Lecture Notes

in

Group Theory

Gunnar Traustason
(Autumn 2016)

0 Introduction. Groups and symmetry

Group Theory can be viewed as the mathematical theory that deals with symmetry, where symmetry has a very general meaning. To illustrate this we will look at two very different kinds of symmetries. In both case we have 'transformations' that help us to capture the type of symmetry we are interested in. We then have the 'objects' that we are analysing and to each object we will associate a 'symmetry group' that captures the symmetric properties of the object in precise mathematical terms.

I. Isometric symmetry in $\mathbb{R}^2$

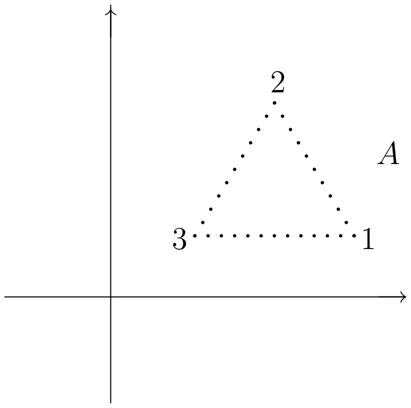
Transformations: Isometries.

An isometry on the plane is a bijection $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distances.

Objects: Figures in the place (that is subsets of the plane).

The symmetry group of a figure A: For any figure(subset) A of the plane, we let G_A be the set of all isometries that preserve the figure (as a set). This is a group with composition as the group multiplication. We call it the *symmetry group* of A.

Example



For the equilateral triangle A, G_A consists of three rotations r, r^2 and $r^3 = e = \text{id}$, with r being a counterclockwise rotation of 120 degrees around the center of A, and three reflections s_1, s_2 and s_3 with respect to the three symmetry axes of A, through the points 1, 2 and 3 respectively.

We can now write a multiplication table for G_A:

	e	r	r^2	s_1	s_2	s_3
e	e	r	r^2	s_1	s_2	s_3
r	r	r^2	e	s_3	s_1	s_2
r^2	r^2	e	r	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r	r^2
s_2	s_2	s_3	s_1	r^2	e	r
s_3	s_3	s_1	s_2	r	r^2	e

Every equilateral triangle in the plane has a group G of isometries that contains three rotations and three reflections as above. It depends on the triangle what exactly these rotations and reflections are but the algebraic structure is always going to be as in the multiplication table above. So the symmetry is captured in the algebraic structure of G.

In fact the group above is ismorphic to S_3, the group of all permutations of $1, 2, 3$. This is because the 6 elements in G_A permute the corner points of the triangle and all the $6 = 3!$ permutations of S_3 occur: r and r^2 correspond to (1 2 3) and (1 3 2) and the three reflections s_1, s_2 and s_3 correspond to the (2 3), (1 3) and (1 2).

The following questions now arise naturally:

(Q1) What symmetries are out there?
(Q2) What are their properties?

Or, translating these into formal mathematics questions:

(q1) What groups are there? (Classification)
(q2) What is their structure like? (Structure theory)

The symmetry we have just looked at is of geometric nature and groups and geometry have some strong links. For example, one can think of Euclidean geometry in the plane as the theory that studies properties that are invariant under isometries (i.e. angle, length, area, triangle, ...). During the 19th century there was a development of a number of different geometries (i.e. affine geometry, projective geometry, hyperbolic geometry, ...) and Felix Klein (1872) made the general observation that, like Euclidean geometry can be characterised by the group of isometries, each geometry can be characterised by some group of transformations. The origin of abstract group theory goes however further back to Galois (1811-1832) and the problem of solving polynomial equations by algebraic methods. This we turn to next.

II. Arithmetic symmetry in $\mathbb{C}$. The origin of group theory.

Transformations: Automorphisms.

A automorphism on $\mathbb{C}$ is a bijective function $f : \mathbb{C} \rightarrow \mathbb{C}$ that preserves the addition and the multiplication:

$$\begin{aligned} f(a+b) &= f(a)+f(b) \\ f(ab) &= f(a)f(b). \end{aligned}$$

Claim. Any automorphism f fixes all the elements in $\mathbb{Q}$.

Proof. Firstly $f(0) = 0$ and $f(1) = 1$ as

$$\begin{array}{l} f(0) + 0 = f(0) = f(0+0) = f(0) + f(0) \\ f(1) \cdot 1 = f(1) = f(1 \cdot 1) = f(1) \cdot f(1). \end{array}$$

and cancellation gives what we want. Notice that we can cancel by $f(1)$ as it can't be 0 (f is bijective and 0 is already taken as a value). Next suppose that $n \geq 1$ is an integer. Then

$$f(n) = f(\underbrace{1+1+\cdots+1}_{n}) = \underbrace{f(1)+f(1)+\cdots+f(1)}_{n} = \underbrace{1+1+\cdots+1}_{n} = n$$

and $f(n) = n$ for all positve integers n. Before going further we observe that f has the property that $f(-a) = -f(a)$ and also that $f(1/a) = 1/f(a)$ whenever $a \neq 0$. The reason for this is the following

$$\begin{array}{l} f(a) + f(-a) = f(a + (-a)) = f(0) = 0 \\ f(a) \cdot f(1/a) = f(a \cdot 1/a) = f(1) = 1. \end{array}$$

Using this we can now finish the proof of the claim. Firstly for $n > 0$ we have $f(-n) = -f(n) = -n$ which shows that f fixes any integer. Finally if $q = a/b$ for some integers a, b, where $b \neq 0$, then

$$f(q) = f(a \cdot 1/b) = f(a) \cdot f(1/b) = f(a) \cdot 1/f(b) = a/b = q$$

and we have proved the claim. $\Box$

Objects: Polynomials in $\mathbb{Q}[x]$.

Let

$$P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

be a polynomial over $\mathbb{Q}$ with distinct roots $x_1, \ldots, x_n$.

Claim. Any automorphism f permutes the complex roots of P.

Proof. We need to show that if t is a root then $f(t)$ is also a root. But this follows from

$$\begin{array}{rcl} 0 & = & f(0) \\ & = & f(a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0) \\ & = & f(a_n t^n) + f(a_{n-1}t^{n-1}) + \cdots + f(a_0) \\ & = & f(a_n)f(t)^n + f(a_{n-1})f(t)^{n-1} + \cdots + f(a_0) \\ & = & a_n f(t)^n + a_{n-1}f(t)^{n-1} + \cdots + a_0 \\ & = & P(f(t)) \end{array}$$

where the 2nd last equality follows from the fact that the coefficients are rational numbers. $\Box$

We have seen that any isomorphism f must permute the roots $x_1, \ldots, x_n$ of P. Hence f induces a permutation in S_n (if we identify $1, 2, \ldots, n$ with $x_1, \ldots, x_n$).

The symmetry group of the polynomial P. (Also called the Galois group of P): We let

$$G_P = \{\sigma \in S_n : \sigma \text{ is induced by an isomorphism }\}.$$

G_P is then the symmetry group of P.

(By saying that $\sigma \in S_n$ is induced by the automorphism $f : \mathbb{C} \to \mathbb{C}$ means that $\sigma(i) = j$ if and only if $f(x_i) = x_j$).

Example 1. Determine G_P where $P = x^2 - 3x + 2$.

Solution. $P = x^2 - 3x + 2 = (x-1)(x-2)$ has only rational roots so every isomorphism must fix these and thus induce the trivial permutation on the roots. Thus $G_P = \{\text{id}\}$.

Example 2. Determine G_P where $P = x^4 - 1$.

Solution. The polynomial $P = x^4 - 1$ has the roots $x_1 = 1$, $x_2 = -1$, $x_3 = i$ and $x_4 = -i$. Here all isomorphisms must fix 1 and -1. This leaves the possibility of swapping i and $-i$, and the isomorphism f on $\mathbb{C}$ that maps z to $\bar{z}$ does that (recall that $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a} \cdot \overline{b}$ which implies that f is a isomorphism). Thus

$$G_P = \{\alpha, \text{id}\}$$

where

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_4 & x_3 \end{pmatrix}$$

or, under the identification of $1, 2, 3, 4$ with x_1, x_2, x_3, x_4,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

i.e. α swaps x_3 and x_4 (or 3 and 4).

Remark. In general G_P is a subgroup of S_n and thus thas at most $n!$ elements (in fact $|G_P|$ divides $|S_n| = n!$ by Lagrange's Theorem).

We say that a polynomial P is solvable by radicals if its roots can be expressed using only the coefficients, the arithmetic operations and extracting roots. That any quadratic $ax^2 + bx + c$ is solvable by radicals is for example a consequence of the formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Such formulas for solving the cubics and the quartics were discovered during the 16th century but despite much effort the quintic continued to remain a challenge. The question was not settled until 1824 when the Norwegian mathematican Niels Henrik Abel demonstrated that the quintic is not in general solvable by radicals. The French mathematician

Évariste Galois (1811-1832) proved this independently and went further by finding a sufficient and necessary condition under which a given polynomial is solvable by radicals. In doing so he developed a new mathematical theory of symmetry, namely group theory. His famous theorem is the following:

Theorem (Galois). A polynomial P is solvable by radicals iff G_P is solvable.

For a group to be solvable means having a structure of a special kind. You will see the precise definition later in the course.

Fact. For each positive integer n there exists a polynomial P_n of degree n such that $G_{P_n} = S_n$ (all the permutations of the n roots).

Theorem. S_n is solvable iff $n \leq 4$. (We will prove this later in the course).

Corollary. For any $n \geq 5$ there exists a polynomial of degree n (namely P_n) that is not solvable by radicals.

1 Definitions and basic properties

I. The group axioms and some examples of groups.

We start by recalling the definition of a group.

Definition. A *group* is a pair $(G, *)$, where G is a set, $*$ is a binary operation and the following axioms hold:

(a) (The associative law)

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in G.$$

(b) (Existence of an identity) There exists an element $e \in G$ with the property that

$$e * a = a \text{ and } a * e = a \text{ for all } a \in G.$$

(c) (The existence of an inverse) For each $a \in G$ there exists an element $b \in G$ such that

$$a * b = b * a = e.$$

Remark. Notice that $* : G \times G \to G$ is a binary operation and thus the 'closure axiom': $a, b \in G \Rightarrow a * b \in G$ is implicit in the definition.

Definition. We say that a group $(G, *)$ is *abelian* or *commutative* if $a * b = b * a$ for all $a, b \in G$.

Remarks.(1) Recall that the identity e is the unique element in G with the property given in (b). To see this suppose we have another identity f. Using the fact that both of these are identities we see that

$$f = f * e = e.$$

we will usually denote this element by 1 (or by 0 if the group operation is commutative).

(2) the element $b \in G$ as in (c) is unique. To see this suppose that c is another inverse to a. Then

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

We call this unique element b, the inverse of a. It is often denoted a^{-1} (or $-a$ when the group operation is commutative).

(3) If it is clear from the context what the group operation $*$ is, one often simply refers to the group G rather then the pair $(G, *)$.

Some examples of groups. (1) Let X be a set and let $\mathrm{Sym}\,(X)$ be the set of all bijective maps from X to itself. Then $\mathrm{Sym}\,(X)$ is a group with respect to composition, $\circ$, of maps. This group is called the *symmetric group* on X and we often refer to the elements of $\mathrm{Sym}\,(X)$ as *permutations* of X. When $X = \{1, 2, \cdots, n\}$ the group is often denoted S_n and called the *symmetric group on n letters*.

(2) Let $(R, +, \cdot)$ be any ring. Then $(R, +)$ is an abelian group. This includes for example the *group of integers* $(\mathbb{Z}, +)$ and the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with repect to addition. It also includes, for any positive integer n, the *group of integers modulo n* $(\mathbb{Z}_n, +)$.

(3) Let again $(R, +, \cdot)$ be any ring with unity 1. Then the set of all invertible elements (the *units*), R^*, is a group with respect to the ring multiplication $\cdot$. This group is referred to as the *group of units* of R. This includes $\mathbb{Q}^*$, $\mathbb{R}^*, \mathbb{C}^*$ and $\mathbb{Z}_n^*$ for any positive integer.

(4) Let V be a finite dimensional vector space over a field K. Consider the ring $\mathrm{End}\,(V)$ of all linear operators $\alpha : V \to V$. Here the group of units is denoted $\mathrm{GL}(V)$ and called the *general linear group on V*.

(5) Let K be a field and let $M_n(K)$ be the ring of all $n \times n$ matrices over K. The group of units here is denoted $\mathrm{GL}_n(K)$ and called the *general linear group* of $n \times n$ matrices over K.

Remarks. (1) We will see later that any group G can be viewed as a subgroup of some group of permutations $\mathrm{Sym}\,(X)$.

(2) One can see that any group G can be viewed as a subgroup of the group of units of some ring R. We will see this later at least in the case when G is finite.

II. Subgroups and Lagrange's Theorem.

Definition. Let G be a group with a subset H. We say that H is a *subgroup* of G if the following two conditions hold.

(a) $1 \in H$,
(b) If $a, b \in H$ then $ab, a^{-1} \in H$.

Recall. One can replace (a) and (b) with the more economical:

(a)' $H \neq \emptyset$,
(b)' If $a, b \in H$ then $ab^{-1} \in H$.

Remark. It is not difficult to see that one could equivalently say that H is a subgroup of G if H is closed under the group multiplication $*$ and that H with the induced multiplication of $*$ on H is a group in its own right. So subgroups are groups contained within G that inherit the multiplication from G.

Notation. We write $H \leq G$ or $G \geq H$ for 'H is a subgroup of G'.

Cosets as equivalence classes. Suppose G is a group with a subgroup H. We define a relation $\simeq$ on G as follows:

$$x \simeq y \text{ iff } x^{-1}y \in H.$$

This relation is an equivalence relation. To see this we need to see that it is reflexive, symmetric and transitive. Firstly it is reflexive as $x^{-1}x = 1 \in H$ implies that $x \simeq x$. To see that it is symmetric suppose $x \simeq y$. Then $x^{-1}y \in H$ and as H is a subgroup it follows that $y^{-1}x = (x^{-1}y)^{-1} \in H$ and thus $y \simeq x$. Finally to see that the relation is transitive notice that if $x \simeq y$ and $y \simeq z$ then $x^{-1}y, y^{-1}z \in H$. Being a subgroup, H is closed under the group multiplication and thus $x^{-1}z = (x^{-1}y)\cdot(y^{-1}z) \in H$. Thus $x \simeq z$.

Notice that $x \simeq y$ if and only if $x^{-1}y \in H$ if and only if $y \in xH$. Hence the equivalence class of x is $[x] = xH$, the left coset of H in G.

