(b) $[xy, z] = [x, z]^y[y, z]$.
(c) $[x, yz] = [x, z][x, y]^z$.
(d) $[x, y^{-1}] = [y, x]^{y^{-1}}$.

Proof : □

Lemma 2.9 (Three Subgroup Lemma) Let $G$ be a group, $N \trianglelefteq G$ and $A, B, C \leq G$ such that $[A, B, C] \leq N$ and $[B, C, A] \leq N$. Then $[C, A, B] \leq N$.

Proof : One easily checks that

$$[a, b^{-1}, c][b, c^{-1}, a][c, a^{-1}, b]^a = e$$

for all $a, b, c \in G$. Hence $[c, a^{-1}, b] \in N$ for all $a \in A$, $b \in B$ and $c \in C$. So $[A, B, C] \leq N$. □
Chapter 3
Composition Series

Definition 3.1 Let $G$ be a group.

1. $G$ is simple if $G \neq 1$ and $G$ has no proper normal subgroups (so if $N \trianglelefteq G$ then $N = 1$ or $N = G$).

2. Let $N \trianglelefteq G$. Then $N$ is a maximal normal subgroup of $G$ if $N \neq G$ and whenever $N \leq M \trianglelefteq G$ then $M = N$ or $M = G$.

3. A composition series for $G$ is a normal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

such that $1 \neq G_i/G_{i-1}$ is simple for $i = 1, \ldots, n$.

The following lemma characterizes maximal normal subgroups.

Lemma 3.2 Let $G$ be a group and $N \trianglelefteq G$. Then $N$ is a maximal normal subgroup of $G$ if and only if $G/N$ is simple.

Proof: Suppose first that $N$ is a maximal normal subgroup of $G$. Then $G/N \neq 1$. Let $X \trianglelefteq G/N$. By Proposition 1.24, $X = M/N$ for some $N \leq M \trianglelefteq G$. Since $N$ is maximal, we have that $M = N$ or $M = G$. So $X = M/N = 1$ or $X = G/N$. Hence $G/N$ is simple.

Suppose next that $G/N$ is simple. Then $N \neq G$. Let $N \leq M \trianglelefteq G$. By Proposition 1.24, $M/N \trianglelefteq G/N$. Since $G/N$ is simple, we have that $M/N = 1$ or $M/N = G$. So $M = N$ or $M = G$. Hence $N$ is a maximal normal subgroup of $G$. \qed

Infinite groups do not necessarily have maximal normal subgroups or composition series. The following proposition shows that finite groups do have maximal normal subgroups and hence also composition series.

Proposition 3.3 Let $G \neq 1$ be a finite group. Then $G$ has maximal normal subgroups.
Proof : The proof is by induction on $|G|$. Suppose first that $|G| = 2$. Then $G$ is simple so $N = 1$ is a maximal normal subgroup of $G$ by Lemma 3.2. Suppose next that $|G| \geq 3$. If $G$ is simple then $N = 1$ is a maximal normal subgroup of $G$ by Lemma 3.2. So assume that $G$ is not simple. Then there exists $N \trianglelefteq G$ with $1 \neq N \neq G$. If $G/N$ is simple then $N$ is maximal normal subgroup of $G$ by Lemma 3.2. So assume that $G/N$ is not simple. By induction, $G/N$ has a maximal normal subgroup $X$. By Proposition 1.24, $X = M/N$ for some $N \leq M \leq G$. Then $G/M \cong (G/N)/(M/N)$ by the Third Isomorphism Theorem. So $G/M$ is simple. Hence $M$ is a maximal normal subgroup of $G$ by Lemma 3.2. 

Corollary 3.4 Let $G \neq 1$ be a finite group. Then $G$ has a composition series.

Proof : The proof is by induction on $|G|$. Suppose first that $|G| = 2$. Then $G$ is simple and $1 = G_0 \trianglelefteq G_1 = G$ is a composition series for $G$. Suppose next that $|G| \geq 3$. By Proposition 3.3, $G$ has a maximal normal subgroup $N$. Then $N \neq G$ and $G/N$ is simple by Lemma 3.2. If $N = 1$ then $1 = G_0 \trianglelefteq G_1 = G$ is a composition series for $G$. So assume that $N \neq 1$. By induction, $N$ has a composition series $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = N$. Then $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k \leq G$ is a composition series for $G$.

It is possible that a group has more than one composition series. The following theorem shows that all composition series have the same length and the same factors.

Theorem 3.5 (Jordan-Hölder) Let $G$ be a group and $1 = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_{m-1} \trianglelefteq A_m = G$ and $1 = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_{n-1} \trianglelefteq B_n = G$ two composition series for $G$ with $m \leq n$. Then $m = n$ and there exists $\sigma \in S_n$ such that $A_i/A_{i-1} \cong B_{\sigma(i)}/B_{\sigma(i)-1}$ for $i = 1, \ldots, n$.

Proof : The proof is by induction on $m$.

Assume first that $m = 1$. Then $G$ is simple. So $B_{n-1} = 1 = B_0$. Hence $n = 1 = m$ and $A_m/A_{m-1} \cong G \cong B_n/B_{n-1}$.

Assume next that $m \geq 2$. Let $k$ be minimal with $B_k \nsubseteq A_{m-1}$. Note that $k$ exists since $B_n \nsubseteq A_{m-1}$. Also $k \neq 0$ since $B_0 \leq A_{m-1}$. Consider the following series :

$$B_kA_{m-1}/A_{m-1} \leq B_{k+1}A_{m-1}/A_{m-1} \leq \cdots \leq B_{n-1}A_{m-1}/A_{m-1} \leq B_nA_{m-1}/A_{m-1} = A_m/A_{m-1}$$

Since $A_m/A_{m-1}$ is simple, we get that $B_kA_{m-1}/A_{m-1} = 1$ or $B_kA_{m-1}/A_{m-1} = A_m/A_{m-1}$. So $B_kA_{m-1} = A_m$ or $B_kA_{m-1} = A_m$. But $B_k \nsubseteq A_{m-1}$. Hence $B_kA_{m-1} = A_m$ and so $B_jA_{m-1} = A_m$ for $j = k, k+1, \ldots, n$. By minimality of $k$, we have that $B_{k-1} \leq A_{m-1}$. Since $B_k \trianglelefteq A_{m-1} \leq B_k$, we have by Proposition 1.24 that $(B_k \cap A_{m-1})/B_{k-1} \leq B_k/B_{k-1}$, which is simple. So $(B_k \cap A_{m-1})/B_{k-1} = 1$ or $(B_k \cap A_{m-1})/B_{k-1} = B_k/B_{k-1}$. Hence $B_k \cap A_{m-1} = B_{k-1}$ or $B_k \cap A_{m-1} = B_k$. Since $B_k \nsubseteq A_{m-1}$, we must have that $B_k \cap A_{m-1} = B_{k-1}$. By the Second Isomorphism Theorem, we get

$$A_m/A_{m-1} = B_kA_{m-1}/A_{m-1} \cong B_k/B_k \cap A_{m-1} = B_k/B_{k-1}$$

For $j = 0, \ldots, n$, put $M_j = B_j \cap A_{m-1}$. Then for $j = 0, \ldots, k-1$, we have that $M_j = B_j$ since $B_j \leq B_{k-1} \leq A_{m-1}$. Also, $M_k = B_{k-1} = M_{k-1}$ and $M_n = A_{m-1}$. So we have a normal series

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_{k-1} \trianglelefteq M_k \trianglelefteq M_{k+1} \trianglelefteq \cdots \trianglelefteq M_{n-1} \trianglelefteq M_n = A_{m-1} \quad (*)$$

14
Note that $M_j/M_{j-1} = B_j/B_{j-1}$ is simple for $j = 1, 2, \ldots, k - 1$. Pick $j \in \{k + 1, \ldots, n\}$. We showed that $B_{j-1}A_{m-1} = A_m$. So $M_jB_{j-1} = (B_j \cap A_{m-1})B_{j-1} = B_j \cap A_{m-1}B_{j-1} = B_j \cap A_m = B_j$ and

$$M_j/M_{j-1} = M_j/M_{j-1} \cap B_{j-1} \cong M_jB_{j-1}/B_{j-1} = B_j/B_{j-1}$$

by the Second Isomorphism Theorem. Hence (*) is a composition series for $A_{m-1}$ of length $n - 1$. Note that $1 = A_0 \leq A_1 \leq A_2 \leq \cdots \leq A_{m-2} \leq A_{m-1}$ is composition series for $A_{m-1}$ of length $m - 1$. By induction, $m - 1 = n - 1$ (and so $m = n$) and there exists a bijection $\theta : \{1, 2, \ldots, m-1\} \mapsto \{1, 2, \ldots, k-1, k+1, \ldots, n\}$ such that $A_j/A_{j-1} \cong M_j^\theta/M_{j-1}^\theta \cong B_j^\theta/B_{j-1}^\theta$ for $j = 1, 2, \ldots, m-1$. Define

$$\sigma : \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\} : j \mapsto \begin{cases} j^\theta & \text{if } j \neq n \\ k & \text{if } j = n \end{cases}$$

Then $\sigma \in S_n$ and $A_j/A_{j-1} \cong B_j^\sigma/B_{j-1}^\sigma$ for $j = 1, 2, \ldots, n$.

\begin{definition}
Let $G$ be a group that has a composition series. The composition factors of $G$ are the quotient groups \{${G_i/G_{i-1}| i = 1, 2, \ldots, n}$\} where $1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{n-1} \leq G_n = G$ is any composition series for $G$. Note that this is well-defined by the Jordan-Hölder Theorem. Also note that we count multiplicities for these factors : the composition factors for $\mathbb{Z}_{12}$ are \{${\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3}$\} since $0 \leq \{0, 6\} \leq \{0, 3, 6, 9\} \leq \mathbb{Z}_{12}$ is a composition series for $\mathbb{Z}_{12}$.
\end{definition}
Chapter 4

Group Actions

4.1 Groups Acting on Sets

Definition 4.1: Let $G$ be a group and $\Omega$ a non-empty set.

(a) We denote by $\text{Sym}(\Omega)$ the set of all permutations of $\Omega$. Then $\text{Sym}(\Omega)$ forms a group under multiplication and is called the symmetric group on $\Omega$.

(b) We say that $G$ acts on $\Omega$ if there exists a homomorphism $\theta : G \mapsto \text{Sym}(\Omega)$. In this case, we put $\omega^g = \omega^{\theta g}$ for all $\omega \in \Omega$ and all $g \in G$.

Examples

(a) $S_n$ acts on $\{1, 2, \ldots, n\}$ for all $n \geq 1$.

(b) $D_n$ acts on the vertices of a regular $n$-gon for all $n \geq 3$.

(c) Let $G$ be a group. Then $G$ acts on itself by conjugation: we define $\theta : G \mapsto \text{Sym}(G) : g \mapsto \theta_g$ where $x^{\theta_g} = g^{-1}xg$ for all $x, g \in G$. Note that $\theta_g$ is a permutation of $G$ (in fact, it’s an automorphism of $G$) and $\theta_g \theta_h = \theta_{gh}$ for all $g, h \in G$.

(d) Let $G$ be a group. Then $G$ acts on itself by right multiplication: we define $\varphi : G \mapsto \text{Sym}(G) : g \mapsto \varphi_g$ where $x^{\varphi_g} = xg$ for all $x, g \in G$. Then $\varphi_g$ is a permutation of $G$ (but not an automorphism of $G$) and $\varphi_g \varphi_h = \varphi_{gh}$ for all $g, h \in G$.

(e) Let $G$ be a group, $H \leq G$ and $\Omega$ the set of right cosets of $H$ in $G$. Then $G$ acts on $\Omega$ by right multiplication: we define $\theta : G \mapsto \text{Sym}(\Omega) : g \mapsto \theta_g$ where $X^{\theta_g} = Xg$ for all $X \in \Omega$. Then $\theta_g \in \text{Sym}(\Omega)$ and $\theta_g \theta_h = \theta_{gh}$ for all $g, h \in G$.

(f) Let $G$ be a group, $n \in \mathbb{N}$ and $\Omega$ the set of all subgroups of $G$ of order $n$. Then $G$ acts on $\Omega$ by conjugation.

(g) Let $G$ be a group acting on a set $\Omega$ and $n \in \mathbb{N}$. Then $G$ acts on $\Omega^n = \underbrace{\Omega \times \Omega \times \cdots \times \Omega}_n$ by defining $(\omega_1, \omega_2, \ldots, \omega_n)^g = (\omega_1^g, \omega_2^g, \ldots, \omega_n^g)$ for all $\omega_1, \omega_2, \ldots, \omega_n \in \Omega$ and all $g \in G$. □
Definition 4.2: Let $G$ be a group acting on the set $\Omega$.

(a) $G$ acts transitively on $\Omega$ if for all $x, y \in \Omega$, there exists $g \in G$ with $x^g = y$.

(b) If $\Sigma \subseteq \Omega$ and $H \subseteq G$, we put $\Sigma^H = \{\sigma^h \mid \sigma \in \Sigma, h \in H\}$. In particular, if $\omega \in \Omega$ then the orbit of $\omega$ under $G$ is the set $\omega^G := \{w^g \mid g \in G\}$.

(c) Let $\omega \in \Omega$. The stabilizer (or centralizer) of $\omega$ in $G$ is the set $G_\omega := \{g \in G \mid \omega^g = \omega\}$. One easily shows that $G_\omega \leq G$.

(d) Let $\Sigma \subseteq \Omega$. The normalizer in $G$ of $\Sigma$ is the set

$$N_G(\Sigma) := \{g \in G \mid \Sigma^g = \Sigma\}$$

The centralizer in $G$ of $\Sigma$ is the set

$$C_G(\Sigma) := \{g \in G \mid \sigma^g = \sigma \text{ for all } \sigma \in \Sigma\}$$

Remark: Let $G$ be acting on the set $\Omega$.

(a) Let $\Sigma \subseteq \Omega$. One easily proves that $C_G(\Sigma) \trianglelefteq N_G(\Sigma) \leq G$. Moreover, $N_G(\Sigma)$ acts on $\Sigma$ and $N_G(\Sigma)/C_G(\Sigma)$ is isomorphic to some subgroup of $\text{Sym}(\Sigma)$.

(b) If $\omega \in \Omega$ then $G_\omega = C_G(\{\omega\}) = N_G(\{\omega\})$.

We prove three important properties of orbits and stabilizers.

Theorem 4.3 Let $G$ be a group acting on the set $\Omega$. Then the orbits in $\Omega$ under $G$ form a partition of $\Omega$.

