Part 4. Structural properties of groups

11. Order of an element

Having seen several different types of concrete groups, we now set out to investigate arbitrary abstract groups.

Definition 11.1. Let G be a group, let e be the identity of G, and let $a \in G$ be arbitrary. Then the *order* of a is the smallest positive integer n such that $a^n = e$ if such n exists, or infinite otherwise.

We will write $|a|$ to denote the order of a in G.

Examples 11.2. In the dihedral group D_n, every reflection $\sigma\rho^i$ has order 2 since

$$\sigma\rho^i \cdot \sigma\rho^i = \sigma\sigma\rho^{-i}\rho^i = \mathrm{id}$$

from Example 10.10.

The rotation $\rho \in D_n$ has order n since $\rho^n = \mathrm{id}$ from Example 10.10 and $\rho^i \neq \mathrm{id}$ for all $i < n$.

Every non-zero element x of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ has an infinite (additive) order since

$$nx \neq 0$$

for all $n \in \mathbb{Z}$ such that $n > 0$.

The identity is the only element of order 1 in any group, since if $x^1 = 1$, then $x = 1$.

Example 11.3. The orders of the elements of $\mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$ (under addition modulo 10) are 1, 10, 5, 10, 5, 2, 5, 10, 5, 10 respectively.

Example 11.4. Let $f = (1\ 2)(3\ 4\ 5) \in S_5$. Then its powers are:

$$\begin{aligned} f^2 &= (3\ 5\ 4) \\ f^3 &= (1\ 2) \\ f^4 &= (3\ 4\ 5) \\ f^5 &= (1\ 2)(3\ 5\ 4) \\ f^6 &= \mathrm{id}. \end{aligned}$$

Hence, the order of f is 6.

Example 11.5. The order of the element 3 in the multiplicative group $\mathbb{Z}_7 \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$ is found by taking powers:

$$3^2 = 2, \quad 3^3 = 2 \cdot 3 = 6, \quad 3^4 = 6 \cdot 3 = 4, \quad 3^5 = 4 \cdot 3 = 5, \quad 3^6 = 5 \cdot 3 = 1.$$

Hence 3 has order 6.

Theorem 11.6. *If G is a finite group, then every element of G has finite order.*

Proof. Let $a \in G$ be arbitrary. Then, since G is closed, $a, a^2, a^3, \ldots, a^i, \ldots \in G$. Since G is finite, there exist $i, j \in \mathbb{N}$ such that $i \neq j$ and $a^i = a^j$. We may assume that $i < j$. But then, multiplying by a^{-j}, we get $a^{i-j} = e$. If $M = \{\, m \in \mathbb{N} \,:\, a^m = e \,\}$, then M is not empty since $i - j \in M$. Hence M has a least element and this is the order of a. □

Theorem 11.7. *Let G be a group, let $a \in G$ such that $|a| = n$, and let $i, j \in \mathbb{Z}$. Then $a^i = a^j$ if and only if n divides $(i - j)$.*

Proof. ($\Leftarrow$) If n divides $(i - j)$, then we may write $i - j = qn$ for some $q \in \mathbb{N}$. Hence

$$a^i = a^{j+qn} = a^j(a^n)^q = a^j e^q = a^j.$$

($\Rightarrow$) Assume that $a^i = a^j$. By the Division Algorithm (Theorem 7.1), we may write $i - j = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. But then

$$a^{(i-j)} = a^{qn+r} = (a^n)^q a^r = a^r$$

and

$$a^{(i-j)} = a^i a^{-j} = a^i a^{-i} = e.$$

Since n is the order of a and $r < n$, we conclude that $r = 0$, and hence n divides $(i - j)$. □

Corollary 11.8. *Let G be a group and let $a \in G$ where $|a| = n$. Then $a^m = e$ if and only if n divides m.*

Proof. Let $i = m$ and $j = 0$ in Theorem 11.7. Then $a^m = a^0 = e$ if and only if n divides $m-0 = m$, as required. □

We are now going to see how to find the orders of elements in various specific groups introduced earlier.

Theorem 11.9. *Let $n \in \mathbb{Z}$ be such that $n > 1$, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, and let $a \in \mathbb{Z}_n$. Then the order of a in $\mathbb{Z}_n$ under addition modulo n is $n/\gcd(a, n)$.*

To prove Theorem 11.9 we require the following lemma.

Lemma 11.10. *Let $a, b \in \mathbb{Z}$. Then the following hold:*

(i) $\gcd(a/\gcd(a,b), b/\gcd(a,b)) = 1$;
(ii) *if* $\gcd(a, b) = 1$ *and a divides bc for some $c \in \mathbb{Z}$, then a divides c.*

Proof. We will use that, by Bézout's Identity (Theorem 7.11), there exist $x, y \in \mathbb{Z}$ such that

$$xa + yb = \gcd(a, b)$$

in the proofs of both parts of the lemma.

(i). We may write

$$x \cdot \frac{a}{\gcd(a,b)} + y \cdot \frac{b}{\gcd(a,b)} = \frac{\gcd(a,b)}{\gcd(a,b)} = 1.$$

But, by Theorem 7.11, $\gcd(a/\gcd(a,b), b/\gcd(a,b))$ is the least positive integer of this form and so

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1.$$

(ii). By Bézout's Identity,

$$xac + ybc = \gcd(a, b) \cdot c = c$$

and since a divides ac and bc, it follows that a divides c. □

Proof of Theorem 11.9. We will denote the order of a by $|a|$. It follows from the definition that

$$\underbrace{a + a + \cdots + a}_{|a| \text{ times}} = |a| \cdot a = 0 \pmod{n}.$$

We can write $a = a_1 \gcd(a, n)$ for some $a_1 \in \mathbb{Z}$. Hence

$$\frac{n}{\gcd(a,n)} \cdot a = \frac{n}{\gcd(a,n)} \cdot a_1 \gcd(a, n) = na_1 = 0 \pmod{n}.$$

But $|a|$ is the least positive integer such that $|a| \cdot a = 0 \pmod{n}$ and so $|a| \leq n/\gcd(a, n)$.

We can also write $n = n_1 \gcd(a, n)$. Since $|a| \cdot a = 0 \pmod{n}$, it follows that there exists $q \in \mathbb{Z}$ such that $|a| \cdot a = qn$. Thus

$$|a| \cdot a = qn \quad \Rightarrow \quad |a|a_1 \gcd(a,n) = qn_1 \gcd(a,n) \quad \Rightarrow \quad |a| \cdot a_1 = qn_1 \quad \Rightarrow \quad n_1 \text{ divides } |a| \cdot a_1.$$

But $\gcd(a_1, n_1) = \gcd(a/\gcd(a,n), n/\gcd(a,n)) = 1$, by Lemma 11.10(i). Hence by Lemma 11.10(ii), n_1 divides $|a|$ and so $n_1 \leq |a|$. We conclude that $|a| = n_1 = n/\gcd(a, n)$, as required. □

Theorem 11.11. *Let $f = (a_1\ a_2\ \ldots\ a_m)$ be an m-cycle in the symmetric group S_n. Then the order of f is m.*

Proof. Since

$$\begin{aligned}
(a_1)f^m &= (a_2)f^{m-1} = \cdots = (a_m)f = a_1 \\
(a_2)f^m &= (a_3)f^{m-1} = \cdots = (a_m)f^2 = (a_1)f = a_2 \\
&\vdots \\
(a_i)f^m &= (a_{i+1})f^{m-1} = \cdots = (a_m)f^i = (a_1)f^{i-1} = \cdots = f_i,
\end{aligned}$$

it follows that $f^m = \mathrm{id}$. Also since $(a_1)f^j = a_{j+1} \neq a_1$ for all $j < m$, it follows that $f^j \neq \mathrm{id}$ for all $j < m$. Hence the order of f is m. □

Definition 11.12. Let $a, b \in \mathbb{Z}$. Then the *least common multiple* of a and b is the smallest positive integer that is a multiple of both a and b; it is denoted by $\operatorname{lcm}(a, b)$.

It is possible to calculate $\operatorname{lcm}(a, b)$ using the equality:

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

and the Euclidean algorithm.

