LECTURE NOTES [ALGEBRA I (S) (MA2202S)]

Contents

1. Properties of the Integers (Divisibility and congruence)

Notation.

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ denotes the integers.
- $\mathbb{Z}^+$ denotes the positive (nonzero) elements in $\mathbb{Z}$.
- $\mathbb{Q} = \{a/b \colon a, b \in \mathbb{Z}, b \neq 0\}$ denotes the rational numbers.
- $\mathbb{R}$ denotes the real numbers.

If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. We write $a \mid b$; if a does not divide b we write $a \nmid b$. For example, $7 \mid 28$ as $28 = 4 \times 7$; $5 \nmid 24$.

The *Division Algorithm:* if $a, b \in \mathbb{Z} - \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \text{ and } 0 \leq r < |b|,$$

where q is the *quotient* and r the *remainder*. For example, $60 = 3 \times 17 + 9$.

Remark: the key fact about the division algorithm is that the set of common divisors of a and b is the set of common divisors of b and r. In particular it implies that $(a, b) = (b, r)$.

If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer d, called the *greatest common divisor of a and b* (or g.c.d. of a and b), satisfying:

(1) $d \mid a$ and $d \mid b$ (so d is a common divisor of a and b), and
(2) if $e \mid a$ and $e \mid b$, then $e \mid d$ (so d is the greatest such divisor).

The g.c.d. of a and b will be denoted by (a, b). If $(a, b) = 1$, we say that a and b are *relatively prime*. For example, $(24, 18) = 6$, $(21, 26) = 1$.

The existence of g.c.d. as defined above requires a proof. Without loss of generality, assume $a, b \in \mathbb{Z}^+$. Consider the set $J = \{ma + nb\}_{m,n \in \mathbb{Z}}$, and take d to be the smallest positive integer in J. By performing division algorithm and using the minimality of d, one sees that any $j \in J$ is a multiple of d. One checks easily that d satisfies the required properties of the g.c.d..

If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer l, called the *least common multiple of a and b* (or l.c.m. of a and b), satisfying:

(1) $a \mid l$ and $b \mid l$ (so l is a common multiple of a and b), and
(2) if $a \mid m$ and $b \mid m$, then $l \mid m$ (so l is the least such multiple).

The l.c.m. of a and b will be denoted by $[a, b]$. It is easy to check that $(a, b) \cdot [a, b] = ab$. (Why?) For example, $(24, 18) = 6$, $(21, 26) = 1$.

The *Euclidean Algorithm* is a procedure which produces a greatest common divisor of two integers a and b. For example,

$$\begin{aligned}
372 &= 5 \times 69 + 27 \\
69 &= 2 \times 27 + 15 \\
27 &= 1 \times 15 + 12 \\
15 &= 1 \times 12 + 3 \\
12 &= 4 \times 3 + 0 \\
(372, 69) &= 3.
\end{aligned}$$

Find the g.c.d. of 1761 and 1567.

If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

that is, the g.c.d. of a and b is a $\mathbb{Z}$-linear combination of a and b. (See the construction of g.c.d. earlier.) Note that the solution of x and y is not unique.

For example,

$$\begin{aligned}
3 &= 15 - 12 \\
&= 15 - (27 - 15) = 2 \times 15 - 27 \\
&= 2 \times (69 - 2 \times 27) - 27 = 2 \times 69 - 5 \times 27 \\
&= 2 \times 69 - 5 \times (372 - 5 \times 69) \\
&= (-5) \times 372 + 27 \times 69.
\end{aligned}$$

An element p of $\mathbb{Z}^+$ is called a *prime* if $p > 1$ and the only positive divisors of p are 1 and p. An integer which is not prime is called *composite*. For example, $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ are primes and $4, 6, 8, 9, 10, 12, 14, \ldots$ are composite.

The *Fundamental Theorem of Arithmetic* says: if $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes, i.e. there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

For example, $372 = 2^2 \cdot 3 \cdot 31$ and $69 = 3 \cdot 23$.

Suppose that positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

where $p_1, p_2, \ldots, p_s$ are distinct and the exponents are ≥ 0. Then the g.c.d. of a and b is

$$(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_s^{\min(\alpha_s,\beta_s)}.$$

We say that a is *congruent to* $b \bmod n$ if $n \mid (a-b)$. The *congruence class* of $a \bmod n$, denoted by $\bar{a}$, consists of the integers which differ from a by an integral multiple of n i.e.

$$\bar{a} = \{a + kn \colon k \in \mathbb{Z}\} = \{a, a \pm n, a \pm 2n, a \pm 3n, \ldots\}.$$

There are precisely n distinct equivalence classes mod n, namely,

$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1},$$

determined by the possible remainders after division by n. The set of equivalence classes is denoted by $\mathbb{Z}/n\mathbb{Z}$. Define *modular arithmetic* as follows: for $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, define their sum and product by

$$\bar{a} + \bar{b} = \overline{a+b} \text{ and } \bar{a} \cdot \bar{b} = \overline{ab}.$$

For example, $\mathbb{Z}/12\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{11}\}$

Theorem 1.1. *The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined as above are both well defined, that is, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\bar{a}_1 = \bar{b}_1$ and $\bar{a}_2 = \bar{b}_2$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$.*

Proof. Since $\bar{a}_1 = \bar{b}_1$, $a_1 \equiv b_1 \bmod n$ i.e. $n \mid a_1 - b_1$. Then $a_1 = b_1 + sn$ for some integer s. Similarly, $a_2 = b_2 + tn$ for some integer t. Then $a_1 + a_2 = (b_1 + b_2) + (s+t)n$ so that $a_1 + a_2 \equiv b_1 + b_2 \bmod n$ i.e. $\overline{a_1 + a_2} = \overline{b_1 + b_2}$.

Similarly, $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + stn)n$, then $a_1 a_2 \equiv b_1 b_2 \bmod n$. □

Define

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \colon \text{ there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}.$$

Fact: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \colon (a, n) = 1\}$. This is clear as both are equivalent to the fact that $ac + nd = 1$, for some $c, d \in \mathbb{Z}$.

2. Binary operations and Groups

Definition 2.1. A *binary operation* $\circ$ on a set G is a function $\circ\colon G \times G \to G$. For any $a, b \in G$, we write $a \circ b$.

A binary operation $\circ$ on a set G is *associative* if for all $a, b, c \in G$ we have $a \circ (b \circ c) = (a \circ b) \circ c$.

A binary operation $\circ$ on a set G is *commutative* if for all $a, b \in G$ we have $a \circ b = b \circ a$.

Let H be a subset of G. If the restriction of $\circ$ to H is a binary operation on H, i.e., for all $a, b \in H$, $a \circ b \in H$, then H is said to be *closed* under $\circ$.

Example.

- Associative and commutative operators: $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{R}, +)$ and $(\mathbb{R}, \times)$.
- Associative and non-commutative operators: $(M_{n\times n}(\mathbb{R}), \times)$, where $M_{n\times n}(\mathbb{R})$ is the set of n-by-n matrices with entries in $\mathbb{R}$.
- Non-associative and non-commutative operators: $(\mathbb{Z}, -)$.

Example. $(\mathbb{Z}^+, -)$ is not a binary operator.

Definition 2.2. A group is an ordered pair $(G, \circ)$ where G is a set and $\circ$ is a binary operator on G satisfying the following axioms:

(1) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$, i.e. $\circ$ is *associative*,
(2) there exists an element e in G, called an *identity* of G we have $a \circ e = e \circ a = a$,
(3) for each $a \in G$ there is an element a^{-1} of G, called an *inverse* of a such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Example.

(1) $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$ for all a.
(2) $\mathbb{Q}^\times := \mathbb{Q} - \{0\}$ and $\mathbb{R}^\times := \mathbb{R} - \{0\}$ are groups under $\times$ with $e = 1$ and $a^{-1} = \frac{1}{a}$.

$(G, \circ)$ is called *a finite group* if in addition G is a finite set.

$(G, \circ)$ is called *abelian or commutative* if $a \circ b = b \circ a$ for all $a, b \in G$.

Example. Define $\mathrm{GL}_n(\mathbb{R}) = \{g \in M_{n\times n}(\mathbb{R})\colon \det(g) \neq 0\}$, i.e. the set of all n-by-n invertible matrices. $\mathrm{GL}_n(\mathbb{R})$ is a group under $\times$ with $e = I_n$ and $A^{-1} = A^{-1}$ for all A. Note that $\mathrm{GL}_n(\mathbb{R})$ is not abelian.

Example. Define the operation $\circ$ on $\mathbb{R}^\times \times \mathbb{R}$ by $(a, b) \circ (c, d) = (ac, ad + b)$. Show that $(\mathbb{R}^\times \times \mathbb{R}, \circ)$ is a group.

Proof. The operation $\circ$ is closed as $(a, b) \circ (c, d)$ is in $\mathbb{R}^\times \times \mathbb{R}$, and so it is a binary operation.

Associative. Let $(a,b),(c,d),(x,y)$ in $\mathbb{R}$.

$$\begin{aligned}((a,b)\circ(c,d))\circ(x,y) =& (ac, ad+b)\circ(x,y) = (acx, acy+ad+b)\\ (a,b)\circ((c,d)\circ(x,y)) =& (a,b)\circ(cx, cy+d) = (acx, acy+ad+b)\\ =& ((a,b)\circ(c,d))\circ(x,y).\end{aligned}$$

Then the operation is associative.

Identity. Assume that (c,d) is an identity. For all $(a,b)\in\mathbb{R}^\times\times\mathbb{R}$, we have $(a,b)\circ(c,d)=(a,b)$. Equivalently,

$$\begin{aligned}(a,b)\circ(c,d)=(a,b) &\iff (ac, ad+b)=(a,b)\\ &\iff ac=a \text{ and } ad+b=b \qquad (\text{ for all } a,b).\end{aligned}$$

Then $c=1$ and $d=0$, $(1,0)$ is an identity.

Inverse. Let (a,b) be in $\mathbb{R}$. If (x,y) is an inverse of (a,b), then $(a,b)\circ(x,y)=(1,0)$. We have

$$\begin{aligned}&(a,b)\circ(x,y)=(ax, ay+b)=(1,0)\\ &ax=1 \text{ and } ay+b=0.\end{aligned}$$

Solve $x=a^{-1}$ and $y=-ba^{-1}$. We also need to check $(a^{-1},-ba^{-1})\circ(a,b)=(1,0)$. Hence $(a^{-1},-ba^{-1})$ is the inverse of (a,b). □

Note that this group is not commutative or (abelian).

Remark: If one makes the identification $(a,b)\leftrightarrow\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}$, then the operation $\circ$ becomes matrix multiplication in $\mathrm{GL}_2(\mathbb{R})$.

Theorem 2.3. *Let $(G,\circ)$ be a group.*

1. *There exists a unique element $e\in G$ such that $e\circ a=a=a\circ e$ for all $a\in G$, that is, the identity of G is unique.*
2. *For all $a\in G$, there exists a unique $b\in G$ such that $a\circ b=e=b\circ a$.*
3. *$(a^{-1})^{-1}=a$ for all $a\in G$.*
4. *$(a\circ b)^{-1}=b^{-1}\circ a^{-1}$.*
5. *(Cancellation Law) For all $a,b,c\in G$, if either $a\circ c=b\circ c$ or $c\circ a=c\circ b$, then $a=b$.*
6. *For all $a,b\in G$, the equations $a\circ x=b$ and $y\circ a=b$ have unique solutions in G for x and y.*

Proof. (1). Let e,f be identities of $(G,\circ)$. Since e is an identity, $e\circ a=a$ for all $a\in S$. Take $a=f$, then $e\circ f=f$. Similarly, since f is an identity, $e\circ f=e$. Thus $f=e\circ f=e$.

(2). Let $a\in G$ and b be its inverse, that is, $a\circ b=b\circ a=e$. Suppose that there exists $c\in G$ such that $a\circ c=c\circ a=e$. It is enough to show

that $b = c$. Now

$$\begin{aligned} b =& b \circ e = b \circ (a \circ c) \\ =& (b \circ a) \circ c \\ =& e \circ c \\ =& c. \end{aligned}$$

(3). a^{-1} is the inverse of a. Vice versa, a is also the inverse of a^{-1}. Since the inverse of a^{-1} is unique, $(a^{-1})^{-1} = a$.

(4).

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ e \circ b = b^{-1} \circ b = e$$

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = e.$$

Thus, $b^{-1} \circ a^{-1}$ is the inverse of $a \circ b$. By the uniquness of the inverse, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

(5). Let $a, b, c \in G$. Suppose $a \circ c = b \circ c$. Now

$$\begin{aligned} & (a \circ c) \circ c^{-1} = (b \circ c) \circ c^{-1} \\ \Rightarrow & a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1}) \\ \Rightarrow & a \circ e = b \circ e \\ \Rightarrow & a = b. \end{aligned}$$

(6). First we consider the equation $a \circ x = b$. Multiplying a^{-1} on the both sides of the equation, $(a^{-1} \circ a) \circ x = a^{-1} \circ b$. Then $x = a^{-1} \circ b$ is a solution of the equation.

Now we show that the solution is unique. Suppose that c is any solution of $a \circ x = b$. Then $a \circ c = b$. Hence

$$\begin{aligned} c =& e \circ c \\ =& (a^{-1} \circ a) \circ c \\ =& a^{-1} \circ (a \circ c) \\ =& a^{-1} \circ b. \end{aligned}$$

This yields the uniqueness of the solution.

Similar arguments hold for the equation $y \circ a = b$.

□

Theorem 2.4. *An ordered pair $(G, *)$ is a group if and only if*

(1) *$\circ$ is an associative binary operator,*
(2) *there exists $e \in G$ such that $e * a = a$ for all $a \in G$, (i.e. e is a left identity) and*
(3) *for all $a \in G$ there exists $b \in G$ such that $b * a = e$, (i.e. b is a left inverse).*

Remark. An equivalent definition of groups is that the right identity and the right inverse exist beside the binary operation is associative.

Proof. "$\Rightarrow$". It follows from the definition of groups.

"$\Leftarrow$". It is sufficient to show that e is a right identity and b is also a right inverse.

Let a be an element in G. By (3), there exists $b \in G$ such that $b * a = e$. For such b, there exists $c \in G$ such that $c * b = e$. We have

$$a = e * a = (c * b) * a = c * (b * a) = c * e.$$

Then

$$a * b = (c * e) * b = c * (e * b) = c * b = e.$$

b is a right inverse of a.

Since

$$a * e = a * (b * a) = (a * b) * a = e * a = a,$$

e is a right identity. □

Remark. Let $\circ$ be an associative binary operation on G, which has the left identity and the right inverse. Then G is not a group in general. For example, let $G = \{e, a\}$ with $a \neq e$. Define the operation table as following

$\circ$	e	a
e	e	a
a	e	a

It is easy to check that $\circ$ is associative. e is the left identity since $e \circ e = e$ and $e \circ a = a$. a has the right inverse $a \circ e = e$. However, there is not right identity as $a \circ e = e$. Hence it is not a group.

Definition 2.5. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = e$. The multiplication table or group table of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

Example. $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$.

	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{11}$	$\bar{1}$	$\bar{5}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

Definition 2.6. For G a group and $x \in G$, define the order of x to be the smallest positive integer n such that $x^n = 1$ (if such n exists), denoted by $o(x)$.

Example.
$(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$.

	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
	1	6	3	6	3	2

Theorem 2.7. *Let $(G, *)$ be a group and a be an element of G with $o(a) = n$.*

(1) *If $a^m = e$ for some positive integer m, then n divides m.*

(2) *For every positive integer t,*

$$o(a^t) = \frac{n}{(t, n)}.$$

In particular if $(t, n) = 1$, we have $o(a^t) = n$.

Proof. (1). By the division algorithm, there exist $q, r \in Z$ such that$m = nq + r$, where $0 \leq r < n$. Now

$$a^r = a^{m-nq} = a^m * a^{-nq} = e * e^{-q} = e.$$

Since $o(a) = n$, n is the smallest positive integer such that $a^n =$ e. But $a^r = e$ and $0 \leq r < n$. We have $r = 0$. Hence n divides m.