Proof: Clearly, no orbit under $G$ is empty. If $\omega \in \Omega$, then $\omega \in \omega^G$. So $\Omega$ is the union of the orbits in $\Omega$ under $G$. Suppose that $\omega, \sigma \in \Omega$ with $\omega^G \cap \sigma^G \neq \emptyset$. Then there exist $a, b \in G$ with $\omega^a = \sigma^b$. Hence $\sigma = \omega^a b^{-1} = \omega^{ab^{-1}}$. So $\sigma^g = \omega^{ab^{-1}g}$ for all $g \in G$. Hence $\sigma^G \subseteq \omega^G$. Similarly, $\omega^G \subseteq \sigma^G$ and so $\omega^G = \sigma^G$.

Proposition 4.4 Let $G$ be a finite group acting on the set $\Omega$. Then $|G| = |\omega^G||G_\omega|$ for all $\omega \in \Omega$.

Proof: Pick $\omega \in \Omega$. We define a relation $\sim$ on $G$ by $g \sim h \iff \omega^g = \omega^h$. Then $\sim$ is an equivalence relation on $G$. Clearly, there are $|\omega^G|$ different equivalence classes. Pick $g \in G$. For all $h \in G$, we have

$$g \sim h \iff \omega^g = \omega^h \iff \omega^{hg^{-1}} = \omega \iff hg^{-1} \in G_\omega \iff h \in G_\omega g$$

So the number of elements in the equivalence class containing $g$ is $|G_\omega g| = |G_\omega|$. Since the equivalence classes form a partition of $G$, we get that $|G| = |\omega^G||G_\omega|$.

Proposition 4.5 Let $G$ be a group acting on the set $\Omega$. Then $G_\omega^g = (G_\omega)^g$ for all $\omega \in \Omega$ and all $g \in G$.

Proof: Pick $\omega \in \Omega$ and $g \in G$. Then for all $h \in G$, we have

$$h \in (G_\omega)^g \iff h \in g^{-1}G_\omega g \iff ghg^{-1} \in G_\omega \iff \omega^{ghg^{-1}} = \omega \iff \omega^g = \omega^h \iff (\omega^g)^h = \omega^g \iff h \in G_\omega$$
4.2 Groups Acting on Groups

**Definition 4.6** Let $N$ and $H$ be groups. We say that $H$ acts on $N$ if there exists a homomorphism $\theta : H \rightarrow \text{Aut}(N)$. In this case, we put $n^h = n^{\theta_h}$ for all $n \in N$ and all $h \in H$.

Examples: Let $G$ be a group and $N \trianglelefteq G$. Then $G$ acts on $N$ by conjugation: we define $\theta : G \rightarrow \text{Aut}(N)$ where $n^g = g^{-1}ng$ for all $n \in N$ and all $g \in G$.

**Remark**: If a group $H$ acts on a group $N$ then $H$ also acts on the set $N$ (since every automorphism of $N$ is also a permutation of $N$). So all the properties about orbits and stabilizers are still true for groups acting on groups.

4.2.1 Conjugacy Classes and the Class Equation

**Definition 4.7** Let $G$ be a group. Then $G$ acts on itself by conjugation. The orbits of this action are called the conjugacy classes of $G$. So a conjugacy class of $G$ is a set of the form $x^G = \{ g^{-1}xg \mid g \in G \}$ where $x \in G$.

Recall that the orbits of a group acting on $\Omega$ form a partition of $\Omega$. The following theorem uses this fact for a specific action.

**Theorem 4.8 (Class Equation)** Let $G$ be a finite group and $C_1, \ldots, C_n$ the non-trivial conjugacy classes in $G$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |C_i|$$

**Proof**: Let $\{C_{n+1}, \ldots, C_{n+m}\}$ be the trivial conjugacy classes in $G$. Note that the conjugacy class $x^G$ is trivial (so $x^G = \{x\}$) if and only if $x \in Z(G)$. So $G$ has $|Z(G)|$ trivial conjugacy classes. Hence $m = |Z(G)|$. By Theorem 4.3, the conjugacy classes in $G$ form a partition of $G$.

So $|G| = \sum_{i=1}^{n+m} |C_i| = \left( \sum_{i=1}^{n} |C_i| \right) + \left( \sum_{i=n+1}^{n+m} |C_i| \right) = \left( \sum_{i=1}^{n} |C_i| \right) + m = |Z(G)| + \sum_{i=1}^{n} |C_i|$. □

4.2.2 The Semi-Direct product

The concept of a group acting on a group leads to a new construction of groups: the semi-direct product.

**Definition 4.9** Let $H, N$ be groups and $\theta : H \rightarrow \text{Aut}(N)$ a homomorphism. We define the following operation $*$ on the set $N \times H = \{(n, h) \mid n \in N, h \in H \}$:

$$(n_1, h_1) \ast (n_2, h_2) = (n_1n_2^{(h_1^{-1})\theta}, h_1h_2)$$ for all $n_1, n_2 \in N$ and all $h_1, h_2 \in H$.

In turns out that $(N \times H, *)$ is a group, called the semi-direct product of $N$ with $H$ and is denoted by $N \rtimes_{\theta} H$ or just $N \rtimes H$. □
Remark: Put \( N^* = \{(n, 1) \mid n \in N\} \) and \( H^* = \{(1, h) \mid h \in H\} \). Then \( N^* \leq N \rtimes_{\theta} H, H^* \leq N \rtimes_{\theta} H, N^* \cap H^* = 1, N \rtimes_{\theta} H = N^*H^* \) and \((n, 1)^{(1, h)} = (n^h, 1)\) for all \( n \in N \) and all \( h \in H \). So if \( H \) acts on \( N \), we can view \( H \) and \( N \) as subgroups of some bigger group in which the action of \( H \) on \( N \) is conjugation.

Examples:

(a) Consider the additive group \( \mathbb{C} \) and \( H = \{e, \sigma\} \leq \text{Aut}(\mathbb{C}) \) where \( \sigma \) is the complex conjugation (so \((a + bi)^\sigma = a - bi\) for all \( a, b \in \mathbb{R}\)). Then \( \mathbb{C} \rtimes H \) is a group and

\[
(z_1, h_1) \ast (z_2, h_2) = \begin{cases} (z_1 + z_2, h_1h_2) & \text{if } h_1 = e \\ (z_1 + \overline{z_2}, h_1h_2) & \text{if } h_1 = \sigma \end{cases}
\]

(b) Let \( \mathbb{F} \) be a field. Then \( \mathbb{F}_0 \) acts on \( (\mathbb{F}, +) \) by multiplication: we define \( \theta : \mathbb{F}_0 \rightarrow \text{Aut}(\mathbb{F}) : \lambda \mapsto \theta_\lambda \) where \( f^{\theta_\lambda} = f\lambda \) for all \( f \in \mathbb{F} \) and all \( \lambda \in \mathbb{F}_0 \). Then \( \mathbb{F} \rtimes_{\theta} \mathbb{F}_0 \) is a group and

\[
(f_1, \lambda_1) \ast (f_2, \lambda_2) = (f_1 + f_2\lambda_1^{-1}, \lambda_1\lambda_2)
\]

The following proposition shows us when \( NH \cong N \rtimes H \) if \( G \) is a group, \( H \leq G \) and \( N \leq G \).

**Proposition 4.10** Let \( G \) be a group, \( N \leq G \) and \( H \leq G \) such that \( N \cap H = 1 \) and \( G = NH \). Then \( G \cong N \rtimes H \) where \( H \) acts on \( N \) by conjugation.

**Proof:** Define \( \theta : H \mapsto \text{Aut}(N) : h \mapsto \theta_h \) where \( n^{\theta_h} = h^{-1}nh \) for all \( n \in N \) and all \( h \in H \). Consider the map

\[
\varphi : N \rtimes_{\theta} H \mapsto G : (n, h) \mapsto nh
\]

Pick \((n_1, h_1), (n_2, h_2) \in N \rtimes_{\theta} H \). Then

\[
((n_1, h_1)(n_2, h_2))^\varphi = (n_1n_2^{(h_1^{-1})\theta}, h_1h_2)^\varphi
\]

\[
= (n_1h_1n_2h_1^{-1}, h_1h_2)
\]

\[
= n_1h_1n_2h_1^{-1}h_1h_2
\]

\[
= n_1h_1n_2h_2
\]

\[
= (n_1, h_1)^\varphi(n_2, h_2)^\varphi
\]

So \( \varphi \) is a homomorphism.

Pick \( g \in G \). Since \( G = NH \), we have that \( g = nh \) for some \( n \in N \) and some \( h \in H \). Hence \((n, h)^\varphi = nh = g \). So \( \varphi \) is onto.

Suppose that \((n, h) \in N \rtimes_{\theta} H \) with \((n, h)^\varphi = 1\). Then \( nh = 1 \). So \( n = h^{-1} \). Since \( N \cap H = 1 \), we get that \( n = h^{-1} = 1 \). So \( \varphi \) is one-to-one.

Hence \( \varphi \) is an isomorphism.

Example: Consider \( D_n \) with \( n \geq 3 \). Put \( N = \{e, r, r^2, \ldots, r^{n-1}\} \) and \( H = \{e, s\} \). Then \( N \subseteq D_n, H \leq D_n, N \cap H = 1 \) and \( D_n = NH \). Hence \( D_n \cong N \rtimes H \).
Chapter 5

Sylow’s Theorems

5.1 Finite $p$-Groups

**Definition 5.1**: Let $G$ be a finite group and $p$ a prime. Then $G$ is a $p$-group if $|G| = p^n$ for some $n \geq 0$.

The following proposition shows that non-trivial $p$-groups have a non-trivial center.

**Proposition 5.2** Let $G$ be a non-trivial finite $p$-group and $1 \neq N \trianglelefteq G$. Then $N \cap Z(G) \neq 1$. In particular, $Z(G) \neq 1$.

**Proof**: Since $N \trianglelefteq G$, $G$ acts on $N$ by conjugation. For $x \in N$, we have

$$x^G = \{x\} \iff g^{-1}xg = x \text{ for all } g \in G \iff xg = gx \text{ for all } g \in G \iff x \in Z(G)$$

So the number of trivial orbits is $|N \cap Z(G)|$. Let $C_1, \ldots, C_k$ be the non-trivial orbits. Then

$$|N| = |N \cap Z(G)| + |C_1| + \cdots + |C_k|$$

since the orbits form a partition of $N$. Note that $|G| = |x^G||G_x|$ for all $x \in N$. In particular, $|x^G|$ divides $|G|$, which is a power of $p$. So the size of an orbit is either 1 or a multiple of $p$. So $p$ divides $|C_i|$ for $i = 1, 2, \ldots, k$. Since $|N|$ divides $|G|$ and $|N| \neq 1$, we have that $p$ divides $|N|$. So $p$ divides $|N \cap Z(G)|$. Hence $N \cap Z(G) \neq 1$.

Putting $N = G$, we get that $Z(G) = G \cap Z(G) \neq 1$. □

The fact that finite non-trivial $p$-groups have a non-trivial center is very useful in induction proofs: $G/Z(G)$ is ‘smaller’ than $G$ and hence we can use induction. We illustrate this in the following proposition.

**Proposition 5.3** Let $G$ be a finite $p$-group. Then $G$ is solvable.

**Proof**: The proof is by induction on $|G|$. If $|G| = 1$ then $G$ is solvable. So assume that $|G| > 1$. By Proposition 5.2, $Z(G) \neq 1$. Then $G/Z(G)$ is a $p$-group and $|G/Z(G)| < |G|$. By induction, $G/Z(G)$ is solvable. Note that $Z(G)$ is solvable since it’s abelian. So $G$ is solvable by Theorem 2.5. □

We mention without proof another property of finite $p$-groups.
Proposition 5.4 Let $G$ be a $p$-group of order $p^n$ where $n \geq 1$. Then the following holds:

(a) $G$ has subgroups of order $p^i$ for $i = 0, 1, \ldots, n$.

(b) For $i = 0, 1, \ldots, n - 1$, every subgroup of $G$ of order $p^i$ is contained in some subgroup of $G$ of order $p^{i+1}$.

Proof : 

5.2 Sylow’s Theorem

In this section, we prove three very important theorems about finite groups, due to Sylow. We start with some preliminary results.

Lemma 5.5 Let $G$ be a finite abelian group and $p$ a prime dividing $|G|$. Then $G$ has an element of order $p$.

Proof : The proof is by induction on $|G|$. If $G$ is simple then $|G| = p$ by HW 4 #1 and any $1 \neq g \in G$ has order $p$. So we may assume that $G$ is not simple. Let $N$ be a proper normal subgroup of $G$ (so $1 < |N| < |G|$). Suppose first that $p$ divides $|N|$. By induction, $N$ has an element of order $p$. So $G$ has an element of order $p$. Suppose next that $p$ does not divide $|N|$. Since $p$ divides $|G|$ and $|G/N| = \frac{|G|}{|N|}$, we have that $p$ divides $|G/N|$. By induction $G/N$ has an element of order $p$. Hence $G$ has an element of order $p$ by HW 5 #1. 

Proposition 5.6 Let $G$ be a finite group, $p$ a prime and $k \geq 0$ such that $p^k$ divides $|G|$. Then $G$ has a subgroup of order $p^k$.

Proof : The proof is by induction on $|G|$. Clearly, we may assume that $k \geq 1$. Let $n$ be the number of non-trivial conjugacy classes of $G$ and $x_1, \ldots, x_n$ an element of each non-trivial conjugacy class. Since $|G| = |x_i^G||G_{x_i}|$ and $|x_i^G| > 1$, we have that $|G_{x_i}| < |G|$ for $i = 1, 2, \ldots, n$. If $p^k$ divides $|G_{x_i}|$ for some $1 \leq i \leq n$, then $G_{x_i}$ has a subgroup of order $p^k$ by induction and hence $G$ has a subgroup of order $p^k$. So we may assume that $p$ does not divide $|G_{x_i}|$ for $i = 1, 2, \ldots, n$. Then $p$ must divide $|x_i^G|$ since $|G| = |x_i^G||G_{x_i}|$, $p^k$ divides $|G|$ but $p^k$ does not divide $|G_{x_i}|$ for $i = 1, 2, \ldots, n$. The Class Equation is:

$$|G| = |Z(G)| + |x_1^G| + \cdots + |x_n^G|$$

Since $p^k$ divides $|G|$ and $p$ divides $|x_i^G|$ for $i = 1, 2, \ldots, n$, we get that $p$ divides $|Z(G)|$. By Lemma 5.5, $Z(G)$ has an element $x$ of order $p$. Then $N := \langle x \rangle \leq G$ and $|N| = p$. Note that $p^{k-1}$ divides $|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p}$. By induction, $G/N$ has a subgroup $H^*$ of order $p^{k-1}$. By Proposition 1.24, $H^* = H/N$ for some $N \leq H \leq G$. Note that $p^{k-1} = |H^*| = |H/N| = \frac{|H|}{|N|} = \frac{|H|}{p}$. So $|H| = p^k$. 