Let $a, b, c \in \mathbb{Z}$. Then

$$\operatorname{lcm}(\operatorname{lcm}(a, b), c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$$

and

$$\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)).$$

In other words, gcd and lcm are associative operations. Hence we can write $\gcd(a, b, c)$ or $\operatorname{lcm}(a, b, c)$ without ambiguity of meaning. Furthermore, we can also write $\gcd(a_1, a_2, \ldots, a_n)$ and $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$ where $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

It is not true that

$$\operatorname{lcm}(a, b, c) = \frac{abc}{\gcd(a, b, c)}!^{1}$$

But it is true that:

$$\operatorname{lcm}(a, b, c) = \frac{abc}{\gcd(ab, ac, bc)}$$

or more generally that

$$\operatorname{lcm}(a_1, \ldots, a_n) = \frac{a_1 \cdots a_n}{\gcd(p_1, p_2, \ldots, p_n)}$$

where $p_1, \ldots, p_n$ are all possible products consisting of $n - 1$ of $\{a_1, \ldots, a_n\}$.

Corollary 11.13. *Let $f \in S_n$ be arbitrary and write f as a product $g_1 g_2 \cdots g_r$ of disjoint cycles of lengths $m_1, m_2, \ldots, m_r$. Then the order of f is* $\operatorname{lcm}(m_1, m_2, \ldots, m_r)$.

Proof. Let $N = \operatorname{lcm}(m_1, m_2, \ldots, m_r)$. Then for every m_i there exists l_i such that $N = l_i m_i$. Since disjoint cycles commute,

$$f^N = g_1^N g_2^N \ldots g_r^N = (g_1^{m_1})^{l_1} (g_2^{m_2})^{l_2} \ldots (g_r^{m_r})^{l_r} = \underbrace{\mathrm{id} \circ \mathrm{id} \circ \ldots \circ \mathrm{id}}_{n \text{ times}} = \mathrm{id}.$$

Hence the order of f is at most N.

On the other hand, if the order of f is m, then $f^m = \mathrm{id}$ and so $g_j^m = \mathrm{id}$ for all j (since, as above, disjoint cycles commute). By Corollary 11.8, it follows that the order m_j of g_j divides m for all $j \in \{1, \ldots, r\}$. Hence m is a common multiple of $m_1, m_2, \ldots, m_r$ and so $N \leq m$. □

Example 11.14. Let us consider the Rubik cube puzzle (Figure 8). A rotation of any face permutes the little cubes. Consider the permutation given by a 90° (clockwise) twist of one face, followed by a 90° twist of an adjacent face. Written as permutations, these moves are:

$$f = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8),$$
$$g = (1\ 10\ 12\ 3)(2\ 9\ 11\ 13).$$

Their product is

$$fg = (1)(2\ 4\ 6\ 8\ 9\ 11\ 13)(3\ 5\ 7\ 10\ 12).$$

It has order $\operatorname{lcm}(5, 7) = 35$.

If you apply this combination of moves 35 times, all the cubicles will be in their old places, but twisted for 120°. If you want to get the old orientation, you have to repeat the move $3 \cdot 35 = 105$ times.

[1] When, say, $a = b = 1$ and $c = 4$; or $a = b = 2$ and $c = 1$.

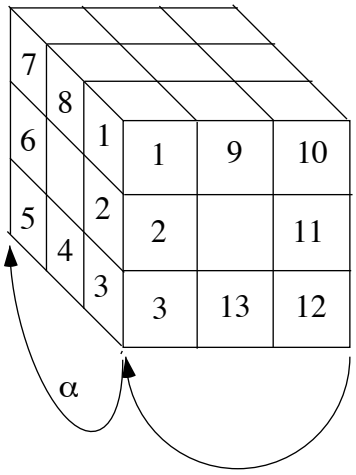

FIGURE 8. Rubik cube

12. SUBGROUPS

A group may contain other groups within it. For example, the group $\mathbb{Q}$ (with respect to addition) contains the group $\mathbb{Z}$, in the sense that $\mathbb{Z} \subseteq \mathbb{Q}$ and that the addition in $\mathbb{Z}$ is the same as the addition in $\mathbb{Q}$ restricted to $\mathbb{Z}$.

Definition 12.1. Let G be a group. A non-empty subset H of G is a *subgroup* of G if it forms a group under the same operation; we denote this by $H \leq G$.

Example 12.2. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ where the operation is addition.

Example 12.3. The multiplicative group $\mathbb{Q} \setminus \{0\}$ is not a subgroup of the additive group $\mathbb{Q}$, because the operations are different. Similarly, $\mathbb{Z}_m$ under addition modulo m is not a subgroup of $\mathbb{Z}_n$ under addition modulo n ($m \neq n$).

Example 12.4. If G is a group and e is the identity of G, then $\{e\}$ is a subgroup if G; called the *trivial subgroup*. Also G itself is a subgroup of G. Any subgroup different from $\{e\}$ and G is called a *proper* subgroup.

It might seem that to check whether a subset H of a group G is a subgroup, we have to check the four axioms. In fact, this can be reduced to checking only two axioms.

Theorem 12.5. *Let H be a non-empty subset of a group G. Then H is a subgroup of G if and only if the following hold:*

Closure: *$xy \in H$ for all $x, y \in H$;*
Inverses: *$x^{-1} \in H$ for all $x \in H$;*

(i.e. H is closed under multiplication and taking inverses).

Proof. ($\Rightarrow$) This follows immediately from the definition.
($\Leftarrow$) Assume that H is closed under multiplication and taking inverses. We verify the axioms:

Closure: This axiom is assumed to hold, so there is nothing to check!
Associativity: Since $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$, it is certainly true that $x * (y * z) = (x * y) * z$ for all $x, y, z \in H \subseteq G$.
Identity: If $a \in H$ is arbitrary, then $a^{-1} \in H$, and hence $e = aa^{-1} \in H$. So, H contains the identity e and $e * x = x * e = x$ for all $x \in H \subseteq G$.
Inverses: This axiom is assumed to hold, so there is nothing to check! □

Example 12.6. Let

$$H = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

We show that H is a subgroup of S_4 by verifying the conditions of Theorem 12.5.

Closure: Follows from the multiplication table:

	id	(12)(34)	(13)(24)	(14)(23)
id	id	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	id	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	id	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	id

Inverses: From the table, we see that shows that H is closed under inverses and that every element is its own inverse.

Example 12.7. The set $GL(n,\mathbb{R})$ of all $n \times n$ invertible matrices (i.e. the matrices with non-zero determinant) with real entries forms a group called the *general linear group* over reals. Let

$$SL(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : \det(A) = 1\},$$

where $\det(A)$ denotes the determinant of A.

We verify that $SL(m,\mathbb{R}) \leq GL(n,\mathbb{R})$ by verifying the conditions of Theorem 12.5.

Closure: Let $A, B \in SL(n,\mathbb{R})$. Then $\det(AB) = \det(A)\det(B) = 1$ and so $AB \in SL(n,\mathbb{R})$.
Inverses: If $A \in SL(n,\mathbb{R})$, then $\det(A^{-1}) = 1/\det(A) = 1$ and so $A^{-1} \in SL(n,\mathbb{R})$.

Hence $SL(n,\mathbb{R}) \leq GL(n,\mathbb{R})$. The group $SL(n,\mathbb{R})$ is called the *special linear group* over $\mathbb{R}$. Analogous constructions can be done over $\mathbb{C}$ and $\mathbb{Q}$, giving the general and special linear groups over these sets.

13. Cyclic groups

In this section we consider a special kind of subgroup of a group arising as all powers of a fixed element.

Theorem 13.1. *Let G be a group and let $g \in G$ be an arbitrary element. Then*

$$\langle\, g \,\rangle = \{g^i : i \in \mathbb{Z}\}$$

is a subgroup of G; called the cyclic subgroup generated by g.

Proof. We must verify the Subgroup Criterion from Theorem 12.5.

Closure: If $a^i, a^j \in H$, then $a^i a^j = a^{i+j} \in H$ by definition.
Inverses: If $a^i \in H$, then $(a^i)^{-1} = a^{-i} \in H$ again by definition.

Hence $H \leq G$ by Theorem 12.5. □

Definition 13.2. If there exists $g \in G$ such that $\langle\, g \,\rangle = G$, then G is called a *cyclic group.*

Example 13.3. The additive group $\mathbb{Z}$ is cyclic, generated by 1 (and also by -1!). Similarly, $\mathbb{Z}_n$ under addition modulo n is generated by 1 and so is cyclic for every n.

Example 13.4. Consider the group $\mathbb{Z}_7 \setminus \{0\}$ under multiplication modulo 7. We have $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. So, this group is cyclic, generated by 3.