(2). Let $o(a^t) = k$. Then $a^{kt} = e$. By (1), n divides kt. Since $(\frac{n}{(n,t)}, \frac{t}{(n,t)}) = 1$, $\frac{n}{(n,t)}$ divides k.

On the other hand,

$$(a^t)^{\frac{n}{(n,t)}} = a^{n\frac{t}{(n,t)}} = e^{\frac{t}{(n,t)}} = e.$$

By (1), k divides $\frac{n}{(n,t)}$. Hence $o(a^t) = \frac{n}{(n,t)}$. □

3. Examples of Groups

A subset S of elements of a group G with the property that every element of G can be written as a finite product of elements of S and their inverses is call a set of *generators* of G We write $G = \langle S \rangle$.

A *presentation* of G is given by generators and relations, written as

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle.$$

Here a relation means an equality of two expressions which are both finite products of elements of S and their inverses.

Cyclic group. A group G is called a *cyclic group* if G is generated by one element, i.e.

$$G = \langle x \rangle.$$

For example, $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ and $\mathbb{Z} = \langle 1 \rangle$.

The quadratic fields.

Let D be a square-free integer, that is, D can not be divided by a perfect square except 1. Define

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \colon a, b \in \mathbb{Q}\}.$$

The addition and the multiplication are defined by, for $a + b\sqrt{D}$ and $x + y\sqrt{D}$ in $\mathbb{Q}[\sqrt{D}]$,

$$(a + b\sqrt{D}) + (x + y\sqrt{D}) := (a + x) + (b + y)\sqrt{D}$$

and

$$(a + b\sqrt{D}) \cdot (x + y\sqrt{D}) = (ax + byD) + (ay + bx)\sqrt{D}.$$

Then $(\mathbb{Q}[\sqrt{D}], +)$ and $(\mathbb{Q}[\sqrt{D}]^\times, \cdot)$ are groups.

The Quaternion group.

The *quaternion group* Q_8 is defined by

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

The product $\cdot$ is defined as follows:

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

Define

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

An element of $\mathbb{H}$ is called a quarternion.

Dihedral groups.
Define the **dihedral group** by

$$D_{2n} = \{r, s \mid r^n = s^2 = 1, rs = sr^{-1}\}.$$

Note that

(1) $1, r, \ldots, r^{n-1}$ are all distinct as $o(r) = n$.
(2) $s \neq r^i$ for any i.
(3) $sr^i \neq sr^j$ for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}.$$

Example. Let sr^i be in D_{2n}. Then $o(sr^i) = 2$.
Example.

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

g	1	r	r^2	r^3	s	sr	sr^2	sr^3
$o(g)$	1	4	2	4	2	2	2	2

Example. Let $n = 12$. Calculate $(sr^9)(sr^6)$.

$$(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-3} = r^9.$$

Example. Define

$$Y = \langle x, y \mid x^4 = y^3 = 1, xy = y^2 x^2 \rangle.$$

It turns out that $Y = \{1\}$, which is difficult to see.

Fact: Among the groups we have seen in this section, D_{2n} $(n \geq 3)$ and Q_8 are non-abelian groups.

Example.

Let $X = \{1, 2, 3\}$ be a set and S_X be the set of all bijective functions from X to X. Then $(S_X, \circ)$ is a group, where $\circ$ is the composition of functions.

Then the identity element is

$$id\colon 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3.$$

Write

$$f\colon 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$$

and

$$g\colon 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3.$$

Then

$$S_X = \{id, f, f^2, g, g \circ f, g \circ f^2\}.$$

Definition 4.1. Let $\Omega = \{1, 2 \ldots, n\}$ be a set. $(S_\Omega, \circ)$ is called *the symmetric group of degree* n, similarly denoted by S_n.

Fact: The order of S_n is $n!$.

Indeed, let σ be in S_n,

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{array}$$

The second row is a permutation of $\{1, 2, \ldots, n\}$.

Cycle decomposition.

The map

$$\begin{array}{cccccc} a_1 & a_2 & a_3 & \cdots & a_{m-1} & a_m \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\ a_2 & a_3 & a_4 & \cdots & a_m & a_1 \end{array}$$

is denoted by $(a_1, a_2, a_3, \ldots, a_{m-1}, a_m)$, called m-cycle.

Then each $\sigma \in S_n$ can be written as a product of disjoint cycles, that is,

$$(a_1, a_2, a_3, \ldots, a_{m_1})(a_{m_1+1}, a_{m_1+2}, \ldots, a_{m_2}) \cdots (a_{m_{k-1}+1}, a_{m_{k-1}+2}, \ldots, a_{m_k}).$$

This cycle decomposition is unique, up to the order of the factors.

For example, σ is given by

$$\begin{array}{cccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{array}$$

The cycle decomposition for σ is written as

$$\sigma = (1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9).$$

Example S_3**.**

Values of σ	Cycle Decomposition of σ
$\sigma(1)=1, \sigma(2)=2, \sigma(3)=3$	1
$\sigma(1)=1, \sigma(2)=3, \sigma(3)=2$	(2,3)
$\sigma(1)=3, \sigma(2)=2, \sigma(3)=1$	(1,3)
$\sigma(1)=2, \sigma(2)=1, \sigma(3)=3$	(1,2)
$\sigma(1)=2, \sigma(2)=3, \sigma(3)=1$	(1,2,3)
$\sigma(1)=3, \sigma(2)=1, \sigma(3)=2$	(1,3,2)

Example. Let $\sigma = (1,3,5)(2,4)$ and $\tau = (1,5)(2,3)$. Find the cycle decomposition of $\sigma\tau$. Then

$$\sigma \circ \tau = (1)(2,5,3,4) = (2,5,3,4)$$

and

$$\tau \circ \sigma = (1,2,4,3)(5) = (1,2,4,3).$$

Fact: S_n is non-abelian for all $n \geq 3$.

Fact: The order of $(a_1, \ldots, a_m)$ is m.

Due to the disjoint nature of cycles in the cycle decomposition, the following result is easy.

Proposition 4.2. *The order of a permutation is the l.c.m of the lengths of the cycles in its cycle decomposition.*

Proposition 4.3. *Any element σ in S_n can be written as a product of 2-cycles.*

Proof. It is enough to show that any m-cycle can be written as a product of 2-cycles. This follows from

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2).$$

□

Theorem 4.4. *Then*

$$S_n = \langle (1,2), (1,3), \ldots, (1,n) \rangle.$$

Proof. By Proposition 4.3, it is sufficient to show that every 2-cycle (a,b) is a product of 2-cycles in $\{(1,2), (1,3), \ldots, (1,n)\}$. Indeed,

$$(a,b) = (1,a)(1,b)(1,a).$$

□

Definition 4.5. Let $\sigma \in S_n$. σ is called an *even permutation* if σ is a product of an even number of 2-cycles; otherwise σ is called an *odd permutation*.

We supply a proof that the above notion is well-defined. We introduce the following polynomial D of n-variables:

$$D = \prod_{i<j}(x_i - x_j).$$

Define $\sigma D = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$. Then one shows that $\sigma D = (-1)^k D$, if σ is written as a product of k number of 2-cycles. Thus the parity of k is independent of the product expression.

For example, $\sigma = (a_1, a_2, \ldots, a_m)$ is an even permutation if m is odd; it is an odd permutation if m is even.

Let A_n be the subset of S_n consisting of all even permutations.

Theorem 4.6. *A_n is a group, called the alternating group.*

Proof. Let σ and τ in A_n. σ and τ are products of even numbers of 2-cycles. Then $\sigma \circ \tau$ are products of even numbers of 2-cycles. Therefore, $\circ$ is a binary operation on A_n.

The identity $e = (1, 2)(2, 1)$ is also in A_n.

For $\sigma \in A_n$, assume that $\sigma = (a_1, a_2)(a_3, a_4) \cdots (a_{2m-1}, a_{2m})$. Then

$$\sigma^{-1} = (a_{2m-1}, a_{2m}) \cdots (a_3, a_4)(a_1, a_2).$$

Thus σ^{-1} is in A_n.

Therefore, A_n is a group.

□

5. Subgroups

Definition 5.1. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses, i.e., $x, y \in H$ implies x^{-1} and $xy \in H$.

If H is a subgroup of G, write $H \leq G$.

Example.

(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.
(2) $A_n \leq S_n$.
(3) Let G be any group. Then $\{e\} \leq G$ and $G \leq G$.
(4) For $x \in G$, $\langle x \rangle \leq G$.

Proposition 5.2 (The Subgroup Criterion)**.** *A subset H of a group G is a subgroup if and only if*

(1) *$H \neq \emptyset$, and*
(2) *for all $x, y \in H$, $xy^{-1} \in H$.*

Proof. "⇒". It follows from the definition.

"⇐". Assume that H satisfies (1) and (2). Taking $y = x$, we have $xx^{-1} = 1 \in H$. By (2), for $x \in H$, $1 \cdot x^{-1}$ is in H and then H is closed under inverse.

For $y \in H$, as above y^{-1} is in H. Then for $x, y^{-1} \in H$, we have $x(y^{-1})^{-1} = xy \in H$. □

Definition 5.3. Define $Z(G) = \{g \in G \colon gx = xg \text{ for all } x \in G\}$. This subset is called the *center* of G.

Proposition 5.4. *We have $Z(G) \leq G$.*

Proof. For all $g \in G$, $eg = ge = g$. Thus $\{e\} \in Z(G)$ and $Z(G)$ is not empty.

Let $x, y \in Z(G)$. For all $g \in G$, we have $xg = gx$ and $yg = gy$. Then $(xy)g = x(yg) = xgy = gxy$. Hence $xy \in Z(G)$ and $Z(G)$ is closed under product.

Also multiplifying x^{-1} on the both sides of $xg = gx$ on the left and right, we have $gx^{-1} = x^{-1}g$. Hence $x^{-1} \in Z(G)$ and $Z(G)$ is closed under inverse. Therefore, $Z(G)$ is a subgroup of G. □

Proposition 5.5. *Let $n \geq 3$.*

$$Z(D_{2n}) = \begin{cases} \{1, r^{n/2}\} & \text{if } n \text{ is even} \\ \{1\} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Assume that n is odd. For r^i with $1 \leq i \leq n-1$, consider $r^i s$ and sr^i. Then $r^i s = sr^{-i} \neq sr^i$, and r^i with $1 \leq i \leq n-1$ and s are

not in $Z(D_{2n})$. For $r^i s$ with $1 \leq i \leq n-1$, consider $(r^i s) \cdot s$ and $s \cdot (r^i s)$. Then $(r^i s) \cdot s = r^i \neq r^{-i} = s \cdot (r^i s)$, and $r^i s$ with $1 \leq i \leq n-1$ is not in $Z(D_{2n})$. Hence $Z(D_{2n}) = \{1\}$.

Assume that n is even. By a similar argument, r^i and $r^i s$ with $1 \leq i \neq \frac{n}{2} \leq n-1$ are not in $Z(D_{2n})$. Since $r^{n/2}$ commutes with r and s, $r^{n/2}$ is in $Z(D_{2n})$. Also, by $n \geq 3$, $r^{\frac{n}{2}-1} \neq r^{\frac{n}{2}+1}$ and then

$$(r^{n/2} s) \cdot r = r^{\frac{n}{2}-1} s \neq r^{\frac{n}{2}+1} s = r \cdot (r^{n/2} s).$$

Hence $Z(D_{2n}) = \{1, r^{n/2}\}$.

□

Definition 5.6. Let A be any nonempty subset of G. Define $C_G(A) = \{g \in G \colon gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G.

Define $gAg^{-1} = \{gag^{-1} \colon a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \colon gAg^{-1} = A\}$.

Proposition 5.7. *Let A be any nonempty subset of G. Then $C_G(A)$ and $N_G(A)$ are subgroups of G.*

Proof. See the tutorial. □

Example. Let $G = S_3$ and $A = \{1, (1,2,3), (1,3,2)\}$. Then

$$C_G(A) = A \text{ and } N_G(A) = G.$$

Definition 5.8. Let A be any subset of the group G define

$$\langle A \rangle = \cap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called subgroup of G generated by A. In the other words,

$$\langle A \rangle = \{a_1^{n_1} a_2^{n_2} \cdots a_r^{n_r} \colon a_i \in A,\ \forall n_i \in \mathbb{Z},\ \forall r \in \mathbb{Z}_{\geq 0}\}.$$

5.1. **The lattice of subgroups of a group.**

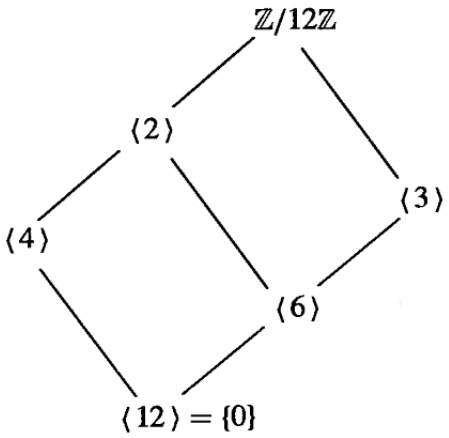


FIGURE 1. The lattice of subgroups of $\mathbb{Z}/12\mathbb{Z}$

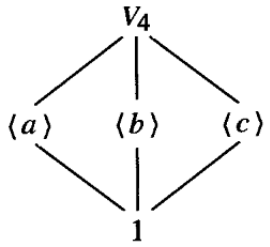


FIGURE 2. The lattice of subgroups of V_4 (the Klein 4-group)

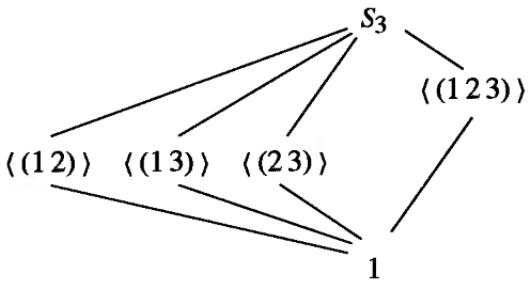


FIGURE 3. The lattice of subgroups of S_3

6. Cyclic groups

Recall that a group G is *cyclic* if G can be generated by a single element, i.e., $G = \langle x \rangle$.

Example.

(1) $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group and $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$.

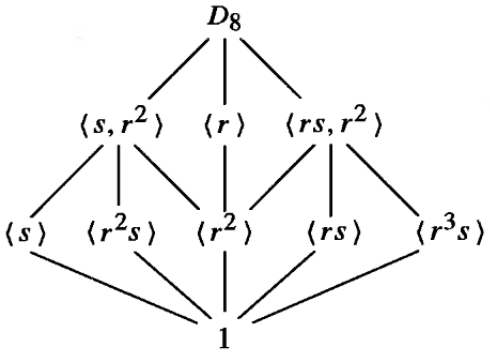


FIGURE 4. The lattice of subgroups of D_8

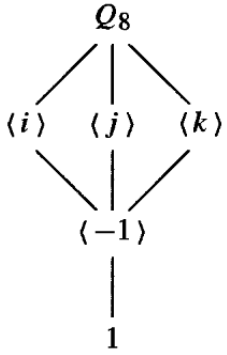


FIGURE 5. The lattice of subgroups of Q_8

(2) $(\mathbb{Z}, +)$ is a cyclic group and $\mathbb{Z} = \langle 1 \rangle$.

Proposition 6.1. *If $G = \langle x \rangle$, then $|G| = o(x)$. More specifically,*

(1) *if $|G| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of G, and*
(2) *if $|G| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

Proof. Let $o(x) = n$. First, consider $n < \infty$. The elements $1, x, x^2, \ldots, x^{n-1}$ are all the distinct. If it is not, say $x^a = x^b$ with $0 \leq a, b < n$ and then $x^{|a-b|} = e$, contrary to n being the order. Hence G has at least n elements. On the other hand, every element in G is of form x^t. Use the Division Algorithm to write $t = nq + r$ with $0 \leq r < n$, so $x^t = x^r$ is in $\{1, x, x^2, \ldots, x^{n-1}\}$. Therefore $G = \{1, x, x^2, \ldots, x^{n-1}\}$.