Corollary 5.7 (Cauchy) Let $G$ be a finite group and $p$ a prime dividing $|G|$. Then $G$ has an element of order $p$. 

21
**Proof**: By Proposition 5.6, $G$ has a subgroup of order $p$. Then any $1 \neq h \in H$ has order $p$. \qed

**Definition 5.8** Let $G$ be a finite group and $p$ a prime.

(a) $H$ is a $p$-subgroup of $G$ if $H \leq G$ and $H$ is a $p$-group.

(b) Let $H \leq G$. Then $H$ is a maximal $p$-subgroup of $G$ if $H$ is a $p$-subgroup of $G$ and whenever $H \leq M$ with $M$ a $p$-subgroup of $G$ then $M = H$.

(c) Let $n = \text{ord}_p(|G|)$ (so $p^n$ divides $|G|$ but $p^{n+1}$ does not divide $|G|$). A subgroup $H$ of $G$ is called a Sylow $p$-subgroup of $G$ if $H$ is a $p$-subgroup of $G$ and $|H| = p^n$.

(c) The set of all Sylow $p$-subgroups of $G$ is denoted by $\text{Syl}_p(G)$. \hfill $\triangleright$

**Remarks**: Let $G$ be a finite group and $p$ a prime.

(a) By Proposition 5.6, $G$ has Sylow $p$-subgroups.

(b) Clearly, Sylow $p$-subgroups of $G$ are maximal $p$-subgroups of $G$. It follows from the Third Sylow Theorem that every maximal $p$-subgroup of $G$ is indeed a Sylow $p$-subgroup of $G$. \hfill $\triangleright$

We need one more technical lemma before we can prove the three Sylow theorems.

**Lemma 5.9** Let $p$ be a prime, $G$ a finite group acting on a finite non-empty set $\Omega$ such that for all $\omega \in \Omega$, there exists a $p$-subgroup $P(\omega)$ of $G$ with $\{\sigma \in \Omega \mid \sigma^{P(\omega)} = \sigma\} = \{\omega\}$ (so $P(\omega)$ has exactly one trivial orbit on $\Omega$, namely $\omega$). Then $|\Omega| \equiv 1 \mod p$ and $G$ acts transitively on $\Omega$.

**Proof**: Pick $\omega \in \Omega$. Since $|P(\omega)| = |\sigma^{P(\omega)}||P(\omega)_\sigma|$, we get that $|\sigma^{P(\omega)}|$ is either 1 or a multiple of $p$ for all $\sigma \in \Omega$. But $P(\omega)$ has only one trivial orbit on $\Omega$, namely $\omega^{P(\omega)}$. Since the orbits form a partition of $\Omega$, we get that $|\Omega| \equiv 1 \mod p$.

Suppose that $G$ is not transitive on $\Omega$. Pick $\omega \in \Omega$. Note that $G$ acts on $\omega^G$ and $\Omega \setminus \omega^G$ and under the same assumptions as in the lemma. Hence we get that $|\omega^G| \equiv 1 \mod p$ and $|\Omega \setminus \omega^G| \equiv 1 \mod p$. But then $|\Omega| \equiv 2 \mod p$, a contradiction. So $G$ is transitive on $\Omega$. \qed

**Theorem 5.10 (Sylow)** Let $G$ be a finite group and $p$ a prime. Then the following holds:

(a) $|\text{Syl}_p(G)| \equiv 1 \mod p$.

(b) All Sylow $p$-subgroups of $G$ are conjugate.

(c) If $H$ is a $p$-subgroup of $G$, then there exists $S \in \text{Syl}_p(G)$ with $H \leq S$. 

22
Proof : We may assume that \( p \) divides \( |G| \). Let \( \Omega \) be the set of all maximal \( p \)-subgroups of \( G \). Note that \( \Omega \neq \emptyset \) since \( |G| \) is finite. Moreover, \( 1 \notin \Omega \) by Cauchy’s Theorem. Then \( G \) acts on \( \Omega \) by conjugation (indeed, pick \( P \in \Omega \) and \( g \in G \); then \( P^g \) is a \( p \)-subgroup of \( G \); suppose that \( Q \) is a \( p \)-subgroup of \( G \) containing \( P^g \); then \( Q^{g^{-1}} \) is a \( p \)-subgroup of \( G \) containing \( P \); by maximality of \( P \), we get that \( P = Q^{g^{-1}} \) and so \( Q = P^g \); hence \( P^g \in \Omega \)). Also by definition of \( \Omega \), we have that if \( H \) is a \( p \)-subgroup of \( G \), then \( H \leq P \) for some \( P \in \Omega \).

First, we prove that this action of \( G \) on \( \Omega \) satisfies the conditions of Lemma 5.9. Pick \( \omega := P \in \Omega \). Put \( P(\omega) = P \). Clearly, we have that \( \omega^{P(\omega)} = \{\omega^g \mid g \in P(\omega)\} = \{P^g \mid g \in P\} = \{P\} = \{\omega\} \). Suppose that \( \sigma := Q \in \Omega \) with \( \sigma^{P(\omega)} = \{\sigma\} \). So \( Q^g = Q \) for all \( g \in P \). Hence \( P \leq N_G(Q) \). But \( Q \leq N_G(Q) \).

Hence \( PQ \leq N_G(Q) \). But \( |PQ| = \frac{|P||Q|}{|P \cap Q|} \). Hence \( PQ \) is a \( p \)-subgroup of \( G \) containing \( P \) and \( Q \). By maximality of \( P \) and \( Q \), we have that \( P = PQ = Q \). Hence \( P(\omega) \) has only one trivial orbit on \( \Omega \). By Lemma 5.9, we have that \(|\Omega| \equiv 1 \mod p \) and \( G \) is transitive on \( \Omega \).

Next, we prove that \( \Omega = Syl_p(G) \) (note that this finishes the proof of the theorem). Pick \( \omega := P \in \Omega \). Suppose that \( P \notin Syl_p(G) \). Put \( M = N_G(P) \). Then \( |G| = |\omega^G||G_\omega| = |\Omega||M| \). Since \(|\Omega| \equiv 1 \mod p \), we see that \( \operatorname{ord}_p(|G|) = \operatorname{ord}_p(|M|) > \operatorname{ord}_p(|P|) \). Note that \( P \leq M \). So \( p \) divides \(|M/P| \). Hence by Proposition 5.6, there exists a subgroup \( H^* \) of \( M/P \) of order \( p \). By Proposition 1.24 \( H^* = H/P \) for some \( P \leq H \leq M \). Then \( |H| = |H^*||P| = p|M| \). Hence \( H \) is a \( p \)-subgroup of \( G \) and \( P < H \), a contradiction to the maximality of \( P \). So \( P \in Syl_p(G) \).

\[ \square \]

Remark : Since the size of an orbit divides the order of a group, we have that \(|Syl_p(G)| \) divides \(|G| \) and \(|Syl_p(G)| \equiv 1 \mod p \).

Sylow’s Theorem can be used to prove that there are no simple groups of a specific order. We need a couple more facts before we illustrate this.

Proposition 5.11 Let \( G \) be a finite group and \( p \) a prime such that \( G \) has exactly one Sylow-\( p \)-subgroup \( S \). Then \( S \leq \operatorname{char} G \) and so also \( S \leq G \).

Proof : Pick \( \theta \in \operatorname{Aut}(G) \). Then \( S^\theta \in Syl_p(G) = \{S\} \). Hence \( S^\theta = S \).

\[ \square \]

Proposition 5.12 Let \( G \) be a simple group and \( H < G \) such that \( n := [G : H] \) is finite. Then \( G \) is finite and \(|G| \) divides \( n! \).

Proof : Let \( \theta : G \to S_n \) describe the action of \( G \) on the set of right cosets of \( H \) by right multiplication. Since \( H \neq G \), we have that \( G \) does not act trivially and so \( \operatorname{Ker} \theta \neq G \). Hence \( \operatorname{Ker} \theta = 1 \) since \( G \) is simple and \( \operatorname{Ker} \theta \leq G \). By the First Isomorphism Theorem, we get that \( G \) is isomorphic to a subgroup of \( S_n \). Since \(|S_n| = n! \), we get that \(|G| \) divides \( n! \) by Lagrange’s Theorem.

\[ \square \]

5.3 Applications of Sylow’s Theorems

One of the standard applications of Sylow’s Theorems is to prove that there are no simple groups of a certain order. We illustrate a couple of techniques.
If $G$ is a finite group and $p$ is a prime dividing $|G|$, we put $n_p = |\text{Syl}_p(G)|$. By Sylow’s Theorems, we get that $n_p$ divides $|G|$ and $n_p \equiv 1 \mod p$. So we can easily calculate the possible candidates for $n_p$. We assume that $G$ is not a $p$-group (if $G$ is a $p$-group then $G$ is simple if and only if $|G| = p$).

(1) $n_p = 1$ immediately (without counting)

If $n_p = 1$ then $P \leq G$ by Proposition 5.11 where $P \in \text{Syl}_p(G)$ and so $G$ is not simple.

(2) small index argument

Let $P \in \text{Syl}_p(G)$. Then $n_p = [G : N_G(P)]$. So if $G$ is simple and $|G|$ does not divide $n_p!$, then by Proposition 5.12, $N_G(P) = G$; so $P \leq G$, a contradiction.

Note that if $p$ is a prime, then $\text{ord}_p(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

(3) counting elements whose order is a prime power

If $n_p \neq 1$, we might be able to count the number of elements in $\cup \{S \in \text{Syl}_p(G)\}$. This is particularly easy if $\text{ord}_p(|G|) = 1$: if $P, Q \in \text{Syl}_p(G)$ with $P \neq Q$, then $P \cap Q = 1$ and so $|\cup \{S \in \text{Syl}_p(G)\}| = 1 + n_p(p - 1)$. Sometimes it is possible this way to establish that $n_p = 1$ for some prime $p$ and so $G$ is not simple.

(4) playing $p$-subgroups off against each other

Let $P \in \text{Syl}_p(G)$. Then $n_p = |G : N_G(P)|$ and so $|N_G(P)| = \frac{|G|}{n_p}$. Suppose that $q \neq p$ is a prime with $q$ dividing $|N_G(P)|$. Sometimes we can find a $q$-subgroup of $G$ with a ‘big’ normalizer. Then by the small index argument, $G$ is not simple. A candidate for this $q$-subgroup is a Sylow-$q$-subgroup of $N_G(P)$.

(5) studying normalizers of intersections of Sylow-$p$-subgroups

Again, we try to find a subgroup of $G$ with a ‘big’ normalizer but this time, a candidate is the intersection of two Sylow-$p$-subgroups (the method in 4. doesn’t work if $|N_G(P)| = |P|$). If the intersection of any two Sylow-$p$-subgroups is trivial, we typically try a counting argument to deduce that $G$ is not simple. So suppose that $P$ and $Q$ are two different Sylow-$p$-subgroups with $P \cap Q \neq 1$. Sometimes, $P \cap Q \leq P, Q$ (because $[P : P \cap Q] = p$). Then $P, Q \leq N_G(P \cap Q)$. So $|N_G(P \cap Q)| \geq |PQ| = \frac{|P||Q|}{|P \cap Q|}$. Since $|N_G(P \cap Q)|$ divides $|G|$ and is divisible by $|P|$, this often leads to $N_G(P \cap Q) = G$ (using the small index argument) and so $G$ is not simple.

We illustrate these methods with the following exercises (the numbering of the exercises corresponds to the numbering of the methods).

**Examples** : Prove that there are no simple groups of the following orders :

(1) **200**

Let $G$ be a group of order $200 = 2^3 \cdot 5^2$. We get $\begin{cases} n_2 \in \{1, 5, 25\} \\ n_5 = 1 \end{cases}$

So $G$ is not simple since $n_5 = 1$. 

24
(2) \(5103\)

Let \(G\) be a simple group of order \(5103 = 3^6 \cdot 7\). We get
\[
\begin{cases}
  n_3 \in \{1, 7\} \\
  n_7 \in \{1, 729\}
\end{cases}
\]

Suppose that \(G\) is simple. Then \(n_3 = 7\) and \(n_7 = 729\). By the Small Index Argument, \(5103\) divides \(7!\), a contradiction since \(7! = 5040\) (or since \(\text{ord}_3(7!) = 2\)).

(3) \(380\)

Let \(G\) be a group of order \(380 = 2^2 \cdot 5 \cdot 19\). We get
\[
\begin{cases}
  n_2 \in \{1, 5, 19, 95\} \\
  n_5 \in \{1, 76\} \\
  n_{19} \in \{1, 20\}
\end{cases}
\]

Suppose that \(n_5 \neq 1\) and \(n_{19} \neq 1\). Then \(G\) contains \(76 \cdot (5 - 1) = 304\) elements of order 5 and \(20 \cdot (19 - 1) = 360\) elements of order 19, a contradiction since \(304 + 360 > 380\). Hence \(n_5 = 1\) or \(n_{19} = 1\). So \(G\) is not simple.

(4) a) \(4389\)

Let \(G\) be a group of order \(4389 = 3 \cdot 7 \cdot 11 \cdot 19\). We get
\[
\begin{cases}
  n_3 \in \{1, 7, 19, 133\} \\
  n_7 \in \{1, 11\} \\
  n_{11} \in \{1, 133\} \\
  n_{19} \in \{1, 77\}
\end{cases}
\]

Suppose that \(G\) is simple. Then \(n_p \neq 1\) for \(p = 3, 7, 11, 19\). So \(n_7 = 11\) and \(n_{11} = 133\). Hence \(|N_G(P_7)| = 77\) for any \(P_7 \in \text{Syl}_7(G)\) and \(|N_G(P_{11})| = 33\) for any \(P_{11} \in \text{Syl}_{11}(G)\). Let \(P \in \text{Syl}_7(G)\). Since 11 divides \(|N_G(P)|\), we can pick \(Q \in \text{Syl}_{11}(N_G(P))\). Then \(|Q| = 11\). So \(Q \in \text{Syl}_{11}(G)\). However, a group of order 77 has a unique Sylow-11-subgroup (\(n_{11} = 1\) for such a group). So \(Q \leq N_G(P)\). Hence \(N_G(P) \leq N_G(Q)\), a contradiction since \(|N_G(P)| = 77\) does not divide \(|N_G(Q)| = 33\). So \(G\) is not simple.

b) \(3675\)

Let \(G\) be a group of order \(3675 = 3 \cdot 5^2 \cdot 7^2\). We get
\[
\begin{cases}
  n_3 \in \{1, 7, 25, 49, 175, 1225\} \\
  n_5 \in \{1, 21\} \\
  n_7 \in \{1, 15\}
\end{cases}
\]

Suppose that \(G\) is simple. Then \(n_p \neq 1\) for \(p = 3, 5, 7\). So \(n_5 = 21\) and \(n_7 = 15\). Let \(P \in \text{Syl}_5(G)\). Then \(|N_G(P)| = 175 = 5^2 \cdot 7\). Let \(Q \in \text{Syl}_7(N_G(P))\). Then \(Q \leq N_G(P)\) since a group of order 175 has only one Sylow-7-subgroup. So \(P \leq N_G(P) \leq N_G(Q)\). Pick \(Q^* \in \text{Syl}_7(G)\) with \(Q \leq Q^*\). Since \(|Q| = 5\) and \(|Q^*| = 25\), we have that \([Q^* : Q] = 5\) and so \(Q \leq Q^*\). Hence \(Q^* \leq N_G(Q)\).

