Contents

Chapter 1

Preliminary

$R \subset A \times A$ is an equivalence relations if

Reflexive: $\forall a \in A, (a, a) \in R$.

Symmetric: $(a, b) \in R \implies (b, a) \in R$.

Transitive: $(a, b) \in R, (b, c) \in R \implies (a, c) \in R$.

A binary relations can be also denoted as aRb whenever $(a, b) \in R$.
If A is a set and if $\sim$ is an equivalence relation on A, then the equivalence class of $a \in A$ is the set $\{x \in A \,|\, x \sim a\}$ denoted by $\mathrm{cl}(a)$.

Theorem 1.1. *Equivalence classes partition the set into mutually disjoint subsets and conversely, mutually disjoint subsets give rise to equivalence classes.*

If S and T are non-empty sets, then a mapping from S to T is a subset $M \subset S \times T$ such that for every $s \in S$ there is a unique $t \in T$ that $(s, t) \in M$. $\sigma : S \to T$ maybe denoted as $t = s\sigma$ or $t = \sigma(s)$.

Chapter 2

Group Theory

2.1 Introduction

Definition: A set S equipped with an associative binary operation is a **semigroup**.

A semigroup can have multiple left or right identities. However, if it has both left identity, e, and right identity, f, then those two are equal since $e = ef = f$. Two sided identity are unique. We have the same story with inverses.

Definition: A non-empty set of elements G together with a binary operation $\circ$ are said to be a **group** if

Closure: $\forall a, b \in G, a \circ b \in G$.

Associative: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$.

Identity: $\exists e \in G$ such that $\forall a \in G, a \circ e = e \circ a = a$.

Inverse: $\forall a \in G\ \exists b \in G$ such that $a \circ b = b \circ a = e$.

Example 2.1. The set of n_{th} roots of unity forms a group under multiplication.

Example 2.2. The interval $[0, 1[$ forms a group under the following operation.

$$x + y = \begin{cases} x + y & x + y < 1 \\ x + y - 1 & x + y \geq 1 \end{cases}$$

This is called the **group of real numbers modulu 1**.

Example 2.3. The set of all symmetries of a regular n-gon forms a group under composition. i.e. applying two symmetries results in a another symmetry. This is called **dihedral group of order** n, denoted by D_n. We can easily show that $|D_n| = 2n$.

Example 2.4. The permutations of a set form a group under composition, called the **symmetric group**, denoted by S_n for finite sets of size n.

Example 2.5. The **general linear group**, $\mathrm{GL}_n(\mathbb{F})$ is set of all non-singular $n \times n$ matrices from field $\mathbb{F}$.

Example 2.6. The **Heisenberg group**

$$H(\mathbb{F}) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c \in \mathbb{F} \right\}.$$

Example 2.7. The **Quaternion group**, $Q_8 = \{1, -i, i, -i, j, -j, k, -k\}$ with $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$.

Definition: A group G is said to be **abelian** or **commutative** if for any two element a and b commute. i.e. $a \circ b = b \circ a$.

Definition: The number of elements in a group is called the **order** of the group and it is denoted by $|G|$.

Definition: Let $\langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\}$. If for some choice of a, $G = \langle a \rangle$, then G is said to be a **cyclic group**. More generally, for a set $W \subset G$, $\langle W \rangle = \bigcap W \subset H \subset GH$ where H is a subgroup of G.

Lemma 2.1. *Given $a, b \in G$ the equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.*

Proof. Note that a^{-1} and b^{-1} are unique. Therefore, $x = a^{-1}b$ and $y = ba^{-1}$ are unique. □

Exercises

1. Let S be a finite semi-group. Prove that there exists $e \in S$ such that $e^2 = e$.

   Proof. Pick $a \in S$ and consider $a_i = a^{2^i}$ for $i \geq 1$. After some point, a_is repeat, by the pigeon hole principle. Let that point be a_j. Therefore, for some $m \geq 1$.

   $$a_j = (a_j)^{2^m}$$

   Let $e = a_j^{2^m-1}$, then

   $$e^2 = a_j^{2^{m+1}-2} = a_j^{2^m} a_j^{2^m-2} = a_j a_j^{2^m-2} = e$$

   we are done. ■

2. Show that if a group G is abelian, then for $a, b \in G$ and any integer n, $(ab)^n = a^n b^n$.

   Proof. Induct over positive n. It is trivially true for $n = 1$. Suppose it is true for $n = k$, then

   $$(ab)^{k+1} = (ab)^k ab = a^k b^k ab = a^k ab^k b = a^{k+1} b^{k+1}$$

   For negative n, note that

   $$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \implies (ab)^n = ((ab)^{-1})^{-n} = (a^{-1}b^{-1})^{-n} = a^n b^n$$

   hence it is true for all integers n. ■

3. If a group has an even order, then there exists $a \neq e$ such that $a^2 = e$.

Proof. Let $A = \{g \,|\, g \neq g^{-1}\}$ and $B = \{g \,|\, g = g^{-1}\}$. Note that, $|A|$ is even since $g \in A \implies g^{-1} \in A$. Moreover, $|G| = |A| + |B|$, therefore $|B|$ must be even and since $e \in B$, $|B| \geq 2$. ■

4. For any $n > 2$ construct a non-abelian group of order $2n$.

   Proof. Consider ϕ, ψ where $\psi^n = \phi^2 = e$ and $\psi\phi = \phi\psi^{-1}$. Then

   $$G = \left\{I, \phi, \psi, \psi^2, \ldots, \psi^{n-1}, \phi\psi, \ldots, \phi\psi^{n-1}\right\}$$

   is a group of order $2n$. Because, by the product rules defined, any combination of ψ and ϕ can be reduced to $\phi^b\psi^k$ where $b = 0, 1$ and $k = 0, 1, \ldots, n-1$. It is cleary non-abelian as well. ■

5. Find the order of $\mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathrm{SL}_2(\mathbb{Z}_p)$ for a prime p.

   Proof.

   $$|\mathrm{GL}_2(\mathbb{Z}_p)| = (p+1)p(p-1)^2$$
   $$|\mathrm{SL}_2(\mathbb{Z}_p)| = (p+1)p(p-1)$$

   which be can be calculate with some basic casing. ■

6. Prove that finiteness of $\mathrm{GL}_n(\mathbb{F})$ is equivalent to finiteness of $\mathbb{F}$.

2.2 Subgroup

Definition: A non-empty subset H of a group G is called a **subgroup** if under the product in G, H itself forms a group. H is a subgroup of G is denoted by $H \leq G$. If H is proper subgroup of, $H < G$.

Lemma 2.2. *H is a subgroup of G if and only if*

1. $\forall a, b \in H, ab \in H$.
2. $\forall a \in H, a^{-1} \in H$.

Proof. If H is a subgroup, then the conditions hold. Suppose H is a subset of G that satisfies the conditions. Then,

1. $e \in H$ since $(a \in H \implies a^{-1} \in H) \implies e = aa^{-1} \in H$.
2. Associativity is inherited from G.

invertibility and closure are given from the conditions. Therefore, H is a subgroup. □

Lemma 2.3. *If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.*

Proof. Since H is non-empty there exists a $a \in H$. By closure, a^n for positive integer n, are also in H. We know that for some N, $a^N = e$ and therefore $a^{-1} = a^{N-1} \in H$. By , H is a subgroup. □

Definition: Let G be a group and H a subgroup of G. For $a, b \in G$ we say that a is congruent to $b \mod H$, written as $a \equiv b \mod H$ if $ab^{-1} \in H$.

Lemma 2.4. *The relation $a \equiv b \mod H$ is an equivalence relation.*

Proof. We show the equivalence axioms:

1. for any a, $a \equiv a \mod H$ becuase, $aa^{-1} = e \in H$.
2. for any a, b, $a \equiv b \mod H \implies b \equiv a \mod H$ since $ab^{-1} \in H$ because of invertibility implies that $(ab^{-1})^{-1} = ba^{-1} \in H$.
3. for any a, b, c, $a \equiv b \mod H, b \equiv c \mod H \implies a \equiv c \mod H$ since $ab^{-1}, bc^{-1} \in H$ because of closure implies that $ab^{-1}bc^{-1} = bc^{-1} \in H$. □

Definition: If H is a subgroup of G and $a \in G$, then $Ha = \{ha \,|\, h \in H\}$ is a **right coset** of H in G. Similary, $aH = \{ah \,|\, h \in H\}$ is a **left coset** of H in G.

Lemma 2.5. *For all $a \in G$,*

$$Ha = \{x \in G \,|\, a \equiv x \mod H\}$$

Proof. Suppose $x \in G$ and $x \equiv a \mod H$. That is, $xa^{-1} = h$ for some $h \in H$. Then, $x = ha$. Suppose $h \in H$ and $x = ha$. Then, $xa^{-1} = h$ and hence $x \equiv a \mod H$. □

This implies, two right/left coset of H are either identical or disjoint.

Lemma 2.6. *There is a one-to-one correspondence between any two right/left cosets of H.*

Proof. Let R_1, R_2 be two right cosets of H with $a_1 \in R_1$ and $a_2 \in R_2$. Note that, $R_1 = Ha_1$ and $R_2 = Ha_2$, therefore the map $g \mapsto ga_1^{-1}a_2$ is a bijective map from R_1 to R_2. □

Theorem 2.7 (Lagrange's theorem). *If G is a finite group and H is a subgroup of G, then $|H| \mid |G|$.*

Proof. By and , and from finiteness of G, the order of G is equal to the number of right cosets multiplied by the cardinality of a right coset which is equal to the order of H. Hence, $|H| \mid |G|$ ■

Definition: If H is a subgroup of G, the **index** of H in G is the number of distince right cosets of H, denoted by $[G : H]$ or $i_G(H)$.

Definition: Let G be a group and $a \in G$, then the **order** or **period** of a is the least positive integer m such that $a^m = e$. If no such integer exists we say that a is of infinite order. The order of a is denoted by $\text{ord}_G(a)$.

Corollary 2.8. *If G is a finite group, then*

1. $|G| = i_G(H)|H|$.
2. $\text{ord}_G(a) \mid |G|$.

3. $a^{|G|} = e$.