Theorem 1.1 *(Lagrange) Let G be a finite group with a subgroup H. Then $|H|$ divides $|G|$.*

Proof Using the equivalence relation above, G gets partitioned into pairwise disjoint equivalence classes, say

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

and adding up we get

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r \cdot |H|.$$

Notice that the map from G to itself that takes g to a_ig is a bijection (the inverse is the map $g \mapsto a_i^{-1}g$) and thus $|a_iH| = |H|$. $\Box$

Remark. If we had used instead the relation $x \simeq y$ iff $xy^{-1} \in H$, we would have had $[x] = Hx$. Hence G also partions into a pairwise disjoint union of right cosets. (Recall that in general the partions into right cosets and into left cosets are different).

Examples. (1) The subsets $\{1\}$ and G are always subgroups of G.

(2) The subset $C_n = \{a \in \mathbb{C} : a^n = 1\}$ is a subgroup of $(\mathbb{C}, \cdot)$. In fact $1^n = 1$ and if $a, b \in C_n$ then $(ab)^n = a^nb^n = 1$ and $(a^{-1})^n = (a^n)^{-1} = 1$. Thus both the subgroup criteria (a) and (b) hold.

(3) $H = \{\text{id}, (1,\ 2)\}$ is a subgroup of S_3. Clearly (a) holds as id $\in H$ and direct inspection shows that (b) holds as well.

Definition. Let G be a group and $a \in G$. The *cyclic subgroup* generated by a is $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Remark. We have that $1 = a^0 \in \langle a \rangle$. We also have that $\langle a \rangle$ is closed under the group multiplication and taking inverses since $a^n \cdot a^m = a^{n+m}$ and $(a^n)^{-1} = a^{-n}$. Hence $\langle a \rangle$ is a subgroup of G. It is clearly the smallest subgroup of G that contains a.

Definition. We say that a group G is cyclic if there exists an element $a \in G$ where $G = \langle a \rangle$.

Definition. Let G be a group and $a \in G$. The order of a, denoted $o(a)$, is defined as follows. If there is a positive integer m such that $a^m = 1$ then $o(a)$ is the smallest such integer. If there is on the other hand no such positive integer we say that a is of infinite order and write $o(a) = \infty$.

Remarks.(1) If $o(a) = n < \infty$, then

$$\langle a \rangle = \{1 = a^0, a^1, \ldots, a^{n-1}\}$$

where the elments $1, a, a^2, \ldots, a^{n-1}$ are distinct. To see why the elements are different suppose for a contraction that $a^r = a^s$ for some $0 \leq r < s \leq n-1$. But then $a^{s-r} = 1$ where $0 < s - r \leq n - 1 < n$. This however contradicts the fact that $n = o(a)$ is the smallest positive integer where $a^n = 1$.

(2)Thus $o(a) = n = |\langle a \rangle|$. Note also that $a^m = 1$ iff $n|m$. It follows that $a^r = a^s$ if and only if $n|(r-s)$. (The structure of the group is just like that of $\mathbb{Z}_n$).

(3) Let G be a finite group and $a \in G$. As $o(a) = |\langle a \rangle|$ that divides $|G|$ by Lagrange, we have from Remark (2) that $a^{|G|} = 1$.

Let $G = \langle a \rangle$ be a finite cyclic group. By Lagrange any subgroup has a order d that is a divisor of n. For cyclic groups there is conversely exactly one subgroup of order d for each divisor d.

Proposition 1.2 *Let $G = \langle a \rangle$ be a finite cyclic group of order n and let d be a divisor of n. The subgroup $\langle a^{n/d} \rangle$ is the unique subgroup of order d.*

Proof. Let H be a subgroup of order d. As $\langle a^{n/d} \rangle$ has also d elements it suffices to show that $H \subseteq \langle a^{n/d} \rangle$. Let $a^m \in H$. By Remark (3) above we have $1 = a^{m|H|} = a^{md}$ and, by Remark (2), it follows that $n = o(a)$ divides md. Hence n/d divides m, say $m = r \cdot (n/d)$, and $a^m = (a^{n/d})^r \in \langle a^{n/d} \rangle$. $\Box$

Proposition 1.3 *Let p be a prime number and G be a group such that $|G| = p$. The group G is cyclic.*

Proof As $p \geq 2$ there has to be some element $a \neq 1$ in G. Then $|\langle a \rangle| \geq 2$ and (by Lagrange's Theorem) $|\langle a \rangle|$ divides $|G| = p$. As p is a prime we must have $|\langle a \rangle| = p$ and thus $\langle a \rangle = G$. $\Box$.

III. Congruences and quotient groups.

Definition. Let G be a group. A *congruence* on G is an equivalence relation $\simeq$ on G that satisfies:

$$a_1 \simeq a_2, b_1 \simeq b_2 \Rightarrow a_1 b_1 \simeq a_2 b_2.$$

Remark. This extra condition is needed to introduce a well defined multiplication on the equivalence classes $[a] \cdot [b] = [ab]$.

Lemma 1.4 *Let G be a group with congruence $\simeq$. Then $N = [1]$ is a subgroup of G that satisfies:*

$$g^{-1}Ng \subseteq N$$

for all $g \in G$. Furthermore $a \simeq b$ if and only if $a^{-1}b \in N$.

Proof. To see that N is a subgroup, we go through the subgroup criteria. As $\simeq$ is reflexive we have $1 \simeq 1$ and thus $1 \in N = [1]$. It remains to see that N is closed under group multiplication and taking inverses. For the first of these, notice that of $a, b \in N$ then $a, b \simeq 1$ and the congruence property gives us that $ab \simeq 1 \cdot 1 = 1$. Thus $ab \in N$. To see that N is closed under taking inverses, suppose that $a \in N$ then $a \simeq 1$ and the congruence property gives us that $1 = a^{-1}a \simeq a^{-1} \cdot 1 = a^{-1}$. This shows that $a^{-1} \in N$.

It remains to see that N has the requested extra property. So suppose $a \in N$. Then $a \simeq 1$ and the congruence property implies that $g^{-1}ag \simeq g^{-1} \cdot 1 \cdot g = 1$. Hence $g^{-1}ag \in N$. Finally we have $a \simeq b$ iff $1 = a^{-1}a \simeq a^{-1}b$ iff $a^{-1}b \in [1] = N$. □

Definition. A subgroup H of G is said to be a normal subgroup if

$$g^{-1}Hg \subseteq H \quad \forall g \in G.$$

Notation. We write $H \trianglelefteq G$ or $G \trianglerighteq H$ for 'H is a normal subgroup of G'

Lemma 1.5 *Let G be a group with a normal subgroup N and define a relation $\simeq$ on G by $x \simeq y$ if and only if $x^{-1}y \in N$. Then $\simeq$ is a congruence on G and $[a] = aN$. In particular $[1] = N$.*

Proof We have seen in the proof of Lagrange's Theorem that $\simeq$ is an equivalence relation and that $[a] = aN$. It remains to see that the congruence property holds. So suppose that $a_1 \simeq a_2$ and $b_1 \simeq b_2$. This means that $a_1^{-1}a_2, b_1^{-1}b_2 \in N$. We want to show that $a_1b_1 \simeq a_2b_2$. But this follows from

$$(a_1b_1)^{-1}(a_2b_2) = b_1^{-1}(a_1^{-1}a_2)b_2 = (b_1^{-1}b_2) \cdot b_2^{-1}(a_1^{-1}a_2)b_2.$$

As N is normal we have that $b_2^{-1}(a_1^{-1}a_2)b_2 \in N$ and thus the equation above shows that $(a_1b_1)^{-1}a_2b_2$ is a product of two elements from N. As N is a subgroup of G, this product is in N. Hence $a_1b_1 \simeq a_2b_2$. □

Remark. It follows from Lemmas 1.4 and 1.5 that there is a 1-1 correspondence between congruences on G and normal subgroups of G.

Remarks. (1) We write often more shortly H^a instead of $a^{-1}Ha$ and call it a *conjugate* of H by a. Similarly if $x \in G$ then $x^a = a^{-1}xa$ is a *conjugate* of x by a.

(2) Let $x, a, b \in G$ and 1 be the identity element in G. Then

$$\begin{aligned} &x^{ab} = (ab)^{-1}xab = b^{-1}(a^{-1}xa)b = (x^a)^b \\ &x^1 = 1^{-1} \cdot x \cdot 1 = x. \end{aligned}$$

It follows then that if $H \leq G$ we also have $H^{ab} = (H^a)^b$ and $H^1 = H$.

(3) Notice that H^a is a subgroup of G: firstly $1 = a^{-1} \cdot 1 \cdot a = 1^a \in H^a$ and then $x^a y^a = a^{-1}xaa^{-1}ya = a^{-1}(xy)a = (xy)^a$ and $(x^a)^{-1} = (a^{-1}xa)^{-1} = a^{-1}x^{-1}a = (x^{-1})^a$. In fact the group H^a has the same structure as H. (The conjugation by a is a bit like a renaming or an ornament).

Lemma 1.6 *The following are equivalent:*

(a) $H \trianglelefteq G$,
(b) $H^a = H$ *for all* $a \in G$,
(c) $Ha = aH$ *for all* $a \in G$.

Proof (b)⇒(a) is obvious. To prove (a)⇒(b), notice that (a) implies in particular that for any $a \in G$ we have $H^{a^{-1}} \subseteq H$ and therefore

$$H = H^e = H^{a^{-1}a} = (H^{a^{-1}})^a \subseteq H^a.$$

This gives $H^a = H$. It now only remains to show that (b)⇔(c). But this is easy

$$a^{-1}Ha = H \ \Leftrightarrow a \cdot a^{-1}Ha = aH \ \Leftrightarrow Ha = aH.$$

This finishes the proof. □

Definition. Let G be a group with a subgroup H. The number of left cosets of H in G is called the *index* of H in G and is denoted $[G : H]$.

Remark. Suppose that G is finite. Recall from the proof of Lagrange's Theorem that we get a partition of G into a union of pairwise disjoint union of left cosets

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

As each of the cosets have order $|H|$, it follows that $|G| = r \cdot |H|$. Hence $[G : H] = r = |G|/|H|$. (Likewise we have that G can be written as a pairwise disjoint union of right cosets and the same reasoning shows that their number is also $|G|/|H|$.

Examples. (1) Every subgroup N of an abelian group G is normal (since then obviously $aN = Na$ for all $a \in G$).

(2) The trivial subgroup $\{1\}$ and G itself are always normal subgroups of G.

(3) If H is a subgroup of G such that $[G : H] = 2$ then $H \trianglelefteq G$ (since the left cosets are $H, G \setminus H$ which are also the right cosets. Hence the right cosets are the same as the left cosets).

The quotient group G/N. Let G be a group with a congruence $\simeq$ and a corresponding normal subgroup N. Let

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

with a binary operation $[a] \cdot [b] = [ab]$ (that is $aN \cdot bN = abN$). Notice that this is well defined as $\simeq$ is a congruence. To see that G/N is a group with respect to this binary operation we check that the three group axioms hold.

Firstly there is an identity element, namely $[1] = N$ as $[1] \cdot [a] = [1 \cdot a] = [a]$ and

$[a] \cdot [1] = [a \cdot 1] = [a]$.

Secondly every element $[a] \in G/N$ has an inverse, namely $[a^{-1}]$ since $[a] \cdot [a^{-1}] = [a \cdot a^{-1}] = [1]$ and $[a^{-1}] \cdot [a] = [a^{-1} \cdot a] = [1]$.

Finally associativity in G/N follows from associativity in G:

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

Remark. That the binary operation on G/N is well defined followed from the fact that $\simeq$ is a congruence. There is another way of seeing this using the fact that N is normal in G. First we introduce set products in the natural way. So if $X, Y \subseteq G$ then we let $X \cdot Y = \{xy : \, x \in X, y \in Y\}$. Then, using this set product as the action on G/N, we get

$$[a] \cdot [b] = aN \cdot bN = abNN = abN = [ab].$$

Hence the binary operation (being the same as the set multiplication) is well defined. Notice that we used the fact that N is normal when applying $Nb = bN$. Also $N \cdot N \subseteq N$ as N is a subgroup and $N = N \cdot \{1\} \subset N \cdot N$ as $1 \in N$. Thus $N \cdot N = N$.

Remark. Notice that the size of the group G/N is $[G : N]$ and when G is finite this is the same as $|G|/|N|$.

Examples. (1) We always have $G \trianglelefteq G$. The congruence with respect to the normal subgroup G is $x \simeq y \Leftrightarrow x^{-1}y \in G$. As the latter holds for any $x, y \in G$ we are identifying all the elements. Hence

$$G/G = \{[1]\} = \{G\}$$

is the trivial group with only one element.

(2) The trivial subgroup $N = \{1\}$ is always normal in G. The congruence in this case is given by $x \simeq y \Leftrightarrow x^{-1}y \in N \Leftrightarrow x^{-1}y = 1 \Leftrightarrow y = x$. Thus

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

The structure is just like the structure of G: $\{a\} \cdot \{b\} = \{ab\}$. (The curly bracket is there just as a decoration).

(3) Let $G = S_3 = \{\text{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ and $N = A_3 = \{\text{id}, (1\,2\,3), (1\,3\,2)\}$. Here $[G : N] = 2$ and thus G/N has two elements. Notice that these are

$$N = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} = [\text{id}] = [(1\ 2\ 3)] = [(1\ 3\ 2)]$$

and

$$(1\ 2)N = \{(1\ 2), (2\ 3), (1\ 4)\} = [(1\ 2)] = [(1\ 3)] = [(2\ 3)].$$

(So here we have identified all the even permutations and likewise all the odd permutations). $G/N = \{1 = [\text{id}],\ a = [(1\ 2)]\}$. This is the unique group structure with 2 elements: $1 \cdot a = a \cdot 1 = a$, $1 \cdot 1 = 1$ and $a \cdot a = 1$.

IV. Homomorphisms and isomorphisms

Definition. Let G, H be groups. A map $\phi : G \to H$ is a *homomorphism* if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Furthermore ϕ is an *isomorphism* if it is bijective. A group G is said to be *isomorphic to* H if there is an isomorphism $\phi : G \to H$. We then write $G \cong H$.

Remarks. (1) If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms then their composition $\psi \circ \phi : G \to K$ is also a homomorphism. This is simply because $\psi(\phi(ab)) = \psi(\phi(a) \cdot \phi(b)) = \psi(\phi(a)) \cdot \psi(\phi(b))$. In particular if $G \cong H$ and $H \cong K$ then $G \cong K$.

(2) If $\phi : G \to H$ is an isomorphism then $\phi^{-1} : H \to G$ is also an isomorphism. To see this let $a = \phi(x), b = \phi(y) \in H$. Then

$$\phi^{-1}(a \cdot b) = \phi^{-1}(\phi(x) \cdot \phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(a) \cdot \phi^{-1}(b).$$

In particular if $G \cong H$ then also $H \cong G$.

(3) If $G \cong H$ then there is no structural difference between G and H. You can think of the isomorphism $\phi : G \to H$ as a renaming function. If $ab = c$ then $\phi(a), \phi(b), \phi(c)$ are the new a, b, c. We want the new c to be the product of the new a and b. This means $\phi(ab) = \phi(a)\phi(b)$.

