

Chapter 2.

Subgroups, homomorphisms, quotients

3. Subgroups

Definition 3.1. Let G be a group and H a subset of G . If H is itself a group under the multiplication in G then H is said to be a *subgroup* of G ; this is denoted by $H \leq G$.

Remark 3.2. If H, K are subgroups of G with $H \subseteq K$ then H is actually a subgroup of K , i.e. $H \leq K$. To show this pictorially, we use lattice diagrams (draw one in lecture!).

Example 3.3. For an arbitrary group G , the sets $\{e\}$ and G are subgroups of G . The former is called the *trivial (sub)group*. A subgroup H of a group G is *proper* if $\{e\} \neq H \neq G$.

Example 3.4. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

According to our definition, in order to check that a subset is a subgroup, we have to check four conditions. Actually, the number of conditions that one has to check can be reduced to one, as the following theorem shows.

Theorem 3.5. *The following three conditions are equivalent for a non-empty subset H of a group G :*

- (i) H is a subgroup of G ;
- (ii) for any two $x, y \in H$ we have $xy \in H$ and $x^{-1} \in H$;
- (iii) for any two $x, y \in H$ we have $xy^{-1} \in H$.

Proof. (i) \Rightarrow (ii) follows directly from the definition of a subgroup, while (ii) \Rightarrow (iii) is obvious.

(iii) \Rightarrow (i) Choose an arbitrary $a \in H$ and put $x = y = a$ in (iii). We obtain $e = aa^{-1} \in H$, so that H contains the identity. Next, put $x = e$ and $y = a$ to obtain $a^{-1} \in H$. Therefore, H is closed for taking inverses. Finally, for arbitrary two $a, b \in H$ put $x = a$ and $y = b^{-1}$, to obtain $ab \in H$ and conclude that H is closed for multiplication. Since multiplication is associative in G it is associative in H as well, and so H is a subgroup of G . ■

Alternating groups A_n

As a further example we introduce another family of groups called alternating groups. Recall that every permutation from S_n can be written as a product of transpositions.

Definition 3.6. A permutation $\sigma \in S_n$ is said to be even (respectively, odd) if σ can be written as a product of an even (respectively, odd) number of transpositions. The set of all even permutations is denoted by A_n .

Theorem 3.7. A_n is a subgroup of S_n .

Proof. Let $\alpha, \beta \in A_n$, and write them as products of even number of transpositions: $\alpha = \sigma_1\sigma_2 \dots \sigma_{2k}$, $\beta = \tau_1\tau_2 \dots \tau_{2l}$. Then

$$\alpha\beta^{-1} = \sigma_1\sigma_2 \dots \sigma_{2k}\tau_{2l}^{-1} \dots \tau_2^{-1}\tau_1^{-1},$$

which is again a product of an even number of transpositions. Hence, by Theorem 3.5, it follows that $A_n \leq S_n$. ■

At this stage we cannot be sure that A_n is a proper subgroup of S_n (i.e. that $A_n \neq S_n$). This is resolved by the following:

Theorem 3.8. A permutation $\sigma \in S_n$ cannot be both even and odd.

Proof. (Omitted in lectures, 2003 – 04) Let

$$\sigma = \tau_1\tau_2 \dots \tau_s$$

be an arbitrary decomposition of σ into a product of transpositions, and let

$$\sigma = \gamma_1\gamma_2 \dots \gamma_r$$

be the decomposition of σ into a product of disjoint cycles, with cycles of length 1 included. We shall show that

$$s \equiv n - r \pmod{2}. \tag{2.1}$$

Since the decomposition into disjoint cycles is unique (up to the order of factors) it follows that r is uniquely determined by σ , and then from (2.1) it follows that $s \pmod{2}$ is also uniquely determined by σ .

We prove our assertion by induction on s . If $s = 0$, then it follows that σ is the identity permutation. But then every γ_i is a 1-cycle, so that $r = n$, and (2.1) becomes $0 \equiv 0 \pmod{2}$, which is obviously true. Let us assume that (2.1) holds for some σ which is decomposed into a product of s transpositions. We shall show that when we multiply σ by an arbitrary transposition (thus increasing s for 1), r either increases or decreases by one, so that (2.1) remains valid.

Let $(i j)$ be an arbitrary transposition. We note that it has a common entry with either one or two cycles from $\{\gamma_1, \dots, \gamma_r\}$, and hence is disjoint with all the others.

Assume first that $(i j)$ has common entries with one cycle, say with $\gamma_k = (i i_1 \dots i_m j j_1 \dots j_p)$. Then we have

$$\gamma_k(i j) = (i i_1 \dots i_m)(j j_1 \dots j_p).$$

Thus, the cycle γ splits into two new cycles, and the number r of disjoint cycles increases by one.

If $(i j)$ has common entries with two cycles, say $\gamma_k = (i i_1 \dots i_m)$ and $\gamma_l = (j j_1 \dots j_p)$, then we have

$$\gamma_k \gamma_l(i j) = (i i_1 \dots i_m j j_1 \dots j_p).$$

This time two cycles γ_k and γ_l merge into one new cycle, and thus r decreases by one. This completes the proof of the theorem. ■

The group A_n is called the *alternating group* on $\{1, \dots, n\}$. Its order is $|A_n| = n!/2$; this can be proved directly, but it also follows from some general theory later on.