4. If $|G|$ *is a prime, then* G *is cyclic.*

Let A be a non-empty subset of G. The smallest subgroup of G that contains A is denoted by $\langle A \rangle$

$$\langle A \rangle = \bigcap_{\substack{A \subset H \\ H \leq G}} H$$

Lemma 2.9. *Let* A *be a non-empty subset of* G*. Let*

$$\bar{A} = \left\{ a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \,\middle|\, n \in \mathbb{Z}_0^+, a_i \in A, \epsilon_i = \pm 1 \right\}$$

. Then $\langle A \rangle = \bar{A}$*.*

Proof. First note that $\bar{A}$ is a subgroup of G that contains A, hence $\langle A \rangle \subset \bar{A}$. Moreover, since $\langle A \rangle$ is a subgroup of G that contains A, then $a_i^{\epsilon_i} \in \langle A \rangle$, hence their product is in $\langle A \rangle$ as well. That is, $\bar{A} \subset \langle A \rangle$, thus $\langle A \rangle = \bar{A}$. ■

Definition: Let $H, K \leq G$. The **join** of subgroups H and K denoted by $\langle H, K \rangle$ is the smallest subgroup which contains both subgroups.

Subgroups of a groups can be represented by a lattice such as below.

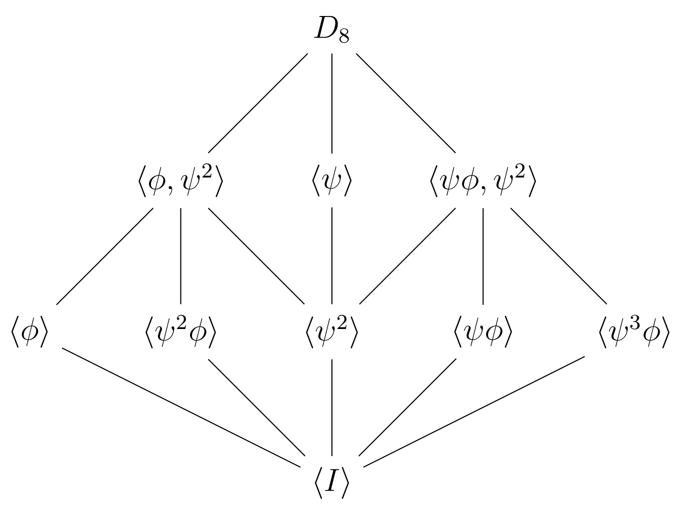

Figure 2.1: The subgroup lattice of D_8

Exercises

1. Suppose G is abelian group. Show that, the **torsion subgroup** $\{g \in G \,|\, \mathrm{ord}_G(g) < \infty\}$ is a subgroup of G. Also, show that this is not generally true when G is non-abelian.

2.3 A counting principle

Let H and K be two subgroups of G, then

$$HK = \{hk \,|\, h \in H, k \in K\}$$

Lemma 2.10. *HK is a subgroup of G if and only if $HK = KH$.*

Proof. Suppose HK is a subgroup. If $hk \in HK$, then

$$k^{-1}h^{-1} \in HK \implies k^{-1} \in H, h^{-1} \in K \implies k \in H, h \in K \implies hk \in KH$$

hence $HK \subset KH$. If $kh \in KH$, then

$$hk \in HK \implies k^{-1} \in H, h^{-1} \in K \implies k \in H, h \in K \implies kh \in HK$$

thus $HK = KH$. Suppose $HK = KH$ with $h_1k_1, h_2k_2 \in HK$.

1. for closure we have

$$h_1k_1h_2k_2 = h_1k_1(k_2'h_2') = h_1(k_1k_2')h_2' = h_1(k^*h_2') = h_1h_2''k^{*'}$$

2. for inverse

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1'k_1'$$

■

Corollary 2.11. *If H and K are subgroups of an abelian group G, then HK is a subgroup of G.*

Lemma 2.12. *If H and K are finite subgroups G, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. If $h_1 \in H \cap K$ then $hk = (hh_1)(h_1^{-1}k)$. Therefore, hk appears at least $|H \cap K|$ times. If $hk = h'k'$, then $h'^{-1}h = k'k^{-1} \in H \cap K$. Let $u = h'^{-1}h$ then $h' = hu^{-1}$ and $k' = uk$. Thus, all duplicates are accounted for. □

Corollary 2.13. *If H and K are subgroups of G and $|H|, |K| > \sqrt{|G|}$, then $H \cap K \neq \{e\}$.*

Proof. $HK \subset G$ therefore, $|HK| \leq |G|$ and

$$|G| \geq |HK| = \frac{|H||K|}{|H \cap K|} > \frac{|G|}{|H \cap K|}$$

which implies that $|H \cap K| > 1$. ■

Exercises

1. Let G be a group such that the intersection of all of its subgroups that are different from $\{e\}$ is different from $\{e\}$. Prove that every element in G has finite order.

Proof. For the sake of contradiction, suppose $a \in G$ has infinite order. Then, a^k are all different and

$$\bigcup_{k=1}^{\infty} \langle a^k \rangle = \{e\}$$

which is a contradiction. ■

2. Show that there is one-to-one correspondence between the right and left cosets of a subgroup.

3. Suppose H and K are finite index subgroups in G. Show that $H \cap K$ is a finite subgroup in G.

   Proof. Let $Ha_1, \ldots, Ha_n$ be the right cosets of H in G and $Kb_1, \ldots, Kb_m$ be the right costs of K in G. Then,

$$G = G \cap G = \bigcap_i Ha_i \cap \bigcap_j Kb_j = \bigcap_{i,j} Ha_i \cap Kb_j$$

   Suppose $Ha_i \cap Kb_j$ is not empty. Let $g \in Ha_i \cap Kb_j$, then $Hg = Ha_i$ and $Kg = Kb_j$. Thus,

$$Ha_i \cap Kb_j = Hg \cap Kg = (H \cap K)g$$

   Therefore, $Ha_i \cap Kb_j$ are either empty or a right coset of $H \cap K$. Since there finitely many $Ha_i \cap Kb_j$, there finitely many right cosets of $H \cap K$ in G. Moreover, $[G : H \cap K] \leq [G : H][G : K]$ by this construction. Note that, $H \cap K$ is finite index in H, and let $(H \cap K)c_1, \ldots, (H \cap K)c_l$ be the right cosets of $H \cap K$ in H. We claim that $(H \cap K)c_r a_i$ are the right cosets of $H \cap K$ in G. By definition, for each $x \in G$, there exists i such that $x \in Ha_i$and hence $x = ha_i$ for some $h \in H$. Similary, there exists r such that $h \in (H \cap K)c_r$ and hence $h = fc_r$ for some $f \in H \cap K$. Therefore, $x = fc_r a_i$ and $x \in (H \cap K)c_r a_i$. Lastly, we must show that $(H \cap K)c_r a_i$ are disjoint. Consider $(H \cap K)c_{r_1} a_{i_1}$ and $(H \cap K)c_{r_2} a_{i_2}$. Since $(H \cap K)c_{r_1}, (H \cap K)c_{r_2} \subset H$, then

$$\begin{aligned}(H \cap K)c_{r_1} a_{i_1} = (H \cap K)c_{r_2} a_{i_2} &\implies a_{i_1} = a_{i_2}, (H \cap K)c_{r_1} = (H \cap K)c_{r_2} \\ &\implies a_{i_1} = a_{i_2}, c_{r_1} = c_{r_2}\end{aligned}$$

   As a result, $[G : H \cap K] = [G : H][H : H \cap K]$. ■

4. Let H be a finite index subgroup in G. Show that there is only finitely many subgroups of form aHa^{-1} in G.

   Proof. Let $a_1H, \ldots, a_nH$ be left cosets of H. Then, $Ha_1^{-1}, \ldots, Ha_n^{-1}$ are right cosets of H. Suppose $aH = a_iH$, then $Ha^{-1} = Ha_i^{-1}$ and therefore, $aHa^{-1} = a_iHa_i^{-1}$. Since there are finitely many $a_iHa_i^{-1}$, then there are finitely many aHa^{-1}. ■

5. If an abelian group has subgroups of orders m and n, respectively, then show it has a subgroup whose order is the least common multiple of m and n.

6. Let G be a finite (abelian) group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n. Prove that G must be a cyclic group.

2.4 Normal subgroups

Definition: A subgroup N of G is **normal** if $\forall g \in G, n \in N,\ gng^{-1} \in N$.

Lemma 2.14. *N is normal if and only if $gNg^{-1} = N$ for every $g \in G$.*

Proof. By definition, $gNg^{-1} \subset N$. Let $n \in N$, then $g^{-1}ng = n'$ for some $n' \in N$. Hence, $n \in gNg^{-1}$ for all $n \in N$. □

Lemma 2.15. *N is a normal subgroup if and only if every left coset of N is a right coset.*

Proof. If N is normal, then by 2.14, $gN = Ng$ for all g. Suppose, for all $g \in G$, $gN = Nh$ for some $h \in G$. Then, $h = gn \implies gN = Ngn$ for $n \in N$. This implies, $gNn^{-1} = gN = Ng$ and therefore, $gNg^{-1} = N$ which by 2.14 means that N is normal. □

Lemma 2.16. *N is a normal subgroup if and only if the product of two right cosets of N is a right coset as well.*

Proof. If N is normal, then

$$NaNb = N(aN)b = N(Na)b = Nab$$

Then, suppose $NaNb = Nc$ for all $a, b \in G$ and some $c \in G$. This implies $NaNb = Nab$ and therefore, $NaNa^{-1} = N \implies NaN = Na$.

$$\begin{aligned} NaN = Na &\implies \forall n, an \in Na \implies aN \subset Na \\ Na^{-1}N = Na^{-1} &\implies \forall n \exists n', a^{-1}n = n'a^{-1} \implies na = an' \implies Na \subset aN \end{aligned}$$

therefore, $aN = Na$. □

Definition: G/N is called a **quotient group** is the set of all right cosets of N.

Theorem 2.17. *If N is normal in G, then G/N is a group. Furthermore, for finite G, $|G/N| = \frac{|G|}{|N|}$.*

Proof. Checking axioms is pretty easy. Note that, $|G/N| = i_G(N)$. ■

Exercises

1. The groups in which all subgroups are normal are called **Dedekind groups**. Non-abelian dedekind groups are called **Hamiltonian groups**. Show that quaternion group is a Hamiltonian group.

2. Show that if K is a normal subgroup of N and N is a normal subgroup of G, then K is not necessarily a subgroup of G.

2.5 Homomorphism

Definition: A mapping ϕ from a group G to another group $\bar{G}$ is a **homomorphism** if for all $a, b \in G$

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

Lemma 2.18. *Suppose G is a group, N a normal subgroup of G, $\phi : G \to G/N$ given by $\phi(x) = Nx$ for all $x \in G$. Then, ϕ is a homomorphism.*

Proof. Note that $\phi(xy) = Nxy$ and $\phi(x)\phi(y) = NxNy = Nxy$. □

Definition: If ϕ is a homomorphism of G into $\bar{G}$, the **kernel** of ϕ, K_ϕ is defined as $K_\phi = \{x \in G \,|\, \phi(x) = \bar{e}\}$.

