

Chapter 4.

Structure of groups

13. Simple groups

Consider an arbitrary group G , and assume that G has a proper normal subgroup N . One may think of G as being decomposed into two groups, namely N and G/N . For example, the order of G is equal to $|N||G/N|$. Also, these two groups reflect parts of the subgroup structure of G : N contains all subgroups of G contained in N , whereas, by the Correspondence theorem, the subgroups of G/N are in 1-1 correspondence with subgroups of G containing N .

In this context, it is natural to expect that the groups which cannot be decomposed in this way are significant.

Definition 13.1. A non-trivial group which has no proper normal subgroups is said to be *simple*.

It is easy to characterise all abelian simple groups.

Theorem 13.2. *Let G be an abelian group. Then G is simple if and only if G is isomorphic to \mathbb{Z}_p for a prime number p .*

Proof. By Lagrange's theorem, the group \mathbb{Z}_p has no proper subgroups, and hence is simple. For the converse let G be an arbitrary simple abelian group, and let $a \in G$, be an arbitrary non-identity element. Consider the subgroup H of G generated by a . Since every subgroup of an abelian group is normal, we must have $H = G$. In other words, G must be cyclic. By Theorem 5.2, G is either isomorphic to \mathbb{Z} or is isomorphic to \mathbb{Z}_n for some $n \in \mathbb{N}$. However, \mathbb{Z} has non-trivial subgroups, and is not simple. Similarly, if $n = kl$ is a non-prime number, the group \mathbb{Z}_n has a non-trivial subgroup, for example the subgroup generated by k . Therefore, we conclude that G must be isomorphic to a group \mathbb{Z}_p , where p is a prime. ■

Non-abelian simple groups are much harder to determine. The following theorem gives one infinite class of such groups.

Theorem 13.3. *The alternating group A_n is simple for every $n \geq 5$.*

Proof. In order to prove the theorem, the following two facts about a normal subgroup $N \trianglelefteq A_n$:

- I) if N contains a non-identity permutation then N contains a 3-cycle;
- II) if N contains one three-cycle then it contains all 3-cycles.

By Example 4.8, the set of all 3-cycles generates A_n . We conclude that if N is non-trivial then $N = A_n$, and thus complete the proof of the theorem. We prove the above statements in the reverse order.

II) Let $(i j k) \in N$, and let $(p q r)$ be an arbitrary three-cycle. We have to prove that $(p q r) \in N$.

Let us assume that $r \neq k$, and let $\pi = (i j)(k r) \in A_n$. Since N is normal in A_n , we have

$$\pi^{-1}(i j k)^2\pi = \pi^{-1}(i k j)\pi = (j r i) = (i j r) \in N.$$

We have therefore shown that, if we replace the third entry of a three-cycle in N by an arbitrary element, we obtain another permutation in N .

Our strategy is to repeatedly use this fact to “transform” $(i j k)$ to $(p q r)$.

From above, we have $(i j r) \in N$. Writing this as $(r i j)$, we may now replace the third entry j by q , thus giving $(r i q) = (i q r) \in N$. Next, write this three-cycle as $(q r i)$ and replace i by p , obtaining $(q r p) = (p q r) \in N$, as required.

I) Let $n \geq 5$, let $N \trianglelefteq A_n$ be a non-trivial normal subgroup of A_n , and let $\sigma \in N$ be a non-identity permutation. Write σ as a product of disjoint cycles

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

Since disjoint cycles commute, we may assume that the γ_i are written in order of decreasing length. We consider the possible cases and examine them separately:

- γ_1 has length at least four (case 1).
- Otherwise, γ_1 has length less than four, i.e. three or two.
 - If γ_1 is a three-cycle, then either:
 - * $r = 1$ and result is immediate;
 - * $r > 1$, γ_1 and γ_2 both have length three (case 2);
 - * $r > 1$, γ_2 has length two (case 3);

– Otherwise γ_1 is a two-cycle (hence so are the other γ_i). Then either:

- * $r = 2$, i.e. $\sigma = \gamma_1\gamma_2$ (case 4);
- * $r > 2$ (case 5).