So \(PQ^* \leq N_G(Q)\). But \(|PQ^*| = |P||Q^*| = 5^2 \cdot 7^2\). Hence \([G : N_G(Q)] \leq 3\). By the Small Index Argument, \(G = N_G(Q)\). So \(Q \leq G\), a contradiction.

(5) \(144\)

Let \(G\) be a group of order \(144 = 2^4 \cdot 3^2\). We get
\[
\begin{cases}
  n_2 \in \{1, 3, 9\} \\
  n_3 \in \{1, 4, 16\}
\end{cases}
\]

Suppose that \(G\) is simple. Then \(n_2 \neq 1\) and \(n_3 \neq 1\). By the Small Index Argument, \(n_2 \neq 3\) and \(n_3 \neq 4\). So \(n_2 = 9\) and \(n_3 = 16\). Then \(|N_G(P_2)| = 16\) for any \(P_2 \in \text{Syl}_2(G)\) and \(|N_G(P_3)| = 9\) for
any $P_3 \in \text{Syl}_3(G)$. Suppose that $P \cap Q = 1$ for any $P, Q \in \text{Syl}_3(G)$ with $P \neq Q$. Then $G$ has $16 \cdot (9 - 1) = 128$ elements of order a power of three. Since $|G| - 128 = 16$, we see that $G$ has only one Sylow-2-subgroup (so $n_2 = 1$), a contradiction. Hence there exist $P, Q \in \text{Syl}_3(G)$ with $P \neq Q$ and $P \cap Q \neq 1$. Since $|P| = |Q| = 3^2$, we get that $|P \cap Q| = 3$. So $[P : P \cap Q] = 3 = [Q : P \cap Q]$.

Hence $P \cap Q \leq P$ and $P \cap Q \leq Q$. So $PQ \subseteq N_G(P \cap Q)$. But $|PQ| = \frac{|P||Q|}{|P \cap Q|} = 27$. So $N_G(P \cap Q) \leq G$, 9 divides $|N_G(P \cap Q)|$ and $|N_G(P \cap Q)| \geq 27$. So $[G : N_G(P \cap Q)] \in \{1, 2, 4\}$. By the Small Index Argument, $G = N_G(P \cap Q)$. So $P \cap Q \leq G$, a contradiction.
PART II

RING THEORY
Chapter 6

Basic Definitions and Properties

6.1 Rings

**Definition 6.1**: A *ring* is a non-empty set $R$ with two binary operations (addition, denoted by $+$ and multiplication, denoted by $\cdot$ or the empty notation) such that

(i) $(R, +)$ is an abelian group

(ii) the multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

(iii) the distributive laws hold: $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$

**Remarks**:

(1) We denote the neutral element of $(R, +)$ by $0$ and the additive inverse of $a \in R$ by $-a$.

(2) Property (ii) ensures us that an expression like $abc$ makes sense.

(3) For $n \in \mathbb{Z}$ and $r \in R$, we put $0r = 0$, $nr = r + r + \cdots + r$ if $n > 0$ and $nr = (-r) + (-r) + \cdots + (-r)$ $n$ times if $n < 0$. Then we have that $mr + nr = (m + n)r$ for all $m, n \in \mathbb{Z}$ and all $r \in R$.

(4) For $n \in \mathbb{N}_0$ and $r \in R$, we put $r^n = r \cdot r \cdots r$. Then $r^m \cdot r^n = r^{m+n}$ for all $m, n \in \mathbb{N}_0$ and all $r \in R$.

**Definition 6.2**: Let $(R, +, \cdot)$ be a ring.

(a) $R$ is *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in R$.

(b) $R$ has an *identity* (notation: $R$ has 1) if there exists $e \in R$ such that $a \cdot e = a = e \cdot a$ for all $a \in R$. We typically denote the identity in $R$ by $1$. 

27
(c) Let $R$ have 1. An element $a \in R$ is a unit if $a$ has a multiplicative inverse (so there exists $b \in R$ with $a \cdot b = 1 = b \cdot a$). The set of all units in $R$ is denoted by $R^\times$. Note that $(R^\times, \cdot)$ is a group. 

Remarks: Let $R$ be a ring with identity.

1. The identity in $R$ is unique.

2. For $a \in R^\times$ we denote the multiplicative inverse of $a$ (which is unique) by $a^{-1}$. For $n \in \mathbb{N}$ and $a \in R^\times$, we put $a^0 = 1$, $a^n = a \cdot a \cdots a$ if $n > 0$ and $a^n = (a^{-1})^{-n}$ if $n < 0$. Then $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$ and all $a \in R^\times$. 

Examples:

(a) $R = \{0\}$ is a ring where $1 = 0$. We call this the trivial ring.

(b) Let $(G, +)$ be an abelian group. Define $a \cdot b = 0$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a ring.

(c) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are rings.

(d) Let $n \in \mathbb{N}_0$. Calculating modulo $n$ is a ring. We denote this ring by $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. We will see later that $\mathbb{Z}_n$ is an example of a quotient ring.

(e) Let $X$ be a non-empty set and $R$ a ring. Then the set $\mathcal{F}(X, R) := \{f \mid f : X \rightarrow R\}$ is a ring where we define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$ for all $f, g \in \mathcal{F}(X, R)$ and all $x \in X$. Then $(\mathcal{F}(X, R), +, \cdot)$ is a ring. Sometimes we can put further restrictions on $f$. E.g.: $\{f \mid f : [a, b] \rightarrow \mathbb{R}, f$ is continuous over $[a, b]\}$ is a ring.

(e) Let $R$ be a ring and $n \in \mathbb{N}_0$. Then the set $R^{n \times n}$ of all $n \times n$-matrices with entries in $R$ is a ring under the usual matrix addition and multiplication.

(f) Let $R$ be a ring. Then the set $R[x]$ of all polynomials in $x$ with coefficients in $R$ is a ring under the usual polynomial addition and multiplication. So $R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}; a_0, a_1, \ldots, a_n \in R\}$

Note that $x$ is just a ‘place holder’: an element in $R[x]$ is not a function! But we can clearly associate with the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ the function $f : R \mapsto R : t \mapsto a_0 + a_1 t + \cdots + a_n t^n$.

(g) Let $R$ be a ring. The set of $R[[x]]$ of all formal power series in $x$ over $R$ is a ring under formal addition and multiplication of power series. So $R[[x]] = \left\{ \sum_{n=0}^{+\infty} a_n x^n \mid a_n \in R \text{ for all } n \geq 0 \right\}$

$$
\left( \sum_{n=0}^{+\infty} a_n x^n \right) + \left( \sum_{n=0}^{+\infty} b_n x^n \right) = \sum_{n=0}^{+\infty} (a_n + b_n) x^n
$$
\[
\left( \sum_{n=0}^{\infty} a_n x^n \right) \cdot \left( \sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{n} a_k b_{n-k} \right) x^n
\]

Note that an element of \( R[[x]] \) does not correspond to a function from \( R \) to \( R \) this time.

(f) The ring \( 2\mathbb{Z} := \{ \ldots, -4, -2, 0, 2, 4, \ldots \} \) has no identity.

(g) The Hamiltonian Quaternions are the set \( \mathbb{H} := \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \} \) where the addition is component wise and the multiplication is defined in such a way that the distributive laws hold; any real number commutes with \( i, j, k \); \( ij = -ji = k, jk = -kj = i, ki = -ik = j \) and \( i^2 = j^2 = k^2 = -1 \). So

\[
(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2) j + (c_1 + c_2) k + (d_1 + d_2) k
\]

Then \( \mathbb{H} \) is a non-commutative ring with 1 in which every nonzero element has a multiplicative inverse! \( \square \)

**Proposition 6.3** Let \( R \) be a ring. Then the following holds :

(a) \( 0 \cdot a = 0 = a \cdot 0 \) for all \( a \in R \).

(b) \( (-a) \cdot b = a \cdot (-b) = -(a \cdot b) \) for all \( a, b \in R \). In particular, if \( R \) has 1 then \( -a = (-1) \cdot a \) for all \( a \in R \).

(c) \( (-a) \cdot (-b) = ab \) for all \( a, b \in R \).

**Proof** : (a) Pick \( a \in R \). Then \( 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \). Adding \(-0 \cdot a\) to both sides, we get that \( 0 = 0 \cdot a \). Similarly, \( a \cdot 0 = 0 \).

(b) Pick \( a, b \in R \). Then \( a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0 \) by (a). So \(-a \cdot b = (-a) \cdot b \). Similarly, \(-a \cdot b = a \cdot (-b) \). In particular, if \( R \) has 1 then \((-1) \cdot a = -1 \cdot a = -a \).

(c) Pick \( a, b \in R \). By (b), we get that \(-a \cdot (-b) = -a \cdot (-b) = -(a \cdot b) = a \cdot b \). \( \square \)

**Definition 6.4** : Let \( R \) be a ring.

(a) \( R \) is a division ring or skew field if \( R \) has 1 and every nonzero element in \( R \) has a multiplicative inverse.

(b) \( R \) is a field if \( (R \setminus 0, \cdot) \) is a commutative group (so a field is a commutative division ring).

(c) An element \( 0 \neq a \in R \) is a zero divisor if there exists \( 0 \neq b \in R \) such that \( a \cdot b = 0 \) or \( b \cdot a = 0 \).

(d) \( R \) is an integral domain if \( R \) is commutative, \( R \) has 1 and \( R \) has no zero divisors. \( \square \)
Examples:

(a) \( \mathbb{Z} \) is an integral domain but not a field.

(b) \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are fields.

(c) \( \mathbb{H} \) is a division ring but not a field.

(d) In \( \mathbb{Z}_6 \), we have that \( 2, 3 \) and \( 4 \) are zero divisors while \( 1 \) and \( 5 \) are units.

(e) Let \( R = \{ f \mid f : [0, 1] \rightarrow \mathbb{R} \} \). Then \( f \in R \) is a unit if and only if \( f(x) \neq 0 \) for all \( x \in [0, 1] \). Moreover, if \( f \neq 0 \) is not a unit then \( f \) is a zero divisor.

(f) Let \( S = \{ f \mid f : [0, 1] \rightarrow \mathbb{R}, f \text{ is continuous over } [0, 1] \} \). We still have that \( f \in S \) is a unit if and only if \( f(x) \neq 0 \) for all \( x \in [0, 1] \). But \( S \) has nonzero elements that are neither a unit nor a zero divisor; e.g. \( f(x) = 2x - 1 \) for all \( x \in [0, 1] \).

The following proposition shows that cancellation holds under certain conditions.

**Proposition 6.5** Let \( R \) be a ring and \( a, b, c \in R \) such that \( 0 \neq a \) is not a zero divisor and \( ab = ac \) or \( ba = ca \). Then \( b = c \).

**Proof**: Suppose that \( ab = ac \). Then \( 0 = ab + (-ac) = ab + a(-c) = a(b + (-c)) \). Since \( a \) is not a zero divisor, we get that \( b + (-c) = 0 \). Hence \( b = c \). Similarly, if \( ba = ca \) then \( b = c \). \( \square \)

### 6.2 Subrings, Ideals and Quotient Rings

#### 6.2.1 Subrings

**Definition 6.6**: Let \( (R, +, \cdot) \) be a ring and \( S \) a nonempty subset of \( R \). Then \( S \) is a subring of \( R \) if \( (S, +, \cdot) \) forms a ring where \( S \) inherits the addition and multiplication from \( R \).

**Remarks**: Let \( R \) be a ring.

(a) Let \( \emptyset \neq S \subseteq R \). Then \( S \) is a subring of \( R \) if and only if \( (S, +) \) is an abelian group and \( S \) is closed under multiplication. So we have to check that \( a - b \in S \) and \( ab \in S \) for all \( a, b \in S \).

(b) If \( S \) is a subring of \( R \) then there is no relation between the identity in \( S \) (if \( S \) has 1) and the identity in \( R \) (if \( R \) has 1).

**Examples**:

(a) \( \mathbb{Z} \) is a subring of \( \mathbb{Q} \); \( \mathbb{Q} \) is a subring of \( \mathbb{R} \); \( \mathbb{R} \) is a subring of \( \mathbb{C} \) and \( \mathbb{C} \) is a subring of \( \mathbb{H} \). Note that all these rings have the same identity, namely 1.

(b) The set \( \{ f \mid f : [0, 1] \rightarrow \mathbb{R}, f \text{ is continuous over } [0, 1] \} \) is a subring of \( \{ f \mid f : [0, 1] \rightarrow \mathbb{R} \} \).
(c) Put \( R = \mathbb{Z}_{24} \), \( S = \{0, 2, 4, \ldots, 22\} \) and \( T = \{0, 8, 16\} \). Then \( T \) is a subring of \( S \) and \( S \) is a subring of \( R \). Note that \( T \) has identity \( 16 \), \( S \) has no identity and \( R \) has identity \( 1 \).

(d) Let \( R \) be a ring and \( n \in \mathbb{N}_0 \). Then the set \( \{A = (a_{ij})_{1 \leq i,j \leq n} \in R^{n \times n} \mid a_{ij} = 0 \text{ for all } 1 \leq i < j \leq n\} \) of upper-triangular \( n \times n \) matrices with entries over \( R \) is a subring of \( R^{n \times n} \).

(e) \( 4\mathbb{Z} \) is a subring of \( 2\mathbb{Z} \). Note that neither \( 4\mathbb{Z} \) nor \( 2\mathbb{Z} \) has identity.

(f) The set of Gaussian Integers \( \mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \) is a subring of \( \mathbb{C} \).