Lemma 2.19. *If $\phi : G \to \bar{G}$ is a homomorphism, then*

1. $\phi(e) = \bar{e}$.
2. $\phi(x^{-1}) = (\phi(x))^{-1}$.

Proof.

$$\phi(xe) = \phi(x) = \phi(x)\phi(e) \implies \phi(e) = \bar{e}$$

and

$$\phi\big(x^{-1}\big)\phi(x) = \phi\big(x^{-1}x\big) = \bar{e} \implies \phi\big(x^{-1}\big) = (\phi(x))^{-1}$$

□

Lemma 2.20. *If ϕ is a homomorphism, then K_ϕ is a normal subgroup of G.*

Proof. Pick an arbitray $x \in G$ and $y \in K_\phi$. Then,

$$\phi\big(xyx^{-1}\big) = \phi(x)\phi(y)\phi\big(x^{-1}\big) = \bar{e}$$

hence, $xyx^{-1} \in K_\phi$. □

Lemma 2.21. *If ϕ is a homomorphism, then the set all iverse images of $\bar{g} \in \bar{G}$ under ϕ is given by $K_\phi x$ for any particular inverse image of $\bar{g}$.*

Proof. Suppose y is another inverse image of $\bar{g}$.

$$\begin{aligned} &\phi(y) = \bar{g} && \phi(x) = \bar{g} \\ &\implies \phi\big(yx^{-1}\big) = \bar{e} && \implies yx^{-1} \in K_\phi \end{aligned}$$

which means $y \in K_\phi x$. Also, clearly each $y \in K_\phi x$ is an inverse image of $\bar{g}$. □

Definition: A homomorphism $\phi : G \to \bar{G}$ is an **isomorphism** if ϕ is <u>one-to-one</u>.

Definition: Two groups G and $\bar{G}$ are **isomorphic** if there exists an isomorphism of G <u>onto</u> $\bar{G}$. Isomorphic groups are denoted by $G \approx \bar{G}$.

Corollary 2.22. *Let ϕ be a homomorphism. Then, ϕ is an isomorphism if and only if $K_\phi = \{e\}$.*

Proof. If ϕ is an isomorphism, then it is injective and hence only $e \in K_\phi$. Suppose $K_\phi = \{e\}$, then we must show that ϕ is a injective function. Suppose $\phi(x) = \phi(y)$, then by 2.21, $yx^{-1} \in K_\phi$. Thus, $y = x$ and ϕ is injective. □

Theorem 2.23. *If $\phi : G \to \bar{G}$ is a surjective homomorphism, then $G/K_\phi \approx \bar{G}$*

Proof. Consider the following mapping, $\psi : G/K_\phi \to \bar{G}$. For any $X \in K/\phi$, $\psi(X) = \phi(g)$ for some $g \in X$. This is well-defined since if $g, g' \in X$, then $g' = xg$ for some $x \in K_\phi$ and hence

$$\phi(g') = \phi(g)\phi(x) = \phi(g)$$

Furthermore, ψ is injective. Suppose $xK_\phi, yK_\phi \in G/K_\phi$. Then,

$$\psi(xK_\phi) = \psi(yK_\phi) \implies \phi(x) = \phi(y) \implies xy^{-1} \in K_\phi$$

which implies that $x \in K_\phi y$ and hence $K_\phi y = K_\phi x$. Moreover, this map is surjective. Let $\bar{g} \in \bar{G}$. Since ϕ is surjective, then there exists an inverse image g. Therefore, $\psi(gK_\phi) = \bar{g}$. Finally, we must show that ψ is a homomorphism. Since K_ϕ is normal in G we have

$$\psi(xK_\phi yK_\phi) = \psi(xyK_\phi) = \phi(xy) = \phi(x)\phi(y) = \psi(xK_\phi)\psi(yK_\phi)$$

which concludes the proof. □

Thus, we can find all homomorphic images of G by going through normal subgroups of G.

Definition: A group is **simple** if it has no non-trivial homomorphic images. i.e. it has no non-trivial normal subgroup.

Theorem 2.24 (Cauchy's theorem for finite abelian groups). *Suoppose G is a finite abelian group, and $p \mid |G|$ where p is a prime number. Then, there is an element $a \neq e$ such that $a^p = e$.*

Proof. We induct over $|G|$. For G with a single element, the theorem is true trivially. If G has non-trivial subgroup H, then G is cyclic and hence all its elements satisfy the condition. Suppose H is a non-trivial group of G. Since G is abelian, then H is normal in G. If $p \mid |H|$ then by induction we are done. Suppose otherwise, then $p \mid |G/H|$. Consder a set S where each element correspond to a right coset of H. Clearly, there is a isomorphism between G/H and S. Since S is a subgroup of G and $p \mid |S|$ by induction hypothesis we are done. ■

Theorem 2.25 (Sylow's theorem for finite abelian groups). *Suppose the group G is a finite abelian group and $p^\alpha \mid\mid |G|$, then G has a unique subgroup of order p^α.*

Proof. We first prove the existence of such group. For $\alpha = 0$, the claim holds trivially as $\{e\}$ is a subgroup of order 1. . Suppose $H = \left\{x \in G \,\middle|\, x^{p^n} = e\right\}$ is a subgroup of G. Since $p \mid |G|$ there is a non identity element g such that $g^p = e$. Hence $g \in H$. We show that $q \not| |H|$ for any other prime $q \neq p$. Since otherwise there is a an element $h \in H$ where $h \neq e$ and $h^q = e$ by 2.24. Since q and p^n are coprime, then $h = e$ which is a contradiction. Lastly, we claim that $p^\alpha \mid\mid |H|$. Suppose the contrary that $p^\beta \mid\mid |H|$ for some $\beta < \alpha$. Then, the quotient group of H, $p \mid |G/H|$. By 2.24, there is a right coset $Hx \neq H$ such that $(Hx)^p = Hx^p = H$. This implies that $x^p \in H$ which means $(x^p)^{p^n} = e$ for some n. $x^{p^{n+1}} = e \implies x \in H$. which is a contradtion. Thus, $|H| = p^\alpha$.

Finally, suppose $K \neq H$ is another subgroup of G such that $|K| = p^\alpha$. Then, note that

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^{2\alpha}}{|H \cap K|} \implies p^\gamma \mid\mid |HK|$$

However, this is a contradiction since HK is a subgroup in G. Therefore H is unique in G.■

Lemma 2.26. *Suppose $\phi : G \to \bar{G}$ is a surjective homomorphism and $\bar{H}$ is a subgroup of $\bar{G}$. Let $H = \{x \in G \,|\, \phi(x) \in \bar{H}\}$. Then, H is a subgroup of G and $H \supset K_\phi$. If $\bar{H}$ is normal in $\bar{G}$, then H is normal. Moreover, this association sets up a one-to-one mapping from the set of all subgroups $\bar{G}$ onto the set of all subgroups of G which contain K_ϕ.*

Proof. Since $\bar{e} \in \bar{H}$, then $K_\phi \subset H$. Let $x, y \in H$. $xy \in H$ since $\phi(xy) = \phi(x)\phi(y) \in \bar{H}$ and $x^{-1} \in H$ since $\phi(x^{-1}) = (\phi(x))^{-1} \in \bar{H}$. Thus, H is a subgroup in G. Assume that $\bar{H}$ is normal and pick arbitray elements $g \in G$ and $h \in H$.

$$\phi\big(ghg^{-1}\big) = \phi(g)\phi(h)(\phi(g))^{-1} \in \bar{H} \implies ghg^{-1} \in H$$

hence H is normal in G. Let $\bar{H}, \bar{H}'$ be two subgroups of $\bar{G}$ and $H = \phi^{-1}\big(\bar{H}\big), H' = \phi^{-1}\big(\bar{H}'\big)$. Thus far we have proved that $H, H' \supset K_\phi$ are subgroups of G and ϕ^{-1} is surjective. If $\bar{H} \neq \bar{H}'$, then there is an element $x \in \bar{H}$ but $x \notin \bar{H}'$. We should see that for any $y = \phi^{-1}(x)$, $y \subset H$ but $y \notin H'$. Since $\phi(y) = x \in \bar{H}$, then $y \in H$. If $y \in H'$, then $\phi(y) = x \in \bar{H}'$ which is a contradiction. Therefore, ϕ^{-1} is a injective as well. So ϕ^{-1} is a bijection between the subgroups of $\bar{G}$ and subgroups of G that contain K_ϕ. □

Theorem 2.27. *Let $\phi : G \to \bar{G}$ be a surjective homomorphism, $\bar{N}$ a normal subgroup of $\bar{G}$, and $N = \{x \in G \,|\, \phi(x) \in N\}$. Then, $G/N \approx \bar{G}/\bar{N}$ and equivalently $G/N \approx (G/K_\phi)/(N/K_\phi)$.*

Proof. The last equivalency results immediately from 2.23. ■

Exercises

1. Let U be a subset of a group G. The subgroup generated by U, denoted by $\langle U \rangle$ is the smallest subgroup that contains U. Show that $\langle U \rangle$ exists and give a construction for it.

2. Let $U = \{xyx^{-1}y^{-1} \,|\, x, y \in G\}$. In this case,$\langle U \rangle$ is usually written as $\hat{G}$ and is called the **commutator subgroup** of G.

   (a) Prove $\hat{G}$ is normal in G.

   (b) Prove $G/\hat{G}$ is abelian.

   (c) If G/N is abelian, prove that $N \supset \hat{G}$.

   (d) Prove that if H is a subgroup of G and $H \supset \hat{G}$, then H is normal in G.

   (e) Let $G = \mathrm{GL}_2(\mathbb{R})$ and $N = \mathrm{SL}_2(\mathbb{R})$. Show that $N = \hat{G}$.

3. Show that $Q_8 \approx \mathrm{GL}_2(\mathbb{C})$.

2.6 Cyclic groups

We claim that cyclic groups of the same order are isomorphic. To show this, first consider the following proposition.