Case 1. If $\gamma_1 = (i_1 i_2 \dots i_k)$, where $k \geq 4$, then let $\pi = (i_1 i_2 i_3)$. Note that π is necessarily disjoint from (and hence commutes with) $\gamma_2, \dots, \gamma_r$. Since N is normal in G , and since $\gamma_1, \dots, \gamma_r$ are disjoint we have

$$\begin{aligned} N \ni \sigma^{-1}\pi^{-1}\sigma\pi &= (\gamma_2 \dots \gamma_r)^{-1}\gamma_1^{-1}(\pi^{-1}\gamma_1\pi)\gamma_2 \dots \gamma_r \\ &= \gamma_1^{-1}(\pi^{-1}\gamma_1\pi) = (i_k \dots i_2 i_1)(i_2 i_3 i_1 i_4 i_5 \dots i_k) = (i_1 i_2 i_4). \end{aligned}$$

Therefore, in this case, N contains a three-cycle, as required.

Case 2. Let $\gamma_1 = (i j k)$, and let $\gamma_2 = (p q s)$. If we define $\pi = (k p q)$, then similarly as before we have

$$N \ni \sigma^{-1}\pi^{-1}\sigma\pi = (k j i)(s q p)(i j p)(q k s) = (i s k p q).$$

Thus we have reduced this case to Case 1.

Case 3. Let $\gamma_1 = (i j k)$. Since γ_2 is a transposition, so are $\gamma_3, \dots, \gamma_r$. Then we have

$$N \ni \sigma^2 = \gamma_1^2\gamma_2^2 \dots \gamma_r^2 = \gamma_1^2 = (i k j),$$

and hence N contains a three-cycle.

Case 4. Let $\gamma_1 = (i j)$, and let $\gamma_2 = (k l)$. Since $n \geq 5$, we can choose $m \notin \{i, j, k, l\}$. But then for $\pi = (i j m)$ we have

$$N \ni \sigma\pi^{-1}\sigma\pi = (i j)(k l)(j m)(k l) = (i m j),$$

and hence N contains a three-cycle.

Case 5. Since σ is even, we must have at least four transpositions, i.e. $r \geq 4$. Let $\gamma_1 = (i j)$, $\gamma_2 = (k l)$, $\gamma_3 = (p q)$, $\gamma_4 = (s t)$. Define $\pi = (l p)(j k)$, so that

$$N \ni \sigma\pi^{-1}\sigma\pi = (i j)(k l)(p q)(s t)(i k)(j p)(l q)(s t) = (i p l)(j k q).$$

This reduces this case to Case 2. ■

Another class of simple groups arises in the context of matrix groups. Consider the special linear group $SL(m, \mathbb{F})$, where $m \geq 2$ and \mathbb{F} is a finite field. The set $N := \{kI : k \in \mathbb{F}, k^m = 1\}$ is easily seen to be a normal subgroup of $SL(m, \mathbb{F})$. The quotient $SL(m, \mathbb{F})/N$ is called the *projective special*

linear group, and is denoted by $PSL(m, \mathbb{F})$. It turns out that $PSL(m, \mathbb{F})$ is simple.

So, what is currently known about simple groups? All finite simple groups have been classified. There are some infinite families such as A_n and $PSL(m, \mathbb{F})$ and 26 simple groups (called sporadic simple groups) which belong to neither of the families. The largest sporadic simple group (called the Monster) has order

$$808017424794512875886459904961710757005754368000000000.$$

The classification of finite simple groups is one of the major achievements of 20th century mathematics.

14. Composition series

As indicated in the previous section, if a group G is not simple, it can be ‘decomposed’ into two groups N and G/N , where N is a proper normal subgroup. Then, if they are not simple, one can ‘decompose’ N and G/N . If G is finite, then this process will eventually stop, and one will obtain a collection of simple groups. So, every finite group is in some sense built of simple groups.

Two questions arise in this context. Firstly, given a finite group G , describe different ways of decomposing G into collections of simple groups. This question is addressed by the Jordan–Hölder theorem below. The second question is, given two groups H and K , describe different ways in which one can ‘put them together’ to form a new group which ‘decomposes’ into H and K . This is a much harder question, and is the main subject of a branch of group theory called extension theory.

Definition 14.1. A *subnormal series* of a group G is a chain of subgroups $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_n$ such that $G_{i+1} \trianglelefteq G_i$ for all i , $0 \leq i < n$. The *factors* of this series are the quotients G_i/G_{i+1} , $0 \leq i < n$. The *length* of the series is n . The series is a *composition series* if $G_n = \{e\}$ and all factors are simple.