4. Generators

We describe a neat way of defining a subgroup in a given group, without listing all of its elements.

Theorem 4.1. *Let G be a group, and let $H_i, i \in I$, be a collection of subgroups of G . Then the intersection $\bigcap_{i \in I} H_i$ is also a subgroup of G .*

Proof. Let us write $H = \bigcap_{i \in I} H_i$. Each H_i contains the identity e of G , so that $e \in H$, and H is non-empty. Let $a, b \in H$ be two arbitrary elements.

This means that $a, b \in H_i$ for all $i \in I$. By Theorem 3.5 it follows that $ab^{-1} \in H_i$ for all $i \in I$, and hence $ab^{-1} \in H$. Therefore, H is a subgroup by Theorem 3.5. ■

Definition 4.2. Let G be a group, and let X be a subset of G . Let H_i , $i \in I$, be the family of all subgroups of G which contain the set X . Then $\bigcap_{i \in I} H_i$ is called the *subgroup generated by X* , and is denoted by $\langle X \rangle$.

$\langle X \rangle$ is the smallest subgroup of G which contains X . The elements of X are called *generators* for $\langle X \rangle$. A subgroup may be generated by several of its subsets. If $X = \{a_1, \dots, a_n\}$ then we write $\langle a_1, \dots, a_n \rangle$ instead of $\langle X \rangle$.

Definition 4.2 does not yield a practical way for calculating the elements of a subgroup, given a generating set. Therefore we need the following

Theorem 4.3. Let G be a group and let $X \subseteq G$. The subgroup $\langle X \rangle$ consists of all possible products of elements from X and their inverses, i.e.

$$\langle X \rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} : n \in \mathbb{N}, x_i \in X, \epsilon_i = \pm 1, i = 1, \dots, n\}.$$

Proof. Let us denote the set on the right hand side by H . Since $\langle X \rangle$ is a subgroup, and since it contains X , it must also contain all products of elements from X and their inverses. Therefore we have $H \subseteq \langle X \rangle$. If $x = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$ and $y = y_1^{\delta_1} y_2^{\delta_2} \dots y_m^{\delta_m}$ are two arbitrary elements of H , then

$$xy^{-1} = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} y_m^{-\delta_m} \dots y_2^{-\delta_2} y_1^{-\delta_1} \in H.$$

Therefore H is a subgroup of G by Theorem 3.5. It clearly contains X , and since $\langle X \rangle$ is the smallest subgroup containing X , we must have $\langle X \rangle \subseteq H$. ■

In the special case where X contains a single element a , we have $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$. The *order* of a is defined to be the order of this subgroup. Explicitly,

Definition 4.4. For $a \in G$, if there exists a positive integer m such that $a^m = e$ then the *order* of a is the smallest such integer m . If no such integer m exists, then a is said to be *of infinite order*.

Corollary 4.5. If all elements from X have finite orders then

$$\langle X \rangle = \{x_1 x_2 \dots x_n : n \geq 1, x_1, \dots, x_n \in X\}.$$

Proof. If $a^n = e$ then $a^{-1} = a^{n-1}$, and so the inverse of a generator can be replaced by a positive power of that generator. ■

Example 4.6. $\mathbb{Z} = \langle 1 \rangle$; $\mathbb{Z}_n = \langle 1 \rangle$; $K_4 = \langle a, b \rangle$; $Q_8 = \langle i, j \rangle$.

Example 4.7. We have seen that every permutation from S_n can be written as a product of transpositions. Hence S_n is generated by the set of all transpositions. Actually, one may show that S_n is generated by two permutations $(1\ 2)$ and $(2\ 3\ \dots\ n)$.

Example 4.8. Note that

$$(i\ j)(i\ k) = (i\ j\ k), \quad (i\ j)(k\ l) = (i\ k\ l)(i\ k\ j).$$

Therefore a product of two transpositions can be written as a 3-cycle or as a product of two 3-cycles. It follows that a product of an even number of transpositions can be written as a product of three cycles. We conclude that the alternating group A_n is generated by the set of all 3-cycles.

Corollary 4.5 gives the following method for computing all the elements of a subgroup generated by a finite set $X = \{x_1, \dots, x_m\}$ in a finite group G :

1. let $a_1 := e$; $i := 1$; $l := 1$;
2. while $i \leq l$ do the following steps;
3. for each $j = 1, \dots, m$ do step 4;
4. if $a_i x_j$ is not in the list then let $l := l + 1$ and $a_l = a_i x_j$; otherwise do nothing;
5. $i := i + 1$.

Intuitively, one multiplies the elements from the lists by the generators and adds the new elements at the end of the list until closure occurs.

