Lecture Note on Algebra

Anthony Hong[1]

January 8, 2024

[1]Thanks to Professor Beheshti Zavareh for her teaching Math5031-32 Algebra I & II; thanks to Albert Peng for his permission to edit his tex file of Math5031 and also J.S. Milne's tex file

Contents

Chapter 1

Groups

1.1 Recap: Groups, Cosets, and Homomorphisms

Definition 1.1.1 (Group)**.** We define a binary operation (multiplication) $* : G \times G \to G$ on a nonempty set G, and $(G, \cdot)$ is called a **group** if $*$ satisfies the following rules.

(1) the multiplication is closed on G;

(2) associativity of multiplication: $a * (b * c) = (a * b) * c, \forall a, b, c \in G$;

(3) G has an **identity element** (i.e. $\exists e \in G$ s.t. $\forall g \in G : e * g = g * e = g$);

(4) each element $g \in G$ has an **inverse** (i.e. $\exists g^{-1} \in G$ s.t. $g * g^{-1} = g^{-1} * g = e$).

Remark 1.1.2. Several remarks are in order:

1. We will denote $ab = a * b$ and $a^m * a^n = a^{n+m} = a^n * a^m$ and $(a^m)^n = a^{mn} = (a^n)^m$.
2. A **magma** is a tuple $(G, *)$ with (1) above; a **semigroup** is an associative magma, i.e. tuple $(G, *)$ with (1) and (2) above; a **monoid** is a semigroup with an identity element, i.e., tuple $(G, *)$ with (1), (2), and (3) above.
3. Let $(R, +, *)$ be a ring with unity 1. That is, $(R, *)$ is a monoid. An element x is called a **unit** or **invertible element** if it has an inverse, so the set of all invertible elements $U(R)$ is a group, called **group of units** in R.
4. Rules (3) and (4) in definition 1.1.1 are equivalent to the following condition (proof of the equivalence outlined in the exercise 1):

(5) $\forall a, b \in G :$ equations $ax = b, ya = b$ have solutions in G.

Definition 1.1.3 (Abelian Group)**.** A group G is called **Abelian** if $\forall a, b \in G : ab = ba$.

Definition 1.1.4 (Subgroup)**.** A non-empty subset $H \subseteq G$ is a **subgroup**, denoted as $H \leq G$, if

(1) $a \in H \implies a^{-1} \in H$

(2) $a, b \in H \implies ab \in H$

Proposition 1.1.5.

1. $H \leq G$ implies that H is a group with operation of G (see [8] Theorem 2.1);
2. $H \subseteq G$ is a subgroup iff $e \in H$ and $a, b \in H \implies ab^{-1} \in H$ (see [8] Theorem 2.2).

3. G finite, then a nonempty subset H of G is a subgroup iff $a, b \in H \Rightarrow ab \in H$ (see [8] Corollary 2.4).

Theorem 1.1.6. The inverse and the identity element of a group are both unique.

Proof. Suppose $e, e' \in G$ and $\forall g \in G$ we have

$$e \cdot g = g \cdot e = g \tag{1.1}$$
$$e' \cdot g = g \cdot e' = g \tag{1.2}$$

Putting $g = e$ in (1.2) results in $e = e \cdot e'$ and putting $g = e'$ in (1.1) results in $e \cdot e' = e'$. So $e = e'$. Suppose h and k are inverses of g, so that in particular $hg = e$ and $gk = e$. Then $(hg)k = ek = k$, but $h(gk) = he = h$. But the associativity law tells us $(hg)k = h(gk)$, which says $k = h$. ■

Example 1.1.7. The trivial group $G = \{e\}$ with $*$ defined by $e * e = e$. $(\mathbb{C}, \times)$ is not a group. What would the inverse element of 0 be? But if we write $\mathbb{C}^\times$ for the set of nonzero complex numbers then $(\mathbb{C}^\times, \times)$ is a group. Equally the nonzero real numbers or rational numbers under multiplication are groups. Let $\mathrm{GL}(n, \mathbb{C})$ be the set of $n \times n$ invertible matrices over the complex numbers. Then $\mathrm{GL}_n(\mathbb{C})$ with matrix multiplication is a nonabelian group.

Definition 1.1.8 (group homomorphism)**.** Let G, G' be a group. $\phi : G \to G'$ is a **homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. f is an **isomorphism** if the homomorphism is bijective, denoted by $G \cong H$. An injective homomorphism is called a **monomorphism**. A surjective homomorphism is called a **epimorophism**. If $G = G'$, we say the homomorphism is an **endomorphism**. If furthermore that endomorphism is also bijective, we say it is an automorphism.

Theorem 1.1.9. Let $f : (G, *) \to (G', \circ)$ be a homomorphism.

1. $f(e) = e'$, where e' is the identity in G';
2. If $a \in G$, then $f\left(a^{-1}\right) = f(a)^{-1}$;
3. If $a \in G$ and $n \in \mathbb{Z}$, then $f\left(a^n\right) = f(a)^n$;
4. $H \leq G \Rightarrow f(H) \leq G'$ and $H' \leq G' \Rightarrow f^{-1}(H') \leq G$;

Proof.

1. Applying f to the equation $e = e * e$ gives $f(e) = f(e * e) = f(e) \circ f(e)$. Now multiply each side of the equation by $f(e)^{-1}$ to obtain $e' = f(e)$.
2. Applying f to the equations $a * a^{-1} = e = a^{-1} * a$ gives $f(a) * f\left(a^{-1}\right) = e' = f\left(a^{-1}\right) * f(a)$. It follows from Theorem 1.10, the uniqueness of the inverse, that $f\left(a^{-1}\right) = f(a)^{-1}$.
3. Induction shows $f\left(a^n\right) = f(a)^n$ for all $n \geq 0$, and then $f\left(a^{-n}\right) = f\left(\left(a^{-1}\right)^n\right) = f\left(a^{-1}\right)^n = f(a)^{-n}$.
4. $e' \in f(H)$ by 1. Let $x', y' \in f(H)$, then $\exists x, y \in H$ s.t. $f(x) = x', f(y) = y'$. Thus $xy^{-1} \in H \Rightarrow x'y'^{-1} = f(xy^{-1}) \in f(H)$. Now, $e \in f^{-1}(H')$ by 1. Let $x, y \in f^{-1}(H')$. Then $f(xy^{-1}) = f(x)f(y)^{-1} \in H' \Rightarrow xy^{-1} \in f^{-1}(H')$.

■

Example 1.1.10 (Klein-four group)**.** For small groups $(G, *)$ we can completely describe the group operation by drawing a table called a **group table** or **Cayley table**. It is a $n \times n$ matrix whose i, j entry is the group element $g_i g_j$, where $n = |G|$. For example, one can show that $\mathbf{V} = \{1, -1, i, -i\} \subseteq \mathbb{C}$ with multiplication of complex numbers $\cdot$ is a group, where the group table is given below. This is an abelian group. One can also show that it is isomorphic to $\{1, (12)(34), (13)(24), (14)(23)\}$ with composition of permutation as multiplication (i.e., as a subgroup of S_4) and also to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong D_2 = \langle a, b | a^2 = b^2 = (ab)^2 = e \rangle$.

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Example 1.1.11 (Quaternion group)**.** The quaternion group, Q_8, is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{gathered} 1 \cdot a = a \cdot 1 = a, \quad \text{for all } a \in Q_8 \\ (-1) \cdot (-1) = 1, \quad (-1) \cdot a = a \cdot (-1) = -a, \quad \text{for all } a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 \\ i \cdot j = k, \quad j \cdot i = -k \\ j \cdot k = i, \quad k \cdot j = -i \\ k \cdot i = j, \quad i \cdot k = -j. \end{gathered}$$

It is tedious to check the associative law (it can be proven by a less computational mean), but the other axioms are easily checked. Note that Q_8 is a non-abelian group of order 8.

Example 1.1.12. Consider the set of nonzero real numbers, $\mathbb{R}^*$, with the group operation of multiplication. The identity of this group is 1 and the inverse of any element $a \in \mathbb{R}^*$ is just $1/a$. We will show that

$$\mathbb{Q}^* = \{p/q : p \text{ and } q \text{ are nonzero integers } \}$$

is a subgroup of $\mathbb{R}^*$. The identity of $\mathbb{R}^*$ is 1 ; however, $1 = 1/1$ is the quotient of two nonzero integers. Hence, the identity of $\mathbb{R}^*$ is in $\mathbb{Q}^*$. Given two elements in $\mathbb{Q}^*$, say p/q and r/s, their product pr/qs is also in $\mathbb{Q}^*$. The inverse of any element $p/q \in \mathbb{Q}^*$ is again in $\mathbb{Q}^*$ since $(p/q)^{-1} = q/p$. Since multiplication in $\mathbb{R}^*$ is associative, multiplication in $\mathbb{Q}^*$ is associative.

Example 1.1.13. Let $SL_2(\mathbb{R})$ be the subset of $GL_2(\mathbb{R})$ consisting of matrices of determinant one; that is, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(\mathbb{R})$ exactly when $ad - bc = 1$. To show that $SL_2(\mathbb{R})$ is a subgroup of the general linear group, we must show that it is a group under matrix multiplication. The 2×2 identity matrix is in $SL_2(\mathbb{R})$, as is the inverse of the matrix A :

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

It remains to show that multiplication is closed; that is, that the product of two matrices of determinant one also has determinant one. We will leave this task as an exercise. The group $SL_2(\mathbb{R})$ is called the **special linear group**.

Example 1.1.14. It is important to realize that a subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G, it must inherit the binary operation of G. The set of all 2×2 matrices, $\mathbb{M}_2(\mathbb{R})$, forms a group under the operation of addition. The 2×2 general linear group is a subset of $\mathbb{M}_2(\mathbb{R})$ and is a group under matrix multiplication, but it is not a subgroup of $\mathbb{M}_2(\mathbb{R})$. If we add two invertible matrices, we do not necessarily obtain another invertible matrix. Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but the zero matrix is not in $GL_2(\mathbb{R})$.

Two subtleties regarding the binary operation need to be addressed:

Theorem 1.1.15 (associative invariance of bracketing)**.** For each way of bracketing the multiplication of n elements $a_1, \cdots, a_n \in A$, we denote it as

$$\pi_i (a_1 \cdot a_2 \cdot \cdots \cdot a_n), i = 1, 2, \cdots, N$$

where it can be proved that $N = (2n-2)!/[n!(n-1)!]$. For example, let $n = 3$ and we will have $N = 2$ ways to bracket the three elements: $\pi_1 (a_1 \cdot a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3$ and $\pi_2 (a_1 \cdot a_2 \cdot a_3) = a_1 \cdot (a_2 \cdot a_3)$. We now claim that these N ways of bracketing are the same if associativity of order 3 holds for the set A (i.e. $\pi_1 (a_1 \cdot a_2 \cdot a_3) = \pi_2 (a_1 \cdot a_2 \cdot a_3)$, or $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$), and then the notation $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ is well-defined.

Proof. See exercise 1.1-7. ■

Theorem 1.1.16 (commutative invariance of permutation)**.** If both associativity and commutativity hold for a binary operation $\cdot$, then permutating the following multiplication in any order results the same

$$a_1 \cdot a_2 \cdot \cdots \cdot a_N$$

Proof. See exercise 1.1-8. ■

Definition 1.1.17. If G is a group and $a \in G$, then the **cyclic subgroup generated by** a, denoted by $\langle a \rangle$, is the set of all the powers of a. A group G is called **cyclic** if there is $a \in G$ with $G = \langle a \rangle$; that is, G consists of all the powers of a.

It is plain that $\langle a \rangle$ is, indeed, a subgroup of G. Notice that different elements can generate the same cyclic subgroup. For example, $\langle a \rangle = \langle a^{-1} \rangle$.

Example 1.1.18. Let $C_n = \{e^{2\pi ik/n} : k \in \mathbb{Z}\}$, a subset of the complex numbers. This is a group under multiplication: certainly multiplication is a binary operation on this set, for

$$e^{2\pi ik/n} e^{2\pi il/n} = e^{2\pi i(k+l)/n}$$

which is an element of C_n. You can check the other group axioms. C_n is a cyclic group, because every element is a power of $\zeta = e^{2\pi i/n}$, and ζ has order n so $|C_n| = n$. Any generator of C_n is called a **primitive n-th root of unity**.

Definition 1.1.19. If G is a group and $a \in G$, then the **order of** a is $|\langle a \rangle|$, the number of elements in $\langle a \rangle$.

Theorem 1.1.20. If G is a group and $a \in G$ has finite order m, then m is the smallest positive integer such that $a^m = 1$.

Proof. If $a = 1$, then $m = 1$. If $a \neq 1$, there is an integer $k > 1$ so that $1, a, a^2, \ldots, a^{k-1}$ are distinct elements of G while $a^k = a^i$ for some i with $0 \leq i \leq k-1$. We claim that $a^k = 1 = a^0$. If $a^k = a^i$ for some $i \geq 1$, then $k - i \leq k - 1$ and $a^{k-i} = 1$, contradicting the original list $1, a, a^2, \ldots, a^{k-1}$ having no repetitions. It follows that k is the smallest positive integer with $a^k = 1$.

It now suffices to prove that $k = m$; that is, that $\langle a \rangle = \{1, a, a^2, \ldots, a^{k-1}\}$. Clearly $\langle a \rangle \supset \{1, a, a^2, \ldots, a^{k-1}\}$. For the reverse inclusion, let a^l be a power of a. By the division algorithm, $l = qk + r$, where $0 \leq r < k$. Hence, $a^l = a^{qk+r} = a^{qk} a^r = a^r$ (because $a^k = 1$), and so $a^l = a^r \in \{1, a, a^2, \ldots, a^{k-1}\}$. ■

Theorem 1.1.21. Every subgroup of a cyclic group is cyclic.

Proof. The main tools used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If $H = \{e\}$, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n. Since H is a subgroup, $g^{-1} = a^{-n}$ must also be in H. Since either n or $-n$ is positive, we can assume that H contains positive powers of a and $n > 0$. Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well-Ordering. We claim that $h = a^m$ is a generator for H. We must show that every $h' \in H$ can be written as a power of h. Since $h' \in H$ and H is a subgroup of G, $h' = a^k$ for some integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

So $a^r = a^k h^{-q}$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that a^m was in H; consequently, $r = 0$ and so $k = mq$. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h. ■

Corollary 1.1.22. The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Proof. First, $n\mathbb{Z} = \{\cdots, -2n, -n, 0, n, 2n, \cdots\} = \langle n \rangle$. Then let $H \leq \mathbb{Z}$. Since $\mathbb{Z}$ is cyclic, $H = \langle n \rangle$ for some $n \in \mathbb{Z}$ by above theorem. ■

Proposition 1.1.23. Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Proof. First suppose that $a^k = e$. By the division algorithm, $k = nq + r$ where $0 \leq r < n$; hence,

$$e = a^k = a^{nq+r} = a^{nq} a^r = e a^r = a^r.$$

Since the smallest positive integer m such that $a^m = e$ is n, we have $r = 0$. Conversely, if n divides k, then $k = ns$ for some integer s. Consequently,

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$

■

Proposition 1.1.24. An infinite cyclic group $\langle a \rangle \cong \mathbb{Z}$ has exactly two generators $a, -a$. Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

Proof. The first statement is trivial. We show the second: we wish to find the smallest integer m such that $e = b^m = a^{km}$. By above proposition, this is the smallest integer m such that n divides km or, equivalently, n/d divides $m(k/d)$. Since d is the greatest common divisor of n and k, n/d and k/d are relatively prime. Hence, for n/d to divide $m(k/d)$ it must divide m. The smallest such m is n/d. ■

Theorem 1.1.25. The intersection of any family of subgroups of a group G is again a subgroup of G.

Proof. Let $\{S_i : i \in I\}$ be a family of subgroups of G. Now $1 \in S_i$ for every i, and so $1 \in \bigcap S_i$. If $a, b \in \bigcap S_i$, then $a, b \in S_i$ for every i, and so $ab^{-1} \in S_i$ for every i; hence, $ab^{-1} \in \bigcap S_i$, and $\bigcap S_i \leq G$. ■

Corollary 1.1.26. If X is a subset of a group G, then **subgroup generated by** X, defined as

$$\langle X\rangle := \bigcap_{X\subseteq H\leq G} H$$

is the smallest subgroup H of G containing X, that is, if $X \subset S$ and $S \leq G$, then $H \leq S$.

Proof. There are subgroups of G containing X; for example, G itself contains X; define H as the intersection of all the subgroups of G which contain X. Note that H is a subgroup, by Theorem 1.1.25, and $X \subset H$. If $S \leq G$ and $X \subset S$, then S is one of the subgroups of G being intersected to form H; hence, $H \leq S$, and so H is the smallest such subgroup. ■

Definition 1.1.27. If X is a nonempty subset of a group G, then a word on X is an element $w \in G$ of the form

$$w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n},$$

where $x_i \in X, e_i = \pm 1$, and $n \geq 1$.

Theorem 1.1.28. Let X be a subset of a group G. If $X = \varnothing$, then $\langle X\rangle = 1$; if X is nonempty, then $\langle X\rangle$ is the set of all the words on X:

$$\langle X\rangle = \{w = x_1^{e_1}x_2^{e_2}\dots x_n^{e_n} | x_i \in X, e_i = \pm 1, n \geq 1\}$$

Proof. If $X = \varnothing$, then the subgroup $1 = \{1\}$ contains X, and so $\langle X\rangle = 1$. If X is nonempty, let W denote the set of all the words on X. It is easy to see that W is a subgroup of G containing $X : 1 = x_1^{-1}x_1 \in W$; the inverse of a word is a word; the product of two words is a word. Since $\langle X\rangle$ is the smallest subgroup containing X, we have $\langle X\rangle \subset W$. The reverse inclusion also holds, for every subgroup H containing X must contain every word on X. Therefore, $W \leq H$, and W is the smallest subgroup containing X. ■

Definition 1.1.29. Let $H \leq G, g \in G$. The **right coset** of H in G represented by g is $Hg = \{hg \,\big|\, h \in H\}$. Similarly, **left coset** is defined as $gH = \{gh \,\big|\, h \in H\}$.

Example 1.1.30 ([8] Example 2.3)**.** Let G be the additive group of the plane $\mathbb{R}^2$: the elements of G are vectors (x, y), and addition is given by the "parallelogram law": $(x, y)+ (x', y') = (x + x', y + y')$. A line ℓ through the origin is the set of all scalar multiples of some nonzero vector $v = (x_0, y_0)$; that is, $\ell = \{rv : r \in \mathbb{R}\}$. It is easy to see that ℓ is a subgroup of G. If $u = (a, b)$ is a vector, then the coset $u + \ell$ is easily seen to be the line parallel to ℓ which contains u.

Example 1.1.31 ([8] Example 2.4)**.** If G is the additive group $\mathbb{Z}$ of all integers, if S is the set of all multiples of an integer $n(S = \langle n\rangle$, the cyclic subgroup generated by $n)$, and if $a \in \mathbb{Z}$, then the coset $a + S = \{a + qn : q \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv a \bmod n\}$; that is, the coset $a + \langle n\rangle$ is precisely the congruence class $[a]$ of $a \bmod n$.

Proposition 1.1.32. Two observations:

- $Ha = Hb \iff H = Hba^{-1} \iff ba^{-1} \in H$;
- $aH = bH \iff a^{-1}bH = H \iff a^{-1}b \in H$.

Corollary 1.1.33. For two cosets, either $Hg_1 = Hg_2$ or $Hg_1 \cap Hg_2 = \varnothing$ (similar for left cosets).

Proof. Let $a = Hg_1 \cap Hg_2$. Then $a = h_1g_2 = h_2g_2$ and $h_2^{-1}h_1 = g_2g_1^{-1} \implies g_2g_1^{-1} \in H \implies Hg_1 = Hg_2$. ■

Example 1.1.34. A right coset is not necessarily a left coset. See [8] Example 2.5.

Proposition 1.1.35. There is a bijection between the set of distinct left cosets of H and distinct right cosets of H: $aH \mapsto Ha^{-1}$.

Proof. $aH = bH \iff a^{-1}b \in H \iff (a^{-1}b)^{-1} \in H \iff b^{-1}a \in H \iff Ha^{-1} = Hb^{-1}$ ■

Definition 1.1.36. The **index** of subgroup H in G, $[G : H]$, is the number of distinct right (left) cosets of H in G.

Theorem 1.1.37 (Lagrange's theorem)**.** If G is a finite group and $S \leq G$, then $|S|$ divides $|G|$ and $[G : S] = |G|/|S|$, or $|G| = [G : S]|S|$.

Proof. By Corollary 1.1.33, G is partitioned into its right cosets

$$G = St_1 \cup St_2 \cup \cdots \cup St_n,$$

and so $|G| = \sum_{i=1}^{n} |St_i|$. But it is easy to see that $f_i : S \to St_i$, defined by $f_i(s) = st_i$, is a bijection, and so $|St_i| = |S|$ for all i. Thus $|G| = n|S|$, where $n = [G : S]$. ■

Corollary 1.1.38. The order of an element of a finite group divides the order of the group.

Proof. The order of an element a of a group G is equal to the order of the cyclic subgroup $\langle a \rangle$ generated by a. Then apply Lagrange's theorem. ■

Corollary 1.1.39. If p is a prime and $|G| = p$, then G is a cyclic group.

Proof. Take $a \in G$ with $a \neq 1$. Then the cyclic subgroup $\langle a \rangle$ has more than one element (it contains a and 1), and its order $|\langle a \rangle| > 1$ is a divisor of p. Since p is prime, $|\langle a \rangle| = p = |G|$, and so $\langle a \rangle = G$. ■

1.1 EXERCISES

1. By steps i.-iv., prove the equivalence between 1.1.1(1)-(4) and 1.1.1(1),(2)+1.1.2(5):

i. Suppose (1), (2), and (5) are true, show that there exists a left identity element e_l such that $e_l a = a$ for any $a \in G$ and show that there exists a left inverse g_l^{-1} for any $g \in G$ such that $g_l^{-1} g = e_l$.
ii. If there is a left inverse element, then there is a right inverse element, and they are the same.
iii. If there is a left identity element, then there is a right identity element, and they are the same.
iv. Show that (1)-(4) imply (5).

2. [3][1.1 ex9] Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

i. Prove that G is a group under addition.
ii. Prove that the nonzero elements of G are a group under multiplication. (Hint: "Rationalize the denominators" to find multiplicative inverses.)

3. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

4. (Cancellation property): suppose $\cdot$ is an internal binary operation for the set A. We say that the operation - is left-cancellative if $\forall a, b \in A : a \cdot b = a \cdot c \Rightarrow b = c$ and rightcancellative if $\forall a, b \in A : b \cdot a = c \cdot a \Rightarrow b = c$. When the operation is both left and right cancellative we simply say it is cancellative. Show that:

i. The cross product of vectors does not obey cancellation law.
ii. Determine when does matrix multiplication obey the cancellation law.
iii. Given a finite set G with an operation ; prove that if $\cdot$ is right and left cancellative and associative and G is closed under, then G is a group.
iv. Observe that an operation $\cdot$ of a group $(G, \cdot)$ obeys left (right) cancellation law iff each row (column) of its group table has elements of itself distinct.

5. Show that for x in a group G, (1) $|x| = 1 \Leftrightarrow x = e$; (2) $x^{-1} = x \Leftrightarrow x^2 = e$.

6. Show that for x in a group G, (1) $|x| = \left|x^{-1}\right|$; (2) $|x| = n \Rightarrow \left|x^k\right| = \frac{n}{(k,n)}$.

7. Prove Theorem 1.1.15.

8. Prove Theorem 1.1.16.

9. [8][p.27 ex2.11] Let $a \in G$ have order $n = mk$, where $m, k \geq 1$. Prove that a^k has order m.

10. [8][p.27 ex2.12] Show that

i. every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or the Klein-four group $\mathbf{V}$ (see example 1.1.10).
ii. If G is a group with $|G| \leq 5$, then G is abelian.

11. [8][p.27 ex2.13] If $a \in G$ has order n and k is an integer with $a^k = 1$, then n divides k. Indeed, $\left\{k \in \mathbb{Z} : a^k = 1\right\}$ consists of all the multiplies of n.

12. [8][p.27 ex2.14] If $a \in G$ has finite order and $f : G \to H$ is a homomorphism, then the order of $f(a)$ divides the order of a.

13. [8][p.27 ex2.15] Prove that a group G of even order has an odd number of elements of order 2 (in particular, it has at least one such element). (Hint. If $a \in G$ does not have order 2 , then $a \neq a^{-1}$.)

14. [8][p.27 ex2.17]

i. If $a, b \in G$ commute and if $a^m = 1 = b^n$, then $(ab)^k = 1$, where $k = \operatorname{lcm}\{m, n\}$. (The order of ab may be smaller than k; for example, take $b = a^{-1}$.) Conclude that if a and b have finite order, then ab also has finite order.
ii. Let $G = \mathrm{GL}(2, \mathbb{Q})$ and let $A, B \in G$ be given by

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

Show that $A^4 = E = B^3$, but that AB has infinite order.

15. [8][p.27 ex2.19] Prove that two cyclic groups are isomorphic if and only if they have the same order.

16. If $K \leq H \leq G$ with G not necessarily finite, and if $[G : H], [H : K] < \infty$, then $[G : K] < \infty$ and $[G : K] = [H : K][G : H]$.

17. [8][p.27 ex2.16] If $H \leq G$ has index 2,then $a^2 \in H$ for every $a \in G$.

18. Suppose $f : G \to G'$ is a homomorphism, show that $f(\langle X \rangle) = \langle f(X) \rangle$ for any subset $X \subseteq G$.

1.2 More Groups

We will present the following groups in this section: $\mathbb{Z}$, $\mathbb{Z}_n$, and $\mathbb{Z}_n^\times$; cyclic groups; symmetric group S_n and alternating group A_n; dihedral group D_n.

1.2.1 $\mathbb{Z}$, $\mathbb{Z}_n$, and $\mathbb{Z}_n^\times$

Definition 1.2.1 (Congruence)**.** Let $n, a, b \in \mathbb{Z}$. We say a is congruent to b modulo (or just mod) n if $a - b$ is divisible by n. In this case we write

$$a \equiv b \,(\mathrm{mod} n)$$

Observe that $a \sim b \Leftrightarrow a \equiv b (\mathrm{mod} n)$ is an equivalence relation. The equivalence class is denoted as $[a]_n$, $[a]$, or $\bar{a}$, called the **congruence class**. We denote the collection of all equivalence classes $[a]_n$ under $\sim$ as $\mathbb{Z}_n$.

Theorem 1.2.2. Define a binary operation $+$ on $\mathbb{Z}_n$ by $[a]_n + [b]_n = [a+b]_n$. Then $(\mathbb{Z}_n, +)$ is a group.

Proof. First we need to check that this really does define a binary operation on $\mathbb{Z}_n$. The potential problem is that an eqivalence class $[a]_n$ can have lots of different representatives, e.g. $[5]_3 = [2]_3$, but our definition of $+$ seems to depend on a specific choice of representative. Couldn't it be that $[a]_n = [a']$ and $[b]_n = [b']_n$ but $[a+b]_n \neq [a'+b']_n$? If so our definition of $+$ wouldn't work - it would not be "welldefined." We need to check that if $[a]_n = [a']_n$ and $[b]_n = [b']_n$ then $[a+b]_n = [a'+b']_n$. Because $[a]_n = [a']_n$, a and a' are congruent $\mathrm{mod} n$ so $a = a' + kn$ for some integer k, and similarly $b = b' + ln$ for some integer I. Therefore

$$\begin{aligned} a + b &= a' + kn + b' + ln \\ &= a' + b' + (k+l)n \end{aligned}$$

so $a + b \equiv a' + b' \bmod n$ and $[a+b]_n = [a'+b']_n$. The group axioms are easy to check. $[0]_n$ is clearly an identity element, $[-a]_n$ is inverse to $[a]_n$, and because $+$ is associative on $\mathbb{Z}$ we have $[a]_n + ([b]_n + [c]_n) = [a]_n + [b+c]_n = [a+b+c]_n$ and $([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n = [a+b+c]_n$ so

$$[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$$

and $+$ is associative on $\mathbb{Z}_n$. ■

Theorem 1.2.3. $\mathbb{Z}_n$ is a cyclic group and the generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

Proof. To show $\mathbb{Z}_n$ is cyclic, we only need to show that $\mathbb{Z}_n = \langle x \rangle := \{e, x, \cdots, x^{n-1}\}$ for some $x \in \mathbb{Z}_n$. The choice $x = [1]_n$ would work.
We note that $r = 1 + \cdots + 1$ (r times). Let $b = r$ and $a = 1$ in the prop. 1.1.24 and conclude that the order of r is $\frac{n}{d}$ where $d = \gcd(k, n)$. Since the order of r, a generator of $\mathbb{Z}_n$, is n, we see $\frac{n}{d} = n \Rightarrow d = 1$. ■

Example 1.2.4. Let us examine the group $\mathbb{Z}_{16}$. The numbers $1, 3, 5, 7, 9, 11, 13$, and 15 are the elements of $\mathbb{Z}_{16}$ that are relatively prime to 16 . Each of these elements generates $\mathbb{Z}_{16}$. For example,

$$\begin{array}{lll} 1 \cdot 9 = 9 & 2 \cdot 9 = 2 & 3 \cdot 9 = 11 \\ 4 \cdot 9 = 4 & 5 \cdot 9 = 13 & 6 \cdot 9 = 6 \\ 7 \cdot 9 = 15 & 8 \cdot 9 = 8 & 9 \cdot 9 = 1 \\ 10 \cdot 9 = 10 & 11 \cdot 9 = 3 & 12 \cdot 9 = 12 \\ 13 \cdot 9 = 5 & 14 \cdot 9 = 14 & 15 \cdot 9 = 7 \end{array}$$

We can also use the usual multiplication as binary operation on $\mathbb{Z}_n$:

$$[a]_n \times [b]_n = [ab]_n \tag{1.3}$$

Again, we should check that this really defines a binary operation on $\mathbb{Z}_n$: if $[a]_n = [a']_n$ and $[b]_n = [b']_n$ then we need $[ab]_n = [a'b']_n$. This is true because $a = a' + kn$ and $b = b' + \ln$ for some $k, l \in \mathbb{Z}$ so

$$\begin{aligned} ab &= (a' + kn)(b' + ln) \\ &= a'b' + n(kb' + la' + kln) \end{aligned}$$

so $ab \equiv a'b' (\mathrm{mod} n)$ and therefore $[ab]_n = [a'b']_n$. This does not make $(\mathbb{Z}_n, \times)$ into a group, because 0 has no inverse for the operation $\times$.