Next, suppose that $o(x) = \infty$. If $x^a = x^b$ for some $-\infty < a \neq b < \infty$, then $x^{|a-b|} = 1$, a contradiction. Similarly, we have $G = \{x^n : n \in \mathbb{Z}\}$ and $|G| = \infty$. □

Proposition 6.2. *Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^{(m,n)} = 1$.*

Proof. By the Euclidean Algorithm, there exist a and b such that $ma + nb = (m, n)$. Then

$$x^{(m,n)} = x^{ma+nb} = (x^a)^m (x^n)^b = 1.$$

□

Proposition 6.3. *Let $G = \langle x \rangle$.*

(1) *Assume that $o(x) = \infty$. Then $G = \langle x^a \rangle$ if and only if $a = \pm 1$.*
(2) *Assume that $o(x) = n < \infty$. Then $G = \langle x^a \rangle$ if and only if $(a, n) = 1$.*

Proof. (1). $x^{\pm 1}$ can not be generated by any element x^t in G with $|t| > 1$.

(2). By Proposition 6.1, $G = \langle x^a \rangle$ if and only if $|G| = o(x^a)$. Since $o(x^a) = o(x)$ is equivalent to $n = \frac{n}{(n,a)}$, we have $G = \langle x^a \rangle$ if and only if $(n, a) = 1$. □

Example. $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$.

Theorem 6.4. *Let $G = \langle x \rangle$ be a cyclic group.*

(1) *Every subgroup G is cyclic. More precisely, if $H \leq G$, then either $H = \{1\}$ or $H = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in H$.*
(2) *If $|G| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$.*
(3) *If $|G| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of G of order a. This subgroup is the cyclis group $\langle x^{\frac{n}{a}} \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of G correspond bijectively with the positive divisors of n.*

Proof. (1). Let $H \leq G$. If $H = \{1\}$, the proposition is true. Consider $H \neq \{1\}$. There exists some x^a with $a \neq 0$ such that $x^a \in H$. Since $x^{-a} \in H$, H always contains some positive power of x. Let d be the smallest positive integer such that $x^d \in H$. Then $\langle x^d \rangle \leq H$. Since H is a subgroup of G, any element of H is of the form x^a for some integer a. By the Division Algorithm write $a = qd + r$ with $0 \leq r < d$. Then $x^r = x^a (x^d)^{-q}$ is in H. By the minimality of d it follows that $r = 0$, i.e., $a = qd$. Thus $H \leq \langle x^d \rangle$ and $H = \langle x^d \rangle$.

(2). The proof is similar to the part (1).

(3). Assume that $|G| = n < \infty$ and $a \mid n$. Let $d = \frac{n}{a}$ and then $\langle x^d \rangle$ is a subgroup of order a, showing the existence of a subgroup of order

a. To show uniqueness, suppose H is any subgroup of G of order a. By part (1), we have $H = \langle x^b \rangle$, where b is the smallest positive integer such that $x^b \in H$. By Proposition 6.1, we have

$$\frac{n}{d} = a = |H| = o(x^b) = \frac{n}{(n, b)},$$

so $d = (n, b)$. In particular, $d \mid b$. Since b is a multiple of d, $x^b \in \langle x^d \rangle$, hence $H = \langle x^b \rangle \leq \langle x^d \rangle$. Since $|\langle x^d \rangle| = a = |H|$, we have $H = \langle x^d \rangle$. □

7. Cosets

Definition 7.1. For any $H \leq G$ and any $g \in G$ let

$$gH = \{gh \colon h \in H\} \text{ and } Hg = \{hg \colon h \in H\}$$

called respectively a *left coset* and a *right coset* of H in G.

Any element of a coset is called a *representative* for the coset.

Note that if G is abelian, then the right coset and the left coset are equal, i.e., $gH = Hg$.

Example 1.

Consider the subgroup $\langle n \rangle \leq \mathbb{Z}$. Then one has n distinct left cosets

$$\begin{aligned}
&0 + \langle n \rangle = \{\cdots, -2n, -n, 0, n, 2n, \cdots\} \\
&1 + \langle n \rangle = \{\cdots, 1-2n, 1-n, 1, 1+n, 1+2n, \cdots\} \\
&\vdots \\
&n-1 + \langle n \rangle = \{\cdots, -n-1, -1, n-1, 2n-1, \cdots\}
\end{aligned}$$

Example 2.

Let $G = S_3$ and $H = \langle (1,2) \rangle \leq G$. Then we have 3 left cosets

$$\begin{aligned}
H &= \{1, (1,2)\} = (1,2)H \\
(1,3)H &= \{(1,3), (1,2,3)\} = (1,2,3)H \\
(2,3)H &= \{(2,3), (1,3,2)\} = (1,3,2)H
\end{aligned}$$

and 3 right cosets

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

Proposition 7.2. *Let $H \leq G$ and $a, b \in G$.*

1. *$aH = bH$ if and only if $b^{-1}a \in H$. In particular, $aH = H$ if and only if $a \in H$.*
2. *If $aH \cap bH \neq \emptyset$, then $aH = bH$.*
3. *$|aH| = |H|$ for all $a \in G$.*

Proof. (1). "$\Rightarrow$" By $aH = bH$, $a \in bH$ and $a = bh$ for some $h \in H$. Then $b^{-1}a = h \in H$.

"$\Leftarrow$" If $b^{-1}a \in H$, then $a = bh$ and $b = ah^{-1}$ for some $h \in H$. For any $x \in H$, $ax = bhx$. Then $ax \in bH$ as $hx \in H$ and $aH \subseteq bH$. Similarly, $bx = ah^{-1}x$. Then $bx \in aH$ and $bH \subseteq aH$. Hence $aH = bH$.

(2). Suppose that $aH \cap bH \neq \emptyset$. Let $x \in aH \cap bH$. We have $x = au = bv$ for some $u, v \in H$. Then $b^{-1}a = vu^{-1} \in H$. By (1), we have $aH = bH$.

(3). Define the map $L_a \colon H \to aH$ via $L_a(h) = ah$. Then for any $a \in G$, L_a is bijective as $L_a \circ L_{a^{-1}} = L_{a^{-1}} \circ L_a = id$. Hence $|aH| = |H|$. □

Definition 7.3. The index of a subgroup H in G, denoted by $[G \colon H]$, is the number of left cosets of H in G.

Let $a_1H, a_2H, \ldots, a_tH$ be the family of all the distinct cosets of H in G. Then we have a disjoint

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH.$$

It follows

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|.$$

By Proposition 7.2, $|G| = t|H|$. Then we have the following theorem.

Theorem 7.4 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$. Moreover, $|G| = [G \colon H]|H|$.*

Corollary 7.5. *If G is a finite group and $a \in G$, then the order of a is a divisor of $|G|$.*

Proof. For $a \in G$, let $H = \langle a \rangle$. Then $o(a) = |H| \mid |G|$. □

Corollary 7.6. *If G is a finite group, then $a^{|G|} = 1$ for all $a \in G$.*

Corollary 7.7. *If p is a prime, then every group G of order p is cyclic.*

Proof. Let $a \in G$ and $a \neq 1$. Then $o(a) > 1$. Since $o(a)$ divides $|G| = p$, $o(a) = p$. Thus $G = \langle a \rangle$ and G is cyclic. □

Corollary 7.8 (Fermat's little theorem)**.** *If p is a prime and $a \in \mathbb{Z}/p\mathbb{Z}$, then $a^p \equiv a \bmod p$.*

Definition 7.9. Define the Euler ϕ-function as the number of positive integers $a \leq n$ with $(a, n) = 1$.

Here is a general formula for the values of ϕ: if $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ with $n_i > 0$, then

$$\phi(n) = n(1 - p_1^{-1})(1 - p_2^{-1}) \cdots (1 - p_r^{-1}).$$

Corollary 7.10 (Euler's Theorem)**.** *If $(r, m) = 1$, then $r^{\phi(m)} \equiv 1 \bmod m$.*

Proof. Consider r as an element $\bar{r} \in (\mathbb{Z}/m\mathbb{Z})^\times$. By $|(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$, $\bar{r}^{\phi(m)} = \bar{1}$, that is, $r^{\phi(m)} \equiv 1 \bmod m$. □

8. Normal subgroups and Quotient groups

Definition 8.1. If G is a group and $a \in G$, then a *conjugate* of a is any element in G of the form

$$gag^{-1}$$

where $g \in G$.

Example.

(1) All m-cycles are conjugate.
(2) Two matrices $A, B \in \mathrm{GL}_n(\mathbb{R})$ are conjugate if they are similar; that is, if there is a nonsingular matrix P with $B = PAP^{-1}$.

Definition 8.2. A subgroup H of a group G is called *normal* if $gHg^{-1} = H$ for all $g \in G$, that is, $N_G(H) = G$. Write as $H \trianglelefteq G$.

Example.

- If G is abelian, every subgroup is normal.
- $\{e\} \trianglelefteq G$, $Z(G) \trianglelefteq G$ and $G \trianglelefteq G$.
- $\langle (1,2,3) \rangle \trianglelefteq S_3$ and $\langle (1,2) \rangle$ is not normal.
- $\langle r \rangle \trianglelefteq D_{2n}$.

Proposition 8.3. *Let H be a subgroup of G. The following are equivalent:*

(1) $H \trianglelefteq G$
(2) $gH = Hg$ *for all* $g \in G$
(3) $ghg^{-1} \in H$ *for all* $g \in G$ *and* $h \in H$.

Proof. "(1) $\Leftrightarrow$ (3)" Let $H \trianglelefteq G$. For any $g \in G$, $gHg^{-1} \subseteq H$. Then for any $h \in H$, ghg^{-1} is in H.

Conversely, by $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, then $gHg^{-1} \subseteq H$. For any $h \in H$, $g^{-1}hg \in H$ and then $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$. Hence $H \subseteq gHg^{-1}$ and $gHg^{-1} = H$.

"(1) $\Leftrightarrow$ (2)" Let $gh \in gH$. Since H is normal, $ghg^{-1} \in H$, say $ghg^{-1} = h' \in H$, so that $gh = (ghg^{-1})g = h'g \in Hg$, and so $gH \subseteq Hg$. For the reverse inclusion, let $hg \in Hg$. Since H is normal, $(g^{-1})h(g^{-1})^{-1} = g^{-1}hg \in H$, say $g^{-1}hg = h'' \in H$. Hence, $hg = g(g^{-1}hg) = gh'' \in gH$ and $Hg \subseteq gH$. Therefore, $gH = Hg$ when $H \trianglelefteq G$.

Conversely, if $gH = Hg$ for every $g \in G$, then for each $h \in H$, there is $h' \in H$ with $gh = h'g$; that is, $ghg^{-1} \in H$ for all $g \in G$, and so $H \trianglelefteq G$.

□

If X, Y are two subsets of G, define

$$XY = \{xy\colon x \in X \text{ and } y \in Y\}.$$

This multiplication is associative: $X(YZ)$ is the set of all $x(yz)$, where $x \in X, y \in Y$, and $z \in Z$, $(XY)Z$ is the set of all such $(xy)z$, and these are the same because of associativity in G.

For example, let $G = S_3$, let $H = \langle(1,2)\rangle$ and $K = \langle(1,3)\rangle$. Then

$$HK = \{1, (1,2), (1,3), (1,3,2)\}.$$

It is not a subgroup.

Proposition 8.4. (1) *If H and K are subgroups of a group G, and if one of them is a normal subgroup, then HK is a subgroup of G; moreover, $HK = KH$ in this case.*

(2) *If both H and K are normal subgroups, then HK is a normal subgroup.*

Proof. (1). Assume first that $K \trianglelefteq G$. We claim that $HK = KH$. If $hk \in HK$, then $k' = hkh^{-1} \in K$, because $K \trianglelefteq G$, and $hk = hkh^{-1}h = k'h \in KH$. Hence, $HK \subseteq KH$. For the reverse inclusion, write $kh = hh^{-1}kh = hk'' \in HK$. (Note that the same argument shows that $HK = KH$ if $H \trianglelefteq G$.) We now show that HK is a subgroup. Since $1 \in H$ and $1 \in K$, we have $1 = 1 \cdot 1 \in HK$; if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$; if $hk, h_1k_1 \in HK$, then $hkh_1k_1 = hh_1(h_1^{-1}kh_1)k_1 \in HK$.

(2). If $g \in G$, then Proposition 8.4 gives $gHK = HgK = HKg$, and the same proposition now gives $HK \trianglelefteq G$. □

Theorem 8.5. *Let G/H denote the family of all the left cosets of a subgroup H of G. If H is a normal subgroup, then*

$$aH \cdot bH = abH$$

for all $a, b \in G$, and G/H is a group under this operation.

Proof. For $x \in aH \cdot bH$, $x = ah_1 \cdot bh_2$ for some $h_1, h_2 \in H$. Then $x = ab \cdot (b^{-1}h_1b \cdot h_2)$. By $H \trianglelefteq G$, $b^{-1}h_1b$ is in H. Thus, $x \in abH$ and $aH \cdot bH \subseteq abH$. In the other hand, if $x \in abH$, $x = abh$ for some $h \in H$. Then $x = abhb^{-1} \cdot b$. As $bhb^{-1} \in H$, $abhb^{-1} \in aH$ and $b \in bH$. Thus, $x \in aH \cdot bH$ and $abH \subseteq aH \cdot bH$. Therefore, $aH \cdot bH = abH$.

The operation on G/H is well-defined, that is, for all $a, b \in G$, if $a_1 \in aH$ and $b_1 \in bH$ then $abH = a_1b_1H$. Let $a_1 \in aH$ and $b_1 \in bH$. It follows that $a_1^{-1}a \in H$ and $b_1^{-1}b \in H$. Then

$$(a_1b_1)^{-1}(ab) = b_1^{-1}(a_1^{-1}a)b = b_1^{-1}(a_1^{-1}a)b_1 \cdot b_1^{-1}b.$$

As $a_1^{-1}a \in H$ and $H \trianglelefteq G$, $b_1^{-1}(a_1^{-1}a)b_1 \in H$. Thus, $(a_1b_1)^{-1}(ab) \in H$ and $abH = a_1b_1H$ as claimed.

The operation is associative since the product of the subsets are associative.

The identity is the coset $H = 1H$, for $(1H)(bH) = 1bH = bH = b1H = (bH)(1H)$, and the inverse of aH is $a^{-1}H$, for $(a^{-1}H)(aH) = a^{-1}aH = H = aa^{-1}H = (aH)(a^{-1}H)$. Therefore, G/H is a group. $\square$

Definition 8.6. The group G/H is called the quotient group G mod H.

Example.

(1) Let $G = \mathbb{Z}$ and $H = \langle n \rangle$. Then $G/H = \mathbb{Z}/n\mathbb{Z}$.
(2) Let $H = \{1\}$ or $H = G$. Then $G/H = G$ or $G/H = \{eG\}$ respectively.
(3) Let $G = \mathbb{R}$ and $H = \mathbb{Z}$. Then $G/H = \mathbb{R}/\mathbb{Z}$.
(4) Let $G = \mathbb{Q}$ and $H = \mathbb{Z}$. Then $G/H = \mathbb{Q}/\mathbb{Z}$.

Definition 8.7. A group G is called simple group if its only normal subgroups are $\{e\}$ and G.

Example.

(1) Let G be abelian. G is simple if and only if G is cyclic of simple order p.
(2) A_n is simple for $n \geq 5$. (This will be discussed in some tutorial problems.)