Example 4.9. Let H be the subgroup of S_8 generated by the permutations

$$\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8), \quad \tau = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6).$$

We compute the elements of H as follows (setting $x_1 = \sigma$, $x_2 = \tau$)

$$\begin{aligned}
a_1 &= \text{id} \\
a_2 &= a_1\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \\
a_3 &= a_1\tau = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6) \\
a_4 &= a_2\sigma = (1\ 3)(2\ 4)(5\ 7)(6\ 8) \\
a_5 &= a_2\tau = (1\ 8\ 3\ 6)(2\ 7\ 4\ 5) \\
a_6 &= a_3\sigma = (1\ 6\ 3\ 8)(2\ 5\ 4\ 7) \\
&\quad a_3\tau = (1\ 3)(2\ 4)(5\ 7)(6\ 8) = a_4 \\
a_7 &= a_4\sigma = (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) \\
a_8 &= a_4\tau = (1\ 7\ 3\ 5)(2\ 6\ 4\ 8) \\
&\quad a_5\sigma = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6) = a_3 \\
&\quad a_5\tau = (1\ 4\ 3\ 2)(5\ 8\ 7\ 6) = a_7 \\
&\quad a_6\sigma = (1\ 7\ 3\ 5)(2\ 6\ 4\ 8) = a_8 \\
&\quad a_6\tau = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) = a_2 \\
&\quad a_7\sigma = \text{id} = a_1 \\
&\quad a_7\tau = (1\ 6\ 3\ 8)(2\ 5\ 4\ 7) = a_6 \\
&\quad a_8\sigma = (1\ 8\ 3\ 6)(2\ 7\ 4\ 5) = a_5 \\
&\quad a_8\tau = \text{id} = a_1.
\end{aligned}$$

So H is an 8-element group. By writing down the multiplication table one can actually see that $H \cong Q_8$.

As our final example we introduce another important family of groups.

Dihedral groups D_n

Definition 4.10. Let $n \geq 3$. The *dihedral group* of degree n (denoted by D_n) is the subgroup of S_n generated by the permutations $\alpha = (1\ 2\ \dots\ n)$ and

$$\begin{aligned}
\beta &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & i & \dots & n-2 & n-1 & n \\ 1 & n & n-1 & n-2 & \dots & n+2-i & \dots & 4 & 3 & 2 \end{pmatrix} \\
&= (2\ n)(3\ (n-1)) \dots (\text{product of } \frac{n-1}{2} \text{ or } \frac{n-2}{2} \text{ transpositions}).
\end{aligned}$$

It can be shown that D_n is actually isomorphic to the group of symmetries of a regular polygon with n -sides:

- α corresponds to a rotation through $\frac{2\pi}{n}$
- β corresponds to reflection across a line through 1 (or 2) of the vertices.

Observe that $K_4 \leq D_4$ (in fact $a = \alpha\beta$, $b = \alpha^3\beta$ and $c = \alpha^2$).

In the following theorem we list the basic properties of D_n which we shall need later.

Theorem 4.11. *The following statements are true for the dihedral group D_n :*

(i) $|\alpha| = n, |\beta| = 2;$

(ii) $\beta\alpha = \alpha^{-1}\beta;$

(iii) $|D_n| = 2n;$

(iv) D_n is non-abelian.

Proof. (i) This is obvious.

(ii) This can be proved by direct computation.

(iii) D_n is generated by α and β , so that every element of D_n is a product of these permutations. However, whenever we have $\beta\alpha$ in this product we can replace it by $\alpha^{-1}\beta$, thus moving β 's towards the right hand side of the product. We end up with a product of the form $\alpha^i\beta^j$, with $0 \leq i \leq n-1$, $0 \leq j \leq 1$. Hence $|D_n| \leq 2n$.

To complete the proof of this part we show that the permutations $\alpha^i\beta^j$ ($0 \leq i \leq n-1$, $0 \leq j \leq 1$) are all distinct. Since α has order n , it follows that the permutations α^i ($0 \leq i \leq n-1$) are all distinct, and also that the permutations $\alpha^i\beta$ are all distinct. Assume that we have $\alpha^i\beta = \alpha^j$, so that $\beta = \alpha^{j-i}$. This is possible only if $i = j$, since otherwise α^{j-i} does not fix 1, while β does. But $i = j$ is also impossible since it implies $\beta = \text{id}$, which is clearly not true.

(iv) Note that $1\alpha\beta = 2\beta = n \neq 2 = 1\alpha = 1\beta\alpha$. Hence $\alpha\beta \neq \beta\alpha$, and D_n is non-abelian. ■

5. Cyclic groups

Definition 5.1. A group is said to be *cyclic* if it can be generated by a single element.

The significance of cyclic groups is that on the one hand one can describe them completely, and that, on the other, every group contains them as subgroups. This is particularly significant for abelian groups, as we will see later in the course.

We have seen that the groups \mathbb{Z} and \mathbb{Z}_n ($n \in \mathbb{N}$) are cyclic (generated by 1). Actually, these exhaust all cyclic groups, as the following theorem shows.