(g) Let \( D \in \mathbb{Z} \) such that \( D \) is not a perfect square. We put \( \sqrt{D} = \sqrt{|D|} i \) if \( D < 0 \). We define

\[
\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\} \quad \text{and} \quad \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}
\]

Since \( D \) is not a perfect square we get that every element of \( \mathbb{Z}[\sqrt{D}] \) (resp. \( \mathbb{Q}(\sqrt{D}) \)) can be written uniquely as \( a + b\sqrt{D} \) with \( a, b \in \mathbb{Z} \) (resp. \( \mathbb{Q} \)).

If \( a, b, c, d \in \mathbb{Z} \) then

\[
(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]
\]

\[
(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bd) + (ad + bc)\sqrt{D} \in \mathbb{Z}[\sqrt{D}]
\]

So \( \mathbb{Z}[\sqrt{D}] \) is a subring of \( \mathbb{R} \) (resp. \( \mathbb{C} \)) if \( D \geq 0 \) (resp. \( D < 0 \)).

If \( a, b, c, d \in \mathbb{Q} \) then

\[
(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D} \in \mathbb{Q}(\sqrt{D})
\]

\[
(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bd) + (ad + bc)\sqrt{D} \in \mathbb{Q}(\sqrt{D})
\]

Moreover, if \( 0 \neq \alpha \in \mathbb{Q}(\sqrt{D}) \) then \( \alpha = a + b\sqrt{D} \) where \( a, b \in \mathbb{Q} \) with \( (a, b) \neq (0, 0) \) and so

\[
\frac{1}{\alpha} = \frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a - b\sqrt{D}}{a^2 - b^2D} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D} \sqrt{D} \in \mathbb{Q}(\sqrt{D})
\]

So \( \mathbb{Q}(\sqrt{D}) \) is a subfield of \( \mathbb{R} \) (resp. \( \mathbb{C} \)) if \( D \geq 0 \) (resp. \( D < 0 \)).

We define a very important function on \( \mathbb{Q}(\sqrt{D}) \) called the norm :

\[
N : \mathbb{Q}(\sqrt{D}) \mapsto \mathbb{Q} : a + b\sqrt{D} \mapsto a^2 - b^2D
\]

Clearly, \( N(\alpha) \in \mathbb{Z} \) for all \( \alpha \in \mathbb{Z}[\sqrt{D}] \).

First we prove that \( N \) is ‘multiplicative’:

\[
N(\alpha \beta) = N(\alpha)N(\beta) \text{ for all } \alpha, \beta \in \mathbb{Q}(\sqrt{D})
\]
Let \(a, b, c, d \in \mathbb{Q}\). Then

\[
N((a + b\sqrt{D})(c + d\sqrt{D})) = N(ac + bdD + (ad + bc)\sqrt{D})
= (ac + bdD)^2 - (ad + bc)^2D
\]
\[
= (a^2 - b^2D)(c^2 - d^2D)
= N(a + b\sqrt{D})N(c + d\sqrt{D})
\]

Next, we prove

\[
\text{Let } \alpha \in \mathbb{Z}[\sqrt{D}]. \text{ Then } \alpha \text{ is a unit if and only if } N(\alpha) = \pm 1.
\]

Suppose first that \(\alpha\) is a unit. Then \(\alpha \beta = 1\) for some \(\beta \in \mathbb{Z}[\sqrt{D}]\). Hence

\[
N(\alpha)N(\beta) = N(\alpha \beta) = N(1) = 1
\]

Since \(N(\alpha), N(\beta) \in \mathbb{Z}\), we have that \(N(\alpha) \in \{-1, 1\}\).

Suppose next that \(N(\alpha) = \pm 1\). Put \(\alpha = a + b\sqrt{D}\) where \(a, b \in \mathbb{Z}\). Then \(\pm(a - b\sqrt{D}) \in \mathbb{Z}[\sqrt{D}]\) and

\[
(a + b\sqrt{D})(\pm(a - b\sqrt{D})) = \pm(a^2 - b^2D) = \pm(\pm 1) = 1
\]

So \(a + b\sqrt{D}\) is a unit.

If \(D < 0\), we easily get that

\[
\left(\mathbb{Z}[\sqrt{D}]\right)^\times = \begin{cases} 
{1, -1} & \text{if } D < -2 \\
{1, -1, i, -i} & \text{if } D = -1
\end{cases}
\]

However, if \(D > 0\), we find

\[
\left(\mathbb{Z}[\sqrt{D}]\right)^\times = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z} \text{ with } a^2 - b^2D = \pm 1\}
\]

This time there are infinitely many units. Finding these units involves solving Pell-Fermat equations which may require the use of continued fractions.

6.2.2 Ideals

**Definition 6.7** Let \(R\) be a ring and \(I\) a subring of \(R\).

(i) \(I\) is a left ideal of \(R\) if \(ra \in I\) for all \(a \in I\) and all \(r \in R\)

(ii) \(I\) is a right ideal of \(R\) if \(ar \in I\) for all \(a \in I\) and all \(r \in R\)

(iii) \(I\) is an ideal of \(R\) (or a two-sided ideal) (notation : \(I \subseteq R\)) if \(I\) is a left and right ideal of \(R\).
Examples:

(a) Let $R$ be a ring. Then $R$ and $\{0\}$ are ideals of $R$.

(b) For $n \in \mathbb{Z}$, we have that $n\mathbb{Z} := \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ is an ideal of $\mathbb{Z}$.

(c) The set $\{f \mid f : [0, 1] \to \mathbb{R}, f$ is continuous over $[0, 1]\}$ is a subring but not an ideal of $\{f \mid f : [0, 1] \to \mathbb{R}\}$.

(d) The set $\left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ is a left ideal but not a two-sided ideal of $\mathbb{Z}^{2 \times 2}$.

6.2.3 Quotient Rings

Let $R$ be a ring, $I$ an ideal of $R$ and $R/I$ the set of all cosets of $I$ in $(R, +)$ (so $R/I = \{r + I \mid r \in R\}$). Since $I$ is a normal subgroup of $(R, +)$, we get that $(R/I, +)$ is an abelian group under addition. We have that $(r + I) + (s + I) = (r + s) + I$ for all $r, s \in R$.

We now define a multiplication on $R/I$ as follows:

$$(r + I) \cdot (s + I) := rs + I \quad \text{for all } r, s \in R$$

This time, we have to prove that this is well-defined. So suppose that $r, s, r', s' \in R$ with $r + I = r' + I$ and $s + I = s' + I$. Then $r' = r + x$ and $s' = s + y$ for some $x, y \in I$. Hence

$$r's' = (r + x)(s + y) = rs + xs + ry + xy$$

Since $I$ is an ideal, we get that $xs, ry, xy \in I$. So $r's' + I = rs + I$.

One easily checks that $(R/I, +, \cdot)$ is a ring. The neutral element is $I$. If $R$ has identity, say 1, then $R/I$ has identity, namely $1 + I$.

Definition 6.8 Let $R$ be a ring and $I$ an ideal of $R$.

(a) The ring $(R/I, +, \cdot)$ is called the quotient ring of $R$ by $I$.

(b) For $r \in R$, we put $\overline{r} = r + I$.

Examples:

(a) Let $n \in \mathbb{N}_0$. Then $n\mathbb{Z} \leq \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is a ring with $n$ elements, namely $\{0, \overline{1}, \ldots, \overline{n-1}\}$. We denoted this ring by $\mathbb{Z}_n$ : addition and multiplication modulo $n$.

(b) Put $I = \{x^2 f(x) \mid f(x) \in \mathbb{Z}[x]\}$. Then $I \leq \mathbb{Z}[x]$. Let $f(x) \in \mathbb{Z}[x]$. Note that $f(x) = x^2 g(x) + (ax + b)$ for some $g(x) \in \mathbb{Z}[x]$ and some $a, b \in \mathbb{Z}$. Hence $\mathbb{Z}[x]/I = \{ax + b \mid a, b \in \mathbb{Z}\}$. We easily get that

$$\frac{ax + b + a'x + b'}{ax + b} = \frac{(a + a')x + (b + b')}{a'x + b'}$$

for all $a, a', b, b' \in \mathbb{Z}$.
6.3 The Ring Isomorphism Theorems

**Definition 6.9**: Let $R, S$ be rings.

(a) A **ring homomorphism** is a map $\varphi : R \rightarrow S$ such that

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$
- $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$

(b) Let $\varphi : R \rightarrow S$ be a ring homomorphism. Then $\varphi$ is a ring

- **monomorphism** if $\varphi$ is one-to-one
- **epimorphism** if $\varphi$ is onto
- **isomorphism** if $\varphi$ is bijective
- **endomorphism** if $R = S$
- **automorphism** if $R = S$ and $\varphi$ is bijective

(c) $R$ is **isomorphic** to $S$ (notation : $R \cong S$) if there exists an isomorphism $\varphi : R \rightarrow S$.

(d) Let $\varphi : R \rightarrow S$ be a homomorphism.

- The **kernel** of $\varphi$ (notation : $\text{Ker} \varphi$) is the set $\{ r \in R \mid \varphi(r) = 0 \}$.
- The **image** of $\varphi$ (notation : $\text{Im}(\varphi)$) is the set $\{ s \in S \mid s = \varphi(r) \text{ for some } r \in R \}$. □

**Examples**:

(a) Let $R$ be a ring, $X$ a nonempty set and $c \in X$. Then the following function, called the **evaluation at** $c$, is a ring epimorphism :

$$E_c : \mathcal{F}(X, R) \rightarrow R : f \mapsto f(c)$$

(b) Let $R = \{ f : [0, 1] \rightarrow \mathbb{R} \mid f \text{ is continuous on } [0, 1] \}$ and $c \in [0, 1]$. Then the following map (also called the **evaluation at** $c$) is a ring homomorphism :

$$E_c : R \rightarrow \mathbb{R} : f \mapsto f(c)$$ □

**Proposition 6.10** Let $R, S$ be rings and $\varphi : R \rightarrow S$ a ring homomorphism. Then $\text{Ker} \varphi \subseteq R$ and $\text{Im}(\varphi)$ is a subring of $S$.

**Proof**: For all $a, b \in \text{Ker} \varphi$, we have that $\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$ and so $a - b \in \text{Ker} \varphi$. For all $a \in \text{Ker} \varphi$ and all $r \in R$, we get that $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0 = 0\varphi(r) = \varphi(a)\varphi(r) = \varphi(ar)$ and so $ra, ar \in \text{Ker} \varphi$. Hence $\text{Ker} \varphi \subseteq R$.

Pick $x, y \in \text{Im}(\varphi)$. Then $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in R$. Hence $x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \in \text{Im}(\varphi)$ and $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \text{Im}(\varphi)$. So $\text{Im}(\varphi)$ is a subring of $S$. □

**Remarks**: Let $\varphi : R \rightarrow S$ be a ring homomorphism.
(a) If $R$ has an identity 1 then so does $\text{Im}(\varphi)$, namely $\varphi(1)$; moreover if $r \in R$ is a unit then so is $\varphi(r)$ (as an element of $\text{Im}(\varphi)$) with $(\varphi(r))^{-1} = \varphi(r^{-1})$.

(b) Since $\varphi$ is a group homomorphism, we get that $\varphi$ is one-to-one if and only if $\text{Ker} \varphi = \{0\}$. □

Similarly as in group theory, we have three isomorphism theorems and one lattice theorem.

**Theorem 6.11 (First Isomorphism Theorem)** Let $R, S$ be rings and $\varphi : R \mapsto S$ a ring homomorphism. Then $R/\text{Ker} \varphi \cong \text{Im}(\varphi)$.

**Proof** : Put $\theta : R/\text{Ker} \varphi \mapsto \text{Im}(\varphi) : r \mapsto \varphi(r)$. Note that $\theta$ is well-defined : if $\overline{a} = \overline{b}$ for some $a, b \in R$ then $a - b \in \text{Ker} \varphi$; so $0 = \varphi(a - b) = \varphi(a) - \varphi(b)$ and $\varphi(a) = \varphi(b)$. One easily proves that $\theta$ is a ring epimorphism. For $r \in R$, we have that $\theta(\overline{r}) = 0 \iff \varphi(r) = 0 \iff r \in \text{Ker} \varphi \iff \overline{r} = 0$. So $\theta$ is one-to-one. Hence $\theta$ is an isomorphism. □

**Theorem 6.12 (Second Isomorphism Theorem)** Let $R$ be a ring, $S$ a subring of $R$ and $I \trianglelefteq R$. Then $S + I := \{s + i \mid s \in S, i \in I\}$ is a subring of $R$, $S \cap I$ is an ideal of $S$ and $(S + I)/I \cong S/(S \cap I)$.

**Proof** : Check that $S + I$ is a subring of $R$ since $S$ is a subring of $R$ and $I \trianglelefteq R$. Consider the map $\varphi : S \mapsto (S + I)/I : s \mapsto s + I$. Then $\varphi$ is a ring epimorphism. Moreover, for $s \in S$, we have that $s \in \text{Ker} \varphi \iff \varphi(s) = 0 \iff s + I = I \iff s \in I$. So $\text{Ker} \varphi = S \cap I$. Hence $S \cap I \trianglelefteq S$ and $S/(S \cap I) \cong (S + I)/I$ by the First Isomorphism Theorem. □

**Theorem 6.13 (Third Isomorphism Theorem)** Let $R$ be a ring and $I, J \trianglelefteq R$ with $I \subseteq J$. Then $J/I \trianglelefteq R/I$ and $(R/I)/(J/I) \cong R/J$.

**Proof** : Note that $I \subseteq J$ since $I \subseteq R$. Consider the map $\varphi : R/I \mapsto R/J : r + I \mapsto r + J$. Note that $\varphi$ is well-defined : if $a + I = b + I$ for some $a, b \in R$ then $a - b \in I \subseteq J$ and so $a + J = b + J$. Check that $\varphi$ is a ring epimorphism. For $r \in R$, we have that $r + I \in \text{Ker} \varphi \iff \varphi(r + I) = 0 \iff r + J = J \iff r \in J$. So $\text{Ker} \varphi = J/I$. Hence $J/I \trianglelefteq R/I$ and $(R/I)/(J/I) \cong R/J$ by the First Isomorphism Theorem. □

**Theorem 6.14 (Lattice Isomorphism Theorem)** Let $R$ be a ring and $I \trianglelefteq R$. Then the following holds :

(a) If $S$ is a subring (resp. left ideal, right ideal, two-sided ideal) of $R$ containing $I$ then $S/I$ is a subring (resp. left ideal, right ideal, two-sided ideal) of $R/I$.