9. Homomorphisms and The Isomorphism Theorems

Definition 9.1. If $(G, *)$ and $(H, \circ)$ are groups (we have displayed the operation in each), then a function $f\colon G \to H$ is a *homomorphism* if

$$f(x * y) = f(x) \circ f(y)$$

for all $x, y \in G$. If f is also a bijection, then f is called an *isomorphism*. Two groups G and H are called isomorphic, denoted by $G \cong H$, if there exists an isomorphism $f\colon G \to H$ between them.

Examples.

(1) Define the map $f\colon S_n \to \{\pm 1\}$ via

$$f(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then f is a homomorphism.

(2) Let $G = \langle x \rangle$ be a cyclic group of order n. Define the map $f\colon G \to \mathbb{Z}/n\mathbb{Z}$ via $f(x^a) = \bar{a}$. Then f is an isomorphism.

(3) Consider the map $f\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} - \{0\}$ defined by

$$f(g) = \det(g).$$

Then f is a homomorphism.

(4) Let G be an arbitary group and $a \in G$. Define $\gamma_a\colon G \to G$ via $\gamma_a(g) = aga^{-1}$. Then γ_a is an isomorphism.

(5) $S_3 \cong D_6$.

(6) $\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \cong V_4$ (Klein 4-group).

Definition 9.2. If $f\colon G \to H$ is a homomorphism, define

$$\ker f = \{x \in G\colon f(x) = 1\} = f^{-1}(e_G)$$

and

$$\mathrm{im} f = \{h \in H\colon h = f(x) \text{ for some } x \in G\} = f(G).$$

Lemma 9.3. *Let $f\colon G \to H$ be a homomorphism of groups.*

(1) $f(1) = 1$.

(2) $f(x^{-1}) = f(x)^{-1}$. *Morover,* $f(x^n) = f(x)^n$ *for* $n \in \mathbb{Z}$.

(3) $\ker f$ *is a normal subgroup of* G *and* $\mathrm{im} f$ *is a subgroup of* H.

Proof. (1). $f(1) = f(1 \cdot 1) = f(1)^2$ implies $f(1) = 1$.

(2). $1 = f(xx^{-1}) = f(x)f(x^{-1})$. Then $f(x^{-1}) = f(x)$. By induction, $f(x^n) = f(x)^n$ for all $n \geq 0$. When $n < 0$, it follows from $x^n = (x^{-1})^{-n}$.

(3). For $g \in G$ and $x \in \ker f$, $f(gxg^{-1}) = f(g)f(x)f^{-1}(g) = f(g)f^{-1}(g) = 1$. Then gxg^{-1} is in $\ker f$ and $\ker f$ is normal.

For $h_1, h_2 \in \mathrm{im} f$, there exist g_1 and g_2 such that $f(g_i) = h_i$ with $i = 1, 2$. Then $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = h_1 h_2^{-1}$ and $h_1 h_2^{-1} \in \mathrm{im} f$. $\square$

Proposition 9.4. *Every normal subgroup $K \trianglelefteq G$ is the kernel of some homomorphism.*

Proof. Define the *natural map* $\pi\colon G \to G/K$ by $\pi(a) = aK$. By $aK \cdot bK = abK$, $\pi(a)\pi(b) = \pi(ab)$; thus, π is a surjective homomorphism. Since K is the identity element in G/K,

$$\ker \pi = \{a \in G\colon \pi(a) = K\} = \{a \in G : aK = K\} = K.$$

□

Theorem 9.5 (First Isomorphism Theorem)**.** *If $f\colon G \to H$ is a homomorphism, then*

$$\ker f \trianglelefteq G \text{ and } G/\ker f \cong \mathrm{im} f.$$

In more detail, if $\ker f = K$ and $\varphi\colon G/K \to \mathrm{im} f \leq H$ is given by $\varphi\colon aK \to f(a)$, then φ is an isomorphism.

Proof. First, we show that φ is well-defined: If $aK = bK$, then $a = bk$ for some $k \in K$, and so $f(a) = f(bk) = f(b)f(k) = f(b)$ as $f(k) = 1$.

Let us now see that φ is a homomorphism. Since f is a homomorphism and $\varphi(aK) = f(a)$,

$$\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK).$$

It is clear that $\mathrm{im}\varphi \leq \mathrm{im} f$. For the reverse inclusion, note that if $y \in \mathrm{im} f$, then $y = f(a)$ for some $a \in G$, and so $y = f(a) = \varphi(aK)$. Thus, φ is surjective. Finally, we show that φ is injective. If $\varphi(aK) = \varphi(bK)$, then $f(a) = f(b)$. Hence, $1 = f(b)^{-1}f(a) = f(b^{-1}a)$, so that $b^{-1}a \in \ker f = K$. Therefore, $aK = bK$, and so φ is injective. We have proved that $\varphi : G/K \to \mathrm{im} f$ is an isomorphism. □

Example. Define $f\colon \mathbb{R} \to S^1$, where S^1 is the circle group, by

$$f\colon x \mapsto e^{2\pi i x}.$$

The map f is a surjective homomorphism. By the first isomorphism theorem,

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

Theorem 9.6 (Second Isomorphism Theorem)**.** *If H and K are subgroups of a group G with $H \trianglelefteq G$, then HK is a subgroup, $H \cap K \trianglelefteq K$, and*

$$K/(H \cap K) \cong HK/H.$$

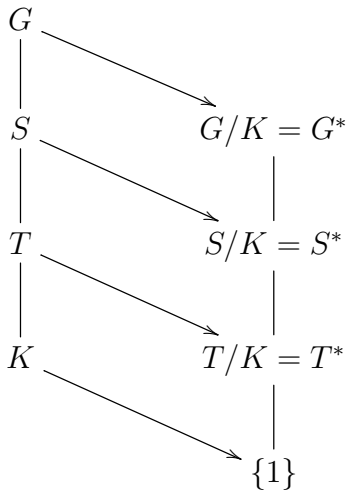
Proof. Since $H \trianglelefteq G$, HK is a subgroup. Normality of H in HK follows from a more general fact: If $H \leq S \leq G$ and if H is normal in G, then H is normal in S (if $ghg^{-1} \in H$ for every $g \in G$, then, in particular, $ghg^{-1} \in H$ for every $g \in S$).

We now show that every coset $xH \in HK/H$ has the form kH for some $k \in K$. Of course, $xH = hkH$, where $h \in H$ and $k \in K$. But $hk = kk^{-1}hk = kh'$ for some $h' \in H$, so that $hkH = kh'H = kH$. It follows that the function $f\colon K \mapsto HK/H$, given by $f\colon k \mapsto kH$, is surjective. Moreover, f is a homomorphism, for it is the restriction of the natural map $\pi\colon G \mapsto G/H$. Since $\ker \pi = H$, it follows that $\ker f = H \cap K$, and so $H \cap K$ is a normal subgroup of K. The first isomorphism theorem now gives $K/(H \cap K) \cong HK/H$. $\square$

Theorem 9.7 (Third Isomorphism Theorem)**.** *If H and K are normal subgroups of a group G with $K \leq H$, then $H/K \trianglelefteq G/K$ and*

$$(G/K)/(H/K) \cong G/H.$$

Proof. Define $f\colon G/K \mapsto G/H$ by $f\colon aK \mapsto aH$. Note that f is a (well-defined) function, for if $a' \in G$ and $a'K = aK$, then $a^{-1}a' \in K \leq H$, and so $aH = a'H$. It is easy to see that f is a surjective homomorphism. Now $\ker f = H/K$, for $aH = H$ if and only if $a \in H$, and so H/K is a normal subgroup of G/K. Since f is surjective, the first isomorphism theorem gives $(G/K)/(H/K) \cong G/H$. $\square$



Theorem 9.8 (Correspondence Theorem)**.** *Let G be a group and $K \trianglelefteq G$, and let $\pi\colon G \to G/K$ be the natural map. Then*

$$S \to \pi(S) = S/K$$

is a bijection between $Sub(G; K)$, the family of all those subgroups S of G that contain K, and $Sub(G/K)$, the family of all the subgroups of G/K.

If we denote S/K by S^*, then $K \leq T \leq S \leq G$ if and only if $T^* \leq S^*$, in which case $[S : T] = [S^* : T^*]$, and $T \trianglelefteq S$ if and only if $T^* \trianglelefteq S^*$,in which case $S/T \cong S^*/T^*$.

Proof. Define the map $f\colon Sub(G; K) \to Sub(G/K)$ by $f\colon S \to S/K$. We will show that f is bijective. Let $K \leq S \leq G$. Assume that $f(S) = f(S')$. Then $\pi(S) = \pi(S')$. So f is injective equivalent to $\pi^{-1}(S/K) = S$. It is easy to see that $S \subset \pi^{-1}(S/K)$. For $a \in \pi^{-1}(S/K)$, then $\pi(a) = \pi(s)$ for some $s \in S$ and $a = sk$ for some $k \in \ker \pi = K$. It follows that $a = sk \in S$ and $\pi^{-1}(S/K) \subset S$.

Next, let $U \leq G/K$ and then $\pi^{-1}(U)$ is a subgroup of G containing $K = \pi^{-1}(1)$. Since $\pi(\pi^{-1}(U)) = U$, f is surjective.

Since $T \leq S \leq G$ implies $T/K = \pi(T) \leq \pi(S) = S/K$. Conversely, assume that $T/K \leq S/K$. If $t \in T$, then $tK \in T/K \leq S/K$ and so $tK = sK$ for some $s \in S$. Hence, $t = sk$ for some $k \in K \leq S$, and so $t \in S$.

Third, we prove that $[S : T] = [S^* : T^*]$. Consider the map $\varphi\colon S/T \to S^*/T^*$ by $\varphi\colon sT \to \pi(s)T^*$.

Finally, if $T \trianglelefteq S$, then $T/K \trianglelefteq S/K$ and $(S/K)/(T/K) \cong S/T$,tat is, $S^*/T^* \cong S/T$, by the third isomorphism theorem. Assume that $T^* \trianglelefteq S^*$. If $t \in T$ and $s \in S$, then

$$\pi(sts^{-1}) = \pi(s)\pi(t)\pi(s)^{-1} \in T.$$

It follows that $sts^{-1} \in T$ and then $T \trianglelefteq S$. □

Proposition 9.9. *If G is a finite abelian group and d is a divisor of $|G|$, then G contains a subgroup of order d.*

Proof. First, we show the result by induction on $n = |G|$ for a prime divisor p of $|G|$. It is obviously true when $n = 1$. For the inductive step, choose $a \in G$ of order $k > 1$. If $p \mid k$, then $o(a^{k/p}) = p$. If $p \nmid k$, consider the cyclic subgroup $H = \langle a \rangle$. Since G is abelian, $H \trianglelefteq G$ and the quotient group $|G/H| = n/k$ is divisible by p. By induction, there is an element $bH \in G/H$ of order p and $p \mid o(b)$.

Next, let d be any divisor of $|G|$, and let p be a prime divisor of d. Then there is a subgroup $S \leq G$ of order p, and G/S is a group of order n/p. By induction on $|G|$, G/S has a subgroup H^* of order d/p. The correspondence theorem gives $H^* = H/S$ for some subgroup H of G containing S, and $|H| = |H^*||S| = d$. □

Definition 9.10. Let G be a group. An isomorphism from G to itself is called an *automorphism* of G. The set of all automorphisms of G forms a group under composition, and is denoted by $\mathrm{Aut}(G)$.

Example. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Example. For each $g \in G$, define $c_g \colon G \to G$ by $c_g(x) = gxg^{-1}$. Then c_g is an automorphism of G. Also we have a homomorphism from G to $\mathrm{Aut}(G)$ defined by $g \to c_g$.

Definition 9.11. Let G be a group. c_g is called an *inner automorphism* of G and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Fact. $\mathrm{Inn}(G) \cong G/Z(G)$.
Example. $\mathrm{Aut}(V_4) \cong S_3$ and $\mathrm{Inn}(V_4) = \{1\}$.

9.1. **Direct products of groups.**

Definition 9.12. If H and K are groups, then their *direct product*, denoted by $H \times K$, is the set of all ordered pairs (h, k) with $h \in H$ and $k \in K$ equipped with the operation $(h, k)(h', k') = (hh', kk')$.

Example.

(1) Let V_4 be the Klein 4-group. We have $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(2) If $(m, n) = 1$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. This is a special case of the so-called Chinese Remainder Theorem.

Proposition 9.13. *If G is a group containing normal subgroups H and K with $H \cap K = \{1\}$ and $HK = G$, then $G \cong H \times K$.*

Proof. First, if $g \in G$, then $g = hk$ for some $h \in H$ and $k \in K$ as $G = HK$. If $g = hk = h'k'$, then $h'^{-1}h = k'k^{-1} \in H \cap K = 1$. We have $h' = h$ and $k' = k$. Then g has a unique factorization hk. Define the function $\varphi \colon G \to H \times K$ by $\varphi(g) = (h, k)$, where $g = hk$, $h \in H$, and $k \in K$ as above. To prove that φ is a homomorphism, we need to show $gg' = hh'kk'$ for $g' = h'k'$, so that $gg' = hkh'k'$. Let $h \in H$ and $k \in K$. Since K is a normal subgroup, $(hkh^{-1})k^{-1} \in K$; since H is a normal subgroup, $h(kh^{-1}k^{-1}) \in H$. But $H \cap K = 1$, so that $hkh^{-1}k^{-1} = 1$ and $hk = kh$. It follows that φ is a homomorphism.

Finally, we show that the homomorphism φ is an isomorphism. If $(h, k) \in H \times K$, then the element $g \in G$ defined by $g = hk$ satisfies $\varphi(g) = (h, k)$; hence φ is surjective. If $\varphi(g) = (1, 1)$, then $g = 1$, so that $\ker \varphi = 1$ and φ is injective. Therefore, φ is an isomorphism. □

Remark: The expression $hkh^{-1}k^{-1}$ is called the commutator of h and k.

Example. Let $G_1, \ldots, G_n$ be groups and let

$$G = G_1 \times G_2 \times \cdots G_n$$

be their direct product. We have $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

Theorem 9.14 (Jordan-Hölder)**.** *Let G be a finite group with $G \neq 1$. Then*

(1) *G has a composition series, namely there exists a sequence of subgroups $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G$, with each N_{i-1} normal in N_i, and N_i/N_{i-1} is simple.*

(2) *The composition factors in a composition series are unique up to order, namely, if $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G$ and $1 = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_s = G$ are two composition series for G, then $r = s$ and there exists some permutation, π, of $\{1, 2, \ldots, r\}$ such that*

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}, \qquad 1 \leq i \leq r.$$

For a proof, see https://crypto.stanford.edu/pbc/notes/group/jordanholder.html.

The Hölder Program

(1) Classify all finite simple groups.

(2) Find all ways of "putting simple groups together" to form other groups.

10. Group action

Theorem 10.1 (Cayley)**.** *Every group G is isomorphic to a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof. For each $a \in G$, define the left translation $\tau_a \colon G \to G$ by $\tau_a(x) = ax$ for every $x \in G$. For $a, b \in G$,

$$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = a(bx) = (ab)x$$

then $\tau_a\tau_b = \tau_{ab}$. It follows that each τ_a is a bijection, for its inverse is τ_a^{-1}

$$\tau_a\tau_a^{-1} = \tau_{aa^{-1}} = \tau_1 = \tau_{a^{-1}a} = id,$$

and so $\tau_a \in S_G$. □

Definition 10.2. If X is a set and G is a group, then G acts on X if there is a function $G \times X \to X$, denoted by $(g, x) \to gx$, such that

(1) $(gh)x = g(hx)$ for all g, $h \in G$ and $x \in X$;
(2) $1x = x$ for all $x \in X$, where 1 is the identity in G.

We also call X a G-set if G acts on X.

Definition 10.3. If G acts on X and $x \in X$, then the orbit of x, denoted by $\mathcal{O}(x)$, is the subset of X

$$\mathcal{O}(x) = \{gx \colon g \in G\} \subseteq X;$$

the stabilizer of x, denoted by Gx, is the subgroup

$$G_x = \{g \in G \colon gx = x\} \leq G.$$

If G acts on a set X, define a relation on X by $x \sim y$ in case there exists $g \in G$ with $y = gx$. It is easy to see that this is an equivalence relation whose equivalence classes are the orbits.