Theorem 5.2. *Let G be a cyclic group. If G is infinite then $G \cong \mathbb{Z}$, while if G is finite of order n then $G \cong \mathbb{Z}_n$.*

Proof. Let a be a generator for G , so that

$$G = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}. \quad (2.2)$$

Assume first that G is infinite, which is equivalent to assuming that a does not have finite order. Define a mapping $f : \mathbb{Z} \rightarrow G$ by $xf = a^x$. This mapping is a homomorphism since $(x + y)f = a^{x+y} = a^x a^y = (xf)(yf)$, and is a surjection by (2.2). To prove that f is an injection (and hence an isomorphism) assume that $xf = yf$ so that $a^x = a^y$, i.e. $a^{x-y} = e$. Since a does not have finite order we must have $x = y$.

If G is finite of order n we proceed along the similar lines, by defining a mapping $f : \mathbb{Z}_n \rightarrow G$, $xf = a^x$. As before it is a homomorphism. By Corollary 4.5 we have

$$G = \langle a \rangle = \{a^i : 0 \leq i \leq n - 1\},$$

so that f is a surjection. Finally we note that all the elements a^i , $0 \leq i \leq n - 1$, are distinct, for $a^i = a^j$ would imply $a^{i-j} = e$, contradicting the fact that n is the order of a . Therefore f is an isomorphism, and hence $G \cong \mathbb{Z}_n$. ■

Theorem 5.3. *Every subgroup of a cyclic group is also cyclic.*

Proof. By the previous theorem it is sufficient to prove the assertion for the groups \mathbb{Z} and \mathbb{Z}_n . We shall prove it for the former; the proof for the latter is very similar. If H is trivial, there is nothing to prove. Otherwise, let m be the smallest positive number in H . We claim that

$$H = \langle m \rangle (= \{mn : n \in \mathbb{Z}\} = m\mathbb{Z}).$$

Clearly $m\mathbb{Z} \subseteq H$. For the converse let $h \in H$ be an arbitrary element of H . By the division algorithm, we can write $h = mn + q$, with $0 \leq q < m$. From $q = h - mn$ it follows that $q \in H$, and since $q < m$, we must have $q = 0$, thus proving $h \in m\mathbb{Z}$. ■

6. Cosets and Lagrange's theorem

Definition 6.1. Let G be a group, let $H \leq G$, and let $a \in G$. The *right coset* of H in G determined by a is the set $Ha = \{ha : h \in H\}$. The corresponding *left coset* is $aH = \{ah : h \in H\}$.

In the following theorem we list some basic properties of cosets.

Theorem 6.2. Let G be a group, and let $H \leq G$.

(i) Every right coset of H has the same number of elements as H itself; in other words $|Ha| = |H|$ for all $a \in G$.

(ii) G is the union of all right cosets of H , i.e. $G = \bigcup_{a \in G} Ha$.

(iii) Any two right cosets of H are either identical, or else they are disjoint; in other words, for any $a, b \in G$ either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.

(iv) For any $a, b \in G$, $Ha = Hb$ if and only if $ab^{-1} \in H$.

Analogous statements hold for left cosets.

Moral of the story The set of right (left) cosets of H in G forms a partition of G .

Proof. (i) Define a mapping $f : H \rightarrow Ha$ by $xf = xa$. From the definition of the coset it follows that f is onto. Also it is one-one since $xf = yf \Rightarrow xa = ya \Rightarrow x = y$, so that it is a bijection, and hence $|H| = |Ha|$.

(ii) Note that $a = ea \in Ha$, so that

$$\bigcup_{a \in G} Ha \subseteq G = \bigcup_{a \in G} \{a\} \subseteq \bigcup_{a \in G} Ha,$$

and the desired equality follows.

(iii) Assume that Ha and Hb have a non-empty intersection, so that $x \in Ha \cap Hb$ for some x . Then we can write $x = h_1a = h_2b$ for some $h_1, h_2 \in H$. Let ha be an arbitrary element of Ha . We have

$$ha = hh_1^{-1}x = hh_1^{-1}h_2b \in Hb.$$

Therefore $Ha \subseteq Hb$, and, by symmetry, $Hb \subseteq Ha$, thus proving that $Ha = Hb$.

(iv) $(\Rightarrow) Ha = Hb \Rightarrow h_1a = h_2b \Rightarrow ab^{-1} = h_1^{-1}h_2 \in H$.

$(\Leftarrow) ab^{-1} \in H \Rightarrow a = ab^{-1}b \in Hb \Rightarrow a \in Ha \cap Hb \Rightarrow Ha = Hb$. ■

Remark 6.3. Given a subgroup H of a group G , one can define a relation $\equiv \pmod{H}$ on G as follows:

$$x \equiv_R y \pmod{H} \iff xy^{-1} \in H.$$

This relation turns out to be an equivalence relation, and right cosets of H in G are the equivalence classes of this relation. Similarly, the equivalence relation defined by $x^{-1}y \in H$ has left cosets of H in G as its equivalence classes.

Theorem 6.4. Let $\mathcal{R} = \{Ha : a \in G\}$ be the set of all right cosets of H in G , and let $\mathcal{L} = \{aH : a \in G\}$ be the set of all left cosets of H in G . Then $|\mathcal{R}| = |\mathcal{L}|$.