We notice that $(\mathbb{Z}_n, \times)$ where multiplication $\times$ is given by eq. (1.3) is a monoid with identity $[1]_n$. Therefore, due to Remark 1.1.2, we define $\mathbb{Z}_n^\times$ as the group of units in $\mathbb{Z}_n$, i.e.,

$$\mathbb{Z}_n^\times = \{l \in \mathbb{Z}_n | \gcd(l, n) = 1\}$$

(That's because $[lm]_n = [1]_n \Leftrightarrow lm \equiv 1 \bmod n) \Leftrightarrow \exists q \in \mathbb{Z}$ s.t. $lm - 1 = qn \Leftrightarrow \exists p(= -q) \in \mathbb{Z}$ s.t. $lm + pn = 1$) If $n = p$ is a prime, then

$$\mathbb{Z}_p^\times = \{l \in \mathbb{Z}_n | \gcd(l, p) = 1\} = \{[1], \cdots, [p-1]\}$$

where we note that The greatest common divisor of 0 and any non-zero number is the non-zero number itself (0 is a multiple of every non-zero number).

Example 1.2.5. If G is a cyclic group of order n, i.e., $G \cong \mathbb{Z}_n$, then $\mathrm{Aut}(G) \cong \mathbb{Z}_n^\times$.

Proof. Let $G = \langle x \rangle$ and

$$\begin{aligned} \phi : G &\to G \\ x &\mapsto x^l \end{aligned}$$

for some $0 \leq l \leq n-1$. Thus $\phi(x^j) = x^{lj}$. Every endomorphism (homomorphism with $G \to G$) is of this form, and we wonder what condition on l can make it an automorphism, i.e., also an isomorphism. In fact, ϕ is an isomorphism iff x^l is a generator of G. By theorem 1.2.3, we see this is the case iff $\gcd(n, l) = 1$. Since $\{l \in \mathbb{Z}_n | \gcd(n, l) = 1\} = \mathbb{Z}_n^\times$, we have an isomorphism:

$$\begin{aligned} \Phi : \mathrm{Aut}(G) &\to \mathbb{Z}_n^\times \\ \phi &\mapsto l \text{ where } \phi(x) = x^l \end{aligned}$$

(For $i = 1, 2$, $\phi_i \mapsto l_i \Rightarrow \phi_i(x) = x^{l_i}$, so $\phi_1 \circ \phi_2(x) = \phi_1(x^{l_2}) = x^{l_1 l_2}$.) ■

1.2.2 Cyclic Groups

We begin with definition of **Euler φ-function**. $\varphi(n)$ is defined as the number of non-negative integers less than n that are relatively prime to n. In other words,

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1 \\ |\{l \in \mathbb{Z}_n : \gcd(l, n) = 1\}| = |\mathbb{Z}_n^\times| & \text{if } n > 1 \end{cases}.$$

Lemma 1.2.6. If $G = \langle a \rangle$ is cyclic of order n, then a^k is also a generator of G if and only if $(k, n) = 1$. Thus the number of generators of G is $\varphi(n)$.

Proof. This is just a restatement of Theorem 1.2.3. ■

Lemma 1.2.7. If G is a cyclic group of order n, then there exists a unique subgroup of order d for every divisor d of n.

Proof. If $G = \langle a \rangle$, then $\langle a^{n/d} \rangle$ is a subgroup of order d, by Question 1.1-9. Assume that $S = \langle b \rangle$ is a subgroup of order d (S must be cyclic, by Theorem 1.1.21). Now $b^d = 1$; moreover, $b = a^m$ for some m. By Question 1.1-11, $md = nk$ for some integer k, and $b = a^m = \left(a^{n/d}\right)^k$. Therefore, $\langle b \rangle \leq \langle a^{n/d} \rangle$, and this inclusion is equality because both subgroups have order d. ■

Theorem 1.2.8. If n is a positive integer, then

$$n = \sum_{d|n} \varphi(d),$$

where the sum is over all divisors d of n with $1 \leq d \leq n$.

Proof. If C is a cyclic subgroup of a group G, let $\text{gen}(C)$ denote the set of all its generators. It is clear that G is the disjoint union

$$G = \bigcup \text{gen}(C),$$

where C ranges over all the cyclic subgroups of G. We have just seen, when G is cyclic of order n, that there is a unique cyclic subgroup C_d of order d for every divisor d of n. Therefore, $n = |G| = \sum_{d|n} |\text{gen}\,(C_d)|$. In Lemma 1.2.6, however, we saw that $|\text{gen}\,(C_d)| = \varphi(d)$; the result follows. ■

We now characterize finite cyclic groups.

Theorem 1.2.9 (characterization of cyclic group)**.** A group G of order n is cyclic if and only if, for each divisor d of n, there is at most one cyclic subgroup of G having order d.

Proof. If G is cyclic, then the result is Lemma 1.2.7. For the converse, recall from the previous proof that G is the disjoint union $\cup \text{gen}(C)$, where C ranges over all the cyclic subgroups of G. Hence, $n = |G| = \sum |\,\text{gen}(C)| \leq \sum_{d|n} \varphi(d) = n$, by Theorem 1.2.8. We conclude that G must have a cyclic subgroup of order d for every divisor d of n; in particular, G has a cyclic subgroup of order $d = n$, and so G is cyclic. ■

Observe that the condition in Theorem 1.2.9 is satisfied if, for every divisor d of n, there are at most d solutions $x \in G$ of the equation $x^d = 1$ (two cyclic subgroups of order d would contain more than d solutions).

1.2.3 S_n and A_n

If X is a nonempty set, a **permutation** of X is a bijection $\alpha : X \to X$. We denote the set of all permutations of X by S_X. We will focus on the special case $X = 1, \cdots, n$, where S_X is denoted by S_n. Elements in it is of the form $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{n-1} & \alpha_n \end{smallmatrix}\right)$ where $a_i = \alpha(i)$. S_n is a group, called **symmetric group**, with function composition as multiplication (and we keep the tradition of function composition that permutation of elements is applied from left to right). For example, $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$ and $\beta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ are permutations of $\{1, 2, 3\}$. The product $\alpha\beta$ is $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$. We compute the product by first applying β and then α:

$$\begin{aligned} \alpha\beta(1) &= \alpha(\beta(1)) = \alpha(2) = 2, \\ \alpha\beta(2) &= \alpha(\beta(2)) = \alpha(3) = 1, \\ \alpha\beta(3) &= \alpha(\beta(3)) = \alpha(1) = 3. \end{aligned}$$

Note that $\beta\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$, so that $\alpha\beta \neq \beta\alpha$.

Definition 1.2.10. Let $i_1, i_2, \ldots, i_r$ be distinct integers between 1 and n. If $\alpha \in S_n$ fixes the remaining $n - r$ integers and if

$$\alpha\,(i_1) = i_2, \alpha\,(i_2) = i_3, \ldots, \alpha\,(i_{r-1}) = i_r, \alpha\,(i_r) = i_1,$$

then α is an r**-cycle**; one also says that α is a cycle of **length** r. Denote α by $(i_1\ i_2\ \cdots\ i_n)$. Every 1-cycle fixes every element of X, and so all 1-cycles are equal to the identity. A 2-cycle, which merely interchanges a pair of elements, is called a **transposition**. Observe that $(1\ 2\ 3\ \cdots\ r-1\ r) = (2\ 3\ \cdots\ r\ 1) = (r\ 1\ \cdots\ r-1)$, so there are exactly r such notations for this r-cycle.

Multiplication is easy when one uses the cycle notation. For example, let us compute $\gamma = \alpha\beta$, where $\alpha = (1\ 2)$ and $\beta = (1\ 3\ 4\ 2)$. Since multiplication is composition of functions, $\gamma(1) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(3) = 3$; Next, $\gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4$, and $\gamma(4) = \alpha(\beta(4)) = \alpha(2) = 1$. Having returned to 1, we now seek $\gamma(2)$, because 2 is the smallest integer for which γ has not yet been evaluated. We end up with $(1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$. The cycles on the right are disjoint as defined below.

Definition 1.2.11. Two permutations $\alpha, \beta \in S_X$ are **disjoint** if every x moved by one is fixed by the other. In symbols, if $\alpha(x) \neq x$, then $\beta(x) = x$ and if $\beta(y) \neq y$, then $\alpha(y) = y$ (of course, it is possible that there is $z \in X$ with $\alpha(z) = z = \beta(z)$). A family of permutations $\alpha_1, \alpha_2, \ldots, \alpha_m$ is **disjoint** if each pair of them is disjoint. Observe that for $\alpha = (i_1\ i_2\ \cdots\ i_r)$ and $\beta = (j_1\ j_2\ \cdots\ j_s)$, α and β are disjoint if and only if $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \varnothing$.

The identity of S_n is 1, or (1). To find the inverse of a permutation just write it backwards. If $\tau = (1243)(67)$ then $\tau^{-1} = (76)(3421)$ which can then be rewritten as $\tau^{-1} = (1342)(67)$.

How does one prove this?

First consider a single cycle: $\sigma = (a_1 a_2 \ldots a_k)$. If $b \notin \{a_1, \ldots, a_k\}$, then $\sigma(b) = b$ so $\sigma^{-1}(b) = b$. Thus b shouldn't appear in the inverse. Next $\sigma(a_i) = a_{i+1}$ so $\sigma^{-1}(a_{i+1}) = a_i$. Thus if $\sigma : a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \mapsto a_1$, then $\sigma^{-1} : a_k \mapsto a_{k-1} \mapsto a_{k-2} \mapsto \cdots \mapsto a_1 \mapsto a_k$. This is precisely the cycle $(a_k, a_{k-1} \ldots, a_2, a_1)$ which is nothing more than σ written backwards.

Now what about a list of cycles? Say $\sigma = \sigma_1 \cdots \sigma_\ell$. Recall that $\sigma^{-1} = (\sigma_1 \cdots \sigma_\ell)^{-1} = \sigma_\ell^{-1} \cdots \sigma_1^{-1}$. So we reverse the list of cycles and then write each one backwards – thus the inverse is just the whole thing written backwards.

One thing to note: This still works even if σ is not written in terms of disjoint cycles.

Proposition 1.2.12. If α and β are disjoint permutations, then $\alpha\beta = \beta\alpha$; that is, α and β commute.

Proof. See [4] Proposition 5.8. ■

Now we present results for factorization or permuations.

Theorem 1.2.13. Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.

Proof. see [8] Theorem 1.1. ■

Theorem 1.2.14. Every permutation $\alpha \in S_n$ is a product of transpositions.

Proof. By Theorem 1.2.13, it is enough to factor cycles: for $n > 1$,

$$\sigma = (a_1\ \ldots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \ldots (a_1\ a_2)$$

■

One can prove that the parity of the number of factors is the same for all factorizations of a permutation a that is, the number of transpositions is always even or odd. We say that a permuation is **even** if it has even parity and is **odd** if it has odd parity. See [8] p.8-9 for more of this.

Corollary 1.2.15. A cycle $\sigma = (a_1\ \ldots\ a_n)$ is even if and only if n is odd.

One of the most important subgroups of S_n is the set of all even permutations, A_n. The group A_n is called the alternating group on n letters.

Theorem 1.2.16. The set A_n is a subgroup of S_n.

Proof. Since the product of two even permutations must also be an even permutation, A_n is closed. The identity is an even permutation and therefore is in A_n. If σ is an even permutation, then

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r$$

where σ_i is a transposition and r is even. Since the inverse of any transposition is itself,

$$\sigma^{-1} = \sigma_r\sigma_{r-1}\cdots\sigma_1$$

is also in A_n. ■

Proposition 1.2.17. The number of even permutations in $S_n, n \geq 2$, is equal to the number of odd permutations; hence, the order of A_n is $n!/2$.

Proof. Let A_n be the set of even permutations in S_n and B_n be the set of odd permutations. If we can show that there is a bijection between these sets, they must contain the same number of elements. Fix a transposition σ in S_n. Since $n \geq 2$, such a σ exists. Define

$$\lambda_\sigma : A_n \to B_n$$

by

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Suppose that $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Then $\sigma\tau = \sigma\mu$ and so

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Therefore, λ_σ is one-to-one. The proof that λ_σ is surjective is left as an exercise. ■

Example 1.2.18 (Subgroups of A_4)**.** The group A_4 is the subgroup of S_4 consisting of even permutations. There are twelve elements α_1-α_{12} in A_4: an identity α_1, three permutations written as products of two disjoint cycles α_2-α_4 (each of them having order 2), and eight cycles α_5-α_{12} fixing one element (each of them having order 3). We have the Cayley table of A_4 below (In this table, an entry k inside the table represents α_k. For example, $\alpha_3\alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

We will find all subgroups of A_4: since the order of $H \leq A_4$ must divide the order of A_4 and $|A_4| = 12 = 1\times 12 = 3\times 4 = 2\times 6$, we see H can have size $1, 2, 3, 4, 6, 12$. H with $|H| = 1$ and 12 are just trivial subgroup and A_4 itself. Thanks to Question 10, we already know the classification of all groups with size smaller than 6: subgroups H with $|H| = 2, 3, 5$ are isomorphic to $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ and H with $|H| = 4$ is isomorphic either to $\mathbb{Z}_4$ or $\mathbf{V}$. There is no subgroup of order 6 (proved in the following lemma).

By observations about α_2-α_4 and α_5-α_{12} we made in the beginning, we see subgroups of order 2 are just $\langle\alpha_2\rangle, \cdots, \langle\alpha_4\rangle$; and subgroups of order 3 are just $\langle\alpha_5\rangle, \cdots, \langle\alpha_{12}\rangle$. Since there is no element with order 4 in A_4, subgroup H of order 4 can only be $\mathbf{V}$, which is contained in A_4 as $\{\alpha_1, \cdots, \alpha_4\}$. Our classification is complete.

Lemma 1.2.19. There is no subgroup of index 2 in A_4.

Proof. Suppose a subgroup H of A_4 has index 2, i.e., $|H| = 6$. We will show for each $g \in A_4$ that $g^2 \in H$. If $g \in H$ then clearly $g^2 \in H$. If $g \notin H$ then gH is a left coset of H different from H (since $g \in gH$ and $g \notin H$), so from $[G : H] = 2$ the only left cosets of H are H and gH. Which one is g^2H ? If $g^2H = gH$ then $g^2 \in gH$, so $g^2 = gh$ for some $h \in H$, and that implies $g = h$, so $g \in H$, but that's a contradiction. Therefore $g^2H = H$, so $g^2 \in H$. Every 3-cycle $(a\ b\ c)$ in A_4 is a square: (abc) has order 3, so $(a\ b\ c) = (a\ b\ c)^4 = \left((a\ b\ c)^2\right)^2$. Thus H contains all 3-cycles in A_4, in total 8 of them, which thus contradicts to $|H| = 6$. ■

1.2.4 D_n

We from example 1.2.18 see that the Klein-four group $\mathbf{V}$ is a subgroup of A_4 and is thus a subgroup of S_4. We remarked in example 1.1.10 that $\mathbf{V}$ is isomorphic to D_2. We call subgroups of S_n **permuation groups**. In last subsection, we examined alternating groups A_n; now we examine another type of permuation groups, the dihedral groups D_n. Such groups consist of the rigid motions of a regular n-sided polygon or n-gon. For $n = 3, 4, \ldots$, we define the **n-th dihedral group** to be the group of rigid motions of a regular n-gon. We will denote this group by D_n. We can number the vertices of a regular n-gon by $1, 2, \ldots, n$. Notice that there are exactly n choices to replace the first vertex. If we replace the first vertex by k, then the second vertex must be replaced either by vertex $k + 1$ or by vertex $k - 1$; hence, there are $2n$ possible rigid motions of the n-gon. We summarize these results in the following theorem.

Theorem 1.2.20. The dihedral group, D_n, is a subgroup of S_n of order $2n$.

Theorem 1.2.21 (Dihedral group)**.** The group $D_n, n \geq 3$, consists of all products of the two elements r and s, where r has order n and s has order 2, and these two elements satisfy the relation $(sr)^2 = 1$.

Proof. The possible motions of a regular n-gon are either reflections or rotations (Figure 1.1).

There are exactly n possible rotations:

$$\text{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

We will denote the rotation $360^\circ/n$ by r. The rotation r generates all of the other rotations. That is,

$$r^k = k \cdot \frac{360^\circ}{n}$$

Label the n reflections $s_1, s_2, \ldots, s_n$, where s_k is the reflection that leaves vertex k fixed. There are two cases of reflections, depending on whether n is even or odd. If there are an even number of vertices, then two vertices are left fixed by a reflection, and $s_1 = s_{n/2+1}, s_2 = s_{n/2+2}, \ldots, s_{n/2} = s_n$. If there are an odd number of vertices, then only a single vertex is left fixed by a reflection and $s_1, s_2, \ldots, s_n$ are distinct (Figure 1.2).

In either case, the order of each s_k is two. Let $s = s_1$. Then $s^2 = 1$ and $r^n = 1$. Since any rigid motion t of the n-gon replaces the first vertex by the vertex k, the second vertex must be replaced by either $k + 1$ or by $k - 1$. If the second vertex is replaced by $k + 1$, then $t = r^k$. If the second vertex is replaced by $k - 1$, then $t = r^k s$. Hence, r and s generate D_n. That is, D_n consists of all finite products of r and s,

$$D_n = \left\{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\right\}.$$

We will leave the proof that $(sr)^2 = 1$ as an exercise. ■

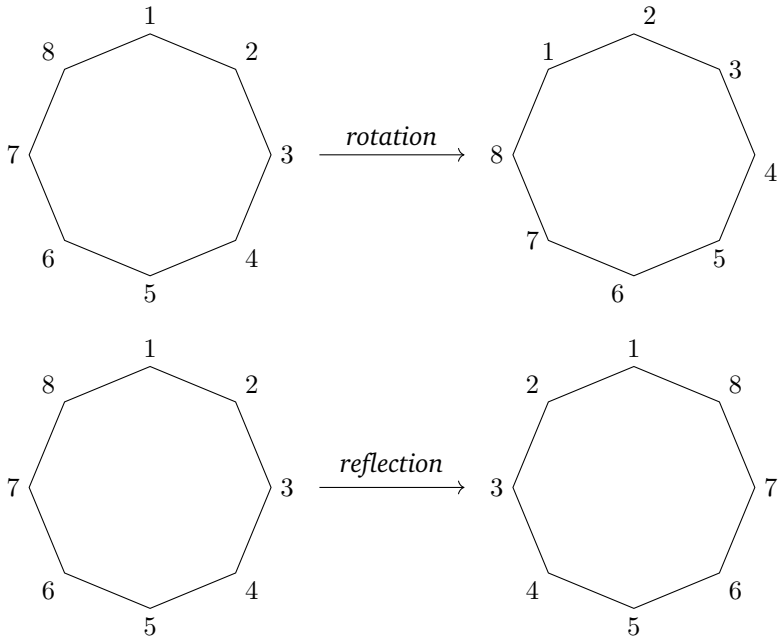


Figure 1.1: Rotations and reflections of a regular n-gon

Example 1.2.22. The group of rigid motions of a square, D_4, consists of eight elements. With the vertices numbered 1,2,3,4 (Figure 1.3), the rotations are

$$\begin{aligned} r &= (1\ 2\ 3\ 4) \\ r^2 &= (1\ 3)(2\ 4) \\ r^3 &= (1\ 4\ 3\ 2) \\ r^4 &= (1) \end{aligned}$$

and the reflections are

$$\begin{aligned} s_1 &= (2\ 4) \\ s_2 &= (1\ 3). \end{aligned}$$

The order of D_4 is 8. The remaining two elements are

$$\begin{aligned} rs_1 &= (12)(34) \\ r^3 s_1 &= (14)(23). \end{aligned}$$

A Supplementary Note

One can also analyze group of symmetry of solids. For example, group of rigid motions of a cube is S_4 (Figure 1.4) (see [4] Theorem 5.27). For more on this, including the Planotic solids, see [1] section 6.12.

1.2 EXERCISES

1. If $1 \leq r \leq n$, then there are $(1/r)[n(n-1)\dots(n-r+1)]$ r-cycles in S_n.

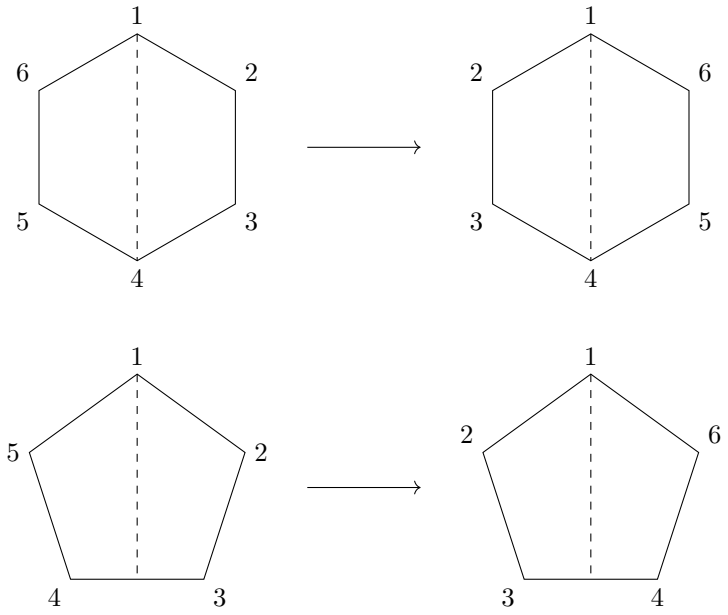


Figure 1.2: Types of reflections of a regular n-gon

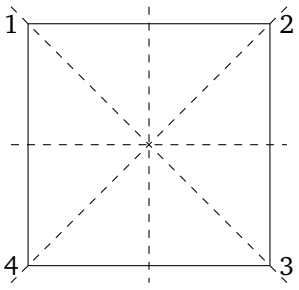


Figure 1.3: The group D_4

2. If $\alpha, \beta \in S_n$ are disjoint and $\alpha\beta = 1$, then $\alpha = 1 = \beta$.

3. Let $\alpha \in S_n$ for $n \geq 3$. If $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$, prove that α must be the identity permutation; hence, the center of S_n is the trivial subgroup (the center of a group G is defined as $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$.)

4. If $\sigma \in A_n$ and $\tau \in S_n$, show that $\tau^{-1}\sigma\tau \in A_n$.

5. Let $\tau = (a_1, a_2, \ldots, a_k)$ be a cycle of length k.

i. Prove that if σ is any permutation, then

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

is a cycle of length k.

ii. Let μ be a cycle of length k. Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.

6. [8][p.24 ex2.9]

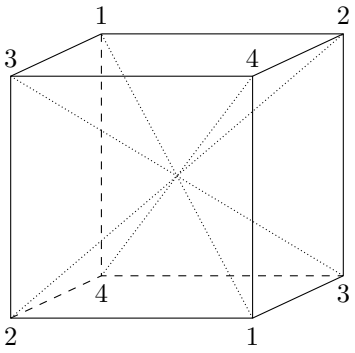


Figure 1.4: cube

i. Prove that S_n can be generated by $(1\ 2), (1\ 3), \cdots, (1\ n)$.
ii. Prove that S_n can be generated by $(1\ 2), (2\ 3), \cdots, (i\ i+1), \cdots, (n-1\ n)$.
iii. Prove that S_n can be generated by the two elements $(1\ 2)$ and $(1\ 2\ \cdots n)$.

7. Draw group tables of S_2 and S_3.

8. [8][p.5 ex1.12]

i. Let $\alpha = \begin{pmatrix} i_0 & i_1 & \dots & i_{r-1} \end{pmatrix}$ be an r-cycle. For every $j, k \geq 0$, prove that $\alpha^k (i_j) = i_{k+j}$ if subscripts are read modulo r.
ii. Prove that if α is an r-cycle, then $\alpha^r = 1$, but that $\alpha^k \neq 1$ for every positive integer $k < r$.
iii. If $\alpha = \beta_1 \beta_2 \dots \beta_m$ is a product of disjoint r_i-cycles β_i, then the smallest positive integer l with $\alpha^l = 1$ is the least common multiple of $\{r_1, r_2, \dots, r_m\}$. Therefore, the order of a permutation $\alpha = \beta_1 \cdots \beta_t$, where β_i is an r_i-cycle, is $\operatorname{lcm}\{r_1, \cdots, r_t\}$.

9. By previous question, deduce that each order-3 cycle is a product of 3-cycles.

10. Dihedral group.

i. Show that $D_n = \langle r, s | r^n, s^2, (sr)^2 \rangle = D_n = \langle r, s | r^n, s^2, (rs)^2 \rangle$, that is, $r^n = 1, s^2 = 1, (sr)^2 = 1$ iff $r^n = 1, s^2 = 1, (rs)^2 = 1$.
ii. Show that $r^k s = s r^{-k}$ in D_n.
iii. Prove that the order of $r^k \in D_n$ is $n / \gcd(k, n)$.

11. Show that there is an index-2 subgroup of Dihedral group D_n.

1.3 Normal Subgroups and Quotient Groups

Definition 1.3.1. Subgroup $H \leq G$ is **normal**, denoted as $H \trianglelefteq G$, if $\forall g \in G,\ gHg^{-1} \subseteq H$.

Note that $gHg^{-1} = \{ghg^{-1} | h \in H\} \leq G$, as $ghg^{-1}(gh'g^{-1})^{-1} \in gHg^{-1}$.

Example 1.3.2.

- If G is an abelian group, then every subgroup of G is normal. The converse is false: see Question 1.3-4.
- $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$: for $A \in \mathrm{GL}(n, \mathbb{R}), B \in \mathrm{SL}(n, \mathbb{R})$ we have $\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(A^{-1}) = 1$.

Proposition 1.3.3 (characterization of normal subgroup)**.** If $H \leq G$, then the following are equivalent.

1. $H \trianglelefteq G$;
2. $\forall g \in G,\ gHg^{-1} = H$;
3. $\forall g \in G,\ Hg = gH$;
4. Every right coset of H is a left coset;
5. Every left coset of H is a right coset.

Proof. 1 equiv to 2: the $\Leftarrow$ direction is clear. Conversely, suppose $\forall g \in G,\ gHg^{-1} \subseteq H$, so $g^{-1}H(g^{-1})^{-1} \subseteq H \implies g^{-1}Hg \subseteq H$. Multiply from left and right to cancel, so $H \subseteq gHg^{-1}$. So $gHg^{-1} = H$.

2 equiv to 3: $\forall g \in G,\ gHg^{-1} = H \iff \forall g \in G, h \in H$, there is some $h' \in H$ such that $h' = ghg^{-1} \iff \forall g \in G, h \in H, \exists h' \in H$ s.t. $h'g = gh$.

We prove that 3,4,5 are equivalent.

3 implies 4: we note that 3 is directly stronger than 4, as 4 can be rephrased as: for a right coset Hg, there is some $g' \in G$ such that $Hg = g'H$.

4 implies 3: Suppose $Hg = aH$ for some a. But then $g \in Hg = aH$, and $g \in gH$. So $aH = gH \implies Hg = gH$.

3 implies 5 implies 3: similarly. ■

Corollary 1.3.4. Any subgroup of index 2 in any group G is normal.

Proof. $[G : H] = 2 \implies$ two distinct left cosets, H, aH where $a \notin H$. Similarly, H and Ha are distinct right cosets. This gives $H \cap aH = \varnothing, H \cap Ha = \varnothing$, so by 4 in proposition 1.3.3, H is normal. ■

If $N \trianglelefteq G$, then the set of cosets of N in G, G/N, form a group under multiplication $(aN)(bN) = abN$. We need to check that

- Well-defined: $aN = a'N$ and $bN = b'N \implies abN = a'b'N$:

$$\begin{aligned} NaNb &= Na\left(a^{-1}Na\right)b \quad \text{(because } N \text{ is normal)} \\ &= N\left(aa^{-1}\right)Nab = NNab = Nab \quad \text{(because } N \leq G\text{)}. \end{aligned}$$

  Thus, $NaNb = Nab$, and so the product of two cosets is a coset.

- Group properties easily follow from the group properties of G (associativity, identity $N = N1 = 1N$, and inverse $a^{-1}N$ $(= Na^{-1})$ for aN $(= Na)$.)

Proposition 1.3.5. If $N \trianglelefteq G$, then the **natural map**, or **canonical projection** (i.e., the function $q : G \to G/N$ defined by $q(a) = Na$) is a surjective homomorphism with kernel N.

Proof. The equation $q(a)q(b) = q(ab)$ is just the formula $NaNb = Nab$; hence, q is a homomorphism. If $Na \in G/N$, then $Na = q(a)$, and so v is surjective. Finally, $q(a) = Na = N$ if and only if $a \in N$, so that $N = \ker(q)$. ■

We define conjugation $\gamma_a : G \to G$, where $\gamma_a(x) = axa^{-1}$, and call $\gamma_a(x) = axa^{-1}$ a **conjugate of** x in a group G, also denoted as x^a. Moreover, for $g \in G$ we set

$$H^g := gHg^{-1}$$

and say that H^g is a **conjugate of** H in G (more precisely, the conjugate of H by g). For any $K \subseteq G$ set

$$H^K := \left\{ H^k \mid k \in K \right\}.$$

We have now shown in Proposition 1.3.5 that every normal subgroup is the kernel of some homomorphism. Different homomorphisms can have the same kernel. For example, if $a = (1\ 2)$ and $b = (1\ 3)$, then $\gamma_a, \gamma_b : S_3 \to S_3$ are distinct and $\ker(\gamma_a) = 1 = \ker(\gamma_b)$.

The quotient group construction is a generalization of the construction of $\mathbb{Z}_n$ from $\mathbb{Z}$. Recall that if n is a fixed integer, then $[a]$, the congruence class of $a \bmod n$, is the coset $a + \langle n \rangle$. Now $\langle n \rangle \trianglelefteq \mathbb{Z}$, because $\mathbb{Z}$ is abelian, and the quotient group $\mathbb{Z}/\langle n \rangle$ has elements all cosets $a + \langle n \rangle$, where $a \in \mathbb{Z}$, and operation $(a + \langle n \rangle) + (b + \langle n \rangle) = a + b + \langle n \rangle$; in congruence class notation, $[a] + [b] = [a + b]$. Therefore, the quotient group $\mathbb{Z}/\langle n \rangle$ is equal to $\mathbb{Z}_n$, the group of integers modulo n. An arbitrary quotient group G/N is often called $G \bmod N$ because of this example.

1.3 EXERCISES

1. [8][p.31 ex2.29]

i. (H. B. Mann). Let G be a finite group, and let S and T be (not necessarily distinct) nonempty subsets. Prove that either $G = ST$ or $|G| \geq |S| + |T|$.
ii. Prove that every element in a finite field F is a sum of two squares.