We say G acts *transitively* on X if there is only one orbit.

Example. We show that G acts on itself by conjugation: that is, for each $g \in G$, define $c_g \colon G \to G$ to be conjugation

$$c_g(x) = gxg^{-1}.$$

To verify axiom (1), note that for each $x \in G$,

$$\begin{aligned}(c_g \circ c_h)(x) =& c_g(c_h(x)) \\ =& c_g(hxh^{-1}) \\ =& g(hxh^{-1})g^{-1} \\ =& (gh)x(gh)^{-1} \\ =& c_gh(x).\end{aligned}$$

Therefore, $c_g \circ c_h = c_{gh}$. To prove axiom (2), note that for each $x \in G$, $c_1(x) = 1x1^{-1} = x$.

Example. Let H be any subgroup of G. Define an action of G on G/H by the left translation

$$\tau_g \colon aH \mapsto gaH \text{ for all } g \in G,\ aH \in G/H.$$

This satisfies the two axioms for a group action. Also, τ_g is a permutation in $S_{G/H}$ and the map $g \mapsto \tau_g$ is a homomorphism from G to $S_{G/H}$.

Proposition 10.4. *Let G be a group and H be a subgroup of G. Let G act on G/H by the left multiplication. Denote $\pi_H \colon G \to S_{G/H}$ to be the homomorphism defined by $g \mapsto \tau_g$. Show that*

(1) *G acts transitively on G/H*
(2) *the stabilizer in G of the point $aH \in G/H$ is the subgroup aHa^{-1}*
(3) *the kernel of π_H is $\cap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H.*

Since the relation defined on X is an equivalence relation whose equivalence classes are the orbits, the orbits partition X.

Proposition 10.5. *If G acts on a set X, then X is the disjoint union of the orbits. If X is finite, then*

$$|X| = \sum_i |\mathcal{O}(x_i)|,$$

where i runs over all orbits and x_i is chosen from each orbit.

Theorem 10.6. *If G acts on a set X and $x \in X$, then*

$$|\mathcal{O}(x)| = [G : G_x].$$

Proof. Consider the map $\varphi \colon G/G_x \to \mathcal{O}(x)$ by $\varphi(gG_x) = gx$. First, φ is well-defined: If $gG_x = hG_x$, then $h = gf$ for some $f \in G_x$ and $hx = gfx = gx$ as $fx = x$.

Second, if $gx = \varphi(gG_x) = \varphi(hG_x) = hx$, then $h^{-1}gx = x$ and $h^{-1}g \in G_x$. Thus $gG_x = hG_x$ and φ is injective.

Finally, if $y \in \mathcal{O}(x)$, then $y = gx$ for some $g \in G$, and so $y = \varphi(gG_x)$. Therefore, φ is bijective and the statement follows. □

Example. The *class equation* of a finite group G is

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)], \tag{10.1}$$

where x_i is selected from each conjugacy class having more than one element.

Theorem 10.7 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Assume that $|G| = pm$. We prove the theorem by induction on $m \geq 1$. When $m = 1$, G is cyclic and the statement is true.

Let $x \in G$ and the number of conjugates $conj_x$ of x is $|conj_x| = [G : C_G(x)]$. If $x \notin Z(G)$, then $conj_x$ has more than one element, and so $|C_G(x)| < |G|$. If $p \mid |C_G(x)|$ for some $x \notin Z(G)$, then there is an element of order p in $C_G(x) \leq G$. Therefore, we may assume that $p \nmid |C_G(x)|$ for all $x \notin Z(G)$. Since p is a prime and $|G| = [G : C_G(x)]|C_G(x)|$, we have $p \mid [G : C_G(x)]$.

Referring to the class equation (10.1), $|Z(G)|$ is divisible by p as p divides $|G|$ and all $[G : C_G(x_i)]$. Since $Z(G)$ is abelian and $p \mid |Z(G)|$, $Z(G)$ contains an element of order p. □

Definition 10.8. Let p be a prime. A finite group G is called a p-group if $|G| = p^n$ for some $n \geq 0$. An infinite group G is called a p-group if every element in G has order a power of p.

Equivalently, G is a p-group if every element in G has a order of power of p. (Refer to Cauchy Theorem 10.7.)

Theorem 10.9. *Let p be a prime and let P be a p-group. Then*

(1) *The center of P is nontrivial: $Z(P) \neq 1$.*
(2) *If H is a nontrivial normal subgroup of P then H intersects the center non-trivially: $H \cap Z(P) \neq 1$. In particular, every normal subgroup of order p is contained in the center.*

Proof. From the class equation, we have

$$|P| = |Z(P)| + \sum_i [P : C_P(x_i)].$$

Within each of the terms in the summation, $C_P(x_i)$ is a proper subgroup of P, and so $[P : C_P(x_i)]$ is a multiple of p. Thus $|Z(P)|$ is a multiple of p.

For Part (2), we consider the action of P on H by conjugation. This yields the orbit counting equation:

$$|H| = |H \cap Z(P)| + \sum_j [P : C_P(y_j)],$$

where the summation is over orbits having more than one element. The same argument proves that $|H \cap Z(P)|$ is a multiple of p. In particular if H is of order p, we must have $H \cap Z(P) = H$, and so H is contained in $Z(P)$. □

Corollary 10.10. *Let P be a p-group with $|P| = p^k$. Then P has a normal subgroup of order p^m, for every $1 \leq m \leq k$.*

Proof. We know $Z(P)$ is a non-trivial p-group. By Cauchy's theorem, $Z(P)$ contains a subgroup H of order p. Then the result follows by applying induction to G/H and the correspondence theorem. $\square$

11. The Sylow Theorems

Definition 11.1. Let G be a group and p be a prime.

(1) Subgroups of G which are p-groups are called *p-subgroups*.
(2) If G s a group of order $p^\alpha m$ where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.
(3) The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 11.2 (Sylow's Theorem)**.** *Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.*

(1) *Sylow p-subgroups of G exist, i.e., $Syl_p(G) \neq \emptyset$.*
(2) *If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exits $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.*
(3) *The number of Sylow p-subgroups of G is of form $1 + kp$, i.e.,*

$$n_p \equiv 1 \bmod p.$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Proof. Assume Syl_p is not empty for all groups of order less than $|G|$.

If p divides $|Z(G)|$, then by Cauchy's Theorem for abelian groups, $Z(G)$ has a subgroup N of order p. Let $\bar{G} = G/N$ and $|\bar{G}| = p^{\alpha-1}m$. By induction, $\bar{G}$ has a subgroup $\bar{P}$ of order $p^{\alpha-1}$. If we let P be the subgroup of G containing N such that $P/N = \bar{P}$ then $|P| = |P/N| \cdot |N| = p^\alpha$ and P is a Sylow p-subgroup of G.

Assume that $p \nmid |Z(G)|$. Let $g_1, g_2, \ldots, g_r$ be representatives of the distinct non-central conjugacy classes of G. By the class equation (10.1), if $p \mid [G\colon C_G(g_i)]$ for all i, then since $p \mid |G|$, we would also have $p \mid |Z(G)|$, a contradiction. Thus for some i, p dose not divide $[G\colon C_G(g_i)]$. For this i, let $H = C_G(g_i)$ so that $|H| = p^\alpha l$ where $p \nmid l$. Since $g_i \notin Z(G)$, $|H| < |G|$. By induction, H has a Sylow p-subgroup P of order p^α. Then P is also a Sylow p-subgroup of G. □

Lemma 11.3. *Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.*

Proof. Consider $H = Q \cap N_G(P)$ and P, as subgroups of $N_G(P)$. Since P is normal in $N_G(P)$, we know that HP is a subgroup of $N_G(P)$.

By the second isomorphism theorem, $HP/P \cong H/H \cap P$, and so its order is p^k for some $k \geq 0$. But then $|HP| = p^{\alpha+k}$, which forces $k = 0$.

This implies that $HP = P$, and so $H \subseteq P$. Therefore $H \subseteq Q \cap P$. □

The proof of part (2). By $Syl_p(G) \neq \emptyset$, take P to be a Sylow p-subgroup in $Syl_p(G)$. Let

$$\mathcal{S} = \{gPg^{-1} \colon g \in G\} = \{P_1, P_2, \ldots, P_r\}$$

be the set of all conjugates of P and let Q be any p-subgroup of G. Consider the action of Q on $\mathcal{S}$ by conjugation. We can write $\mathcal{S}$ as a disjoint union of orbits under this action by Q:

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s.$$

Note that $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$. Without loss of generality, assume that $P_i \in \mathcal{O}_i$, for some $1 \leq i \leq s$. It follows that $|\mathcal{O}_i| = [Q \colon N_Q(P_i)]$. By definition, $N_Q(P_i) = N_G(P_i) \cap Q$ and by Lemma 11.3, $N_G(P_i) \cap Q = P_i \cap Q$. Combining these two facts gives

$$|\mathcal{O}_i| = [Q \colon P_i \cap Q], \qquad 1 \leq i \leq s.$$

Since Q was arbitrary, we may take $Q = P_1$, then $|\mathcal{O}_1| = 1$. For all $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$. Then $|\mathcal{O}_i| = |P_1 \colon P_1 \cap P_i| > 1$, $2 \leq i \leq s$. Since P_1 is a p-group, $[P_1 \colon P_1 \cap P_i]$ must be a power of p, so that $p \mid |\mathcal{O}_i|$, $2 \leq i \leq s$. Thus

$$r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|) \equiv 1 \bmod p.$$

Let Q be any p-subgroup of G. Suppose Q is not contained in P_i for any $1 \leq i \leq r$. In this situation, $Q \cap P_i < Q$ for all i, so $|\mathcal{O}_i| = [Q \colon Q \cap P_i] > 1$, $1 \leq i \leq s$. Thus $p \mid |\mathcal{O}_i|$ for all i, so p divides $|\mathcal{O}_1| + \cdots + |\mathcal{O}_s| = r$, a contradiction. □

Proof. Let Q be any Sylow p-subgroup of G. By the above argument, $Q \leq gPg^{-1}$ for some $g \in G$. Since $|gPg^{-1}| = |Q| = p^\alpha$, we must have $gPg^{-1} = Q$. This establishes part (2). In particular, $\mathcal{S} = Syl_p(G)$ and $n_p = r \equiv 1 \bmod p$.

Since all Sylow p-subgroups are conjugate, $n_p = [G \colon N_G(P)]$ for any $P \in Syl_p(G)$. □

Corollary 11.4. *Let P be a Sylow p-subgroup of G. Then the following are quivalent:*

(1) *P is the unique Sylow p-subgroup of G, $n_p = 1$*
(2) *P is normal in G*
(3) *Let X be any subset of G such that $o(x)$ is a power of p for all $x \in X$. Then $\langle X \rangle$ is a p-group.*

Proof. If (1) holds, for each $a \in G$, the conjugate aPa^{-1} is also a Sylow p-subgroup; by uniqueness, $aPa^{-1} = P$ for all $a \in G$, and so $P \trianglelefteq G$. Conversely, assume that $P \trianglelefteq G$. If Q is any Sylow p-subgroup, then

$aPa^{-1} = Q$ for some $a \in G$; but $aPa^{-1} = P$, by normality, and so $Q = P$.

Assume that (1) holds and X is a subset of G such that $o(x)$ is a power of p for all $x \in X$. For each $x \in X$, there exists some $g \in G$ such that $gxg^{-1} \in gPg^{-1} = P$. Thus $X \subseteq P$ and $\langle X \rangle \leq P$. So $\langle X \rangle$ is a p-subgroup. Conversely, if (3) holds, let X be the union of all Sylow p-subgroups of G. If P is any Sylow p-subgroup, P is a subgroup of the p-group $\langle X \rangle$. Since P is a p-subgroup of G of maximal order, we must have $P = \langle X \rangle$, so (1) holds.

□

Example 11.5. Let G be a group of order pq where p, q are primes, $p \nmid q - 1$ and $q \nmid p - 1$. Show that G is abelian.

Proof. When $p = q$, G is abelian and isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

When $p \neq q$, without loss of generality, assume that $p < q$. Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$.

First, we show that Q is normal. Since $n_q = 1 + kq$ for some $k \geq 0$, $n_q \mid p$, we have $k = 0$. Then $n_q = 1$ and $Q \trianglelefteq G$. Similarly P is normal.

We show that G is cyclic. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Since $P \cap Q = \{1\}$ and $P, Q \trianglelefteq G$, $G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ by Proposition 9.13. By the Chinese Remainder Theorem, $G \cong \mathbb{Z}/pq\mathbb{Z}$ is cyclic. □

Remark that if $p \mid q - 1$, there exists a unique non-abelian group of order pq in which $n_p = q$. We will prove this later. For example, when $pq = 6$, $G \cong S_3$.

12. Application of the Sylow Theorems

Let us list some techniques for producing normal subgroups:

(1) Counting elements.
(2) Permutation representations.
(3) Playing with p-subgroups for different primes p.

12.1. **Counting elements.**

Example 12.1. Let G be a group of order 30. Show that G has a normal subgroup isomorphic to $\mathbb{Z}/15\mathbb{Z}$.

Proof. If there exists a subgroup H of G with $|H| = 15$, then $H \trianglelefteq G$ as $[G\colon H] = 2$. Also, 3 does not divide $5 - 1$. Then $H \cong \mathbb{Z}/15\mathbb{Z}$ by Example 11.5. It suffices to show that there exists a subgroup of G of order 15.

Let $P \in Syl_5(G)$ and $Q \in Syl_3(G)$. If either P or Q is normal, then PQ is a subgroup of G and $|PQ| = 15$. The statement follows.

Assume that P and Q are not normal. Then $n_5 = 6$ and $n_3 = 10$. Let $Syl_5(G) = \{P_1, \ldots, P_6\}$ and $Syl_3(G) = \{Q_1, \ldots, Q_{10}\}$. For any $i \neq j$, $P_i \cap P_j = \{1\}$. Each non-identity element in P_i is of order 5. Then $P_1 \cup \cdots \cup P_6$ contains 24 distinct elements of order 5. Similarly, $Q_1 \cup \cdots \cup Q_{10}$ contains 20 distinct elements of order 3. However, $P_1 \cup \cdots \cup P_6 \cup Q_1 \cup \cdots \cup Q_{10}$ contains 45 distinct elements, a contradiction. Then one of P or Q must be normal in G. □

12.2. **Permutation representations.**

Lemma 12.2. *Let G be a finite simple group. Then $|G|$ divides $[G\colon H]!$ for all proper subgroups H of G.*

In particular, there is no simple group G of order $|G| = p^\alpha m$, where p is prime, $p \nmid m$, and $p^\alpha \nmid (m-1)!$.

Proof. Let H be a proper subgroup of G. Then π_H is a non-identity map from $G \to S_{G/H}$. Otherwise, $\ker \pi_H = G$ is contained in H, a contradiction. Then $|G/\ker \pi_H|$ divides $|G/H|!$. Furthermore, if G is simple, then $\ker \pi_H = \{1\}$ and $G \cong \mathrm{im}\pi_H \leq S_{G/H}$. Hence $|G|$ divides $|S_{G/H}|$. □

Example 12.3. Show that there is no simple group of order 3393.

Proof. Assume that G is a simple group of order 3393. One has $3393 = 3^2 \cdot 13 \cdot 29$. Since $29 \mid |G|$, $29 \mid [G : H]!$ and the minimal index of a proper subgroup is 29. By Sylow Theorem, $n_3 = 1$ or 13. Since G is simple, $n_3 = 13$. For $P \in Syl_3(G)$, $[G\colon N_G(P)] = 13 < 29$, a contradiction. □

Example 12.4. Show that there is no simple group of order 396.