Theorem 13.5. *Let n be a positive integer and let $U_n = \{\, x \in \mathbb{Z}_n \setminus \{0\} : \gcd(x,n) = 1 \,\}$ (see Theorem 7.13(ii)). Then U_n is a cyclic group if and only if $n = 2, 4, p^k$, or $2p^k$ where p is a prime and $p \neq 2$.*

Corollary 13.6. *Let p be a prime. Then $\mathbb{Z}_p \setminus \{0\}$ is a cyclic group.*

Proof. We know from Theorem 7.13(iii) that $\mathbb{Z}_p \setminus \{0\}$ is a group, and since p is prime and either $p = p^1$ or $p = 2$, it follows from Theorem 13.5 that $U_p = \mathbb{Z}_p \setminus \{0\}$ is cyclic. □

Corollary 13.7. *Let G be any group and let $g \in G$ be arbitrary. Then the order of the subgroup $\langle\, g \,\rangle$ generated by g is equal to the order of g.*

Proof. If g has infinite order, then $g^i \neq g^j$ whenever $i \neq j$, since otherwise $g^{i-j} = e$ and the order of g is finite. Hence $\langle\, g \,\rangle$ is infinite.

If g has order n, then, by Theorem 11.7, the only distinct powers of g are $e = g^0$, g, $\ldots$, g^{n-1}, so that $\langle\, g \,\rangle = \{e, g, g^2, \ldots g^{n-1}\}$ and $|H| = n$. □

Example 13.8. Let D_n denote the dihedral group of symmetries of an n-gon where $n \geq 2$; see Example 10.10. If ρ denotes the 'basic' rotation by $360°/n$ and σ is any reflection, then the elements of D_n are:

$$\rho^0 = \mathrm{id},\ \rho^1 = \rho,\ \rho^2, \ldots,\ \rho^{n-1},\ \sigma,\ \sigma\rho,\ \sigma\rho^2, \ldots,\ \sigma\rho^{n-1}.$$

and multiplication is completely determined by the rules: $\rho^n = \mathrm{id}$, $\sigma^2 = \mathrm{id}$, and $\rho\sigma = \sigma\rho^{-1} = \sigma\rho^{n-1}$. It follows from Corollary 13.7 that the subgroup generated by σ has 2 elements and the subgroup generated by ρ has n elements.

Example 13.9. If $(1\ 2\ 3)(4\ 5) \in S_5$, then the order of the subgroup generated by $(1\ 2\ 3)(4\ 5)$ is $\mathrm{lcm}(2, 3) = 6$.

Theorem 13.10. *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group generated by a, and let H be any subgroup of G. If H is trivial, then $H = \langle\, e \,\rangle = \{e\}$ where $e \in G$ is the identity and so H is cyclic.

So we may suppose that H is not trivial. Let m be the smallest positive integer such that $a^m \in H$. We will prove that H is generated by a^m and is hence cyclic. Let x be an arbitrary element of H. Then $x \in G$ and so there exists i such $a^i = x$. By the Division Algorithm (Theorem 7.1), we can write $i = mq + r$ for some positive integers q and r such that $0 \leq r \leq m-1$. Then

$$a^r = a^{i-mq} = a^i(a^m)^{-q} \in H.$$

But $r < m$ and m is the least power of a belonging to H, and so $r = 0$. Thus $a^i(a^m)^{-q} = a^0 = e$ and so $a^i = (a^m)^q$, which is a power of a^m, as required. □

Example 13.11. We can use Theorem 13.10 to list all the subgroups of a finite cyclic subgroup. For example, we know that $\mathbb{Z}_{12}$ under addition modulo 12 is a cyclic group and so every one of its subgroup is cyclic also. Hence if we list the subgroups generated by each element, then we will have a list of all the subgroups. Some subgroups can be generated by different elements and so they will show up more than once. So

$$\langle\, 0 \,\rangle = \{0\},\quad \langle\, 1 \,\rangle = \mathbb{Z}_{12} = \langle\, 5 \,\rangle = \langle\, 7 \,\rangle = \langle\, 11 \,\rangle,\quad \langle\, 2 \,\rangle = \{0, 2, 4, 6, 8, 10\} = \langle\, 10 \,\rangle,$$
$$\langle\, 3 \,\rangle = \{0, 3, 6, 9\} = \langle\, 9 \,\rangle,\quad \langle\, 4 \,\rangle = \{0, 4, 8\} = \langle\, 8 \,\rangle,\quad \langle\, 6 \,\rangle = \{0, 6\}.$$

14. Alternating groups

We are now going to introduce an important subgroup of the symmetric group S_n.

Theorem 14.1. *Every permutation can be written as a product of 2-cycles (also called transpositions).*

Proof. Let $f \in S_n$ be arbitrary. From Theorem 9.3, we know that a permutation can be written as a product of disjoint cycles. So we may assume without loss of generality that f is a cycle, i.e. $f = (i_1\ i_2 \ldots\ i_k)$. But

$$(i_1\ i_2\ \ldots\ i_k) = (i_{k-1}\ i_k)\ldots(i_2\ i_3)(i_1\ i_2),$$

which proves the theorem. □

A decomposition of a permutation into a product of transpositions is by no means unique; for instance

$$(2\ 3) = (1\ 2)(2\ 3)(1\ 3).$$

However, the parity of the number (if it is odd or even) of transpositions in any decomposition of a given permutation does not change.

Definition 14.2. A permutation is *even* if it can be written as a product of an even number of transpositions.

A permutation is *odd* if it can be written as a product of an odd number of transpositions.

Example 14.3. Let's consider S_3. The elements of S_3 are:

$$(),\quad (1\ 2),\quad (1\ 3),\quad (2\ 3),\quad (1\ 2\ 3),\quad (1\ 3\ 2).$$

If we write each element as a product of transpositions, then we can say if they are odd or even:

$$() = (1\ 2)(1\ 2),\quad (1\ 2),\quad (1\ 3),\quad (2\ 3),\quad (1\ 2\ 3) = (2\ 3)(1\ 2),\quad (1\ 3\ 2) = (3\ 2)(1\ 3).$$

So the elements of S_3 are even, odd, odd, odd, even, and even, respectively.

Corollary 14.4. *Let k be a positive integer. Then the following hold:*

(i) *if k is an odd number, then every k-cycle is an even permutation;*
(ii) *if k is an even number, then every k-cycle is an odd permutation.*

Proof. **(i).** Let $f \in S_n$ be a k-cycle where k is odd. Then

$$f = (i_1\ i_2 \dots i_k) = (i_{k-1}\ i_k)(i_{k-2}\ i_{k-1}) \cdot (i_2\ i_1)$$

for some $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$. Since there are $k-1$ transpositions in the above product, it follows that f is even.

(ii). This is analogous to part (i). □

Theorem 14.5. *A permutation cannot be both even and odd.*

Proof. Let P be the n variable polynomial defined by:

$$P = P(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

For example, if $n = 3$, then

$$P(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

and

$$P(a, b, c) = (a - b)(a - c)(b - c).$$

If $\sigma \in S_n$ is any permutation on $\{1, 2, \dots, n\}$, then we define

$$(P)\sigma = P(x_{(1)\sigma}, \dots, x_{(n)\sigma}).$$

For example, if $n = 3$ and $\sigma = (1\ 2\ 3)$, then

$$\begin{aligned} (P)\sigma &= P(x_{1\sigma}, x_{2\sigma}, x_{3\sigma}) = P(x_2, x_3, x_1) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) \\ &= -(x_1 - x_2) \cdot -(x_1 - x_3) \cdot (x_2 - x_3) = P(x_1, x_2, x_3). \end{aligned}$$

Another example, if $n = 3$ and $\sigma = (2\ 3)$, then

$$\begin{aligned} (P)\sigma &= P(x_{1\sigma}, x_{2\sigma}, x_{3\sigma}) = P(x_1, x_3, x_2) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) \\ &= -P(x_1, x_2, x_3). \end{aligned}$$

Note that

$$(P)(\sigma\tau) = P(x_{1\sigma\tau}, x_{2\sigma\tau}, \dots, x_{n\sigma\tau}) = P = (x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})\tau = ((P)\sigma)\tau.$$

For example, if $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$, then

$$P(\sigma\tau) = P((1\ 2\ 3)(1\ 2)) = P((2\ 3)) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2)$$

and

$$(P\sigma)\tau = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1)\tau = (x_{2\tau} - x_{3\tau})(x_{2\tau} - x_{1\tau})(x_{3\tau} - x_{1\tau}) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2).$$

Also note that if $\gamma = (k\ l)$ $(k < l)$ is a transposition, then it is possible to prove that

$$(P)\gamma = -P.$$

Using the fact that the only factors from P that change sign in $(P)\gamma$ are $(x_k - x_l)$, $(x_k - x_i)$ and $(x_i - x_l)$where $k < i < l$ and there is an odd number of them $(2(l - k - 1) + 1 = 2(l - k) - 1)$.

