

# Chapter 1

## Group Theory

Most lectures on group theory actually start with the definition of what is a group. It may be worth though spending a few lines to mention how mathematicians came up with such a concept.

Around 1770, Lagrange initiated the study of permutations in connection with the study of the solution of equations. He was interested in understanding solutions of polynomials in several variables, and got this idea to study the behaviour of polynomials when their roots are permuted. This led to what we now call Lagrange's Theorem, though it was stated as [5] *If a function  $f(x_1, \dots, x_n)$  of  $n$  variables is acted on by all  $n!$  possible permutations of the variables and these permuted functions take on only  $r$  values, then  $r$  is a divisor of  $n!$* . It is Galois (1811-1832) who is considered by many as the founder of group theory. He was the first to use the term "group" in a technical sense, though to him it meant a collection of permutations closed under multiplication. Galois theory will be discussed much later in these notes. Galois was also motivated by the solvability of polynomial equations of degree  $n$ . From 1815 to 1844, Cauchy started to look at permutations as an autonomous subject, and introduced the concept of permutations generated by certain elements, as well as several notations still used today, such as the cyclic notation for permutations, the product of permutations, or the identity permutation. He proved what we call today Cauchy's Theorem, namely that if  $p$  is prime divisor of the cardinality of the group, then there exists a subgroup of cardinality  $p$ . In 1870, Jordan gathered all the applications of permutations he could find, from algebraic geometry, number theory, function theory, and gave a unified presentation (including the work of Cauchy and Galois). Jordan made explicit the notions of homomorphism, isomorphism (still for permutation groups), he introduced solvable groups, and proved that the indices in two composition series are the same (now called Jordan-Hölder Theorem). He also gave a proof that the alternating group  $A_n$  is simple for  $n > 4$ .

In 1870, while working on number theory (more precisely, in generalizing

Kummer's work on cyclotomic fields to arbitrary fields), Kronecker described in one of his papers a finite set of arbitrary elements on which he defined an abstract operation on them which satisfy certain laws, laws which now correspond to axioms for finite abelian groups. He used this definition to work with ideal classes. He also proved several results now known as theorems on abelian groups. Kronecker did not connect his definition with permutation groups, which was done in 1879 by Frobenius and Stickelberger.

Apart permutation groups and number theory, a third occurrence of group theory which is worth mentioning arose from geometry, and the work of Klein (we now use the term Klein group for one of the groups of order 4), and Lie, who studied transformation groups, that is transformations of geometric objects. The work by Lie is now a topic of study in itself, but Lie theory is beyond the scope of these notes.

The abstract point of view in group theory emerged slowly. It took something like one hundred years from Lagrange's work of 1770 for the abstract group concept to evolve. This was done by abstracting what was in common to permutation groups, abelian groups, transformation groups... In 1854, Cayley gave the modern definition of group for the first time:

*"A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative."*

Let us start from there.

## 1.1 Groups and subgroups

We start by introducing the object that will interest us for the whole chapter.

**Definition 1.1.** A **group** is a non-empty set  $G$  on which there is a binary operation  $(a, b) \mapsto ab$  such that

- if  $a$  and  $b$  belong to  $G$  then  $ab$  is also in  $G$  (*closure*),
- $a(bc) = (ab)c$  for all  $a, b, c$  in  $G$  (*associativity*),
- there is an element  $1 \in G$  such that  $a1 = 1a = a$  for all  $a \in G$  (*identity*),
- if  $a \in G$ , then there is an element  $a^{-1} \in G$  such that  $aa^{-1} = a^{-1}a = 1$  (*inverse*).

One can easily check that this implies the unicity of the identity and of the inverse.

A group  $G$  is called **abelian** if the binary operation is commutative, i.e.,  $ab = ba$  for all  $a, b \in G$ .

*Remark.* There are two standard notations for the binary group operation: either the additive notation, that is  $(a, b) \mapsto a + b$  in which case the identity is

denoted by 0, or the multiplicative notation, that is  $(a, b) \mapsto ab$  for which the identity is denoted by 1.

- Examples 1.1.**
1.  $\mathbb{Z}$  with the addition and 0 as identity is an abelian group.
  2.  $\mathbb{Z}$  with the multiplication is not a group since there are elements which are not invertible in  $\mathbb{Z}$ .
  3. The set of  $n \times n$  invertible matrices with real coefficients is a group for the matrix product and identity the matrix  $\mathbf{I}_n$ . It is denoted by  $GL_n(\mathbb{R})$  and called the **general linear group**. It is not abelian for  $n \geq 2$ .