Proof. Suppose that G is a simple group of order $396 = 2^2 \cdot 3^2 \cdot 11$. We must have $n_{11} = 12$. Let $P \in Syl_{11}(G)$ and then $[G\colon N_G(P)] = 12$. We have $|N_G(P)| = 33$ and G is isomorphic to a subgroup of S_{12}.

However it is not possible to have a subgroup of order 33 in S_{12} for the following reasons. First this group is cyclic of order 33, with a generator σ. Within S_{12}, σ must be a product of two disjoint cycles of length 3 and 11. We have a contradiction since $3 + 11 > 12$. □

12.3. **Playing with p-subgroups for different primes p.**

Example 12.5. Show that there are no simple groups of order 1785.

Proof. Let G be a simple group of order $1785 = 3 \cdot 5 \cdot 7 \cdot 17$. Then $n_{17} = 35$. Let $Q \in Syl_{17}(G)$. We have $[G\colon N_G(Q)] = 35$ and $|N_G(Q)| = 3 \cdot 17$. Let P be a Sylow 3-subgroup of $N_G(Q)$. The group PQ is abelian by $3 \nmid 17 - 1$, so $Q \leq N_G(P)$ and $17 \mid N_G(P)$. In this case $P \in Syl_3(G)$. The possible values of n_3 are 7, 85 and 595. Since $17 \mid N_G(P)$, $n_3 = 7$. But G has no proper subgroup of index < 17, a contradiction.

□

13. Finite abelian groups

Definition 13.1. (1) A group G is *finitely generated* if there is a finite subset A of G such that $G = \langle A \rangle$.

(2) For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the *free abelian group of rank* r.

Theorem 13.2 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a finitely generated abelian group. Then*

$$G \cong \mathbb{Z}^r \times G'$$

where G' is a finite abelian group.

Theorem 13.3. *Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

(1) *$G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$.*

(2) *for each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^\alpha$,*

$$A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ (where t depend on i)

(3) *the decomposition in (1) and (2) is unique, up to the permutation of factors.*

Let n be a positive integer. A *partition* of n is a sequence $(n_1, n_2, \ldots, n_t)$ of positive integers statisfying

(1) $n_i \geq 1$ for all $i \in \{1, 2, \ldots, t\}$

(2) $n_i \geq n_{i+1}$ for all i

(3) $n_1 + n_2 + \cdots + n_t = n$.

For example, here are the lists of partitions of 5 and their corresponding abelian groups of order p^5:

partitions of 5	Abelian groups
5	$\mathbb{Z}_{p^5}$
4,1	$\mathbb{Z}_{p^4} \times \mathbb{Z}_p$
3,2	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$
3,1,1	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p$
2,2,1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$
2,1,1,1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
1,1,1,1,1	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Lemma 13.4. *Let E be an elementary abelian p-group (i.e., $x^p = 1$ for all $x \in E$). Then for any $x \in E$ there exists $M \leq E$ with $E = M \times \langle x \rangle$.*

Proof. If $x = 1$, just take $M = E$. Otherwise, x is of order p. If $E = \langle x \rangle$, the assertion is clear. We may thus assume $\langle x \rangle \neq E$. Let M be a subgroup of E of maximal order such that x is not in M. We will show that M is of index p in E. If not, we consider $\bar{E} = E/M$, which is clearly an elementary abelian p-group. The image $\langle \bar{x} \rangle$ of $\langle x \rangle$ is a subgroup of order p, and so there exists $\bar{y} \in \bar{E} - \langle \bar{x} \rangle$. Since $\bar{y}$ has order p, we also have $\bar{x} \notin \langle \bar{y} \rangle$. The preimage of $\langle \bar{y} \rangle$ in E is a subgroup of E that does not contain x and whose order is larger than the order of M, contradicting to choice of M. This proves $[E\colon M] = p$ and hence $E = M\langle x \rangle$. Since $M \cap \langle x \rangle = 1$, we have $E = M \times \langle x \rangle$. □

Remark: Under the usual addition and multiplication, $\mathbb{Z}_p$ becomes a field. Denote this finite field by $\mathbb{F}_p$. For an elementary abelian p-group E, one may define a scaler multiplication on E by $\mathbb{F}_p$. In this way, E becomes a vector space over $\mathbb{F}_p$.

Proof. We will prove Parts (1) and (2) of Theorem 13.3.

For Part (1), we let A_i be a p_i-Sylow subgroup of A, which is unique since A is abelian (and so every subgroup if normal). Clearly $|A_i| = p_i^{\alpha_i}$, and $A_i \cap (\times_{j \neq i} A_j) = \{1\}$ by the Lagrange Theorem, and so we have

$$G = A_1 \times A_2 \times \cdots A_k.$$

For Part (2), we define the map $\varphi\colon A \to A$ by $\varphi(x) = x^p$. Since A is abelian, φ is a homomorphism. Then $\ker\varphi = \{x \in A\colon x^p = 1\}$ and $\mathrm{im}\varphi = \{x^p\colon x \in A\}$. By Cauchy Theorem, $\ker\varphi$ is not trivial and it follows $|\mathrm{im}\varphi| < |A|$. By The First Isomorphism Theorem

$$[A\colon \mathrm{im}\varphi] = |\ker\varphi|. \tag{13.1}$$

By induction,

$$\begin{aligned} \mathrm{im}\varphi &\cong \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \langle h_s \rangle \\ &\cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \mathbb{Z}_{p^{\beta_s}}. \end{aligned}$$

By the definition of φ, there exist elements $g_i \in A$ such that $g_i^p = h_i$, $1 \leq i \leq s$. Let $A_0 = \langle g_1, g_2, \ldots, g_s \rangle$. Since $\langle h_i \rangle \cap \langle h_j \rangle = \{1\}$, we have $\langle g_i \rangle \cap \langle g_j \rangle = \{1\}$, and so

$$\begin{aligned} A_0 &= \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \langle g_s \rangle \\ &\cong \mathbb{Z}_{p^{\beta_1+1}} \times \mathbb{Z}_{p^{\beta_2+1}} \times \cdots \mathbb{Z}_{p^{\beta_s+1}}. \end{aligned}$$

Since $\langle g_i \rangle / \langle h_i \rangle = \langle g_i \rangle / \langle g_i^p \rangle \cong \mathbb{Z}_p$ for each i, we see that

- $A_0/\mathrm{im}\varphi$ is an elementary abelian group of order p^s.

Furthermore an element $\prod_i h_i^{c_i}$ in $\mathrm{im}\varphi$ is in $\ker\varphi$ if and only if $\prod_i h_i^{pc_i} = 1$, and so $pc_i | p^{\beta_i}$, namely $c_i | p^{\beta_i - 1}$. We thus have

- $\mathrm{im}\varphi \cap \ker\varphi = \left\langle h_1^{p^{\beta_1 - 1}} \right\rangle \times \left\langle h_2^{p^{\beta_2 - 1}} \right\rangle \times \cdots \times \left\langle h_s^{p^{\beta_s - 1}} \right\rangle$.

Note that $\left\langle h_i^{p^{\beta_i - 1}} \right\rangle \cong \mathbb{Z}_p$, for each i.

If $\ker\varphi \leq \mathrm{im}\varphi$, then

$$|\ker\varphi| = |\mathrm{im}\varphi \cap \ker\varphi| = p^s = [A_0 \colon \mathrm{im}\varphi].$$

By (13.1), we have $A = A_0$, and we are done.

Otherwise, take $x \in \ker\varphi$ with $x \notin \mathrm{im}\varphi$. Consider $A/\mathrm{im}\varphi$, which is an elementary abelian p-group. By Lemma 13.4, $A/\mathrm{im}\varphi = \langle \bar{x} \rangle \times \langle \bar{M} \rangle$. Let M be the preimage of $\bar{M}$ in A. Since $o(\bar{x}) = p$, x is not in M. Now since $x \in \ker\varphi$, we have $x^p = 1$. From this we see that $\langle x \rangle \cap M = \{1\}$ and so $A = \langle x \rangle \times M$. By applying induction to M, the result follows. $\square$

14. Semidirect products

Definition 14.1. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The *semidirect product* $H \rtimes_\varphi K$ of H and K with respect to φ is the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ with the multiplication

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2).$$

Sometimes, we simply write $(h_1, k_1)(h_2, k_2) = (h_1 \ k_1 \cdot h_2, k_1 k_2)$

Proposition 14.2. *$H \rtimes_\varphi K$ is a group.*

Proof. It is easy to see that the multiplication is a binary operation.

The associative law is verified as follows:

$$\begin{aligned}
&((a, x)(b, y))(c, z) \\
=&(a \ (x \cdot b), xy)(c, z) \\
=&(a \ (x \cdot b) \ ((xy) \cdot c), xyz) \\
=&(a \ (x \cdot (b \ y \cdot c)), xyz) \\
=&(a, x)(b \ y \cdot c, yz) \\
=&(a, x)((b, y)(c, z))
\end{aligned}$$

for all $(a, x), (b, y), (c, z) \in G$.

The identity element is $(1, 1)$. The inverse of (h, k) is

$$(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1}).$$

□

For example, if φ is the identity map, then $H \rtimes_\varphi K = H \times K$.

The following result gives a (internal) characterization of a group as a semidirect product of two subgroups.

Theorem 14.3. *Suppose G is a group with subgroups K and H such that*

1. *$H \trianglelefteq G$, and*
2. *$H \cap K = 1$.*

Let $\varphi\colon K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H, i.e. $\varphi(k)\colon H \to H$ by $\varphi(k)\colon h \mapsto khk^{-1}$.

Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then $G \cong H \rtimes K$.

Proof. By Proposition 9.13, the map $\psi\colon hk \mapsto (h,k)$ is a bijection from HK to $H \rtimes K$. Then ψ is a group homomorphism. Indeed,

$$\begin{aligned}\psi(g_1g_2) =& \psi(h_1k_1h_2k_2)\\ =& \psi(h_1(k_1h_2k_1^{-1})k_1k_2)\\ =& (h_1\varphi(k_1)(h_2)k_1k_2)\\ =& (h_1,k_1)(h_2,k_2)\\ =& \psi(g_1)\psi(g_2)\end{aligned}$$

where $g_1 = h_1k_1$ and $g_2 = h_2k_2$. □

Theorem 14.3 can be used to classify groups of order n for certain values of n. The basic idea is to

(1) show every group of order n has proper subgroups H and K satisfying $H \trianglelefteq G$, $H \cap K = 1$ and $G = HK$.
(2) find all possible isomorphism types for H and K
(3) for each pair H, K found in (2) find all possible homomorphisms $\varphi\colon K \to \mathrm{Aut}(H)$
(4) for each triple H, K, φ found in (3) form the semidirect product $H \rtimes K$ (so any group of G of order n is isomorphic to one of these explicitly constructed groups) and among all these semidirect products determine which pairs are isomorphic. This results in a list of the distinct isomorphism types of groups of order n.

We will skip the proof of the following proposition, which will be used throughout the section.

Proposition 14.4. *Let p be a prime and $p \neq 2$. Then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.*

Example 14.5 (Groups of order pq, p and q primes with $p < q$)**.** Let G be any group of order pq, let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$. Since $p < q$, $n_q = 1$ and $Q \trianglelefteq G$. By Theorem 14.3, $G \cong Q \rtimes P$ for some $\varphi\colon P \to \mathrm{Aut}(Q)$. Note that $\mathrm{Aut}(Q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $q-1$. If $p \nmid q-1$, the image $\phi(P)$ must be the trivial group and we get the direct product of Q and P. If $p \mid q-1$, the cyclic group $\mathrm{Aut}(Q)$ contains a unique subgroup of order p, say $\langle\gamma\rangle$. Any homomorphism from P to $\mathrm{Aut}(Q)$ will have to map a (fixed) generator y of P to some γ^i, also denoted by φ_i. Since φ_0 is the trivial homomorphism, $Q \rtimes_{\varphi_0} P \cong Q \times P$. Each φ_i for $i \neq 0$ gives rise to a non-abelian group G_i of order pq. Because there is some generator y_i of P such that $\varphi_i(y_i) = \gamma$ for each φ_i, these groups are easily seen to be isomorphic. Thus there is a unique non-abelian group of order pq.

For example, if G is a non-abelian group of order 21, the group is given by

$$G \cong \left\langle r, s \mid r^7 = s^3 = 1,\ srs^{-1} = r^2 \right\rangle;$$

if G is a non-abelian group of order 39, the group is given by

$$G \cong \left\langle r, s \mid r^{13} = s^3 = 1,\ srs^{-1} = r^3 \right\rangle.$$

Example 14.6 (Groups of order 12)**.** Let G be a group of order 12, let $V \in Syl_2(G)$ and let $T \in Syl_3(G)$. We argue first that either V or T is normal. If not $n_2 = 3$ and $n_3 = 4$. The 4 Sylow 3-groups T_1, T_2, T_3, T_4 will have $2 \times 4 = 8$ distinct elements of order 3, and together with one Sylow 2-group, will give rise to 12 elements. This is impossible as $n_2 = 3$. Thus either V or T is normal. By $T \cap V = 1$, G is a semidirect product. Note that $V \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $T \cong \mathbb{Z}_3$.

Case 1: $V \trianglelefteq G$. We must determine all possible homomorphisms from T into $\mathrm{Aut}(V)$. If $V \cong \mathbb{Z}_4$, then $\mathrm{Aut}(V) = \mathbb{Z}_4^\times \cong \mathbb{Z}_2$ and there are non nontrivial homomorphisms from T into $\mathrm{Aut}(V)$. Thus the only group of order 12 with a normal cyclic Sylow 2-subgroup is $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$.

Assume that therefore that $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. In this case $\mathrm{Aut}(V) \cong S_3$ and there is a unique subgroup of $\mathrm{Aut}(V)$ of order 3, say $\langle \gamma \rangle$. Thus if $T = \langle y \rangle$, there are three possible homomorphisms from T into $\mathrm{Aut}(V)$:

$$\varphi \colon T \to \mathrm{Aut}(V) \text{ defined by } \varphi_i(y) = \gamma^i, \qquad i = 0, 1, 2.$$

φ_0 give rise to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$. Homomorphisms φ_1 and φ_2 give rise to isomorphic semidirect products, which is isomorphic to A_4. (Inside A_4, take a copy of $\mathbb{Z}_3$ as $\langle (123) \rangle$, and a copy of $\mathbb{Z}_2 \times \mathbb{Z}_2$ as the Klein 4-group, which is normal.)

Case 2: $T \trianglelefteq G$. If $V = \langle x \rangle \cong \mathbb{Z}_4$, there are precisely two homomorphisms from V into $\mathrm{Aut}(T) = \mathbb{Z}_3^\times = \langle \lambda \rangle \cong \mathbb{Z}_2$: the trivial homomorphism and the homomorphism which sends x to λ. The trivial homomorphism gives rise to the direct product $\mathbb{Z}_3 \times \mathbb{Z}_4$. The nontrivial homomorphism gives rise to D_{12}.

Finally assume that $V = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. There are precisely three nontrivial homomorphisms from V into $\mathrm{Aut}(T)$ determined by specifying their kernels as one of the three subgroups of order 2 in V. That is,

$$\begin{aligned} \varphi_1 &\colon a \mapsto \lambda \qquad b \mapsto \lambda \\ \varphi_2 &\colon a \mapsto \lambda \qquad b \mapsto 1 \\ \varphi_3 &\colon a \mapsto 1 \qquad b \mapsto \lambda. \end{aligned}$$

Those three semidirect products are all isomorphic to $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

In summary, there are precisely 5 groups of order 12,

$$\mathbb{Z}_{12}, \qquad \mathbb{Z}_2 \times \mathbb{Z}_6, \qquad A_4, \qquad D_{12}, \qquad \mathbb{Z}_3 \rtimes \mathbb{Z}_4.$$

14.1. **Classical groups.** Let p be a prime and then both $(\mathbb{Z}_p, +)$ and $(\mathbb{Z}_p - \{\bar{0}\}, \times)$ are cyclic groups. As noted earlier, $\mathbb{Z}_p$ is also called a finite field, denoted by $\mathbb{F}_p$.