2. [8][p.31 ex2.32] If $H \leq G$, then $H \trianglelefteq G$ if and only if, for all $x, y \in G, xy \in H$ if and only if $yx \in H$.

3. [8][p.31 ex2.33] If $K \leq H \leq G$ and $K \trianglelefteq G$, then $K \trianglelefteq H$.

4. Every subgroup of an abelian group is normal. This exercise shows that the converse is not true: Let G be the subgroup of $\mathrm{GL}(2, \mathbb{C})$ generated by

$$A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

i. Find the order of A and B in G.
ii. Show G has order 8 by listing all the elements of G. Show G is is not abelian.
iii. List all elements of oder 2 in G.
iv. Show that every subgroup of G is normal.

5. If N, H_1, H_2 are subgroups of a group G such that $N \trianglelefteq G$ and $H_1 \trianglelefteq H_2$, then show $NH_1 \trianglelefteq NH_2$.

6. Prove that $A_n \trianglelefteq S_n$ for every n by showing that it is an index-2 subgroup (thus $|A_n| = \frac{1}{2}n!$).

7. [8][p.31 ex2.37]

i. The intersection of any family of normal subgroups of a group G is itself a normal subgroup of G. Conclude that if X is a subset of G, then there is a smallest normal subgroup of G which contains X; it is called the normal subgroup generated by X (or the normal closure of X; it is often denoted by $\langle X \rangle^G$).
ii. If $X = \varnothing$, then $\langle X \rangle^G = 1$. If $X \neq \varnothing$, then $\langle X \rangle^G$ is the set of all words on the conjugates of elements in X.
iii. If $gxg^{-1} \in X$ for all $x \in X$ and $g \in G$, then $\langle X \rangle = \langle X \rangle^G \trianglelefteq G$.

8. [8][p.31 ex2.38] If $H, K \trianglelefteq G$, then $\langle H \cup K \rangle \trianglelefteq G$.

9. Suppose $f : G \to G'$ is a homomorphism. Show that $N \trianglelefteq G \Rightarrow f(N) \trianglelefteq G'$; $N' \trianglelefteq G' \Rightarrow f^{-1}(N') \trianglelefteq G$.

10. Finite product (see Definition 1.4.3) and finite intersection of normal subgroups of G are still normal.

11. Suppose $H \leq G$ and $N \trianglelefteq G$. Show that $H \cap N \trianglelefteq H$ but not necessarily $H \cap N \trianglelefteq G$ Also note that $H \leq N \trianglelefteq G$ does *not* imply $H \trianglelefteq G$; not even $H \trianglelefteq N \trianglelefteq G$ implying $H \trianglelefteq G$. Show such transitivity of normality fails by the counterexample that $K = \langle (1\ 2)(3\ 4) \rangle \trianglelefteq \mathbf{V}$ and $\mathbf{V} \trianglelefteq S_4$ while K is not a subgroup of S_4.

12. (Product formula) If S and T are subgroups of a finite group G, then $|ST||S \cap T| = |S||T|$.

13. Show that conjugacy is an equivalence relation, that is, $x \sim y \iff \exists g \in G$ s.t. $y = x^g := gxg^{-1}$ defines an equivalence relation. We call the equivalence class with respect to this relation **conjugacy class**. Use this definition to show that a subgroup $H \leq G$ is normal if and only if it is a union of conjugacy classes of G.

1.4 Isomorphism Theorems

Facts (proofs are left as exercises): for a group homomorphism $\phi : G \to G'$,

1. $\ker(\phi) := \{a \in G | \phi(a) = e_{G'}\} \trianglelefteq G$
2. $\mathrm{Im}(\phi) := \{\phi(a) | a \in G\} \leq G'$

Theorem 1.4.1 (1st Isomorphism Theorem)**.** If $f : G \to G'$ is a group homomorphism and $K = \ker(f)$ (so $K \trianglelefteq G$), then

$$G/K \cong \mathrm{Im}(f)$$

Proof. Define $\phi : G/K \to \mathrm{Im}(f)$ by $\phi(aK) = f(a)$. ϕ is well-defined and injective: $aK = bK \iff a^{-1}b \in K = \ker(f) \iff f(a^{-1}b) = f(a)^{-1}f(b) = e \iff f(b) = f(a)$. ϕ is a homomorphism: $\phi(a\ker(f)b\ker(f)) = \phi(ab\ker(f))$ since kernel is normal group and that is $f(ab)$. On the other side, $\phi(a\ker(f))\phi(b\ker(f)) = f(a)f(b)$, so this is homomorphism since f is homomorphism. Lastly, ϕ is surjective: if $b \in \mathrm{Im}(f)$, then $b = f(a)$ for some a. So $\phi(a\ker(f)) = b$. ■

Example 1.4.2. $\mathrm{SL}(n, \mathbb{R}) \trianglelefteq \mathrm{GL}(n, \mathbb{R})$. Then $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \simeq (\mathbb{R} - \{0\}, \cdot)$.

Proof. $f : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R} - \{0\}, A \mapsto \det(A)$. This is a group homomorphism, f is surjective, $\ker(f) = \mathrm{SL}(n, \mathbb{R}) \implies \mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \simeq \mathbb{R} - \{0\}$. ■

Definition 1.4.3. For $H, K \leq G$, define **product set**

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

and **inverse set**

$$H^{-1} = \left\{h^{-1} | h \in H\right\}$$

Remark 1.4.4.

1. HK is not necessarily a subgroup of G. For example, consider $G = S_3$ and $H = \{e, (1\ 2)\}$, $K = \{e, (1\ 3)\}$. We have Proposition 1.4.5 (same as [8] Lemma 2.25) instead.
2. Observe that $(AB)^{-1} = B^{-1}A^{-1}$.

Proposition 1.4.5. Let A and B be subgroups of G. Then AB is a subgroup of G if and only if $AB = BA$.

Proof. From $AB \leq G$ we get

$$(AB) = (AB)^{-1} = B^{-1}A^{-1} = BA.$$

If $AB = BA$, then

$$(AB)(AB) = A(BA)B = A(AB)B = AABB = AB$$

and

$$(AB)^{-1} = B^{-1}A^{-1} = BA = AB.$$

Thus $AB \leq G$. ■

Proposition 1.4.6. If $H \leq G$ and $N \trianglelefteq G$, then $HN \leq G$, $HN = NH$, and HN is the subgroup of G generated by $H \cup N$.

Proof. $HN \leq G$: If $a = h_1n_1, b = h_2n_2$, then $ab^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}h_2n_1n_2^{-1}h_2^{-1}$. Clearly, $n_1n_2^{-1} \in N$ so $h_2n_1n_2^{-1}h_2^{-1} \in N$. Thus, $ab^{-1} \in HN$.

$HN = NH$: We need to first show $HN \subseteq NH$. Let $hn \in HN \implies hnh^{-1} = n' \in N \implies hn = n'h \in NH$, so $HN \subseteq NH$. Similar for other direction.

Clearly, $H, N \subseteq HN \leq G$. And for any $K \leq G$, let $H, N \subseteq K$. Since K is a subgroup, $\forall n \in N, h \in H, hn \in K$. Thus $HN \leq K$ is the smallest subgroup. In particular, HN is the subgroup generated by $H \cup N$. ■

Theorem 1.4.7 (2nd Isomorphism Theorem)**.** Let $H \leq G, N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$ and

$$H/H \cap N \simeq HN/N$$

Proof. $H \cap N \trianglelefteq H$ due to Question 1.3-11. Let $\phi : H \to HN/N$ be given by $\phi(h) = hN$. The result follows from the first isomorphism theorem after showing the following three facts. We left them as exercises.

- $\ker(\phi) = \{h \in H | hN = N\} = H \cap N$.
- ϕ is surjective: $hnN = hN = \phi(h)$.
- ϕ is homomorphism.

■

Suppose $H_2 \subseteq H_1, H_1, H_2 \trianglelefteq G$. Then we can define a surjective map called the **enlargement of coset**:

$$\phi : \frac{G}{H_2} \to \frac{G}{H_1}; aH_2 \mapsto aH_1$$

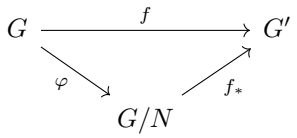
It is well-defined: if $aH_2 = bH_2 \Leftrightarrow b^{-1}a \in H_2 \subseteq H_1 \Rightarrow b^{-1}a \in H_1 \Leftrightarrow aH_1 = bH_2$, then $\phi\left(aH_2\right) = \phi\left(a'H_2\right)$. It is a homomorphism: $\phi\left(aH_2\right)\phi\left(bH_2\right) = \left(aH_1\right)\left(bH_1\right) = aH_1 = \phi\left(abH_2\right)$. It is surjective: for every $aH_1 \in \frac{G}{H_1}$, we have $\phi\left(aH_2\right) = aH_1$. Therefore, by 1st isomorphism theorem, $\frac{G}{H_2}/\operatorname{Ker}(\phi) \cong \frac{G}{H_1}$, so G/H_1 is a quotient of G/H_2.

Remark 1.4.8.

(1) Now, let G be a group and $N \trianglelefteq G$. Let $f : G \to G'$ be a homomorphism whose kernel $K = \ker(f)$ contains N. Then we have a composition

$$f_* = \psi \circ \phi : \frac{G}{N} \to \frac{G}{K} \to G'; aN \mapsto aK \mapsto f(a)$$

where $\psi : G/K \to G'$ is the homomorphism from the 1st isomorphism theorem and $\phi : G/N \to G/K$ is the enlargement of coset. This composition g is the unique homomorphism $f_* : G/N \to G'$, said to be **induced by** f, making the following diagram commutative:



As before, φ is the canonical projection.

(2) Now, let G again be a group. Let $f : G \to G'$ be a homomorphism. Consider $N' \trianglelefteq G'$ and $N := f^{-1}(N') \trianglelefteq G$ instead (the normality is justified by Proposition 1.4.14). Consider the composition

$$g = q \circ f : G \to G' \to \frac{G'}{N'}$$

in replace of the homomorphism f in the above commutative diagram, where $q : G' \to G'/N'$ is the canonical projection. Observe that $K = \ker(g) = \{x \in G | f(x) \in N'\} = f^{-1}(N') = N$, so the enlargement $\phi : G/N \to G/K$ degenerates to the identity homomorphism i and the induced map $g_* : \frac{G}{N} \to \frac{G}{K} \to \frac{G'}{N'}; aN \mapsto aK \mapsto g(a)$ becomes the homomorphism in the first isomorphism theorem $g_* = \psi : \frac{G}{N} \to \frac{G'}{N'}; aN \to g(a)$. The map is then injective as ψ is injective.

Theorem 1.4.9 (3rd Isomorphism Theorem)**.** Suppose $K \leq N \trianglelefteq G$ and $K \trianglelefteq G$. Then

$$N/K \trianglelefteq G/K \text{ and } (G/K)/(N/K) \simeq G/N$$

Proof. First part follows from definition. Application of the first isomorphism theorem to the enlargement of coset map $\phi : G/K \to G/N$, $\phi(gK) = gN$ will prove the second part (check that $\ker(\phi) = N/K$ and ϕ is surjective). ■

Restating the proof that $\phi : G/K \to \mathrm{Im}(f)$, defined in the first isomorphism theorem, is well-defined, we get

Proposition 1.4.10 ([1] Proposition 2.7.1)**.** Let K be the kernel of a homomorphism $\varphi : G \to G'$. Let $b \in G'$, then $\varphi^{-1}(b)$ is called a **fiber**. If $a \in \varphi^{-1}(b)$, then $\varphi^{-1}(b) = aK$, the coset of K containing a. These cosets partition the group G, and they correspond to elements of the image of φ:

$$G/K \longleftrightarrow \mathrm{Im}(\varphi)$$
$$aK \longleftrightarrow \varphi(a)$$

Since $|G/K| = [G : K]$ for finite group G, and $|G/K| = |\mathrm{Im}(\varphi)|$ by the above proposition, we immediately have

Corollary 1.4.11 ([1] Corollary 2.8.13)**.** Let $\varphi : G \to G'$ be a homomorphism of finite groups. Then

- $|G| = |\ker(\varphi)| \cdot |\mathrm{Im}\,\varphi|$;
- $|\ker(\varphi)|$ divides $|G|$;
- $|\mathrm{Im}(\varphi)|$ divides both $|G|$ and $|G'|$.

Proposition 1.4.12. Let $\varphi : G \to G'$ be a homomorphism and $H \leq G$. Then the restriction $\varphi|_H : H \to G'$ is also a homomorphism with $\ker(\varphi|_H) = \ker(\varphi) \cap H$ and $\mathrm{Im}(\varphi|_H) = \varphi(H)$.

Remark 1.4.13. By Corollary 1.4.11, we see $|\mathrm{Im}\,\varphi_H| = |\varphi(H)|$ divides $|H|$ and $|G'|$. Therefore, if $|H|$ and $|G'|$ have no common factors, then $|\varphi(H)| = 1 \implies \varphi(H) = e_{G'} \implies \varphi$ is a trivial homomorphism. [1] Example 2.10.3 gives an application of this observation on the sign homomorphism from S_n to $\{\pm 1\} \cong \mathbb{Z}_2$. This will require some readings in permutation matrices that define the sign homomorphism ([1] handles the sign of permutation in a neater way than [8] does).

Proposition 1.4.14 ([1] Proposition 2.10.4)**.** Let $\varphi : G \to \mathcal{G}$ be a homomorphism with kernel K and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Denote the inverse image $\varphi^{-1}(\mathcal{H})$ by H. Then H is a subgroup of G that contains K. If $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$, then H is a normal subgroup of G. If φ is surjective and if H is a normal subgroup of G, then $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$.

Theorem 1.4.15 (4th Isomorphism Theorem (Correspondence Theorem))**.** Let $N \trianglelefteq G$, then $\phi : G \to G/N, \phi(g) = gN$ induces a 1-1 correspondence $\Phi : H \to \phi(H) = H/N$ between subgroups of G which contain N and subgroups of G/N:

$$\begin{aligned} \mathcal{S} = \{\text{subgroups of } G \text{ that contain } N\} &\longleftrightarrow \mathcal{S}' = \{\text{subgroups of } G/N\} \\ \text{a subgroup } H \text{ of } G \text{ that contains } N &\longrightarrow \text{its image } \phi(H) = H/N \text{ in } G/N \\ \text{its inverse image } \phi^{-1}(\mathcal{H}) \text{ in } G &\longleftarrow \text{a subgroup } \mathcal{H} \text{ of } G/N \end{aligned}$$

Moreover, if we denote H/N by H^*, then

- For $H_{1,2} \in \mathcal{S}$, $H_1 \leq H_2$ if and only if $H_1^* \leq H_2^*$, and then $[H_2 : H_1] = [H_2^* : H_1^*]$;
- For $H_{1,2} \in \mathcal{S}$, $H_1 \trianglelefteq H_2$ if and only if $H_1^* \trianglelefteq H_2^*$, and then $H_2/H_1 \cong H_2^*/H_1^*$.

Remark 1.4.16. For the proof of the above theorem, see [8] Theorem 2.28. Also note that [1] Theorem 2.10.5 relaxes the assumption to surjective homomorphism ϕ while getting less interesting results than the case ϕ being the canonical projection.

1.4 EXERCISES

1. [8][p.31 ex2.29] Prove that a homomorphism $f : G \to H$ is an injection if and only if $\ker(f) = 1$.
2. [8][p.37 ex2.48] (Modular Law). Let A, B, and C be subgroups of G with $A \leq B$. If $A \cap C = B \cap C$ and $AC = BC$ (we do not assume that either AC or BC is a subgroup), then $A = B$.
3. [8][p.37 ex2.49] (Dedekind Law). Let H, K, and L be subgroups of G with $H \leq L$. Then $HK \cap L = H(K \cap L)$ (we do not assume that either HK or $H(K \cap L)$ is a subgroup).

1.5 Simple and Solvable Groups

Definition 1.5.1. A group G is called **simple** if it has no normal subgroup other than $\{e\}$ and G.

Example 1.5.2. If G is finite and abelian, then G is simple iff G is cyclic of prime order. (*proof later*).

Example 1.5.3. Consider the alternating group A_n. By Question 1.3-6, we see $A_n \trianglelefteq S_n$.

$A_2 = \{e\}$ is simple. $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ is cyclic of prime order 3 and is thus simple (apply previous example). A_4 is *not* simple: $\mathbf{V}$ is normal in A_4 because it is the union of conjugacy classes in A_4 (see Question 1.5-1 and Question 1.3-13).

Theorem 1.5.4. A_n is simple if $n \geq 5$

Proof. The proof is made up of the following three facts:

(1) $A_n, n \geq 5$ is generated by 3-cycles;

(2) Every two 3-cycles are conjugate with each other in A_n: σ_1, σ_2 are 3-cycles, then $\exists \tau \in A_n : \tau\sigma_1\tau^{-1} = \sigma_2$.;

(3) every normal subgroup $N \neq \{e\}$ in A_n has at least one 3-cycle.

Together they prove the statement: suppose $N \neq \{e\}$, and we want to show $N = A_n$. (3) gives a 3-cycle $\sigma_1 \in N$, so $\forall \tau \in A_n$, $\tau\sigma_1\tau^{-1} = \sigma_2 \in N$ as $N \trianglelefteq A_n$. (2) then implies that all 3-cycles are in N. (1) states that $A_n = \langle \text{3-cycles} \rangle$ is the smallest subgroup of A_n containing all 3-cycles, so $N \trianglelefteq A_n$ has to be equal to A_n.

We prove the three facts:

(1): $T = \{(a\,b\,c) \mid 1 \leq a < b < c \leq n\} \subset A_n$, then $\langle T \rangle \subset A_n$. If

$$\sigma = (a\,b)(c\,d) = \begin{cases} e, & \text{if } \{a,b\} = \{c,d\} \\ (a\,c\,b)(a\,c\,d), & \text{if } a,b,c,d \text{ all distinct} \\ (a\,d\,b) & \text{if } a = c \end{cases}$$

Then $\sigma \in \langle T \rangle \implies A_n \subseteq T$.

(2) is due to a more general theorem, namely Theorem permutations are conjugate iff they have the same cycle structure.

(3): See Exercise 1.5-2. ■

Theorem 1.5.5. Permutations $\alpha, \beta \in S_n$ are conjugate if and only if they have the same cycle structure.

Proof. See [8] Theorem 3.5 or Math5031 HW3 Q4. ■

Theorem 1.5.6. Jordan-Holder Theorem. If G is any finite group, then there is a unique tower of subgroups

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

such that N_i/N_{i-1} is simple.

Definition 1.5.7. A **tower of subgroups**

$$G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G_0 = G$$

is **subnormal** if $G_{i+1} \trianglelefteq G_i$ and **normal** if furthermore $G_i \trianglelefteq G$ for each i. A subnormal series is called **abelian** if each G_i/G_{i+1} is abelian. A group G is called **solvable** if there is an abelian series

$$\{e\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 \leq G_0 = G.$$

Example 1.5.8.

- Any abelian group is solvable.
- S_3 is solvable.
- S_4 is solvable.
- $S_n, n \geq 5$ is not solvable.
- D_n is not simple and is solvable.

Proof.

- For an abelian group G, any $N \leq G$ is normal and abelian, so $N/\{e\}$ is abelian. The factor group G/N is abelian because the natural homomorphism $\phi : G \to G/N$ is surjective.
- $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$. Question 1.3-6 gives $|A_3| = \frac{1}{2}3! = 3$ which is prime, so $A_3 \cong \mathbb{Z}_3$ is abelian. It is also normal in S_3 with index 2, so $S_3/A_3 \cong Z_2$ is abelian.

- Solvablility of S_4 is due to $\{e\} \trianglelefteq \mathbf{V} \trianglelefteq A_4 \trianglelefteq S_4$. $A_4 \trianglelefteq S_n$ and S_4/A_4 abelian. $\mathbf{V} \trianglelefteq A_4$ (see example 1.5.3) and $\mathbf{V}/\{e\}$ is abelian.
- Let $N \trianglelefteq S_n$. Since $A_n \trianglelefteq S_n$, by 2nd isomorphism theorem, $N \cap A_n \trianglelefteq A_n$. Since A_n for $n \geq 5$ is simple, we see $N \cap A_n = \{e\}$ or A_n.

  If $N \cap A_n = A_n$, then $A_n \leq N \leq S_n \implies N = A_n$ or $N = S_n$ because Question 1.1-16 implies $2 = [S_n : A_n] = [S_n : N][N : A_n]$.

  If $N \cap A_n = \{e\}$ and if $N \neq \{e\}$, then: $\sigma_1, \sigma_2 \neq e, \sigma_1, \sigma_2 \in N$, then $\sigma_1\sigma_2 \in N$, and $\sigma_1\sigma_2 = e$ because $\sigma_1\sigma_2$ is even (so $\sigma_1\sigma_2$ is also in A_n). Thus $N = \{e, \sigma, \sigma^{-1}\}$ and $\sigma^2 = \sigma^{-1}$. σ has order 3, which by Question 1.2-9 implies that it is a product of 3-cycles. But by parts (1) and (2) of theorem 1.5.4, we see $N = A_n$. Therefore, $N = \{e\}, N$, or $S_n \implies S_n, n \geq 5$ is not solvable.
- The index-2 subgroup in Question 1.2-11 is the cyclic subgroup generated by the rotation $\langle r \rangle$ and is thus abelian and is also normal in D_n due to corollary 1.3.4. Then $\{e\} \trianglelefteq \langle r \rangle \trianglelefteq D_n$ is the desired abelian subnormal series as $D_n/\langle r \rangle$ is a group of order 2, isomorphic to $\mathbb{Z}_2$.

■

Definition 1.5.9. Let $x, y \in G$. The **commutator** of $x, y := xyx^{-1}y^{-1} = [x, y]$

Note that $[x, y] = e \iff xy = yx$, and $[x, y]^{-1} = [y, x]$. This gives us a notion of how far a group is from abelian.

Definition 1.5.10. G', the **commutator subgroup**, is the subgroup generated by all the commutators $[x, y]$, where $x, y \in G$. $G' = \{[x_1, y_1][x_2, y_2] \cdots [x_k, y_k] \mid x_i, y_i \in G\}$

Proposition 1.5.11.

- $G' = \{e\} \iff G$ is ableian
- $G' \trianglelefteq G$
- G/G' is abelian

Proof. Insert gg^{-1} between the elements: $g[xy]g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}] \in G'$.

Similarly, $g[x_1, y_1] \cdots [x_k, y_k]g^{-1} = (g[x_1, y_1]g^{-1}) \cdots (g[x_k y_k]g^{-1})$

G/G' is abelian: we want to show that $abG' = baG'$. $a^{-1}b^{-1}ab = [a^{-1}, b^{-1}] \in G'$. So it is true. ■

Proposition 1.5.12. If $N \trianglelefteq G$, then G/N is abelian $\iff G' \leq N$

Proof. $\implies$: $\forall a, b \in G, G/N$ abelian so $a^{-1}b^{-1}N = b^{-1}a^{-1}N$. Then $aba^{-1}b^{-1} \in N \implies [a, b] \in N \implies G' \leq N$

$\impliedby$: $a^{-1}b^{-1}ab = [a^{-1}, b^{-1}] \in G' \subseteq N \implies a^{-1}b^{-1}ab \in N$ ■

Example 1.5.13. $(S_n)' = A_n$. See Question 1.5-3.

Let $G^{(0)} := G, G^{(1)} = G', \cdots, G^{(i)} = (G^{(i-1)})'$. $G^{(i+1)} \trianglelefteq G^{(i)}$ and $G^{(i+1)}/G^{(i)}$ is abelian.

Proposition 1.5.14. G is solvable iff $G^{(m)} = \{e\}$ for some $m \geq 1$.

Proof. $\impliedby$: $\{e\} = G^{(m)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G$ is an abelian tower.

$\implies$: If $\{e\} = G_m \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$ is abelian, then $G_1 \trianglelefteq G_0, G_0/G_1$ abelian $\implies G' \leq G_1, G_2 \trianglelefteq G_1, G_1/G_2$ abelian $\implies (G_1)' \leq G_2$ implies together that $G^{(2)} \leq G_1' \leq G_2 \implies G^{(2)} \leq G_2$.

By induction, $G^{(i)} \leq G_i \forall i, G^{(m)} \leq G_m = \{e\}$. ■

The following proposition is a good exercise (Math5031 HW2 Q4) for one to review all the isomorphism theorems and various normality theorems.

Proposition 1.5.15. If $N \trianglelefteq G$, then $N, G/N$ are solvable $\iff$ G is solvable.

Proof. G **solvable** $\implies$ N **solvable**:
Let

$$\{e\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

be a subnormal series where G_i/G_{i+1} is abelian. Let $N_i = N \cap G_i$. We claim that

$$\{e\} = N \cap \{e\} = N_m \trianglelefteq N_{m-1} \trianglelefteq \cdots N_0 = N \cap G = N$$

is the desired subnormal series where N_i/N_{i+1} is abelian.

We apply Question 1.3-11 three times: $G_i \leq G, N \trianglelefteq G \Rightarrow N_i = G_i \cap N \trianglelefteq G_i$ and $G_{i+1} \trianglelefteq G_i \Rightarrow N_i \cap G_{i+1} = N_{i+1} \trianglelefteq G_{i+1}$. Similarly, $N_i \trianglelefteq G_i$ with the third application to $N_i \trianglelefteq G_i, N_{i+1} \trianglelefteq G_{i+1}$, which implies $N_i \cap N_{i+1} = N_{i+1} \trianglelefteq N_i$.

Applying Remark 1.4.8 (2) with homomorphism the inclusion of N_i in G_i, $f = \iota : N_i \hookrightarrow G_i$, $N' = G_{i+1}$, and $N = \iota^{-1}(G_{i+1}) = N_i \cap G_{i+1} = N_{i+1}$, we obtain an injective homomorphism $g_* : N_i/N_{i+1} \to G_i/G_{i+1}$. Thus G_i/G_{i+1} being abelian implies N_i/N_{i+1} being abelian (note that injectivity is necessary for this implication: $\varphi(xy) = \varphi(x)\varphi(y) \overset{\text{abelian codomain}}{=\!=\!=} \varphi(y)\varphi(x) = \varphi(yx) \overset{injectivity}{\implies} xy = yx$).

G/N **solvable** $\implies$ G/N **solvable**:
Let

$$\{e\} = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

be a normal series where each G_i/G_{i+1} is abelian. Let $H_i = NG_i/N$. Proposition 1.4.6 implies that $NG_{i+1} = G_{i+1}N, NG_i = G_iN$. Notice that $N \subseteq G_{i+1}N \trianglelefteq G_iN$ due to Question 1.3-5. Since $N \subseteq G_{i+1}N \trianglelefteq G_iN, N \trianglelefteq G_iN$, the 3rd isomorphism theorem states that

$$H_{i+1} = \frac{NG_{i+1}}{N} \trianglelefteq \frac{NG_i}{N} = H_i$$

The remaining is to show $\frac{H_i}{H_{i+1}}$ is abelian: first observe that

$$(*): \quad G_iN = G_i\left(G_{i+1}N\right)$$

and then

$$\frac{H_i}{H_{i+1}} = \frac{\frac{NG_i}{N}}{\frac{NG_{i+1}}{N}} \overset{3rd\text{ iso}}{\cong} \frac{G_iN}{G_{i+1}N} \overset{(*)}{=} \frac{G_i\left(G_{i+1}N\right)}{G_{i+1}N} \overset{2nd\text{ iso}}{\cong} \frac{G_i}{G_i \cap G_{i+1}N}$$

where each of the isomorphism theorem's conditions are satisfied (the only nontrivial relationship is $G_{i+1}N \trianglelefteq G_iN$ and is proved above).

$$3^{\text{rd}} : N \subseteq G_{i+1}N \trianglelefteq G_iN, N \trianglelefteq G_iN.$$
$$2^{\text{nd}} : G_i \leq G_iN, G_{i+1}N \trianglelefteq G_iN.$$

By enlargement of coset map and $G_{i+1} \subseteq G_i \Rightarrow G_{i+1} \subseteq G_i \cap G_{i+1}N$, we see $\frac{G_i}{G_i \cap G_{i+1}N}$ is isomorphic to a quotient of $\frac{G_i}{G_{i+1}}$, which is abelian, so $\frac{G_i}{G_i \cap G_{i+1}N}$ is abelian (quotient of abelian group is abelian because the canonical projection is a surjective homomorphism).

G/N **solvable and** N **solvable** $\implies$ G **solvable**:
N and G/N are solvable $\Rightarrow$ G is solvable. Suppose

$$\{e\} = N_m \trianglelefteq N_{m-1} \trianglelefteq \cdots \trianglelefteq N_0 = N$$
$$\left\{e_{G/N}\right\} = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_0 = \frac{G}{N}$$

Then by 4th isomorphism theorem, for each H_i which is a subgroup of $\frac{G}{N}$, we can find a unique subgroup K_i of G containing N such that $\frac{K_i}{N} = H_i$. Then

$$\{e\} = N_m \trianglelefteq N_{m-1} \trianglelefteq \cdots \trianglelefteq N_0 = N = K_n \trianglelefteq K_{n-1} \trianglelefteq \cdots \trianglelefteq K_0 = G$$

The fact $K_{i+1} \trianglelefteq K_i$ is from properties of the 1 -1 correspondence $\Phi : \{K : A \subseteq K \leq G\} \leftrightarrow \{\bar{A} = \frac{A}{N} : \frac{A}{N} \leq \frac{G}{N}\}$. Recall that $A \subseteq B \Leftrightarrow \bar{A} \subseteq \bar{B}$ and $A \trianglelefteq G \Leftrightarrow \bar{A} \trianglelefteq \bar{G}$ where A and B are two subgroups containing N. By the two properties we see

$$K_n \subseteq K_{n-1} \subseteq \cdots \subseteq K_0$$
$$\forall i : K_i \trianglelefteq G$$

Also note that $p \geq q \Rightarrow K_p \leq K_q$. That's because $K_p \subseteq K_q$ and $K_p \leq G$. Thus for each $i = 1$, $K_2 \leq G, K_2 \subseteq K_1 \trianglelefteq K_0 = G \Rightarrow K_2 = K_2 \cap K_1 \trianglelefteq K_1$. We set induction hypothesis that $K_{i+1} \trianglelefteq K_i$ then have $K_{i+2} \leq K_i, K_{i+2} \subseteq K_{i+1} \trianglelefteq K_i \Rightarrow K_{i+2} = K_{i+2} \cap K_{i+1} \trianglelefteq K_{i+1}$. The induction establishes the series as normal. We now show that K_i/K_{i+1} is abelian due to the third isomorphism theorem (conditions are satisfied: $N = K_0 \subseteq K_{i+1} \trianglelefteq K_i, N = K_0 \trianglelefteq K_i$):

$$\frac{K_i}{K_{i+1}} \cong \frac{\frac{K_i}{N}}{\frac{K_{i+1}}{N}} = \frac{H_i}{H_{i+1}}$$

Therefore, G is also solvable. ■

Remark 1.5.16. The proof of a more general nature can be seen in [5] 6.1.1 and 6.1.2, but need an equivalence proof (6.1.5) of their first definition of solvability and the definition we used in class (or used by Serge Lang). 6.1.1 shows that subgroups and homomorphic images of solvable groups are solvable, which implies the $\Rightarrow$ direction of the above statement, because N is normal subgroup of G and G/N is the homomorphic image of the map $\psi : G \to \frac{G}{N}; x \mapsto xN$.