Theorem 14.2. *Every finite group G has a composition series.*

Proof. We prove the theorem by induction on G , the case $|G| = 1$ being trivial. Let $|G| > 1$, and assume that the theorem is valid for every group of smaller order. If G is simple then $G \geq \{e\}$ is a composition series for G . Otherwise let G_1 be a proper normal subgroup of G which is not contained in

any other proper normal subgroup. By induction G_1 has a composition series $G_1 \geq G_2 \geq \dots \geq G_n = \{e\}$. By the Correspondence Theorem the quotient G/G_1 is simple, and so $G \geq G_1 \geq G_2 \geq \dots \geq G_n = \{e\}$ is a composition series for G . ■

Example 14.3. The series

$$\begin{aligned}\mathbb{Z}_{12} &\geq \{0, 3, 6, 9\} \geq \{0, 6\} \geq \{0\}, \\ \mathbb{Z}_{12} &\geq \{0, 2, 4, 6, 8, 10\} \geq \{0, 4, 8\} \geq \{0\}\end{aligned}$$

are both composition series for \mathbb{Z}_{12} . They both have length 3. The factors of the first series are $\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$ and that of the second are $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

Note If G is a finite abelian group, then each factor in its composition series must be \mathbb{Z}_p for some prime p . For: the factors are abelian (since G is) and simple (by definition), and by Theorem 13.2 the only abelian simple groups are \mathbb{Z}_p where p is prime.

The situation in the previous example is no accident.

Definition 14.4. Two subnormal series $G \geq G_1 \geq G_2 \geq \dots \geq G_n$ and $G \geq H_1 \geq H_2 \geq \dots \geq H_m$ of the same group G are said to be *equivalent* if they have equal lengths and there is a one-one correspondence between the factors such that the corresponding factors are isomorphic.

We give the following theorem without a proof.

Theorem 14.5 (Jordan–Hölder) *If a group G has composition series then any two composition series are equivalent.*

In particular any two composition series of a finite group are equivalent. Thus a finite group is composed from simple groups, and the ingredients are uniquely determined by the group.

15. The centre and the derived subgroup

Another common idea in group theory is to consider abelian groups as ‘well understood’ (in light of Theorem 12.7, for example), and then to try and somehow measure how far from being abelian a group G under consideration is. The main tools in this are two distinguished subgroups of G – the centre and the derived subgroup.

Definition 15.1. The *centre* of a group G is the set $Z(G) = \{x \in G : xa = ax \text{ for all } a \in G\}$.

Theorem 15.2. *Let G be a group. Then*

- (i) $Z(G) \trianglelefteq G$;
- (ii) G is abelian if and only if $Z(G) = G$.

Proof. (i) Let $x, y \in Z(G)$ be arbitrary. For every $a \in G$ we have $axy = xay = xya$ so that $xy \in Z(G)$, and also $x^{-1}a = ax^{-1}$ implying $x^{-1} \in Z(G)$. Therefore $Z(G)$ is a subgroup of G . To prove that it is normal we prove that $Z(G)$ is closed under conjugation. Indeed, if $x \in Z(G)$ and $a \in G$ then $a^{-1}xa = a^{-1}ax = ax = x \in Z(G)$.

(ii) This is immediate since G is abelian $\Leftrightarrow \forall x, a \in G, xa = ax \Leftrightarrow \forall x \in G, xa = ax \quad \forall a \in G \Leftrightarrow \forall x \in G, x \in Z(G)$. ■

Example 15.3. Consider the quaternion group Q_8 . Clearly, $1, -1 \in Z(Q_8)$. Also, $i \notin Z(Q_8)$, because $ij = k \neq -k = ji$. In a similar way, one shows that no other element of Q_8 is in the centre, so that $Z(Q_8) = \{1, -1\}$. (Recall we showed earlier in the course that $\{1, -1\}$ (which we called H) is a normal subgroup of Q_8 .)

Definition 15.4. Let G be a group. The *commutator* of two elements $a, b \in G$ is the element $[a, b] = a^{-1}b^{-1}ab$. The *derived subgroup* G' of G is the subgroup of G generated by all commutators, i.e.

$$G' = \langle \{[a, b] : a, b \in G\} \rangle.$$

Remark 15.5. The product of two commutators is not necessarily a commutator. Hence the commutator subgroup does not consist wholly of commutators, but rather of all possible products of commutators (and their inverses, but they are also commutators, as we will soon see).