Proposition 2.28. *1. If $G = \langle g \rangle$, then $|G| = \mathrm{ord}_G(g)$.*

2. If $x \in G$ and $x^m = x^n = e$, then $x^{\gcd(m,n)} = e$.

Theorem 2.29. *Cyclic groups of the same order are isomorphic.*

Given the above theorem, we let Z_n denotes the cyclic group of order n, which is unique upto isomorphism.

Proposition 2.30. *Let $G = \langle g \rangle$.*

1. *If $\operatorname{ord}_G(g) = \infty$, then $G = \langle g^a \rangle$ if and only if $a = \pm 1$.*
2. *If $\operatorname{ord}_G(g) = n < \infty$, then $G = \langle g^a \rangle$ if and only if $\gcd(n, a) = 1$. Hence, G has $\phi(n)$ generators.*

Proposition 2.31. *Let $G = \langle g \rangle$. All subgroups of G are cyclic. That is, if $H \leq G$, then $H = \langle g^d \rangle$ for some $d \in \mathbb{Z}$.*

1. *If $\operatorname{ord}_G(g) = \infty$, then for all $a, b \in \mathbb{Z}_0^+$ with $a \neq b$, $\langle g^a \rangle \neq \langle g^b \rangle$. Moreover, for $m \in \mathbb{Z}$, $\langle g^m \rangle = \langle g^{|m|} \rangle$. This implies, that all subgroups of G correspond bijectively with $\mathbb{Z}_0^+$.*
2. *If $\operatorname{ord}_G(g) = n < \infty$, then for all $a \mid n$, $\langle g^a \rangle$ is a subgroup and for all m, $\langle g^m \rangle = \langle g^{\gcd(m,n)} \rangle$. This implies, that all subgroups of G correspond bijectively to divisors of n.*

2.7 Automorphism

Definition: An isomorphism of a group onto iteslf is called an **automorphism**.

Lemma 2.32. *If G is a group, then $\mathscr{A}(G)$, the set of all automorphisms of G is also a group. The $\mathscr{A}(G)$ is also denoted by $\operatorname{Aut}(G)$.*

Proof. The $\operatorname{Aut}(G)$ is a group under composition. Suppose $\theta, \phi, \psi \in \operatorname{Aut}(G)$.

1. It is closed under composition. Since ϕ, θ are both bijective, then their composition is a bijection as well. Moreover, it is a homomorphisms
$$\phi(\psi(xy)) = \phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\psi(y))$$
therefore, $\phi \circ \psi \in \operatorname{Aut}(G)$.
2. The identity is the identity transformation I.
$$I \circ \phi = \phi \circ I = \phi$$
3. the inverse of each automorphisms is its inverse map. Suppose ϕ^{-1} is inverse of ϕ
$$xy = \phi\big(\phi^{-1}(x)\big)\phi\big(\phi^{-1}(y)\big) = \phi\big(\phi^{-1}(x)\phi^{-1}(x)\big) \implies \phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$$
4. composition is associative
$$\phi \circ (\psi \circ \theta) = (\phi \circ \psi) \circ \theta$$

for any maps ϕ, ψ, θ from G to G. □

Example 2.8. $T_g : G \to G$ with $xT_g = g^{-1}xg$. T_g is an automorphisms. T_g is called the **inner automorphism corresponding to** g. Let $\mathscr{T}(G) = \{T_g \in \operatorname{Aut}(G) \mid g \in G\}$ is the **inner automorphism group** and is also denoted by $\operatorname{Inn}(G)$. $\Psi : G \to \operatorname{Aut}(G)$ given by $g\Psi = T_g$ is a homomorphism. The kernel of Ψ is the **center** of G, $Z(G)$, the set of the elements that commute with all other elements. Note that, if $g_o \in K_\Psi$, then $T_{g_0} = I$, hence $g_0^{-1}xg_0 = x$ implying $g_0x = xg_0$ for all $x \in G$. If $g_0 \in Z(G)$, then $xg_0 = g_0x$ for all x, thus $T_{g_0} = I$ and $g_0 \in K_\Psi$.

Lemma 2.33. $G/Z \approx \mathrm{Inn}(G)$.

Proof. Since $K_\psi = Z$, this is an immediate result of 2.23, by considering $\Psi : G \to \mathrm{Inn}(G)$. □

Lemma 2.34. *Let G be a group and ϕ be an automorphism of G. If $a \in G$ is of order $|a| > 0$, then $|\phi(a)| = |a|$.*

Proof. For any homomorphism $\phi : G \to \bar{G}$, $|\phi(a)| \mid |a|$ since

$$\phi(a)^{|a|} = \phi\big(a^{|a|}\big) = \phi(e) = \bar{e}$$

since both ϕ and ϕ^{-1} are homomorphism from G to G, then

$$\begin{aligned} &|\phi(a)| \mid |a| \\ &\big|\phi^{-1}(\phi(a))\big| = |a| \mid |\phi(a)| \\ \implies &|\phi(a)| = |a| \end{aligned}$$

□

Exercises

1. A subgroup C of G is said to be a **characteristics subgroup** of G if $CT \subset C$ for all automorphisms T of G. For any group G, prove that the commutator subgroup $\hat{G}$ is a characteristic subgroup of G.

2. Let G be a finite group, T an automorphism of G with property that $xT = x$ if and only if $x = e$. Suppose futher that $T^2 = I$. Prove that G must be abelian.

3. Let G be a finite group, T an automorphism of G that sends more than three-quarters of the elements of G onto their inverses. Prove that $xT = x^{-1}$ and that G is abelian.

4. Let G be a group of order $2n$. Suppose that half of the elements of G are of order 2, and the other half form a subgroup H of order n. Prove that H is of odd order and is an abelian subgroup of G.

2.8 Group Action

Definition: The **action** of a group G on a set A is a map $\cdot : G \times A \to A$ which satisfies:

1. $g \cdot (h \cdot a) = (gh) \cdot a$ for all $g, h \in G$ and $a \in A$.

2. $e \cdot a = a$ for all $a \in A$.

Suppose $\cdot$ is an action of G on A. Then, $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$ is a permutation of A. Furthermore, $\tau : G \to S_A$, $g \mapsto \sigma_g$ is a homomorphism.

Example 2.9. The **trivial action** is given by $g \cdot a = a$ for all $g \in G$ and $a \in A$. In contrast, in a **faithful action** of G on A, no $g \neq e$ satisfies $g \cdot a = a$ for all A. In other words, in a faithful action, each element of G produces a different permutation. Thus τ is an injective homomorphism.

Unless it is ambiguous, we omit the $\cdot$, and write $g \cdot a$ as ga.

Definition: The **kernel** of an action is $\{g \in G \,|\, ga = a \; \forall a \in A\}$.

Definition: The **stabilizer** of a is $\{g \in G \,|\, ga = a\}$.

2.9 Cayley's theorem

Theorem 2.35 (Cayley). *Every group is isomorphic to a subgroup of $A(S)$ for some set S.*

Proof. Take $S = G$ and let $\tau_g : S \to S$ be given by $\tau_g : x \mapsto xg$ for a $g \in G$. We claim that $\theta : G \to A(S)$ given by $\theta : g \mapsto \tau_g$ is an isomorphism. First, we must show that θ is well defined. That is, for all $g \in G$, $\tau_g \in A(S)$. Note that, if $xg = yg$, then $x = y$, hence τ_g is injective. For every $y \in G$, $y = yg^{-1}\tau_g$, hence τ_g is surjective. Thus, $\tau_g \in A(S)$. Second, we show that θ is a homomorphism. For all $g, h, x \in G$, $x(gh) = (xg)h$ therefore, $\tau_{gh} = \tau_g\tau_h$. Finally, to show that θ is an isomorphism, we must show that it is injective. If for all $x \in G$, $x\tau_g = x\tau_h$, then $g = h$. Which was what was wanted. ■

The construction above, describes a group G as a subgroup of $A(G)$ that for finite G, is of order $|G|!$. Too BIG. We wish to make it smaller. Consider the following results.

Theorem 2.36. *If G is a group, H a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism $\theta : G \to A(S)$ and the kernel of θ is the largest normal subgroup of G which is contained in H.*

Proof. Let $\tau_g : S \to S$ be given by $Hx\tau_g = Hxg$ and then let $\theta : G \to A(S)$ be given by $\theta : g \mapsto \tau_g$. One can easily check that, $\tau_g \in A(S)$ for all g and that θ is a homomorphism. Suppose K is the kernel of θ. Since K is a kernel of a homomorphism, it is normal. Moreover, if $g \in K$, then $Hxg = Hx$ for all $x \in G$. In particular, $Hg = H$ which implies that $g \in H$. As a result, $K \subset H$. Lastly, suppose K' is another normal subgroup of G which is contained in H. If $g' \in K'$, then for all $x \in G$, $xg'x^{-1} \in K' \subset H'$. That is, there exists a $h_x \in H$ such that $xg' = hx$ which implies $Hxg' = Hx$ for all x. Therefore, $g' \in K$ and $K' \subset K$. Which was what was wanted. ■

Given the above theorem, if H has no non-trivial normal subgroup of G inside it, then θ is an isomorphism.

Lemma 2.37. *If G is a finite group, and $H \neq G$ is a subgroup of G such that $|G| \nmid i(H)!$, then H must contain a non-trivial normal subgroup of G. In particular, G is not simple.*

Proof. Suppose H contains no non-trivial normal subgroup of G. Then, by preceding theorem, θ is an isomorphism and G is isomorphic to a subgroup of $A(S)$, where $A(S) = i(H)!$. By Lagrange, theorem, $|G| \mid i(H)!$ which was what was wanted. ■

Exercises

1. Let $|G| = pq$, $p > q$ are primes, prove
   (a) G has a subgroup of order p and a subgroup of order q.
   (b) If $q \nmid p - 1$, then G is cyclic.
   (c) Given two primes, p and q with $q \mid p - 1$, there exists a non-abelian group of order pq.
   (d) Any two non-abelian groups of order pq are isomorphic.

2.10 Permutation group

Suppose S is a finite set having n elements $x_1, \ldots, x_n$. If $\phi \in A(S)$, then ϕ is a one-to-one correspondence and it can be represented as

$$\phi : \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}$$

where $x_{i_j} = \phi(x_j)$. More simply

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

By considering composition of $\theta, \psi \in A(S)$, we can define multiplication on their representation.

For $\theta \in A(S)$ and $a, b \in S$, $a \overset{\theta}{\equiv} b \iff a = b\theta^i$ for some $i \in \mathbb{Z}$. This defines an equivalence relation.