(b) If $S^\ast$ is a subring (resp. left ideal, right ideal, two-sided ideal) of $R/I$, then $S^\ast = S/I$ where $S := \{s \in R \mid s + I \in S^\ast\}$ is a subring (resp. left ideal, right ideal, two-sided ideal) of $R$ containing $I$.

**Proof** : □
Chapter 7

Properties of Ideals

Definition 7.1: Let \( R \) be a ring.

(a) Let \( A \subseteq \mathbb{R} \). Then \((A)\) is the \textit{ideal generated by} \( A \). So \((A) = \cap\{I \mid A \subseteq I \subseteq R\}\). Then \((A)\) is the smallest ideal of \( R \) containing \( A \) in the following sense: if \( A \subseteq I \subseteq R \) then \((A) \subseteq I\).

(b) A \textit{principal ideal} of \( R \) is an ideal generated by one element (so it is of the form \((a)\) for some \( a \in R \)).

Proposition 7.2 Let \( R \) be a ring with 1. Then the following holds:

(a) Let \( \emptyset \neq A \subseteq R \). Then

\[
(A) = \{r_1a_1s_1 + \cdots + r_n a_n s_n \mid n \in \mathbb{N}; r_i, s_i \in R \text{ and } a_i \in A \text{ for } i = 1, 2, \ldots, n\}
\]

In particular, if \( R \) is commutative, then

\[
(A) = \{r_1a_1 + \cdots + r_n a_n \mid n \in \mathbb{N}; r_i \in R \text{ and } a_i \in A \text{ for } i = 1, 2, \ldots, n\}
\]

(b) Let \( a \in \mathbb{R} \). Then

\[
(a) = \{r_1a_1s_1 + \cdots + r_n a_n s_n \mid n \in \mathbb{N}; r_i, s_i \in R \text{ for } i = 1, 2, \ldots, n\}
\]

In particular, if \( R \) is commutative, then

\[
(a) = \{ra \mid r \in R\}
\]

\textbf{Proof}: One easily checks that the given sets are indeed ideals containing \( A \) (resp. \( a \)). Clearly, these sets are contained in every ideal containing \( A \) (resp. \( a \)). So these sets are the ideals generated by \( A \) (resp. \( a \)). \( \square \)

Examples

(a) We know that \( \{n\mathbb{Z} \mid n \in \mathbb{Z}\} \) is the set of ideals of \( \mathbb{Z} \). Since \( n\mathbb{Z} = (n) \) for all \( n \in \mathbb{Z} \), we see that every ideal of \( \mathbb{Z} \) is a principal ideal.
(b) Consider the ring \( \mathbb{Z}[x] \). We’ll show that \((2, x)\) is not a principal ideal. We easily get that
\[
(2, x) = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\} = \{2a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}; a_0, a_1, \ldots, a_n \in \mathbb{Z}\}
\]
So \((2, x)\) is the set of all polynomials in \( \mathbb{Z}[x] \) whose constant term is even. In particular, \((2, x) \neq \mathbb{Z}[x]\). Suppose that \((2, x)\) is a principal ideal, say \((2, x) = (f(x)) = \{f(x)g(x) \mid g(x) \in \mathbb{Z}[x]\}\) for some \(f(x) \in \mathbb{Z}[x]\). Then \(2 = f(x)h(x)\) for some \(h(x) \in \mathbb{Z}[x]\). Clearly, \(\text{deg}(f(x)) = \text{deg}(h(x)) = 0\). So \(f(x) = a\) and \(h(x) = b\) for some \(a, b \in \mathbb{Z}\). Since \(2 = ab\), we get that \(a \in \{-1, 1, 2, -2\}\). If \(a = \pm 1\), then \(g(x) = (\pm g(x))(\pm 1) \in (\pm 1) = (2, x)\) for all \(g(x) \in \mathbb{Z}[x]\), a contradiction since \((2, x) \neq \mathbb{Z}[x]\). Hence \(a = \pm 2\). Since \(x \in (2, x) = (\pm 2) = (2)\), we have that \(x = 2k(x)\) for some \(k(x) \in \mathbb{Z}[x]\), a clear contradiction. Hence \((2, x)\) is not a principal ideal.

Definition 7.3: Let \( R \) be a ring and \( I, J \subseteq R \).

(a) We put
\[
I + J = \{i + j \mid i \in I, j \in J\}
\]
Then \(I + J \subseteq R\). In fact, \(I + J = (I, J)\).

(b) We put
\[
IJ = \{i_1j_1 + \cdots + i_nj_n \mid n \in \mathbb{N}; i_k \in I \text{ and } j_k \in J \text{ for } k = 1, 2, \ldots, n\}
\]
Then \(IJ \subseteq R\). In fact, \(IJ \subseteq I \cap J\).

Example: Let \(a, b \in \mathbb{Z}\), not both zero. Then
\[
a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\} = \gcd(a, b)\mathbb{Z}
\]
since \(\gcd(a, b)\) is the smallest positive linear combination of \(a\) and \(b\). Also,
\[
(a\mathbb{Z})(b\mathbb{Z}) = \{(ax)(by) \mid n \in \mathbb{Z}; x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{Z}\} = ab\mathbb{Z}
\]
but
\[
a\mathbb{Z} \cap b\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\} \cap \{by \mid y \in \mathbb{Z}\} = \text{lcm}(a, b)\mathbb{Z}
\]
So in general, \((a\mathbb{Z})(b\mathbb{Z}) \neq a\mathbb{Z} \cap b\mathbb{Z}\).

Theorem 7.4 Let \( R \) be a ring with 1.

(a) Let \( I \) be a left ideal of \( R \). Then \( I = R \) if and only if \( I \) contains a unit.

(b) \( R \) is a division ring if and only if the only left ideals of \( R \) are \( \{0\} \) and \( R \).
Proof : (a) If \( I = R \) then \( 1 \in I \). So assume that \( I \) contains a unit \( u \). Then there exists \( v \in R \) such that \( uv = 1 = vu \). So for any \( r \in R \), we have that \( r = r(vu) = (rv)u \in I \) since \( I \) is a left ideal of \( R \). Hence \( I = R \).

(b) Suppose first that \( R \) is a division ring. Let \( \{0\} \neq I \) be a left ideal of \( R \). Pick \( 0 \neq a \in I \). Then \( a \) is a unit. So \( I = R \) by (a). Suppose next that \( R \) has only two left ideals (namely \( \{0\} \) and \( R \)). Pick \( 0 \neq a \in R \). Put \( I = \{ ra \mid r \in R \} \). Then \( I \) is a left ideal of \( R \) containing \( a \). So \( I \neq \{0\} \) and hence \( I = R \). So there exists \( b \in R \) with \( ba = 1 \). Note that \( b \neq 0 \). Similarly, there exists \( c \in R \) with \( cb = 1 \). Hence \( c = c(ba) = (cb)a = a \). Hence \( ab = 1 \) and \( a \) has a multiplicative inverse (namely \( b \)). So \( R \) is a division ring.

Remark : This theorem remains true if ‘left ideal’ is replaced by ‘right ideal’.

Corollary 7.5 Let \( R \) be a commutative ring with \( 1 \). Then \( R \) is a field if and only if the only ideals of \( R \) are \( \{0\} \) and \( R \).

Proof : This follows immediately from Theorem 7.4.

Definition 7.6 : Let \( R \) be a ring and \( M \subseteq R \).

(a) \( M \) is a proper ideal of \( R \) if \( m \neq R \).

(b) \( M \) is a maximal ideal of \( R \) if \( M \) is a proper ideal of \( R \) and whenever \( M \subseteq I \subseteq R \) then \( I = M \) or \( I = R \).

Theorem 7.7 Let \( R \) be a commutative ring with \( 1 \) and \( M \) a proper ideal of \( R \). Then \( M \) is a maximal ideal if and only if \( R/M \) is a field.

Proof : By Corollary 7.5, \( R/M \) is a field if and only if \( R/M \) has exactly two ideals. By the Lattice Theorem, \( R/M \) has exactly two ideals if and only if \( R \) has exactly two ideals containing \( M \). But \( R \) has exactly two ideals containing \( M \) if and only if \( M \) is a maximal ideal.

Example : Put \( R = \{ f : [0, 1] \rightarrow \mathbb{R} \mid f \) is continuous on \([0, 1]\} \). Let \( c \in [0, 1] \). Then the map

\[ E_c : R \rightarrow \mathbb{R} : f \mapsto f(c) \]

is a ring epimorphism. Hence \( R/\ker E_c \cong \mathbb{R} \) by the First Isomorphism Theorem. Hence \( \ker E_c \) is a maximal ideal of \( R \) by Theorem 7.7.

Theorem 7.8 Let \( R \) be a ring with \( 1 \) and \( I \) a proper ideal of \( R \). Then \( I \) is contained in a maximal ideal of \( R \).

38
Proof: Put \( S = \{ J \mid I \subseteq J \subseteq R, J \neq R \} \). Then \( S \neq \emptyset \) since \( I \in S \). Note that \( \subseteq \) is a partial order on \( S \). Let \( B \) be a chain in \( S \). Put \( J = \bigcup_{B \in B} B \). Pick \( x, y \in J \). Then there exist \( X, Y \in B \) with \( x \in X \) and \( y \in Y \). Since \( B \) is a chain, we have that \( X \subseteq Y \) or \( Y \subseteq X \), say \( X \subseteq Y \). Then \( x, y \in Y \). Since \( Y \subseteq R \), we get that \( x - y \in Y \subseteq J \). So \( (J, +) \) is an abelian group. Pick \( x \in J \) and \( r \in R \). Then there exists \( X \in B \) with \( x \in X \). Since \( X \subseteq R \), we get that \( rx, xr \in X \subseteq J \). Hence \( J \) is maximal if and only if it is a maximal ideal of \( R \) containing \( I \).

Corollary 7.9 Let \( R \) be a ring with 1. Then \( R \) has maximal ideals.

Proof: By Theorem 7.8, \( R \) has a maximal ideal containing \( \{0\} \).

Definition 7.10: Let \( R \) be a commutative ring and \( P \) a proper ideal of \( R \). Then \( P \) is a prime ideal of \( R \) if

\[
\forall a, b \in R : ab \in P \Rightarrow a \in P \text{ or } b \in P
\]

Theorem 7.11 Let \( R \) be a commutative ring with 1 and \( P \) a proper ideal of \( R \). Then \( P \) is a prime ideal of \( R \) if and only if \( R/P \) is an integral domain.

Proof: Since \( R \) is commutative with 1, we have that \( R/P \) is an integral domain if and only if \( R/P \) has no zero divisors. We get

\[
R/P \text{ has no zero divisors } \iff \forall x, y \in R/P : xy = 0 \Rightarrow x = 0 \text{ or } y = 0
\]

\[
\iff \forall a, b \in R : ab = 0 \Rightarrow a = 0 \text{ or } b = 0
\]

\[
\iff \forall a, b \in R : ab \in P \Rightarrow a \in P \text{ or } b \in P
\]

\[
\iff P \text{ is a prime ideal}
\]

Corollary 7.12 Let \( R \) be a commutative ring with 1. Then every maximal ideal of \( R \) is a prime ideal of \( R \).

Proof: Let \( M \) be a maximal ideal of \( R \). By Theorem 7.7, \( R/M \) is a field. So \( R/M \) is an integral domain. Hence \( M \) is a prime ideal by Theorem 7.11.

Examples:

(a) Consider the ring \( \mathbb{Z} \). Let \( n \in \mathbb{N}_0 \). Using Theorem 7.11 and Theorem 7.7, we get that

\[
n\mathbb{Z} \text{ is a prime ideal of } \mathbb{Z} \iff \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain}
\]

\[
\iff n \text{ is a prime}
\]

\[
\iff \mathbb{Z}/n\mathbb{Z} \text{ is a field}
\]

\[
\iff n\mathbb{Z} \text{ is a maximal ideal of } \mathbb{Z}
\]

Note however that \( \{0\} \) is a prime ideal but not a maximal ideal of \( \mathbb{Z} \).

39
(b) Consider the ring $\mathbb{Z}[x]$ and the evaluation at 0:

$$E_0 : \mathbb{Z}[x] \mapsto \mathbb{Z} : f(x) \mapsto f(0)$$

Then $E_0$ is a ring epimorphism. Note that

$$\ker E_0 = \{ f(x) \in \mathbb{Z}[x] \mid f(0) = 0 \} = \{ a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}_0; a_1, \ldots, a_n \in \mathbb{Z} \} = (x)$$

By the First Isomorphism Theorem, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. So $(x)$ is a prime ideal by Theorem 7.11 but $(x)$ is not a maximal ideal by Theorem 7.7.
Chapter 8

Euclidean Domains, PID’s and UFD’s

8.1 Euclidean Domains and PID’s

Definition 8.1: Let $R$ be commutative ring.

(a) Let $a, b \in R$ with $b \neq 0$. Then $b$ divides $a$ (notation : $b|a$) if $a = bc$ for some $c \in R$.

(b) Suppose $R$ has 1. Let $a, b \in R$. Then $a$ is associate to $b$ (notation : $a \sim b$) if $a = bu$ for some $u \in R^\times$.

(c) A norm on $R$ is a function $N : R \mapsto \mathbb{N}$ with $N(0) = 0$.

(d) A norm $N$ on $R$ is called a Euclidean norm if for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

- $a = bq + r$
- $r = 0$ or $N(r) < N(b)$

Proposition 8.2 (Division Algorithm) Let $F$ be a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. Then there exist $q(x), r(x) \in F[x]$ such that

- $a(x) = b(x)q(x) + r(x)$
- $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$

Moreover, $q(x)$ and $r(x)$ are unique with these properties.

Proof:

Remark: We call $q(x)$ (resp. $r(x)$) the quotient (resp. remainder) of $a(x)$ divided by $b(x)$.
**Definition 8.3** : Let $R$ be an integral domain.

(a) $R$ is a **Euclidean Domain** if there exists a Euclidean norm $N$ on $R$.

(b) $R$ is a **Principal Ideal Domain** (notation : PID) if every ideal of $R$ is principal.

(c) We put $\tilde{R} = R^x \cup \{0\}$. ▽

**Examples :**

(a) Let $F$ be a field. Let $N : F \mapsto \mathbb{N}$ be any norm on $R$. Let $a, b \in F$ with $b \neq 0$. Put $q = ab^{-1}$ and $r = 0$. Then $a = bq + r$ and $r = 0$. So $N$ is a Euclidean norm on $F$. Hence $F$ is a Euclidean Domain.

Note that $F$ has only two ideals : $\{0\} = (0)$ and $F = (1)$. So $F$ is also a PID.