Proof. Let us define a mapping $f : \mathcal{R} \rightarrow \mathcal{L}$ by $(Ha)f = a^{-1}H$. Note that the expression Ha for a coset is not necessarily unique; actually, we have $Ha = Ha_1$ for all $a_1 \in Ha$. Therefore, one has to prove that f is well defined, meaning that the image of Ha does not depend on the choice of a representative a . One shows this as follows:

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H \Leftrightarrow (Ha)f = (Hb)f.$$

(Note that we have used Theorem 6.2 (iv), and its dual for left cosets.) If we read the above sequence of equivalences from right to left we obtain a proof that f is one-one. Finally f is onto since for any left coset aH we have $(Ha^{-1})f = aH$. Therefore f is a bijection, and hence $|\mathcal{R}| = |\mathcal{L}|$. ■

Definition 6.5. The *index* of H in G (denoted by $[G : H]$) is the number of right cosets of H in G , and is equal to the number of left cosets of H in G .

Example 6.6. For any group G , $[G : G] = 1$ and $[G : \langle e \rangle] = |G|$.

Example 6.7. Consider the subgroup $H = \{(), (1\ 2)\}$ of S_3 . The right and left cosets of H are

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

We see that $[S_3 : H] = 3$. We also see that right cosets and left cosets of a subgroup do not necessarily coincide.

Example 6.8. Let H be the two-element subgroup $\{1, -1\}$ of Q_8 . Obviously, both 1 and -1 commute with every element of Q_8 so that the left and right cosets of H in Q_8 coincide. Direct computation shows that the distinct cosets are $\{1, -1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$. Here we have $[Q_8 : H] = 4$.

Theorem 6.9 (Lagrange) Let G be a finite group and $H \leq G$. Then $|G| = [G : H]|H|$. In particular, the order of a subgroup divides the order of the group. Also the order of an element divides the order of the group.

Proof. This follows immediately from Theorem 6.2 (i), (ii) and (iii). ■

Corollary 6.10. *Every group of prime order p is isomorphic to \mathbb{Z}_p .*

Proof. Let $|G| = p$ and let $e \neq a \in G$ be arbitrary. By Lagrange's Theorem, the order of a divides p , and hence we must have $|a| = p$. But this means that a generates whole of G , i.e. G is cyclic of order p . ■

Remark 6.11. The following generalisation of Lagrange's Theorem holds: if $K \leq H \leq G$ then $[G : K] = [G : H][H : K]$. If G is finite this can be proved from Lagrange's Theorem: $[G : H][H : K] = (|G|/|H|)(|H|/|K|) = |G|/|K| = [G : K]$. In the infinite case more work has to be done.

7. Homomorphisms

Homomorphisms are mappings between groups which preserve multiplication.

Definition 7.1. Let G and H be groups. A mapping $f : G \rightarrow H$ is a *homomorphism* if $(xy)f = (xf)(yf)$ holds for all $x, y \in G$.

Example 7.2. Let G be a group. The identity mapping $G \rightarrow G$ is a homomorphism. Also the mapping $f : G \rightarrow G, xf = e$ is a homomorphism.

Example 7.3. Note that even and odd permutations multiply according to the following table:

	even	odd
even	even	odd
odd	odd	even

The above is a group isomorphic to \mathbb{Z}_2 . We conclude that the mapping $f : S_n \rightarrow \mathbb{Z}_2$ given by

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

is a homomorphism.

Example 7.4. It is well known that the determinants of matrices over any field satisfy the identity $|AB| = |A||B|$. Therefore the mapping $d : \text{GL}(n, \mathbb{F}) \rightarrow \mathbb{F}^*$, from the general linear group $\text{GL}(n, \mathbb{F})$ into the multiplicative group \mathbb{F}^* of the field \mathbb{F} , defined by $Ad = |A|$ is a homomorphism.

Definition 7.5. Let $f : G \rightarrow H$ be a homomorphism of groups. The *kernel* of f is

$$\ker f = \{x \in G : xf = e_H\}.$$

The *image* of a set $X \subseteq G$ under f is

$$Xf = \{xf : x \in X\}.$$

The image of the whole G is denoted by $\text{im } f$. The *inverse image* of $X \subseteq H$ under f is

$$Xf^{-1} = \{x \in G : xf \in X\}.$$

Example 7.6. For the homomorphisms f and d from Examples 7.3 and 7.4 we have

$$\begin{aligned} \ker f &= \{\sigma \in S_n : \sigma f = 0\} = \{\sigma \in S_n : \sigma \text{ is even}\} = A_n, \\ \text{im } f &= \mathbb{Z}_2, \\ \ker d &= \{A \in \text{GL}(n, \mathbb{F}) : |A| = 1\}, \\ \text{im } d &= \mathbb{F}^*. \end{aligned}$$

Remark 7.7. The notation Xf^{-1} for the inverse image of a set under f does not implicitly assume that f has an inverse. Indeed, it is not necessarily true that $Xff^{-1} = X$ and $Yf^{-1}f = Y$ ($X \subseteq G$, $Y \subseteq H$). However, we always have

$$X \subseteq Xff^{-1} \quad (X \subseteq G), \text{ and } Yf^{-1}f \subseteq Y \quad (Y \subseteq H).$$

Theorem 7.8. Let G and H be two groups, and let $f : G \rightarrow H$ be a homomorphism.