It follows from the above that if a permutation σ is even, then $\sigma = \gamma_1 \cdots \gamma_{2k}$ for some k and so

$$(P)\sigma = (P)\gamma_1 \cdots \gamma_{2k} = (-1)^{2k} P = P.$$

Similarly, if σ is odd, then $\sigma = \gamma_1 \cdots \gamma_{2k+1}$ for some k and so

$$(P)\sigma = (P)\gamma_1 \cdots \gamma_{2k+1} = (-1)^{2k+1} P = -P.$$

Since $-P \neq P$, it follows that a permutation is either even or odd but that it cannot be both. □

Corollary 14.6. *The composition of an odd and an even permutation is odd, the composition of an odd permutation and an odd permutation or an even permutation and an even permutation is even.*

Theorem 14.7. *Let $A_n = \{ f \in S_n : f \text{ is even} \}$. Then A_n is a subgroup of S_n and $|A_n| = n!/2$.*

Proof. We start by checking that A_n is a subgroup. We verify the Subgroup Criterion from Theorem 12.5:

Closure.: Let $\sigma, \tau \in A_n$. Then there exist transpositions $\gamma_1, \gamma_2, \ldots, \gamma_{2k}, \delta_1, \delta_2, \ldots, \delta_{2l}, \in S_n$ such that $\sigma = \gamma_1\gamma_2 \cdots \gamma_{2k}$ and $\tau = \delta_1 \ldots \delta_{2l} \in A_n$. Hence

$$\sigma\tau = \gamma_1 \ldots \gamma_{2k}\delta_1 \ldots \delta_{2l} \in A_n$$

Inverses.: If $\sigma \in A_n$, then $\sigma = \gamma_1\gamma_2 \cdots \gamma_{2k}$ as above. Hence

$$\sigma^{-1} = \gamma_{2k}^{-1} \ldots \gamma_1^{-1} = \gamma_{2k} \ldots \gamma_1 \in A_n.$$

Hence A_n is a subgroup of S_n.

Let O_n be the set of all odd permutations of S_n. Then clearly $S_n = A_n \cup O_n$ and $A_n \cap O_n = \varnothing$ by Theorem 14.5. We define a function $\Psi : S_n \longrightarrow S_n$ by $(\sigma)\Psi = \sigma(1\ 2)$. We will show that Ψ is a bijection.

Surjective: Let $\sigma \in S_n$ be arbitrary. Then

$$\sigma = \sigma(1\ 2)(1\ 2) = (\sigma(1\ 2))\Psi$$

and so Ψ is surjective.

Injective: Let $\sigma_1, \sigma_2 \in S_n$. Then

$$(\sigma_1)\Psi = (\sigma_2)\Psi \Rightarrow \sigma_1(1\ 2) = \sigma_2(1\ 2) \Rightarrow \sigma_1 = \sigma_2$$

and so Ψ is injective.

Hence Ψ is a bijection.

If $\sigma \in A_n$, then $\sigma = \gamma_1\gamma_2 \cdots \gamma_{2k}$ for some transpositions $\gamma_1, \gamma_2, \ldots, \gamma_{2k} \in S_n$. Hence $(\sigma)\Psi = \sigma(1\ 2) = \gamma_1\gamma_2 \cdots \gamma_{2k}(1\ 2) \in O_n$ is odd. Likewise, if $\sigma \in O_n$, then $(\sigma)\Psi \in A_n$. In other words, Ψ maps A_n into O_n and O_n into A_n. Therefore $(A_n)\Psi^2 \subseteq (O_n)\Psi \subseteq A_n$. But Ψ is a bijection and so Ψ^2 is a bijection, and A_n is finite, thus $(A_n)\Psi^2 = (O_n)\Psi = A_n$. We conclude that Ψ is a bijection between A_n and O_n, so that $|A_n| = |O_n|$. It follows that $n! = |S_n| = |A_n| + |O_n| = 2|A_n|$, and hence $|A_n| = n!/2$. □

Definition 14.8. A_n is called the *alternating group* on $\{1, \ldots, n\}$.

Example 14.9. The 15-puzzle (see Figure 9) was invented by S. Loyd, who offered $1000 for a sequence of moves swapping 14 and 15.

Any arrangement of the tiles can be interpreted as a permutation of numbers $1, \ldots, 16$, with 16 denoting the empty tile. Every move of the puzzle is a transposition of the empty tile 16 and a number in $\{1, 2, \ldots, 15\}$.

We also refer to the positions in the puzzle as pairs (i, j) where i is the row of the tile and j is the column of the tile starting with $(1, 1)$ for the empty tile. We define the *taxicab distance* between the position (i, j) and $(1, 1)$ to be $(j - 1) + (i - 1)$.

Every move of the puzzle changes the parity of the permutation describing the arrangement of the puzzle and the parity of the taxicab distance from the position of the empty tile to $(1, 1)$. In particular, the permutation describing the arrangement of the puzzle is even if and only if the taxicab distance from the empty tile to $(1, 1)$ is an even number.

Since the empty tile should begin and end in position $(1, 1)$, it follows that the taxicab distance from the empty tile to $(1, 1)$ is 0 and so the permutation describing the arrangement of the puzzle must also be even. In other words, we can produce only even permutations of the tiles. The permutation (14 15) is odd, so that the desired sequence of moves does not exist.

Example 14.10. Every basic rotation of Rubik cube is a product of two 4-cycles (see Example 11.14), and hence is even. Every sequence of moves is a product of these basic rotations, and hence also must be even. Therefore, there is no sequence of moves which swaps two cubicles, and leaves all the others in their places.

15. Cosets and Lagrange's Theorem

Every subgroup of a group G induces an important decomposition of G.

Definition 15.1. Let G be a group, let H be a subgroup of G, and let $a \in G$ be any element. Then the *left coset* of H in G determined by a is the set

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

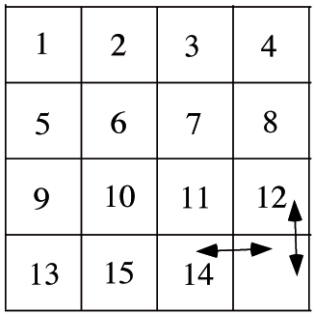

FIGURE 9. The 15-puzzle

The *right coset* of H in G determined by a is the set

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

Example 15.2. The left and right cosets of the cyclic subgroup $H = \{\mathrm{id}, (1\ 2)\} = \langle\, (1\ 2)\,\rangle$ of the symmetric group S_3 are:

$$\begin{array}{ll}
L_1 = \mathrm{id}H = \{\mathrm{id}, (1\ 2)\} & R_1 = H\mathrm{id} = \{\mathrm{id}, (1\ 2)\}, \\
L_2 = (1\ 2)H = \{(1\ 2), \mathrm{id}\} & R_2 = H(1\ 2) = \{(1\ 2), \mathrm{id}\}, \\
L_3 = (1\ 3)H = \{(1\ 3), (1\ 3\ 2)\} & R_3 = H(1\ 3) = \{(1\ 3), (1\ 2\ 3)\}, \\
L_4 = (2\ 3)H = \{(2\ 3), (1\ 2\ 3)\} & R_4 = H(2\ 3) = \{(2\ 3), (1\ 3\ 2)\}, \\
L_5 = (1\ 2\ 3)H = \{(1\ 2\ 3), (2\ 3)\} & R_5 = H(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3)\}, \\
L_6 = (1\ 3\ 2)H = \{(1\ 3\ 2), (1\ 3)\} & R_6 = H(1\ 3\ 2) = \{(1\ 3\ 2), (2\ 3)\}.
\end{array}$$

Example 15.2 shows that the left and the right coset determined by the same element are not always equal. However, if H is a subgroup of an abelian group G, then

$$aH = \{\, ah \ :\ h \in H \,\} = \{\, ha \ :\ h \in H \,\} = Ha$$

for all $a \in G$, and so the left and right coset determined by a are equal.

Example 15.3. The cosets of the trivial subgroup $\{e\}$ in any group G are:

$$g\{e\} = \{g\}$$

for all $g \in G$.

Let G be any group. Then G is a subgroup of G and so the cosets of G are:

$$gG = G$$

for all $g \in G$. In other words, G has only one coset in G, namely, G.

We may also notice some interesting regularities: all the cosets have equal sizes; some of them are equal (e.g. $L_3 = L_5$), and the others are disjoint (e.g. $L_3 \cap L_6 = \varnothing$). This is not a coincidence.