1. $a \overset{\theta}{\equiv} a$ for all a, since $a = a\theta^0$.
2. $a \overset{\theta}{\equiv} b$ implies $b \overset{\theta}{\equiv} a$, since $a = b\theta^i \implies b = a\theta^{-1}$.
3. $a \overset{\theta}{\equiv} b$ and $b \overset{\theta}{\equiv} c$ implies $a \overset{\theta}{\equiv} c$, since $a = b\theta^i$ and $b = c\theta^j$ implies $a = c\theta^{i+j}$.

We call the equivalence classes of $s \in S$, the **orbit** of s under θ. The orbit of s consists of all elements in form of $s\theta^i$, $i \in \mathbb{Z}$. If S is finite, then there is a smallest positive integer $l = l(s)$ such that $s\theta^l = s$. By **cycle** of θ we mean the ordered set $(s, s\theta, \ldots, s\theta^{l-1})$.

Lemma 2.38. *Every permutation is a product of its cycles.*

Proof. Note that the cycles of a permutation are disjoint, and each is a permutation, hence their product is a permutation. Suppose ψ is the permutation of the product of cycles of θ. ψ is well-defined since the product of disjoint permutation is commutative. Futhermore, for each $s \in S$, $s\psi = \theta s$ thus, $\theta = \psi$. ☐

Lemma 2.39. *Every cycle can be written as a product of 2-cycle or **transpositions**.*

Proof. Every m-cycle can be written as a product of 2-cycles.

$$\begin{pmatrix} 1 & 2 & \ldots & m \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \ldots \begin{pmatrix} m-1 & m \end{pmatrix}$$ ☐

Definition: A permutation $\theta \in S_n$ is said to be an **even permutation** if it can be represented as a product of an even number of transpositions,

The proof of well-definition of even permutation involves the polynomial $p(x_1, \ldots, x_n)$

$$p(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)$$

Define the action of $\theta \in A(S_n)$ on the polynomial p

$$\theta \cdot p = \prod_{i<j} (x_{\theta(i)} - x_{\theta(j)})$$

It can be easily seen that $\theta \cdot p = \pm p$. In fact, if θ is a transposition, then $\theta \cdot p = -p$. Since this is an action on p, if θ is the product of m transposition, $\theta \cdot p = (-1)^m p$. Therefore, even permutations are well-defined. That is, no permutation can be written as a product of even number of transpositions and odd number of transpositions simultaneously.

Let $A_n \subset S_n$ be the set of even permutations. A_n is a subgroup of S_n and it is called the **alternating group**.

Lemma 2.40. *The alternating group is a normal subgroup of S_n of index 2, .*

Proof. A way to prove this lemma, is to show that every odd permutation is in one coset of A_n.

Another way, is to show that $\Psi : S_n \to W$ given by

$$\theta\Psi = \begin{cases} 1 & \theta \text{ is even} \\ -1 & \theta \text{ is odd} \end{cases}$$

is an onto homomorphism. W is the group of $\{1, -1\}$ under multiplication. Then A_n is the kernel of Ψ. Since $S_n/A_n \approx W$, then

$$\frac{|S_n|}{|A_n|} = |W| = 2$$

Which was what was wanted. □

Exercises

1. (a) What is the order of an n-cycle.
   (b) What is the order of the product of disjoint cycles of length $m_1, m_2, \ldots, m_k$.
   (c) How do you find the order of a given permutation?
2. Prove that A_5 has no non-trivial normal subgroups.
3. If $n \geq 5$ prove that A_n is the only non-trivial normal subgroup in S_n.

2.11 Another counting principle

Definition: If $a, b \in G$, then b is said to be a **conjugate** of a in G, denoted by $a \sim b$, if there exists an element $c \in G$ such that $b = c^{-1}ac$

Lemma 2.41. *Conjugacy is an equivalence relation on G.*

Proof.
1. $a \sim a$ for all $a \in G$, $a = e^{-1}ae$.
2. $a \sim b \implies b \sim a$ for all $a, b \in G$, since $a = c^{-1}bc$ implies that $b = cac^{-1}$.
3. $a \sim b, b \sim c \implies a \sim c$ for all $a, b, c \in G$, since $a = d^{-1}bd = d^{-1}e^{-1}ced = (ed)^{-1}c(ed)$.
   □

For $a \in G$ let $C(a) = \{x \in G \,|\, x \sim a\}$. $C(a)$ is called the **conjugate class** of a in G. It consists all elements in form of $y^{-1}ay$ for $y \in G$. Suppose G is a finite group and A is a set of representative of conjugacy classes. Then,

$$|G| = \sum_{a \in A} |C(a)|$$

Definition: Suppose $a \in G$. The **normalizer** of a in G, denoted by $N(a)$, is the set of all elements that commute with a, $N(a) = \{x \in G \,|\, ax = xa\}$.

Lemma 2.42. *$N(a)$ is a subgroup of G.*

Proof. Suppose $x, y \in N(a)$, then $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$. And $x^{-1}a = ax^{-1}$ holds. Therefore, $N(a)$ is a subgroup of G. □

Theorem 2.43. *If G is a finite group, then $|C(a)| = i_G(N(a))$. i.e. the number of elements conjugate to a in G is the index of normalized of a in G.*

Proof. Let S be the set of right cosets of $N(a)$ in G. Consider $\varphi : S \to C(a)$ given by $\varphi : N(a)g \mapsto g^{-1}ag$. This, function is well-defined since if $N(a)g = N(a)h$, then $g = nh$ for some $n \in N(a)$. Then, $g^{-1}ag = h^{-1}n^{-1}anh = h^{-1}ah$. Similary, it is injective. If $N(a)g\varphi = N(a)h\varphi$, then $g^{-1}ag = h^{-1}ah \implies a = (gh^{-1})a(hg^{-1}) \implies hg^{-1} \in N(a)$ hence $N(a)g = N(a)h$. φ is clearly surjective. Suppose $x \in C(a)$, then there exists $g \in G$ such that $x = g^{-1}ag$. Then, $N(a)g\varphi = g^{-1}ag = x$. Therefore, φ is a bijection and $|C(a)| = i_G(N(a))$.■

Corollary 2.44. *The class equation of G*

$$|G| = \sum_{a \in A} \frac{|G|}{|N(a)|}$$

Recall that the center $Z(G)$ of a group G is the set of all $a \in G$ such that $ax = xa$ for all $x \in G$.

Lemma 2.45. *$a \in Z(G)$ if and only if $N(a) = G$. If G is finite, $a \in Z(G)$ if and only if $|N(a)| = |G|$.*

Proof. It can be readily proven by applying the definitions. □

2.11.1 Applications of 2.43

Theorem 2.46. *If $|G| = p^n$ where p is a prime number, then $Z(G) \neq \{e\}$.*

Proof. Let $z = |Z(G)|$. For each $a \in Z(G)$, $|C(a)| = 1$. For each $b \notin Z(G)$, $N(a) \neq G$, hence $|N(a)| = p^k$ for some $0 < k < n$. Therefore, $|C(a)| = p^{n-k}$ with $n - k \geq 1$. Hence,

$$\begin{aligned} p^n &= \sum_{a \in A} |C(a)| \\ &= \sum_{A \cap Z(G)} |C(a)| + \sum_{A \cap (Z(G))^c} |C(a)| \\ &= z + \sum_{A \cap (Z(G))^c} |C(a)| \end{aligned}$$

We have shown that, for $a \notin Z(G)$, then $p \mid |C(a)|$, thus $p \mid z$. Since $e \in Z(G)$, then $Z(G)$ contains at least p elements. ■

Corollary 2.47. *If $|G| = p^2$ where p is a prime number, then G is abelian.*

Proof. Based on the proof last theorem, $|Z(G)| = p, p^2$. Suppose $|Z(G)| = p$ and $a \notin Z(G)$. Then, $Z(G) \subsetneq N(a)$. By Lagrange's theorem, $|N(a)| \mid |G|$, thus $|N(a)| = p^2$ which means $a \in Z(G)$, a contradiction. Therefore, $|Z(G)| = p^2$ and G is abelian. ■

Theorem 2.48 (Cauchy). *If p is a prime number and $p \mid |G|$, then G has an element of order p.*

Proof. If $|G| = p$, then G is cyclic and the theorem holds. Suppose, the statement is true for all groups with $|G| = pk$ for $1 \leq k \leq n-1$, we will show that it is also true for $|G| = np$. That is, we will prove the theorem by induction. If G has a non-trivial subset H where $p \mid |H|$, then we would be done. Suppose, that p divides the order of no non-trivial subgroup of H. Consider the normalizer subgroups, $N(a)$. If a normalizer subgroup is trivial, then $N(a) = G$ and hence $a \in Z(G)$. If it is not trivial, then its index divides p.

$$p^n = z + \sum_{A \cap (Z(G))^c} |C(a)| \implies p \mid z$$

That is $p \mid |Z(G)|$. Therefore, $Z(G) = G$ which means G is abelian. By Cauchy's theorem for abelian groups, there exists $a \neq e$ such that $a^p = e$. ■

Recall that every permutation in S_n can be decomposed into disjoint cycles. We shall say a permutation $\sigma \in S_n$ has the **cycle decomposition** $\{n_1, \ldots, n_r\}$ if it can be written as product of disjoint cycles of length $n_1, \ldots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$.

Lemma 2.49. *Two permutations in S_n are conjugate if and only if they have the same cycle decomposition.*

Proof. Conjugation in S_n leaves the cyclic decomposition unchanged. Also, for any two permutations with the same cyclic decomposition, we can find a $\theta \in S_n$ such that $\sigma_1 = \theta^{-1}\sigma_2\theta$. □

Corollary 2.50. *The number of conjugate classes in S_n is $p(n)$, the number of partitions of n.*

Proof. Every conjugate class corresponds to a partition of n. □

Exercises

1.

2.12 Centralizers and Normalizers

Definition: Let A be a non-empty subset of G. $C_G(A) = \{g \in G \mid gag^{-1} = a \;\forall a \in A\}$ is called the **centralizer** of A in G. $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ is the **normalizer** of A in G.

Example 2.10. $Z(G) = C_G(G)$.

Proposition 2.51. *For all $A \subset G$, $C_G(A)$ and $N_G(A)$ are subgroups of G and*

$$C_G(A) \leq N_G(A) \leq G$$

Proposition 2.52. $C_G(Z(G)) = G$.