- (i) $e_G f = e_H$.
- (ii) $a^{-1} f = (af)^{-1}$ for all $a \in G$.
- (iii) $\ker f \leq G$.
- (iv) If $K \leq G$ then $Kf \leq H$ (i.e. the homomorphic image of a subgroup is again a subgroup).
- (v) If $L \leq H$ then $Lf^{-1} \leq G$ (i.e. the inverse homomorphic image of a subgroup is again a subgroup).

Name	Description
monomorphism	injective homomorphism
epimorphism	surjective homomorphism
isomorphism	bijective homomorphism
endomorphism	homomorphism $G \rightarrow G$
automorphism	isomorphism $G \rightarrow G$

Table 2.1: Types of homomorphisms

Proof. (i), (ii) Exercise.

(iii) We use the criterion (iii) from Theorem 3.5. If $x, y \in \ker f$ then we have $xf = yf = e_H$, and hence

$$(xy^{-1})f = (xf)(y^{-1}f) = (xf)(yf)^{-1} = e_H e_H^{-1} = e_H,$$

and hence $xy^{-1} \in \ker f$.

(iv) Let $z, t \in Kf$ be arbitrary. By the definition of Kf there exist $x, y \in K$ such that $xf = z$ and $yf = t$. But then $xy^{-1} \in K$, and hence

$$zt^{-1} = (xf)(yf)^{-1} = (xy^{-1})f \in Kf,$$

proving that $Kf \leq H$.

(v) Let $x, y \in Lf^{-1}$. This means that $xf, yf \in L$. But then

$$(xy^{-1})f = (xf)(yf)^{-1} \in L,$$

so that $xy^{-1} \in Lf^{-1}$, and therefore $Lf^{-1} \leq G$. ■

Definition 7.9. The subgroup $\ker d$ from Example 7.6 is denoted by $\text{SL}(n, \mathbb{F})$, and is called the *special linear group*.

It is obvious that isomorphisms are precisely bijective homomorphisms. Various other of homomorphisms have acquired specific names. These are shown in Table 2.1.

8. Normal subgroups, quotient groups

We have seen that the kernel of any homomorphism is a subgroup. One may ask whether the converse is also true, i.e. whether every subgroup is the kernel of a homomorphism. This turns out not to be the case, as we will see at the end of this section.

Theorem 8.1. *Let G be a group and $N \leq G$. The following conditions are equivalent:*

- (i) *every right coset of N in G is also a left coset of N in G ;*
- (ii) *$Na = aN$ for all $a \in G$;*
- (iii) *for every $a \in G$ and every $n \in N$ we have $a^{-1}na \in N$ (in other words $a^{-1}Na \subseteq N$ for all $a \in G$);*
- (iv) *$a^{-1}Na = N$ for all $a \in G$.*

Proof. (i) \Rightarrow (ii) Let $a \in G$ be arbitrary. By (i), the right coset Na is also a left coset, i.e. $Na = bN$ for some $b \in G$. Since $a \in Na$ and $a \in aN$, we have $a \in aN \cap bN$. By Theorem 6.2 (iii) we have $aN = bN$, and hence $Na = aN$.

(ii) \Rightarrow (iii) Since $na \in Na = aN$, there exists $n_1 \in N$ such that $na = an_1$. But then $a^{-1}na = a^{-1}an_1 = n_1 \in N$.

(iii) \Rightarrow (iv) By (iii) we have $a^{-1}Na \subseteq N$, and also $aNa^{-1} \subseteq N$ (replace a by a^{-1}). If we multiply the latter inclusion by a^{-1} from the left and by a from the right we obtain $N \subseteq a^{-1}Na$, and so $a^{-1}Na = N$.

(iv) \Rightarrow (i) From $a^{-1}Na = N$ it follows $Na = aN$, and hence every right coset Na is also the left coset aN . ■

Definition 8.2. A subgroup N of a group G satisfying the equivalent conditions of Theorem 8.1 is said to be *normal*; this is denoted by $N \trianglelefteq G$.

Remark 8.3. *The process of sending $n \in N$ to $a^{-1}na$ ($a \in G$) is called conjugation by a , and we will investigate it further later in the course. Informally, by part (iii) of Theorem 8.1, we can think of the definition of a normal subgroup as saying ‘an element can’t escape from a normal subgroup by conjugation’.*

Example 8.4. • In every group G the subgroups $\langle e \rangle$ and G are normal.

- Every subgroup of an abelian group is normal (here $a^{-1}na = a^{-1}an = n$ for all $a \in G$ and $n \in N$).
- In Example 6.7 the subgroup H is not normal in S_3 .
- In Example 6.8 the subgroup H is normal in Q_8 .