1.5 EXERCISES

1. If G is a group, by a conjugacy class of G we mean all elements of G which are conjugate to a fixed element (so it is an orbit of G for the action of G on G by conjugation).

i. Find all conjugacy classes of A_4.
ii. Show that if $[G : Z(G)] = n$, then every conjugacy class has at most n elements.

2. Use the following steps to show every normal subgroup $N \neq \{e\}$ of $A_n, n \geq 5$, contains a 3-cycle. This finishes the proof of the fact that A_n is simple if $n \geq 5$.

i. Show that if N contains a permutation of the form $\sigma = (1\ 2\ \cdots\ r)\mu$ (where μ is a product of cycles disjoint from $\{1, 2, \ldots, r\}$) with $r \geq 4$, then N contains a 3-cycle by letting $\rho = (1\ 2\ 3)$ and computing $\sigma^{-1}\rho^{-1}\sigma\rho$.
ii. Show that if N contains a permutation of the form $\sigma = (1\ 2\ 3)(4\ 5\ 6)\mu$ (where μ is a product of cycles disjoint from $\{1, 2, \ldots, 6\}$), then N contains a 3-cycle by letting $\rho = (1\ 2\ 4)$ and computing $\sigma^{-1}\rho^{-1}\sigma\rho$.
iii. Show that if N contains a permutation of the form $\sigma = (1\ 2\ 3)\mu$, where μ is a product of 2-cycles a product of 2-cycles which are mutually disjoint and are also disjoint form $\{1, 2, 3\}$, then N contains a 3-cycle by computing σ^2.
iv. Show that if N contains a permutation of the form $\sigma = (1\ 2)(3\ 4)\mu$, where μ is a product of 2-cycles which are mutually disjoint and are also disjoint from $\{1, 2, 3, 4\}$, then N contains a 3-cycle by letting $\rho = (1\ 2\ 3)$, computing $\eta = \sigma^{-1}\rho^{-1}\sigma\rho$ and $\zeta = (1\ 5\ 2)\eta(1\ 2\ 5)$.

Remark: This problem divides into three subcases: (1) the cycle has length ≥ 4 (corresponded to **i**); (2) the cycle has length ≤ 3 (but with at least on of them being 3) (corresponded to **ii** and **iii**); (3) the cycle has length ≤ 2 (corresponded to **iv**). WLOG, each case can be converted to the considerations of the explicit forms given in the above problem.

3. The commutator subgroup of S_n is A_n (Hint: show that every 3-cycle is a commutator, and use the fact that A_n is generated by 2-cycles.)

4. (A simple group of infinite order) Let A_∞ be defined in the following way: identify A_{n-1} with the subgroup of A_n consisting of those permutations which fixes n, and let A_∞ be the union $\bigcup_{n\geq 1} A_n$.

i. Show that A_∞ is a group.
ii. Prove A_∞ is a simple group.

1.6 Group Actions

Definition 1.6.1. Let G be a group and X be a set, an **action of G on X** is a function $\alpha : G \times X \to X, (g, x) \mapsto g \cdot x$ such that

- $e \cdot x = x$, $\forall x \in X$.
- $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, $\forall x_1, x_2 \in X, g \in G$

Note that $\forall g \in X,\ L_g : X \to X,\ x \mapsto g \cdot x$ is a permutation. L_g is bijective, as $g \cdot x = g \cdot x' \implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot x') \implies e \cdot x = e \cdot x'$. Besides, $\forall x \in X, L_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = x$.

A group action $G \curvearrowright X$ gives rise to a homomorphism $\phi : G \to S_X,\ g \mapsto L_g$ (not necessarily injective): $\phi(g_1 g_2)(x) = (g_1 g_2) \cdot x = \phi(g_1)(g_2 \cdot x) = \phi(g_1) \circ \phi(g_2)(x)$.

Example 1.6.2.

1. Trivial action. $\forall g \in G, x \in X, g \cdot x = x$.
2. Conjugation on elements of G. $X = G, g \cdot x = gxg^{-1}$.
3. Conjugation on subgroups of G. Let X be set of subgroups of G, $g \in G, H \in X$. Then $g \cdot H = gHg^{-1} \leq G$ (for $a, b \in gHg^{-1}$, $a = ghg^{-1}, b = gh'g^{-1} \implies ab = g(hh')g^{-1}$.)
4. G acts on G by translation. $X = G, g \cdot x = gx$.

Definition 1.6.3. Suppose G acts on $X, x \in X$. Then the **stabilizer** is defined as

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

It is a subgroup of G because

- $e \in G_x$;
- $g \in G_x$ then $g \cdot x = x \Rightarrow x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x \Rightarrow g^{-1} \in G_x$.
- $g, g' \in G_x \Rightarrow (gg') \cdot x = g(g'x) = gx = x$.

Definition 1.6.4. We also define an **orbit** of X.

$$O_x = \{gx \,\big|\, g \in G\} \subseteq X$$

Note: $x \sim y$ if $y \in O_x$, so $y = gx$ for some g. Thus, any two orbits are either equal or disjoint, and they form a partition of X.

Example 1.6.5. For Example 1.6.2 above, the stabilizer and orbit are

1. $G_x = G, O_x = \{x\}$.
2. $G_x = \{g \in G \mid gx = xg\}$, $O_x = \{gxg^{-1} \mid g \in G\}$, the conjugacy class of x in G.
3. O_H = all subgroups conjugate to H, $G_H = \underbrace{\{g \in G \mid gHg^{-1} = H\}}_{\text{normalizer}} \leq H$
4. $G_x = \{g \in G \mid gx = x\} = \{e\}, O_x = \{gx \mid g \in G\} = G$

Definition 1.6.6. As mentioned above, the **normalizer** of H in G is

$$H \trianglelefteq N_G(H) = \{g \in G \mid gH = Hg\} \leq G$$

It is the largest subgroup of G in which H is normal.

Definition 1.6.7. An action is **transitive** if there is only one orbit, $O_x = X$. Equivalently, $\forall x, y \in X$, $\exists g \in G$ s.t. $g \cdot x = y$.

Theorem 1.6.8 (Orbit-Stabilizer Theorem)**.** Let X be a G-set, then $\forall x \in X$,

$$|O_x| = [G : G_x], \text{ or } |G| = |O_x||G_x|$$

Proof. Define $\psi : O_x \to$ set of left cosets of G_x, $gx \mapsto gG_x$.

Well-defined (since we can't make sure $gx = gx' \implies x = x$): $gx = g'x \iff x = g^{-1}g'x \iff g^{-1}g' \in G \iff gG_x = g'G_x$.

Surjective: clear. ■

Definition 1.6.9. For group G, the **center** of G, $Z(G)$, is defined as

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

Proposition 1.6.10.

- $Z(G) = G \iff G$ abelian
- $Z(G) \trianglelefteq G$

Proof. The first statement is trivial.

$Z(G) \leq G$: $e \in Z(G)$. $g \in Z(G) \Rightarrow g^{-1} \in Z(G)$ as $g'g^{-1} = g^{-1}g'$, and if $g_1, g_2 \in Z(G)$ then $g_1g_2g' = g_1g'g_2 = g'(g_1g_2)$ so $g_1g_2 \in Z(G)$.

$Z(G) \trianglelefteq G$: let $g \in Z(G)$ and $h \in G$. We want to show that $hgh^{-1} \in Z(G)$. $\underline{hgh^{-1}}g' = h\underline{h^{-1}g}g' = gg'$ but $g'\underline{hg}h^{-1} = g'\underline{gh}h^{-1} = g'g$. Since $hgh^{-1}g' = g'hgh^{-1}$ we see $gg' = g'g$. ■

Example 1.6.11. $Z(S_n) = \{e\}, n \geq 3$. This is a nontrivial fact. $Z(A_n) = \{e\}, n \geq 4$. That's because for $n \geq 5$, A_n is simple but $Z(A_n) \trianglelefteq Z(A_n) = \{e\}$ or $Z(A_n) = A_n$. For $n = 4$, find an element not commuting with any element in the Klein-four group $\mathbf{V}$.

Example 1.6.12. If G acts on its subgroups in conjugation, $H \leq G$,

$$| \underbrace{O_H}_{\text{subgps conj to } H} | = [G : N_G(H)] \qquad N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Theorem 1.6.13 (Burnside's Lemma)**.** If G, X finite, X is a G-set, then the number of orbits of the action $G \curvearrowright X$ is $\frac{1}{|G|}\sum_{g\in G}|F_g|$, where F_g is the set of elements of X fixed by g.

Proof. Consider $S = \{(g,x) \mid gx = x\} \subset G \times X$. We can count S in two different ways.

1. $\forall g \in G$, there are $|F_g|$ elements fixed by g so $|S| = \sum_{g\in G}|F_g|$.
2. $\forall x \in X$, there are $|G_x|$ elements of X fixed in x, which equals $|G|/[O_x]$.

So $\sum_{g\in G}|F_g| = \sum_{x\in X}\frac{|G|}{|O_x|} = |G|\sum_{\text{distinct orbits } O_x}\frac{1}{|O_x|}|O_x| = |G| \times$ num orbits in X ■

Corollary 1.6.14. If G acts transitively on X, and $|X| > 1$, then there is $g \in G$ such that $F_g = \varnothing$. In other words, $\forall x, y \in X, \exists g$ s.t. $gx = y$. Equivalently, X has 1 orbit.

Proof. Burnside's Lemma gives $|G| = \sum_{g\in G}|F_g| = F_e + \sum_{g\neq e}|F_g|$.

If $|F_g| \geq 1 \forall g$, then $|G| = |X| + \sum_{g\neq e}|F_g| \geq |X| + (|G| - 1) \implies |X| \leq 1$, a contradiction. ■

Class Formula is obtained by letting G acts on G via conjugation. If $x \in G = X$,

$$G_x = \underbrace{\{g \in G \mid gx = xg\}}_{N(x)} \leq G, \quad O_x = \{gxg^{-1} \mid g \in G\}$$

O_x gives a partition of G. So $|G| = \sum_{\text{distinct orbits}}|O_x| = \sum_{\text{distinct orbits}}[G : G_x = N(x)]$

$|O_x| = 1 \iff x \in Z(G)$. So we can write that summing all distinct conjugacy class with more than 1 elements.

$$|G| = Z(G) + \sum[G : G_x]$$

Corollary 1.6.15. If $|G| = p^r$, p prime, then $Z(G) \neq \{e\}$.

Proof. Since $|G| = |Z(G)| = \sum[G : G_x]$, so if $Z(G) = \{e\}$, we get $p^r = 1 + \sum\frac{|G|}{|G_x|}$. where $|G|/|G_x| > 1$ and is a divisor of $|G| = p^r$. This implies that $p \mid 1$, a contradiction $\implies Z(G) \neq 1$ ■

Corollary 1.6.16. If $|G| = p^2$, then G is ableian.

Proof. If G is not abelian, then $|Z(G)| = p$, so $Z(G)$ is proper subgroup of G. Pick $a \in G - Z(G)$, then $N(a) = \{b \mid ab = ba\} \neq G$. However $Z(G)$ is proper subgroup of $N(a)$ and $N(a)$ proper subgroup of G, a contradiction (a in $N(a)$ but not in $Z(G)$).

[1] 7.3.4 claims that G with $|G| = p^2$ is either cyclic or a product of two cyclic groups of order p. ■

Corollary 1.6.17. If $|G| = p^r$, then G is solvable.

Proof. Proof by induction on r, $r = 1$ true.

Suppose this holds for $1, ..., r-1$. Consider $Z(G) \trianglelefteq G$ and $Z(G) \neq \{e\}$. Here $|Z(G)|$ and $|G/Z(G)|$ are powers of p. So by hypothesis, $Z(G)$ and $|G/Z(G)|$ solvable $\implies G$ also solvable. ■

1.6 EXERCISES

1. [8][p.45 ex3.5] Prove that $Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$.

2. [8][p.45 ex3.6]

i. Prove, for every $a, x \in G$, that $C_G\left(axa^{-1}\right) = aC_G(x)a^{-1}$.
ii. Prove that if $H \leq G$ and $h \in H$, then $C_H(h) = C_G(h) \cap H$.

3. [8][p.45 ex3.9]

i. Prove that $N_G\left(aHa^{-1}\right) = aN_G(H)a^{-1}$.
ii. If $H \leq K \leq G$, then $N_K(H) = N_G(H) \cap K$.
iii. If $H, K \leq G$, prove that $N_G(H) \cap N_G(K) \leq N_G(H \cap K)$. Give an example in which the inclusion is proper.

1.7 Sylow Theorems

Suggestion: read through [1] Chapter 7, which includes many additional topics aside from a good guide through Sylow theorems; for classification of simplicity and solvability of group with order less than 60, see Math5031 HW4.

Theorem 1.7.1. Suppose $|G| = p^r m$, $r \geq 1$, $\gcd(p, m) = 1$. Then G has a subgroup of size p^s for any $0 \leq s \leq r$.

Lemma 1.7.2. If G is abelian and $p \mid |G|$, then G has a subgroup of order p.

Proof. Induction on order of G. If $|G| = p$, there is nothing to prove. Suppose $|G| > p$, Let $e \neq a \in G, t = ord(a)$. Then $H = \langle a \rangle = \{e, a, \cdots, a^{t-1}\} \leq G$, so $p^r m = |G| = |H|[G : H] = t \cdot k$. There are two cases:

1. If $p \mid t$, then $\left|\left\langle a^{\frac{t}{p}} \right\rangle\right| = p$.
2. Otherwise, let $n = |G|, n = tn'$ so $p \mid n' = |G/H| < n$. So, by induction hypothesis, G/H has subgroup of order p, so has an element $\bar{b}$ of order p. Consider the canonical projection $\phi : G \to G/H$, so if $\phi(b) = \bar{b}$, then $p \mid ord(b)$. So we can apply case 1 to b and get a subgroup of order p due to the following remark.

■

Remark 1.7.3. If $\phi : G \to G'$ is a group homomorphism and $g \in G$ and $ord(\phi(g)) \mid \underbrace{ord(g)}_{m}$, so $g^m = e \to \phi(g)^m = e$. $(a^k = e \implies ord(a) \mid k)$

Proof of theorem. Recall that class formula states that when G acts on G by conjugation, $|G| = |Z(G)| + \sum[G : G_x]$, summing over distinct orbits with more than 1 element.

Fix p induction on G. If $|G| = p$, we are done. Now, let's have two cases where (1) $p \mid |Z(G)|$ and (2) p doesn't divide $|Z(G)|$.

In case 1, by lemma, $Z(G)$ has subgroup H of order p. Since $H \leq Z(G)$ and $Z(G) \trianglelefteq G$, we get $H \trianglelefteq G$ so G/H is a group of size $p^{r-1}m$. So by induction hypothesis G/H has a subgroup of order s for all $0 \leq s \leq r-1$. Any subgroup of G/H is K/H for $H \leq K \leq G$. So $|H| = p, |K/H| = p^s \implies |K| = p^{s+1}$. So this holds for $1 \leq s+1 \leq r$.

In case 2, G is not abelian, and we make two subcases.

1. Suppose $\forall x \notin Z(G), p \mid [G : G_x]$. This case is not possible since $p \mid |G|$ and p doesn't divide $Z(G)$

2. $\exists x \in Z(G), p \nmid [G : G_x] = |G|/|G_x| \implies p^r \mid |G_x|$, and $|G_x| < |G|$. By induction hypothesis, G_x and therefore G has a subgroup of $p^s, 0 \leq s \leq r$.

■

Definition 1.7.4. A group G is a **p-group** if $|G| = p^r$. So $\forall e \neq a \in G, p \mid ord(a)$. And if $|G| = p^r m, gcd(m, p) = 1$, $H \leq G$, then H is a **p-subgroup** if $|H| = p^s$, and H is a **p-sylow subgroup** if $|H| = p^r$.

Theorem 1.7.5. If $p \mid |G|$, then

1. Every p subgroup is contained in a $p-$sylow subgroup.
2. Any two $p-$sylow subgroups are conjugate.
3. If $r =$ number of p-sylow subgroups, then $r \mid |G|$ and $r \equiv 1 \mod p$

Proposition 1.7.6. If H is a p-subgroup and P is a sylow p-subgroup, then H is contained in a conjugate of P: $\exists g \in G, H \leq gP^{-1}g$

Implication: The proposition shows the first and second part of them.

Part 1. $|gPg^{-1}| = |P|$, so the conjugate is also a sylow P-sylow ■

Part 2. P, P' sylow, then $\exists g$ s.t. $P' \subseteq gPg^{-1}$. Then $|gPg^{-1}| = |P| = p^r$ and $|P'| = r \implies P' = gPg^{-1}$.

■

Proposition Proof. Let S be the set of conjugates of P and H acts on S by conjugation, so that $h \cdot gPg^{-1} := hgPg^{-1}h^{-1}$. Then $S = \sum_{\text{distinct orbits}} |O_s| =$ number of fixed points $+ \sum_{\text{distinct w/ size}>1} |O_s|$.

Now the goal is to show that there $\exists$ a fixed point. Since $|O_s| = [H : H_s]$ and $|H| = p^s$, then $p \mid |O_s|$.

Here, $|S| = [G : N_G(P)] \implies |S| = \frac{|G|}{|N_G(P)|}$. Since $P \trianglelefteq N_G(P) \leq G$ and $p^r \mid |N_G(P)|$, I get $p \nmid |S|$ and so $p^r \mid |N_G(P)|$.

Let gPg^{-1} be a fixed point. Then $\forall h \in H, hgPg^{-1}h^{-1} = gPg^{-1} \implies P = g^{-1}h^{-1}gPg^{-1}hg \implies P = g^{-1}h^{-1}gP(g^{-1}h^{-1}g)^{-1} \implies g^{-1}h^{-1}g \in N_G(P)$. So $\forall h \in H \implies g^{-1}Hg \subseteq N_G(P)$.

Let $K = g^{-1}Hg$, $K, P \leq N_G(P)$ and $P \trianglelefteq N_G(P)$.

So by the second isomorphism theorem, $KP/P \simeq K/K \cap P \implies |KP| = \frac{|P||K|}{|K \cap P|}$ and $|KP| \mid |G|$, and $|P||K|$ is a power of $p \implies \frac{|K|}{|K \cap P|} = 1 \implies K \subseteq P \implies g^{-1}Hg \subseteq P \implies H \subseteq gPg^{-1}$. ■

Part 3 Proof. By part 2, $r =$ number of all conjugates of $P = [G : N_G(P)]$, and $[G : N_G(P)] \mid |G|$.

To show $r \equiv 1 \mod p$, let $H = P$ from proof of the proposition, so that $r =$ number of fixed points + a multiple of p

If gPg^{-1} is a fixed point, then by the proof $P \subseteq gPg^{-1}$, but $|P| = |gPg^{-1}|$ so $P = gPg^{-1}$. So only one fixed point $\implies r \equiv 1 (mod\, p)$ ■

Note: $r = 1 \iff gPg^{-1} = P \, \forall g \in G \iff P \trianglelefteq G$

Corollary 1.7.7. If $|G| = pq$ where p, q are distinct primes and $p \not\equiv 1 (\mod q)$ and $q \not\equiv 1 (\mod p)$. Then G is cyclic.

Example 1.7.8. $|G| = 33 = 3 \times 11$. $3 - 1 = 2$ is relatively prime with 11; $11 - 1 = 10$ is relatively prime with 3. Therefore, $G \cong \mathbb{Z}_{33}$ due to above corollary.

Proof. Let r_1 be the number of sylow p-subgroups and r_2 be the number of sylow q-subgroups. Then $r_1 \mid pq, r_1 \equiv 1 \mod p \implies r_1 = 1$, and similarly $r_2 = 1$

If $H_1, H_2 \leq G$ with $|H_1| = p$ and $|H_2| = q$, then by the note, $H_1, H_2 \trianglelefteq G$.

$H_1 = \{e, a, ..., a^{p-1}\} = \langle a \rangle, H_2 = \{e, b, ..., b^{q-1}\} = \langle b \rangle$. For $aba^{-1} \in H_2$ and $ba^{-1}b^{-1} \in H_1$, $aba^{-1}b^{-1} \in H_1 \cap H_2 = \{e\} \implies ab = ba \implies ord(ab) \in \{1, p, q, pq\}$. So $(ab)^p = a^p b^p = b^p \neq e \implies ord(ab) = pq \implies G = \langle ab \rangle$. ■

Several observations in summary:

1. Any abelian group is solvable.
2. group with prime order is cyclic, abelian, and thus solvable.
3. group with prime order is simple because for $H \leq G$ we have $|H||G| = p \Rightarrow |H| = 1$ or $|H| = p$.
4. A simple group is solvable iff it is abelian.

Our goal is to show the following theorem:

Theorem 1.7.9. Any group of order < 60 is solvable (note that $|A_5| = 60$).

Our plan:

(1) G prime order $\overset{obs(2)}{\implies}$ we're done.

(2) G not prime order. We want to find a nontrivial $N \trianglelefteq G$ s.t. $N, G/N$ are solvable, which then implies that G is solvable as we proved in last section.

We can also show, for example,

Theorem 1.7.10. If $|G| \leq 30$, and G is not of prime order, then G is not simple.

which will give us the following corollary:

Corollary 1.7.11. If $|G| \leq 30$, then G is solvable.

Proposition 1.7.12. If $|G| = n$ and p is the smallest prime divisor of n and $H \leq G$ has index p, then $H \trianglelefteq G$

Proof. If $p = 2$, this is proved before ($[G : H] = 2$ is the smallest prime and index-2 subgroup is normal).

Suppose $H \ntrianglelefteq G$. Then there is $g \in G$ s.t. $gHg^{-1} \neq H$. Let $K = gHg^{-1} \leq G$.

By product formula, $|HK| = |H| \frac{|K|}{|H \cap K|}$, where the latter fraction is an integer which divides $|K| = |gHg^{-1}| = |H| = p$ and so divides $|G| = pm$. Then either $\frac{|K|}{|H \cap K|} = 1$ or $\frac{|K|}{|H \cap K|} = p$.

For the first case, $H \cap K = K \implies K \subseteq H \implies gHg^{-1} \subseteq H \implies gHg^{-1} = H$, not true.

For second case, $|HK| = p|H| = |G| \implies HK = G \implies g^{-1} \in HK = HgHg^{-1}$. So for some $h, h' \in H, hgh' = e \implies g = h^{-1}h'^{-1} \in H \implies gHg^{-1} = H$, a contradiction. So $H \trianglelefteq G$. ■

Corollary 1.7.13. If $|G| = pq^r$, and p, q are distinct prime and $p < q$. Then G has a normal subgroup.

Proof. By Sylow Theorem, there is a sylow q-subgroup H, so $[G : H] = p$. H is normal from the previous corollary. ■

Corollary 1.7.14. If $|G| = pq, p \neq q$, then G has a non-trivial normal subgroup.

Proposition 1.7.15. If $|G| = pq^2$, and p, q are distinct prime, then G is not simple.

Proof. If $p < q$, we are done by previous corollary.

So if $p > q$, let r be the number of sylow p-subgroups and s be number of sylow q subgroups.

Goal is to show that $r = 1$ or $s = 1$ since the only sylow subgroup is normal.

Since $r \equiv 1 \mod p, r \mid |G| = pq^2 \implies r \mid q^2$. So either $r = 1, r = q, r = q^2$. If $r = 1$, we are done. $r = q$ is impossible since $q \equiv 1 \mod p$ and $p \mid q - 1$ but $p > q$. So assume $r = q^2$.

So because $s \equiv 1 \mod q, s \mid |G| = pq^2$, then $s \mid p \implies s = 1$ or $s = q$. If $s = 1$, we are done. So assume $s = p$.

Then we have q^2 subgroups of order p and p subgroups of order q^2. Then $|G| \geq 1 + q^2(p-1) + q^2 - 1$, so there is only 1 q-sylow subgroup. So $s = 1$, and we are done. ■

Corollary 1.7.16. Every group of size $\leq n$ which is not of prime is *not simple*.

[Check Video]

Fact: If $|G| = 24$, then G is not simple.

Proof. Let r be the number of sylow 2-subgroups and s be the number of sylow 3-subgroups.

$$\begin{cases} r \equiv 1 \mod 2 \\ r \mid 3 \end{cases} \implies \begin{cases} r = 1, \text{ so we have normal subgroup} \\ r = 3 \end{cases}$$

So assume $r = 3$, and we have sylow 2-subgroups $H_1, H_2, H_3, |H_i| = 8$. Let $S = \{H_1, H_2, H_3\}$ and G acts on S by conjugation.

So there is a homomorphism $\phi : G \to S_3$, the group of permuations of S.

Use the fact that $\ker \phi \trianglelefteq G$ and we calim that $\ker \phi \neq \{e\}$ or G.

- $\ker \phi \neq \{e\}$: $|G| = 24$, $|S_3| = 6 \implies \phi$ not injective $\implies \ker \phi \neq \{e\}$
- $\ker \phi \neq G$: H_1, H_2 are conjugate by Sylow Theorem, so $\exists g \in G$ s.t. $gH_1g^{-1} = H_2 \implies g \cdot H_1 \neq H_1 \implies \phi(g) \neq e$.

$$\begin{cases} s \equiv 1 \mod 3 \\ s \mid 8 \end{cases} \implies \begin{cases} s = 1, \text{ so we have normal subgroup} \\ s = 4 \end{cases}$$

So assume $s = 4$ ■

Fact: Any group of order < 60 is solvable. *Hint: 36 similar to 24, and 40 and 56 use counting of elements (union larger than elements?)*

1.8 Direct Product and Semidirect Product of Groups

Suggestion: for the classification theorem of abelian group, check both the handwritten lecture note and [8]

1.8.1 Direct Product of Groups

Let G_1, G_2 be groups. Then $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$, and $(g_1, g_2)(g_1', g_2') = (g_1g_1', g_2g_2')$. The identity element is (e_1, e_2) and $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

Let I be an index set $G_i, i \in I$. Then

$$\prod_{i\in I} G_i = \{(x_i)_{i\in I} \,\big|\, x_i \in G_i\}$$

are the **direct product** of G_i, where $(x_i)_{i\in I}(y_i)_{i\in I} = (x_i y_i)_{i\in I}$.

Then, the **direct sum** of *abelian groups* where A_i abelian, $\forall i \in I$.

$$\bigoplus_{i\in I} A_i \le \prod_{i\in I} A_i, \;\; \bigoplus_{i\in I} A_i = \{(a_i)_{i\in I} \,\big|\, \text{ there are only finitely many non-zero } a_i\}$$

Notice that if I is *finite*, then $\bigoplus_{i\in I} A_i = \prod_{i\in I} A_i$.

Definition 1.8.1. Let A be an ableian group. Then

- $a \in A$ is **torsion** if ord(a) is finite: $\exists n > 0, na = 0$
- A_{tor} is the set of torsion elements in A, $A_{tor} \le A$ since $na = 0, mb = 0 \implies nm(a+b) = 0$
- A is **torsion-free** if $A_{tor} = \{0\}$.
- A is **torsion** if $A_{tor} = A$

Example 1.8.2. $\mathbb{Z}$ is torsion-free. $\mathbb{Z}/m$ is torsion, and any finite abelian group is torsion.

Theorem 1.8.3. If A is a torsion abelian group, then $A \simeq \bigoplus_{p_i \text{ prime}} A(p)$, where $A(p)$ are elements a in A such that $ord(a)$ is a power of p, $p^r a = 0 \exists r \ge 1$.

Proof. Plan: We have $A \simeq A_{tor} \bigoplus A/A_{tor}$, where A/A_{tor} is torsion-free. Both parts are finitely generated. Then we show that A_{tor} is finite. Then since A/A_{tor} is finitely generated, and torsion free, $A/A_{tor} \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Then, show that A_{tor} finite is a direct sum of abelian p-groups, thus a direct sum of cyclic group.

Let $\phi : \oplus_{p \text{ prime}} A(p) \to A$ is homomorphism, $(x_p) \mapsto \sum x_p \in A$.

ϕ surjective: $a \in A, ord(a) = m = p_1^{r_1} \cdots p_n^{r_n}$, p_i distinct prime. Then proceed by induction on n. If $n = 1$, then $ord(a) = p_1^{r_1} \implies a \in A(p) \implies a \in \text{Im}(\phi)$. Then for n, $ord(a) = p_1^{r_1} \cdots p_n^{r_n} \iff ap_1^{r_1} \cdots p_n^{r_n} = 0$. So since $p_1^n \cdots p_{n-1}^{r_{n-1}}$ and $p_n^{r_n}$ coprime, $\exists s, t \in \mathbb{Z}$ s.t. $sp_1^n \cdots p_{n-1}^{r_{n-1}} + tp_n^{r_n} = 1$, $asp_n^n \cdots p_{n-1}^{r_{n-1}} + atp_n^{r_n} = a$. Since the two numbers are in $\text{Im}\,\phi$, their sum is in $\text{Im}(\phi)$.

ϕ injective: Suppose $\phi((x_0)) = 0$, and $\exists q, x_q \ne 0$, then $\sum x_p = 0 \implies x_q = -\sum_{p\ne q} x_p \implies x_q = -x_{p_1} - ... - -x_{p_n}$. ord$(x_{p_i}) = p_i^{s_i} \implies p_1^{s_1} \cdots p_r^{s_r}(-x_{p_1} - ... - x_{p_r}) = 0 \iff q(p_1^{s_1} \cdots p_r^{s_r}) = 0 \implies ord(q) \,\big|\, p_1^{s_1} \cdots p_r^{s_r}$, a contradiction. ■

Example 1.8.4. $A = \mathbb{Q}/\mathbb{Z}$, where $A(p) = \{\frac{a}{b} + \mathbb{Z} \,\big|\, \frac{p^r a}{b} \in \mathbb{Z}\}$ for some r.Then $\frac{p^r a}{b} = c \implies \frac{a}{b} = \frac{c}{p^r}$, so $= \{\frac{c}{p^r} + \mathbb{Z} \,\big|\, c \in \mathbb{Z}, r \ge 0\}$

<u>*Lemma:*</u> Every finitely generated torsion abelian group is finite.