Theorem 15.4. *Let G be a group, and let H be a subgroup of G. Then the following hold:*

(i) *H is a left coset of itself;*
(ii) *$a \in aH$ for all $a \in G$;*
(Every element belongs to the left coset determined by it.)
(iii) *$G = \bigcup_{a \in G} aH$.*
(G is the union of the left cosets of H.)
(iv) *If $a, b \in G$, then either $aH = bH$, or $aH \cap bH = \varnothing$.*
(Cosets of H are either equal or disjoint.)
(v) *$|aH| = |H|$ for all $a \in G$.*
(All the left cosets of H have equal size.)

Analogous statements hold for right cosets.

Proof. **(i).** $H = eH$.

(ii). $a = ae \in aH$, since $e \in H$.

(iii). Clearly $aH \subseteq G$ for every $a \in G$ because G is closed under multiplication. Therefore $\bigcup_{a\in G} aH \subseteq G$. Conversely, since $b \in bH$ by (ii), it follows that $b \in bH \subseteq \bigcup_{a\in G} aH$ for all $b \in G$. Hence $G \subseteq \bigcup_{a\in G} aH$. It follows that $G = \bigcup_{a\in G} aH$.

(iv). Assume that $aH \cap bH \neq \varnothing$. We are going to prove that $aH = bH$. Then there exists $x \in aH \cap bH$ and so $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Hence $a = xh_1^{-1}$.

Let $y = ah \in aH$ be arbitrary. Then we may write

$$y = ah = xh_1^{-1}h = bh_2h_1^{-1}h.$$

Since $h, h_1, h_2 \in H$, it follows that $h_2h_1^{-1}h \in H$ and so $y \in bH$. We have shown that $aH \subseteq bH$, and the reverse inclusion can be proved by a similar argument.

(v). Let $f : H \longrightarrow aH$ be defined by $(x)f = ax$. We will show that f is a bijection. Let $x, y \in H$ such that $(x)f = (y)f$. Then $ax = ay$ and so $x = y$. Hence f is injective. If $ah \in aH$ is arbitrary, then $(h)f = ah$ and so f is surjective. It follows that f is a bijection and so $|H| = |aH|$. □

Theorem 15.5 (Lagrange)**.** *Let G be a group of finite order and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof. Let $C_1, \ldots, C_k$ be the distinct cosets of H. Then, by Theorem 15.4(v), $|C_1| = \ldots = |C_k| = |H|$. Also, by Theorem 15.4(iii), $G = \bigcup_{i=1}^{k} C_i$ and, by Theorem 15.4(iv), $C_i \cap C_j = \varnothing$ if $i \neq j$. Hence

$$|G| = |C_1| + \cdots + |C_k| = \underbrace{|H| + \cdots + |H|}_{k} = k|H|,$$

and the theorem follows. □

Corollary 15.6. *Let G be a group of finite order and let H be a subgroup of G. Then the number of (left or right) cosets of H in G is $|G|/|H|$.*

Example 15.7. The left and right cosets of the subgroup $H = \{0, 3, 6, 9\} = \langle\, 3 \,\rangle$ in $\mathbb{Z}_{12}$ are:

$$\begin{aligned} 0 + H &= \{0, 3, 6, 9\} = 3 + H = 6 + H = 9 + H \\ 1 + H &= \{1, 4, 7, 10\} = 4 + H = 7 + H = 10 + H \\ 2 + H &= \{2, 5, 8, 11\} = 5 + H = 8 + H = 11 + H \end{aligned}$$

Example 15.8. The left and right cosets of the cyclic subgroup $H = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ of S_3 are:

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

Example 15.9. Consider the cyclic subgroup $H = \langle\, 2 \,\rangle = \{0, 2, 4, 6, 8, 10\}$ of $\mathbb{Z}_{12}$ under addition modulo 12. How many cosets does H have in $\mathbb{Z}_{12}$? From Corollary 15.6, there are $|\mathbb{Z}_{12}|/|H| = 12/6 = 2$ cosets.

If a subgroup K of $\mathbb{Z}_{12}$ has 3 cosets, then what is $|K|$? Again from Corollary 15.6, $|\mathbb{Z}_{12}|/|K| = 3$ is the number of cosets and so $|K| = 12/3 = 4$.

How many subgroup of order 7 does $\mathbb{Z}_{12}$ have? None, by Lagrange's Theorem the order of a subgroup must divide the order of the group, but 7 does not divide 12.

Definition 15.10. The number of (left or right) cosets of a subgroup H in a group G is called the *index* of H in G and is written $[G : H]$.

So, the index of H (from Example 15.8) in S_3 is 2, and the index of H (from Example 15.7) in $\mathbb{Z}_{12}$ is 3.

Theorem 15.11. *Let G be a finite group, and let $a \in G$ be arbitrary. Then the order of a divides the order of G.*

Proof. By Corollary 13.7, the order $|a|$ of a is equal to the order of the cyclic subgroup $\langle\, a \,\rangle$ of G generated by a. By Theorem 15.5, the order of $\langle\, a \,\rangle$ divides the order of G. Hence $|a|$ divides the order of G. □

We give an interesting application.

Theorem 15.12. *Every group of prime order is cyclic.*

Proof. Let G be a group of prime order p, and let $a \in G$ be any non-identity element. Let n denote the order of a in G. Then since a is not the identity, it follows that $n \neq 1$. By Theorem 15.11, n divides the order of G which is p. But p is prime and so $n = p$. It follows that G is cyclic generated by a. □

16. Homomorphisms of groups

In this section, we will study functions from one group to another that preserve group structure.

Definition 16.1. Let G and H be groups with operations $*$ and $\bullet$ respectively. A function $f : G \longrightarrow H$ is called a *homomorphism* if $(x * y)f = (x)f \bullet (y)f$ for all $x, y \in G$.

If the operation in both groups is denoted as multiplication, then the above rule becomes $(xy)f = (x)f\ (y)f$. (The image of the product is the product of images.)

Example 16.2. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be defined by $(x)f = x \pmod n$. Then

$$(xy)f = xy \pmod n = (x \pmod n \cdot y \pmod n) = (x)f \cdot (y)f$$

for all $x, y \in \mathbb{Z}$ and so f is a homomorphism.

Example 16.3. Let G and H be groups and let $f : G \longrightarrow H$ be defined by $f(x) = e_H$ (the identity of H). Then

$$(xy)f = e_H = e_H e_H = (x)f \cdot (y)f$$

for all $x, y \in G$ and so f is a homomorphism.

Example 16.4. If G is any group, then the identity function $\mathrm{id} : G \longrightarrow G$ is a homomorphism since

$$(xy)\mathrm{id} = xy = (x)\mathrm{id} \cdot (y)\mathrm{id}$$

for all $x, y \in G$.

Example 16.5. Let $GL(n, \mathbb{R})$ denote the group of $n \times n$ matrices with entries in $\mathbb{R}$ and non-zero determinant under the usual matrix multiplication and let $\mathbb{R} \setminus \{0\}$ denote the real numbers under multiplication. If $f : GL(n, \mathbb{R}) \longrightarrow \mathbb{R} \setminus \{0\}$ is defined by $(A)f = \det(A)$, then

$$(AB)f = \det(AB) = \det(A) \cdot \det(B) = (A)f \cdot (B)f$$

for all $A, B \in GL(n, \mathbb{R})$ and so f is a homomorphism.

Example 16.6. Let $f : S_n \longrightarrow \mathbb{Z}_2$ be defined by

$$(\sigma)f = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Even and odd permutations multiply according to the rules

	even	odd
even	even	odd
odd	odd	even.

Therefore, if $\sigma, \tau \in S_n$, then

$$(\sigma\tau)f = \begin{cases} 0 & \sigma \text{ even, } \tau \text{ even} \\ 0 & \sigma \text{ odd, } \tau \text{ odd} \\ 1 & \sigma \text{ even, } \tau \text{ odd} \\ 1 & \sigma \text{ odd, } \tau \text{ even.} \end{cases} = (\sigma)f + (\tau)f.$$

Next, we derive some basic properties of homomorphisms.

Theorem 16.7. *Let G and H be groups with identities e_G and e_H, respectively. If $f : G \longrightarrow H$ is a homomorphism, then*

(i) $(e_G)f = e_H$ *(homomorphisms map the identity to the identity);*

(ii) $\big((a)f\big)^{-1} = (a^{-1})f$ *for all $a \in G$ (homomorphisms map inverses to inverses).*

Proof. **(i).** Let $x \in G$ be arbitrary. Then, since $xe_G = x$ and f is a homomorphism, it follows that $(x)f = (xe_G)f = (x)f \cdot (e_G)f$. Cancelling $(x)f$ (in H!) we obtain $(e_G)f = e_H$.