Theorem 8.5. *Let G be a group, let $N \trianglelefteq G$, and let G/N be the set of all (left) cosets of N in G . Then G/N is a group (called the factor group or the quotient group) under the binary operation*

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

Proof. The only problem is to prove that the above multiplication is well defined, i.e. that the result does not depend on the choice of coset representatives. The associativity will then follow from the associativity in G , the coset $eN (= N)$ will be the identity element, and $a^{-1}N$ will be the inverse of aN .

So let us assume that $aN = a_1N$ and $bN = b_1N$, which is equivalent to $a^{-1}a_1, b^{-1}b_1 \in N$ by the dual of Theorem 6.2 (iv). We have to show that $abN = a_1b_1N$. To this end note that

$$(ab)^{-1}a_1b_1 = b^{-1}a^{-1}a_1b_1 = (b^{-1}a^{-1}a_1b)(b^{-1}b_1).$$

Since $a^{-1}a_1 \in N$, and since N is closed under conjugation, it follows that $b^{-1}a^{-1}a_1b \in N$. Now, from $b^{-1}b_1 \in N$ and the fact that N is a subgroup, we obtain $(ab)^{-1}a_1b_1 \in N$, and hence $abN = a_1b_1N$ by the dual of Theorem 6.2 (iv). ■

Example 8.6. Let us consider the quaternion group Q_8 , and let $H = \{1, -1\} \leq Q_8$ be the subgroup considered in Example 6.8. In Example 8.4 we showed that $H \trianglelefteq Q_8$, and hence we can form the factor group G/H . In this group we have

$$\begin{aligned} (iH)(iH) &= i^2H = (-1)H = \{-1, 1\} = H, \\ (iH)(jH) &= (ij)H = kH = \{k, -k\}, \\ (jH)(iH) &= (ji)H = (-k)H = \{-k, k\} = (iH)(jH). \end{aligned}$$

Thus we obtain the following multiplication table for G/H :

	H	iH	jH	kH
H	H	iH	jH	kH
iH	iH	H	kH	jH
jH	jH	kH	H	iH
kH	kH	jH	iH	H

We see that G/H is isomorphic to the Klein four group K_4 .

We now show that normal subgroups are precisely kernels of homomorphisms.

Theorem 8.7. (i) If $f : G \longrightarrow H$ is a homomorphism of groups then $\ker f \trianglelefteq G$.

(ii) Conversely, if $N \trianglelefteq G$ then the map $\pi : G \longrightarrow G/N$ defined by $a\pi = aN$ is an epimorphism and $\ker \pi = N$.

Proof. (i) We know that $\ker f \leq G$ by Theorem 7.8 (iii). To prove it is normal, choose an arbitrary $n \in \ker f$ and $a \in G$, and then observe that

$$\begin{aligned}(a^{-1}na)f &= (a^{-1}f)(nf)(af) = (a^{-1}f)e_H(af) = (a^{-1}f)(af) \\ &= (a^{-1}a)f = e_G f = e_H.\end{aligned}$$

Thus $a^{-1}na \in \ker f$, and hence $\ker f$ is normal.

(ii) For any $a, b \in G$ we have

$$(ab)\pi = (ab)N = (aN)(bN) = (a\pi)(b\pi),$$

and hence π is a homomorphism. It is clear that π is onto. Finally we have

$$a \in \ker \pi \Leftrightarrow a\pi = e_G N = N \Leftrightarrow aN = e_G N \Leftrightarrow a \in N,$$

so that $\ker \pi = N$. ■

Example 8.8. In Example 7.6 we have seen that A_n is the kernel of a homomorphism from S_n into \mathbb{Z}_2 . Therefore $A_n \trianglelefteq S_n$. Similarly, we have $SL(n, \mathbb{F}) \trianglelefteq GL(n, \mathbb{F})$.

9. The isomorphism theorems and the correspondence theorem

Isomorphism theorems explore the connections between subgroups, homomorphisms and quotients.

The first isomorphism theorem asserts that quotients and homomorphic images are one and the same.

Theorem 9.1 (The first isomorphism theorem) If $f : G \longrightarrow H$ is a homomorphism of groups then

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

Proof. Let $K = \ker f$ and $I = \text{im } f$. Define a mapping $h : G/K \rightarrow I$ by

$$(aK)h = af.$$

For any two $a, a_1 \in G$ we have

$$\begin{aligned} aK = a_1K &\Leftrightarrow a^{-1}a_1 \in K = \ker f \Leftrightarrow (a^{-1}a_1)f = e_H \\ &\Leftrightarrow af = a_1f \Leftrightarrow (aK)h = (a_1K)h. \end{aligned}$$

If we read the above sequence of equivalences from left to right it shows that h is well defined, while if we read it from right to left it shows that h is one-one. To show that h is onto, choose an arbitrary $b \in I = \text{im } f$, represent it as $b = af$ for some $a \in G$, and then observe that $(aK)h = af = b$. Finally, h is a homomorphism since

$$((aK)(bK))h = (abK)h = (ab)f = (af)(bf) = ((aK)h)((bK)h),$$

thus completing the proof. \blacksquare

Example 9.2. Let $n \in \mathbb{N}$, and define a mapping $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $xf = x \pmod{n}$. It is clear that f is an epimorphism. Also note that $xf = 0$ if and only if $x = 0 \pmod{n}$, i.e. if and only if x is divisible by n . In other words

$$\ker f = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}.$$

By the First Isomorphism Theorem we have

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker f \cong \text{im } f = \mathbb{Z}_n.$$