Proof. If $ord(a_i) = m_i$, and $A = \langle a_1, ..., a_k\rangle = \{n_1 a_1 + ... + n_k a_k \,\big|\, n_i \in \mathbb{Z}\} = \{n_1 a_1 + ... + n_k a_k \,\big|\, n_1 \in \mathbb{Z}, 0 \le n_i < m_i\}$, which is finite. ■

Theorem 1.8.5. Every finite abelian p-group is a direct sum of cyclic groups.

<u>*Lemma:*</u> If A is a finite abelian p-group which is <u>not cyclic</u>, then A has at least 2 subgroups of order p.

Lemma Proof. See homework ■

Theorem Proof. Let $a \in A$ be an element of maximal order. We prove by induction on $|A|$ that there is a $B \leq A$ such that $A =< a > \oplus B$. This means that if $B_1, B_2 \leq A$ s.t. $B_1 \cap B_2 = \{0\}$.

If $|A| = p$, we are done.

Let $ord(a) = p^s$. Then $< a >$ has a unique subgroup of order p. Let $< b >$ be another subgroup of order p in A s.t. $\langle a \rangle \cap \langle b \rangle = \{0\}$, which exists due to the previous lemma.

Consider $\bar{A} = A/ < b >, |\bar{A}| = \frac{|A|}{p} < |A|$. Then there is $\bar{a} = a + < b >$, an element of maximal order in $\bar{A}$.

By the induction hypothesis, there is a $\bar{B}$ such that $\bar{A} =< \bar{a} > \oplus \bar{B}$.

So $\bar{B} \leq \bar{A} = A/ < a > \implies \bar{B} = B/ < a >$ for $B \leq A$ with $< a > \subset B_0$. Then $A =< a > \oplus B$

■

Definition 1.8.6. A group A is **free** if A has a basis $\{a_i\}_{i \in I}$ s.t. $\forall a \in A, a = \sum_{i \in I} \lambda_i a_i$ in a unique way. So if A has a basis with n elements, $A \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ elements}}$.

Proposition 1.8.7. Free abelian groups are torsion-free

Proof. $A =< a_i >$. Suppose $b \neq 0 \in A$ s.t. $mb = 0, b = \sum a_i \implies mb = \sum (m\lambda_i)a_i \implies m\lambda = 0 \forall i \implies b = 0$, a contradiction. ■

Example 1.8.8. Torsion-free abelian groups are not necessarily free. Consider $\mathbb{Q}$ as an example.

Proposition 1.8.9. Every *finitely-generated* torsion-free abelian group is free, $A \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$.

Proof. Let $A =< a_1, ..., a_n >$ and induct on n. If $n = 1, A =< a_1 >$ is torsion-free $\implies |A| = \infty \implies A \simeq \mathbb{Z}$.

$n - 1 \implies n$: Let $B := \{a \in A \,\big|\, ma \in < a_1 > \exists m > 0\}$.

Claim: B is cyclic, $B \leq A \implies B$ finitely generated.

Let $B =< b_1, ..., b_l > \forall i \exists m_i, m_i b_i \in < a_1 >$. Let $m = m_1 \cdots m_l$. Then $mb \in < a_1 > \forall b \in B$.

Now look at $\phi : B \to < a >, b \mapsto mb$. Then $\mathrm{Im}(\phi) \leq < a_1 >$.

So $\mathrm{Im}(\phi)$ is cyclic: $\mathrm{Im}\,\phi =< \lambda a_1 >, \lambda \geq 1$. Let $b_1 \in B$ s.t. $\phi(b_1) = \lambda a_i$.

Then $B =< b_1 >$. If $b \in B, mb \in im\phi \implies mb = t\lambda = tmb_1$ for some $t \implies m(b - tb_1) = 0$. Since A torsion free, this means $b = tb_1 \implies b \in < b_1 >$.

A/B is generated by $a_2 + B, ..., a_n + b$ and is torsion-free, where if $m(a+B) = 0, ma \in B \implies \exists \lambda : \lambda ma \in < a_1 > \implies a \in B$.

By the induction hypothesis, A/B is free $\implies$ by proposition last time, $A = B \oplus C \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$., so this is free. ■

Proposition 1.8.10. Every subgroup of a finitely generated abelian group is finitely generated.

Idea: This implies that A_{tor} is finitely generated. Combining with previous result that a finitely generated and torsion group is finite, I can then write $A_{tor} = \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{r_m}}$.

Proof. Let $H \leq A, A = \langle a_1, ..., a_n \rangle$, and proceed by induction on n. If $n = 1$, this is cyclic so clearly true.

$n - 1 \implies n$: Let $B = \langle a_1, ..., a_{n-1} \rangle \leq A$. Then by induction hypothesis, $H \cap B = \langle h_1, ..., h_{n-1} \rangle$ generated by at most $n - 1$ elements.

Also, $A/B =< a_n + B >$.

Note that $\frac{H+B}{B} \simeq \frac{H}{H\cap B}$. Since $\frac{H+B}{B} \leq \frac{A}{B}$, it is also cyclic, so $\frac{H}{H\cap B}$ cyclic, generated by some $\langle h_n + (H \cap B)\rangle, h_n \in H$.

So $H =< h_1, .., h_n >$, I need to show that they actually generate H. If $h \in H$, then $h + (H \cap B) = \lambda_n h_n + (H \cap B) \implies h - \lambda_n h_n \in (H \cap B) \implies h - \lambda_n h_n = \sum_{i=1}^{n-1} \lambda_i h_i \implies h = \sum_{i=1}^{n} \lambda_i h_i$. ■

Proposition 1.8.11. If A is abelian and $B \subseteq A$ such that A/B is a free abelian group, then there is a subgroup $C \leq A$ such that $A = B \oplus C$.

Proof. Let $\{a_i + B\}_{i\in I}$ be a basis for A/B. Let $C =< a_i >\leq A$. We claim that $A = B \oplus C$.

First show $B \cap C = \{0\}$: Suppose $\sum_{i\in I} \lambda_i a_i \in B$, then $\sum_{i\in I} \lambda_i a_i + B = B$, so $\sum_{i\in I} \lambda_i (a_i + B) = B$, where B is the 0 of A/B. So, $\lambda_i = 0 \forall i$.

To show $A = B + C$: If $a \in A$, then $a + B = \sum_{i\in I} \lambda_i (a + B)$ in A/B, so $a + B = \sum_{i\in I} (\lambda_i a_i) + B$, so $a - \underbrace{\sum_{i\in I} \lambda_i a_i}_{\in C} \in B$. ■

Summary: Since A is finitely generated, A/A_{tor} is torsion-free, and A finitely generated $\implies$ A/A_{tor} is finitely generated. So, by previous proposition, A/A_{tor} is free.

Then by the other proposition, $\exists C \leq A, A = A_{tor} \oplus C$. So C is finitely generated, and can be written as $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$

Definition 1.8.12. Let F be a group (not necessarily abelian) and $X \subset F$. Then F is a **free group** with basis X if it satisfies the following universal property:

- $\forall$ group G and every function $f : X \to G$, there is a *unique* homomorphism $\phi : F \to G$ extending f.

For a set X, the **free group generated** by $X = \{a_1 \cdots a_k \mid a_i \in \{e\} \cup X \cup X^{-1}\}$

Example 1.8.13. If $X = \{x\}$, the free group generated by $X = \{x^r \mid r \in \mathbb{Z}\} \simeq \mathbb{Z}$

Example 1.8.14. $X = \{x, y\}$, then $F = \{x^{k_1} y^{r_1} \cdots x^{k_n} y^{r_n} \mid r_n, k_n \in \mathbb{Z}, n > 0\}$.

Fact: Every group is a quotient of a free group. $G =< x_i >, i \in I$.

Let F be free group generated by $\{x_i\}_{i\in I}$. By the universal property, $\exists$ homomorphism $\phi : F \to G, \phi$ surjective. Let $N = \ker(\phi), N \trianglelefteq F$. Then $F/N \simeq G$.

If $N =< y_j >, j \in J$. Then $< x_i, i \in I \mid y_j = e, j \in J >$ is a presentation of G.

Example 1.8.15. $G = \mathbb{Z}_6, \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Let $\phi : \mathbb{Z} \to \mathbb{Z}_6$, $1 \mapsto \bar{1}$. $N =< 6 >\subseteq \mathbb{Z}$. $Z_6 =< x \mid x^6 = e >$

Example 1.8.16. $S_3 = \{e, \underbrace{(1\,2)}_{x_1}, \underbrace{(1\,3)}_{x_2 x_1}, \underbrace{(2\,3)}_{x_2^2 x_1}, \underbrace{(1\,2\,3)}_{x_2}, \underbrace{(1\,3\,2)}_{x_2^2}\}$ Then $S_3 =< x_1, x_2 >$. So a *presentation* of $S_3 =< x_1, x_2 \mid x_1^2 = e, x_2^3 = e, x_2 x_1 = x_1 x_2^2 >$

Proposition 1.8.17. Let G be a free group generated by x, y. G is finitely generated, $H \leq G$ generated by $\{yxy^{-1}, y^2xy^{-2}, y^3xy^{-3}, ...\}$. Then H is not finitely generated.

1.8.2 Semi-Direct Product of Groups

Previously for A abelian, $H, K \leq A, H \cap K = \{0\}, A = H + K$, we denote $A = H \oplus K$, where $H \times K \simeq A, (h, k) \mapsto h + k$.

More generally, if G is a group, $H, K \leq G$ s.t. $H \cap K = \{e\}, G = HK$ and $hk = kh \forall h \in H, k \in K$, then $H \times K \simeq G, (h, k) \mapsto hk$.

Proof. $(h,k) \mapsto hk, (h',k') \mapsto h'k', (hh', kk') \mapsto hh'kk' = hkh'k'$.

$(h,k) \mapsto e \implies hk = e \implies k = h^{-1} \implies k \in K \cap H \implies k, h = e.$ ■

In particular if it is not the case that $hk = kh \forall h \in H, k \in K$, then $G \not\simeq H \times K$.

Example 1.8.18. $G = S_3$, $H = \{e, (1\,2\,3), (1\,3\,2)\}, K = \{e, (1\,2)\}$. $HK = S_3, H \cap K = \{e\}$. But $S_3 \not\simeq H \times K \simeq Z_3 \times \mathbb{Z}_2$.

If $K \leq G, H \trianglelefteq G$, then $HK \leq G$.

Example 1.8.19. Let K act on H (normal to G) by conjugation. Then $\phi : K \to Aut(H)$ is $k \mapsto \phi_k$, $\phi_k(h) = khk^{-1} \forall h$.

Definition 1.8.20. Let H and K be two groups and $\phi : K \to Aut(H)$ a homomorphism, $k \mapsto \phi_k$. Then $(H \times K)$ with operation $(h,k)(h',k') = (h\phi_k(h'), kk')$ is a group, denoted by $H \rtimes K$, the **semi-direct product** of H and K.

Proof of Group Properties. Identity: (e,e). $(e,e)(h,k) = (e\phi_e(h), k) = (h,k)$. $(h,k)(e,e) = (h, \phi_k(e), k) = (h,k)$.

Inverse of $(h,k) = (\phi_{k^{-1}}(h^{-1}), k^{-1})$. $(h,k)(\phi_{k^{-1}}(h^{-1}), k^{-1}) = (h\phi_k(\phi_{k^{-1}})(h^{-1}), e) = (e,e)$. ■

Fact: If ϕ is the identity homomorphism $\phi_k = e$ on H, then $H \rtimes K \simeq H \times K$.

$H \times K$ contains copies H and K as normal subgroup. $H \to H \times K$, $h \mapsto (h,e)$.

$(h',k')(h,e)(h',k^{-1}) = (h'hh^{-1}, e)$, and $H \trianglelefteq (H \rtimes K)$

Proposition 1.8.21. If $H, K \leq G, H \trianglelefteq G, H \cap K = \{e\}, G = HK$, then $G \simeq H \rtimes K$. $k \mapsto Aut(H), k \mapsto \phi_k$, $\phi_k(h) = khk^{-1}$.

Corollary 1.8.22. $S_3 \simeq \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. Notice that this means that ϕ trivial or $\mathbb{Z}_3 \rtimes \mathbb{Z}_2 = \mathbb{Z}_2$ or $\phi_1(1) = 2$ which is S_3

Proposition Proof. $f : H \rtimes K \to G, (h,k) \mapsto hk$. To show f injective, $f(h,k) = e \implies hk = e \implies h, k = e$. ■

1.9 Classification of Small Groups

By order,

2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_4$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Non-abelian: S_3
7. $\mathbb{Z}_7$
8. $\mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Non-abelian D_4, Q_8
9. $\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$
10. $\mathbb{Z}_{10}, \mathbb{Z}_5 b \oplus \mathbb{Z}_2$. Non-abelian: D_5
11. $\mathbb{Z}_{11}$

12. $\mathbb{Z}_3 \oplus \mathbb{Z}_4, \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Non-abelian: $D_6 (= \mathbb{Z}_2 \times S_3), A_4, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$,

In particular, $\phi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_3)$, which is $\mathbb{Z}_2$. $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 0, 3 \mapsto 1$

Chapter 2

Rings

Definition 2.0.1. A non-empty set R is a **ring** if there are operations multiplication($\cdot$) and addition $(+)$ on R such that

- $(R, +)$ is an abelian group.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- $a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot a$.
- There is an element $1 \in R$ s.t. $a \cdot 1 = 1 \cdot a = a \forall a \in R$.

Properties:

- Unity is unique. $1 = 1 \cdot 1' = 1'$
- $0 \cdot a = 0, \forall a \in R : 0a = (0 + 0)a = 0a + 0a \implies 0a = 0$
- $(-a)b = a(-b) = -(ab).(-a)b + ab = (-a + a)b = 0b = b \implies (-a)b = -(ab)$

Example 2.0.2. $(\mathbb{R}, +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot), (\mathbb{R}[x], +, \cdot), (\mathbb{R}[[x]], +, \cdot)$, which is the ring of formal power series. $\{a_0 + a_1x + a_2x^2 + ... \mid a_i \in \mathbb{R}\}$.

Definition 2.0.3. Let R, S be rings, $f : R \to S$ is a **ring homomorphism** if

- $f(a + b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$
- $f(1_R) = f(1_S)$

Example 2.0.4. $f : \mathbb{R} \to M_2(\mathbb{R}), r \mapsto \begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix}$ satisfies 1 and 2 but not 3.

Definition 2.0.5. $S \subseteq R$ is a **subring** if $(S, +) \leq (R, +)$ and $1 \in S$ and S is closed under multiplication.

Definition 2.0.6. $I \subset R$ is a **left ideal** if

- $(I, +) \leq (R, +)$
- $\forall r \in R, a \in I$, we have $ra \in I$.

A **right ideal** is similarly defined. In particular, $I \subset R$ is an **ideal** if *both right and left ideals*.

Fact: If $f : R \to S$ is a ring homomorphism, then

- $\ker(f)$ is an ideal of R

- $\mathrm{Im}(f)$ is a subring of S.

Definition 2.0.7. Let $I \subset R$ be an ideal

$$R/I := \{r + I \,\big|\, r \in R\}$$

is a ring with $(r_1 + I)(r_2 + I) := r_1 r_2 + I$, $(r_1 + I)(r_2 + I) := (r_1 + r_2) + I$

Definition 2.0.8.
- R is **commutative** if $ab = ba \forall a, b \in R$.
- R is a **division ring** if every $0 \neq a \in R$ has a multiplicative inverse.
- A commutative division ring is a **field**.
- If $a, b \in R, a, b \neq 0$ but $ab = 0$, then a, b are called **zero devisors**.
- A *commutative ring* with no zero divisor is an **integral domain**.

Example 2.0.9.
- $\mathbb{Z}$ is an integral domain
- $\mathbb{Z}_n$ is a field $\iff$ n is prime.

2.1 Ideals and Quotient Rings

Let $I \subset R$ be an ideal, then we have $R/I = \{r + I \,\big|\, r \in R\}$, with $(r + I)(s + I) = rs + I$.

Proof of Well-defined Multiplication. Want to check that $r+I = r'+I$ and $s+I = s'+I \implies rs+I = r's'+I$. $r - r', s - s' \in I$. On the other side, $rs - r's' = r(s - s') + (r - r')s' \in I$, which is true. ■

R/I is a ring, with unity $1 + R$ and zero $0 + R$. The *canonical homomorphism* is given by

$$f : R \to R/I, \quad r \mapsto r + I$$

where f is clearly surjective and $ker(f) = I$.

Ring Isomorphism Theorems

First Isomorphism Theorem. If $f : R \to S$ is a ring homomorphism, then

$$R/ker(f) \simeq \mathrm{Im}(f)$$

[Second Isomorphism Theorem.] If $S \subseteq R$ is a subring and $I \subset R$ is an ideal, then $S \cap I$ is an ideal of S and I is an ideal in

$$S + I = \{s + i \,\big|\, s \in S, i \in I\} \leq R$$

and

$$S/S \cap I \simeq S + I/I$$

Ideal in $S + I$. $(s + i)(s' + i') = ss' + is' + si' + ii'$, with $is' + si' + ii' \in I$ ■

[Third Isomorphism Theorem.] If $I \subset J \subseteq R$, I, J ideals in R, then $J/I = \{j + I \,\big|\, j \in J\}$ is an ideal of R/I and

$$\frac{R/I}{J/I} \simeq R/J$$

[Fourth Isomorphism Theorem.] (Correspondance Theorem) Let $I \subset R$ be an ideal. There is a 1-1 correspondence between subrings of R/I and subrings of R containing I.

2.2 Maximal Ideals and Prime Ideals

Definition 2.2.1. An ideal $M \subsetneq R$ is called a **maximal ideal** if for any $I \subseteq R$ with $M \subseteq I \subseteq R$, then $I = M$ or $I = R$.

Every **proper ideal** is contained in a maximal ideal by *Zorn's Lemma*.

[Zorn's Lemma] If S is a *partially ordered* set in which every *totally ordered subset* has an upper bound contains a maximal element. It is *Partially ordered* if

$$\begin{cases} a \leq a \\ a \leq b \text{ and } b \leq a \implies a = b \\ a \leq b \text{ and } b \leq c \implies a \leq c \end{cases}$$

So it follows that if $S' \subset S$ is totally ordered, then $\bigcup_{I \in S'} I$ is in S and an upper bound in S.

Proposition 2.2.2. I is maximal ideal $\iff$ R/I is a field.

Proof. $\implies$: Assume $r + I \neq I$, so $r \notin I$. If R is a commutative ring, $X \subseteq R$, then the ideals generated by X, $\langle X \rangle = \{r_1 x_1 + \cdots r_k x_k \mid k \geq 1, r_i \in R, x_i \in X\}$.

Then let $J = \langle r, I \rangle \subseteq R$, then clearly $I \subseteq J \subseteq R$. Since J ideal and I maximal ideal, $I = J$ or $J = R$, but $r \in J - I$, so $J = R \implies 1 \in J = \langle i, J \rangle \implies 1 = r'r + i$. Thus $1 - rr' \in I \implies (1 + I) = (r + I)(r' + I)$, where $(r' + I)$ is the inverse of $(r + I)$.

$\impliedby$: If R/I is a field and $I \subseteq J \subseteq R$, then J/I is an ideal of R/I. The only proper ideals of a field is $\{0\}$ ■

Definition 2.2.3. If $I \subsetneq R$ is an ideal, we say I is **prime** if $ab \in I \implies a \in I$ or $b \in I$ for $a, b \in R$.

Example 2.2.4. $R = \mathbb{Z}$, and let $m\mathbb{Z}$ be an ideal, $m \in \mathbb{Z}$. $m\mathbb{Z}$ is prime iff m is prime

Proof. $\implies$: If $m = ab$, and $a, b > 1$, then $ab = m \in m\mathbb{Z}$ but $a, b \notin m\mathbb{Z}$

$\impliedby$: If $ab \in m\mathbb{Z}$, then $m \mid ab \implies m \mid a$ or $m \mid$ ■

Proposition 2.2.5.

1. Every maximal ideal is prime
2. $I \subsetneq R$ is prime $\iff$ R/I is an integral domain.
3. P is a prime ideal $\iff$ $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ for ideals $I, J \subseteq R$. In particular, $IJ := \{\sum_{i=1}^{n} a_i b_i \mid n \geq 1, a_i \in I, b_i \in J\}$ is an ideal of R and $IJ \subseteq I \cap J$.

Proof (1): If M is maximal and $ab \in M$ and $a \notin M$, then the ideal generated by a, M, $\langle a, M \rangle := \{ra + m, m \in M, r \in R\}$ is an ideal where $M \subsetneq \langle a, M \rangle \subset R$. Then $\langle a, M \rangle = R$ since M maximal, so $1 = ra + m$ for some $r \in R, m \in M \implies b = rab + mb$, so $b \in M$. ■

Proof (2): $\implies$: If $(a + I)(b + I) = 0$, then $ab + I = 0$, so $ab \in I \implies a \in I$ or $b \in I$, so $a + I = \bar{0}$ or $b + I = \bar{0}$, where $\bar{0}$ is the zero of R/I.

$\impliedby$: If $ab \in I$, then $(a + I)(b + I) = \bar{0}$, so $a + I = \bar{0}$ or $b + I = \bar{0}$, so $a \in I$ or $b \in I$. ■

Proof (3): If P is prime and $IJ \subseteq P$ but $I \subsetneq P$ and $J \subsetneq P$, then pick $a \in I \backslash P$ and $b \in J \backslash P$, then $ab \in IJ$ but $ab \notin P$, a contradiction

Conversely, assume $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ for ideals $I, J \subseteq R$. Let $I = \langle a \rangle = \{ra \,|\, r \in R\}$ and $J = \langle b \rangle = \{rb \,|\, r \in R\}$. Then $IJ = \langle ab \rangle$ (check this). So $IJ \subseteq P$, so $a \in I \subseteq P$ or $b \in J \subseteq P$, so $a \in P$ or $b \in P$. ■

Example 2.2.6. $m\mathbb{Z} \subseteq \mathbb{Z}$ is prime $\iff$ $m\mathbb{Z}$ is maximal $\iff$ m is prime.

Proof. $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n \,|\, m$, so prime implies maximal ideal. Alternatively, consider proposition 2. ■

Example 2.2.7. $\{0\}$ is a prime ideal $\iff$ R is an integral domain. This also follows from proposition 2.

2.3 Chinese Remainder Theorem

For $0 < m_1, ..., m_n \in \mathbb{Z}, gcd(m_i, m_j) = 1$, then for any $r_1, ..., r_n \in \mathbb{Z}$, the system of equation

$$\begin{cases} x \equiv r_1 (\mod m_1) \\ \vdots \\ x \equiv r_n (\mod m_n) \end{cases} \quad \text{has a solution}$$

In rings, I reformulate this problem for a commutative ring R, where $I_1, ..., I_n$, $n \geq 2$ are ideals in R such that $I_i + I_j = R$ for every $i, j, i \neq j$. Then for any $r_1, ..., r_n \in R$, there is $x \in R$ s.t. $x - r_i \in I_i \, \forall 1 \leq i \leq n$.

Proof. Proceed with induction on n: If $n = 2, I_1 + I_2 = R \implies \exists a_i \in I_i$ s.t. $a_1 + a_2 = 1$. Then let $x = r_1 a_1 + r_2 a_1$, then $x - r_1 = r_1(a_2 - 1) + r_2 a_1 = -r_1 a_1 + r_2 a_1 \in I_1$. Similar for $x - r_2$.

$2 \implies n$: For $I_1, ..., I_n$, let $J = I_2 \cdots I_n$. Claim: $I + J = R$.

So for $I_1 + I_i = R \forall i \geq 2, \exists a_i \in I_1, b_i \in I_i$ s.t. $a_i + b_i = 1 \implies 1 = \prod_{i=2}^{n}(a_i + b_i) = I_1 + J$. By case 2 of the theorem, $\exists y_1 \in R$ s.t. $y_1 - 1 \in I_1, y_1 - 0 \in J \implies y_1 \in I_2 \cdots I_n$. In a similar way, $\forall 1 \leq i \leq n$, we find $y_i \in R$ s.t. $y_i - 1 \in I_i$ and $y_i = I_1 \cdots \hat{I}_i \cdot I_n \subseteq I_j \forall j \neq i$. Note that $I \cap J \subseteq IJ$.

Let $x = r_1 y_1 + ... + r_n y_n$. Then $x - r_i = r_1 y_1 + \cdots r_i(y_i - 1) + \cdots r_n y_n$. Every y_i is in I_i, so this entire expression is in I_i. ■

2.4 Product of Rings

Let R, S be rings, then

$$R \times S = \{(r, s) \,|\, r \in R < s \in S\}$$

where $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$. and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1, s_2)$

Corollary 2.4.1. If $I_1, ..., I_n$ are ideals of R such that $I_i + I_j = R$ for $i \neq j$. Then

$$\frac{R}{\bigcap_{i=1}^{n} I_n} \simeq \prod_{i=1}^{n} R/I_i$$

Proof. Define $\phi : R \to \prod_{i=1}^{n} R/I_i$ by $\phi(r) = (r + I_1, ..., r + I_n)$, and ϕ is a ring homomorphism. $\ker(\phi) = \cap_{i=1}^{n} I_i$.

ϕ surjective: $\forall (r_1 + I_1, ..., r_n + I_n) \in \prod_{i=1}^{n} R/I_i$, by the chinese remainder theorem, $\exists x \in R$ s.t. $x + I_i = r_i + I_i$, so by the first isomorphism theorem, we get the result. ■

Example 2.4.2. If $R = \mathbb{Z}$, and prime factorization $m = p_1^{r_1} \cdots p_n^{r_n}$, $I_i = p_i^{r_i}\mathbb{Z}$. Then note that $I_i = p_i^{r_i}\mathbb{Z}$, $I_i + I_j = \mathbb{Z}$, and $\cap_{i=1}^n I_i = m\mathbb{Z}$. So,

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_{i=1}^n \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

as rings. Also,

$$\mathbb{Z}_m \simeq \prod_{i=1}^n \mathbb{Z}_{p_i}^{r_i}$$

as rings.

2.5 Localization

Suppose R is an integral domain. Consider the equivalence relation $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$. Then, we can mod out by equivalence relationship.

$$\{\frac{a}{b} \,\big|\, a, b \in R, b \neq 0\}/\sim$$

Then we define the ring structure such that for $b, d \neq 0$, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$. There are well-defined. The unity is $\frac{1}{1}$, and the zero is $\frac{0}{1}$. This is a commutative ring, and any non-zero element $\frac{a}{b}, a, b \neq 0$ has a multiplicative inverse $\frac{b}{a}$. Thus we get a field, namely the field of fraction of R (Quotient field).

Definition 2.5.1. Suppose R is a commutative ring. Then $S \subset R$ is a **multiplicative subset**, where $1 \in S$ and $a, b \in S \implies ab \in S$, and $0 \notin S$

Example 2.5.2.

- For $0 \neq r \in R$, $S = \{1, r, r^2, ...\}$
- $P \subsetneq R$ be a prime ideal and $S = R \backslash P$. Then $a, b \notin P \implies ab \notin P$.

Define $S^{-1}R = \{(r, s) \,\big|\, r \in R, s \in S\}/\sim$. Then consider the equivalence relationship $(r, s) \simeq (r', s') \iff \exists s'' \in S$ s.t. $s''(rs' - sr') = 0$.

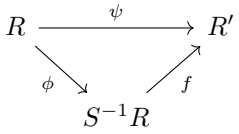
If $0 \in S$, then $(r, s) \simeq (0, 0)$, and everything is 1 equivalence relationship. So from now on, we assume $0 \notin S$. Then we have ring structure on $S^{-1}R$, $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$, and $\frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}$.

Operations are well-defined: If $\frac{r}{s} = \frac{r_0}{s_0}$, then $\exists s'', s''(rs_0 - r_0 s) = 0$. Then I want to check that $\frac{r}{s} + \frac{r'}{s'} = \frac{r_0}{s_0} + \frac{r'}{s'} \iff \frac{rs'+r's}{ss'} = \frac{r_0 s'+r's_0}{s_0 s'} \iff \cdots = 0$. Last step consists of annoying factorization.

There is a natural ring homomorphism defined by $\phi : R \to S^{-1}R, \phi(r) = \frac{r}{1}$.

In particular if R is an integral domain (so $rs' = r's$), $S^{-1}R$ is a subring of the field of fractions of R, which we can write as $R \subset S^{-1}R \subset K$, where K is the field of fractions.

Note that $\phi : R \to S^{-1}R$ has the property that $\phi(s)$ is invertible. Namely $\forall s \in S, \phi(s) = \frac{s}{1}$, so $\frac{s}{1}\frac{1}{s} = \frac{1}{1}$. And if $\psi : R \to R'$ is a ring homomorphism such that $\psi(s)$ invertible in R', then $\exists! f : S^{-1}R \to R'$ such that $f \circ \phi = \psi$ [Check video for graph]



Proposition 2.5.3. Assume R is an integral domain.

- If $S = R \setminus \{0\}$, then $S^{-1}R$ is the field of fractions of R.
- If $S = \{1, f, f^2, ..., \}$ where $f \in R$ s.t. $f^n \neq 0 \forall n$, $R_f = S^{-1}R = \{\frac{a}{f^r} \,\big|\, a \in R, r \geq 0\}$.

- If $P \subset R$ is a prime ideal and $S = R \setminus P$, $R_P = S^{-1}R = \{\frac{a}{b} \mid a, b \in R, b \notin P\}$
- If $P \subsetneq R$ is a prime ideal, then R_p is a **local ring**. i.e. it has a *unique* maximal ideal. This unique maximal ideal is defined as $\{\frac{a}{b} \mid a, b \in R, b \notin P, a \in P\}$. If $b \notin P$, then there is an inverse which is not possible since $P \subsetneq R$.

2.6 Principal Ideal Domains (PIDs)

Definition 2.6.1. For *integral domain* R, an ideal $I \subseteq R$ is **principal** if it is generated by one element $I = \langle a \rangle = \{ra \mid r \in R\}$. Then R is **PID** if every ideal is *principal*.