Proposition 2.53. *If $A \subset B$, then $C_G(B) \leq C_G(A)$.*

Proposition 2.54. *If $H \leq G$, then $H \leq N_G(H)$ and $H \leq C_G(H)$ if and only if H is abelian. Furthermore, $N_H(A) = N_G(A) \cap H$ and $N_H(A) \leq H$.*

Proposition 2.55. *If $A \subset G$, then $N_G(A) \geq Z(G)$.*

Proposition 2.56. *$Z(H(\mathbb{F})) \approx \mathbb{F}$, the additive group of the field $\mathbb{F}$.*

2.13 Sylow's theorem

Theorem 2.57 (Sylow). *If p is a prime number and $p^\alpha \mid |G|$, then G has a subgroup of order p^α.*

We give three proofs for this theorem.

Proof. Let $|G| = p^\alpha m$ where $p^r \mid\mid m$ for some $r \geq 0$. Consider $\mathcal{M}$, the set of all p^α-element subsets of G. Clearly, $|\mathcal{M}| = \binom{p^\alpha m}{p^\alpha}$. Let $e_p(n)$ be $p^{e_p(n)} \mid\mid n$. We claim that $p^r \mid\mid |\mathcal{M}|$. Note that

$$e_p(|\mathcal{M}|) = e_p((p^\alpha m)!) - e_p((p^\alpha)!) - e_p((p^\alpha(m-1))!)$$

For any m and α

$$e_p((p^\alpha m)!) = m e_p((p^\alpha)!) + e_p(m!)$$

therefore,

$$\begin{aligned} e_p(|\mathcal{M}|) &= e_p((p^\alpha m)!) - e_p((p^\alpha)!) - e_p((p^\alpha(m-1))!) \\ &= e_p(m!) - e_p((m-1)!) \\ &= e_p\left(\frac{m!}{(m-1)!}\right) \\ &= e_p(m) \end{aligned}$$

which proves the claim. Define the equivalence relation $\sim$ on $\mathcal{M}$ as following. $M_1, M_2 \in \mathcal{M}$ are equivalent if there exists a $g \in G$ such that $M_1 = M_2 g$. There is at least one equivalence class that the number of elements in that class does not divide p^{r+1}. As otherwise, $p^{r+1} \mid |\mathcal{M}|$ which is a contradiction. Suppose $\{M_1, \ldots, M_n\}$ where $p^{r+1} \nmid n$ is that equivalence class. Let $H = \{g \in G \mid M_1 g = M_1\}$. It can be easily shown that H is a subgroup of G. We will show that $i_G(H) = n$. Let $\phi : Hg \mapsto M_1 g$

- ϕ is well-defined. Let $Hg_1 = Hg_2$, then $g_2 = hg_1$ where $h \in H$. Hence

$$M_1 g_2 = M_1 h g_1 = M_1 g_1$$

- ϕ is injective. Suppose $M_1 g_1 = M_1 g_2$, then $M_1 g_1 g_2^{-1} = M_2$ thus $g_1 g_2^{-1} \in H \implies Hg_1 = Hg_2$.

- ϕ is clearly surjective.

Note that $\{M_1 g \,|\, g \in G\} = \{M_1, \ldots, M_n\}$ by definition. Then, $i_G(H) = n$. which implies $p^\alpha \mid |H|$. For each $m_1 \in M_1$, $m_1 H_1 \subset M_1$, therefore, H has at most p^α distinct elements. Thus $|H| = p^\alpha$. ■

Corollary 2.58. *If $p^m \mid |G|$, $p^{m+1} \nmid |G|$, then G has a subgroup of order p^m.*

The second proof is by induction.

Proof. For $|G| = 2$, the only prime divisor is 2 and G itself is a subgroup of G with order 2. Suppose for all groups with order less than $|G|$, the theorem holds and suppose $p^\alpha \mid |G|$. If G has a non-trivial subgroup H where $p^\alpha \mid |H|$, then by induction hypothesis there exists a subgroup T of H with p^α elements. We are done, since T is a subgroup of G as well. Suppose, G does not have a non-trivial subgroup whose order is divisible by p^α. Consider the normalizer groups $N(a)$. If $N(a) = G$, then $a \in Z(G)$. Otherwise, $p^\alpha \nmid |N(a)|$, hence $p \mid i_G(N(a))$. By class equation, 2.44,

$$|G| = |Z(G)| + \sum_{A \cap (Z(G))^c} i_G(N(a))$$

which implies that $p \mid |Z(G)|$. By Cauchy's theorem, there exists an element $b \in Z(G)$ with order p. Let $B = \langle b \rangle$. Since $B \subset Z(G)$ it commutes with all elements of G and hence it is a normal subgroup. Let $\bar{G} = G/B$, then $\left|\bar{G}\right| = |G|/|B| = |G|/p$. Therefore, $p^{\alpha-1} \mid \left|\bar{G}\right|$ and by the induction hypothesis, there exists a subgroup $\bar{P}$ with order of p^α. Let $P = \left\{x \in G \,\middle|\, Bx \in \bar{P}\right\}$, then P/B is isomorphic to $\bar{P}$ and hence $|P| = \left|\bar{P}\right||B| = p^\alpha$. Which was what was wanted. ■

A subgroup of G of order p^m where $p^m \,||\, |G|$ is called a p-**Sylow group**.

For the third proof of Sylow's theorem, consider the following lemmas.

Lemma 2.59. *S_{p^k} has a p-Sylow group.*

Proof. For $k = 1$, the order of p-Sylow group is p. Therefore, $H = \left\langle \begin{pmatrix} 1 & 2 & \ldots & p \end{pmatrix} \right\rangle$ is a p-Sylow group. Suppose that $S_{p^{k-1}}$ has a p-Sylow group. Consider the permutation $\sigma \in S_{p^k}$ defined as following

$$\sigma = \begin{pmatrix} 1 & p^{k-1}+1 & \ldots & (p-1)p^{k-1}+1 \end{pmatrix} \begin{pmatrix} 2 & p^{k-1}+2 & \ldots & (p-1)p^{k-1}+2 \end{pmatrix}$$
$$\ldots \begin{pmatrix} p^{k-1} & 2p^{k-1} & \ldots & p^k \end{pmatrix}$$

Let $A_n = \left\{\tau \in S_{p^k} \,\middle|\, i\tau = i \text{ for } i \leq (n-1)p^{k-1} \text{ and } i > np^{k-1}\right\}$ for $n = 1, \ldots, p$ the set of all permutations that only change the elements $(n-1)p^{k-1}+1, \ldots, np^{k-1}$. It can be easily shown that A_n is a subgroup of S_{p^k}. Futhermore, $A_n = \sigma^{-n} A_1 \sigma^n$ and $|A_1| = (p^{k-1})!$, in fact $A_1 \approx S_{p^{k-1}}$. Therefore, A_n has a p-Sylow group P_n, where $P_n = \sigma^{-n} P_1 \sigma^n$. Let $T = P_1 P_2 \ldots P_n$. Since $P_i \subset A_i$ and A_i are disjoint, then P_i are disjoint and hence they commute. Thus T is a subgroup of S_{p^k} with order $|P_1|^p = p^{p e_p\left(p^{k-1}!\right)}$. Which means T is a not a p-Sylow group. Note that $\sigma \notin T$ and $P_i \sigma^j = \sigma^j P_{i+j}$. Consider $P = \{\sigma^j t \,|\, t \in T, 0 \leq j < p\}$, we claim that P is a subgroup of S_{p^k}.

1. Let $t = q_1 \dots q_p$ where $q_i \in P_1$. Then,
$$\begin{aligned} \sigma^j t \sigma^k t' &= \sigma^j q_1 \dots q_{p-1} q_p \sigma^k \ t' \\ &= \sigma^j q_1 \dots q_{p-1} \sigma^k q_p' \ t' \\ &= \sigma^{j+k} q_1' \dots q_{p-1}' q_p' \ t' \end{aligned}$$
where $q_i' \in P_{i+j}$. Since P_i are commutative, then $q_1' \dots q_p' t' \in T$.

2. The inverse of $\sigma^j t$ can be easily found.

The order of P is $p\,|T| = p^{pe_p\left(p^{k-1}!\right)+1} = p^{e_p\left(p^k!\right)}$. Which means, P is a p-Sylow subgroup of S_{p^k}. ∎

Definition: Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim_B^A y$ if $y = axb$ for some $a \in A$ and $b \in B$.

Lemma 2.60. *The relation $\sim_B^A$ defines an equivalence relation on G. The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$.*

Proof.

1. For all $x \in G$, $x = exe$ and hence $x \sim_B^A x$.

2. For all $x, y \in G$, if $x \sim_B^A y$, then $y = axb$ for some $a \in A$ and $b \in B$, hence $x = a^{-1} y b^{-1}$, therefore, $y \sim_B^A x$.

3. For all $x, y, z \in G$, if $x \sim_B^A y$ and $y \sim_B^A z$, then $y = a_1 x b_1$ and $z = a_2 y b_2$ for some $a_1, a_2 \in A$ and $b_1, b_2 \in B$, hence $z = a_2 a_1 x b_1 b_2$, therefore, $x \sim_B^A z$. □

Lemma 2.61. *If A, B are finie subgroups of G then*
$$|AxB| = \frac{|A||B|}{|A \cup xBx^{-1}|}$$

Proof. Note that $|AxB| = |AxBx^{-1}|$
$$|AxB| = \left|AxBx^{-1}\right| = \frac{|A||xBx^{-1}|}{|A \cap xBx^{-1}|} = \frac{|A||B|}{|A \cap xBx^{-1}|}$$
which proves the lemma. □

Lemma 2.62. *Let G be a finite group and suppose G is a subgroup of the finite group M. Suppose further that M has a p-Sylow group subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.*

Proof. Let $p^m \mid\mid |M|$ and $p^n \mid\mid |G|$ with $n \leq m$. Therefore, $|Q| = p^m$ and since $G \cap xQx^{-1} \overset{\text{gp}}{\subset} xQx^{-1}$ for all $x \in M$, then $|G \cap xQx^{-1}| = p^{m_x}$ for some $m_x \leq n$. Note that by the above's lemma
$$|GxQ| = \frac{|G||Q|}{|G \cup xPx^{-1}|} = \frac{p^n \alpha p^m}{p^{m_x}} = p^{n+m-m_x}\alpha$$

We claim that there exists $x \in M$ such that $m_x = n$. As otherwise, m_x would be strictly smaller than n, hence $n - m_x \geq 1$. Thus,

$$|M| = \sum_{x \in A} |GxQ|$$

would divide p^{m+1} which is a contradiction. Therefore, let x be such that $m_x = n$ and $P = G \cap xQx^{-1}$

$$|P| = \frac{|G||Q|}{|G \cap xQx^{-1}|} = \frac{p^n \alpha p^m}{p^m \alpha} = p^n$$

which means that P is a p-Sylow group of G. □

We now present the thrid proof.