Lemma 1.7 *Let $\phi : G \to H$ be a homomorphism, then*

(a) $\phi(1_G) = 1_H$,
(b) $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof (a) We have

$$1_H \cdot \phi(1_G) = \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G)$$

and cancellation gives $1_H = \phi(1_G)$.

(b) Using (a) we have

$$\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1_G) = 1_H$$

and

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_G) = 1_H.$$

Hence $\phi(a^{-1})$ is the inverse of $\phi(a)$. $\Box$

Examples (1) Let N be a normal subgroup of G. The map $\phi : G \to G/N,\ a \mapsto [a] = aN$ is a homomorphism as $\phi(ab) = [ab] = [a] \cdot [b] = \phi(a) \cdot \phi(b)$.

(2) Let $\mathbb{R}^+$ be the set of all the postive real numbers. There is a (well known) isomorphism $\phi : (\mathbb{R}, +) \to \mathbb{R}^+, \cdot)$ given by $\phi(x) = e^x$. (As $e^{x+y} = e^x e^y$. This is a bijective

homomorphism).

Lemma 1.8 *Let $\phi : G \to H$ be a homomorphism, then*

(a) $A \leq G \;\Rightarrow\; \phi(A) \leq H$.
(b) $B \leq H \;\Rightarrow\; \phi^{-1}(B) \leq G$.
(c) $B \trianglelefteq H \;\Rightarrow\; \phi^{-1}(B) \trianglelefteq G$.

Proof To prove (a) and (b) we apply the usual three subgroup criteria, i.e. the subset in question needs to contain the identity and be closed under multiplication and taking inverses. For (a) this follows from $1_H = \phi(1_G)$, $\phi(x)\phi(y) = \phi(xy)$ and $\phi(x)^{-1} = \phi(x^{-1})$. Notice that, as $A \leq G$, we have $1_G \in A$ and $xy, x^{-1} \in A$ whenever $x, y \in A$. Similarly for proving (b), it is first clear that $1_G \in \phi^{-1}(B)$ as $\phi(1_G) = 1_H \in B$ (since $B \leq H$). Furthermore, if $x, y \in \phi^{-1}(B)$, then $\phi(x), \phi(y) \in B$. As $B \leq H$, it follows that $\phi(xy) = \phi(x)\phi(y) \in B$ and $\phi(x^{-1}) = \phi(x)^{-1} \in B$. This shows that $xy, x^{-1} \in \phi^{-1}(B)$.

For the proof of part (c) suppose furthermore that the subgroup B of H is normal. Let $x \in \phi^{-1}(B)$ and $g \in G$. Then $\phi(g^{-1}xg) = \phi(g)^{-1}\phi(x)\phi(g) \in \phi(g)^{-1}B\phi(g) \subseteq B$. Hence $g^{-1}xg \in \phi^{-1}(B)$. This shows that $\phi^{-1}(B)$ is normal in G. □.

V. The Isomorphism Theorems

Let $N \trianglelefteq G$ and consider the homomorphism $\phi : G \to G/N,\ a \mapsto [a] = aN$. Let

$$\mathcal{S}_N(G) = \{H :\ N \leq H \leq G\}$$

and

$$\mathcal{S}(G/N) = \{R :\ R \leq G/N\}.$$

Consider the map $\Psi : \mathcal{S}_N(G) \to \mathcal{S}(G/N),\ \Psi(H) = \phi(H) = H/N$.

Remark. Thus $\Psi(H)$ is the set $\phi(H) = \{\phi(a) : a \in H\}$.

Theorem 1.9 *(Correspondence Theorem). Ψ is a bijection and furthermore $H \trianglelefteq G$ iff $\Psi(H) \trianglelefteq G/N$.*

Proof. (Ψ is injective). Let $N \leq H, K \leq G$ and suppose that $\Psi(H) = H/N$ is equal to $\Psi(K) = K/N$. Then

$$H = \bigcup_{xN \in H/N} xN = \bigcup_{xN \in K/N} xN = K.$$

(Ψ is surjective). Let R be a subgroup of G/N. Then, by Lemma 1.8, $\phi^{-1}(R)$ is a subgroup of G (that clearly contains N as all the elements in N map to the identity element of G/N that is in R) and as ϕ is surjective, we have

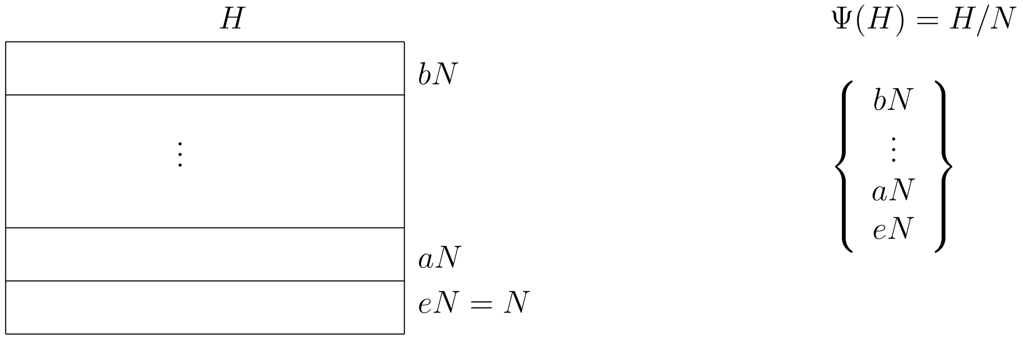
$$\Psi(\phi^{-1}(R)) = \phi(\phi^{-1}(R)) = R.$$

(Notice that $N \subseteq H$ implies that $N = g^{-1}Ng \subseteq g^{-1}Hg$ and thus the subgroup $g^{-1}Hg$ is also in $\mathcal{S}_N(G)$). This shows that Ψ is a bijection. Finally we are going to use

$$\Psi(g^{-1}Hg) = \phi(g^{-1}Hg) = \phi(g)^{-1}\phi(H)\phi(g) = \phi(g)^{-1}\Psi(H)\phi(g).$$

We have that $H \trianglelefteq G$ iff $g^{-1}Hg = H$ for all $g \in G$. As Ψ is a bijection this holds iff $\Psi(g^{-1}Hg) = \Psi(H)$ for all $g \in G$. In view of the identity above this holds iff $\phi(g)^{-1}\Psi(H)\phi(g) = \Psi(H)$ for all $g \in G$. But as ϕ is surjective this is true iff $r^{-1}\Psi(H)r = \Psi(H)$ for all $r \in G/N$ that is iff $\Psi(H) \trianglelefteq G/N$. $\Box$

The picture that is good to keep in mind is the following.


H
bN
$\vdots$
aN
$eN = N$
$\Psi(H) = H/N$
$\left\{ \begin{array}{c} bN \\ \vdots \\ aN \\ eN \end{array} \right\}$

$\Psi(H)$ is the collection of all the cosets of N in H and H is the pairwise disjoint union of these cosets. Thus if we know H we get $\Psi(H)$ as the cosets of N in H and if we know $\Psi(H)$ we get H as the union of the cosets in $\Psi(H)$.

Definition. Let $\phi : G \to H$ be a group homomorphism. The *image* of ϕ is

$$\operatorname{im}\phi = \{\phi(g) : \, g \in G\}$$

and the *kernel* of ϕ is

$$\ker\phi = \{g \in G : \phi(g) = 1\}.$$

Notice that as $G \leq G$, it follows from Lemma 1.8 that $\operatorname{im}\phi = \phi(G)$ is a subgroup of H. Also, as $\{1\} \trianglelefteq H$ it follows from Lemma 1.8 that $\ker\phi = \phi^{-1}(\{1\})$ is a normal subgroup of G.

Theorem 1.10 *(1st Isomorphism Theorem). Let $\phi : G \to H$ be a homomorphism. Then $Im\,\phi \leq H$, $Ker\,\phi \trianglelefteq G$ and*

$$G/Ker\,\phi \cong Im\,\phi.$$

Proof As we have noted previously, it follows from Lemma 1.8 that $\operatorname{Im}\phi \leq H$ and $\operatorname{Ker}\phi \trianglelefteq G$. Define a map $\Phi : G/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ by setting $\Phi([a]) = \phi(a)$. This map is clearly surjective. We next show that it is well defined and injective. This follows from

$$\begin{aligned}
\Phi([a]) = \Phi([b]) \;&\Leftrightarrow\; \phi(a) = \phi(b) \\
&\Leftrightarrow\; \phi(a^{-1}b) = \phi(a)^{-1}\phi(b) = 1 \\
&\Leftrightarrow\; a^{-1}b \in \operatorname{Ker}\phi \\
&\Leftrightarrow\; [a] = [b]
\end{aligned}$$

To show that Φ is an isomorphism, it remains to show that Φ is a homomorphism. This follows from

$$\Phi([a]\cdot[b]) = \Phi([ab]) = \phi(ab) = \phi(a)\phi(b) = \Phi([a])\cdot\Phi([b]).$$

This finishes the proof. □

Theorem 1.11 *(2nd Isomorphism Theorem). Let $H \leq G$ and $N \trianglelefteq G$. Then $HN \leq G$, $H \cap N \trianglelefteq H$ and*

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

Proof We apply the 1st Isomorphism Theorem. Consider the homomorphism

$$\phi : G \to G/N,\ a \mapsto aN.$$

Let ψ be the restriction of ϕ on H. This gives us a homomorphism $\psi : H \to G/N$. By the 1st Isomorphism Theorem we have that $\operatorname{Im}\psi = \{hN : h \in H\}$ is a subgroup of G/N. By the correspondence theorem we have that this subgroup is of the form U/N, where U is a subgroup of G that is given by

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

Thus $\operatorname{Im}\psi = HN/N$. It remains to identify the kernel. The identity of G/N is the coset $eN = N$. Then for $h \in H$, we have

$$\begin{aligned} \psi(h) = N \quad &\Leftrightarrow \quad hN = N \\ &\Leftrightarrow \quad h \in N. \end{aligned}$$

As $h \in H$ this shows that the kernel of ψ is $H \cap N$. Thus by the 1st Isomorphism Theorem, $H \cap N \trianglelefteq H$ and

$$H/H \cap N = H/\operatorname{Ker}\psi \simeq \operatorname{Im}\psi = HN/N$$

This finishes the proof. □

Theorem 1.12 *(3rd Isomorphism Theorem). Suppose that $H, N \trianglelefteq G$ and $N \leq H$. Then $H/N \trianglelefteq G/N$ and*

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

Proof Again we apply the 1st Isomorphism Theorem. This time on the map

$$\phi : G/N \to G/H\, aN \mapsto aH.$$

Let us first see that this is well defined. If $aN = bN$ then $a^{-1}b \in N \subseteq H$ and thus $aH = bH$. It is also a homomorphism as

$$\phi(aN \cdot bN) = \phi(abN) = abH = aH \cdot bH = \phi(aN) \cdot \phi(bN).$$

We clearly have that $\operatorname{Im}\phi = G/H$ and it remains to identify the kernel. The identity in G/H is the coset $eH = H$ and then

$$\begin{aligned} \phi(aN) = H \quad &\Leftrightarrow \quad aH = H \\ &\Leftrightarrow \quad a \in H. \end{aligned}$$

The kernel thus consists of the cosets aN of G/N where $a \in H$. That is the kernel is H/N. The 1st Isomorphism Theorem now gives us that $H/N \trianglelefteq G/N$ (that we had proved already in the proof of the correspondence theorem anyway) and that

$$(G/N)/(H/N) = (G/N)/\operatorname{Ker}\phi \cong \operatorname{Im}\phi = G/H.$$

This finishes the proof. □

2 Direct products and abelian groups

I. Direct products.

Closure properties for the set of normal subgroups of G.

(1) If $H, K \trianglelefteq G$ then $H \cap K \trianglelefteq G$. To see that this is a subgroup notice that $1 \in H$ and $1 \in K$ as both are subgroups and hence $1 \in H \cap K$. Now let $a, b \in H \cap K$. As $H \leq G$ and $a, b \in H$ we know that $ab, a^{-1} \in H$. Similarly as K is a subgroup, containing a, b, we have $ab, a^{-1} \in K$. Thus $ab, a^{-1} \in H \cap K$. To see $H \cap K$ is normal notice that for $g \in G$, we have $(H \cap K)^g \subseteq H^g = H$ and $(H \cap K)^g \subseteq K^g = K$ and thus $(H \cap K)^g \subseteq H \cap K$.

(2) We also have that if $H, K \trianglelefteq G$ then $HK \trianglelefteq G$: It follows from the 2nd Isomorphism Theorem that $HK \leq G$. To see that HK is normal notice that we have $(HK)^g = H^g K^g = HK$ for $g \in G$.

Normal products. We have seen that if $H, K \trianglelefteq G$ then $HK \trianglelefteq G$. Inductively it follows that if $H_1, \ldots, H_n \trianglelefteq G$, then $H_1 \cdots H_n \trianglelefteq G$. Since $H_i H_j = H_j H_i$ for $1 \leq i < j \leq n$, we have

$$H_{\sigma(1)} \cdots H_{\sigma(n)} = H_1 \cdots H_n$$

for all $\sigma \in S_n$.

Lemma 2.1 *Let H and K be finite subgroups of G where K is normal. Then*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Proof By the 2nd Isomorphism Theorem, we have

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

Taking the orders on both sides gives. $|HK|/|K| = |H|/|H \cap K|$. The result follows immediately from this. $\Box$.

Remark. In particular it follows that $|HK| = |H| \cdot |K|$ if and only if $H \cap K = \{1\}$.

Definition Let $H_1, \ldots, H_n \trianglelefteq G$. The product $H_1 \cdots H_n$ is said to be an (internal) *direct product* of $H_1, \ldots, H_n$ if

$$H_i \cap \prod_{j \neq i} H_j = \{1\}$$

for $i = 1, \ldots, n$.

Remark. Suppose $1 \leq i < j \leq n$. As $H_j \leq \prod_{k \neq i} H_k$, we know in particular that

$H_i \cap H_j = \{1\}$ it follows from Exercise 1 on sheet 2 that all the elements in H_i commute with all the elements in H_j. So if $x_i \in H_i$ then

$$x_{\sigma(1)} \cdots x_{\sigma(n)} = x_1 \cdots x_n$$

for all $\sigma \in S_n$.