The above examples are the easiest groups to think of. The theory of algebra however contains many examples of famous groups that one may discover, once equipped with more tools (for example, the Lie groups, the Brauer group, the Witt group, the Weyl group, the Picard group,...to name a few).

**Definition 1.2.** The **order** of a group  $G$ , denoted by  $|G|$ , is the cardinality of  $G$ , that is the number of elements in  $G$ .

We have only seen infinite groups so far. Let us look at some examples of finite groups.

- Examples 1.2.**
1. The **trivial group**  $G = \{0\}$  may not be the most exciting group to look at, but still it is the only group of order 1.
  2. The group  $G = \{0, 1, 2, \dots, n-1\}$  of integers modulo  $n$  is a group of order  $n$ . It is sometimes denoted by  $\mathbb{Z}_n$  (this should not be confused with  $p$ -adic integers though!).

**Definition 1.3.** A **subgroup**  $H$  of a group  $G$  is a non-empty subset of  $G$  that forms a group under the binary operation of  $G$ .

- Examples 1.3.**
1. If we consider the group  $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$  of integers modulo 4,  $H = \{0, 2\}$  is a subgroup of  $G$ .
  2. The set of  $n \times n$  matrices with real coefficients and determinant of 1 is a subgroup of  $GL_n(\mathbb{R})$ , denoted by  $SL_n(\mathbb{R})$  and called the **special linear group**.

At this point, in order to claim that the above examples are actually subgroups, one has to actually check the definition. The proposition below gives an easier criterion to decide whether a subset of a group  $G$  is actually a subgroup.

**Proposition 1.1.** *Let  $G$  be a group. Let  $H$  be a non-empty subset of  $G$ . The following are equivalent:*

1.  $H$  is a subgroup of  $G$ .
2. (a)  $x, y \in H$  implies  $xy \in H$  for all  $x, y$ .  
(b)  $x \in H$  implies  $x^{-1} \in H$ .

3.  $x, y \in H$  implies  $xy^{-1} \in H$  for all  $x, y$ .

*Proof.* We prove that  $1. \Rightarrow 3. \Rightarrow 2. \Rightarrow 1.$

1.  $\Rightarrow$  3. This part is clear from the definition of subgroup.
3.  $\Rightarrow$  2. Since  $H$  is non-empty, let  $x \in H$ . By assumption of 3., we have that  $xx^{-1} = 1 \in H$  and that  $1x^{-1} \in H$  thus  $x$  is invertible in  $H$ . We now know that for  $x, y \in H$ ,  $x$  and  $y^{-1}$  are in  $H$ , thus  $x(y^{-1})^{-1} = xy$  is in  $H$ .
2.  $\Rightarrow$  1. To prove this direction, we need to check the definition of group. Since closure and existence of an inverse are true by assumption of 2., and that associativity follows from the associativity in  $G$ , we are left with the existence of an identity. Now, if  $x \in H$ , then  $x^{-1} \in H$  by assumption of 2., and thus  $xx^{-1} = 1 \in H$  again by assumption of 2., which completes the proof. □

We will often use the last equivalence to check that a subset of a group  $G$  is a subgroup.

Now that we have these structures of groups and subgroups, let us introduce a map that allows to go from one group to another and that respects the respective group operations.

**Definition 1.4.** Given two groups  $G$  and  $H$ , a **group homomorphism** is a map  $f : G \rightarrow H$  such that

$$f(xy) = f(x)f(y) \text{ for all } x, y \in G.$$

Note that this definition immediately implies that the identity  $1_G$  of  $G$  is mapped to the identity  $1_H$  of  $H$ . The same is true for the inverse, that is  $f(x^{-1}) = f(x)^{-1}$ .

**Example 1.4.** The map  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$ ,  $x \mapsto \exp(x)$  is a group homomorphism.

**Definition 1.5.** Two groups  $G$  and  $H$  are **isomorphic** if there is a group homomorphism  $f : G \rightarrow H$  which is also a bijection.

Roughly speaking, isomorphic groups are “essentially the same”.

**Example 1.5.** If we consider again the group  $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$  of integers modulo 4 with subgroup  $H = \{0, 2\}$ , we have that  $H$  is isomorphic to  $\mathbb{Z}_2$ , the group of integers modulo 2.

A crucial definition is the definition of the order of a group element.

**Definition 1.6.** The **order** of an element  $a \in G$  is the least positive integer  $n$  such that  $a^n = 1$ . If no such integer exists, the order of  $a$  is infinite. We denote it by  $|a|$ .

Note that the critical part of this definition is that the order is the *least* positive integer with the given property. The terminology *order* is used both for groups and group elements, but it is usually clear from the context which one is considered.