(ii). From

$$(a)f \cdot (a^{-1})f = (aa^{-1})f = (e_G)f = e_H,$$

and the uniqueness of inverses, it follows that $(a^{-1})f = \big((a)f\big)^{-1}$. □

We also note that there are certain natural subgroups related to homomorphisms.

Definition 16.8. Let G and H be groups, let e_H be the identity of H, and let $f : G \longrightarrow H$ be a homomorphism. Then the set

$$\ker(f) = \{\, x \in G \,:\, (x)f = e_H \,\}$$

is called the *kernel* of f. Also if $X \subseteq G$, then we write

$$(X)f = \{(x)f : x \in X\}$$

to denote the image of X under f. The set $(G)f$ is also denoted by $\operatorname{im}(f)$ and is called the *image* of f.

Example 16.9. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be the homomorphism defined by $(x)f = x \pmod n$ from Example 16.2. Then

$$m \in \ker(f) \iff (m)f = 0 \iff m = 0 \pmod n \iff n|m,$$

and hence $\ker(f) = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ consists of all integer multiples of n. The image of f is the whole $\mathbb{Z}_n$ (i.e. f is onto).

Example 16.10. Let $f : S_n \longrightarrow \mathbb{Z}_2$ be the homomorphism defined by

$$(\sigma)f = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

from Example 16.6. Since the identity of $\mathbb{Z}_2$ is 0, it follows that

$$\ker(f) = \{\, \sigma \in S_n \,:\, (\sigma)f = 0 \,\} = \{\, \sigma \in S_n \,:\, \sigma \text{ is even} \,\} = A_n.$$

Also since S_n $(n \geq 1)$ contains both odd and even permutations, it follows that $\operatorname{im}(f) = \mathbb{Z}_2$.

Definition 16.11. Let G and H be groups and let $f : G \longrightarrow H$ be a homomorphism. If $Y \subseteq H$, then the *inverse image* of Y is defined to be:

$$(Y)f^{-1} = \{\, x \in G \,:\, (x)f \in Y \,\}.$$

Theorem 16.12. *Let $f : G \longrightarrow H$ be a homomorphism of groups. Then the following hold:*

(i) $\ker(f)$ *is a subgroup of* G*;*
(ii) $\ker(f) = (e_H)f^{-1}$ *where* e_H *is the identity of* H*;*
(iii) if K *is a subgroup of* G*, then the image* $(K)f$ *is a subgroup of* H*;*
(iv) if M *is a subgroup of* H*, then the inverse image* $(M)f^{-1}$ *is a subgroup of* G*.*

Proof. **(i).** Let $a, b \in \ker(f)$. Then $(a)f = (b)f = e_H$ by the definition of $\ker(f)$. We verify that $\ker(f)$ satisfies the Subgroup Criteria:

Closure: $(ab)f = (a)f(b)f = e_He_H = e_H$ and so $ab \in \ker(f)$;
Inverses: $(a^{-1})f = \big((a)f\big)^{-1} = e_H^{-1} = e_H$ and so $a^{-1} \in \ker(f)$.

Thus $\ker(f)$ is closed for multiplication and inverses, and hence it is a subgroup of G.

(ii). From the definitions, $\ker(f) = \{x \in G : (x)f = e_H\} = \{x \in G : (x)f \in \{e_H\}\} = (e_H)f^{-1}$.

(iii). Let $u, v \in (K)f$. Then there exist $x, y \in K$ such that $u = (x)f$ and $v = (y)f$. Since K is a subgroup, it follows that $xy \in K$ and $x^{-1} \in K$. Again we verify the Subgroup Criteria:

Closure: $uv = (x)f(y)f = (xy)f \in (K)f$.
Inverses: $u^{-1} = \big((x)f\big)^{-1} = (x^{-1})f \in (K)f$.

Hence $(K)f \leq H$.

(iv). Let $m, n \in (M)f^{-1}$. Then $x = (m)f, y = (n)f \in M$. Again we verify that the Subgroup Criteria:

Closure: $(mn)f = (m)f(n)f = xy \in M$ and so $mn \in (M)f^{-1}$;

Inverses: $(m^{-1})f = \big((m)f\big)^{-1} = x^{-1} \in M$ and so $m^{-1} \in (M)f^{-1}$.

Hence $(M)f^{-1}$ is a subgroup of G. □

Theorem 16.13. *Let G and H be groups and let $f : G \longrightarrow H$ be a homomorphism. Then f is injective (one-one) if and only if* $\ker(f) = \{e_G\}$.

Proof. ($\Rightarrow$) It follows from Theorem 16.12(i) that $e_G \in \ker(f)$. Let $x \in \ker(f)$. Then $(x)f = (e_G)f = e_H$ by the definition of $\ker(f)$. But f is injective and so $x = e_G$. Hence $\ker(f) = \{e_G\}$.

($\Leftarrow$) Let $x, y \in G$ be such that $(x)f = (y)f$. Then $(x)f\big((y)f\big)^{-1} = e_H$ and so $(xy^{-1})f = (x)f(y^{-1})f = (x)f\big((y)f\big)^{-1} \in \ker(f)$. From the assumption that $\ker(f) = \{e_G\}$, it follows that $xy^{-1} = e_G$. But then $x = y$ and so f is injective. □

17. Isomorphisms

Let's compare the groups $\mathbb{Z}_3$ under addition modulo 3 and the cyclic subgroup H of S_3 generated by (1 2 3). The multiplication tables of these groups are:

$+$ (mod 3)	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\circ$	id	(1 2 3)	(1 3 2)
id	id	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	id	(1 2 3)

The two tables differ only in the names of the symbols, but not in their positions. More formally, there is function $f : \mathbb{Z}_3 \longrightarrow H$ (namely $(0)f = \text{id}$, $(1)f = (1\ 2\ 3)$, $(2)f = (1\ 3\ 2)$) which is a bijection and satisfies $(i + j)f = (i)f \circ (j)f$.

Definition 17.1. Let G and H be groups. A function $f : G \longrightarrow H$ is an *isomorphism* if it is a bijection and a homomorphism. We say that G and H are *isomorphic* if there is an isomorphism $f : G \longrightarrow H$; this is denoted $G \cong H$.

Example 17.2. The Klein 4-group K_4 (defined in Example 5.1) has elements $\{e, a, b, c\}$ and multiplication defined by:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The group $U_8 = \{1, 3, 5, 7\}$ under multiplication modulo 8 has multiplication table:

$\cdot$ (mod 8)	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The function $f : K_4 \longrightarrow U_8$ defined by

$$f = \begin{pmatrix} e & a & b & c \\ 1 & 3 & 5 & 7 \end{pmatrix}$$

is an isomorphism (verify that the 16 equalities $(xy)f = (x)f(y)f$ hold) and so $K_4 \cong U_8$.

Theorem 17.3. *Let G, H and K be groups. Then:*

(i) $G \cong G$;
(ii) if $G \cong H$, *then* $H \cong G$;
(iii) if $G \cong H$ *and* $H \cong K$, *then* $G \cong K$.

Proof. **(i).** The identity function on G is an isomorphism.

(ii). If $f : G \longrightarrow H$ is an isomorphism, then so is $f^{-1} : H \longrightarrow G$.

(iii). If $f : G \longrightarrow H$ and $g : H \longrightarrow K$ are isomorphisms, then so is their composition $f \circ g : G \longrightarrow K$. □

If we are only interested in group theoretic properties, then it makes sense to regard isomorphic groups as the same. The main general task of group theory can be formulated as: classify all non-isomorphic groups. In general this is impossible, and one has to settle for various partial results in this direction. Probably the easiest such is the following theorem.

Theorem 17.4. *Let G be a cyclic group. Then the following hold:*

(i) if G is infinite, then $G \cong \mathbb{Z}$;
(ii) if G is finite and the order of G is n, then $G \cong \mathbb{Z}_n$.

Proof. Since G is cyclic, there exists $a \in G$ such that $G = \{ a^i : i \in \mathbb{Z} \}$.