Theorem 15.6. *Let G be a group. The derived subgroup of G is the smallest normal subgroup N of G such that the quotient G/N is abelian.*

Note that we are using “smallest” in the group theoretic sense, i.e. N is the smallest subgroup with a certain property if every other subgroup with this property must contain N .

Proof. G' is a subgroup of G by definition. To prove that it is normal we will prove that it is closed under conjugation. Let $x \in G'$ be arbitrary. By the definition of G' , we can express x as a product $x = c_1c_2 \dots c_n$ of commutators and their inverses. Next note that

$$[a, b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b, a],$$

i.e. that the inverse of a commutator is again a commutator. Thus each c_i is a commutator, say $c_i = [z_i, t_i]$. If we conjugate x by an element $a \in G$ we obtain

$$a^{-1}xa = (a^{-1}c_1a)(a^{-1}c_2a) \dots (a^{-1}c_na).$$

Finally we note that

$$a^{-1}c_ia = a^{-1}z_i^{-1}t_i^{-1}z_it_ia = [a^{-1}z_ia, a^{-1}t_ia],$$

and therefore $a^{-1}xa \in G'$.

To prove that G/G' is abelian, take any two $a, b \in G$. Then $(ba)^{-1}(ab) = [a, b] \in G'$ implies $baG' = abG'$, i.e. $(aG')(bG') = (bG')(aG')$.

Now let N be any other normal subgroup of G such that G/N is abelian. Thus for arbitrary $a, b \in G$ we have $(ab)N = (aN)(bN) = (bN)(aN) = (ba)N$, so that $[a, b] = (ba)^{-1}(ab) \in N$. Thus N contains all the commutators, and hence contains the subgroup G' generated by them. ■

Example 15.7. Since the quaternion group Q_8 is not abelian we have $Q'_8 \neq \{1\}$. On the other hand $Q_8/\{1, -1\}$ is isomorphic to the abelian group K_4 , as was shown in Example 8.6, and hence $Q'_8 = \{1, -1\}$.

16. Soluble groups

One can take the idea of comparing arbitrary groups to abelian groups further, by considering those groups which are in some sense composed of abelian groups.

One possible approach to this is to note that the composition factors of a finite abelian group are clearly cyclic of prime orders. So one may consider non-abelian groups all composition factors of which are cyclic of prime orders.

Another approach is to recall that a group is abelian if and only if the derived group G' is trivial; see Theorem 15.6. We extend this idea by making the following definition:

Definition 16.1. Let G be a group. Define *higher commutator subgroups* $G^{(i)}$, $i = 0, 2, 3, \dots$ inductively by $G^{(0)} = G$, $G^{(i+1)} = (G^{(i)})'$.

Clearly we have a subnormal series $G \geq G' \geq G'' \geq \dots$. Thus a group is abelian if this series has length 1 and ends in the trivial subgroup. A generalisation of this would be groups for which $G^{(m)} = \{e\}$ for some $m \geq 1$.

It turns out that the two approaches coincide.

Theorem 16.2. *The following conditions are equivalent for a finite group G :*

(i) all composition factors of G are cyclic of prime order;

(ii) $G^{(m)} = \{e\}$ for some $m \geq 1$.

Proof. (i) \Rightarrow (ii) Let $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_n = \{e\}$ be any composition series for G . For each i , $0 \leq i < n$, the quotient G_i/G_{i+1} is cyclic of prime order, and hence is abelian. Therefore we have $G'_i \subseteq G_{i+1}$ by Theorem 15.6, since G'_i is the smallest such. In particular we have $G' \subseteq G_1$, and by induction we have $G^{(i)} \subseteq G_i$. We conclude that $G^{(n)} = \{e\}$.

(ii) \Rightarrow (i) Assume that $G^{(m)} = \{e\}$. For each i , $0 \leq i < m$, the quotient $G^{(i)}/G^{(i+1)}$ is abelian by Theorem 15.6. In particular all the composition factors of this quotient are cyclic of prime orders. Let $G^{(i)}/G^{(i+1)} = \overline{N}_{i,0} \geq \overline{N}_{i,1} \geq \dots \geq \overline{N}_{i,s_i} = G^{(i+1)}/G^{(i+1)}$ be any composition series. By the Correspondence Theorem each $\overline{N}_{i,j}$ is equal to $N_{i,j}/G^{(i+1)}$ for some $N_{i,j}$, $G^{(i+1)} \leq N_{i,j} \leq G^{(i)}$. Also since normality is preserved in the Correspondence Theorem we have a subnormal series

$$\begin{aligned} G = G_0 &= N_{0,0} \geq N_{0,1} \geq \dots \geq N_{0,s_0} = G' = N_{1,0} \geq N_{1,1} \geq \dots \\ &\geq N_{1,s_1} = G'' = N_{2,0} \geq \dots \\ &\geq G^{(m-1)} = N_{m-1,0} \geq N_{m-1,1} \geq \dots \geq N_{m-1,s_{m-1}} = G^{(m)} = \{e\}. \end{aligned}$$