Proof. Let $|G| = n$. By the Cayley's theorem, we can isomorphically embed G in S_n. Let $p^k > n$. Then, S_n is a subgroup of S_{p^k} and therefore G is a subgroup of S_{p^k}. By the last lemma, G has a p-Sylow group. ■

Theorem 2.63 (Second part of Sylow's theorem). *If G is a finite group, p is a prime and $p^n \,||\, |G|$, then any two subgroups of G of order p^n are conjugate.*

Proof. Let A and B be two p-Sylow groups of G with order p^n. Consider the double coset decomposition of G with respected to A and B.

$$|AxB| = \frac{|A||B|}{|A \cap xBx^{-1}|} = p^{2n - m_x}$$

where $m_x = |A \cap xBx^{-1}|$. If $A \neq xBx^{-1}$ for any $x \in G$, then $m_x < n$ for all $x \in G$. Therefore, $2n - m_x \geq n + 1$ for all $x \in G$. Particularly, if A is the set of representatives of equivalence classes of $\sim^A_B$,

$$|G| = \sum_{x \in A} |AxB|$$

which means $p^{n+1} \mid |G|$ which is a contradiction. Therefore, there exists a $x \in G$ such that $A = xBx^{-1}$. ■

Definition: Suppose H is a subgroup of G. The **normalizer** of H is the subgroup $N(H) = \{x \in G \,|\, x^{-1}Hx = H\}$.

Lemma 2.64. *Let H be a subgroup of G. Then, the number of distinct conjugates of H is $i_G(N(H))$.*

Proof. Let S be the set of right cosets of $N(H)$ in G and T be the set of conjugates of H. Consider $\varphi : S \to T$ given by $\varphi : N(H)g \mapsto g^{-1}Hg$. This, function is well-defined since if $N(H)g = N(H)h$, then $g = nh$ for some $n \in N(H)$. Then, $g^{-1}Hg = h^{-1}n^{-1}Hnh = h^{-1}Hh$. Similary, it is injective. If $N(H)g\varphi = N(H)h\varphi$, then $g^{-1}Hg = h^{-1}Hh \implies H = (gh^{-1})H(hg^{-1}) \implies hg^{-1} \in N(H)$ hence $N(H)g = N(H)h$. φ is clearly surjective. Suppose $x^{-1}Hx \in T$ then, $N(H)x\varphi = x^{-1}Hx$. Therefore, φ is a bijection and $|T| = |S| = i_G(N(H))$.□

Corollary 2.65. *The number of p-Sylow subgroups in G equals $|G|/|N(P)|$ where P is any p-Sylow subgroup of G. In particular, this number is a divisor of $|G|$.*

Proof. p-Sylow subgroups are conjugates. □

Theorem 2.66 (Second part of Sylow's theorem). *The number of p-Sylow subgroups in G, is of the form $1 + kp$.*

Proof. Let $p^n \mid\mid G$ and consider the double coset decomposition of G with respect to P and P.

$$|PxP| = \frac{(|P|)^2}{|P \cap xPx^{-1}|}$$

if $x \in N(P)$, then $P \cap xPx^{-1} = P$ and hence $|P \cap xPx^{-1}| = p^n$. Otherwise, $P \cap xPx^{-1} \subsetneq P$ and hence $|P \cap xPx^{-1}| = p^{m_x}$ for some $m_x < n$. Therefore,

$$|G| = \sum_{x \in N(P)} |PxP| + \sum_{x \notin N(P)} |PxP|$$

If $x \in N(P)$, then $xPx^{-1} = P \implies PxP = Px$. Hence, the first summation is

$$\sum_{x \in N(P)} |Px| = |P| i_{N(P)}(P) = |N(P)|$$

and the second summation is divisible by p^{n+1} hence there exists an intger u such that

$$\sum_{x \notin N(P)} |PxP| = p^{n+1}u$$

therefore

$$|G| = |N(P)| + p^{n+1}u \implies i_G(N(P)) = 1 + \frac{p^{n+1}u}{|N(P)|}$$

Moreover, p^{n+1} does not divide G and hence it does not divide $N(P)$. Thus, $p^{n+1}u/|N(P)|$ is an integer divisible by p. ■

Exercises

1. Let N be a subgroup of of finite group G such that $i_G(N)$ is the smallest prime factor of $|G|$. Prove N is normal.

2.

2.14 Direct product

Let A and B be any two groups and $G = A \times B$. Define the operation $\circ_G$ as $(a_1, b_1) \circ_G (a_2, b_2) = (a_1 \circ_A a_2, b_1 \circ_B b_2)$. It can be readily verified that G is group under the operation $\circ_G$. We call $(G, \circ_G)$ the **external direct product** of A and B.

Now suppose $G = A \times B$ and consider $\bar{A} = \{(a, f) \in G \mid a \in A\}$ where f is the unit element of B. Then, $\bar{A}$ is a normal subgroup in G and is isomorphic to A. We claim that $G = \bar{A}\bar{B}$ and every $g \in G$ has a unique decomposition in the form of $g = \bar{a}\bar{b}$ where $\bar{a} \in \bar{A}$ and $\bar{b} \in \bar{B}$. Thus we have realized G as an **internal product** $\bar{A}\bar{B}$ of two normal subgroups.

Definition: Let G be a group and $N_1, \ldots, N_n$ normal subgroups of G such that

1. $G = N_1 \ldots N_n$.
2. Any $g \in G$ can be uniquely represented as $g = n_1 n_2 \ldots n_n$ where $n_i \in N_i$.

We then say that G is the **internal direct product** of $N_1, \ldots, N_n$.

Lemma 2.67. *Suppose that G is the internal product of $N_1, \ldots, N_n$. Then for $i \neq j$, $N_i \cap N_j = \{e\}$ and if $a \in N_i$ and $b \in N_j$ then $ab = ba$.*

Theorem 2.68. *Suppose that G is the internal product of $N_1, \ldots, N_n$ and let $T = N_1 \times \cdots \times N_n$. Then G and T are isomorphic.*

2.15 Maximial subgroups

Definition: A subgroup $M < G$ is **maximal** if there exists no subgroup H such that $M < H < G$.

Theorem 2.69. *Every proper subgroup of a finite group has a maximal subgroup.*

2.16 Finitely generated group

Definition: A group G is **finitely generated** if there is a finite set A such that $G = \langle A \rangle$.

Proposition 2.70. *Every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.*

2.17 Finite abelian groups

Theorem 2.71 (The fundamental theorem on finite abelian groups). *Every finite abelian group is the direct product of cyclic groups.*

Definition: If G is an abelian group of order p^n, p a prime, and $G = A_1 \times \cdots \times A_k$ where A_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, then the integers $n_1, n_2, \ldots, n_k$ are called the **invariants** of G.

Definition: Ig G is an abelian group and s is any integer, then $G(s) = \{x \in G \mid x^s = e\}$.

Lemma 2.72. *If G and G' are isomorphic abelian groups, then for every integer s, $G(s)$ and $G'(s)$ are isomorphic.*

Chapter 3

Ring Theory

Definition: A non-empty set R is an **associative ring** if in R there are defined two operations $(+, \cdot)$ such that for all $a, b, c \in R$

1. R is closed under $+$.
2. $+$ is commutative.
3. $+$ is associative.
4. There exists an element $0 \in R$, which is the identity element of $+$.
5. For each a, there exists b such that $a + b = b + a = 0$.
6. R is closed under $\cdot$.
7. $\cdot$ is associative.
8. $\cdot$ is distributive over $+$. That is, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

If there is an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$, R is said to be a **ring with unity**. If $\cdot$ is commutative, R is said to be a **commutative ring**. If the non-zero elements of R form an abelian group under $\cdot$, R is said to be a **field**.

Example 3.1. Consider the **real quaternions**, $Q = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\}$ with multiplication rules; $i^2 = j^2 = k^2 = ijk = 1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Then, Q is a non-commutative ring and its non-zero elements form a non-commutative group under multiplication.

3.1 Some special classed of ring

Definition: If R is a commutative ring, then a non-zero element $a \in R$ is a **zero-divisor** if there exists another non-zero element b such that $ab = 0$.

Definition: A commutative ring is an **integral domain** if it has no zero-divisors.

Definition: A ring in which all non-zero elements form a group under multiplication is called a **division ring** or **skew-field**.

Definition: A field is a commutative division ring.

Lemma 3.1. *for all $a, b, c \in R$*

1. $a \cdot 0 = 0 \cdot a = 0$.
2. $a(-b) = (-a)b = -ab$.
3. $(-a)(-b) = ab$.

If $1 \in R$

1. $(-1)a = -a$.
2. $(-1)(-1) = 1$.

Lemma 3.2. *A finite integral domain is a field.*

Corollary 3.3. *If p is a prime, $\mathbb{Z}_p$ is a field.*

Definition: An integral domain D is said to be of characteristic 0 if the relation $ma = 0$ where $a \neq 0$ and $m \in \mathbb{Z}$ holds only if $m = 0$. D is of finite characteristic if there exists a positive integer m such that for all $a \in D$, $ma = 0$. The characteristic of D is the samllest such integer. We say that a ring R has n**-torsion** if there exists $a \neq 0$ in R such that $na = 0$ and $ma \neq 0$ for $0 < m < n$.

3.2 Homomorphisms

Definition: A mapping ϕ from the ring R into the ring R' is a homomorphism if

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

and

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

for all $a, b \in R$.

Lemma 3.4. *If $\phi : R \to R'$ is a homomorphism*

1. $\phi(0) = 0$.
2. $\phi(-a) = -\phi(a)$.

Definition: Suppose $\phi : R \to R'$ is a homomorphism. The kernel $I(\phi) = \{a \in R\}\phi(a) = 0$.

Lemma 3.5. *If $\phi : R \to R'$ is a homomorphism*

1. *$I(\phi)$ is a subgroup of R under addition.*
2. *If $a \in I(\phi)$ and $r \in R$, then $ra, arI(\phi)$.*

Definition: A homomorphism R into R' is an isomorphism of it is one-to-one. R and R' are isomorphic if there is an onto isomorphism between them.