Example 2.6.2.
- $\mathbb{Z}$ is PID. Every ideal generated by some n.
- $\mathbb{R}[x]$ is a PID. If $I \neq \{0\}$ is an ideal and $0 \neq f(x) \in I$ has the smallest degree, then $I = \langle f(x) \rangle$. If $g \in I$, dividing g by f means that $g(x) = q(x)f(x) + r(x)$. So $r(x)$ or $deg(r) < deg(f)$. By $r(x) = g(x) - q(x)f(x) \in I$, by $degr(x) \geq degf(x) \implies r = 0 \implies g \in \langle f \rangle$.
- $\mathbb{R}[x, y]$ is not a PID. $\langle x, y \rangle = \{f(x, y) \mid f(0, 0) = 0\}$ not principal.
- $\mathbb{Z}[x]$ is not a PID. $\langle x, y \rangle = \{f(x) \mid f(0) \text{ is even}\}$ not principal.

Definition 2.6.3.
- For an integral domain R, $a \in R$ is **prime** if $\langle a \rangle$ is a prime ideal. Equivalently, $a \mid bc \implies a \mid b$ or $a \mid c$.
- $0 \neq a \in R$ is **irreducible** if it is not a unit and if $a = xy$, then x is a unit or y is a unit.

Proposition 2.6.4. A *prime* element is *irreducible*.

Proof. If a is prime and $a = xy$, then $a \mid x$ or $a \mid y$, so $x = ax'$ or $y = ay'$, so $a = ax'y$ or $a = xay' \implies a(1 - x'y) = 0$ or $a(1 - xy') = 0 \implies 1 = x'y$ or xy', so y is a unit or x is a unit. ■

Example 2.6.5. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

It is clear to see that this is closed under multiplication. We claim that $3 \in R$ is irreducible but not prime. We let $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, and define the norm as $|a + \sqrt{-5}| := \sqrt{a^2 + 5b^2}$. Then squaring, $9 = (a^2 + 5b^2)(c^2 + 5d^2)$. Clearly neither of the values can be 3. so $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$. Thus $(a, b) = (\pm 1, 0) \implies (a + b\sqrt{-5})$ is a unit, or $c + d\sqrt{-5}$ is a unit. Thus 3 is irreducible.

But $3^2 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}) \implies 3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$. and $3 \nmid (2 + \sqrt{-5})$ and $3 \nmid 2 - \sqrt{-5}$ since $2 + \sqrt{5} \neq 3(a + b\sqrt{-5})$, for $a, b \in \mathbb{Z}$.

Proposition 2.6.6. If R is a PID, then irreducible $\implies$ prime.

Proof. Suppose $a \in R$ is irreducible, then it suffices to show that a is a prime ideal. Then the ideal generated by a, $(a) \neq R$ since a is not a unit. So there is a maximal ideal M where $(a) \subseteq M \subsetneq R$.

Since R is a PID, $M = (b)$ for some $b \implies (a) \subseteq (b) \implies a = bc$ for some c. $(b) \neq R$ so b is not a unit. Since a irredcible, c has to be a unit. So $b = c^{-1}a \implies b \in (a) \implies (b) \subseteq (a)$, so $(a) = (b)$, so (a) maximal and therefore prime. ■

Proposition 2.6.7. Every prime ideal is maximal in a PID.

Proof. If $I = (a)$ prime, then $(a) \subseteq M \subsetneq R$ where M is maximal, then let $M = (b) \implies a \in (b) \implies a = bc$. a is prime so it is irredcible, so c is a unit. So $b \in (a) \implies (a) = (b) \implies (a)$ maximal. ■

2.7 Unique Factorization Domains (UFDs)

Definition 2.7.1. Let R be an integral domain. For $a, b \in R$, we say a, b **associates** if $(a) = (b)$.

Note: $(a) = (b) \iff a = bu$.

Proof. $\impliedby$: $(a) \subseteq (b)$ and $b = u^{-1}a \implies (b) \subseteq (a)$.

$\implies$: $a = bx$ and $b = ay \implies a = axy \implies a(1 - xy) - 0 \implies (1 - xy) = 0 \implies x$ is a unit. ■

Definition 2.7.2. If R is an integral domain, then R is a **unique factorization domain** (UFD) if every non-zero $x \in R$ can be written as a unique product of irreducible elements (up to associates and reordering).

Example 2.7.3. If $x = a_1 \cdots a_r = b_1 \cdots b_m$. Then a_i, b_j all irreducible, and $r = m$ and after reordering, a_i and b_j are associate.

Example 2.7.4. For $\mathbb{Z}$, the units are ± 1. Prime elements are $\{\pm p \mid p \text{ prime}\}$. $\mathbb{Z}$ is UFD.

Example 2.7.5. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proposition 2.7.6. Integral Domain R is a UFD $\iff$

1. Every irreducible element is prime.
2. R satisfies the ascending chain condition for principle ideals. Namely, $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_m) \subseteq \cdots$, and $\exists (a_n) = (a_{n+1}) = \cdots$

Proof. $\implies$: First assume R is a UFD.

(1). If $a \in R$ irreducible and $a \mid bc$, so for $bc = ax$, write b, c, x as a product of irreducible elements, where $b = q_1 \cdots q_l, c = y_1 \cdots y_t, x = x_1 \cdots x_k$. So $bc = ax \implies q_1 \cdots q_l y_1 \cdots y_t = a x_1 \cdots x_k$. Since R UFD, $\exists q_i$ or y_i associate to a. Assume WLOG $uq_i = a$ for a unit a, so $u^{-1}a = q_i \mid b \implies b = b'u'a \implies a \mid b$

(2). $(a) \subseteq (b) \iff b \mid a$. If $(a) \subsetneq (b)$, then $a = bc$, where c is a non-unit. So the number of irreducible factors of $b <$number of irreducible factors of a, so there can't be infinitely many strict inclusion in the chain.

Conversely, assume (1) and (2) holds. To show the existnece of factorization, let for a not unit and cannot be written as product of irreducible elements, let $S = \{(a)\}$. We want to show that S is empty using Zorn's lemma. Since S is a partially ordered set (by inclusion), every ascending chain has an upper bound, so by Zorn's lemma, S has a maximal element (a).

Then when a is not a unit and not irreducible (and since $(a) \in S$), so $a = bc$), where $a = bc, b, c$ not unit. Thus $(a) \subsetneq (b)$ and $(a) \subsetneq (c) \implies (b), (c) \notin S$. So b and c are products of irreducible elements, so a is a product of irredcible elements, which is a contradiction.

Uniqueness: Suppose $a = x_1 \cdots x_n = y_1 \cdots y_m$, where x_i, y_j irreducible. Then $y_1 \mid x_1 \cdots x_n$ and y_i prime $\implies y_1 \mid x_i$ for some i. So, $x_i = uy_1$ and x_i irreducible $\implies u$ is a unit, so y_1, x_i associates.

■

Theorem 2.7.7. Every PID is a UFD.

Proof. (1) It is proved that every irreducible element is prime.

(2) If $(a_1) \subset (a_2) \subset \cdots$. Let $I = \bigcup (a_i)$, then I is an ideal. Since R is a PID, we want $I = (b)$. Since $b \in I, \exists i$ s.t. $b \in (a_i)$, so $(b) \subseteq (a_i)$. But $(a_i) \subseteq (b)$, so $(a_i) = (b)$, so $(a_i) = (a_{i+1}) = (a_{i+1}) = ...$ ■

Remark: Fields $\subset$ Euclidean Rings $\subset$ PIDs $\subsetneq$ UFDs $\subsetneq$ integral domains $\subset$ rings.

Definition 2.7.8. If R is an integral domain and $a, b \in R$. Then d is the **greatest common divisor** of a, b if

- $d \mid a$ and $d \mid b$.
- If $d' \mid a$ and $d' \mid b$, then $d' \mid d$

Fact: In a UFD, gcd exists.

For $a = a_1 \cdots a_t a_{t+1} \cdots a_n, b = b_1 \cdots b_t b_{t+1} \cdots m$, a_i, b_j irreducible, we can rearrage it so that a_i, b_i associates for $1 \leq i \leq t$, and otherwise they don't associate. So $\gcd(a,b) = a_1 \cdots a_t$.

Remark: In $\mathbb{Z}[\sqrt{5}]$, the gcd does not exist.

Fact: In a PID, $\gcd(a,b)$ is a "linear combination" of a, b.

If $(a,b) = (d)$, then $d \mid a$ and $d \mid b$ and if $d' \mid a$ and $d' \mid b$, then $(a,b) \subseteq (d') \implies (d) \subseteq (d') \implies d' \mid d$

2.8 Euclidean Domains

Definition 2.8.1. An *integral domain* R is a **Euclidean domain** if there is a map $d : R \setminus \{0\} \longrightarrow \mathbb{Z}_+$ s.t.

- if $a, b \in R$, $b \mid a$, then $d(b) \leq d(a)$
- If $a, b \in R \setminus \{0\}, \exists t, r \in R$ s.t. $a = tb + r$, where $r = 0$ or $d(r) < d(b)$

Example 2.8.2.

- $R = \mathbb{Z}, d(a) = |a|$.
- If $\mathbb{R} = F[x]$ where f is a field, then $d(f(x))$= deg(f).
- For any field F, $d(a) = 0 \, \forall a \in F \setminus \{0\}$.

Proposition 2.8.3. Euclidean domains are PIDs.

Proof. If $\{0\} \notin I \subsetneq R$ is an ideal, then let $a \in I$ be a non-zero element with the smallest degree. We want to claim that $I = (a)$.

If $0 \leq b \in I$, we write $b = at + r, r = 0$ or $d(r) < d(a)$. But $r = b - at \in I$, so $d(r) \geq d(a)$, so it has to be that $r = 0$, so $b \in (a)$. ■

Example 2.8.4. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an Euclidean domain.

Proof. Let $d : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{Z}_+$ be $d(a + bi) = a^2 + b^2$.

d is multiplicative: $d((a+bi)(a'+b'i)) = d((aa'-bb')+(ab'+a'b)i) = (a^2+b^2)(a'^2+b'^2) = d(a+bi)d(a'+b'i)$.

(1): If $a = bc$, where $a, b, c \neq 0$, then $d(a) = d(b)d(c) \geq d(b)$.

(2): Suppose $x, y \in \mathbb{Z}[i]$ and we want to divide x by y. If $y = n \in \mathbb{Z}_+$, $x = a + bi$ and I write $a = nq + r, r = 0$ or $|r| < n$ and $b = nq' + r, r' = 0$ or $|r'| < \frac{n}{2}$. This is possible since if $a = nq + r, \frac{n}{2} \leq r < n$, then $a = n(q+1) + (r-n), |r-n| < \frac{n}{2}$.

Then $x = a + bi = (nq + r) + i(nq' + r') = n(q + iq') + (r + ir')$, and $d(r + ir') = r^2 + r'^2 < \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2} < n^2 = d(n)$.

Now suppose we are dividing x by an arbitary y, and we use the previous result by letting $n = y\bar{y} = d(y) > 0$. So we can divide $x\bar{y}$ by n where

$$x\bar{y} = qn + r, \qquad d(r) < d(n) \implies x\bar{y} = q\bar{y}y + r$$

Then claim that $x = qy + (x - qy)$, where $d(x - qy) < d(y)$. Notice that

$$d(x - qy)d(\bar{y}) = d(x\bar{y} - qy\bar{y}) = d(r) < d(n) = d(y)^2 \implies d(x - qy) < d(y)$$

Thus, this result holds. ■

Example 2.8.5. This is not unique. $3 = (1+i)(1-i)+1, d(1) < d(1-i)$. Also $3 = (2-i)(1-i)-i$, $d(-i) < d(1-i)$

Remember that gcd exists in any UFD. So if $d = gcd(a,b)$, then $d \mid a, d \mid b$ and $d' \mid a, d' \mid b \implies d' \mid d$.

IF R is a PID, $\exists x, y \in R, d = ax + by$.

If R is a Euclidean Domain, and $a, b \in R \neq 0$, I can find the gcd using the following algorithm

$$\begin{aligned} a &= bq_0 r_0 && \implies gcd(a,b) = gcd(b, r_0) \\ b_0 &= r_0 q_1 + r_1 && \implies gcd(b, r_0) = gcd(r_0, r_1) \\ &\vdots \\ r_{n+1} &= r_{n+2} q_{n+3} + 0 && \implies gcd = r_{n+2} \end{aligned}$$

2.9 Polynomial Rings

Definition 2.9.1. For any commutative ring R, we define a **polynomial ring**

$$R[x] = \{a_0 + ... + a_n x^n \mid a_i \in R\}$$

If $f(x) = a_n x^n + ... + a_1 x + a_0$, where a_n is the **leading coefficient**, n is the **degree** of $f(x)$, and a_0 is the **constant term**. If $a_n = 1$, then $f(x)$ is **monic**.

Division Algorithm: If R is an integral domain and non-zero $f(x), g(x)$ with $g(x)$ monic, then there are unique polynomials $q(x), r(x) \in R[x]$ s.t. $f(x) = g(x)q(x) + r(x)$, where $r = 0$ or $deg(r) < deg(g)$.

Proof. For existence, let n be degree of f and m be degree of g, proceed by induction on n.

If $n = 0$, then $f(x) = g(x) \times 0 + f(x)$. $deg(f) = 0 < deg(g)$ if g is non-constant. If g is a constant $= b_0 \neq 0$, then $a_0 = b_0 \frac{a_0}{b_0} + 0$, so still $deg(r) < deg(g)$. Note that $b_0 = 1$ since g monic.

If the statement holds for $deg(f) < n$, I can write $f(x) = a_n x^n + ... + a_0, g(x) = x^m + ... + b_0$. Let $f_1(x) = f(x) - a_n x^{n-m} g(x)$. Clearly, since $deg(f_1) < n$, by induction hypothesis, I can write $f_1(x) = g(x)q_1(x) + r_1(x)$, with $r_1 = 0$ or $deg(r_1) < deg(g)$. So rewriting,

$$\begin{aligned} f(x) &= f_1(x) + a_n x^{n-m} g(x) \\ &= g(x)q_1(x) + r_1(x) + a_n x^{n-m} g(x) \\ &= g(x) \underbrace{q_1 + a_n x^{n-m}}_{q(x)} + r_1(x) \end{aligned}$$

Uniqueness: $f = gp_q + r_1 = gq_2 + r_2 \implies g(q_1 - q_2) = r_2 - r_1$. Suppose they are not equal. Clearlyt $deg(r_1 - r_2) < deg(g)$. Also, $deg(g(q_1 - q_2) \geq deg(g)$ since R is a UFD (so $deg(f) + deg(g) = deg(fg)$). This is a contradiction unless both sides are 0, so $q_1 = q_2$ and $r_1 = r_2$

■

Remark: If F is a field, the same argument shows for any non-zero $f(x), g(x) \in F[x]$.

Corollary 2.9.2. If R is an integral domain, $f(x) \in R[x]$ and $a \in R$. Then $f(a) = 0 \iff x - a \mid f(x)$

Proof. Suppose $f(a) = 0$. Write $f(x) = (x-a)q(x) + r(x)$, where $r = 0$ or $deg(r) \leq 0 \implies f(a) = r$. So $f(a) = 0 \iff r = 0$ ■

Corollary 2.9.3. If R is an integral domain and $f(x) \in R[x]$ has degree n, then $f(x)$ has $\leq n$ zeros.

Example 2.9.4. It is important for this to satisfy integral domain property. In $\mathbb{Z}_8$, $f(x) = x^2 - 1$ has roots $1, 3, 5, 7$

Corollary 2.9.5. If F is a field, $F[x]$ is a Euclidean domain.: $d(f(x)) = deg(f)$. So $F[x]$ is a UFD.

Definition 2.9.6. Let R be a UFD. For non-zero $a_1, ..., a_n \in R$, $d = \gcd(a_1, ..., a_n)$ exists, where a_n is unique up to associates. Then for $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$, the **content** of $f(x), c(x) := \gcd(a_n, ..., a_1, a_0)$. And f is **primitive** if $c(f)$ is a unit.

Lemma 2.9.7. $c(fg) = c(f)c(g)$ up to units.

Proof. Case I: Suppose f, g primitive, want to show that fg is primitive. If $f = a_n x^n + ... + a_1 x + a_0, g = b_m x^m + ... + b_1 x b_0$, then $fg = c_{n+m}x^{n+m} + ... + c_1 x + c_0$. If fg is not primitive, $\exists$ prime $p \in R$ s.t. $p \mid c_i \forall i$. However, f, g primitive. Suppose i_0 is the smallest i such that $p \nmid a_i$ and j_0 be the smallest j such that $p \nmid b_j$. Then $p \nmid c_{i_0+j_0}$, where $c_{i_0+j_0} = a_0 b_{i_0+j_0} + ... + a_{i_0-1} b_{j_0+1} + a_{i_0} b_{j_0} + ... + a_{i_0+j_0} b_0$. This is a contradiction.

Case II: Let f, g be arbitrary. Let $f = c(f)f_1, g = c(g)g_1$, with f_1, g_1 primitive so $f_1 g_1$ primitive. So $fg = c(f)c(g)f_1 g_1 \implies c(fg) = c(f)c(g)$ ■

Lemma 2.9.8. If F is the quotient field of R and $f(x) \in R[x]$ is primitive, then $f(x)$ irreducible in $R[x] \iff f(x)$ irreducible in $F[x]$

Proof. $\impliedby$: Suppose $f(x)$ not irreducible in $R[x]$, then $f(x) = f_1(x)f_2(x)$ for f_1, f_2 non-units in $R[x]$. If $deg(f_1) = 0$, then it is a constant $c \implies f = cf_2 \implies c \mid f \implies c$ unit since f primitive, a contradiction.

Then suppose $deg(f_2), deg(f_1) \geq 1$. Since units of $F[x]$ are non-zero constants, $f(x)$ not irreducible.

$\implies$: Suppose $f(x) \in R[x]$ can be written as $f = f_1 f_2, f_1, f_2 \in F[x], deg(f_1, f_2) \geq 1$. Write $f_1 = \frac{b_n}{c_n}x^n + ... + b_0 c_0, \quad b_i, c_i \in R$. So if $r_1 = c_1 \cdots c_n \in R$, then $r_1 f_1 \in R[x]$. Let $g = cf_1$. Similarly there is $r_2 \in R$ s.t. $g_2 = r_2 f_2 \in R[x] \implies g_1 g_2 = r_1 r_2 f_1 f_2$. So $g_1 = c(g_1)h_1, g_2 = c(g_2)h_2$ with $h_1, h_2 \in R[x]$ primitive. So $c(g_1)c(g_2)h_1 h_2 = r_1 r_2 f \implies$ taking contents, $c(g_1)c(g_2) = r_1 r_2$ up to units.

So $ucc(g_1)c(g_2) = r_1 r_2$ for unit u, so $uh_1 h_2 = f \implies (uh_1)h_2 = f$. Combining with $deg(h_1) = deg(g_1) = deg(g_1) \geq 1$, we have f irreducible in $R[x]$. ■

Example 2.9.9. $f(x) = 2x + 2 \in F[x]$ is irreducible in $\mathbb{Q}[x]$ but not in $F[x]$

Theorem 2.9.10. If R is a UFD, then $R[x]$ is a UFD.

Proof. Case 1: If $f(x)$ primitive, then $f(x) \in F[x]$ can be written as $f(x) = f_1(x) \cdots f_n(x)$, where $f_i(x)$ irreducible in $F[x]$. $\exists b_i \in R$ s.t. $b_i f_i(x) = g_i(x) \in R[x]$.

Then, let $c_i = c(g_i) \implies c_i h_i(x) = b_i f_i(x)$ for some $h_i(x)$ primitive in $R[x]$. Write this as $f_i = \frac{c_i h_i}{b_i}$, so $b_1 \cdots b_n f(x) = c_1 \cdots c_n h_1(x) \cdots h(x)$. Therefore, $b_1 \cdots b_n = c_1 \cdots c_n$ up to units, so $c_1 \cdots c_n = u b_1 \cdots b_n$, so $f(x) = u h_1(x) \cdots h_n(x)$

Uniqueness: If $f(x) = p_1 \cdots p_n(x) = q_1(x) \cdots q_m(x)$, where p_i, q_j irreducible in $R[x]$. Then $f(x)$ primitive $\implies p_i, q_j$ primitive $\forall j \implies$ by the lemma, p_i, q_j irreducible in $F[x] \forall i, j$. Since $F[x]$ is a UFD, $n = m$, $p_- = q_j$ up to reordering and multiplying So $p_i = \frac{a_i}{b_i} q_i$, $a, b \in R \implies b_i p_i(x) = a_i q_i(x) \implies$ by p_i, q_i primitive that $b_i = a_i$ up to a unit, $b_i = u_i a_i \implies u_i p_i = q_i \implies p_i = q_i$ up to unit.

Case 2: Let $f(x) \in R[x]$ be arbitrary, let $c = c(f) \implies f(x) = cg(x)$, where $g(x)$ is primitive. From case 1, we can write $g(x) = g_1(x) \cdots g_n(x)$, where $g_i \in R[x]$ irreducible. Then $f(x) = cg_1(x) \cdots g_n(x)$.

When we factor c in R, $c = c_1 \cdots c_m \implies f(x) = c_1 \cdots c_m g_1(x) \cdots g_n(x)$, all irreducible in $R[x]$.

Uniqueness: Suppose $f(x) = f_1 \cdots f_n = g_1 \cdots g_m$, where $f_i, g_j \in R[x]$ irreducible. Consider cases when their degree is 0 and greater than 0. ■

Corollary 2.9.11. If R UFD, then $R[x_1, ..., x_n]$ is a UFD for $n \geq 1$.

2.10 Eisenstein Criterion for Irreducibility

Let R be UFD, $f(x) = a_n x^n \cdots + a_1 x + a_0 \in R[x]$, $n \geq 0, a_n \neq 0$.

Theorem 2.10.1. If p is a prime element in R s.t.

- $p \mid a_i, 0 \leq i < n$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Then, $f(x)$ is irreducible.

Example 2.10.2. $x^2 + y^2 + 1 \in \mathbb{C}[x, y]$ is irredcible

Proof. Consider $R = \mathbb{C}[x]$ as a UFD and $\mathbb{C}[x, y] = \mathbb{C}[x][y]$. Rewrite as $y^2 + (x+1)(x-i)$, where $(x+1)(x-i)$ irreducible in $R = \mathbb{C}[x]$. We have $x + i \mid x^2 + 1, x + i \nmid 1, (x^2+1)^2 \nmid x^2 + 1 \implies x^2 + y^2 + 1$ irreducible. ■

Example 2.10.3. $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ is irreducible for p prime.

Proof. Consider $f(x+1) = (x+1)^p + (x+1)^{p-2} + ... + (x+1) + 1$.

$$\begin{aligned} f(x+1) &= \sum_{i=0}^{p} (x+1)^i \\ &= \sum_{i=0}^{p-1} \sum_{j=0}^{i} \binom{i}{j} x^j, \qquad 0 \leq i \leq p-1, 0 \leq j \leq i \\ &= \sum_{j=0}^{p-1} \left(\sum_{i=j}^{p-1} \binom{i}{j} \right) x^j \end{aligned}$$

Set $c_j = \sum_{i=j}^{p} \binom{i}{j}$, and I claim that $p \mid c_j, c_{p-1} = \binom{p-1}{p-1} = 1$. Using the identity $\binom{j}{j} + \cdots + \binom{m}{j} = \binom{m+1}{j+1}$, $c_j = \binom{p}{j+1} = \frac{p!}{(j+1)!(p-j-1)!}$. Also $c_0 = \binom{p}{1} = 1$, so $p^2 \nmid c_0$. Therefore by eisenstein criterion, $f(x+1)$ irreducible, so $f(x)$ irreducible. ■

Proof of Eisenstein Criterion. If $f(x) = g(x)h(x)$ non-units with $g(x) = b_r x^r + \cdots b_1 x + b_0, h(x) = c_k x^k + \cdots c_1 x + c_0$. If $deg(g) = 0, g(x) = b_0$ and $b_0 \mid a_i \forall i \implies$ since f primitive, b_0 is a unit, a contradiction.

So assume $r \geq 1$. Then $p \mid a_0 = b_0 c_0, p^2 \nmid b_0 c_0 \implies$ either $p \mid b_0, p \nmid c_0$ or $p \nmid b_0, p \mid c_0$. Also, $p \nmid a_n = b_r c_k \implies p \nmid b_r$

Now, let $i \geq 1$ be the smallest number such that $p \nmid b_i$, and we have $i \leq r > n$. Then $a_i = b_0 c_i + b_i c_{i-1} + ... + b_{i-1} c_1 + b_i c_0$. However, $p \mid a_i$ and $p \mid b_0 c_i + b_i c_{i-1} + ... + b_{i-1} c_1 \implies p \mid b_i c_0 \implies p \mid b_i$ or $p \mid c_0$, both not true. Therefore contradiction. ■

Chapter 3

Modules

Definition 3.0.1. Suppose we have arbitrary ring R and abelian group M such that there is $R \times M \to M$, $(r, m) \mapsto rm$ with distributivity. This is a **left module**, and satisfies the distributivity below:

- $(r+s)m = rm + sm$
- $r(m_1 + m_2) = rm_1 + rm_2$
- $(rs)m = r(sm)$
- $1_R m = m$

Fact: If R is a field, then this is a vector space.

Modules also satisfy the following properties:

- $r0_M = 0_M$
- $0_R m = 0_M$
- $(-r)m = -(rm)$

Definition 3.0.2. If $\varnothing \neq N \subset M$, then N is a **submodule** if it is a subspace of M and $r \in R, n \in N \implies rn \in N$.

Example 3.0.3.
- Let R be a ring and R be a module over R. Submodules are (left) ideals in this case.
- Every abelian group is a module over $\mathbb{Z}$. Then submodules correspond to subgroups.

Definition 3.0.4. If M, N are R modules, then $f : M \to N$ is a R-**homomorphism** if f is a group homomorphism and $f(rm) = rf(m) \forall r \in R, m \in M$. Note that $ker(f) \subset M$ as a submodule, and $\mathrm{Im}(f) \subseteq N$ as a submodule.

Remark: If f is an isomorphism, $f^{-1} : N \to M$ is also a R-homomorphism.

3.1 Isomorphism Theorems

If $N \subseteq M$ is a submodule, then M/N has the structure of a R-module.

$$r(m + N) := rm + N$$

well-defined: Does $m + N = m' + N \implies r(m + N) = r(m' + N)$?. yes, because $m - m' \in N$ and $r(m - m') \in N$

Isomorphism Theorem 1: If $f : M \to N$ is a R-homomorphism, then

$$M/\ker(f) \simeq \mathrm{Im}(f) \text{ as } R\text{-modules}$$

Theorem 2: If N_1, N_2 are submodules of M, then $N_1 + N_2 := \{x + y \mid x \in N_1, y \in N_2\}$ is a submodule of M, and $N_1 \cap N_2$ is also a submodule of M, and

$$\frac{N_2}{N_1 \cap N_2} \simeq \frac{N_1 + N_2}{N_1}, \quad f : N_2 \to \frac{N_1 + N_2}{N_1},\ f(n_2) = n_2 + N_1$$

Theorem 3: If $N \subseteq M$ and $K \subseteq N$ are submodules, then N/K is a submodule of M/K, and

$$\frac{M/K}{N/K} \simeq M/N$$

Theorem 4: If $N \subseteq M$ is a submodule, the canonical map $M \to M/N, m \mapsto m + N$ induces a 1-1 correspondence between submodules of M/N and submodules of M containing N

3.2 Direct Product and Sum of Modules

Let R be an arbitray ring and $\{M_i\}_{i\in\mathcal{I}}$ be a family of R-modules. The **direct product** is defined as

$$\prod_{i\in\mathcal{I}} M_i = \{(x_i)_{i\in\mathcal{I}} \mid x_i \in M_1\},\ r(x_i)_{i\in\mathcal{I}} = (rx_i)_{i\in\mathcal{I}}$$

Direct Sum is defined $\bigoplus_{i\in\mathcal{I}} M_i = \{(x_i)_{i\in I} \mid x_i \in M_i, \text{all but finitely zero}\}$

Remark: If M is a module and $N_1, N_2 \subseteq M$ are submodules such that

- $M_1 \cap M_2 = \{0\}$
- $M_1 + M_2 = M$

Then $M \simeq M_1 \oplus M_2 \simeq M, (m_1, m_2) \mapsto m_1 + m_2$.

3.3 Exact Sequences

Definition 3.3.1. Let R be a ring and M, M', M'' be R-modules. A sequence of R-homomorphism $M' \xrightarrow{f} M \xrightarrow{g} M''$ is called **exact** if $\mathrm{Im}(f) = ker(g)$. More generally, sequence $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ is **exact** if $\mathrm{Im}(f_i) = ker(f_{i+1})$.

Example 3.3.2. The sequence $0 \to M' \xrightarrow{f} M$, is *exact* if and only if f is injective.

Example 3.3.3. The sequence $M \xrightarrow{g} M'' \to 0$ is *exact* if and only if g is surjective

Definition 3.3.4. If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence, then it is called a **short exact sequence**

Example 3.3.5. If $N \subseteq M$ is a submodule, $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$.

Proposition 3.3.6. Let $0 \longrightarrow M' \underset{\psi}{\overset{f}{\rightleftharpoons}} M \underset{\phi}{\overset{g}{\rightleftharpoons}} M'' \longrightarrow 0$ be a short exact sequence of R-modules. Then the following conditions are equivalent.

1. $\exists$ R-homomorphism $\phi : M'' \to M$ s.t. $g \circ \phi = id_{M''}$
2. $\exists$ R-homomorphism $\psi : M \to M'$ s.t. $\psi \circ f = id_{M'}$

and they imply $M \simeq M' \oplus M''$. In this case, we say the sequence **splits**

Example 3.3.7. $R = \mathbb{Z}_4, M = \mathbb{Z}_4, N = \{0, 2\}$. Then $0 \to N \to \mathbb{Z}_4 \to \mathbb{Z}_4/N \to 0$. Notice that $\psi(1) = 0 \implies \psi(2) = 0$ and $\psi(1) = 2 \implies \psi(2) = 0$. Therefore this does not split.

Proof of Proposition. $(1) \implies (2)$: If $m \in M$, then $g(\phi(g(m))) = g(m) \implies g(m - \phi(g(m))) = 0 \implies m - \phi(g(m)) \in ker(g) = \text{Im}(f) \implies \exists! x \in M'$ s.t. $f(x) = m - \phi(g(m))$.

Let $\psi(m) = x$. We need to check that ψ is a R-homomorphism (exercise), and $\psi \circ f = id_{M'}$: if $y \in M'$, let $m = f(y)$. Then $m - \phi(g(m)) = f(y) - \phi(\underbrace{g(f(y))}_{=0}) = f(y)$. By definition of $\psi : \psi(m) = y \implies \psi(f(y)) = y \, \forall y$

$(2) \implies (1)$: Suppose $x \in M''$, then $\exists y \in M$ s.t. $g(y) = x$. Then let $\phi(x) = y - f(\psi(y))$.