## 1.2 Cyclic groups

Let us now introduce a first family of groups, the cyclic groups.

**Definition 1.7.** A group  $G$  is **cyclic** if it is generated by a single element, which we denote by  $G = \langle a \rangle$ . We may denote by  $C_n$  a cyclic group of  $n$  elements.

**Example 1.6.** A finite cyclic group generated by  $a$  is necessarily abelian, and can be written (multiplicatively)

$$\{1, a, a^2, \dots, a^{n-1}\} \text{ with } a^n = 1$$

or (additively)

$$\{0, a, 2a, \dots, (n-1)a\} \text{ with } na = 0.$$

A finite cyclic group with  $n$  elements is isomorphic to the additive group  $\mathbb{Z}_n$  of integers modulo  $n$ .

**Example 1.7.** An  $n$ th root of unity is a complex number  $z$  which satisfies the equation  $z^n = 1$  for some positive integer  $n$ . Let  $\zeta_n = e^{2i\pi/n}$  be an  **$n$ th root of unity**. All the  $n$ th roots of unity form a group under multiplication. It is a cyclic group, generated by  $\zeta_n$ , which is called a **primitive root of unity**. The term “primitive” exactly refers to being a generator of the cyclic group, namely, an  $n$ th root of unity is primitive when there is no positive integer  $k$  smaller than  $n$  such that  $\zeta_n^k = 1$ .

Here are some properties of cyclic groups and its generators.

**Proposition 1.2.** *If  $G$  is a cyclic group of order  $n$  generated by  $a$ , the following conditions are equivalent:*

1.  $|a^k| = n$ .
2.  $k$  and  $n$  are relatively prime.
3.  $k$  has an inverse modulo  $n$ , that is there exists an integer  $s$  such that  $ks \equiv 1 \pmod{n}$ .

*Proof.* Before starting the proof, recall that since  $a$  generates  $G$  of order  $n$ , we have that the order of  $a$  is  $n$  and in particular  $a^n = 1$ . The fact that  $|a^k| = n$  means in words that the order of  $a^k$  is also  $n$ , that is,  $a^k$  is also a generator of  $G$ . We first prove that 1.  $\iff$  2., while 2.  $\iff$  3. follows from Bezout identity.

1.  $\Rightarrow$  2. Suppose by contradiction that  $k$  and  $n$  are not relatively prime, that is, there exists  $s > 1$  such that  $s|k$  and  $s|n$ . Thus  $n = ms$  and  $k = sr$  for some  $m, r \geq 1$  and we have

$$(a^k)^m = a^{srms} = a^{nr} = 1.$$

Now since  $s > 1$ ,  $m < n$ , which contradicts that  $n$  is the order of  $a^k$ .

2.  $\Rightarrow$  1. Suppose that the order of  $a^k$  is not  $n$ , then there exists  $m < n$  such that  $(a^k)^m = 1$  and thus  $n|km$  since  $n$  is the order of  $a$ . If  $k$  and  $n$  were to be relatively prime, then  $n$  would divide  $m$ , which is a contradiction since  $m < n$ .
2.  $\Rightarrow$  3. If  $k$  and  $n$  are relatively prime, then by Bezout identity, there exist  $r, s$  such that  $1 = kr + ns$  and thus  $kr \equiv 1$  modulo  $n$ .
3.  $\Rightarrow$  2. If  $kr \equiv 1$  modulo  $n$  then  $1 = kr + ns$  for some  $s$  and the greatest common divisor of  $k$  and  $n$  must divide 1, which shows  $k$  and  $n$  are relatively prime.

□

**Corollary 1.3.** *The set of invertible elements modulo  $n$  forms a group under multiplication, whose order is the Euler function  $\varphi(n)$ , which by definition counts the number of positive integers less than  $n$  that are relatively prime to  $n$ .*

**Example 1.8.** Consider the group  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ , the group  $\mathbb{Z}_6^*$  of invertible elements in  $\mathbb{Z}_6$  is  $\mathbb{Z}_6^* = \{1, 5\}$ . We have that  $\varphi(6) = \varphi(2)\varphi(3) = 2$ .

### 1.3 Cosets and Lagrange's Theorem

**Definition 1.8.** Let  $H$  be a subgroup of a group  $G$ . If  $g \in G$ , the **right coset** of  $H$  generated by  $g$  is

$$Hg = \{hg, h \in H\}$$

and similarly the **left coset** of  $H$  generated by  $g$  is

$$gH = \{gh, h \in H\}.$$

In additive notation, we get  $H + g$  (which usually implies that we deal with a commutative group where we do not need to distinguish left and right cosets).