Proposition 2.2 *Let $H_1, \ldots, H_n \trianglelefteq G$ and suppose that $H_1 H_2 \cdots H_n$ is an internal direct product.*

(a) Every element $a \in H_1 \cdots H_n$ is of the form

$$a = x_1 x_2 \cdots x_n$$

for unique $x_i \in H_i$, $i = 1, \ldots, n$.
(b) If $x_i, y_i \in H_i$ for $i = 1, \ldots, n$ then

$$x_1 \cdots x_n \cdot y_1 \cdots y_n = (x_1 y_1) \cdots (x_n y_n).$$

Proof (a) If $x_1 \cdots x_n = y_1 \cdots y_n$ for some $x_i, y_i \in H_i$, then for each $1 \leq i \leq n$

$$x_i \prod_{j \neq i} x_j = y_i \prod_{j \neq i} y_j$$

and thus

$$y_i^{-1} x_i = (\prod_{j \neq i} y_j) \cdot (\prod_{j \neq i} x_j)^{-1}$$

and thus $y_i^{-1} x_i$ is in $H_i \cap \prod_{j \neq i} H_j = \{1\}$ and $x_i = y_i$.

(b) Using the fact that y_i commutes with x_j when $j > i$ we have

$$\begin{aligned} x_1 x_2 \cdots x_n y_1 y_2 \cdots y_n &= x_1 y_1 x_2 \cdots x_n y_2 \cdots y_n \\ &\vdots \\ &= (x_1 y_1)(x_2 y_2) \cdots (x_n y_n). \end{aligned}$$

This finishes the proof. □

Remarks. (1) The last Proposition shows that the structure of the internal direct product $H_1 H_2 \cdots H_n$ only depends on the structure of $H_1, \ldots, H_n$. Each element is like an n-tuple $(x_1, \ldots, x_n)$ and we multiply two such componentwise. Later we will formalise this when we introduce the external direct product.

(2) Notice that it follows from part (a) of last proposition that for an internal direct product $H_1 H_2 \cdots H_n$, we have

$$|H_1 \cdots H_n| = |H_1| \cdots |H_n|.$$

The internal direct products are useful for helping us sorting out the structure of a given group. Next we discuss external direct products that are useful for constructing new groups from old groups.

Definition. Let $H_1, \ldots, H_n$ be groups. The (external) *direct product* of $H_1, \ldots, H_n$ is the cartesian set product

$$H_1 \times \cdots \times H_n$$

with multiplication

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Remark. Since each H_i is a group it is immediate that the direct product is also a group with identity $(1_{H_1}, \ldots, 1_{H_n})$. The inverse of $(a_1, a_2, \ldots, a_n)$ is $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$. The associatative law follows from the fact that it holds in each component.

Next result tells us that the internal direct product is the same as the external direct product.

Lemma 2.3 *Suppose G is the internal direct product of $H_1, \ldots, H_n$. Then*

$$G \cong H_1 \times \cdots \times H_n.$$

Proof (See sheet 4)

II. Abelian groups.

In this section, we will use additive notation. Thus we use $+$ for the group operation, $-a$ for the inverse of a and 0 for the group identity. We also talk about direct sums rather than direct products.

Notice that every subgroup of an abelian group G is normal. Thus for subgroups $H_1, H_2, \ldots, H_n$ of G we have that $H_1 + \cdots + H_n$ is an internal direct sum of $H_1, \ldots, H_n$ if

$$H_i \cap \sum_{j \neq i} H_j = \{0\}$$

for $i = 1, \ldots, n$. The external direct sum of $H_1, \ldots, H_n$ is also denoted

$$H_1 \oplus H_2 \oplus \cdots \oplus H_n$$

instead of $H_1 \times H_2 \times \cdots \times H_n$.

The cyclic group generated by a, $\langle a \rangle = \{na : n \in \mathbb{Z}\}$, will often be denoted $\mathbb{Z}a$.

Definition. Let G be any abelian group and let p be a prime. The subset

$$G_p = \{x \in G : \ o(x) \text{ is a power of } p\}$$

is called the *p-primary subgroup* of G.

Lemma 2.4 *G_p is a subgroup of G.*

Proof As the order of 0 is $1 = p^0$, it is clear that $0 \in G_p$. Now let $x, y \in G_p$ with orders p^n, p^m. Then $p^{\max\{n,m\}}(x+y) = p^{\max\{n,m\}}x + p^{\max\{n,m\}}y = 0 + 0 = 0$ and thus $o(x+y)$ divides $p^{\max\{n,m\}}$ and is thus also a power of p. Hence $x + y \in G_p$ and as $o(-x) = o(x) = p^n$ we also have that $-x \in G_p$. Hence $G_p \leq G$. □

Remark. If G is finite then $|G_p|$ must be a power of p. This follows from Exercise 4(a) on sheet 3. If there was another prime $q \neq p$ that divided $|G_p|$ then by this exercise we would have an element in G_p of order q but this contradicts the definition of G_p.

Definition. An abelian group is said to be a *p-group* if $G = G_p$.

Next lemma reduces the study of finite abelian groups to the study of finite abelian groups of prime power order.

Lemma 2.5 *Let G be a finite abelian group where $|G| = p_1^{r_1} \cdots p_n^{r_n}$ for some positive integers $r_1, \ldots, r_n$. Then G is the internal direct sum of $G_{p_1}, G_{p_2}, \ldots, G_{p_n}$. Furthermore $|G_{p_i}| = p_i^{r_i}$.*

Proof Let $x \in G$. Then by Lagrange's Theorem $o(x)$ divides $|G|$, say $o(x) = p_1^{s_1} \cdots p_n^{s_n}$. The numbers

$$q_1 = \frac{o(x)}{p_1^{s_1}}, \ldots, q_n = \frac{o(x)}{p_n^{s_n}}$$

are then coprime and we can find integers $a_1, \ldots, a_n$ such that $a_1 q_1 + \cdots + a_n q_n = 1$. Thus

$$x = (a_1 q_1 + \cdots + a_n q_n)x = a_1 q_1 x + \cdots + a_n q_n x$$

and as $p_i^{s_i}(a_i q_i x) = a_i o(x) x = 0$ we have that $a_i q_i x \in G_{p_i}$. Thus $G = G_{p_1} + \cdots + G_{p_n}$. To see that the sum is direct let $x \in G_{p_i} \cap \sum_{j \neq i} G_{p_j}$, say

$$x = x_i = \sum_{j \neq i} x_j$$

where the order of x_k is p^{e_k}. Then $p_i^{e_i} x = 0$ and also $(\prod_{j \neq i} p_j^{e_j})x = 0$ and the order of x divides two coprime numbers. Hence $o(x) = 1$ and thus $x = 0$. This shows that the intersection is trivial and hence we have a direct sum.

By the remark made before the Lemma, we know that $|G_{p_i}| = p_i^{s_i}$ for some integer s_i. Since G is the direct sum of $G_{p_1}, \ldots, G_{p_n}$, we have

$$p_1^{r_1} \cdots p_n^{r_n} = |G| = \prod_{i=1}^{n} |G_{p_i}| = p_1^{s_1} \cdots p_n^{s_n}.$$

Comparison of the two sides gives $s_i = r_i,\ i = 1, \ldots, n$. □

Remark. Thus $G \cong G_{p_1} \oplus \cdots \oplus G_{p_n}$. And the study of finite abelian groups reduces to understanding the finite abelian p-groups.

Definition. Let G be a finite group. The *exponent* of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$. (Or with additive notation $nx = 0$ for all $x \in G$).

Abelian groups of exponent p as vector spaces. Let G be a finite abelian group of exponent p. Then $px = 0$ for all $x \in G$ and the group addition induces a scalar multiplication from the field Z_p as follows. For $[m] = m + \mathbb{Z}p$ we let $[m]x = mx = \underbrace{x + \cdots + x}_{m}$. This is well defined and turns G into a vector space over $\mathbb{Z}_p$. One also has that a subset H of G is a subgroup of the group G if and only if H is a subspace of the vector space G. (See Sheet 5, exercise 1 for the details).

Lemma 2.6 *Let G be a finite abelian group of exponent p. Then G can be written as an internal direct sum of cyclic groups of order p.*

Proof Viewing G as a vector space over $\mathbb{Z}_p$ we know that it has a basis $x_1, \ldots, x_n$ as all these elements are non-trivial and as the exponent of G is p, they must all be of order p. To say that these elements form a basis for the vector space G is the same as saying that we have a direct sum of one dimensional subspaces

$$G = \mathbb{Z}_p x_1 + \cdots + \mathbb{Z}_p x_n.$$

This happens if and only if

$$\mathbb{Z}_p x_j \cap \sum_{k \neq j} \mathbb{Z}_p x_k = \{0\}$$

for $j = 1, \ldots, n$. But as $\mathbb{Z}_p x_k = \mathbb{Z} x_k$, this is the same as saying that

$$\mathbb{Z} x_j \cap \sum_{k \neq j} \mathbb{Z} x_k = \{0\}$$

for $j = 1, \ldots, n$ which is the same as saying that

$$G = \mathbb{Z} x_1 + \cdots + \mathbb{Z} x_r$$

is an internal direct sum of cyclic subgroup of order p. $\Box$.

Remark. If we have the direct sum $G = \mathbb{Z} x_1 + \cdots + \mathbb{Z} x_n$ then $|G| = p^n$. The number of direct summands is thus unique and is $\log_p(|G|)$.

Lemma 2.7 *We have that sum $H_1 + \cdots + H_n$ is direct if and only if for any $x_i \in H_i$, $i = 1, \ldots, n$ we have*

$$x_1 + \cdots + x_n = 0 \Rightarrow x_1 = \ldots = x_n = 0.$$

Proof To prove this, notice first that a direct sum would have this property by Proposition 2.2. Conversely, suppose that this property holds and take some $x_i = \sum_{j \neq i}(-x_j)$ in $H_i \cap \sum_{j \neq i} H_j$. Then $x_1 + \cdots + x_n = 0$ and thus $x = x_i = 0$ by the property. So the intersection is trivial and the sum is direct. $\Box$.

Proposition 2.8 *Let G be a finite abelian p-group. G can be written as an internal direct sum of non-trivial cyclic groups. Furthermore the number of cyclic summands of any given order is unique for G.*

Proof (See later).

From Lemma 2.5 and Proposition 2.8 we can derive the main result of this chapter.

Theorem 2.9 *(The Fundamental Theorem for finite abelian groups). Let G be a finite abelian group. G can be written as an internal direct sum of non-trival cyclic groups of prime power order. Furthermore the number of cyclic summands for any given order is unique for G.*

Remark. Suppose that $G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$ is a direct sum of cyclic group of prime power order. Notice that

$$G = \mathbb{Z}x_{\sigma(1)} + \mathbb{Z}_{\sigma(2)} + \cdots + \mathbb{Z}_{\sigma(n)}$$

for all $\sigma \in S_n$.

Convention. We order the cyclic summands as follows. First we order them with respect to the primes involved in ascending order. Then for each prime we order the summands in ascending order.

Example. If G is finite abelian group written as an internal direct sum

$$G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4 + \mathbb{Z}x_5$$

of cyclic groups of orders $9, 2, 4, 3, 4$, then we order the summands so that they come instead in orders $2, 4, 4, 3, 9$. Notice then that G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

Remarks. (1) This discussion shows that any finite abelian group is isomorphic to a unique external direct sum

$$\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$$

where $p_1 \leq p_2 \leq \cdots \leq p_r$ and if $p_i = p_{i+1}$ then $e_i \leq e_{i+1}$.

(2) Finding all abelian groups of a given order $n = p_1^{m_1} \cdots p_r^{m_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes, reduces then to the problem of finding, for $i = 1, \ldots, r$, all possible partitions $(p_i^{e_1}, \ldots, p_i^{e_l})$ of the number $p_i^{m_i}$. This means that

$$1 \leq e_1 \leq e_2 \leq \ldots \leq e_l \text{ and } e_1 + \cdots + e_l = m_i.$$

Example. Find (up to isomorphism) all abelian groups of order 72.

Solution. We have $72 = 2^3 \cdot 3^2$. The possible partitions of 2^3 are (8), $(2, 4)$, $(2, 2, 2)$ whereas the possible partions for 3^2 are (3^2), $(3, 3)$. We then have that the abelian groups of order 72 are

$$\begin{array}{lll} \mathbb{Z}_8 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{array}$$

We now turn to the proof of Proposition 2.8. First as a preparation here are two subgroups that will play an important part in the proof.

Some useful subgroups. Let G be a finite abelian group. The following subgroups are going to play an important role in the proof of our next main result. That these are subgroups is shown on exercise sheet 3 (using multiplicative notation).

$$PG = \{px : x \in G\}, \quad G[p] = \{x \in G : px = 0\}.$$

As $G[p]$ is of exponent p it can be viewed as a vector space over $\mathbb{Z}_p$.

Proof of Proposition 2.8 First we deal with the existence of such a decomposition into a direct sum.

Let the exponent of G be p^n. We prove the proposition by induction on n. If $n = 1$ then the result holds by Lemma 2.6. Now suppose that $n \geq 2$ and that the result holds for smaller values of n. The exponent of pG is p^{n-1} and by the induction hypothesis we have that pG is a direct sum of non-trivial cyclic groups, say

$$pG = \mathbb{Z}px_1 + \cdots + \mathbb{Z}px_r. \tag{1}$$

Suppose the order of x_i is p^{m_i} (notice that $m_i \geq 2$ as $px_i \neq 0$). Then $p^{m_1-1}x_1, \ldots, p^{m_r-1}x_r$ are in $G[p]$. As $G[p]$ is of exponent p, it can be viewed as a vector space over $\mathbb{Z}_p$ and we can then extend to a basis $(p^{m_1-1}x_1, \ldots, p^{m_r-1}x_r, x_{r+1}, \ldots, x_s)$ for $G[p]$. It follows that we have a direct sum

$$G[p] = \mathbb{Z}p^{m_i-1}x_1 + \cdots + \mathbb{Z}p^{m_r-1}x_r + \mathbb{Z}x_{r+1} + \cdots + \mathbb{Z}x_s. \tag{2}$$

We now want to show that $G = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$ is a direct sum.

First we show that $x_1, \ldots, x_s$ generate G. Let $x \in G$. Then by (1)

$$px = a_1px_1 + \cdots + a_rpx_r$$

for some integers $a_1, \ldots, a_r$. Thus $x - (a_1x_1 + \cdots + a_rx_r)$ is in $G[p]$ and thus by (2) in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$. Hence x is also in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$.

It remains to see that the sum $G = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$ is direct. Suppose that

$$a_1x_1 + \cdots + a_sx_s = 0.$$

We want to show that $a_1x_1 = \ldots = a_sx_s = 0$. Now multiplying by p we get

$$a_1px_1 + \cdots + a_rpx_r = 0$$

and since the $\mathbb{Z}px_1 + \cdots + \mathbb{Z}px_r$ is direct, it follows that $pa_1x_1 = \ldots = pa_rx_r = 0$. Thus p^{m_j-1} divides a_j for $j = 1, \ldots, r$, say $a_j = b_jp^{m_j-1}$. So we have

$$b_1p^{m_1-1}x_1 + \cdots + b_rp^{m_r-1}x_r + a_{r+1}x_{r+1} + \ldots + a_sx_s = 0.$$

As $G[p] = \mathbb{Z}p^{m_1-1}x_1 + \cdots + \mathbb{Z}p^{m_r-1}x_r + \mathbb{Z}x_{r+1} + \cdots + \mathbb{Z}x_s$ is direct we must have $b_1p^{m_1-1}x_1 = \ldots = b_rp^{m_r-1}x_r = a_{r+1}x_{r+1} = \ldots = a_sx_r = 0$. That is $a_1x_1 = \ldots = a_sx_s = 0$. This finishes the inductive proof.