(b) Define the norm $N : Z \mapsto N : z \mapsto |z|$ on $Z$. Let $a, b \in Z$ with $b \neq 0$. Let $q$ (resp. $r$) be the quotient (resp. remainder) of $a$ divided by $b$. Then $a = bq + r$ and $N(r) = |r| = r < |b| = N(b)$. So $N$ is a Euclidean norm on $Z$. Hence $Z$ is a Euclidean Domain.

We’ve seen before that every ideal of $Z$ is principal ($nZ = (n)$ for all $n \in Z$). Hence $Z$ is also a PID.

(c) Let $F$ be a field. Define the norm $N : F[x] \mapsto \mathbb{N} : f(x) \mapsto \begin{cases} \deg(f(x)) & \text{if } f(x) \neq 0 \\ 0 & \text{if } f(x) = 0 \end{cases}$ on $F[x]$. Let $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. Let $q(x)$ (resp. $r(x)$) be the quotient (resp. remainder) of $a(x)$ divided by $b(x)$. Then $a(x) = b(x)q(x) + r(x)$ and either $r(x) = 0$ or $N(r(x)) = \deg(r(x)) < \deg(b(x)) = N(b(x))$. So $N$ is a Euclidean norm on $F[x]$. Hence $F[x]$ is a Euclidean Domain.

(d) Consider the Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$. We defined the norm $N : Z[i] \mapsto \mathbb{N} : a + bi \mapsto a^2 + b^2$ on $Z[i]$. Let $\alpha, \beta \in Z[i]$ with $\beta \neq 0$. Since $Z[i] \subseteq Q[i]$ and $Q(i)$ is a field, we have that $\alpha\beta^{-1} = x + yi$ for some $x, y \in Q$. Let $m, n \in Z$ such that $|x - m|, |y - n| \leq \frac{1}{2}$. Put $q = m + ni \in Z[i]$, $r = \alpha - \beta q \in Z[i]$ and $\theta = \alpha\beta^{-1} - q = (x - m) + (y - n)i \in Q(i)$. Then $\alpha = \beta q + r$. Note that $N(\theta) = (x - m)^2 + (y - n)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$ and $\alpha = \beta q + \theta \beta$. So $r = \theta \beta$. Hence $N(r) = N(\theta \beta) = N(\theta)N(\beta) < N(\beta)$. So $N$ is a Euclidean norm on $Z[i]$. Hence $Z[i]$ is a Euclidean Domain.

(e) We’ve seen that $(2, x)$ is not a principal ideal of the ring $Z[x]$. Hence $Z[x]$ is not a PID. ▽

**Theorem 8.4** Let $R$ be a Euclidean Domain. Then $R$ is a PID.

**Proof :** Let $N$ be a Euclidean norm on $R$. Let $I \subseteq R$. If $I = \{0\}$ then $I = (0)$. So we may assume that $I \neq \{0\}$. Let $0 \neq b \in I$ with $N(b)$ minimal among all nonzero elements of $I$. Since $b \in I$, we have that $(b) \subseteq I$. Pick $a \in I$. Then there exist $q, r \in R$ with $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$. So $r = a - bq \in I$. If $r \neq 0$, then $N(r) < N(b)$, a contradiction to the choice of $b$. Hence $r = 0$. So $a = bq \in (b)$. Hence $I \subseteq (b)$. So $I = (b)$ and $R$ is a PID. □
**Remark:** The converse of this theorem is false. We will later prove that

\[ Z \left[ \frac{1 + \sqrt{-19}}{2} \right] := \left\{ a + b \frac{1 + \sqrt{19}i}{2} \mid a, b \in \mathbb{Z} \right\} \]

is a PID but not a Euclidean Domain.

**Theorem 8.5** Let \( R \) be a PID and \( \{0\} \neq P \) a prime ideal of \( R \). Then \( P \) is a maximal ideal of \( R \).

**Proof:** Let \( P \subseteq I \subseteq R \). Since \( R \) is a PID, we have that \( I = (a) \) and \( P = (p) \) for some \( a, p \in R \). So \( p \in (p) = P \subseteq I = (a) \). Hence \( p = ar \) for some \( r \in R \). Since \( P \) is a prime ideal, we get that \( a \in P \) or \( r \in P \). If \( a \in P \) then \( I = (a) \subseteq P \) and so \( I = P \). So suppose that \( r \in P = (p) \). Then \( r = pb \) for some \( s \in R \). Hence \( p = ar = pab \). So \( ab = 1 \) and \( a \) is a unit. Hence \( I = (a) = R \). So the only ideals of \( R \) containing \( P \) are \( P \) and \( R \). Hence \( P \) is a maximal ideal of \( R \). \( \square \)

### 8.2 PID But Not Euclidean Domain

In this section, we give an example of a PID that is not a Euclidean Domain.

**Definition 8.6** Let \( R \) be an integral domain. An element \( u \in R \setminus \tilde{R} \) is a *universal side divisor* if for all \( x \in R \) there exists \( z \in \tilde{R} \) such that \( u \) divides \( x - z \).

**Proposition 8.7** Let \( R \) be a Euclidean domain but not a field. Then \( R \) has universal side divisors.

**Proof:** Note that \( R \setminus \tilde{R} \neq \emptyset \) since \( R \) is not a field. Let \( N : R \rightarrow \mathbb{N} \) be a Euclidean norm on \( R \). Pick \( u \in R \setminus \tilde{R} \) with \( N(u) \) minimal among all elements of \( R \setminus \tilde{R} \). Let \( x \in R \). Then \( x = uq + r \) for some \( q, r \in R \) with either \( r = 0 \) or \( N(r) < N(u) \). If \( r \neq 0 \) then \( N(r) < N(u) \) and so \( r \notin (R \setminus \tilde{R}) \) by choice of \( u \). Either way, we get that \( r \in \tilde{R} \). Since \( x - r = uq \), we have that \( u \) divides \( x - r \). Hence \( u \) is a universal side divisor. \( \square \)

**Example:** Consider the ring \( R := Z \left[ \frac{1 + \sqrt{-19}}{2} \right] \).

Let \( N \) be the standard norm on \( \mathbb{Q}(\sqrt{-19}) \) (so \( N(a + b\sqrt{-19}) = a^2 + 19b^2 \) for all \( a, b \in \mathbb{Q} \)). Then we get that

\[ N \left( a + b \frac{1 + \sqrt{-19}}{2} \right) = \left( a + \frac{b}{2} \right)^2 + 19 \left( \frac{b}{2} \right)^2 = a^2 + ab + 5b^2 \quad \text{for all } a, b \in \mathbb{Q} \]

Using this norm, we can deduce the following:

- \( \forall \alpha \in R : N(\alpha) = 1 \iff \alpha \in R^x \)
- \( R^x = \{-1, 1\} \) and so \( \tilde{R} = \{0, -1, 1\} \)
- \( \forall \alpha, \beta \in R : \beta \neq 0 \text{ and } \beta \text{ divides } \alpha \implies N(\beta) \text{ divides } N(\alpha) \) (as natural numbers)
Suppose that $R$ is a Euclidean Domain. Since $R$ is not a field, we get that $R$ has universal side divisors by Proposition 8.7. Let $u \in R$ be a universal side divisor. Consider $x = 2 \in R$. Then $u$ divides one of the elements of $\{x - 1, x, x + 1\} = \{1, 2, 3\}$. Hence $N(u)$ divides one of the elements of $\{N(1), N(2), N(3)\} = \{1, 4, 9\}$ as natural numbers. Keeping in mind the smallest values of $N$ on $R$, we get that $N(u) \in \{1, 4, 9\}$. Since $u \not\in R^\times$, we have that $N(u) \neq 1$. So $N(u) \in \{4, 9\}$. Now consider $y = \frac{1 + \sqrt{-19}}{2} \in R$. Then $u$ divides one of the elements of $\{y - 1, y, y + 1\} = \{-\frac{1 + \sqrt{-19}}{2}, \frac{1 + \sqrt{-19}}{2}, \frac{3 + \sqrt{-19}}{2}\}$. Hence $N(u)$ divides one of the elements of $\left\{N\left(-\frac{1 + \sqrt{-19}}{2}\right), N\left(\frac{1 + \sqrt{-19}}{2}\right), N\left(\frac{3 + \sqrt{-19}}{2}\right)\right\} = \{5, 7\}$ as natural numbers, a contradiction since $N(u) \in \{4, 9\}$.

Hence we proved

\[
\left[\frac{1 + \sqrt{-19}}{2}\right] \text{ is not a Euclidean Domain.}
\]

**Proposition 8.8** Let $R$ be an integral domain and $N : R \mapsto \mathbb{N}$ a norm on $R$ such that

(a) $\forall r \in R : N(r) = 0 \iff r = 0$

(b) $\forall a, b \in R \setminus \{0\} : \text{ either } a \in (b) \text{ or } 0 < N(c) < N(b) \text{ for some } c \in (a, b)$

Then $R$ is a PID.

**Proof:** Let $I \subseteq R$. If $I = \{0\}$ then $I = (0)$. So we may assume that $I \neq \{0\}$. Pick $0 \neq b \in I$ with $N(b)$ minimal among all nonzero elements of $I$. Clearly, $(b) \subseteq I$. Let $a \in I$. If $a = 0$ then $a \in (b)$. So we may assume that $a \neq 0$. If $a \notin (b)$ then $0 < N(c) < N(b)$ for some $c \in (a, b)$ and so $0 \neq c \in I$, a contradiction to the choice of $b$. Hence $a \in (b)$. So $I \subseteq (b)$ and $I = (b)$. Hence $R$ is a PID. \qed

**Example:** Consider the ring $R := Z \left[\frac{1 + \sqrt{-19}}{2}\right]$. Let $N$ be the standard norm on $\mathbb{Q}(\sqrt{-19})$ (so $N(a + b\sqrt{-19}) = a^2 + 19b^2$ for all $a, b \in \mathbb{Q}$). We will show that this norm satisfies Proposition 8.8. Let $\alpha, \beta \in R \setminus \{0\}$. Note that $\mathbb{Q}(\sqrt{-19})$ is a field. If $\frac{\alpha}{\beta} \in R$ then $\alpha \in (\beta)$. So we may assume that $\frac{\alpha}{\beta} \notin R$. Hence we have that

\[
\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{c} \quad \text{for some } a, b, c \in \mathbb{Z} \text{ with } c > 1 \text{ and } \gcd(a, b, c) = 1
\]

We will show the following

\[
\exists s, t \in R : 0 < N\left(\frac{\alpha}{\beta} s - t\right) < 1 \quad (*)
\]

Suppose that $c = 2$. Then $a \not\equiv b \mod 2$ since $\frac{\alpha}{\beta} \notin R$. Put $s = 1$ and $t = \frac{(a-1)+b\sqrt{-19}}{2}$. Then (*) holds.
Suppose that \( c = 3 \). If \( a^2 + 19b^2 \equiv 0 \mod 3 \) then \( a^2 + b^2 \equiv 0 \mod 3 \) and so \( a \equiv b \equiv 0 \mod 3 \), a contradiction since \( \gcd(a, b, c) = 1 \). Hence \( a^2 + 19b^2 = 3q + r \) with \( q \in \mathbb{N} \) and \( r \in \{1, 2\} \). Put \( s = a - b \sqrt{-19} \) and \( t = q \). Then (*) holds.

Suppose that \( c = 4 \). If \( a \not\equiv b \mod 2 \) then \( a^2 + 19b^2 = 4q + r \) with \( q \in \mathbb{N} \) and \( r \in \{1, 3\} \); so (*) holds for \( s = a - b \sqrt{-19} \) and \( t = q \). If \( a \equiv b \mod 2 \) then \( a \equiv b \equiv 1 \mod 2 \) since \( \gcd(a, b, c) = 1 \); hence \( a^2 + 19b^2 = 8q + 4 \) with \( q \in \mathbb{N} \) and (*) holds for \( s = a - b \sqrt{-19} \) and \( t = q \).

Suppose that \( c \geq 5 \). Since \( \gcd(a, b, c) = 1 \), we have that \( ax + by + cz = 1 \) for some \( x, y, z \in \mathbb{Z} \). Then \( ay - 19bx = cq + r \) where \( q, r \in \mathbb{Z} \) and \( |r| \leq \left\lfloor \frac{c}{2} \right\rfloor \). Put \( s = y + x \sqrt{-19} \) and \( t = q - z \sqrt{-19} \). Then

\[
0 < N \left( \frac{\alpha}{\beta} s - t \right) = N \left( \frac{a + b \sqrt{-19}}{c} \left( y + x \sqrt{-19} \right) - (q - z \sqrt{-19}) \right) \\
= N \left( \frac{ay - 19x - cq}{c} + \frac{ax + by + cz}{c} \sqrt{-19} \right) \\
= N \left( \frac{r + \sqrt{-19}}{c} \right) \\
= \frac{r^2 + 19}{c^2}
\]

If \( c = 5 \) then \( |r| \leq 2 \) and so \( \frac{r^2 + 19}{c^2} \leq \frac{23}{25} < 1 \). If \( c > 5 \) then \( |r| \leq \frac{c}{2} \) and so \( \frac{r^2 + 19}{c^2} \leq \frac{1}{4} + \frac{19}{36} = \frac{28}{36} < 1 \). So (*) holds.

In all cases, we have that (*) holds. Since \( N \) is multiplicative, we get that \( 0 < N(\alpha s - \beta t) < N(\beta) \).

Note that \( \alpha s - \beta t \in (\alpha, \beta) \).

By Proposition 8.8, we have that \( R \) is a PID. We’ve shown before that \( R \) is not a Euclidean Domain. So we proved

\[
\mathbb{Z} \left[ \frac{1 + \sqrt{-19}}{2} \right] \text{ is a PID but not a Euclidean Domain.}
\]

### 8.3 UFD’s

**Definition 8.9** : Let \( R \) be an integral domain and \( r \in R \setminus \tilde{R} \).

(a) \( r \) is irreducible if \( \forall a, b \in R \colon r = ab \Rightarrow a \in R^\times \) or \( b \in R^\times \)

(b) \( r \) is reducible if \( r \) is not irreducible.

(c) \( r \) is prime if \( \forall a, b \in R \colon r|ab \Rightarrow r|a \) or \( r|b \)

So \( r \in R \setminus \tilde{R} \) is prime if and only if (r) is a nonzero prime ideal of \( R \).