By the Third Isomorphism Theorem for a general factor in the above series we have

$$\frac{N_{i,j}}{N_{i,j+1}} \cong \frac{N_{i,j}/G^{(i+1)}}{N_{i,j+1}/G^{(i+1)}} = \frac{\overline{N}_{i,j}}{\overline{N}_{i,j+1}}.$$

Therefore all composition factors of G are cyclic of prime orders, as required.

■

Definition 16.3. A group G satisfying equivalent conditions of Theorem 16.2 is said to be *soluble*.

Example 16.4. The quaternion group Q_8 is soluble.

We have seen in Example 15.7 that $Q'_8 = \{1, -1\} \cong \mathbb{Z}_2$; since \mathbb{Z}_2 is abelian we have $Q''_8 = \{1\}$.

Alternatively, we have the composition series $Q_8 \geq \langle i \rangle \geq \langle -1 \rangle \geq \{1\}$, whose factors are $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2$.

Example 16.5. The alternating group A_n ($n \geq 5$) (and indeed any non-abelian simple group) is not soluble: it obviously does not satisfy condition (i) of Theorem 16.2.

Solubility was one of the first properties of groups the mathematicians investigated. The reason for this is that it is related to solubility of algebraic equations (hence the name). Galois showed how to associate a permutation group to any algebraic equation. Then he proved that the equation can be solved by using the basic operations of arithmetic ($+$, $-$, \cdot , $/$) together with the operation of taking arbitrary roots if and only if the corresponding group is soluble. The fact that a general algebraic equation of degree n is soluble if and only if $n \leq 4$ is then an immediate consequence of the fact that the symmetric group S_n is soluble if and only if $n \leq 4$, which, in turn, is an immediate consequence of the fact that A_n is simple and non-abelian if and only if $n \geq 5$.

The class of all finite soluble groups turns out to be rather extensive. For example, A_5 is the only non-soluble group of order less than 100. We will now define a subclass of this class.

Definition 16.6. Let G be a group. For any two subgroups $H, K \leq G$ define $[H, K]$ to be the subgroup of G generated by all commutators $[h, k]$ with $h \in H$, $k \in K$. Now define inductively a series of subgroups $\gamma_i(G)$, $i = 0, 1, 2, \dots$ as follows

$$\gamma_0(G) = G, \quad \gamma_{i+1}(G) = [\gamma_i(G), G].$$

It is easy to see that $\gamma_{i+1}(G) \leq \gamma_i(G)$.

Definition 16.7. A group G is *nilpotent* if $\gamma_m(G) = \{e\}$ for some m .

We have the following two theorems about nilpotent groups which we will use later (though we will not prove them here).

Theorem 16.8. *Every nilpotent group is soluble, but the converse is not true.*

Theorem 16.9. *The direct product of two, and indeed finitely many, nilpotent groups is nilpotent.*

17. Conjugation

We know that a subgroup N of a group G is normal if and only if $a^{-1}Na \subseteq N$ for all $a \in G$. This suggests that it might be worth investigating the following relation on G .

Definition 17.1. Let G be a group. Two elements $x, y \in G$ are *conjugate* if there exists $a \in G$ such that $a^{-1}xa = y$; this is denoted by $x \sim y$.

Theorem 17.2. *The relation \sim is an equivalence relation.*

Proof.

- Reflexive: for each x we have $e^{-1}xe = x$, and so $x \sim x$.
- Symmetric: if $x \sim y$ then $a^{-1}xa = y$ for some $a \in G$, which is equivalent to $(a^{-1})^{-1}y(a^{-1}) = x$, and hence we have $y \sim x$.
- Transitive: if $x \sim y$ and $y \sim z$ with $a^{-1}xa = y$ and $b^{-1}yb = z$ then $(ab)^{-1}x(ab) = b^{-1}a^{-1}xab = b^{-1}yb = z$, and hence $x \sim z$.

■

Definition 17.3. The equivalence classes of the relation \sim are called *conjugacy classes* of G .