To deal with uniqueness part, write G as a direct sum of cyclic groups of p-power order

$$G = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_r + \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_s$$

where $a_1, \dots, a_r$ have order at most p^{m-1} whereas $b_1, \dots, b_s$ have order at least p^m (notice that as G is a p-group the orders of all these elements are powers of p). Then

$$|\frac{p^{m-1}G}{p^mG}| = \frac{|\mathbb{Z}p^{m-1}b_1| \cdots |\mathbb{Z}p^{m-1}b_s|}{|\mathbb{Z}p^m b_1| \cdots |\mathbb{Z}p^m b_s|} = \frac{o(p^{m-1}b_1)}{o(p^m b_1)} \cdots \frac{o(p^{m-1}b_s)}{o(p^m b_s)}.$$

Notice that, in a finite abelian p-group, we have that if $a \neq 0$ then $o(pa) = \frac{1}{p}o(a)$ (If p^l is the order of a then p^{l-1} is the order of pa). The formula above thus implies that

$$|\frac{p^{m-1}G}{p^mG}| = p^s$$

and thus the number of summands of order at least p^m is $\log_p |\frac{p^{m-1}G}{p^mG}|$. Similarly the number of summands of order at least p^{m+1} is $\log_p |\frac{p^mG}{p^{m+1}G}|$. The number of summands of order exactly p^m is thus the difference

$$\log_p |\frac{p^{m-1}G}{p^mG}| - \log_p |\frac{p^mG}{p^{m+1}G}|.$$

This shows that the number of summands of order exactly p^m is an invariant that does not depend on what the decomposition is. □

3 Composition series and solvable groups

I. Simple groups. The primes of group theory.

We now introduce an important notion, namely that of a simple group. These can be thought of as the atoms or the primes of group theory.

Definition. A group G is simple if $G \neq \{1\}$ and the only normal subgroups of G are $\{1\}$ and G.

Example. The abelian simple groups are the cyclic groups of prime order. See exercise sheet 6.

Remark. Look at Exercise 5 on sheet 4. According to this exercise we have that if G is a direct product of non-abelian simple groups, then the simple factors are unique up to order (and not only up to isomorphism!). Thus we had here something analogous to a unique prime factorisation of a number. When we also allow for abelian simple factors the result would be similar and we get that the factors are unique (this time up to isomorphism). The problem is that not all finite groups can be written as direct products of simple groups. Example is S_3 and $\mathbb{Z}_4$. It turns out that any finite group can still in a different sense been built out of simple groups. To describe what this means we need to talk first about composition series.

Definition. Let G be a group.

(1) A *subnormal series* of G is a series

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_n = G$$

where $H_{i-1} \trianglelefteq H_i$, $i = 1, \ldots, n$. The quotient groups

$$H_1/H_0, H_2/H_1, \ldots, H_n/H_{n-1}$$

are called the *factors* of the series.

(2) A subnormal series is called a *composition series* if

$$H_1/H_0, H_2/H_1, \ldots, H_n/H_{n-1}$$

are simple groups, called the *composition factors*.

Example. Let $G = \mathbb{Z}a$ be a cyclic group of order 6. Then the subgroup $3G$ is of order 2 and index 3 and we get a subnormal series

$$\{0\} \leq 3G \leq G$$

with factors $3G/\{0\} \cong \mathbb{Z}_2$ and $G/3G \cong \mathbb{Z}_3$. Similarly the subgroup $2G$ is a subgroup of order 3 and index 2 that gives us another subnormal series

$$\{0\} \leq 2G \leq G$$

with factors $2G/\{0\} \cong \mathbb{Z}_3$ and $G/2G \cong \mathbb{Z}_2$. In fact these are both composition series as the factors are simple. Notice that the composition factors turn out to be the same (up to order). In fact this is always true.

The Jordan-Hölder Theorem. *Suppose that a group G has composition series*

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

and

$$\{1\} = K_0 < K_1 < \ldots < K_m = G.$$

Then $n = m$ and the composition factors $H_1/H_0, \ldots, H_n/H_{n-1}$ are the same (up to order) as $K_1/K_0, \ldots, K_n/K_{n-1}$.

Remarks. (1) Let G be a group with a normal subgroup N. It follows from the correspondence theorem that G/N is simple iff $G \neq N$ and there is no normal subgroup M in G such that $N < M < G$.

(2) Suppose that for some group G we have a subnormal series

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

that is not a composition series. Then some quotient H_m/H_{m-1} is not simple and by remark (1) there exists some subgroup K of G such that $H_{m-1} < K < H_m$ where K is normal in H_m. Notice also that (as H_{m-1} is normal in H_m) H_{m-1} is normal in K. By adding K, we thus get a subnormal series that is longer.

(3) Let G be a finite group. It has a subnormal series (for example $\{1\} < G$). Applying remark (2) we can continue adding terms while the series is not a composition series. Each time we get a longer series and as G is finite, this procedure must terminate in a composition series for G. Hence every finite group has a composition series.

Examples (1) G be an internal direct product of $S_1, \ldots, S_n$ where S_i is simple. The map

$$\phi : S_1 \cdots S_n \to S_n,\ a_1 a_1 \cdots a_n \mapsto a_n$$

is a group homomorphism with kernel $S_1 \cdots S_{n-1}$. By the first Isomorphism Theorem we have

$$\frac{S_1 \cdots S_n}{S_1 \cdots S_{n-1}} \cong S_n$$

we thus get a compostion series

$$\{0\} < S_1 < S_1 S_2 < \ldots < S_1 \cdots S_n = G$$

with composition factors $\frac{S_1 \cdots S_i}{S_1 \cdots S_{i-1}} \cong S_i$. This shows that there exists at least one group with $S_1, \ldots, S_n$ as composition factors. (We can take $S_1 \times S_2 \times \cdots \times S_n$).

(2) Let n be a positive intger. All finite abelian groups of order n have the same composition factors (Sheet 6). So normally there are a number of different groups that have some given composition factors $S_1, \ldots, S_n$.

The Jordan Hölder theorem suggests the following possible strategy for finding all finite groups.

(a) Find all the simple groups.
(b) For any given choice $S_1, \ldots, S_r$ of simple groups find all the possible groups G whose composition factors are $S_1, \ldots, S_r$.

Remarks. (1) Classifying all finite groups is generally concidered too hard. These are too rich and for a given choice of simple groups $S_1, \ldots, S_n$ there is a great variety of ways of obtaining a group G with these as composition factors. As the number, n, of simple factors increases this becomes more and more complicated.

(2) On the other hand (a) is done! This is one of the real triumphs of 20th century mathematics. The classification result was announced in 1981. The proof is a collection of a number of journal articles by many different mathematicians and runs over 10000 journal pages!

According to the classification of finite simple groups, these are

(1) The cyclic groups of prime order, $\mathbb{Z}_p$,
(2) The alternating groups, $A_n, n \geq 5$,
(3) The simple groups of Lie type (a number of infinite families that crop up in a geometrical context)
(4) Twenty six exceptional groups that do not belong to any of the infinite families above.

The groups in (1) are dealt with on sheet 6. In the next chapter we deal with (2).

II. Solvable groups

Definition. We say that a group is solvable if it has a subnormal series with abelian factors.

Examples (1) Every abelian group is solvable.
(2) We have that S_3 has a composition series

$$\{1\} < A_3 < S_3$$

with factors $A_3/\{1\} \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$. As the factors are abelian S_3 is solvable.

Remark. We will see on sheet 6 that S_4 is solvable. In next chapter we will however see that S_n is not solvable for $n \geq 5$. This is the underlying reason for the fact that we can't solve the quintic by radicals.

Proposition 3.1 *A finite group G is solvable if and only its composition factors are cyclic of prime order.*

Proof ($\Leftarrow$). A composition series with abelian factors is a subnormal series with abelian factors.

($\Rightarrow$). Suppose G is finite solvable group with subnormal series

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

where the factors are abelian. If this series is not a composition series, then some factor H_i/H_{i-1} is not simple and we can insert some K, such that $H_{i-1} < K < H_i$, to get a longer series. Notice that $K/H_{i-1} \leq H_i/H_{i-1}$ and thus abelian. Also we have by the 3rd Isomorphism Theorem that

$$H_i/K \cong \frac{H_i/H_{i-1}}{K/H_{i-1}}$$

that is a quotient of the abelian group H_i/H_{i-1} and thus abelian. Thus the new longer series also has abelian factors. Continuing adding terms until we get a composition series, gives us then a composition series with abelian factors and thus factors that are cyclic of prime order. □

How common are finite solvable groups? In fact surprisingly common. We mention two famous results.

Theorem A (Burnside's (p,q)-Theorem, 1904) Let p, q be prime numbers. Any group of order $p^n q^m$ is solvable.

Theorem B. (The odd order Theorem, Feit-Thompson, 1963). Any group of odd order is solvable.

(This is really a magnificent result. The proof is almost 300 pages and takes up a whole issue of a mathematics journal. Thompson received the Field's medal for his contribution).

4 Permutation groups and group actions

I. Permutation groups and the simplicity of A_n, $n \geq 5$

Convention. We will work with permutations from right to left. So if $\alpha, \beta \in S_n$ then for $\alpha\beta$, we apply β first and then α.

Lemma 4.1 *Let $\alpha \in S_n$. Then*

$$\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1} = (\alpha(i_1)\ \alpha(i_2)\ \ldots\ \alpha(i_m)).$$

Proof First suppose that $k = \alpha(j)$ is not in $\{\alpha(i_1),\, \alpha(i_2),\, \cdots, \alpha(i_m)\}$. Then j is not in $\{i_1,\, i_2,\, \cdots, i_m\}$ and

$$\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1}(\alpha(j)) = \alpha(i_1\ i_2\ \ldots\ i_m)(j) = \alpha(j).$$

This shows that $\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1}$ fixes the elements outside $\{\alpha(i_1),\, \alpha(i_2),\, \cdots, \alpha(i_m)\}$. It remains to show that this map cyclically permutes $\alpha(i_1),\, \alpha(i_2),\, \cdots, \alpha(i_m)$. But

$$\alpha(i_1\ i_2\ \cdots\ i_m)\alpha^{-1}(\alpha(i_r)) = \alpha(i_1\ i_2\ \cdots\ i_m)(i_r) = \alpha(i_{r+1})$$

where i_{m+1} is interpreted as i_1. This finishes the proof. $\Box$

Orbits. Let $i \in \{1, \ldots, n\}$. Recall that the α-orbit containing i is the subset $\{\alpha^r(i) : r \in \mathbb{Z}\}$ and that $\{1, \ldots, n\}$ partitions into a pairwise disjoint union of α-orbits.

Cycle structure. Suppose that the orbits of $\alpha \in S_n$ are $O_1, O_2, \ldots, O_r$ of sizes $l_1 \geq l_2 \geq \cdots \geq l_r$. We then say that α has a cycle structure of type $(l_1, \ldots, l_r)$.

Example. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\ 3\ 4\ 2\ 5)(6\ 7)(8).$$

Then α is of type $(5, 2, 1)$.

Definition. Let G be a group and $x \in G$. The *conjugacy class* of G containing x is $x^G = \{x^g : g \in G\}$.

On sheet 6, we see that G is a pairwise disjoint union of its conjugacy classes.

By Lemma 4.1, we have that if α is a permutation of some type $(l_1, \ldots, l_r)$, then the conjugacy class α^{S_n} consists of all permutations of that type. It follows also that if a normal subgroup N contains a permutation of type $(l_1, l_2, \ldots, l_r)$ then it contains all permutations of that type.

Example. $[(1\ 2)(3\ 4)]^{S_4} = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.

Remarks. We have the following formula (check it)

$$(i_1\ i_2\ \cdots i_m) = (i_1\ i_m)(i_1\ i_{m-1})\cdots(i_1\ i_2). \tag{3}$$

Remark As every permutation in S_n can be written as a product of disjoint cycles, this formula implies that every permutation in S_n can be written as a product of 2-cycles.

Recall. A permutation $\alpha \in S_n$ is said to be even/odd if it can be written as a product of even/odd number of 2-cycles. We also know that no permutation is both even and odd and thus S_n gets partitioned into even and odd elements. We denote by A_n the collection of all even elements. This is a subgroup that contains half the elements of S_n and for any odd element a in S_n, we have

$$S_n = A_n \cup aA_n.$$

In particular A_n is of index 2 in S_n and is thus normal.

Remark. By (3) we have that $(i_1\ \cdots\ i_m)$ is a even/odd permutation if and only if m is odd/even.

Remark Any even permutation in A_n can be written as a product of even number of 2-cycles. So every permutation in A_n is a product of elements of one the following forms (for i, j, r and s distinct)

$$(i\ j)(i\ r) = (i\ r\ j)$$

$$(i\ j)(r\ s) = (i\ j)(i\ r)(r\ i)(r\ s) = (i\ r\ j)(r\ s\ i).$$

It follows that any permutation in A_n can be written as a product of 3-cycles.

Lemma 4.2

(a) If $N \trianglelefteq S_n$ contains a 2-cycle then $N = S_n$.
(b) If $N \trianglelefteq A_n$ contains a 3-cycle then $N = A_n$.

Proof (a) Let $(i_1\ i_2)$ be a 2-cycle of N. Let $(j_1\ j_2)$ be any other 2-cycle of S_n. Let α be a permutation that maps i_k to j_k. By Lemma 4.1 we have that $(j_1\ j_2) = \alpha(i_1\ i_2)\alpha^{-1}$ which being a conjugate of $(i_1\ i_2)$ is also in N. So every 2-cycle is in N and as S_n is generated by 2-cycles it follows that $N = S_n$.

(b) The proof is similar. Let $(i_1\ i_2\ i_3)$ be a 3-cycle of N and let $(j_1\ j_2\ j_3)$ be any other 3-cycle of A_n. Let $\alpha \in S_n$ be a permutation that maps i_k to j_k. If $\alpha \in A_n$ then $(j_1\ j_2\ j_3) = \alpha(i_1\ i_2\ i_3)\alpha^{-1}$ is in N as before. If α on the other hand is odd then consider first instead $\beta = (j_1\ j_2)\alpha \in A_n$. The element

$$(j_2\ j_1\ j_3) = \beta(i_1\ i_2\ i_3)\beta^{-1}$$

is then in N and then also $(j_1\ j_2\ j_3) = (j_2\ j_1\ j_3)^{-1}$. So all the 3-cycles are contained in N and as A_n is generated by the 3-cycles, it follows that $N = A_n$. $\Box$

Lemma 4.3 *Suppose $n \geq 5$ and that $\{id\} \neq N \trianglelefteq A_n$. Then $|N| > n$.*

Proof As $N \neq \{\text{id}\}$, we have some $\text{id} \neq x \in N$. It suffices to show then x^{A_n} has at least n elements since then N would contain these elements plus the identity and thus more than n elements. Write x as a product of disjoint cycles and suppose that the longest cycle in the product has length m. There are two possibilities.