Lemma 3.6. *The homomorphism $\phi : R \to R'$ is an isomorphism if and only if $I(\phi) = \{0\}$.*

3.3 Ideals and quotient ring

Definition: A non-empty subset U of R is a **two-sided ideal** of R if

1. U is a subgroup of R under addition.

2. For all $u \in U$ and $r \in R$, $ur, ru \in U$.

R/U is the set of distinct cosets of U in R as a group under addition. R/U is a ring with $(a+U)(b+U) = ab + U$.

If R is commutative or it has unit element, then R/U is commutative or has unit element. But the converse is not necessarily true. — give an example.

Lemma 3.7. *If U is an ideal of the ring R. then R/U is a ring and is a homomorphic image of R.*

Theorem 3.8. *Suppose $\phi : R \to R$" is a homomorphism and let $U = I(\phi)$. Then, $R' \approx R/U$. Moreover, there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R that contain U. This correspondence can be achieved by associating with an ideal W' of R', the ideal W in R defined by $W = \{x \in R \mid \phi(x) \in W'\}$, then $W' \approx R/W$.*

3.4 More ideals and quotient rings

Lemma 3.9. *Let R be a commutative ring with unit element whose only ideals are (0) and R. Then, R is a field.*

Definition: An ideal $M \neq R$ is said to be **maximal ideal** of R whenever U is an ideal of R such that $M \subset U \subset R$, then either UR or $U = M$.

If a ring has unit element, then using axiom of choice it can be shown that there is a maximal ideal.

Theorem 3.10. *If R is a commutative ring with unit element and M is an ideal of R, then M is maximal ideal if and only if R/M is a field.*

3.5 The field of quotients of integral domain

Definition: A ring R can be **imbedded** in ring R' if there is an isomorphism of R inot R'. If R and R' have unit elements, this isomorphism should take 1 onto $1'$. R' will be called an **over ring or extension** of R.

Theorem 3.11. *Every integral domain can be imbedded in a field.*

Proof. Take a look at quotients $\frac{a}{b}$. $M = \{(a, b) \mid a, b \in D, b \neq 0\}$. $(a, b) \sim (c, d)$ if $ad = bc$. F be the set of equivalence classes. F is a field and D can be imbedded in F. ∎

F is caled the **field of quotients** of D.

3.6 Euclidean ring

Definition: An integral domain R is an **Euclidean ring** if for every $a \neq 0$ in R there exists a non-negative integer $d(a)$ such that

1. For all non-zero $a, b \in R$, $d(a) \leq d(ab)$.
2. For all non-zero $a, b \in R$, there exists $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

$\langle a \rangle = \{xa \mid x \in R\}$.

Theorem 3.12. *Let R be a Euclidean ring and let A be an ideal of R. Then, there exists $a_0 \in A$ such that A consists exactly of $a_0 x$ as x ranges over R.*

Definition: An integral domain R with unit element is a **principle ideal ring** if every ideal A of R is of the form $A = \langle a \rangle$ for some $a \in R$

Corollary 3.13. *A Euclidean ring possesses a unit element.*

Definition: If $a \neq 0$ and b are in a commutative ring R, then a is said to divide b there exists $c \in R$ such that $b = ac$ denoted by $a \mid b$.

Remark 1.

1. $a \mid b,\ b \mid c \implies a \mid c$.
2. $a \mid b,\ a \mid c \implies a \mid (b \pm c)$.
3. $a \mid b \implies a \mid bx$ for all $x \in R$.

Definition: If $a, b \in R$, then $d \in R$ is the **greatest common divisor** of a and b if

1. $d \mid a,\ d \mid b$.
2. $c \mid a,\ c \mid b \implies c \mid d$.

It is denoted as $d = (a, b) = \gcd(a, b)$.

Lemma 3.14. *Let R be a Euclidean ring. Then, any two elements a and b in R have a greatest common divisor d. Moreover, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.*

Definition: Let R be a commutative ring with unit element. An element $a \in R$ is a **unit** in R if there exists an element b such that $ab = 1$.

A unit is an element whose multiplicative inverse exists in R.

Lemma 3.15. *Let R be an integral domain with unit element and suppose that for $a, b \in R$ both $a \mid b$ and $b \mid a$ are true. Then, $a = ub$, where u is a unit in R.*

Definition: In a commutative ring R with unit element, two elements a and b are **associates** if $b = ua$ for some unit $u \in R$.

Lemma 3.16. *Let R be a Euclidean ring and $a, b \in R$ be non-zero elements. If b is not a unit in R, then $d(a) < d(ab)$.*

Definition: Let R be a Euclidean. A non-unit elemnt $\pi \in R$ is **prime** if whenever $\pi = ab$, one of a or b is a unit in R.

Theorem 3.17. *Let R be a Euclidean ring. Then, every element is either a unit in R or can be written as a product of finite number prime elements.*

Definition: Let R be a Euclidean ring. Two elements a and b in R are **relatively prime** if their greatest common divisor is a unit in R.

Lemma 3.18. *Let R be a Euclidean ring. If $a \mid bc$ but a and b are relatively prime, then $a \mid c$.*

Lemma 3.19. *If π is a prime element in a Euclidean ring R, then $\pi \mid ab \implies \pi \mid a$ or $\pi \mid b$.*

Theorem 3.20 (Unique factorization theorem). *Let R be a Euclidean ring and $a \neq 0$ be non-unit element of R. Suppose that $a = \pi_1 \dots \pi_n = \pi'_1 \dots \pi'_m$ where π_i and π'_j are prime elements. Then, $n = m$ and each π_i is an associate of a π'_j and each π'_j is an associate of a π_i.*

Combining unique factorization theorem with 3.17 gives that every non-zero element in R can be written uniquely up to associates as a product of primes in R.

Lemma 3.21. *The ideal $A = \langle a_0 \rangle$ is a maximal ideal of the Euclidean ring R if and only if a_0 is a prime element.*

3.7 A particular Euclidean ring

The domain of **Gaussian integers** $\mathbb{Z}[i] = \left\{ a + bi \,\middle|\, a, b \in \mathbb{Z}, i = \sqrt{-1} \right\}$ is a Euclidean ring, with $d(a + bi) = a^2 + b^2$.

Theorem 3.22. *$\mathbb{Z}[i]$ is a Euclidean ring.*

Lemma 3.23. *Let p be a prime integer and suppose for integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then, p can be written as a sum of two squares of integers. i.e. there exists integers a and b such that $a^2 + b^2 = p$.*

Lemma 3.24. *If $p \equiv 1 \mod 4$, we can solve the congruence $x^2 \equiv -1 \mod p$.*

Theorem 3.25. *If p is a prime of form $4n + 1$, then $p = a^2 + b^2$ for some integers a and b.*

3.8 Polynomial rings

Let F be a field. $F[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0, a_i \in F\}$ is the ring of polynomials in the indeterminate x.

Definition: If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + \cdots + b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if $m = n$ and for each $i \geq 0$, $a_i = b_i$.

Definition: $p(x) + q(x) = c_0 + \cdots + c_kx^k$ where $c_i = a_i + b_i$.

Definition: $p(x)q(x) = c_0 + \cdots + c_kx^k$ where $c_i = \sum_{t=0}^{i} a_tb_{i-t}$.

Therefore, $F[x]$ is a commutative ring with unit element.

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, then the **degree** of f is n. *i.e.* the degree of f, $\deg f = \min\{n \geq 0 \mid a_k = 0, \ \forall k > n\}$. The zero polynomial can be defined to be of infinite degree.

Lemma 3.26. *If $f(x), g(x) \neq 0$ are two polynomials in $F[x]$, then*

$$\deg(fg) = \deg(f) + \deg(g)$$

Corollary 3.27. *$f(x), g(x) \neq 0$, then $\deg(f) \leq \deg(fg)$.*

Corollary 3.28. *$F[x]$ is an integral domain.*

Since $F[x]$ is an integeral domain, we can construct its field of quotients which is the field of rational functions in x over F.

Lemma 3.29 (The division algorithm). *Given two polynomials $f(x)$ and $g(x) \neq 0$, there exists two polynomials $t(x), r(x) \in F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r < \deg g$.*

Theorem 3.30. *$F[x]$ is a Euclidean ring.*

Theorem 3.31. *$F[x]$ is a principle ideal group.*

Lemma 3.32. *Given two polynomials $f(x), g(x) \in F[x]$, the greatest common divisor $d(x) = (f(x), g(x))$ can be realized as $d(x) = \lambda(x)f(x) + \mu(x)g(x)$ for some $\lambda(x), \mu(x) \in F[x]$.*

Definition: A polynomial $p(x) \in F[x]$ is **irreducible** over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, one of $a(x)$ or $b(x)$ has degree 0.

Lemma 3.33. *Any polynomial in $F[x]$ can be written in a unique manner as product of irreducible polynomials in $F[x]$.*

Lemma 3.34. *The ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal if and only $p(x)$ is irreducible.*

3.9 Polynomials over field of rationals

Definition: The polynomial $f(x) = a_0+a_1x+\cdots+a_nx^n$ where $a_i \in \mathbb{Z}$ is said to be **primitive** if the greatest common divisor of $a_0, \ldots, a_n$ is 1.

Lemma 3.35. *If $f(x)$ and $g(x)$ are primitive, then $f(x)g(x)$ is a primitive polynomial.*

Definition: The **content** of a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_i \in \mathbb{Z}$ is the $\gcd(a_0, \ldots, a_n)$.

Theorem 3.36 (Guass' lemma). *If primitive polynomial $f(x)$ can be factored as a product of two polynomials with rational coefficients, it can be factored as the product of two polynomials with integer coefficients.*

Definition: A polynomial is said to be **integer monic** if all of its coefficients are integers and its highest coefficient is 1.

Corollary 3.37. *If an integer monic polynomial $f(x)$ can be factored as a product of two polynomials with rational coefficients, it can be factored as a product of two integer monic polynomials.*

Theorem 3.38 (The Eisenstein criterion). *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}$. Suppose that for some p, $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1$, $p \mid a_0$, but $p^2 \nmid a_0$. Then, $f(x)$ is irreducible over rationals.*

3.10 Polynomial rings over commutative rings

$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R\}$. For the rest of this section R is assumed to be commutative and have unit element. $R[x_1, \ldots, x_n]$ is the ring of polynomials in the indeterminate $x_1, \ldots, x_n$. It can be constructed as $R[x_1][x_2] \ldots [x_n] = \left\{\sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}\right\}$.

Lemma 3.39. *If R is an integral domain, so is $R[x]$ and by induction, $R[x_1, \ldots, x_n]$ is an integral domain.*