This is well-defined: If $y' \in M$ such that $g(y') = x$. I want to check that $y - f(\psi(y)) = y' - f(\psi(y'))$, or $y - y' = f(\psi(y - y'))$. But $g(y - y') = 0$. Since $\ker(g) = \text{Im}(f)$, $\exists z \in M'$ s.t. $y - y' = f(z) \implies f(\psi(y - y')) = f(\psi(f(z))) = f(z) = y - y'$. So ϕ well-defined.

Also $g \circ \phi = id_{M''}$: If $x \in M''$, $\phi(x) = y - f(\psi(y))$ for some $y \in M$ with $g(y) = x$, so $g(\phi(x)) = g(y) - g(f(\psi(y))) = g(y) = x$, since $g \circ f = 0$. Also ϕ is a R-homomorphism, since $\forall r, s \in R, x_1, x_2 \in M'', \phi(rx_1 + sx_2) = r\phi(x_1 + s\phi(x_2))$.

Direct Sum: Define

$$M' \oplus M'' \xrightarrow{\alpha} M, (x, y) \mapsto f(x) + \phi(x)$$

$$M \xrightarrow{\beta} M' \oplus M'', m \mapsto (\psi(m), g(m))$$

Then $\beta \circ \alpha(x, y) = \beta(f(x) + \phi(y)) = (x, y)$, since $\psi \circ \phi = 0$ (Show this as an exercise:) ■

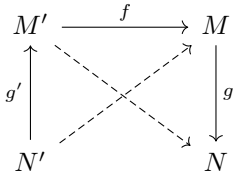
3.4 Module Homomorphism

Definition 3.4.1. Let M, N be R-module, with $Hom_R(M, N)$ being the **set of R-homomorphism** $f : M \longrightarrow N$, and $Hom_R(M, N)$ has the structure of an R-module.

Let $f, g \in Hom_R(M, N)$ if $f + g \in Hom_R(M, N)$. Note $(rf)(m) = rf(m), (f + g)(m) = f(m) + g(m)$. We have

$$Hom_R(M, N) \xrightarrow{-\circ f} Hom_R(M', N)$$

$$Hom_R(N, M') \xrightarrow{f \circ -} Hom_R(N, M)$$

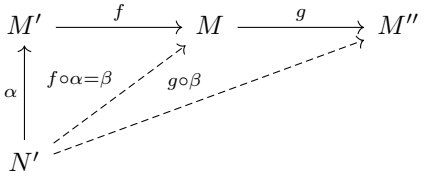


Lemma 3.4.2. If $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is a short exact sequence of R-modules and N is a R-module, then

$$(1). \quad 0 \to Hom_R(N, M') \xrightarrow{\psi} Hom_R(N, M) \xrightarrow{\phi} Hom_R(N, M'') \text{ exact}$$

$$(2). \quad 0 \longrightarrow Hom_R(M'', N) \longrightarrow Hom(M, N) \longrightarrow Hom(M', N) \text{ exact}$$

Proof.



$Hom_R(N, M') \to_R Hom(N, M)$ injective: If $f \circ \alpha = 0$ for some $\alpha \in Hom_R(N, M')$, then since f injective, $\alpha = 0$.

$\phi \circ \psi = 0 (\implies \text{Im}(\psi) \subset ker(\phi))$: If $\alpha \in Hom_R(N, M')$, then $\phi \circ \psi(\alpha) = g \circ f \circ \alpha = 0$, where $g \circ f = 0$ since it is exact.

If $\beta \in \ker(\phi)$, then $g \circ \beta = 0$, so for any $x \in N, g(\beta(x)) = 0$, so $\beta(x) \in \text{Im}(f) \implies$ there is a unique $y \in M'$ such that $f(y) = \beta(x)$. Let $\alpha : N \to M'$ be defined by $\alpha(x) = y$, then α is a R-homomorphism (Exercise). And clearly $\beta = f \circ \alpha$, so $\beta \in \text{Im}(\psi)$ ■

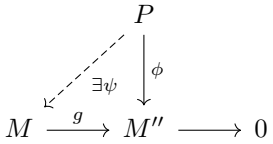
Remark: If $M' \subseteq M$ is a submodule, then $0 \to M' \to M \to M/M'$ is a short exact sequence. If $g : M \to M''$ is a surjective R homomorphism, then $0 \to ker(g) \to M \to M'' \to 0$ is a short exact sequence.

3.5 Free Module

Definition 3.5.1. If M is a R-module, and $S \subset M$ is a **basis** if $\forall m \in M, m = r_1 s_1 + ... + r_k s_k$ in a *unique* way with $r \in R, s \in S$. Equivalently, if $0 = r_1 s_1 + ... + r_k s_k$, then $r_1 = ... = r_k = 0$. If $\{s_i\}_{i \in \mathcal{I}}$ is a basis for M, then $M \simeq \bigoplus_{i \in \mathcal{I}} R$. Then, M is **free** is it has a *basis*.

Definition 3.5.2. If R is a ring and P is a R-module, then P is a **projective module** if it satisfies the following:

1. If g, ϕ are R homomorphism, $\exists \psi : P \to M$, R-homomorphism s.t. $g \circ \psi = \phi$

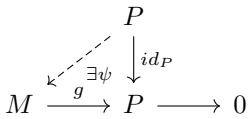


2. If $0 \to M' \to M \to P \to 0$ is exact, then it splits.
3. There is a R-module N such that $N \oplus P$ is a *free module*.
4. If $0 \to M' \to M \to M''$ is exact, then

$$0 \to Hom(P, M') \to Hom(P, M) \to Hom(P, M'') \to 0$$

is exact.

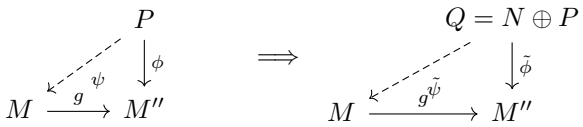
$(1) \implies (2)$. If $0 \to M' \to M \to P \to 0$ is exact, then by (1) $\exists \psi : P \to M$ s.t. $g \circ \psi = id_P$, so the sequence splits



■

(2) $\implies$ (3). Let $\{x_i\}_{i\in\mathcal{I}}$ be a generating subset of P as a R-module. Then, $g : \bigoplus_{i\in I} R \to P, (r_i)_{i\in I} \mapsto \sum_{i\in I} r_i x_i$. is surjective. Then, $0 \to ker(g) \to \bigoplus_{i\in I} R \to P \to 0$ is a short exact sequence. By (2) this splits, so free R-module $\bigoplus_{i\in I} R \simeq ker(g) \oplus P$. ■

(3) $\implies$ (4). It is enough to show that $Hom(P, M) \to Hom(P, M'')$ is surjective. If P is free and $(x_i)_{i\in I}$ is a basis for P and let $y_i = \phi(x_i)$ and $z_i \in m$ s.t. $g(z_i) = y_i$. Then let $\psi(x_i) = z_i$ and $\psi(\sum r_i x_i) = \sum r_i z_i$. Then $g \circ \psi = \phi$. If $N \bigoplus P$ is free, then $\tilde{\phi}(r, p) = \phi(p)$ is a R homomorphism, $\exists\tilde{\psi} : N \oplus P \to M$ such that $g \circ \tilde{\psi} = \tilde{\phi}$. Define $\psi : P \to M, \psi(p) = \tilde{\psi}(n, p)$, then $g \circ \psi = \phi$.



■

(4) $\implies$ (1). The surjective map $g : M \to M'$ gives a short exact sequence $0 \to ker(g) \to M \to M'' \to 0$. So by (4) there is a surjective map $Hom(P, M'') \to Hom(P, M)$. This is exactly 1. ■

Example 3.5.3. $R = \mathbb{Z}_6$. Let $\mathbb{Z}_6$ be a $\mathbb{Z}_6$-module and $I_1 = \{0, 3\}, I_2 = \{0, 2, 4\}$. Then $I_1 \cap I_2 = \{0\}$ and $I_1 + I_2 = \mathbb{Z}_6 \implies \mathbb{Z}_6 = I_1 + I_3$. So by 3, I_1, I_2 are projective modules but not free.

3.6 Finitely Generated Modules over PIDs

Theorem 3.6.1. If R is a PID and M is a finitely generated module over R, then

$$M \simeq R \oplus \cdots \oplus R \oplus \frac{R}{p_1^{n_1}} \oplus \cdots \oplus \frac{R}{p_k^{n_k}}$$

where $p_1, ..., p_k$ are irredcible (prime) elements of R. In particular, finitely generated projective modules are free over R.

Let R be an integral domain and M be a R-module, $m \in M$. m is torsion if there is $0 \neq r \in R$ s.t. $rm = 0$. So let M_{tor} be set of torsion elements in M, so M_{tor} is a submodule, where $m_1, m_2 \in M_{tor} \implies m_1 + m_2 \in M_{tor}$. M is torsion if $M = M_{tor}$, and if torsion-free if $M_{tor} = \{0\}$. Free modules are torsion-free.

Recall that for abelian groups, torsion free does not imply free, take $\mathbb{Q}$ as example. Meanwhile, torsion free and finitely generated implies free group.

However in arbitrary integral domain, torsion free and finitely generated does *not* imply free group. One example would be $R = \mathbb{C}[x, y], M = (x, y)$ [proof of example not written down]

Fact: Suppose R is a PID

- A submodule of a finitely generated R-module is finitely generated
- If M is finitely generated R-module, then $M \simeq M_{tor} \oplus N$ for a free R-module N.

Note, making it a PID makes everything similar to $\mathbb{Z}$

3.7 Tensor Products

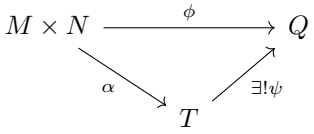
Let R be a ring and M, N be R-modules. Let F be a free module generated by elements $(m, n), m \in M, n \in N$. $F = \{r_1(m_1, n_1) + ... + r_k(m_k, n_k) \,|\, r_i \in R, m_i \in M, n_i \in N\}$. D is the submodule of F generated by elements of the forms below

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
- $(rm, n) - r(m, n)$
- $(m, rn) - r(m, n)$

with $r \in R, m, m_1, m_2 \in M, n, n_1, n_2 \in N$.

Let $T := F/D$ be an R-module. Note there is a map $\alpha : M \times N \longrightarrow T, \alpha(m, n) = (m, n) + D$. This map is bilinear: $\alpha(r_1 m_1 + r_2 m_2, n) = r_1\alpha(m_1, n) + r_2\alpha(m_2, n)$ and $\alpha(m, r_1 n_1 + r_2 n_2) = r_1\alpha(m, n_1) + r_2\alpha(m, n_2)$

Proof of above requires us to show $(r_1 m_1 + r_2 m_2, n) - r_1(m_1, n) - r_2(m_2, n) \in D$. Rewrite expression into $((r_1 m_1 + r_2 m_2, n) - (r_1 m_1, n) - (r_2 m_2, n)) + ((r_1 m_1, n) - r_1(m_1, n)) + ((r_2 m_2, n) - r_2(m_2, n))$



T has the following *universal property*: If Q is a R-module and $\phi : M \times N \longrightarrow Q$ is a bilinear map, then there is a unique R-homomorphism $\psi : T \to \mathbb{Q}$ with $\phi = \psi \circ \alpha$, and define $\psi((r_1(m_1, n_1) + ... + r_k(m_k, n_k)) + D) = r_1\phi(m_1, n_1) + ... + r_k\phi(m_k, n_k)$.

We need to check that ψ is well-defined and is a R-homomorphism. For well-defined, it suffices to show that elements $\in D$.

We denote **tensor product** of M and N as $M \otimes_R N = T = F/D$. Any element is of the form

$$r_1(m_1, n_1) + ... + r_k(m_k, n_k) + D = \underbrace{(r_1 m_1, n_1) + ... + (r_k m_k, n_k) + D}_{:= r_1 m_1 \otimes n_1 + ... + r_k m_k \otimes n_k}$$

Proposition 3.7.1. The following properties are satisfied:

1. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$
2. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
3. $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$
4. $0 \otimes n = 0 = m \otimes 0$

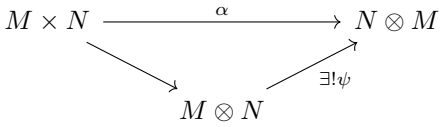
Example 3.7.2.

- $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$: $a \otimes \frac{b}{c} = a \otimes \frac{bp}{cp} = pa \otimes \frac{b}{cp} = 0 \otimes \frac{b}{cp} = 0$.
- $\mathbb{Z}_2 \otimes \mathbb{Z}_3 = \{0\} : 0 \otimes x = 0, 1 \otimes 0, 2 = 0$. Finally $1 \otimes 1 = 1 \otimes (2 + 2) = 2 \otimes 1 + 2 \otimes 1 = 0 + 0 = 0$.
- $gcd(m, n) = 1, \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$

Proposition 3.7.3. If M, N, P are R-modules, then

- $M \otimes_R N \simeq N \otimes_R M$
- $(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P)$
- $M \otimes_R (N \oplus P) \simeq M \otimes_R N \bigoplus M \otimes_R P$
- $M \otimes_R R \simeq R \otimes_R M \simeq M$

Proposition 1 Proof. $M \times N \xrightarrow{\alpha} N \otimes M$ is clearly bilinear, $(m,n) \mapsto n \otimes m$



By the universal property, we have R-homomorphism $\psi(m \otimes n) = \alpha(m,n) = n \otimes m$. Conversely, $\exists R$-homomorphism $\phi : N \otimes M \to M \otimes N$, and $n \otimes m \mapsto m \otimes n$, and $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps. ■

Proposition 2 Proof. Fix $m \in M$ and define $\alpha_m : N \times P \to (M \otimes N) \otimes P, (n,p) \mapsto (m \otimes n) \otimes p$. Then, α_m is bilinear: $\alpha_m(n, p_1 + p_2) = \alpha_m(n,p_1) + \alpha_m(n,p_2)$. $\alpha_m(n_1 + n_2, p) = \alpha_m(n_1,p) + \alpha_m(n_2,p)$. $\alpha_m(m,p) = r\alpha_m(n,p)$. $\alpha_m(n,rp) - r\alpha_m(n,p)$. Together, this implies that $\exists R$-homomorphism $\psi_m : N \otimes P \longrightarrow (M \otimes N) \otimes P$.

Now, we have a bilinear map $\psi : M \times (N \otimes P) \to (M \otimes N) \otimes P, \psi(m,x) = \psi_m(x)$ and show that this is bilinear.

- $\psi(m, x_1 + x_2) = \psi(m,x_1) + \psi(m,x_2)$
- $\psi(m, rx) = r\psi(m,x)$

So ψ_m is a R-homomorphism. Also $\psi(m_1 + m_2, x) = \psi(m_1,x) + \psi(m_2,x)$ and $\psi(rm,x) = r\psi(m,x)$ so $\psi_{m_1+m_2} = \psi_{m_1} + \psi_{m_2}$.

Since there is a bilinear map, $\exists R$-homomorphism $\gamma : M \otimes (N \otimes P) \to (M \otimes N) \otimes P, m \otimes (n \otimes p) = (m \otimes n) \otimes p$.

Similarly, there is a $R-$homomorphism $\beta : (M \otimes N) \otimes P = M \otimes (N \otimes P), (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$. γ, β are inverse maps, so they are isomorphisms. ■

Proposition 4 Proof. There is a binear map $M \times R \xrightarrow{\alpha} M, (m,r) \mapsto rm$ bilinear. So there is an R-homomorphism $\psi : M \otimes R \to M, m \otimes r \mapsto rm$. Also there is an R-homomorphism $\phi : M \to M \otimes R, m \mapsto m \otimes 1$. $\psi \circ \phi = id, \phi \circ \psi(m \otimes r) = \phi(rm) = rm \otimes 1 = m \otimes r \implies \phi \circ \psi = id \implies \phi$ isomorphism. ■

Example 3.7.4. Consider $R[x] \otimes_R R[x]$, where R is a commutative ring, we claim that $R[x] \otimes R[x] \simeq R[x,y]$.

Let $\phi : R[x] \otimes_R r[x] \to R[x,y]$ be the R-homomorphism induced by the bilinear map $R[x] \times R[x] \longrightarrow R[x,y], (f(x), g(x)) \mapsto f(x)g(y)$.

To define ψ, note that $R[x,y]$ is a free module over R with basis $x^i y^j, 0 \le i,j$. Let $\psi : R[x,y] \to R[x] \otimes_R R[x]$ be such that $\psi(x^i y^j) = x^i \otimes x^j$.

ϕ, ψ are inverse maps: $x^i y^j \xrightarrow{\psi} x^i \otimes x^j \xrightarrow{\phi} x^i y^j$, $f(x) \otimes g(x) = \sum_{i,j} c_{i,j} x^i \otimes x^j, x^i \otimes x^j \xrightarrow{\phi} x^i y^j \xrightarrow{\psi} x^i \otimes x^j$.

Proposition 3.7.5. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules, and let N be an R module, then

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$$

is exact. Here, $M' \xrightarrow{f} M$ induces $M' \otimes N \xrightarrow{f \otimes id} M \otimes N$, $\sum m_i' \otimes n_i \mapsto \sum f(m_i') \otimes n_i$.

Lemma 3.7.6. Let M, N, Q be R modules, then $Hom_R(M \otimes_R N, Q) \simeq Hom_R(M, Hom_R(N,Q))$.

Corollary 3.7.7. If $Q = R$, $(M \otimes_R N)^\vee \simeq Hom_R(M, N^\vee)$.

Example 3.7.8. Let k be a field, $R = k[x,y]/(x,y), M = R/(x), N = R/(y)$. Then, $M \otimes_R N = R/(x) \otimes R(y) \simeq R/(x,y)$. Also, $(M \otimes_R N)^\vee \simeq (R/(x,y))^\vee = Hom_R(R/(x,y), R) = \{0\}$.

Also, $M^\vee = Hom(R/(x), R) \simeq M, N^\vee = Hom(R/(y), R) \simeq N$. Consider $\phi : R/(x) \to R, 1 \mapsto \bar{f}, 0 = \bar{x} \mapsto \overline{xf} = 0, f \in k[x,y] \implies xf \in (xy) \implies f \in (y)$.

So $M^\vee \otimes N^\vee \simeq M \otimes N \simeq R/(x,y) \neq \{0\}$.

Proposition Proof using Lemma. If $M' \to M \to M'' \to 0$ is exact, then let Q be an arbitrary R-module and take $Hom(-, Hom_R(N, Q))$. Then we have exact sequence

$$0 \to Hom(M'', Hom_R(M'', Q)) \to Hom_R(M, Hom_R(N, Q)) \to Hom_R(M', Hom(N, Q))$$

So we have an exact sequence

$$0 \to Hom_R(M'' \otimes N, Q) \to Hom_R(M \otimes N, Q) \to Hom_R(M' \otimes N, Q)$$

So by homework 9 question, $M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$ is exact. ■

Example 3.7.9. Let $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \to Z_2$ be a short exact sequence of $\mathbb{Z}$-modules and tensored with $\mathbb{Z}_2$, where $f : a \mapsto 2a$.

Then, $\underbrace{\mathbb{Z} \otimes \mathbb{Z}_2}_{\simeq \mathbb{Z}_2} \to \mathbb{Z} \otimes \mathbb{Z}_2$. [fill in from notes]

Proof of Lemma. Define $\phi : Hom_R(M \otimes_R N, Q) \to Hom_R(M, Hom_R(N, Q))$, where $(\alpha : M \otimes N \to P) \mapsto (\beta : M \to Hom_R(N, Q))$. $\beta : m \mapsto \beta_m, \beta(n) = \alpha(m \otimes n) \in Q$.

I need to show that β is R-homomorphism, ϕ is R-homomorphism.

β homomorphism: $\beta \in Hom_R(M, Hom_R(N, Q))$: Show that $\beta_{r_1 m_1 + r_2 m_2} = r_1\beta_{m_1} + r_2\beta_{m_2}$. So, $\beta_{r_1 m_1 + r_2 m_2}(n) = \alpha((r_1 m_1 + r_2 m_2) \otimes n) = \alpha(r_1(m_1 \otimes n) + r_2(m_2 \otimes n))$, and $(r_1\beta_{m_1} + r_2\beta_{m_2})(n) = r_1\alpha(m_1 \otimes n) + r_2\alpha(m_2 \otimes n)$, which is true

ϕ homomorphism shown similarly.

Also define $\psi : Hom_R(M, Hom_R(N, Q)) \to Hom_R(M \otimes_R N, Q)$ with $\beta : M \to Hom_R(N, Q)$ given. Define bilinear map $M \times N \to Q, (m, n) \mapsto \beta(m)(n)$, this gives a map $\alpha : M \otimes_R N \to Q$.

So ϕ, ψ are inverse maps. ■

Definition 3.7.10. A module F is **flat** if for any short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, the following sequence is exact:

$$0 \to M' \otimes F \xrightarrow{f \otimes id} M \otimes F \xrightarrow{g \otimes id} M'' \otimes F \to 0$$

Equivalently, F is **flat** if for any R-homomorphism $f : M' \to M, M' \otimes F \to M \otimes N$ is injective.

Example 3.7.11. $\mathbb{Z}_2$ is not a flat $\mathbb{Z}$-module. Consider $\mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$. $\mathbb{Z} \otimes \mathbb{Z}_2 \to \mathbb{Z} \otimes \mathbb{Z}_2, a \otimes b \mapsto 2a \otimes b = a \otimes 2b = 0$. Not injective, so this is not flat.

Example 3.7.12. Suppose R is an integral domain:

- Free modules are flat. If F is a free R-module, $F \simeq \bigoplus_{i \in I} R, f : M' \to M$ is an injective map that gives the following injectvitiy.

$$\begin{array}{ccc} M' \otimes F & & M' \otimes (\bigoplus_i R) & & \bigoplus_i M' \otimes R & & \bigoplus_i M' \\ \downarrow{\scriptstyle f \otimes id} & \simeq & \downarrow{\scriptstyle f \otimes id} & \simeq & \downarrow{\scriptstyle \bigoplus f \otimes id} & \simeq & \downarrow{\scriptstyle \oplus f} \\ M \otimes F & & M \otimes (\bigoplus_i R) & & \bigoplus_i M \otimes R & & \bigoplus_i M \end{array}$$

- More generally, projective modules are flat. If P is projective, $\exists P'$ s.t. for a free module F, $F = P \oplus P'$. Then if $M' \to M$ is injective, then $M' \otimes F \to M \otimes F$ by the previous example. So $M' \otimes P \bigoplus M' \otimes P' \longrightarrow M \otimes P \bigoplus M \otimes P'$ is an injective map $\implies M' \otimes P \to M \otimes P$ is injective.

- Flat module does not necessarily imply projective modules. $\mathbb{Q}$ as a $\mathbb{Z}$-module is flat. [Check 11/29 minute 30 for proof] But $\mathbb{Q}$ is not projective. Suppose $\mathbb{Q} \oplus P'$ is free, then pick a basis and write $(1,0) = \lambda_1 x_1 + ... + \lambda_n x_n$, $x_1, ..., x_n$ part of a basis and $\lambda_1, ..., \lambda_n \in \mathbb{Z}$. Pick N where $N > |\lambda_1|, ..., |\lambda_n|$. Then write $(\frac{1}{N}, 0)$ as a combination of basis elements, where $(\frac{1}{N}, 0) = c_1 x_1 + ... + c_n x_n$, where $c_1, ..., c_n \in \mathbb{Z}$ may be 0. So $(1,0) = Nc_1 x_1 + ... + Nc_n x_n$. If $c_i \neq 0$, then $|Nc_i| > |\lambda_i|$, so they cannot be equal.
- If F is a flat R-module, then it is torsion-free. We need to show that if $0 \neq x \in F$ and $0 \neq r \in R$, then $rx \neq 0$. Let $R \xrightarrow{f} R$, $s \mapsto rs$ be multiplication by r. Then f is injective since R is an integral domain. So, $R \otimes F \xrightarrow{f \otimes id} R \otimes F$ is injective. $0 \neq 1 \otimes x \mapsto r \otimes x = 1 \otimes rx$. So $1 \otimes rx \neq 0, rx \neq 0$

Note: Free $\implies$ Projective $\implies$ Flat $\implies$ Torsion-free

Let $R \xrightarrow{f} S$ be a ring homomorphism.

- Any S-module M has the structure of an R-module, $rm : f(r)m$
- Now, suppose N is a module over R. $N \otimes_R S$ is a R-module which has the structure of S-module, $s(n_1 \otimes s_1) := n_1 \otimes ss_1$

If $\phi : N_1 \to N_2$ is a R-homomorphism, $\phi \otimes id : N_1 \otimes S \to N_2 \otimes_R S$ is a S-homomorphism.

Chapter 4

Category Theory

Definition 4.0.1. A category $\mathcal{C}$ consists of a collection (class) of objects $Obj(\mathcal{C})$. For any two objects A, B of $\mathcal{C}$, a set of morphisms $Hom_{\mathcal{C}}(A, B)$ satisfies for any object $A \subset Obj(\mathcal{C})$, there is a morphism $1_A \in Hom_{\mathcal{C}}(A, A)$ and a composition function $Hom_{\mathcal{C}}(A, B) \times Hom_{\mathcal{C}}(B, C) \longrightarrow Hom_{\mathcal{C}}(A, C), (f, g) \mapsto gf$. which is associative: $(hg)f = h(gf), f1_A = f, 1_B f = f$.

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

Example 4.0.2.

- $\mathcal{C}$ is a category of sets $Obj(\text{set})$, and $Hom_{\text{set}}(A, B)$ are functions from A to B.
- Let S be a set with a relation $\sim$ that is reflexive and transitive, and $\mathcal{C}$ is a category $obj(\mathcal{C})$. $Hom_{\mathcal{C}}(a, b) = \phi$ if $a \not\sim b$ and $\{(a, b)\}$ if $a \sim b$.

  $a \in obj(\mathcal{C}), 1_a = (a, a)$ with composition $(a, b) \in Hom(a, b), (b, c) \in Hom(b, c)$ therefore $(b, c)(a, b) = (a, c)$.
- Let $\mathcal{C}$ be a category, $A \in Obj(\mathcal{C})$ and $\mathcal{C}_A$ be a new catory, where objects are morphism from any object of $\mathcal{C}$ to A.

  $$Hom_{\mathcal{C}_A}(f, g) = \{\sigma \in Hom_{\mathcal{C}}(B, C) \mid g\sigma = f\}$$

  and $Hom_{\mathcal{C}_A}(f, g) \times Hom_{\mathcal{C}_A}(g, h) \to Hom_{\mathcal{C}_A}(f, h), (\sigma, \alpha) \mapsto \alpha\sigma$. So $h(\alpha\sigma) = (h\alpha)\sigma = g\sigma = f$, and $1_B f = f$.

4.1 Morphisms

Definition 4.1.1. Let $\mathcal{C}$ be a category, $f \in Hom_{\mathcal{C}}(A, B)$. Then f is an **isomorphism** if it has a two-sided inverse under composition with $g \in Hom(B, A)$ so that $gf = 1_A, fg = 1_B$. This inverse is unique, and is denoted by f^{-1}.

This has the properties that

- $(1_A)^{-1} = 1_A$
- $(fg)^{-1} = g^{-1}f^{-1}$
- $(f^{-1})^{-1} = f$

Example 4.1.2.

- If $\mathcal{C}$ is a set, then isomorphism are bijections.
- $\sim$ on S: (a, b) is an isomorphism $\iff b \sim a$

Definition 4.1.3. $f \in Hom_{\mathcal{C}}(A, B)$ is a **monomorphism** if $\forall C \in Obj(\mathcal{C})$ and $g_1, g_2 \in Hom_{\mathcal{C}}(A, C)$ with fg_1, fg_1, we have $g_1 = g_2$.

Definition 4.1.4. f is an **epimorophism** if $\forall C \in Obj(\mathcal{C}), h_1, h_2 \in Hom_{\mathcal{C}}(B, C)$ with $h_1 f = h_2 f$, we have $h_1 = h_2$

Example 4.1.5.
- For $\mathcal{C}$ a set, a monomorphism is injective and epimorphism is surjective.
- For $S, \sim$, all morphisms are monomorphism and epimorphism.

4.2 Initial and Final Objects

Definition 4.2.1. For category $\mathcal{C}, I \in Obj(\mathcal{C})$ is **initial** if for any $A \in Obj(\mathcal{C}), Hom_{\mathcal{C}}(I, A)$ has one element. $F \in Obj(\mathcal{C})$ is **final** if for any $A \in Obj(\mathcal{C})$, then $Hom_{\mathcal{C}}(A, F)$ has one element.

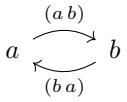
Example 4.2.2.
- For $\mathcal{C}$ a set, $\varnothing$ is the initial object, any singleton set is a final object.
- For $(S, \sim)$ with $(\mathbb{Z}, \leq)$, there is no initial or final object.

Note: Initial and final objects are unique up to isomorphism.

Example 4.2.3.
- For category of sets, initial object is $\varnothing$ and final object is singleton set.
- For category of groups, initial object is $\{e\}$ and final is also $\{e\}$.
- For category of rings, intial object is $\mathbb{Z}$, final object is $\{0\}$.
- For category of R-modules, initial element is $\{0\}$ and final is $\{0\}$.
- For category of fields, there are no initial and final objects

Definition 4.2.4. A category $\mathcal{C}$ is a **groupoid** if every morphism is an isomorphism.

Example 4.2.5. If $\sim$ on S is an equivalence relation,

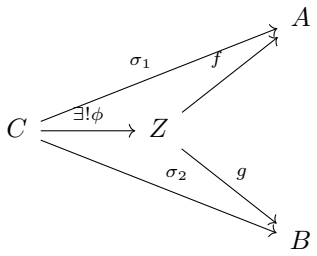


Definition 4.2.6. If $A \in Obj(\mathcal{C})$ isomorphisms $\in Hom(A, A)$ are **automorphism**, they form a group denoted by $Aut(A)$

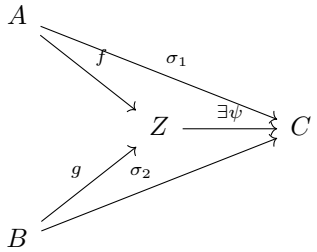
Fact: A *group* is a *groupoid* of 1 object!