Case 1. $m \geq 3$.

Here x is of the form

$$x = (i\ j\ k\ \cdots)y$$

where $(i\ j\ k\ \cdots)$ is one of the cycles of longest length and y is the product of the remaining cycles. Now take any distinct $r, s, t, u, v \in \{1, 2, \ldots, n\}$. Let $\alpha \in S_n$ such that $\alpha(i) = r$, $\alpha(j) = s$ and $\alpha(k) = t$. Notice that by Lemma 4.1, we have

$$x^{\alpha^{-1}} = (r\ s\ t\ ...)y^{\alpha^{-1}}.$$

The same is true if α is replaced by $(u\ v)\alpha$ (notice that we are using $n \geq 5$ here), so we can assume that α is even. It follows that we can choose r, s, t to be any elements in $\{1, 2, \ldots, n\}$ that we like. We can now easily find at least n elments in x^{A_n}. For example we can take the elements

$$(1\ 2\ 3\ \cdots)y_1,\ (1\ 2\ 4\ \cdots)y_2,\ (1\ 3\ 2\ \cdots)y_3,\ (1\ 4\ 2\ \cdots)y_4,\ \cdots,\ (1\ n\ 2\ \cdots)y_n$$

Case 2. $m = 2$.

As x is even we have to have at least two 2-cycles in the product. It follows that

$$x = (i\ j)(k\ l)y$$

where $(i\ j), (k\ l)$ are two of the 2-cycles and y is the product of the remaining cycles.

Now take any distinct $r, s, t, u \in \{1, 2, \ldots, n\}$. Let $\alpha \in S_n$ such that $\alpha(i) = r$, $\alpha(j) = s$, $\alpha(k) = t$ and $\alpha(l) = u$. Notice that

$$x^{\alpha^{-1}} = (r\ s)(t\ u)y^{\alpha^{-1}}$$

and the same holds when α is replaced by $(r\ s)\alpha$ (as $(s\ r) = (r\ s)$). We can therefore again suppose that α is even. As r, s, t, u can be chosen arbitrarily we can now again easily find at least n elments in x^{A_n}. For example we can take these to be

$$(1\ 2)(3\ 4)y_1,\ (1\ 2)(3\ 5)y_2,\ (1\ 3)(2\ 4)y_3,\ (1\ 4)(2\ 3)y_4,\ \cdots,\ (1\ n)(2\ 3)y_n.$$

So in both cases we have at least n elments in x^{A_n} and as N also contains the identity element, it follows that N has at least $n + 1$ elements. $\Box$

Theorem 4.4 *The group A_n is simple for $n \geq 5$.*

Proof We prove this by induction on $n \geq 5$. The induction basis, $n = 5$, is dealt with on Sheet 7. Now for the induction step, suppose $n \geq 6$ and that we know that A_{n-1} is simple. Let $G(n) = \{\alpha \in A_n : \alpha(n) = n\}$. Notice that $G(n) \cong A_{n-1}$ and thus simple by induction hypothesis. Now let $\{\mathrm{id}\} \neq N \trianglelefteq A_n$, we want to show that $N = A_n$.

Step 1. $N \cap G(n) \neq \{\mathrm{id}\}$.

We argue by contradiction and suppose that $N \cap G(n) = \{\mathrm{id}\}$. This means that the only element in N that fixes n is id. Now take $\alpha, \beta \in N$ and suppose that $\alpha(n) = \beta(n)$. Then $\alpha^{-1}\beta(n) = \alpha^{-1}(\alpha(n)) = n$ and by what we have just said it follows that $\alpha^{-1}\beta = \mathrm{id}$ or $\alpha = \beta$. Hence, a permutation α in N is determined by $\alpha(n)$ and since there are at most n values, we have that $|N| \leq n$. But his contradicts Lemma 4.3.

Step 2. $N = A_n$.

Now $\{\mathrm{id}\} \neq N \cap G(n) \trianglelefteq G(n)$ (by the 2nd Isomorphism Theorem) and since $G(n)$ is simple by induction hypothesis, it follows that $N \cap G(n) = G(n)$. In particular, N contains a 3-cycle and thus $N = A_n$ by Lemma 4.2. □

II. Group actions

Theorem 4.5 *(Cayley). Any group G is isomorphic to a subgroup of Sym (G).*

Proof For $a \in G$ consider the map $L_a : G \to G, x \mapsto ax$. Notice that L_a is bijective with inverse $L_{a^{-1}}$ and thus $L_a \in \mathrm{Sym}\,(G)$. Now consider the map

$$\phi : G \to \mathrm{Sym}\,(G), a \mapsto L_a.$$

Notice that $(L_a \circ L_b)(x) = abx = L_{ab}(x)$ and thus $\phi(ab) = L_{ab} = L_a \circ L_b = \phi(a) \circ \phi(b)$. Thus ϕ is a homomorphism. This homomorphism is injective since if $\phi(a) = \phi(b)$ then $a = a \cdot 1 = L_a(1) = L_b(1) = b \cdot 1 = b$. Thus G is ismorphic to $\mathrm{im}\,\phi$ where the latter is a subgroup of Sym (G). □

Definition. Let X be a set and G a group. We say that X is a G-set if we have a right multiplication from G, i.e. a map

$$\phi : X \times G \to X, (x, g) \mapsto x \cdot g$$

satisfying

(a) $x \cdot 1 = x \quad \forall x \in X$
(b) $(x \cdot a) \cdot b = x \cdot (ab) \;\; \forall a, b \in G$ and $x \in X$.

Remark. One also says that G acts on X. Notice that $x \cdot g$ is just a notation for $\phi(x, g)$. Notice also that for every $a \in G$ we have that the map $X \to X : x \mapsto x \cdot a$ is a permutation with inverse $X \to X : x \mapsto x \cdot a^{-1}$.

Examples. (1) Let $X = G$ be a group. We can consider this as a G-set with respect to the natural right group multiplication $x * g = xg$. Clearly $x * 1 = x1 = x$ and $(x * a) * b = (xa)b = x(ab) = x * (ab)$ by the associativity in G.

(2) Let $H \leq G$ and let X be the collection of all the right cosets of H in G. We can again consider X as a G-set with respect to the natural right group multiplications $Hg{*}a = Hga$ again it is easy to see that $Hg{*}1 = Hg$ and $(Hg{*}a){*}b = Hg{*}(ab) = Hgab$.

(3) Let G be a group and $X = G$. We define a group action by G on X by letting $x * a = a^{-1}xa = x^a$. Then X becomes a G-set as $x^1 = x$ and $(x^a)^b = x^{ab}$.

(4) Let X be the collection of all the subgroups of G. We can consider X as a G-set with respect to the conjugation action. That is the right multiplication is given by $H * g = g^{-1}Hg = H^g$. Again X is a G-set.

Definition. Let X be a G-set. The *stabilizer* of $x \in X$ is

$$G_x = \{g \in G : \ x \cdot g = x\}$$

and the *G-orbit* of $x \in X$ is

$$x \cdot G = \{x \cdot g : \ g \in G\}.$$

Lemma 4.6 $G_x \leq G$

Proof Firstly by condition (a) we have $1 \in G_x$. Now suppose that $a, b \in G_x$. Using condition (b) we then have $x \cdot (ab) = (x \cdot a) \cdot b = x \cdot b = x$ and $ab \in G_x$. It remains to show that G_x is closed under taking inverses. But this follows from

$$x = x \cdot 1 = x \cdot (aa^{-1}) = (x \cdot a) \cdot a^{-1} = x \cdot a^{-1}.$$

This finishes the proof. □

Theorem 4.7 *(The Orbit Stabilizer Theorem). Let X be a G-set and $x \in X$. Let $\mathcal{H}$ be the collection of all the right cosets of G_x in G. The map*

$$\Psi : \mathcal{H} \to x \cdot G, \, G_x a \mapsto x \cdot a$$

is a bijection. In particular

$$|x \cdot G| = |\mathcal{H}| = [G : G_x].$$

(In other words the cardinality of the G-orbit generated by x is the same as the cardinality of the collection of the right cosets of G_x in G).

Proof $\underline{\Psi \text{ is well defined and injective}}$. We have

$$x \cdot a = x \cdot b \Leftrightarrow x \cdot ab^{-1} = x \Leftrightarrow ab^{-1} \in G_x \Leftrightarrow G_x b = G_x a.$$

As Ψ is clearly surjective, this finishes the proof. □

Proposition 4.8 *Let X be a G-set. The relation*

$$x \sim y \quad \textit{if} \quad y \in x \cdot G$$

is an equivalence relation on X and the equivalence classes are the G-orbits.

Proof As $x = x \cdot 1$ it is clear that $x \sim x$ and we have that $\sim$ is reflexive. Now suppose that $y = x \cdot a$. Then $x = y \cdot a^{-1}$. This shows that $\sim$ is symmetric. It now remains to show that $\sim$ is transitive. But if $y = x \cdot a$ and $z = y \cdot b$ then $x \cdot (ab) = (x \cdot a) \cdot b = y \cdot b = z$. Hence we get $x \sim z$ from $x \sim y$ and $y \sim z$ and this shows that $\sim$ is transitive and thus an equivalence relation.

Finally $x \sim y$ iff $y \in x \cdot G$. Hence the equivalence class containing x is the G-orbit $x \cdot G$. $\Box$

Corollary 4.9 *Suppose that the G-orbits of X are are $x_i \cdot G$, $i \in I$. Then*

$$|X| = \sum_{i \in I} [G : G_{x_i}].$$

Proof We have that $X = \cup_{i \in I} x_i G$ where the union in pairwise disjoint. Thus

$$|X| = \sum_{i \in I} |x_i \cdot G| = \sum_{i \in I} [G : G_{x_i}].$$

Where the final equality follows from the Orbit Stabilizer Theorem.

5 Finite groups and Sylow Theory

Definition. Let G be a group and $x \in G$. The *centralizer* of x in G is

$$C_G(x) = \{g \in G : \, gx = xg\}.$$

Remark. We are going to see shortly that $C_G(x)$ is a stabilizer of x with respect to a certain action. Hence it will follow that $C_G(x)$ is a subgroup of G. This we can also see more directly.

Conjugacy action and the class equation. Let G be a finite group. We can then think of G as a G-set where the right multiplication is defined by

$$x * g = x^g = g^{-1}xg.$$

The G-orbit $x * G$ is then $\{x * g = x^g : \, g \in G\} = x^G$, the *conjugacy class* of x, and the stabilizer of x is

$$G_x = \{g \in G : \, x = x * g = g^{-1}xg\} = \{g \in G : \, xg = gx\} = C_G(x).$$

The orbit- stabiliser theorem thus tells us that

$$|x^G| = [G : C_G(x)]$$

We next write G as a disjoint union of G-orbits, that is conjugacy classes:

$$\begin{aligned} G \;\; = \;\; & \underbrace{a_1^G \cup a_2^G \cup \cdots \cup a_r^G}_{\text{each of size } \geq 2} \\ & \cup \underbrace{b_1^G \cup b_2^G \cup \cdots b_s^G}_{\text{each of size } 1} \end{aligned}$$

Recall that $Z(G)$ is the set of all those elements that commute with every element of G and that this is a normal subgroup of G. Now $x \in Z(G)$ if and only if $x = g^{-1}xg = x^g$ for all $g \in G$. It follows that $x \in Z(G)$ if and only if it's conjucacy class $\{x^g : \, g \in G\}$ consists only of one element x. Therefore $Z(G) = \{b_1, \ldots, b_s\}$ and

$$G = Z(G) \cup a_1^G \cup a_2^G \cup \cdots \cup a_r^G.$$

and $|G| = |Z(G)| + \sum_{i=1}^r |a_i^G|$. Using the Orbit-Stabilizer Theorem we can deduce from this the *class equation*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(a_i)]$$

where the sum is taken over the r conjugacy classes with more than one element (so each $[G : C_G(a_i)] > 1$).

Definition. Let p be a prime. A finite group G is said to be a p-group if $|G| = p^m$ for some $m \geq 0$.

Remark. The trivial group $G = \{1\}$ is a p-group for any prime p.

Theorem 5.1 *If G is a non-trivial finite p-group, then $Z(G)$ is non-trivial.*

Proof We use the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

Since $1 \neq |G|$ is of p-power order it follows that $|G|$ and each index $[G : C_G(a_i)]$ are divisible by p. From the class equation it then follows that $|Z(G)|$ is divisible by p. In particular it has at least two elements. □

Example. The result above does not hold for finite groups in general. For example $Z(S_3) = \{1\}$.

Theorem 5.2 *(Cauchy). Let G be a finite group with order that is divisible by a prime p. Then G contains an element of order p.*

Remark. From exercise 4 on sheet 3, we know that this is true when G is abelian.

Proof We prove this by induction on $|G|$. If $|G| = 1$ then the result is trivial ($|G|$ is then not divisible by any prime p so the statement will not get contradicted). Now suppose that $|G| \geq 2$ and that the result holds for all groups of smaller order. Consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

If any of the $|C_G(a_i)|$ is divisible by p, then, as $|C_G(a_i)| < |G|$, we can use the induction hypothesis to conclude that $C_G(a_i)$ contains an element of order p (and thus G as well). Thus we can assume that none of $|C_G(a_i)|$ are divisible by p. But then, as $|G| = [G : C_G(a_i)] \cdot |C_G(a_i)|$, all the indices $[G : C_G(a_i)]$ are divisible by p and the class equation implies that $|Z(G)|$ is divisible by p. But $Z(G)$ is abelian so it follows from the remark that it then contains an element of order p. □

Theorem 5.3 *Let G be a finite p-group and suppose that $|G| = p^n$. There exist a chain of normal subgroups of G*

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

where $|H_i| = p^i$ for $i = 0, 1, \ldots, n$.

Proof. We use induction on $|G| = p^n$. If $n = 0$ then $\{1\} = H_0 = G$ is the chain we want. Now suppose that $n \geq 1$ and that the result holds for all p-groups of smaller order. By Theorem 5.1, we have that $Z(G)$ is non-trivial and by Cauchy's Thoerem (the abelian version suffices) we know that there is a subgroup H_1 of $Z(G)$ such that $|H_1| = p$. Notice that $H_1 \trianglelefteq G$ (as all the elements of H_1 commute with all the elements of G and thus

$gH_1 = H_1g$ for all $g \in G$). Now $|G/H_1| = p^{n-1}$ and by induction hypothesis, there is a normal chain of subgroups

$$\{1\} = K_0 < K_1 < \cdots < K_{n-1} = G/H_1.$$

By the Correspondence Theorem this chain corresponds to a normal chain of intermediate subgroups between H_1 and G

$$H_1 < H_2 < \cdots < H_n = G$$

where $K_{i-1} = H_i/H_1$. Then $|H_i| = |K_{i-1}| \cdot |H_1| = p^{i-1} \cdot p = p^i$ and the chain

$$\{1\} = H_0 < H_1 < \cdots < H_n = G$$

is the chain we want. □.