In other words, the conjugacy class of an element $x \in G$ is the set of all elements of G conjugate to x .

Example 17.4. The conjugacy class of the identity e is $\{e\}$. Indeed, if $e \sim x$ then, by the definition, $a^{-1}ea = x$, and so $x = e$.

Like the cosets of a subgroup, conjugacy classes partition the group. However, unlike the cosets, the conjugacy classes are generally not all of the same size.

The following theorem comes useful when trying to determine the normal subgroups of a group.

Theorem 17.5. *Let G be a group and let H be a subgroup of G . Then H is normal if and only if H is a union of conjugacy classes of G .*

Proof. H is normal $\Leftrightarrow H$ is closed under conjugation by any element of $G \Leftrightarrow$ for every $h \in H$ the whole conjugacy class of h is contained in $H \Leftrightarrow H$ is a union of conjugacy classes. ■

Conjugation is also connected with the automorphisms of a group. (Recall that an automorphism of a group G is any isomorphism $G \rightarrow G$.)

First of all one should note that the set of all automorphisms of a group G forms a group under the composition of mappings (product of two automorphisms is an automorphism, the inverse of an automorphism is an automorphism). This group is called the *automorphism group of G* and is denoted by $\text{Aut}G$.

For every $a \in G$, let $\tau_a : G \rightarrow G$ be the mapping defined by $x\tau_a = a^{-1}xa$, and let $\text{Inn}G = \{\tau_a : a \in G\}$.

Theorem 17.6. For any group G the set $\text{Inn}G$ is a subgroup of $\text{Aut}G$.

Proof. First we show that each τ_a is an automorphism, i.e. $\text{Inn}G$ is a subset of $\text{Aut}G$. For an arbitrary $y \in G$ let $x = aya^{-1}$, so that $x\tau_a = a^{-1}aya^{-1}a = y$; thus τ_a is surjective. If $x\tau_a = y\tau_a$ for some $x, y \in G$ then $a^{-1}xa = a^{-1}ya$ and so $x = y$; thus τ_a is injective. Finally, for any $x, y \in G$ we have $(x\tau_a)(y\tau_a) = a^{-1}xaa^{-1}ya = a^{-1}xya = (xy)\tau_a$, and so τ_a is a homomorphism.

It remains to show that $\text{Inn}G \leq \text{Aut}G$. Let $a, b \in G$ be arbitrary; then from $x(\tau_a\tau_b) = b^{-1}a^{-1}xab = (ab)^{-1}x(ab) = x\tau_{ab}$ it follows that $\tau_a\tau_b = \tau_{ab}$. Also, from $x(\tau_a\tau_{a^{-1}}) = aa^{-1}xaa^{-1} = x$ it follows that $\tau_a^{-1} = \tau_{a^{-1}}$. So $\text{Inn}G$ is closed for multiplication and taking inverses, and so is a subgroup. ■

In general it is not easy to determine the conjugacy classes of a group G . However, it is relatively easy to do this in the symmetric group. The basic observation for this is the following formula for conjugating a cycle $\gamma = (i_1 i_2 \dots i_r) \in S_n$ by a permutation $\pi \in S_n$:

$$\pi^{-1}\gamma\pi = (i_1\pi i_2\pi \dots i_r\pi). \quad (4.4)$$

The proof is straightforward.

Definition 17.7. Two permutations τ and σ are said to have the *same disjoint cycle structure* if the decompositions of σ and τ contain the same numbers of cycles of each length.

Thus, for example, the permutations $(1\ 2\ 3)(4\ 5)$ and $(1\ 2\ 5)(3\ 4)$ have the same disjoint cycle structure, while $(1\ 2\ 3)(4\ 5)$ and $(1\ 2)(3\ 4)$ do not.

Theorem 17.8. Two permutations $\sigma, \tau \in S_n$ are conjugate in S_n if and only if they have the same disjoint cycle structure.

Proof. (\Rightarrow) If $\sigma \sim \tau$ then there exists $\pi \in S_n$ such that $\pi^{-1}\sigma\pi = \tau$. If $\sigma = \gamma_1\gamma_2 \dots \gamma_r$ is the decomposition of σ into disjoint cycles, then

$$\tau = \pi^{-1}\sigma\pi = \pi^{-1}\gamma_1\gamma_2 \dots \gamma_r\pi = (\pi^{-1}\gamma_1\pi)(\pi^{-1}\gamma_2\pi) \dots (\pi^{-1}\gamma_r\pi),$$

is the decomposition of τ into disjoint cycles by (4.4) above. Hence σ and τ have the same disjoint cycle structure.