(i). Since G is infinite, all powers of a are distinct (by Theorem 11.7). Let $f : \mathbb{Z} \longrightarrow G$ be defined by $(i)f = a^i$. Then f is **surjective** since $\operatorname{im}(f) = \{ a^i : i \in \mathbb{Z} \} = G$. If $i, j \in \mathbb{Z}$ such that $(i)f = (j)f$, then $a^i = a^j$ and so $i = j$. Hence f is **injective**. If $i, j \in \mathbb{Z}$, then

$$(i + j)f = a^{i+j} = a^i a^j = (i)f \cdot (j)f$$

and so f is a **homomorphism**. Hence f is an isomorphism.

(ii). Since G has order n, it follows that $G = \{e, a, \ldots, a^{n-1}\}$ by Theorem 11.7. Let $f : \mathbb{Z}_n \longrightarrow G$ be defined by $(i)f = a^i$. It is possible to verify that f is an isomorphism using a similar argument to (i). □

Corollary 17.5. *Every group of prime order p is isomorphic to the additive group $\mathbb{Z}_p$.*

Proof. Every group of prime order is cyclic (Theorem 15.12). Hence by the previous theorem, $G \cong \mathbb{Z}_p$. □

In order to prove that two groups G and H are not isomorphic, you should demonstrate that there is no isomorphism from G onto H. Usually, in practice, this is much easier than it sounds, and is accomplished by finding a property that holds in one group, but not in the other.

Example 17.6. The groups $\mathbb{Z}_4$ and $\mathbb{Z}_6$ are not isomorphic because they have different orders.

Example 17.7. $\mathbb{Z}_6 \ncong S_3$ because $\mathbb{Z}_6$ is abelian and S_3 is not (although they both have order 6).

Example 17.8. The dihedral group D_{12} is not isomorphic to S_4 because D_{12} has 13 elements of order 2 (12 reflections, and the rotation for 180°), while S_4 has only 9 such elements (transpositions, and products of two disjoint transpositions). (Note that $|D_{12}| = |S_4| = 24$ and that they are both non-abelian.)

Example 17.9. Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, with multiplication naturally extending the rules

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

The full Cayley table is

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

.

The group Q_8 is called the *quaternion group*. We will show that Q_8 is not isomorphic to $\mathbb{Z}_8$ (under addition modulo 8) or the dihedral group D_4.

The orders of the elements in Q_8 are:

x	1	-1	i	$-i$	j	$-j$	k	$-k$
$\lvert x\rvert$	1	2	4	4	4	4	4	4

Since $\mathbb{Z}_8$ is cyclic, it must contain an element of order 8 and so Q_8 and $\mathbb{Z}_8$ are not isomorphic.

The orders of the elements of $D_4 = \{\mathrm{id}, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ are:

x	id	ρ	ρ^2	ρ^3	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
$\lvert x\rvert$	1	4	2	4	2	2	2	2

So, D_4 has 2 elements of order 4 but Q_8 has 6 elements of order 4. Hence D_4 and Q_8 are not isomorphic.

Theorem 17.10 (Cayley)**.** *Every group G is isomorphic to a subgroup of the symmetric group S_G.*

Proof. Let $a \in G$ be arbitrary. Then we will associate a permutation τ_a of the elements of G to a as follows. Let $\tau_a : G \longrightarrow G$ be defined by

$$(x)\tau_a = xa.$$

We must prove that $\tau_a \in S_G$, i.e. that τ_a is a bijection. If $g \in G$ is arbitrary, then

$$g = ga^{-1}a = (ga^{-1})\tau_a$$

and so τ_a is **surjective**. If $g, h \in G$ such that $(g)\tau_a = (h)\tau_a$, then $ga = ha$ and so, by cancelling a, it follows that $g = h$. Hence τ_a is **injective**.

Let $\Psi : G \longrightarrow S_G$ be defined by

$$(a)\Psi = \tau_a.$$

We will show that Ψ is a injective homomorphism. If $a, b \in G$ such that $(a)\Psi = (b)\Psi$, then $\tau_a = \tau_b$. So, $(g)\tau_a = (g)\tau_b$ for all $g \in G$ and so $ga = gb$, and by cancelling g, it follows that $a = b$. Thus Ψ is **injective**. Let $a, b \in G$. Then

$$(x)(\tau_a\tau_b) = ((x)\tau_a)\tau_b) = (xa)\tau_b = xab = (x)\tau_{ab}$$

for all $x \in G$. Hence the permutations $\tau_a\tau_b$ and τ_{ab} are equal. Therefore

$$(a)\Psi(b)\Psi = \tau_a\tau_b = \tau_{ab} = (ab)\Psi$$

and so Ψ is a **homomorphism**.

By Theorem 16.12(iii), $\mathrm{im}\,(\Psi) = \{\tau_a : a \in G\}$ is a subgroup of S_G and $\Psi : G \longrightarrow \mathrm{im}\,(\Psi)$ is obviously surjective. We conclude that $G \cong \mathrm{im}\,(f) \leq S(G)$. □

The permutations τ_a can be read off easily from the Cayley table of G – they correspond to its columns. Of course, if $|G| = n$, then you can rename the elements of G as numbers $1, \ldots, n$ (in an arbitrary way), and thus represent G as a subgroup of S_n.

Example 17.11. In the quaternion group Q_8, we have, for example,

$$\tau_i = \begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ i & -i & -1 & 1 & -k & k & j & -j \end{pmatrix}$$

or, after renaming,

$$\tau_i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 8 & 7 & 5 & 6 \end{pmatrix}$$

The practical use of Cayley's Theorem is limited: it is not very likely that one can obtain much useful information about groups of order, say, eight, by considering subgroups of the group S_8 of order 40320.

18. Normal subgroups

We have seen that every homomorphism $f : G \longrightarrow H$ is associated with two distinguished subgroups: $\ker(f) \leq G$ and $\mathrm{im}(f) \leq H$. It is natural to ask the converse question: given a subgroup of a group G, is this subgroup the kernel or the image of some homomorphism?

Every subgroup is the image of some homomorphism: if $H \leq G$ and we define $f : H \longrightarrow G$ by $(x)f = x$, then $\mathrm{im}(f) = H$.

The situation for kernels is different. In order to describe it, we introduce a special class of subgroups.

Theorem 18.1. *Let G be a group and let N be a subgroup of G. Then the following are equivalent:*

(i) every left coset of N is also a right coset (and vice versa);
(ii) $aN = Na$ for every $a \in G$;
(iii) $ana^{-1} \in N$ for all $a \in G$ and for all $n \in N$;
(iv) $aNa^{-1} = \{ana^{-1} : n \in N\} = N$ for all $a \in G$.

Proof. (i)⇒(ii) Let $a \in G$. Then, by part (i), there exists $b \in G$ such that $aN = Nb$. But $a \in aN = Nb$ and $a \in Na$, and so $a \in Na \cap Nb$. It follows, by Theorem 15.4(iv) (for right cosets!), that $Nb = Na$, and hence $aN = Nb = Na$, as required.

(ii)⇒(iii) Let $a \in G$ and let $n \in N$. Then by part (ii) we know that $aN = Na$. Hence $an \in aN = Na$ and so there exists $n_1 \in N$ such that $an = n_1 a$. But then

$$ana^{-1} = aa^{-1}n_1 = n_1 \in N,$$

as required.

(iii)⇒(iv) If $n \in N$ is arbitrary, then $ana^{-1} \in N$ by part (iii) and so $aNa^{-1} \subseteq N$. If $n \in N$ is arbitrary, then by part (iii) (applied to a^{-1} instead of a) it follows that $a^{-1}na = n_1 \in N$. But then

$$n = aa^{-1}naa^{-1} = an_1a^{-1} \in aNa^{-1}.$$

Hence $N = aNa^{-1}$.

(iv)⇒(i) We show that $aN \subseteq Na$ and $Na \subseteq aN$. Let $a \in G$ and $n \in N$ be arbitrary. Then, by part (iv), $ana^{-1} = n_1 \in N$. But then $an = n_1 a \in Na$. This shows that $aN \subseteq Na$. A similar argument shows the converse inclusion. Hence $aN = Na$, and so every left coset is also a right coset. □

Definition 18.2. A subgroup N of a group G is *normal* if it satisfies any (and hence all) of the conditions in Theorem 18.1; this is denoted $N \trianglelefteq G$.

Example 18.3. $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$, as left and right cosets are equal.

Example 18.4. Every subgroup of an abelian group is normal, since $aN = Na$ is satisfied.

Example 18.5. The cyclic subgroup of S_3 generated by $(1\ 2)$ is not normal in S_3 because the left and right cosets do not coincide; see Example 15.2.