Remark. In particular this last result tells us that the converse to Lagrange's Theorem holds when G is a p-group. To see the converse of Lagrange's Theorem doesn't hold in general consider the group A_5. This is a simple group with 60 elements that has no subgroup with 30 elements. This is because a subgroup with 30 elements would have index 2 and thus be normal contradicting the simplicity of A_5.

Definition. Let G be a finite group of order $p^n \cdot m$ where p does not divide m. A subgroup of order p^n is called a *Sylow p-subgroup* of G.

Remark. A more elegant way of saying that H is a Sylow p-subgroup of G is to say that H is a p-group such that $[G : H]$ is not divisible by p.

We are now going to prove a number of very nice and useful results about these. In particular we will see that these subgroups always exist and are (for a given group G) all isomorphic. We will also get some information about the number of the Sylow p-subgroups. These results, known collectively as the Sylow theorems, are going to be an important tool to understand the structure of the larger group G.

Theorem 5.4 *(1st Sylow Theorem) Let G be a finite group and p a prime number. There exists a Sylow p-subgroup of G.*

Proof We prove this by induction on $|G|$. If $|G| = 1$ then $\{1\}$ is the Sylow p-subgroup for any prime p and thus the Sylow p-subgroups exist trivially in this case. Suppose now that $|G| \geq 2$, and that the result holds for groups of smaller order. Let p be any prime and suppose that $|G| = p^n m$ where $p \not| m$. If $n = 0$ then the trivial subgroup $\{1\}$ would be a Sylow p-subgroup. We can thus assume that $n \geq 1$. We use the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

Suppose first that some of $[G : C_G(a_i)]$ is not divisible by p. Notice that $|G| = [G : C_G(a_i)] \cdot |C_G(a_i)|$ and as p does not divide $[G : C_G(a_i)]$, whereas p^n divides $|G|$, it follows that p^n divides $|C_G(a_i)|$. But $|C_G(a_i)| < |G|$ and thus by induction hypothesis $C_G(a_i)$

contains a Sylow p-subgroup that is of order p^n and thus a Sylow p-subgroup of G as well.

We are then left with the case when all of the indices $[G : C_G(a_i)]$ are divisible by p. Then $|G|$ is divisible by p and from the class equation it then follows that p divides the order of $|Z(G)|$. By Cauchy's Theorem (we only need the abelian version) we know that $Z(G)$ has a subgroup N of order p which has to be normal in G, since $Ng = gN$ for all $g \in G$. By induction hypothesis, G/N contains a Sylow p-subgroup that is a subgroup of order p^{n-1}. By the Correspondence Theorem this subgroup is of the form P/N for some $N \leq P \leq G$. Notice that $|P| = |N| \cdot |P/N| = p \cdot p^{n-1} = p^n$ and thus P is a Sylow p-subgroup of G. □

Corollary 5.5 *Let G be a group of finite order and let p^r be any power of a prime that divides the order of G. Then there exists a subgroup of order p^r.*

Proof Suppose that $|G| = p^n m$ where $p \not| m$. By the first Sylow theorem there is a subgroup P of order p^n and by Theorem 5.3 we know that P has a subgroup of order p^r. □

For the proof of the 1st Sylow Theorems we used arguments that involved counting the elements of G. For our proofs of the other Sylow theorems we will be counting cosets instead.

Counting cosets If $H, K \leq G$ and let X be the set of all right cosets of H in G. Then K acts naturally on X through right multiplication: $Ha * x = Hax$. This turns X into a K-set. The next Lemma gives us a useful formula of counting the number of cosets that belongs to any given K-orbit.

Lemma 5.6 *The number of cosets in the K-orbit containing Ha are*

$$|Ha * K| = [K : K \cap H^a].$$

Proof We apply the Orbit-Stablizer Theorem. We need to determine the stablizer of the coset Ha in K. Now

$$Hak = Ha \ \Leftrightarrow \ Haka^{-1} = H \ \Leftrightarrow \ aka^{-1} \in H \ \Leftrightarrow k \in a^{-1}Ha = H^a$$

As k was in K to start with, this shows that the stablizer of Ha is $K \cap H^a$ and the Orbit-Stabilizer Theorem tells us that $|Ha * K| = [K : K \cap H^a]$. □

A formula for counting cosets. As before we let X be the set of all right H-cosets that we consider as a K-set. Suppose that

$$X = Ha_1 * K \cup Ha_2 * K \cup \cdots \cup Ha_m * K$$

is the partition of X into disjoint K-orbits. Using Lemma 5.6 this implies that

$$\begin{aligned} [G : H] &= |X| \\ &= |Ha_1 * K| + |Ha_2 * K| + \cdots + |Ha_m * K| \\ &= [K : K \cap H^{a_1}] + [K : K \cap H^{a_2}] + \cdots + [K : K \cap H^{a_m}]. \end{aligned}$$

Remark. We know from Theorem 5.3 that any Sylow p-subgroup contains a subgroup of an order that is an arbitrary p-power divisor of $|G|$. Now we show that the converse is true. Every subgroup of p-power order is contained in some Sylow p-subgroup. In fact we prove something much stronger.

Theorem 5.7 *Let $H \leq G$ where H is a subgroup of p-power order. Let P be any Sylow p-subgroup of G. Then*

$$H \leq P^a$$

for some $a \in G$.

Proof Suppose that $|G| = p^n m$ where $p \not| m$. Let X be the collection of all the right P cosets that we consider as a H-set. By the formula for counting cosets, we have

$$m = [G : P] = [H : H \cap P^{a_1}] + [H : H \cap P^{a_2}] + \ldots + [H : H \cap P^{a_m}] \qquad (4)$$

for some $a_1, \ldots, a_m \in G$. We claim that $H \cap P^{a_i} = H$ for some $i = 1, \ldots, m$. Otherwise all the indices on the RHS of (4) would be divisible by p and we would get the contradiction that m is divisible by p. Hence $H \cap P^{a_i} = H$ for some $i \in \{1, \ldots, m\}$ or equivalently $H \subseteq P^{a_i}$. □

The 2nd Sylow theorem is a direct consequence of this.

Theorem 5.8 *(2nd Sylow Theorem). Any two Sylow p-subgroup are conjugate. (So they form a single conjugacy class).*

Proof Let P and Q be Sylow subgroups of G. By last theorem we know that

$$Q \subseteq P^a$$

for some $a \in G$. But these two groups have the same order. Hence we have $Q = P^a$. □

Remark. The map $\phi : P \to P^a$, $x \mapsto x^a$ is an isomorphism and thus P and P^a are isomorphic. So all the Sylow p-subgroups are isomorphic and up to isomorphism we can talk about the Sylow p-subgroup.

We now move on to the third and the last of the Sylow theorems. This is going to give us some information on the number of Sylow p-subgroups that is immensely useful as we will see.

Theorem 5.9 *(3rd Sylow Theorem). Let G be a finite group and p a prime. The number $n(p)$ of Sylow p-subgroups of G satisfies:*

(i) $n(p) = 1 + pr$, for some non-negative integer r.
(ii) $n(p)$ divides $|G|$.

Proof (See at the end of this chapter).

Remarks. (1) Suppose that $|G| = p^n m$ whre p does not divide m. Let P be a Sylow p-subgroup of G. As $|G| = p^n m = |P| \cdot [G : P]$ and as $n(p) = 1 + pr$ divides $|G|$ while being coprime to p, we must have that $n(p)$ divides $m = [G : P]$.

(2) Let P be a Sylow p-subgroup of G. The Sylow p-subgroups form a single conjugacy class

$$\{ a^{-1}Pa : a \in G\}$$

The number $n(p)$ of these is one iff all of them are equal to P, i.e. iff $P \trianglelefteq G$.

Example 1. Let G be a group of order $2 \cdot p^r$ where p is an odd prime and $r \geq 1$. By the Sylow theorems there exist a subgroup of order p^r that is then of index 2 and therefore normal. Hence G can't be simple if it is of order $2p^r$.

Example 2. Let G be a group of order pq where p and q are primes and $p > q$. Now the number $n(p)$ of Sylow p-subgroups, satisfies

$$n(p) = 1 + pr \text{ and } n(p) \text{ divides } |G|/p = q$$

The only possible $n(p)$ satisfying these criteria is $n(p) = 1$. It follows that there is only one subgroup of order p and this must then be normal in G. We have thus shown that there are no simple groups of order pq.

Example 3. To demonstrate the usefulness of the Sylow theorems, let us see how we can use them to see that there is no simple group of order $12 = 3 \cdot 2^2$. Firstly we have by the 1st Sylow theorem (or Cauchy's thm) that there is a subgroup of order 3 and the number $n(3)$ of these satisfies

$$n(3) = 1 + 3r \text{ and } n(3) \text{ divides } |G|/3 = 4.$$

There are only two possibilities, $n(3) = 1$ or $n(3) = 4$. In the first case there is a normal subgroup of order 3. Let us look at the latter case. We have 4 groups of order 3 and therefore $4 \cdot 2 = 8$ elements of order 3 (in each of the Sylow 3-subgroups there are two elements of order 3 and as the intersection of any two of these is $\{1\}$ we get exactly $4 \cdot 2 = 8$ elements of order 3). There remain 4 elements that must form a unique Sylow 2-subgroup Q (which has order 4). Notice that none of the elements of order 3 can be in Q as 3 does not divide 4. As $n(2) = 1$ we now have that $Q \trianglelefteq G$.

Example 4. Let p, q be distinct primes. We will see that there is no simple group of order $p^2 q$. We consider two cases. If $p > q$ then $n(p) = 1 + pr$ should divide q and as $p > q$ this can only happen if $n(p) = 1$. But in this case we have a normal Sylow p-subgroup. We can thus assume that $p < q$. Now

$$n(q) = 1 + qr \text{ divides } |G|/q = p^2.$$

If $n(q) = 1$ we have a normal Sylow q-subgroup, so we can suppose that $n(q) > 1$. As $q > p$ the only possibility is that $n(q) = p^2$. We then have

$$1 + qr = p^2 \Leftrightarrow qr = p^2 - 1 = (p - 1)(p + 1).$$

As the prime q is greater than p, it follows that q divides $p+1$ and again as $q > p$, we must have $q = p+1$. The only two primes that are one apart are 2 and 3. Thus $p = 2$ and $q = 3$ and $|G| = p^2 \cdot q = 12$. But by Example 3, there is no simple group of order 12 and we are done.

Remark. We mentioned before a famous result of Burnside, the Burnside's (p, q)- Theorem. This said that any group G of order $p^n q^m$ is solvable. This means that there are not composition factors that are non-abelian. In particular G can't be non-abelian simple.

Later in the notes and on the exercise sheets we will apply the Sylow theorems to find all groups of order up to and including 15. We will also see that there is no non-abelian simple group of order less than 60 ($|A_5| = 60$). Before leaving this section we add another weapon to our list. This is Poincaré's Lemma that is often of great help.

Definition. Suppose $H \leq G$. The subgroup

$$H_G = \bigcap_{g \in G} H^g$$

is called the *core* of H in G.

Remarks. (1) As $H = H^e$ is one of the conjugates of H it is clear that $H_G \leq H$ and we will see later that $H_G \trianglelefteq G$ as a part of Poincaré's Lemma. This we can also see directly. Let $a \in G$ then

$$H_G^a = \bigcap_{g \in G} H^{ga} = \bigcap_{b \in G} H^b = H_G,$$

where the last identity holds from the fact that $Ga = G$.

(2) If $N \leq H$ and $N \trianglelefteq G$ then for all $g \in G$ we have $N = N^g \leq H^g$. It follows that

$$N \leq \bigcap_{g \in G} H^g = H_G.$$

This shows that H_G is the largest normal subgroup of G that is contained in H.

Theorem 5.10 *Suppose G is a group (possibly infinite) and let $H \leq G$ such that $[G : H] = n < \infty$. Then*

$$G/H_G \cong K$$

for some $K \leq S_n$.

Proof Let $X = \{gH : g \in G\}$. For each $a \in G$, we get a map $L_a : X \to X$, $gH \mapsto agH$. Notice that L_a is bijective with inverse $L_{a^{-1}}$. Also notice that

$$L_a \circ L_b(gH) = L_a(bgH) = abgH = L_{ab}(gH).$$

Now consider the map $\phi : G \to \mathrm{Sym}\,(X),\ a \mapsto L_a$. We have just seen that $L_{ab} = L_a \circ L_b$ and this implies that $\phi(ab) = \phi(a) \circ \phi(b)$. Thus ϕ is a homomorphism. We next identify the kernel. We have

$$\begin{aligned}\phi(a) = L_a = \mathrm{id} \ &\Leftrightarrow\ agH = gH \ \text{ for all } \ g \in G \\ &\Leftrightarrow\ g^{-1}agH = H \ \text{ for all } g \in G \\ &\Leftrightarrow\ g^{-1}ag \in H \ \text{ for all } g \in G \\ &\Leftrightarrow\ a \in gHg^{-1} \ \text{ for all } \ g \in G.\end{aligned}$$

Therefore the kernel is $\bigcap_{g\in G} H^{g^{-1}} = \bigcap_{a\in G} H^a = H_G$. By the 1st Isomorphism Theorem we have that $H_G \trianglelefteq G$ and

$$G/H_G = G/\ker\phi \cong \mathrm{im}\,\phi$$

where $\mathrm{im}\,\phi \leq \mathrm{Sym}\,(X)$. As $|X| = n$ we have that $\mathrm{Sym}\,(X) \cong S_n$ and thus G/H_G isomorphic to a subgroup of S_n. □.

Corollary 5.11 *(Poincaré's Lemma). Let G be a finite simple group with a subgroup H such that $[G : H] = n > 1$. Then*

$$G \cong K$$

for some $K \leq S_n$. In particular $|G|$ divides $|S_n| = n!$.

Proof H_G is a normal subgroup of G and as H_G is contained in H we can't have $H_G = G$. Now G is simple and we conclude that $H_G = \{1\}$. The result now follows from Theorem 5.11 as $G/\{1\} \cong G$. □

Example 5. Let us give another proof of the fact that there is no simple group of order 12. We argue by contradiction and suppose that G is a simple groups with 12 elements. By the Sylow theorems we have a subgroup of order 4 and thus of index 3. By Corollary 5.12 if follows that $12 = |G|$ divides the $3! = 6$. This is absurd.