4.3 Product and Coproduct

Definition 4.3.1. Let $\mathcal{C}$ be a category with $A, B \in Obj(\mathcal{C})$. Z is a **product** of A, B if $\exists f \in Hom(Z, A), g \in Hom(Z, B)$ such that $\forall C \in Obj(\mathcal{C})$, $\sigma_1 \in Hom(C, A), \sigma_2 \in Hom(C, D), \exists! \phi \in Hom(C, Z)$ s.t. $f \circ \phi = \sigma_1, g \circ \phi = \sigma_2$



Definition 4.3.2. It is a coproduct is the following diagram commutes:



If product (coproduct) of A, B then it is unique up to isomorphism. If Z, Z' coproduct $\psi : Z \to Z', \phi : \mathbb{Z} \to Z$ (replace C with Z' from above). Then $\phi \circ \sigma_2 = g, \psi \circ g = \sigma_2$.

Example 4.3.3. For set A, B, $A \times B$ is the product and the coproduct is the disjoint union $A \sqcup B$. By definition, $\{1, 2\} \sqcup \{2, 3\} = \{1, 2, 2', 3\}$.

Example 4.3.4. For groups G_1, G_2, the product is $G_1 \times G_2$ and the coproduct is free product $G_1 * G_2$ (Note that $G_1 \times G_2$ is only coproduct when it is abelian.)

4.4 Functors

Definition 4.4.1. Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories and $F : \mathcal{C} \to \mathcal{D}$ is a **covariant functor** if $\forall A \in Obj(\mathcal{C})$, $F(A) \in Obj(\mathcal{C})$ and a function $Hom_{\mathcal{C}}(A, B) \to Hom_{\mathcal{D}}(F(A), F(B))$ such that

- $F(1_A) = 1_{F(A)}$. $A \xrightarrow{\beta} B \xrightarrow{\alpha} Z$
- $F(\alpha\beta) = F(\alpha)F(\beta)$. $F(A) \xrightarrow{F(\beta)} F(B) \xrightarrow{F(\alpha)} F(Z)$

4.5 Limits

Definition 4.5.1.

Chapter 5

Answer to Selected Problems

Exercises 1.1

1. Exercise 1.1-1

i. Let $a \in G$. By (5), $ya = a$ has a solution $y_0 \in G$. We need that for other $b \in G$, the equation $y_0 b = b$ also holds. This is true because $ax = b$ has a solution $x_0 \in G$, so $b = ax_0 = y_0 a x_0 = y_0(ax_0) = y_0 b$. This shows the existence of a left identity $e_l = y_0$. The existence of a left inverse directly follows from the fact that there is a solution $y \in G$ for $yg = e_l$.

ii. Let a^{-1} be the left inverse of $a \in G$. Let a' be the left inverse of a^{-1}. Thus, $a^{-1}a = e_l$ and $a'a^{-1} = e_l$. On the one hand, $\left(a'a^{-1}\right)\left(aa^{-1}\right) = e_l\left(aa^{-1}\right) = (e_l a)a^{-1} = aa^{-1}$ on the other hand $\left(a'a^{-1}\right)\left(aa^{-1}\right) = a'\left[\left(a^{-1}a\right)a^{-1}\right] = a'\left(e_l a^{-1}\right) = a'a^{-1} = e_l$ so $aa^{-1} = e_l$.

iii. On the one hand, $\left(aa^{-1}\right)a = e_l a = a$. On the other hand, $\left(aa^{-1}\right)a = a\left(a^{-1}a\right) = ae_l$. Thus, $ae_l = a$, which shows that e_l is also the right identity. Therefore, $e_l = e_r = e$, and this in turn elevates "$a^{-1}a = e_l \Rightarrow aa^{-1} = e_l$" to become "$a^{-1}a = e \Rightarrow aa^{-1} = e$."

iv. For the eq. $ax = b$, just take $x = a^{-1}b$ which is in G as $a^{-1} \in G$ and G is closed under multiplication. Similarly, for the eq. $ya = b$, just take $y = ba^{-1} \in G$.

2. Exercise 1.1-6

i. Trivial.

ii. Follows immediately from prop. 1.1.24.

3. Exercise 1.1-7: Let the statement be $p(n)$. We use the strong induction. First we see that $n = 2, 3$ the claim is true. Now assume that for $n \leq N-1$ the proposition $p(n)$ is true. To show $p(N)$ is true, we only need to show that for any bracketing $\pi\left(a_1 \cdot a_2 \cdot \cdots \cdot a_n\right)$ we have

$$\pi\left(a_1 \cdot a_2 \cdot \cdots \cdot a_n\right) = a_1 \cdot \left(a_2 \cdot \cdots \cdot a_n\right)$$

where the bracket on the RHS is well-defined by our induction hypothesis. any bracketing $\pi\left(a_1 \cdot a_2 \cdot \cdots \cdot a_n\right)$, its last step of computation has to be of the form $b_1 \cdot b_2$ where

$$b_1 = a_1 \cdot a_2 \cdot \cdots \cdot a_i, b_2 = a_{i+1} \cdot a_{i+2} \cdot \cdots \cdot a_n$$

Since $i, n-i \leq N-1$, we by induction hypothesis have them well-defined. To show

$$\begin{aligned}\pi\left(a_1 \cdot \cdots \cdot a_n\right) &= \left(a_1 \cdot a_2 \cdot \cdots \cdot a_i\right) \cdot \left(a_{i+1} \cdot \cdots \cdot a_n\right) \\ &= a_1 \cdot \left(a_2 \cdot \cdots \cdot a_n\right)\end{aligned}$$

we see for $i = 1$ there is nothing to prove, so we assume $i > 1$ and observe

$$\begin{aligned}&\pi\left(a_1 \cdot a_2 \cdot \cdots \cdot a_n\right) \\ &= \left(a_1 \cdot a_2 \cdot \cdots \cdot a_i\right) \cdot \left(a_{i+1} \cdot a_{i+2} \cdot \cdots \cdot a_n\right) \\ &\overset{IH(i)}{=\!=} \left(a_1 \cdot \left(a_2 \cdot \cdots \cdot a_i\right)\right) \cdot \left(a_{i+1} \cdot a_{i+2} \cdot \cdots \cdot a_n\right) \\ &\overset{IH(3)}{=\!=} a_1 \cdot \left(a_2 \cdot \cdots \cdot a_i\right) \cdot \left(a_{i+1} \cdot a_{i+2} \cdot \cdots \cdot a_n\right) \\ &\overset{IH(N-1)}{=\!=\!=} a_1 \cdot \left(a_2 \cdot \cdots \cdot a_i \cdot a_{i+1} \cdot a_{i+2} \cdot \cdots \cdot a_n\right) \\ &= a_1 \cdot \left(a_2 \cdot \cdots \cdot a_n\right)\end{aligned}$$

We're done.

4. Exercise 1.1-8: We proceed by weak induction. For $n = 1, 2$ the statement is true. Suppose the statement is true when $n = N-1$. We want to show that permutating $a_1 \cdot a_2 \cdot \cdots \cdot a_N$, which is $a_{i_1} \cdot a_{i_2} \cdot \cdots \cdot a_{i_N}$, won't change the result. Suppose the permutation sends N to i_k. Let C stand

for commutativity and A stand for associativity. Then

$$\begin{aligned}
&a_{i_1}\cdot a_{i_2}\cdot\cdots\cdot a_{i_N}\\
&=\left(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\right)\cdot\left[a_{i_k}\cdot\left(a_{i_{k+1}}\cdot\cdots\cdot a_{i_N}\right)\right]\\
&=\left(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\right)\cdot\left[a_N\cdot\left(a_{i_{k+1}}\cdot\cdots\cdot a_{i_N}\right)\right]\\
&\overset{C(2)}{=\!=}\left(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\right)\cdot\left[\left(a_{i_{k+1}}\cdot\cdots\cdot a_{i_N}\right)\cdot a_N\right]\\
&\overset{A(2)}{=\!=}\left[\left(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\right)\cdot\left(a_{i_{k+1}}\cdot\cdots\cdot a_{i_N}\right)\right]\cdot a_N\\
&\overset{\text{Thm1.1.15},A(N-1)}{=\!=\!=\!=}\left(a_{i_1}\cdots a_{i_{k-1}}\cdot a_{i_{k+1}}\cdots a_{i_N}\right)\cdot a_N\\
&\overset{IH}{=\!=}\left(a_1\cdot\cdots\cdot a_{N-1}\right)\cdot a_N\\
&\overset{A(N)}{=\!=}a_1\cdot\cdots\cdot a_{N-1}\cdot a_N
\end{aligned}$$

5. Exercise 1.1-9: let $l=|a^k|:=\min\{m:(a^k)^m=1\}$. Then: (1) $a^{kl}=(a^k)^l=1\Rightarrow kl\geq|a|=n=km\Rightarrow l\geq m$; (2) $m\geq l$ (because $1=a^{km}=(a^k)^m$). They combine to show $l=m$.

6. Exercise 1.1-10: When $n=1$, G is automatically abelian. For $n=2,3,5$ which are primes, G is cyclic and thus abelian. For $n=4$, one can use Cayley table to do the classification to see that G is isomorphic to either $\mathbb{Z}_4$ or the Klein-four group V, both abelian.

7. Exercise 1.1-11: $n=\min\{m:a^m=1\}\Rightarrow k\geq n$, $k=np+q\Rightarrow 1=a^k=a^{np+q}=(a^n)^pa^q=a^q$. Since $q<n=\min\{m:a^m=1\}$, we see $q=0$.

8. Exercise 1.1-15: the isomorphism is given by $\phi(x)=y$ and note that isomorphism is bijection.

9. Exercise 1.1-16: We write the distinct cosets of K in G as $\{g_iK\}_{i\in I}$. Thus $G=\amalg_{i\in I}g_iK$. Similarly, we write $K=\amalg_{j\in J}k_jH$. We claim that g_ik_jH are all distinct cosets of H in G. Then, as left cosets form a partition, $[G:H]=\left|\{g_ik_jH\}_{i\in I,j\in J}\right|=|I||J|=[G:K][K:H]$, where we used the fact that $[G:H],[H:K]<\infty$. The claim consists of two parts: (1) every left coset xH of H in G is in $\{g_ik_jH\}_{i\in I,j\in J}$ because it is already clear that each g_ik_jH is a coset of H in G. (2) each g_ik_jH is distinct.
proof of (1): For any left coset xK of K in G, $\exists g_i\in G:xK=g_iK\iff g_i^{-1}x\in H$. Then $g_i^{-1}xH$ is a left coset of subgroup H in K and is one of $\{k_jH\}$: $\exists k_j\in K:g_i^{-1}xH=k_jH\Leftrightarrow\exists h\in H:k_j^{-1}g_i^{-1}x=h$ Thus $x=g_ik_jh$ and $xH=g_ik_jhH=g_ik_jH$.
proof of (2): Suppose not. $g_ik_jH=g_{i'}k_{j'}H$ for some $g_i,k_j,g_i',k_j'\iff(g_ik_j)^{-1}(g_{i'}k_{j'})\in H\subseteq K\Rightarrow g_ik_jK=g_{i'}k_{j'}K\Rightarrow g_iK=g_{i'}K\Rightarrow g_i=g_{i'}$ by distinctiveness in $\{g_iK\}_{i\in I}$. Thus

$$g_i\left(k_jH\right)=g_{i'}\left(k_{j'}H\right)\overset{g_i=g_{i'}}{\Longrightarrow}k_jH=k_{j'}H\Rightarrow k_j=k_{j'}$$

by distinctiveness in $\{k_jH\}_{j\in J}$.

10. Exercise 1.1-17: H has index 2, so there are two left cosets H,aH for some $a\in G$ such that $aH\neq H$, i.e., $a\neq H$. Thus, $a^{-1}\notin H\Rightarrow a^{-1}H\neq H\Rightarrow a^{-1}H=aH\Leftrightarrow(a-1)^{-1}a=a^2\in H$. If $a\in H$, then clearly $a^2\in H$. Therefore, $\forall a\in G$, $a^2\in H$.

11. Exercise 1.1-18: use theorem 1.1.28.

Exercises 1.2

1. Exercise 1.2-6: Since every permutation can be written as product of transpositions, it suffices to show that transpositions can be generated in each of the case. Then note that $(m\quad k)=(1\quad m)(1\quad k)(1\quad m)$, and

$$\begin{aligned}
(m,k)=&(m,m+d)\\
=&(k-1,k)\dots(m+1,m+2)(m,m+1)\\
&(m+1,m+2)^{-1}\dots(k-1,k)^{-1}\\
=&(k-1,k)\dots(m+1,m+2)(m,m+1)\\
&(m+1,m+2)\dots(k-1,k)
\end{aligned}$$

Thus each of $(i,i+1)$ in the generating set of S_n is further generated by (12) and $(12\cdots n)$, proving the result. For the third claim, just observe that $(i\ i+1)=(1\ 2\ \cdots\ n)^{i-1}(1\ 2)(1\ 2\ \cdots\ n)^{-i+1}$.

2. Exercise 1.2-7: $S_2=\{(1),(1\ 2)\}\cong\mathbb{Z}_2$. Group table of S_3: let $\sigma_0=(1),\sigma_1=(1\ 2\ 3),\sigma_2=(1\ 3\ 2),\sigma_3=(2\ 3),\sigma_4=(1\ 3),\sigma_5=(1\ 2)$

$\circ$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_2	σ_0	σ_4	σ_5	σ_3
σ_2	σ_2	σ_0	σ_1	σ_5	σ_3	σ_4
σ_3	σ_3	σ_5	σ_4	σ_0	σ_2	σ_1
σ_4	σ_4	σ_3	σ_5	σ_1	σ_0	σ_2
σ_5	σ_5	σ_4	σ_3	σ_2	σ_1	σ_0

3. Exercise 1.2-9: The permutation ρ has a decomposition as a product of disjoint, hence commuting, (non-trivial) cycles: $\rho=\gamma_1\cdots\gamma_r$. By Question 1.2-iii., The order of ρ is the l.c.m. of the orders of the cycles, so each γ_i has order 3. As

the order of a cycle is its length, this means each γ_i is a 3-cycle.

4. Exercise 1.2-10:

i. $(sr)^2 = 1 \implies (sr)^{-1} = r^{-1}s^{-1} = sr \implies s^{-1}r^{-1}s^{-1} = r \implies s^{-1}r^{-1} = rs \implies (rs)^{-1} = rs$. Vice versa.

ii. $r^k s = sr^{-k}$: start with $(rs)^2 = rsrs = 1 \Leftrightarrow rs = s^{-1}r^{-1} \overset{s^2=e}{=} sr^{-1}$, we see for any $k \in \{0, \cdots, n-1\}$,

$$\begin{aligned} r^k s &= \underbrace{r\cdots rr}_{\#=k} s = \underbrace{r\cdots r}_{\#=k-1} rs \\ &= \underbrace{r\cdots r}_{\#=k-1} sr^{-1} = \underbrace{r\cdots r}_{\#=k-2} (rs)r^{-1} \\ &= \underbrace{r\cdots r}_{\#=k-2} sr^{-1}r^{-1} = \cdots = sr^{-k} \end{aligned}$$

iii. immediately follows from Proposition 1.1.24.

5. Exercise 1.2-11: Let

$$D_n = \left\{e, r, \cdots, r^{n-1}, s, sr, \ldots sr^{n-1}\right\}$$

where r is the rotation and s is the reflection $\left(s^2 = e, r^n = e, (rs)^2 = e\right)$. We note that $H = \left\{e, r, r^2, r^3, \ldots, r^{n-1}\right\} = \langle r\rangle$ is a cyclic subgroup contained in D_n with order n. The complement of it is $H^c = \left\{s, sr, sr^2, sr^3, \ldots sr^{n-1}\right\}$, which has order n as well. Since $H^c = sH$ is the coset of H, H is itself a right coset, and there are no other cosets since they fill the whole group, then the index of H in D_n is 2.

Exercises 1.2

1. Exercise 1.3-4:

i.

$$A^2 = -I,\ A^3 = -A,\ A^4 = I$$

so the order of A in G is 4 .

$$B^2 = -I,\ B^3 = -B,\ B^4 = I$$

so the order of B in G is 4.

ii. We already have six distinct elements $I, -I, A, B, A^3, B^3$ above. G is nonabelian with following two additional elements

$$AB = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix},\ BA = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

iii. By the calculation in **i**, it is obvious that I, A, B, A^3, B^3 don't have order 2, while $-I$ has order 2 as $(-I)^2 = I^2 = I$. We check the rest of the eight:

$$(AB)^2 = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = -I \neq I$$

$$(BA)^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = -I \neq I$$

Thus, the only element with order 2 is $-I$.

iv. By Lagrange's theorem $8 = |G| = |H|[G:H]$ for subgroup H in G. Hence, except for subgroup $\{e\}$ and G, which are trivial subgroups that are also normal, we only have factorization $8 = 2 \times 4$ or $8 = 4 \times 2$, i.e, $|H| = 2$ with $[G:H] = 4$ or $|H| = 4$ with $[G:H] = 2$. By an example in class that "every subgroup of index 2 in any group is normal" we see subgroup H_1 with $|H_1| = 4$ is normal. The remaining is H_2 with $|H_2| = 2$. Subgroups H_2 with $|H_2| = 2$ must include an identity I and another element x. Counting formula tells us that $2 = |H_2| = |\langle x\rangle|\,[H_2 : \langle x\rangle]$ where $\langle x\rangle$ is the cyclic subgroup generated by x and the order of it is just the order of the element x. The only possible factorization is $2 = 2 \times 1$, so x is an element of order 2 and $H_2 = \langle x\rangle$. For this problem, $x = -I = A^2 = B^2$ by part **i** and part **iii**. Thus, $H_2 = \langle -I\rangle = \{I, -I\}$. To show H_2 is normal in G, we take any $M \in G$ and see that $MIM^{-1} = I \in H_2$; $M(-I)M^{-1} = -MM^{-1} = -I \in H_2$ Therefore, all subgroups of G are normal.

2. Exercise 1.3-5: We want to show that $\forall x \in NH_1, y \in NH_2, yxy^{-1} \in NH_1$. Thus, $x = n_1h_1$ for some $n_1 \in N$ and $h_1 \in H_1$, and $y = n_2h_2$ for some $n_2 \in N$ and $h_2 \in H_2$. Then

$$yxy^{-1} = n_2h_2n_1h_1h_2^{-1}n_2^{-1}$$

Since $h_2n_1 \in NH_2$, we have $h_2n_1h_2^{-1} \in N \Rightarrow \exists n_3 \in N : h_2n_1h_2^{-1} = n_3 \Rightarrow h_2n_1 = n_3h_2$. We call this step exchanging trick, since it gives a new element in the normal subgroup to switch

the multiplication. Thus,

$$\begin{aligned} yxy^{-1} &= n_2n_3h_2h_1h_2^{-1}n_2^{-1} \\ &= \underbrace{n_4}_{=n_2n_3\in N}\ \underbrace{h_2h_1h_2^{-1}}_{=h_1'\in H_1}\ \underbrace{n_5}_{n_2^{-1}\in N} = n_4h_1'n_5 \end{aligned}$$

By the above exchanging trick, we see $h_1'n_5 \in NH_1 \Rightarrow h_1'n_5h_1'^{-1} \in N \Rightarrow \exists n_6 \in N : h_1'n_5h_1'^{-1} = n_6 \Rightarrow h_1'n_5 = n_6h_1'$. Thus,

$$yxy^{-1} = n_4h_1'n_5 = \underbrace{n_4n_6}_{\in N}h_1' \in NH_1$$

3. Exercise 1.3-6: $A_n \longleftrightarrow S_n - A_n$, the set of all odd permuations, by $\sigma \mapsto \sigma(1\ 2)$. Thus, $[S_n : A_n] = 2$, $A_n \trianglelefteq S_n$, and $|A_n| = \frac{1}{2}n!$.

4. Exercise 1.3-12: see [8] Theorem 2.20.

5. Exercise 1.3-13: The relation $x \sim y \iff \exists g \in G$ s.t. $y = x^g := gxg^{-1}$ is reflexive ($x^e = x$); is transitive ($x^g = y, y^h = z \Rightarrow x^{hg} = z$); and is symmetric ($x^g = y \Rightarrow y^{g^{-1}} = x$). Let $H \leq G$ be a subgroup. It is normal iff $\forall g \in G,\ gHg^{-1} \subseteq H$, i.e., $\forall h \in H,\ \forall g \in G,\ h^g \in H$, which is just saying that for each $h \in H$, the conjugacy class containing h is contained in H.

Exercises 1.4

Exercises 1.5

1. Exercise 1.5-1.

i. The class equation of G is $|G| = 12 = 1+3+4+4$. The four classes are {e},{(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)},{(1 2 3),(1 4 2),(2 4 3),(1 3 4)},{(1 3 2),(1 4 3),(2 3 4),(1 2 4)}. For a direct derivation without first knowing the result, see Math5031 HW3 Q1 (a).

ii. Let $x \in G$. We first observe a fact: since $Z(G)$ is the set of elements that commute with every element of G and $N(x)$ is the set of elements that commute with x, we get $Z(G) \subseteq N(x)$. Now the center of the group $Z(G)$ is a normal subgroup of G, and we by the counting formula have

$$|G| = |Z(G)|[G : Z(G)] = |Z(G)|n$$

As explained in the first part we by the orbit-stabilizer theorem have

$$|G| = |N(x)||C(x)|$$

for each $x \in G$. above two equations combine to give $|N(x)||C(x)| = |Z(G)|n$ Suppose there is some conjugacy class $C(x)$ with $|C(x)| > n$. Then

$$n|Z(G)| = |N(x)||C(x)| > |N(x)|n \Rightarrow |Z(G)| > |N(x)|$$

which is impossible because $Z(G) \subseteq N(x) \Rightarrow |Z(G)| \leq |N(x)|$. Therefore, each conjugacy class has at most n elements.

2. Exercise 1.5-2.

i. We first note that $\sigma^{-1}\rho^{-1}\sigma\rho \in N$ because $\sigma \in N \trianglelefteq A_n \implies \rho^{-1}\sigma\rho \in N$ and $\sigma^{-1} \in N$. We compute

$$\begin{aligned} \sigma^{-1}\rho^{-1}\sigma\rho =& \mu^{-1}(1\ 2\ \dots\ r)^{-1}(1\ 3\ 2)(1\ 2\ \dots\ r)\mu(1\ 2\ 3) \\ \overset{\mu \text{ disjoint; } r\geq 4>3}{=\!=\!=} & (1\ 2\ \dots\ r)^{-1}(1\ 3\ 2)(1\ 2\ \dots\ r)(1\ 2\ 3) \\ =& (1\ r\ \dots\ 2)(1\ 3\ 2)(1\ 2\ \dots\ r)(1\ 2\ 3) \\ =& (1\ r\ \dots\ 2)(1\ 3\ 2)(1\ 3\ 2\ 4\ 5\ \dots\ r) \\ =& (1\ r\ \dots\ 2)(3\ 1\ 2\ 4\ 5\ \dots\ r) \\ =& (2\ 3\ r) \end{aligned}$$

Thus N contains a 3-cycle $(2\ 3\ r)$.

ii. Similar to the reasoning in **i**, $x = \sigma^{-1}\rho^{-1}\sigma\rho \in N \trianglelefteq A_n$. We compute

$$\begin{aligned}\sigma^{-1}\rho^{-1}\sigma\rho =&\mu^{-1}(4\ 5\ 6)^{-1}(1\ 2\ 3)^{-1}(1\ 2\ 4)^{-1}\\ &(1\ 2\ 3)(4\ 5\ 6)\mu(1\ 2\ 4)\\ \overset{\mu \text{ disjoint}}{=\!=\!=}&(4\ 6\ 5)(1\ 3\ 2)\,[(1\ 4\ 2)(1\ 2\ 3)]\\ &[(4\ 5\ 6)(1\ 2\ 4)]\\ =&(4\ 6\ 5)(1\ 3\ 2)(2\ 3\ 4)(1\ 2\ 5\ 6\ 4)\\ =&(4\ 6\ 5)(3\ 4\ 1)(1\ 2\ 5\ 6\ 4)\\ =&(3\ 6\ 5\ 4\ 1)(1\ 2\ 5\ 6\ 4)\\ =&(1\ 2\ 4\ 3\ 6)\end{aligned}$$

Then consider $\rho' = (1\ 2\ 4)$ and apply a similar process as **i** to x:

$$\begin{aligned}x^{-1}\rho'^{-1}x\rho' =&(1\ 6\ 3\ 4\ 2)(1\ 4\ 2)\\ &(1\ 2\ 4\ 3\ 6)(1\ 2\ 4) = (2\ 4\ 6)\end{aligned}$$

which is in N as $x \in N \trianglelefteq A_n \Rightarrow \rho'^{-1}x\rho' \in N$ and $\rho'^{-1} \in N$.

iii. In this case $\mu^{-1} = \mu$, so $\mu\mu = 1$. Noticing $\sigma \in N \leq A_n$ for the last step, we have

$$\begin{aligned}\sigma^2 =&(1\ 2\ 3)\mu(1\ 2\ 3)\mu\\ \overset{\mu \text{ disjoint}}{=\!=\!=}&(1\ 2\ 3)(1\ 2\ 3)\mu\mu\\ =&(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \in N\end{aligned}$$

iv. We compute

$$\begin{aligned}\eta =&\sigma^{-1}\rho^{-1}\sigma\rho\\ =&\mu^{-1}(3\ 4)(1\ 2)(1\ 3\ 2)(1\ 2)(3\ 4)\mu(1\ 2\ 3)\\ \overset{\mu \text{ disjoint}}{=\!=\!=}&(1\ 4)(2\ 3)\end{aligned}$$

and $\zeta = (1\ 5\ 2)\eta(1\ 2\ 5) = (1\ 3)(4\ 5)$. Similar to the reasoning in **i**, we see $\eta \in N$ as $\sigma \in N \trianglelefteq A_n \implies \rho^{-1}\sigma\rho \in N$ and $\sigma^{-1} \in N$. Besides, $\zeta = (1\ 5\ 2)\eta(1\ 2\ 5) = (1\ 5\ 2)\eta(1\ 5\ 2)^{-1} \in N$. Lastly, we observe that $\eta\zeta = (1\ 2\ 3\ 4\ 5)$. This then converts to case **i** for $r = 5$. Thus $(2\ 3\ r) = (2\ 3\ 5)$ is in N.

3. Exercise 1.5-3. We first see two facts: (1) every 3 -cycle (i, j, k) with $i \leq j \leq k$ is a commutator in 2 -cycles:

$$(i,j,k) = (i,k)(i,j) = (i,j)(i,k)(i,j)(i,k) = [(i,j),(i,k)]$$

(2) A_n is generated by 3-cycles (proved in Example 1.5.3). Immediately from (1) and (2), we see every element of A_n is a product of commutators. We then only need to show that every product of commutators is some element in A_n: each commutator is of the form $[x, y]$ where $x \in S_n, y \in S_n$ can be written as product of transpositions, i.e., $x = \sigma_1\sigma_2\cdots\sigma_k, y = \tau_1\tau_2\cdots\tau_l$ for some integers k, l. We then compute:

$$\begin{aligned}[x,y] = xyx^{-1}y^{-1} =&\sigma_1\sigma_2\cdots\sigma_k\tau_1\tau_2\cdots\tau_l\\ &(\sigma_1\sigma_2\cdots\sigma_k)^{-1}(\tau_1\tau_2\cdots\tau_l)^{-1}\\ =&\sigma_1\sigma_2\cdots\sigma_k\tau_1\tau_2\cdots\tau_l\sigma_k\cdots\sigma_2\sigma_1\tau_l\cdots\tau_2\tau_1\end{aligned}$$

There are in total $2(k + l)$ transpositions. Since $2(k+l)$ is even and products of even permutations are still even permutations, making products of commutators belong to A_n.

4. Exercise 1.5-4. Part one is trivial. Part two: First of all, $A_\infty = \cup_{n\geq 1}A_n = \bigcup_{n\geq 5}A_n$ simply because $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_5 \subseteq A_6 \cdots$. To show that A_∞ is simple, we need to show that each $N \trianglelefteq A_\infty$ has to be trivial or the whole A_∞. First notice that each A_n is a group and thus a subgroup of the group A_∞, i.e., $A_n \leq A_\infty$. Then $N \cap A_n \trianglelefteq A_n$ due to the 2^{nd} isomorphism theorem. When $n \geq 5$, this normal subgroup $N \cap A_n$ must be $\{e\}$ or A_n due to the simplicity, i.e., A_n is simple for all $n \geq 5$. We analyze the two cases: If $N \cap A_n = A_n$ for some $n \geq 5$, then $A_n \subseteq N$. Then for all $m \geq n, A_n \subseteq N \cap A_m \Rightarrow N \cap A_m \neq \{e\} \Rightarrow N \cap A_m = A_m \Rightarrow A_\infty = \bigcup_{i\geq 5}A_i = \bigcup_{i\geq n}A_i = \bigcup_{i\geq n}N \cap A_i = N \cap \left(\bigcup_{i\geq n}A_i\right) \Rightarrow A_\infty \subseteq N$ But $N \trianglelefteq A_\infty \Rightarrow N \subseteq A_\infty$, so $A_\infty = N$. If $N \cap A_n = \{e\}$ for some $n \geq 5$. Then for all $m \geq n, N \cap A_m$ cannot be A_m as for if $A_m = N \cap A_m$ then $A_n \subseteq A_m = N \cap A_m \Rightarrow A_n \subseteq N \Rightarrow N \cap A_n = A_n \neq \{e\}$ which is a contradiction. Thus, for all $m \geq n, N \cap A_m = \{e\}$. Thus, $N = N \cap A_\infty = N \cap (\cup_{i\geq 5}A_i) = N \cap N \cap (\cup_{i\geq n}A_i) = \cup_{i\geq n}N \cap A_i = \cup_{i\geq n}\{e\} = \{e\}$. Thus, N is either trivial or the whole group, proving the simplicity of A_∞.

Exercises 1.6

Bibliography

[1] Artin, Michael. *Algebra*, Pearson, 2nd edition, 2010.

[2] Burton, David M. *A First Course in Rings and Ideals*, Addison-Wesley, 1970.

[3] Dummit, David Steven, and Foote, Richard M. *Abstract Algebra*, Wiley, 2004.

[4] Judson, Thomas. *Abstract Algebra: Theory and Applications*, Virginia Commonwealth University Mathematics, 2009.

[5] Kurzweil, Hans, and Stellmacher, Bernd. *The Theory of Finite Groups: An Introduction*, Springer, 2004.

[6] Lang, Serge. *Algebra*, Springer Science+Business Media, 2012.

[7] Mac Lane, Saunders. *Categories for the Working Mathematician*, Springer Science+Business Media, 2013.

[8] Rotman, Joseph J. *An Introduction to the Theory of Groups*, Springer Science+Business Media, 1995.

[9] Rotman, Joseph J. *An Introduction to Homological Algebra*, Springer Science+Business Media, 2009.