Example 9.3. The homomorphism $d : GL(n, \mathbb{F}) \rightarrow \mathbb{F}^*$, sending each matrix into its determinant, is obviously onto. Therefore we have

$$GL(n, \mathbb{F})/SL(n, \mathbb{F}) = GL(n, \mathbb{F})/(\ker d) \cong \text{im } d = \mathbb{F}^*.$$

Example 9.4. From Example 7.6 we have that $S_n/A_n \cong \mathbb{Z}_2$. In particular, we have

$$2 = |\mathbb{Z}_2| = |S_n/A_n| = [S_n : A_n] = |S_n|/|A_n|.$$

Since $|S_n| = n!$, it follows that $|A_n| = n!/2$.

Theorem 9.5 (The second isomorphism theorem) *Let G be a group, let $H \leq G$ and let $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$, $N \trianglelefteq HN = NH \leq G$ and*

$$H/(H \cap N) \cong HN/N.$$

Proof. First we prove that $HN = NH$ and that it is a subgroup of G . Indeed we have

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH.$$

Now take two elements h_1n_1 and h_2n_2 from HN . Since we have $n_1n_2^{-1} \in N$, it follows that $n_1n_2^{-1}h_2^{-1} \in NH = HN$, and hence $n_1n_2^{-1}h_2^{-1} = h_3n_3$ ($h_3 \in H$, $n_3 \in N$). Now we have

$$(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_3n_3 \in HN,$$

proving $HN \leq G$.

It is clear that $N = eN \subseteq HN$. Also, since $N \trianglelefteq G$, its left and right cosets coincide in G . But since $HN \leq G$, it follows that the left and right cosets of N in HN must also coincide, and so $N \trianglelefteq HN$.

Now we can form the quotient HN/N . Define a mapping $f : H \rightarrow HN/N$, by defining $af = aN$. As an exercise prove that f is a well defined epimorphism. For $a \in H$ we have

$$a \in \ker f \Leftrightarrow af = N \Leftrightarrow aN = N \Leftrightarrow a \in N,$$

so that $\ker f = H \cap N$. In particular, $H \cap N \trianglelefteq H$. By the first isomorphism theorem we have

$$H/(H \cap N) = H/\ker f \cong \text{im } f = HN/N,$$

exactly as required. ■

The third isomorphism theorem describes quotients of quotients.

Theorem 9.6 (The third isomorphism theorem) *Let G be a group, let $H, K \trianglelefteq G$, and let $K \leq H$. Then $H/K \trianglelefteq G/K$ and*

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

Proof. Define a mapping $f : G/K \rightarrow G/H$ by $(aK)f = aH$. Prove as an exercise that f is a well defined epimorphism with kernel equal to H/K , and the theorem follows from the first isomorphism theorem. ■

The correspondence theorem establishes a one-one correspondence between the subgroups of a quotient and certain subgroups of the original group.

Theorem 9.7 (The correspondence theorem) *Let G be a group and let $N \trianglelefteq G$. Also let*

$$\mathcal{A} = \{H : N \leq H \leq G\}, \mathcal{B} = \{K : K \leq G/N\}.$$

The mapping $f : \mathcal{A} \rightarrow \mathcal{B}$ defined by

$$Hf = H/N = \{hN : h \in H\} \quad (N \leq H \leq G)$$

is a bijection. Under this bijection normal subgroups correspond to normal subgroups. Also, the correspondence “preserves” inclusion.

Proof. Denote by π the natural epimorphism $G \rightarrow G/N$, $x \mapsto xN$. Clearly, for $H \in \mathcal{A}$, Hf is equal to the image $H\pi$ of H under π . By 7.8 (iv) it follows that $Hf \leq G/N$, and so f is well defined.

Next we prove that f is 1-1. To this end let $H_1, H_2 \in \mathcal{A}$ be such that $H_1f = H_2f$, i.e. $H_1/N = H_2/N$. Let $a \in H_1$ be arbitrary. From $aN \in H_1/N = H_2/N$, it follows that $aN = bN$ for some $b \in H_2$. In particular $a = bn$ for some $n \in N$. But since $N \subseteq H_2$, it follows that $a \in H_2$. This proves that $H_1 \subseteq H_2$. By symmetry we have $H_2 \subseteq H_1$, and so $H_1 = H_2$ as required.

To prove that f is onto, we take an arbitrary $K \in \mathcal{B}$. Let $H = K\pi^{-1} = \{x \in G : xN \in K\} \leq G$. Since π is onto, we have $Hf = H\pi = K$. Also, since for each $n \in N$ we have $nN = N = eN \in K$, we also have $N \leq H$, and therefore $H \in \mathcal{A}$.

The last statement is left as an exercise. ■