Let $V = \mathbb{F}_p^n$, which is an elementary abelian group ($pv = 0$ for all $v \in V$). Clearly $|V| = p^n$.

Proposition 14.7. *Consider $V = \mathbb{F}_p^n$ as a group under the addition. Then*

$$\mathrm{Aut}(V) = \mathrm{GL}_n(\mathbb{F}_p) \qquad |\mathrm{Aut}(V)| = (p^n{-}1)(p^n{-}p)(p^n{-}p^2)\cdots(p^n{-}p^{n-1}).$$

Proof. Let $g \in \mathrm{GL}_n(\mathbb{F}_p)$ and write

$$g = [v_1, v_2, \ldots, v_n]$$

where each v_i is a column vector. For $1 \le i \le n$, then v_i is in the set

$$V \smallsetminus \{c_1v_1 + c_2v_2 + \cdots + c_{i-1}v_{i-1} \colon c_1, c_2, \ldots, c_{i-1} \in \mathbb{F}_p\}.$$

Then there are $p^n - p^{i-1}$ choices of v_i. Hence

$$|\mathrm{Aut}(V)| = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}).$$

□

Example.

(1) $\mathrm{Aut}(V) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.
(2) $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I_2\}$ are simple for all primes $p \ge 5$.

Proposition 14.8. $\mathrm{GL}_2(\mathbb{F}_p)$ *has $p+1$ Sylow p-subgroups.*

Proof. Note that $|\mathrm{GL}_2(\mathbb{F}_p)| = p(p{-}1)^2(p{+}1)$. Then a p-Sylow subgroup has size p. By

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nb \\ 0 & 1 \end{pmatrix},$$

$\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order p, so it generates a p-Sylow subgroup. Since all p-Sylow subgroups are conjugate, any matrix with order p is conjugate to γ^m for some m with $(m, p) = 1$. Since

$$\begin{pmatrix} m^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

every element of order p is conjugate to γ. We have

$$\begin{aligned} g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N_{\mathrm{GL}_2}(P) &\iff g\gamma g^{-1} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \\ &\iff \begin{pmatrix} 1 - \frac{ac}{\Delta} & \frac{a^2}{\Delta} \\ -\frac{c^2}{\Delta} & 1 + \frac{ac}{\Delta} \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \\ &\iff c = 0 \end{aligned}$$

where $\Delta = ad - bc$. Thus

$$N_{\mathrm{GL}}(P) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_p^\times,\ b \in \mathbb{F}_p \right\}$$

and so $|N_{\mathrm{GL}}(P)| = (p-1)^2 p$. Therefore, $n_p = [\mathrm{GL}_2(\mathbb{F}_p) \colon N_{\mathrm{GL}}(P)] = p + 1$. □

14.2. **More examples.**

Example 14.9 (Groups of order p^3, p an odd prime)**.** Let G be a group of order p^3. If G is abelian, then G is isomorphic it one of the following groups

$$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p, \qquad \mathbb{Z}_p \times \mathbb{Z}_{p^2}, \qquad \mathbb{Z}_{p^3}.$$

Assume that G is not abelian. We know that $|Z(G)| = p$ and

the map $x \mapsto x^p$ is a group homomorphism from G into $Z(G)$.

The image of this homomorphism is either of order p or trivial, and so the kernel has order p^2 or p^3. In the former case G must contain an element of order p^2 (by picking an element outside the kernel) and in the latter case every non-identity element of G has order p. Denote $E = \{x \in G \colon x^p = 1\}$, which is the kernel of the p-th power map.

Case 1: G has an element of order p^2. Let x be an element of order p^2 and $H = \langle x \rangle$. We have $H \trianglelefteq G$ (any subgroup of index p in G has to be normal). Both E and H have order p^2, and since they are not identical, E is not contained in H. Take an element y in E but not in H and let $K = \langle y \rangle \cong \mathbb{Z}_p$. Since $H \cap K = \{1\}$, $G \cong H \rtimes K$ with respect to some $\varphi \colon K \to \mathrm{Aut}(H)$. We only need to consider the nontrivial homomorphisms. By Proposition 14.4, $\mathrm{Aut}(H) = (\mathbb{Z}_{p^2})^\times$ is a cyclic group of order $p(p-1)$ and so contains a unique subgroup of order p, given by $\langle \gamma \rangle$ where

$$\gamma(x) = (1 + p)x, \qquad x \in \mathbb{Z}_{p^2}.$$

Indeed by direct verification, $1+p$ is of order p in $(\mathbb{Z}_{p^2})^\times$. Then the only non-trivial homomorphism φ from K to $\mathrm{Aut}(H)$ is given by $\varphi(y) = \gamma$.

More precisely,

$$G = \left\langle x, y \mid x^{p^2} = y^p = 1,\ yxy^{-1} = x^{1+p} \right\rangle.$$

(In the above we are using the usual multiplicative notation in a group.)

Case 2: every non-identity element of G has order p. Let H be any subgroup of G of order p^2. For example we may take an order p subgroup in $G/Z(G)$ (which is of order p^2) and take H to be its inverse image. Then $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Let $K = \langle y \rangle$ for any element y of $G \smallsetminus H$. Since H has index p, $H \trianglelefteq G$ and since K has order p but is not contained in H, $H \cap K = 1$. Then G is isomorphic to $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$, for some nontrivial homomorphism $\varphi\colon K \to \mathrm{Aut}(H)$. Recall $\mathrm{Aut}(H) \cong \mathrm{GL}_2(\mathbb{F}_p)$ and $|\mathrm{Aut}(H)| = (p^2-1)(p^2-p)$. Since φ is nontrivial, φ is injective, whose image is a Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Conjugating by an element of $\mathrm{GL}_2(\mathbb{F}_p)$ if necessary, we may assume that φ is given by $\varphi(y) = \gamma$, where

$$\gamma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Writing $H = \langle a \rangle \times \langle b \rangle$, the corresponding automorphism of H is given by

$$\gamma\colon a \mapsto ab, \qquad \gamma\colon b \mapsto b.$$

One thus has a non-abelian group $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$. More precisely,

$$G = \left\langle a, b, x \mid a^p = b^p = x^p = 1,\ ab = ba,\ xax^{-1} = ab,\ xbx^{-1} = b \right\rangle.$$

Obviously, the two non-abelian groups from Case 1 and Case 2 are non-isomorphic.

In summary, we have 5 non-isomorphic groups of order p^3: three abelian groups and two non-abelian groups.

15. Group Representations: Elementary Notions

Let G be a finite group.

Definition 15.1. (1) A finite dimensional representation of G is a homomorphism

$$\pi : G \to \mathrm{GL}(V),$$

where V is a finite dimensional complex vector space.

(2) A subspace $U \subseteq V$ is called invariant if

$$\pi(x)U \subseteq U, \qquad x \in G.$$

The spaces $\{0\}$ and V are called trivial invariant subspaces.

(3) π is said to be irreducible if it has no non-trivial invariant subspaces.

When V is endowed with a positive definite Hermitian form $<,>$ (or an inner product), a homomorphism

$$\pi : G \to U(V)$$

is called a unitary representation. Here $U(V)$ is the group of unitary operators with respect to the form $<,>$.

Lemma 15.2. *Suppose that (π, V) is a finite dimensional representation of G. Then there exists a positive definite Hermitian form such that π is unitary with respect to this form.*

Proof. Take any positive definite Hermitian form $(,)$ on V, define a new form $<,>$ by averaging as follows:

$$< u, v >= \frac{1}{|G|} \sum_{g \in G} (\pi(g)u, \pi(g)v).$$

Then clearly π is unitary with respect to $<,>$. □

Proposition 15.3. *Let π be a finite dimensional representation of G, then V is a direct sum of irreducible (sub)representations.*

Proof. We may assume that π is unitary. We claim that if U is an invariant subspace, then the orthogonal complement $U^{\perp}$ of U is also invariant.

To see this, let $u \in U^{\perp}$, then for any $v \in U$, then

$$< \pi(g)u, v >=< u, \pi(g^{-1})v >= 0.$$

We continue the proof. If π is irreducible, then there is nothing to prove. If not, let U be a nontrivial invariant subspace, then we have

$$V = U \oplus U^{\perp},$$

as representations of G. We then continue (for a finite number of times) until we get a direct sum of irreducible representations. $\square$

Definition 15.4. (1) Given two representations $\pi_i : G \to \mathrm{GL}(V_i)$ $(i = 1, 2)$, an operator $T \in Hom(V_1, V_2)$ is called intertwining if

$$T\pi_1(g) = \pi_2(g)T, \qquad \text{for all } g \in G.$$

The space of intertwining operators is denoted by $Hom_G(V_1, V_2)$.

(2) Two representations $\pi_i : G \to \mathrm{GL}(V_i)$ $(i = 1, 2)$ are called equivalent if there exists an invertible intertwining map T, namely

$$T\pi_1(g)T^{-1} = \pi_2(g), \qquad g \in G.$$

We write $\pi_1 \cong \pi_2$.

(3) Representations which are not equivalent are called inequivalent.

Theorem 15.5 (Schur's Lemma)**.** (1) *Given two irreducible representations $\pi_i : G \to \mathrm{GL}(V_i)$ $(i = 1, 2)$ and $T \in Hom_G(V_1, V_2)$, then T is either 0 or invertible. Consequently if π_1 and π_2 are inequivalent, then*

$$Hom_G(V_1, V_2) = 0.$$

(2) *If $T \in Hom_G(V_1, V_1)$, then $T = \lambda I$ for some $\lambda \in \mathbb{C}$. Consequently if π_1 and π_2 are equivalent, then*

$$\dim Hom_G(V_1, V_2) = 1.$$

Proof. (1) Let $T \in Hom_G(V_1, V_2)$. Consider $\ker(T) \subseteq V_1$. It is an invariant subspace since

$$T(\pi_1(g)v_1) = \pi_2(g)(Tv_1) = 0, \qquad g \in G,\ v_1 \in \ker(T).$$

By the irreducibility, we either have $\ker(T) = V_1$, in which case $T = 0$, and we are done, or $\ker(T) = 0$, in which case T is injective. We assume the latter.

Now it is also easy to see that $\mathrm{im(T)} \subseteq \mathrm{V_2}$ is invariant. As T is injective, we see that $\mathrm{im(T)} \neq 0$. Therefore $\mathrm{im(T)} = \mathrm{V_2}$ by irreducibility.

(2) By the Fundamental Theorem of Algebra, T has an eigenvalue, say λ. Clearly $T - \lambda I \in Hom_G(V_1, V_1)$. Its kernel (the λ-eigenspace of T) is invariant and is not the zero space. By the irreducibility, we must have $\ker(T - \lambda I) = V$, namely $T = \lambda I$. $\square$

Corollary 15.6. *Write*

$$V \cong \sum_i m_i V_i$$

as direct sums of inequivalent irreducible representations V_i, where $m_i \in \mathbb{Z}^+$ are non-negative integers. Then for each i, $m_i = \dim Hom_G(V_i, V)$.

Proof. We have

$$Hom_G(V_i, V) = Hom_G(V_j, \sum_j m_j V_j) \cong \sum_j m_j Hom_G(V_i, V_j),$$

and by Schur's Lemma, its dimension is equal to m_i. □

Remark: The integer m_i is called the multiplicity of V_i in V.

Proposition 15.7. *A finite dimensional representation (π, V) of a finite group G is irreducible if and only if $Hom_G(V, V) = \mathbb{C}I$.*

Proof. Write $V \cong \sum_i m_i V_i$, then $Hom_G(V, V) = \sum_{i,j} m_i m_j Hom_G(V_i, V_j)$, and so $\dim Hom_G(V, V) = \sum_i m_i^2$. This dimension is 1 if and only if one of m_i is 1 and the rest is 0, i.e., V is irreducible. □

We look at the special case where G is a finite abelian group.

Proposition 15.8. *If G is finite abelian, and (π, V) is an irreducible finite dimensional representation of G, then V is one dimensional.*

Proof. Since G is abelian, we see that for each $g \in G$,

$$\pi(g) \in Hom_G(V, V).$$

Thus $\pi(g) = \lambda(g)I$, for some $\lambda(g) \in \mathbb{C}$.

Now since all $\pi(g)$ are scalar operators, any subspace of V is invariant. Then the irreducibility forces V to be one dimensional. □

Remark: A 1-dimensional representation is called a character: it is a homomorphism

$$G \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times.$$

Example. Let $G = S_n$. The map $\chi\colon G \to \mathbb{C}^\times$ defined by $\chi(\sigma) = \mathrm{sgn}(\sigma)$ is a character.

16. Group Representations: Characters

We fix a finite group, as in the previous chapter.

Definition 16.1. Let (π, V) be a representation, the character of π, denoted by χ_π, is the function on G given by

$$\chi_\pi(g) = Tr(\pi(g)), \qquad g \in G.$$

Remark: For a linear operator A on a vector space V, its trace may be computed using matrix representation of A in any basis:

$$Tr(A) = \sum_i v_i^*(Av_i),$$

where $\{v_i\}$ is a basis of V and $\{v_i^*\}$ its dual basis. Note that $v_i^*(Av_i)$ is the coefficient of Av_i in front of v_i.

Clearly equivalent representations have the same characters.

Definition 16.2. (1) Let (π, V) be a representation. The dual representation or the contragradient representation (π^*, V^*) is defined as follows: V^* is the dual space of V, and

$$(\pi^*(g)v^*)(v) = v^*(\pi(g)^{-1}v), \qquad g \in G,\ v^* \in V^*,\ v \in V.$$

(2) Given two representations (π_i, V_i), $i = 1, 2$, the tensor product representation $(\pi_1 \otimes \pi_2, V_1 \otimes V_2)$ is defined by

$$(\pi_1 \otimes \pi_2)(g)(v_1 \otimes v_2) = \pi_1(g)v_1 \otimes \pi_2(g)v_2, \qquad g \in G,\ v_1 \in V_1,\ v_2 \in V_2.$$

Remark: If we fix a basis of V, then we can represent $\pi(g)$ as an invertible matrix. With respect to the dual basis in V^*, the matrix corresponding to $\pi^*(g)$ is then the transpose inverse of $\pi(g)$.

Proposition 16.3 (Elementary properties of characters)**.**

(1) $\chi_\pi(e) = \dim V$.
(2) $\chi_\pi(g) = \chi_\pi(hgh^{-1})$, for $h, g \in G$. We say that χ_π is a class function.
(3) $\chi_{\pi^*}(g) = \chi_\pi(g^{-1}) = \overline{\chi_\pi(g)}$, for $g \in G$.
(4) $\chi_{\pi_1 \otimes \pi_2}(g) = \chi_{\pi_1}(g)\chi_{\pi_2}(g)$, for $g \in G$.

Proof. (1) and (2) are obvious. We prove (3) and (4).

(3) Let $\{v_i\}_{1 \le i \le n} \subseteq V$ be any basis of V, and $\{v_i^*\}_{1 \le i \le n} \subseteq V^*$ its dual basis. Then

$$Tr(\pi^*(g)) = \sum_i (\pi^*(g)v_i^*)(v_i) = \sum_i v_i^*(\pi(g)^{-1}v_i) = Tr(\pi(g)^{-1}).$$

This is the first equality.

To see the second equality, we assume (as we may) that π is unitary, so that $\pi(g)$ is unitary for each $g \in G$. As such $\pi(g)$ is diagonalizable,

and $Tr(\pi(g))$ is the sum of its eigenvalues λ_i ($1 \leq i \leq n$, $n = \dim V$). Here $|\lambda_i| = 1$. Then both quantities in Equation (1.1) are equal to

$$\sum_{i=1}^{n} \frac{1}{\lambda_i} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{Tr(\pi(g))}.$$

The result follows.