We end this section by proving the 3rd Sylow Theorem. We need first some preliminary work.

Definition Let $H \leq G$. The *normalizer* of H in G is

$$N_G(H) = \{g \in G : \ H^g = H\}.$$

One can easily check that this is a subgroup of G (in fact it follows also from next remark as $N_G(H)$ turns out to be a stabiliser with respect to a certain G-action) and clearly $H \trianglelefteq N_G(H)$.

Remarks. (1) Let X be the set of all subgroups of G. As we have seen before G acts naturally on X by conjugation and so we can think of X as a G-set with respect to this action. The stabilizer of the subgroup H is then $N_G(H)$ and the Orbit-Stabilizer theorem tells us that the number of conjugates of H, that is the size of the G orbit $\{H^g : g \in G\}$, is $[G : N_G(H)]$.

(2) Let P be a Sylow p-subgroup of G. By the 2nd Sylow Theorem, we know that the Sylow p-subgroups form a single conjugacy class $\{P^g : g \in G\}$. By Remark (1) the total number of all Sylow p-subgroups is then $n(p) = [G : N_G(P)]$.

Lemma 5.12 *Let P be a Sylow p-subgroup of G. Then P is the unique Sylow p-subgroup of $N_G(P)$.*

Proof Let Q be any Sylow p-subgroup of $N_G(P)$. By the second Sylow Theorem we have

$$Q = P^a$$

for some $a \in N_G(P)$. But then $Q = P^a = P$ since a normalizes P. $\Box$.

Proof of the 3rd Sylow Theorem. Let P be a Sylow p-subgroup of G. Since the Sylow p-subgroups form a single conjugacy class

$$\{P^a : \; a \in G\},$$

we know from the remark above that their number is

$$n(p) = [G : N_G(P)].$$

In particular $n(p)$ divides $|G|$. This proves (ii). To prove (i) we need more work. Let $N = N_G(P)$ and let X be the collection of all the right N cosets of G that we consider as a P-set. Write X as a disjoint union of P-orbits, say

$$X = Na_1 * P \cup Na_2 * P \cup \cdots \cup Na_m * P$$

where we assume that the first orbit $Na_1 * P$ is the one containing the coset $N \cdot 1 = N$ and we can also then assume that $a_1 = 1$ From this we get that

$$\begin{aligned} n(p) &= |Na_1 * P| + |Na_2 * P| + \cdots + |Na_m * P| \\ &= [P : P \cap N^{a_1}] + [P : P \cap N^{a_2}] + \cdots + [P : P \cap N^{a_m}]. \end{aligned}$$

Now notice that $P \cap N^{a_i} = P$ iff $P \leq N^{a_i}$ iff $P^{a_i^{-1}} \leq N$. However, by Lemma 5.9, this happens iff $P^{a_i^{-1}} = P$ that happens iff $a_i \in N_G(P)$. But then $Na = Na_i \in Na_i * P$ and as the only orbit containing N is $Na_1 * P$, it follows that $i = 1$. (Notice also that $a_1 \in N_G P$ and thus $[P : P \cap N^{a_1}] = 1$). We conclude from this that $[P : P \cap N^{a_i}]$ is divisble by p for $i = 2, \ldots, m$ and that $[P : P \cap N^{a_1}] = 1$. Hence $n(p) = 1 + pr$ for some non-negative integer r. $\Box$

6 Semidirect products and groups of order ≤ 15

I. Semidirect products.

We will now introduce a generalization of direct products that is very useful for describing and constructing groups. As with direct products these come in two disguises internal and external semidirect products.

Notation. Suppose that N is a group and $\phi : N \to N$ is an automorphism. In this section we will use b^ϕ for the value of b under ϕ (instead of $\phi(b)$). This will actually make things look clearer. We will also operate a composition of two automorphisms from left to right. Thus

$$b^{\psi\circ\phi} = (b^\psi)^\phi.$$

Definition. Let G be a group and $N \trianglelefteq G, H \leq G$. We say that G is the *internal semidirect product* of N by H if $G = HN$ and $H \cap N = \{1\}$.

Remark. The definition is thus very similar to the definition of an internal direct product. The only differenct is that one of the groups H does not have to be normal in general. When H is normal as well then we get a direct product.

Lemma 6.1 *Let G be an internal semidirect product of N by H, then the following hold.*

(1) Every element $g \in G$ can be written uniquely as $g = ab$ with $a \in H$ and $b \in N$.

(2) Let $a_1, a_2 \in H$ and $b_1, b_2 \in N$. Then

$$(a_1b_1) \cdot (a_2b_2) = (a_1a_2) \cdot (b_1^{a_2}b_2)$$

Proof (1) If $a_1b_1 = a_2b_2$ then $a_2^{-1}a_1 = b_2b_1^{-1}$ is in $H \cap N$ and thus trivial. So $a_1 = a_2$ and $b_1 = b_2$).

(2) We have

$$(a_1b_1) \cdot (a_2b_2) = (a_1a_2) \cdot (a_2^{-1}b_1a_2b_2) = (a_1a_2) \cdot (b_1^{a_2}b_2).$$

This finishes the proof. $\Box$

Remark. Thus, like for internal direct products, we can treat elements like pairs ab where a is the H component and b is the N component. Furthermore multiplying two such elements a_1b_1 and a_2b_2 gives us a new element whose H compenent is a_1a_2 and whose

N component is $b_1^{a_2}b_2$. It follows that if we know the structure of H and N and if we know how H acts on N by conjugation, then we know the structure of the semidirect product G. If you for example had a multiplication table for H and N and you knew how H acts on N by conjugation then you could write down a multiplication table for G.

Remark. For $a \in H$, let $\phi_a : N \to N$ be the conjugation by a. We have seen previously that this map is an automorphism. Now

$$x^{\phi_{ab}} = x^{ab} = (x^a)^b = (x^{\phi_a})^{\phi_b} = x^{\phi_a \circ \phi_b}.$$

Consider the map $\Psi : H \to \mathrm{Aut}\,(N)$, $a \mapsto \phi_a$. As $\Psi(ab) = \phi_{ab} = \phi_a \circ \phi_b = \Psi(a) \circ \Psi(b)$, this map is a homomorphism. Notice also

$$a_1b_1 \cdot a_2b_2 = (a_1a_2) \cdot (b_1^{a_2}b_2) = (a_1a_2) \cdot (b_1^{\phi_{a_2}}b_2) = (a_1a_2) \cdot (b_1^{\Psi(a_2)}b_2)$$

This motivates the following structure.

Definition Let N, H be groups and let $\Psi : H \to \mathrm{Aut}\,(N)$ be a homomorphism. The external semidirect product $H \ltimes_\Psi N$, of N by H with respect to Ψ, is the cartesian set product of H and N with the binary operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1^{\Psi(a_2)}b_2)$$

$H \ltimes_\Psi N$ **is a group**. First let us check the associativity. Firstly

$$\begin{aligned}[(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3) &= (a_1a_2, b_1^{\Psi(a_2)}b_2) \cdot (a_3, b_3) \\ &= (a_1a_2a_3, (b_1^{\Psi(a_2)}b_2)^{\Psi(a_3)}b_3)\end{aligned}$$

Since $\Psi(a_3) \in \mathrm{Aut}\,(N)$ and since Ψ is a homorphism, we get

$$\begin{aligned}(b_1^{\Psi(a_2)}b_2)^{\Psi(a_3)}b_3 &= b_1^{\Psi(a_2)\Psi(a_3)}b_2^{\Psi(a_3)}b_3 \\ &= b_1^{\Psi(a_2a_3)}b_2^{\Psi(a_3)}b_3.\end{aligned}$$

Then secondly

$$\begin{aligned}(a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] &= (a_1, b_1) \cdot (a_2a_3, b_2^{\Psi(a_3)}b_3) \\ &= (a_1a_2a_3, b_1^{\Psi(a_2a_3)}b_2^{\Psi(a_3)}b_3).\end{aligned}$$

This shows that the associative law holds. To see that $(1, 1)$ is the identity. Notice that any automorphism maps 1 to itself and that $\Psi(1) = \mathrm{id}$. Thus

$$(1, 1) \cdot (a, b) = (1 \cdot a, 1^{\Psi(a)}b) = (a, b)$$

and

$$(a, b) \cdot (1, 1) = (a \cdot 1, b^{\Psi(1)} \cdot 1) = (a, b^{\mathrm{id}} \cdot 1) = (a, b).$$

Finally, the inverse of (a, b) is $(a^{-1}, (b^{\Psi(a^{-1})})^{-1})$ since

$$(a, b) \cdot (a^{-1}, (b^{\Psi(a^{-1})})^{-1}) = (a \cdot a^{-1}, b^{\Psi(a^{-1})}(b^{\Psi(a^{-1})})^{-1}) = (1, 1)$$

and

$$\begin{aligned}(a^{-1},(b^{\Psi(a^{-1})})^{-1})\cdot(a,b) &= (aa^{-1},((b^{\Psi(a^{-1})})^{-1})^{\Psi(a)}b)\\ &= (1,(b^{\Psi(a^{-1})\Psi(a)})^{-1}b)\\ &= (1,(b^{\Psi(1)})^{-1}b)\\ &= (1,(b^{\mathrm{id}})^{-1}b)\\ &= (1,1).\end{aligned}$$

Remark. Consider an internal semidirect product of N by H and let $\Psi : H \to \mathrm{Aut}\,(N)$ be the homomorphism that maps a to ϕ_a where the latter is the automorphism that takes b to b^a. Using the data N, H and Ψ, we can also construct the external semidirect product $H \ltimes_\Psi N$. Not surprisingly, the two are isomorphic (see Exercise 1 on Sheet 10).

II. Groups of order less than 16.

In this section (and on the exercise sheets) we play with our new tools and find all groups of order up to and including 15. We have already shown previously (Exercise 2 on sheet 9) that the only group of order 15 is $\mathbb{Z}_{15}$ and we have no difficulty with groups of order 1. When p is a prime, there is exactly one group of order p, the cyclic group $\mathbb{Z}_p$ of order p. On exercise sheet 8 we also show that there are only two groups of order p^2, namely $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Semidirect products of cyclic groups. Suppose that $G = HN$ is an internal semidirect product of a cyclic group $N = \langle a \rangle$ by another cyclic group $\langle b \rangle$. We have that

$$a^b = a^r \tag{5}$$

for some $r \in \mathbb{Z}$. Inductively it follows that $a^{b^n} = a^{r^n}$ and then that $(a^m)^{b^n} = (a^{b^n})^m = a^{mr^n}$. Thus the structure of G is determined by (5) and the orders of a and b.

We will now introduce an infinite family of groups, many of which will crop up in the list of groups of orders 1 to 15.

Example.(D_{2n}, the dihedral group of order $2n$). Consider a regular n-gon in the complex plane with corners $1, u, u^2, \ldots, u^{n-1}$ where $u = e^{2\pi i/n}$ (draw a figure). The symmetry group of this regular n-gon is generated by a counter clockwise rotation a of $2\pi/n$ around the origin and the reflection b in the real axis. This can be described explicitly as follows:

$$\begin{aligned}a(z) &= e^{2\pi i/n}\cdot z\\ b(z) &= \bar{z}.\end{aligned}$$

Let us calculate

$$\begin{aligned}b^{-1}ab(z) &= bab(z)\\ &= ba(\bar{z})\\ &= b(e^{2\pi i/n}\cdot \bar{z})\\ &= e^{-2\pi i/n}z\\ &= a^{-1}(z).\end{aligned}$$

This means that the symmetry group is a group of order $2n$ that is a semidirect product of $\langle a\rangle$, a cyclic group of order n, and $\langle b\rangle$, a cyclic group of order 2. Furthermore the action of $\langle b\rangle$ on $\langle a\rangle$ is determined by $a^b = a^{-1}$. The unique group of order $2n$ with a normal cyclic subgroup $\langle a\rangle$ of order n, and a cyclic subgroup $\langle b\rangle$ where $a^b = a^{-1}$ is called the dihedral group of order $2n$ and is denoted D_{2n}.

Theorem 6.2 *Let p be an odd prime. There are (up to isomorphism) exactly two groups of order $2p$ these are*

$$\mathbb{Z}_{2p} \;\; \textit{and} \;\; D_{2p}.$$

Proof By the Sylow theorems (or Cauchy's thm) there is a subgroup $N = \langle a\rangle$ of order p. Since N is of index 2 it is normal. There is also a group $H = \langle b\rangle$ of order 2. Clearly $H \cap N = \{1\}$, since it is a subgroup of both H and N and thus its order divides both 2 and p. So we have that G is a semidirect product of N by H. To determine the group structure it remains to see how H can act on N. Now

$$b^{-1}ab = a^r$$

for some $0 \le r \le p-1$. Using the fact that b is of order 2, we see that

$$a = b^{-1}(b^{-1}ab)b = b^{-1}a^r b = (b^{-1}ab)^r = a^{r^2}.$$

This implies that $a^{r^2-1} = 1$ and thus p must divide $r^2 - 1 = (r-1)(r+1)$. The only possibilities for this to happen is when $r = 1$ or $r = p-1$. In the first case the group is abelian and $G = \langle ba\rangle$ is a cyclic group of order $2p$. (Notice that $(ba)^2 = a^2 \neq 1$ and $(ba)^p = b \neq 1$ so the order of ba is $2p$ by Lagrange's theorem). In the latter case we have the relations

$$a^p = 1, \;\; b^2 = 1, \;\; bab^{-1} = a^{p-1} = a^{-1}$$

which gives us D_{2p} as we have seen. □

Remark. The only orders up to 15 that are not covered by 1, 15, p, p^2 and $2p$ are 8 and 12. These are dealt with on the excercise sheets 9 and 10.

We end by constructing a certain group of order 12, using the external semidirect product.

Example. Let $N = \langle a\rangle$ be a cyclic group of order 3 and $H = \langle b\rangle$ be a cyclic group of order 4. The map

$$\phi : N \to N,\, x \mapsto x^{-1}$$

is in Aut (N). The map

$$\Psi : H \to \mathrm{Aut}\,(N),\;\, b^r \mapsto \phi^r$$

is a homomorphism. It is well defined as $b^r = b^s \Rightarrow b^{s-r} = 1 \Rightarrow 4|(r-s) \Rightarrow \phi^{s-r} = \mathrm{id} \Rightarrow \phi^r = \phi^s$. Consider the external semidirect product $T = H \ltimes_\Psi N$. It is a group of order 12 with a cyclic normal Sylow 3-subgroup of order 3 and a cyclic Sylow 2-subgroup of order 4.

From our study in this chapter and the exercise sheets we can conclude that the groups of order ≤ 15 are (up to isomorphism)

order	groups
1	$\{1\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, D_6
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_8, Q
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_{10}
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_4 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, A_4, D_{12}, T
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_{14}
15	$\mathbb{Z}_{15}$