**Remark** : If \( r \) is irreducible (resp. prime) and \( t \sim r \) then \( t \) is irreducible (resp. prime).

**Examples** :
(a) Consider the ring $\mathbb{Z}$. For $n \in \mathbb{Z}$, we have that

$$n \text{ is irreducible } \iff n \text{ is prime } \iff n = \pm p \text{ for some prime number } p$$

(b) Consider the Gaussian integers $R := \mathbb{Z}[i]$. Let $N$ be the usual norm on $R$ (so $N(a + bi) = a^2 + b^2$ for all $a, b \in \mathbb{Z}$). Then we have the following:

- $\forall \alpha \in R : N(\alpha) = 1 \iff \alpha \in R^\times$
- $R^\times = \{1, -1, i, -i\}$ and so $\tilde{R} = \{0, 1, -1, i, -i\}$

Consider the element $2 + i$. Suppose that $2 + i = \alpha \beta$ for some $\alpha, \beta \in R$. Then $5 = N(2 + i) = N(\alpha \beta) = N(\alpha)N(\beta)$. Hence $N(\alpha) = 1$ or $N(\beta) = 1$. So $\alpha \in R^\times$ or $\beta \in R^\times$. Hence $2 + i$ is irreducible.

(c) Consider the ring $R := \mathbb{Z}[\sqrt{-5}]$. Let $N$ be the usual norm on $R$ (so $N(a + b \sqrt{-5}) = a^2 + 5b^2$ for all $a, b \in \mathbb{Z}$). Then we have the following:

- $\forall \alpha \in R : N(\alpha) = 1 \iff \alpha \in R^\times$
- $R^\times = \{-1, 1\}$ and so $\tilde{R} = \{0, -1, 1\}$
- $\forall \alpha, \beta \in R : \beta \neq 0$ and $\beta$ divides $\alpha \implies N(\beta)$ divides $N(\alpha)$ (as natural numbers)
- the smallest values of $N$ on $R$ are $0, 1, 4, \ldots$

We show that the element $3 \in R$ is irreducible but not a prime.

Suppose that $3 = \alpha \beta$ for some $\alpha, \beta \in R$. Then $9 = N(3) = N(\alpha \beta) = N(\alpha)N(\beta)$. Keeping in mind the smallest values of $N$ on $R$, we get that $N(\alpha) = 1$ or $N(\beta) = 1$. Hence $\alpha \in R^\times$ or $\beta \in R^\times$. So $3$ is irreducible.

Note that $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$. Thus $3|(2 + \sqrt{-5})$. Then $2 + \sqrt{-5} = 3\alpha$ for some $\alpha \in R$. Hence

$$9 = N(2 + \sqrt{-5}) = N(3\alpha) = N(3)N(\alpha) = 9N(\alpha)$$

So $N(\alpha) = 1$. Hence $\alpha \in R^\times = \{-1, 1\}$, a contradiction since $2 + \sqrt{5} \neq \pm 3$. So $3 \nmid (2 + \sqrt{-5})$. Similarly, $3 \nmid (2 - \sqrt{-5})$. Hence $3$ is not a prime.

Proposition 8.10 Let $R$ be an integral domain and $r \in R \setminus \tilde{R}$ prime. Then $r$ is irreducible.

**Proof**: Suppose that $r = ab$ for some $a, b \in R$. So $r|ab$. Since $r$ is prime, we get that $r|a$ or $r|b$, say $r|b$. Then $b = cr$ for some $c \in R$. Hence $r = ab = acr$. So $ac = 1$ and $a \in R^\times$. Hence $r$ is irreducible. □

**Remark**: The converse is not true: we have shown that $3$ is irreducible but not prime in the ring $\mathbb{Z}[\sqrt{-5}]$. □
**Definition 8.11** : Let $R$ be an integral domain. Then $R$ is a Unique Factorization Domain (notation : UFD) if every $r \in R \setminus \hat{R}$ can be written uniquely (up to order and associates) as a product of irreducibles. So for all $r \in R \setminus \hat{R}$, we have

1. $r = p_1 \cdots p_n$ where $n > 0$ and $p_1, \ldots, p_n$ are irreducible (but not necessarily distinct)

2. if $r = p_1 \cdots p_n = q_1 \cdots q_m$ where $m, n > 0$ and $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible then $n = m$ and there exists $\sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$ for $i = 1, 2, \ldots, n$. $\triangleright$

**Theorem 8.12** Let $R$ be a UFD and $r \in R \setminus \hat{R}$ irreducible. Then $r$ is prime.

**Proof** : Let $a, b \in R$ with $r \mid ab$. Then $ab = rc$ for some $c \in R$. If $a = 0$ or $b = 0$ then clearly $r \mid a$ or $r \mid b$. So we may assume that $a \neq 0 \neq b$. If $a \in R^\times$ (resp. $b \in R^\times$) then $b = rca^{-1}$ (resp. $a = rcb^{-1}$) and so $r \mid b$ (resp. $r \mid a$). Hence we may assume that $a, b \in R \setminus \hat{R}$. If $ab \in R^\times$ then $r \in R^\times$, a contradiction. Hence $a, b, ab \in R \setminus \hat{R}$. Since $R$ is a UFD, we have that $a = p_1 \cdots p_m$ and $b = q_1 \cdots q_n$ where $m, n > 0$ and $p_1, \ldots, p_m, q_1, \ldots, q_n$ are irreducible. Writing $c$ as a product of irreducibles if $c \notin R^\times$ and using the fact that $R$ is a UFD, we see that there exists $u \in R^\times$ with $ur \in \{p_1, \ldots, p_m, q_1, \ldots, q_n\}$, say $ur = p_1$. Hence $a = r(\upsilon p_2 \cdots p_m)$. So $r \mid a$. Hence $r$ is prime. \hfill $\Box$

**Example** : We’ve shown that 3 is irreducible but not a prime in the ring $\mathbb{Z}[\sqrt{-5}]$. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

**Lemma 8.13** Let $R$ be a PID and $r \in R \setminus \hat{R}$ irreducible. Then $r$ is prime.

**Proof** : Suppose that $(r) \subseteq M \subseteq R$. Then $M = (m)$ for some $m \in M$. Since $r \in (m)$, we have that $r = ms$ for some $s \in R$. Since $r$ is irreducible, we get that $m \in R^\times$ or $s \in R^\times$. If $m \in R^\times$ then $M = (m) = R$; if $s \in R^\times$ then $M = (m) = (r)$. Hence $M = (r)$ or $m = R$. So $(r)$ is a maximal ideal of $R$. Hence $(r)$ is a nonzero prime ideal of $R$. So $r$ is prime. \hfill $\Box$

**Theorem 8.14** Let $R$ be a PID. Then $R$ is a UFD.

**Proof** : First, we show that every element of $R \setminus \hat{R}$ can be written as a product of irreducibles. Suppose this is not true. Then there exists $r \in R \setminus \hat{R}$ such that $r$ can not be written as a product of irreducibles. We prove the following claim:

There exist $r_n \in R$ for all $n \geq 0$ such that $r_n$ can not be written as a product of irreducibles for all $n \geq 0$ and

$$(r_0) \subset (r_1) \subset (r_2) \subset (r_3) \subset \cdots$$

Indeed, put $r_0 = r$. Suppose that we already have $r_0, \ldots, r_n$ for some $n \geq 0$. Clearly, $r_n$ is not irreducible. Hence $r_n = ab$ for some $a, b \in R \setminus \hat{R}$. If $a$ and $b$ can be written as a product of irreducibles then $r_n$ can be written as a product of irreducibles, a contradiction. So either $a$ or $b$ can not be written as a product of irreducibles, say $a$. Put $r_{n+1} = a$. Since $r_n = r_{n+1}b$, we have that $(r_n) \subseteq (r_{n+1})$. Suppose that $(r_n) = (r_{n+1})$. Then $r_{n+1} = r_n s$ for some $s \in R$. So $r_n = r_{n+1}b = r_n sb$. Since $r_n \neq 0$, we get that $1 = sb$ and so $b \in R^\times$, a contradiction. Hence $(r_n) \subset (r_{n+1})$, which proves the claim. 

47
So we have an infinite strictly increasing sequence of ideals, a contradiction since $R$ is a PID. Hence every element of $R \setminus \tilde{R}$ can be written as a product of irreducibles.

Next, we prove the following by induction on $n$:

If an element of $R \setminus \tilde{R}$ can be written as a product of $n$ irreducibles then this decomposition into irreducibles is unique up to order and associates.

Consider first $n = 1$. Let $r \in R \setminus \tilde{R}$ that can be written as a product of $n$ irreducibles. So $r$ is irreducible. Suppose that $r = p_1 \cdots p_m$ where $m \geq 1$ and $p_1, \ldots, p_m$ are irreducible. Then $r|p_1 \cdots p_m$. Note that $r$ is prime by Lemma 8.13. Hence $r|p_i$ for some $1 \leq i \leq m$, say $r|p_1$. So $p_1 = rs$ for some $s \in R$. Hence $r = p_1 \cdots p_m = rsp_2 \cdots p_m$. Since $r \neq 0$, we have that $1 = sp_2 \cdots p_m$. So $s \in R^x$ and $p_2, \ldots, p_m \in R^x$ if $m \geq 2$. Hence $m = 1$ and $p_1 = rs \sim r$.

So assume that the statement is true for $n = 1, \ldots, k - 1$ for some $k \geq 2$. Let $r \in R \setminus \tilde{R}$ that can be written as a product of $k$ irreducibles, say $r = p_1 \cdots p_k$. Suppose that $r = q_1 \cdots q_m$ where $m \geq 1$ and $q_1, \ldots, q_m$ are irreducible. If $m < k$ then we can use induction to get a contradiction. Hence $m \geq k$.

Note that $p_1|q_1 \cdots q_m$. By Lemma 8.13, $p_1$ is prime and so $p_1|q_i$ for some $1 \leq i \leq m$, say $p_1|q_i$. Hence $q_1 = p_1 s$ for some $s \in R$. So $r = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m = p_1 s q_2 \cdots q_m$. Since $p_1 \neq 0$, we get that

$$p_2 \cdots p_k = (sq_2)q_3 \cdots q_m$$

Since $q_1$ is irreducible and $q_1 = p_1 s$, we get that $s \in R^x$ because $p_1 \notin R^x$. Note that $sq_2$ is irreducible since $s \in R^x$ and $q_2$ is irreducible. By induction, $m - 1 = k - 1$ (and so $m = k$) and we may assume that $q_i \sim p_i$ for $i = 3, \ldots, k$ and $sq_2 \sim p_2$. But $q_2 \sim sq_2$ and $q_1 \sim p_1$. So $q_1 \sim p_i$ for $i = 1, \ldots, k$. $\Box$

**Remark**: The converse is this Theorem is not true. We have seen that $\mathbb{Z}[x]$ is not a PID. We will later prove that $\mathbb{Z}[x]$ is a UFD.

**Example**: Consider the Gaussian integers $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Euclidean Domain, we have that $\mathbb{Z}[i]$ is a PID (by Theorem 8.4) and hence a UFD (by Theorem 8.14). So $28 - 47i$ can be written as a product of irreducibles. To practically find a factorization of $28 - 47i$, we use the norm.

Suppose that $28 - 47i = \alpha \beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Applying the norm $N$ to both sides, we get that

$$41 \cdot 73 = 2993 = 28^2 + (-47)^2 = N(28 - 47i) = N(\alpha \beta) = N(\alpha)N(\beta)$$

Since $N(\alpha), N(\beta) \in \mathbb{N}$, we may assume that $(N(\alpha), N(\beta)) \in \{(1, 2993), (41, 73)\}$. If $(41, 73)$ is impossible then $28 - 47i$ is irreducible. First, we’ll find all $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = 41$. Putting $\alpha = a + bi$, we get that $N(\alpha) = a^2 + b^2 = 41$. Since $a, b \in \mathbb{Z}$ we get

$$(a, b) \in \{(5, 4), (5, -4), (-5, 4), (-5, -4), (4, 5), (4, -5), (-4, 5), (-4, -5)\}$$

So

$$\alpha \in \{5 + 4i, 5 - 4i, -5 + 4i, -5 - 4i, 4 + 5i, 4 - 5i, -4 + 5i, -4 - 5i\}$$

We can divide the eight possibilities in groups of four (grouping associates together):

$$\{1 \cdot (5 + 4i), (-1) \cdot (5 + 4i), i \cdot (5 + 4i), (-i) \cdot (5 + 4i)\} = \{5 + 4i, -5 - 4i, -4 + 5i, 4 - 5i\}$$

$$\{1 \cdot (5 - 4i), (-1) \cdot (5 - 4i), i \cdot (5 - 4i), (-i) \cdot (5 - 4i)\} = \{5 - 4i, -5 + 4i, 4 + 5i, -4 - 5i\}$$

48
Now we try one element of these groups of four. If neither group works, \(28 - 47i\) is irreducible; if one of the groups works then we found a ‘factorization’ of \(28 - 47i\).

First, we try \(5 + 4i\). We easily get

\[
\frac{28 - 47i}{5 + 4i} = \frac{(28 - 47i)(5 - 4i)}{(5 + 4i)(5 - 4i)} = \frac{-48 - 347i}{41} = -\frac{48}{41} - \frac{347}{41}i \notin \mathbb{Z}[i]
\]

So \(28 - 47i\) is not divisible by \(5 + 4i\) (nor by \(-5 - 4i, -4 + 5i\) or \(4 - 5i\)).

Next, we try \(5 - 4i\). We easily get

\[
\frac{28 - 47i}{5 - 4i} = \frac{(28 - 47i)(5 + 4i)}{(5 - 4i)(5 + 4i)} = \frac{328 - 123i}{41} = 8 - 3i \in \mathbb{Z}[i]
\]

Hence we came up with the following factorization:

\[
28 - 47i = (5 - 4i)(8 - 3i)
\]

Since \(N(5 - 4i) = 41\) and \(N(8 - 3i) = 73\) are prime numbers, we have that \(5 - 4i, 8 - 3i\) are irreducible. Hence we have written \(28 - 47i\) as a product of irreducibles.

\[\blacktriangle\]

**Theorem 8.15** Let \(R\) be an integral domain. Then \(R\) is a UFD if and only if \(R[x]\) is a UFD.

**Proof :**

\[\square\]

**Example :** Since \(\mathbb{Z}\) is a Euclidean Domain, we have that \(\mathbb{Z}\) is a UFD and so \(\mathbb{Z}[x]\) is a UFD.

\[\blacktriangle\]

So we have the following proper inclusions among the classes of integral domains:

\[
\text{fields} \subset \text{Euclidean Domains} \subset \text{PID’s} \subset \text{UFD’s} \subset \text{integral domains}
\]

All inclusions are indeed proper:

- \(\mathbb{Z}\) is a Euclidean Domain but not a field
- \(\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]\) is a PID but not a Euclidean Domain
- \(\mathbb{Z}[x]\) is a UFD but not a PID
- \(\mathbb{Z}[^{\sqrt{-5}}]\) is an integral domain but not a UFD

49