(4) Let $\{v_i\}_{1\leq i\leq n}$ (resp. $\{w_j\}_{1\leq j\leq m}$) be a basis of V_1 (resp. V_2), and $\{v_i^*\}_{1\leq i\leq n}$ (resp. $\{w_j^*\}_{1\leq j\leq m}$) be its dual basis of V_1^* (resp. V_2^*). Then

$$\begin{aligned}
\chi_{\pi_1\otimes\pi_2}(g) &= \sum_{i,j} (v_i^* \otimes w_j^*)((\pi_1(g) \otimes \pi_2(g))(v_i \otimes w_j)) \\
&= \sum_{i,j} v_i^*(\pi_1(g)v_i) w_j^*(\pi_2(g)w_j) \\
&= \sum_{i} v_i^*(\pi_1(g)v_i) \sum_{j} w_j^*(\pi_2(g)w_j) \\
&= \chi_{\pi_1}(g)\chi_{\pi_2}(g).
\end{aligned}$$

□

The following lemma tells us how to produce invariants. The process is called averaging.

Lemma 16.4. *For a finite dimensional representation (π, V), define the operator*

$$P = \frac{1}{|G|} \sum_{g\in G} \pi(g),$$

namely $Pv = \frac{1}{|G|} \sum_{g\in G} \pi(g)v$ for $v \in V$. Then $P^2 = P$, and $\mathrm{im(P)} = \mathrm{V^G}$*, where*

$$V^G = \{v \in V | \pi(g)v = v, \forall g \in G\}$$

is the space of G-invariants.

Proof. We compute

$$\begin{aligned}
P^2v = P(Pv) = P(\frac{1}{|G|} \sum_{x\in G} \pi(x)v) &= \frac{1}{|G|} \sum_{x\in G} P(\pi(x)v) \\
&= \frac{1}{|G|^2} \sum_{x,y\in G} \pi(y)\pi(x)v = \frac{1}{|G|^2} \sum_{x,y\in G} \pi(yx)v \\
&= \frac{1}{|G|^2} \sum_{x,z\in G} \pi(z)v = \frac{1}{|G|} \sum_{x\in G} Pv = Pv.
\end{aligned}$$

Also for $y \in G$, we have

$$\pi(y)Pv = \frac{1}{|G|}\sum_{x\in G}\pi(y)\pi(x)v = \frac{1}{|G|}\sum_{x\in G}\pi(yx)v = \frac{1}{|G|}\sum_{z\in G}\pi(z)v = Pv,$$

and so $Pv \in V^G$. Conversely if $w \in V^G$, then

$$Pw = \frac{1}{|G|}\sum_{x\in G}\pi(x)w = \frac{1}{|G|}\sum_{x\in G} w = w.$$

We thus conclude that $\mathrm{im(P)} = \mathrm{V^G}$. □

Remark: A linear operator P on V is called a projection operator onto W if $P^2 = P$ and $W = \mathrm{im(P)}$. We have

$$Tr(P) = \dim W.$$

To see this, fix a basis $\{w_1, ..., w_k\}$ of W and extend it to a basis $\{w_1, ..., w_k, w_{k+1}, ..., w_n\}$ of V. Then $Pw_i = w_i$ for $i \leq k$, and Pw_i is in the span of $\{w_1, ..., w_k\}$ for $i > k$, so $Tr(P) = k$.

Corollary 16.5.

$$\frac{1}{|G|}\sum_{x\in G}\chi_\pi(x) = \dim V^G.$$

Proof. We note that

$$\frac{1}{|G|}\sum_{x\in G}\chi_\pi(x) = \frac{1}{|G|}\sum_{x\in G} Tr(\pi(x)) = Tr(P),$$

where P is the averaging operator defined above. Since P is a projection operator onto V^G, its trace is just $\dim V^G$. □

Theorem 16.6. *Given two representations (π_i, V_i) $(i = 1, 2)$, we have*

$$\frac{1}{|G|}\sum_{x\in G}\overline{\chi_{\pi_1}(x)}\chi_{\pi_2}(x) = \dim Hom_G(V_1, V_2).$$

Proof. We have

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G}\overline{\chi_{\pi_1}(x)}\chi_{\pi_2}(x) =& \frac{1}{|G|}\sum_{x\in G}\chi_{\pi_1^*}\chi_{\pi_2}(x) = \frac{1}{|G|}\sum_{x\in G}\chi_{\pi_1^*\otimes\pi_2}(x)\\ =& \dim(V_1^*\otimes V_2)^G = \dim Hom_G(V_1, V_2).\end{aligned}$$

□

Corollary 16.7 (Schur orthogonality relations)**.** *If (π_i, V_i) are irreducible for $i = 1, 2$, then*

$$\frac{1}{|G|}\sum_{x\in G}\overline{\chi_{\pi_1}(x)}\chi_{\pi_2}(x) = \begin{cases}0, & \pi_1 \ncong \pi_2,\\ 1, & \pi_1 \cong \pi_2.\end{cases}$$

Remark: We have the standard Hermitian inner product on $\mathbb{C}(G)$:

$$< f_1, f_2 >= \frac{1}{|G|} \sum_{x \in G} f_1(x)\overline{f_2(x)}, \qquad f_1, f_2 \in \mathbb{C}(G).$$

Then Schur's orthogonality relations says that irreducible characters form an orthonormal set in $\mathbb{C}(G)$, and in fact as we shall see later, they form an orthonormal basis in the space of class functions on G.

Corollary 16.8. *A finite dimensional representation (π, V) of a finite group G is determined (up to equivalence) by its character. More precisely, if we write $V \cong \sum_i m_i V_i$ as direct sums of inequivalent irreducible representations V_i, then*

$$m_i =< \chi_\pi, \chi_i >,$$

where χ_i is the character of the irreducible representation V_i.

17. Group Representations: Further Results

Let G be a finite group, as before.

Definition 17.1. The left regular representation of G is the representation of G on $\mathbb{C}(G)$ given by

$$(L(g)f)(x) = f(g^{-1}x), \qquad f \in \mathbb{C}(G),\ g, x \in G.$$

Similarly, the right regular representation of G is given

$$(R(g)f)(x) = f(xg), \qquad f \in \mathbb{C}(G),\ g, x \in G.$$

They are obviously unitary representations, with respect to the standard inner product on $\mathbb{C}(G)$.

Definition 17.2. Let $\hat{G}$ denote the set of equivalent classes of (finite-dimensional) irreducible representations of G, called the dual of G.

Let $(\pi, V) \in \hat{G}$. Without loss of generality, we may assume that π is unitary.

Definition 17.3. Let (π, V) be a unitary representation of G. A matrix coefficient of π is a function of the form

$$\phi_{u,v}(x) = < \pi(x)u, v >, \quad x \in G,$$

where $u, v \in V$.

Theorem 17.4 (Schur's orthogonality relations)**.** *Let (π_i, V_i) $(i = 1, 2)$ be (finite-dimensional) irreducible unitary representations of G.*

(1) *If $\pi_1 \ncong \pi_2$, then*

$$\frac{1}{|G|} \sum_{x \in G} < \pi_1(x)u_1, v_1 > \overline{< \pi_2(x)u_2, v_2 >} = 0$$

for $u_1, v_1 \in V_1$, $u_2, v_2 \in V_2$.

(2) *If $\pi_1 = \pi_2 = \pi$, then*

$$\frac{1}{|G|} \sum_{x \in G} < \pi(x)u_1, v_1 > \overline{< \pi(x)u_2, v_2 >} = \frac{1}{\dim \pi} < u_1, u_2 > \overline{< v_1, v_2 >},$$

for $u_1, v_1, u_2, v_2 \in V$.

Proof. The left side of the equality is linear in u_1. Therefore it has the form $< u_1, \eta >$, where η is a certain vector in V depending on u_2, v_1, v_2. For fixed v_1, v_2, the vector η depends linearly on u_2. Therefore we may write $\eta = Au_2$, where A is a certain linear operator from V_2 to V_1 depending on v_1, v_2.

By a change of variable argument, we see that

$$< \pi_1(g)u_1, A\pi_2(g)u_2 > = < u_1, Au_2 >, \qquad g \in G.$$

This implies that A intertwines π_2 and π_1. If $\pi_1 \ncong \pi_2$, A must be zero (by considering its kernel).

In case (ii), we have $A = \lambda I$. Obviously λ depends on v_1 and v_2. Reasoning in the same fashion (by applying Schur's Lemma one more time), we see that the dependence of λ on v_1, v_2 has the form $\lambda = c\overline{< v_1, v_2 >}$, for some c. Thus

$$\frac{1}{|G|}\sum_{x\in G} < \pi(x)u_1, v_1 > \overline{< \pi(x)u_2, v_2 >} = c < u_1, u_2 > \overline{< v_1, v_2 >}.$$

We proceed to determine c. For any $u, v \in V$, we have

$$\frac{1}{|G|}\sum_{x\in G} | < \pi(x)u, v > |^2 = c||u||^2||v||^2.$$

Take $v_1, ..., v_n$ to be an orthnormal basis of V, where $n = \dim V$. Then we have

$$\frac{1}{|G|}\sum_{x\in G} | < \pi(x)u, v_i > |^2 = c||u||^2.$$

Since $\sum_{1\le i\le n} | < \pi(x)u, v_i > |^2 = ||\pi(x)u||^2 = ||u||^2$, we conclude that $cn = 1$. □

Now let $\{v_i\}_{1\le i\le \dim\pi}$ be an orthonormal basis of V, and $\phi^\pi_{i,j}$ be the matrix coefficient given by

$$\phi^\pi_{i,j}(x) =< \pi(x)v_i, v_j >, \quad x \in G.$$

Theorem 17.5. (1) *The matrix coefficients of π, where π ranges over $\hat{G}$, spans $\mathbb{C}(G)$.*

(2)
$$\{(\dim\pi)^{\frac{1}{2}}\phi^\pi_{i,j}\}_{\pi\in\hat{G}, 1\le i,j\le\dim\pi}$$
is an orthonormal basis of $\mathbb{C}(G)$.

(3) *We have the following decomposition of the right regular representation:*
$$\mathbb{C}(G) \cong \sum_{\pi\in\hat{G}} \dim(\pi)\pi.$$

Proof. First we note that for any $\pi \in \hat{G}$, the matrix coefficients of π are invariant subspaces under R (the right regular representation). Suppose (1) is not true. Then we can find a nonzero invariant subspace U of $\mathbb{C}(G)$, which is orthogonal to matrix coefficients of any $\pi \in \hat{G}$.

By reducing U if necessary, we may assume that U is irreducible under R.

Take $u_1, ..., u_m$ to be an orthonormal basis of U. By our construction, we know U is orthogonal to the matrix coefficient $x \mapsto (R(x)u_i, u_j)$, namely

$$\frac{1}{|G|}\sum_{x\in G}(R(x)u_i, u_j)\overline{f(x)} = 0, \qquad \forall f \in U.$$

Since $f \mapsto f(e)$ is a linear functional on U, we can find $z \in U$ such that $f(e) = (f, z)$. We have

$$u(x) = (R(x)u)(e) = (R(x)u, z)$$

for all $u \in U$. On the other hand, we have (by the Schur Orthogonality Relations)

$$0 = \frac{1}{|G|}\sum_{x\in G}(R(x)u_j, u_i)\overline{(R(x)u, z)} = \frac{1}{\dim U}(u_j, u)\overline{(u_i, z)}$$

for all i, j. Since we can take $u = u_j$ and since i is arbitrary, the above equation forces $z = 0$ and gives a contradiction. We thus conclude that the linear span of matrix coefficients of all irreducible π's is all of $\mathbb{C}(G)$.

(2) This follows from (1) and Schur's orthogonality relations.

(3) Fix $(\pi, V) \in \hat{G}$. Define

$$\begin{aligned}\Phi_j : V &\to \mathbb{C}(G),\\ v &\mapsto < \pi(x)v, v_j > \qquad .\end{aligned}$$

Since

$$(\Phi_j(\pi(g)v)(x) = < \pi(x)\pi(g)v, v_j > = < \pi(xg)v, v_j > = (R(g)\Phi_j(v))(x),$$

we see that Φ_j is intertwining, and since π is irreducible, Φ_j has to be injective. Namely Φ_j imbeds (π, V) into $\mathbb{C}(G)$ in a G-equivariant way. In fact, Schur's orthogonality relation tells us that $||\Phi_j(v)||_{\mathbb{C}(G)} = \frac{||v||}{(\dim \pi)^{\frac{1}{2}}}$, i.e., up to a normalization, ϕ_j is an isometric imbedding. Clearly

$$\mathrm{im}(\Phi_\mathrm{j}) = \text{span of } \{< \pi(\mathrm{x})\mathrm{v_i}, \mathrm{v_j} > | 1 \leq \mathrm{i} \leq \dim(\pi)\}.$$

Schur's orthogonality relations also imply that for $j \neq k$, the images of Φ_j and Φ_k are orthogonal to each other. Notice that the span of matrix coefficients of π is the span of $< \pi(x)v_i, v_j >$, $1 \leq i, j \leq \dim(\pi)$. We thus conclude that this space is the orthogonal direct sum of the images of Φ_j for $1 \leq j \leq \dim(\pi)$, and each of the direct summard is equivalent to (π, V). Part (3) follows. □

Lemma 17.6. *Let $(\pi, V) \in \hat{G}$. We have*

$$\frac{1}{|G|}\sum_{x\in G}\pi(xgx^{-1}) = \frac{\chi_\pi(g)}{\dim \pi}I.$$

Consequently

$$\frac{1}{|G|}\sum_{x\in G} < \pi(xgx^{-1})v, w >= \frac{\chi_\pi(g)}{\dim \pi} < v, w >,$$

for $v, w \in V$.

Proof. We easily check that for each $g \in G$, the operator $\frac{1}{|G|}\sum_{x\in G}\pi(xgx^{-1})$ is intertwining, and so by Schur's Lemma it is λI for some $\lambda \in \mathbb{C}$. By taking the trace, we see that $\lambda = \frac{\chi_\pi(g)}{\dim \pi}$. □

Theorem 17.7. *Let G be a finite group. Write $\hat{G} = \{\pi_i\}_{1\le i\le r}$, where r is the number of equivalent classes of (finite dimensional) irreducible representations of G. Then*

(1)
$$\sum_{i=1}^{r} d_i^2 = |G|,$$
where $d_i = \dim \pi_i$.

(2) *Any class function on G is a linear combination of χ_{π_i}, for $1 \le i \le r$.*

(3) *The number r is equal to the number of conjugate classes of G.*

Proof. (1) follows from $\mathbb{C}(G) \cong \sum_{\pi\in\hat{G}} \dim(\pi)\pi$, by dimension counting on the two sides.

For (2), let f be a class function on G, namely it satisfies $f(g) = f(xgx^{-1})$, for any $g, x \in G$. We obviously have

$$f(g) = \frac{1}{|G|}\sum_{x\in G} f(xgx^{-1}).$$

On the other hand, we know that each $f \in \mathbb{C}(G)$ is in the span of matrix coefficients of $\pi \in \hat{G}$. We write

$$f(g) = \sum_{\pi\in\hat{G}}\sum_{i,j} c_{ij} < \pi(g)v_i, v_j > .$$

By the lemma above, we have

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G} f(xgx^{-1}) &= \sum_{\pi\in\hat{G}}\sum_{i,j} c_{ij}(\frac{1}{|G|}\sum_{x\in G} < \pi(xgx^{-1})v_i, v_j >) \\ &= \sum_{\pi\in\hat{G}}\sum_{i,j} c_{ij}\frac{\chi_\pi(g)}{\dim \pi} < v_i, v_j > .\end{aligned}$$

But the left hand side is actually equal to $f(g)$, and therefore f is a linear combination of χ_π, where π ranges over $\hat{G}$.

For (3), we observe that a class function is completely determined by its values on conjugate classes, and so the dimension of the space of class functions is equal to the number of conjugate classes. On the other hand, the characters χ_{π_i}, $1 \leq i \leq r$ are clearly linearly independent (since they are orthogonal to each other). Together with (2), we see that the characters χ_{π_i}, $1 \leq i \leq r$ form a basis of the space of class functions and so the dimension of the space of class functions is also r. $\square$