(\Leftarrow) Let σ and τ have the same disjoint cycle structure. This means that we can write

$$\sigma = \gamma_1\gamma_2 \dots \gamma_r, \quad \tau = \delta_1\delta_2 \dots \delta_r,$$

(ii) If $H \leq G$ then H is a normal subgroup of $N(H)$. Moreover, $N(H)$ is the largest subgroup of G such that H is normal in it. In particular, if $H \trianglelefteq G$ then $N(H) = G$.

Proof. (i) Let $a, b \in N(S)$. To show: $ab^{-1} \in N(S)$. We have

$$a^{-1}Sa = S, \quad b^{-1}Sb = S.$$

From the second equation we obtain $bSb^{-1} = S$, and hence

$$(ab^{-1})^{-1}S(ab^{-1}) = ba^{-1}Sab^{-1} = bSb^{-1} = S.$$

Therefore $N(S) \leq G$.

(ii) For any $h \in H$ we have $h^{-1}Hh = H$, and hence $H \leq N(H)$. Next, for $a \in N(H)$, we have $a^{-1}Ha = H$ by the definition of the normaliser, and so $H \trianglelefteq N(H)$. Finally, if K is any subgroup of G such that $H \trianglelefteq K$, then for every $k \in K$ we have $k^{-1}Hk = H$, so that $K \leq N(H)$. ■

The notion of conjugacy can be extended to subsets of G .

Definition 18.3. Two subsets S and T are conjugate if $a^{-1}Sa = T$ for some $a \in G$.

For example, if $N \trianglelefteq G$ then N is the only conjugate of itself.

Theorem 18.4. Let G be a group, and let S be a non-empty subset of G . The number of distinct conjugates of S in G is equal to $[G : N(S)]$, and divides the order of G by Lagrange's Theorem.

Proof. Define a mapping f from the set of all conjugates of S into the set of right cosets of $N(S)$ by

$$(a^{-1}Sa)f = N(S)a.$$

Note that

$$\begin{aligned} a^{-1}Sa = b^{-1}Sb &\iff (ab^{-1})^{-1}S(ab^{-1}) = S \iff ab^{-1} \in N(S) \\ &\iff N(S)a = N(S)b \iff (a^{-1}Sa)f = (b^{-1}Sb)f. \end{aligned}$$

This shows that f is well defined and that it is injective. It is obvious that f is surjective. Thus we can put the two sets into bijective correspondence, so they have the same number of elements and the theorem follows. ■

Next we characterize the elements which have 1-element conjugacy classes.

Lemma 18.5. *An element x of a group G is the only conjugate of itself if and only if it belongs to the centre $Z(G)$.*

Proof. The conjugacy class of x is the set $\{a^{-1}xa : a \in G\}$. This set is equal to $\{x\} \Leftrightarrow a^{-1}xa = x$ for all $a \in G \Leftrightarrow xa = ax$ for all $a \in G \Leftrightarrow x \in Z(G)$. ■

Now, consider an arbitrary finite group, and denote by C_1, C_2, \dots, C_n all the conjugacy classes of G . Further, assume that C_{r+1}, \dots, C_n are those of them which contain only one element. Then, by Lemma 18.5, we have

$$Z(G) = C_{r+1} \cup \dots \cup C_n.$$

Also, if for each i , $1 \leq i \leq n$, we choose a representative $x_i \in C_i$, then by Theorem 18.4, we have

$$|C_i| = [G : N(x_i)].$$

Finally, we note that

$$|G| = |C_1| + \dots + |C_r| + |C_{r+1}| + \dots + |C_n| = \sum_{i=1}^r [G : N(x_i)] + |Z(G)|.$$

Therefore we have

Theorem 18.6 (The Class Equation) *Let G be a group, let C_i , $1 \leq i \leq n$, be its conjugacy classes, and let $x_i \in C_i$, $1 \leq i \leq n$, be arbitrary. Furthermore, let us assume that each of the classes C_i , $1 \leq i \leq r$, contains at least two elements, while the remaining classes C_i , $r+1 \leq i \leq n$, are one-element. Then*

$$|G| = |Z(G)| + \sum_{i=1}^r [G : N(x_i)]. \quad \blacksquare$$