Lemma 18.6. *If N is a subgroup of G with exactly two left cosets, then N is normal.*

Proof. If N has two left cosets, then these cosets are N and $G \setminus N$. Likewise, the right cosets of N are N and $G \setminus N$, and so every left coset is a right coset, and, by Theorem 18.1, $N \trianglelefteq G$. □

A corollary of the previous lemma is that $A_n \trianglelefteq S_n$; see Question 2 on Tutorial Sheet 6.

Example 18.7. Consider the quaternion group Q_8; see Example 17.9. The set $N = \{1, -1\}$ is a subgroup:

Closure: The multiplication table of N is

	1	-1
1	1	-1
-1	-1	1

and from this we see that N is closed.

Inverses: Clearly from the table $1^{-1} = 1$ and $-1^{-1} = 1$.

Note that both 1 and -1 commute with every element of Q_8 (i.e. $x * 1 = x = 1 * x$ and $-1 * x = x * -1 = -x$ for all $x \in Q_8$). Hence $aN = Na$ for every $a \in Q_8$, and N is normal.

We now return to our investigation of kernels of homomorphisms.

Theorem 18.8. *Let G and H be groups, and let $f : G \longrightarrow H$ be a homomorphism. Then* $\ker(f) \trianglelefteq G$.

Proof. We already showed that $\ker(f) \leq G$ in Theorem 16.12(i). Let $a \in G$ and $n \in \ker(f)$. From $(n)f = e_H$, it follows that

$$(a^{-1}na)f = (a^{-1})f \cdot (n)f \cdot (a)f = (af)^{-1} \cdot e_H \cdot (a)f = (af)^{-1} \cdot (a)f = e_H.$$

Hence $a^{-1}na \in \ker(f)$ for all $a \in G$ and for all $n \in \ker(f)$. Hence by Theorem 18.1(iii) it follows that $\ker(f)$ is a normal subgroup of G. □

19. Quotient groups

We now introduce a method for constructing a new group from a group and a normal subgroup. We will then use this construction to prove that a subgroup H of a group G is normal if and only if there exists a homomorphism f such that $\ker(f) = H$.

Theorem 19.1. *Let G be a group and let $N \trianglelefteq G$. Then the set*

$$G/N = \{aN : a \in G\}$$

of all cosets of N in G under the operation

$$(aN)(bN) = (ab)N$$

is a group.

Proof. We start by showing that the above multiplication is *well-defined*. The point here is that we are defining a product of two *sets*, by choosing a representative element from each, multiplying them together, and then finding the set corresponding to the product. We have to convince ourselves that the resulting set only depends on the original sets, but not on the particular choices of elements.

Let $a, a', b, b' \in G$ such that $aN = a'N$ and $bN = b'N$. We must prove that $abN = a'b'N$. Let $abn \in abN$ be arbitrary. Then since $bN = b'N$ there exists $n_1 \in N$ such that $bn = b'n_1$. Since $N \trianglelefteq G$, there exists $n_2 \in N$ such that $b'n_1 = n_2b'$. Since $aN = a_1N$, it follows that $an_2 = a'n_3$ for some $n_3 \in N$. Finally, since N is normal we have that $n_3b' = b'n_4$ for some $n_4 \in N$. Putting all this together, we obtain

$$abn = ab'n_1 = an_2b' = a'n_3b' = a'b'n_4 \in (a'b')N.$$

This shows that $(ab)N \subseteq (a'b')N$. An analogous argument shows the converse inclusion, and hence $(ab)N = (a'b')N$, as required.

Closure: By definition, the product of two cosets is another coset, and so G/N is closed.
Associativity: Let $a, b, c \in G$. Then:

$$\begin{aligned}((aN)(bN))(cN) &= ((ab)N)(cN) = ((ab)c)N = (a(bc))N = (aN)((bc)N) \\ &= (aN)((bN)(cN)).\end{aligned}$$

Identity: The identity element is $eN = N$:

$$(eN)(aN) = (ea)N = aN = (ae)N = (aN)(eN).$$

Inverses: The inverse of aN is $a^{-1}N$ since

$$(aN)(a^{-1}N) = (aa^{-1})N = eN = (a^{-1}a)N = (a^{-1}N)(aN).$$

□

Example 19.2. Let Q_8 denote the quaternion group defined in Example 17.9 by the multiplication table:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1.

We showed in Example 18.7 that $N = \{1, -1\}$ is a normal subgroup of Q_8. We are going to describe the quotient Q_8/N. The cosets of N in Q_8 are:

$$E = 1N = (-1)N = \{1, -1\}, \qquad I = iN = (-i)N = \{i, -i\}$$

$$J = jN = (-j)N = \{j, -j\}, \qquad K = kN = (-k)N = \{k, -k\}.$$

From the multiplication defined in Theorem 19.1, we obtain the multiplication table of Q_8/N:

	E	I	J	K
E	E	I	J	K
I	I	E	K	J
J	J	K	E	I
K	K	J	I	E

We see that $Q_8/N \cong K_4$, the Klein four group from Example 5.1. (Note that Q_8/N is abelian, although Q_8 is not.)

Example 19.3. We will describe S_n/A_n as we described Q_8/N in the last example. We saw earlier that A_n is a normal subgroup of S_n. The cosets of A_n in S_n are just A_n and $S_n \setminus A_n$. Hence the multiplication table of S_n/A_n is:

	A_n	$S_n \setminus A_n$
A_n	A_n	$S_n \setminus A_n$
S_n	$S_n \setminus A_n$	A_n

Since every group of prime order is cyclic (Theorem 15.12) and every finite cyclic group is isomorphic to $\mathbb{Z}_n$ under addition modulo n (Theorem 17.4), it follows that $S_n/A_n \cong \mathbb{Z}_2$.

We return to the kernels of homomorphisms.

Theorem 19.4. *Let G be a group, and let $N \trianglelefteq G$. Then the function $f : G \longrightarrow G/N$ defined by $(x)f = xN$ is a homomorphism and $\ker(f) = N$.*

Proof. We must check that f is a homomorphism and the $\ker(f) = N$.

Homomorphism: Let $x, y \in G$ be arbitrary. Then

$$(xy)f = (xy)N = (xN)(yN) = (x)f(y)f.$$

Kernel: Let $x \in G$ such that $x \in \ker(f)$. Then $(x)f = xN = N$ by the definition of the kernel. Hence $x \in xN = N$ (by Theorem 15.4(ii)) and so $\ker(f) \subseteq N$. Conversely, if $x \in N$, then $(x)f = xN = N$ and so $x \in \ker(f)$. Thus $N \subseteq \ker(f)$ and so $N = \ker(f)$.

□

20. The first isomorphism theorem

Theorem 20.1 (The First Isomorphism Theorem)**.** *If $f : G \longrightarrow H$ is a homomorphism, then*

$$G/\ker(f) \cong \operatorname{im}(f).$$

Proof. For brevity denote $\ker(f)$ by N, and $\operatorname{im}(f)$ by K. Define a function $\phi : G/N \longrightarrow K$ by $(aN)\phi = (a)f$.

Again we have to prove that this function is well defined. To this end assume that $aN = a_1N$. In particular, $a = a_1n$ for some $n \in N$. But then

$$(aN)\phi = (a)f = (a_1n)f = (a_1)f(n)f = (a_1)fe_H = (a_1)f = (a_1N)\phi.$$

If $y \in K$ is arbitrary, then there exists $x \in G$ such that $(x)f = y$. But then $(xN)\phi = (x)f = y$; hence ϕ is onto. To prove that ϕ is one-one as well, let $aN, bN \in G/N$ be such that $(aN)\phi = (bN)\phi$. This means that $(a)f = (b)f$, and, since f is a homomorphism, we obtain $(a^{-1}b)f = e_H$. This in turn implies $a^{-1}b \in \ker(f) = N$. Write $a^{-1}b = n \in N$, so that $b = an \in aN$. Now we have $b \in aN \cap bN$, which implies $aN = bN$.

Finally, we have

$$((aN)(bN))\phi = ((ab)N)\phi = (ab)f = (a)f(b)f = (aN)\phi(bN)\phi.$$

This completes the proof that ϕ is an isomorphism. □

The importance of the first isomorphism theorem is that one may consider quotients without working with cosets.

Example 20.2. The normal subgroup $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ of $\mathbb{Z}$ is the kernel of the homomorphism $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $(a)f = a \pmod{n}$; see Examples 16.2 and 16.9. Therefore, we have

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(f) \cong \mathrm{im}(f) = \mathbb{Z}_n.$$

References

@bookPolya1988aa, Address = Princeton, NJ, Author = Pólya, G., Edition = second, Publisher = Princeton University Press, Series = Princeton Science Library, Title = How to solve it, Year = 1988