**Example 1.9.** If we consider the group  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$  and its subgroup  $H = \{0, 2\}$  which is isomorphic to  $\mathbb{Z}_2$ , the cosets of  $H$  in  $G$  are

$$0 + H = H, \quad 1 + H = \{1, 3\}, \quad 2 + H = H, \quad 3 + H = \{1, 3\}.$$

Clearly  $0 + H = 2 + H$  and  $1 + H = 3 + H$ .

We see in the above example that while an element of  $g \in G$  runs through all possible elements of the group  $G$ , some of the left cosets  $gH$  (or right cosets  $Hg$ ) may be the same. It is easy to see when this exactly happens.

**Lemma 1.4.** *We have that  $Ha = Hb$  if and only if  $ab^{-1} \in H$  for  $a, b \in G$ . Similarly,  $aH = bH$  if and only if  $a^{-1}b \in H$  for  $a, b \in G$ .*

*Proof.* If two right cosets are the same, that is  $Ha = Hb$ , since  $H$  is a subgroup, we have  $1 \in H$  and  $a = hb$  for some  $h \in H$ , so  $ab^{-1} = h \in H$ .

Conversely, if  $ab^{-1} = h \in H$ , then  $Ha = Hhb = Hb$ , again since  $H$  is a subgroup.  $\square$

While one may be tempted to define a coset with a subset of  $G$  which is not a subgroup, we see that the above characterization really relies on the fact that  $H$  is actually a subgroup.

**Example 1.10.** It is thus no surprise that in the above example we have  $0+H = 2+H$  and  $1+H = 3+H$ , since we have modulo 4 that  $0-2 \equiv 2 \in H$  and  $1-3 \equiv 2 \in H$ .

Saying that two elements  $a, b \in G$  generate the same coset is actually an [equivalence relation](#) in the following sense. We say that  $a$  is equivalent to  $b$  if and only if  $ab^{-1} \in H$ , and this relation satisfies the three properties of an equivalence relation:

- *reflexivity:*  $aa^{-1} = 1 \in H$ .
- *symmetry:* if  $ab^{-1} \in H$  then  $(ab^{-1})^{-1} = ba^{-1} \in H$ .
- *transitivity:* if  $ab^{-1} \in H$  and  $bc^{-1} \in H$  then  $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ .

The [equivalence class](#) of  $a$  is the set of elements in  $G$  which are equivalent to  $a$ , namely

$$\{b, ab^{-1} \in H\}.$$

Since  $ab^{-1} \in H \iff (ab^{-1})^{-1} = ba^{-1} \in H \iff b \in Ha$ , we further have that

$$\{b, ab^{-1} \in H\} = Ha,$$

and a coset is actually an equivalence class.

**Example 1.11.** Let us get back to our example with the group  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$  and its subgroup  $H = \{0, 2\}$ . We compute the first coset  $0+H = H$ , and thus we now know that the equivalence class of 0 is  $H$ , and thus there is no need to compute the coset generated by 2, since it will give the same coset. We then compute the coset  $1+H = \{1, 3\}$  and again there is no need to compute the one of 3 since it is already in the coset of 1. We thus get 2 cosets, and clearly they partition  $\mathbb{Z}_4$ :

$$\mathbb{Z}_4 = \{0, 2\} \sqcup \{1, 3\} = H \sqcup (1+H).$$

It is important to notice that the right (resp. left) cosets partition the group  $G$  (that the union of all cosets is  $G$  is clear since we run through all elements of  $G$  and  $H$  contains 1, and it is easy to see that if  $x \in Ha$  and  $x \in Hb$  then  $Ha = Hb$ ).

**Example 1.12.** Consider  $\mathbb{R}$  as an additive group with subgroup  $\mathbb{Z}$ . Every real number up to addition by an integer looks like a number in  $[0, 1)$ . Thus

$$\mathbb{R} = \cup_{0 \leq x < 1} (x + \mathbb{Z}),$$

and the cosets of  $\mathbb{Z}$  partition  $\mathbb{R}$ .

Furthermore, since the map  $h \mapsto ha$ ,  $h \in H$ , is a one-to-one correspondence, each coset has  $|H|$  elements.

**Definition 1.9.** The **index** of a subgroup  $H$  in  $G$  is the number of right (left) cosets. It is a positive number or  $\infty$  and is denoted by  $[G : H]$ .

If we think of a group  $G$  as being partitioned by cosets of a subgroup  $H$ , then the index of  $H$  tells how many times we have to translate  $H$  to cover the whole group.

**Example 1.13.** In Example 1.12, the index  $[\mathbb{R} : \mathbb{Z}]$  is infinite, since there are infinitely many cosets of  $\mathbb{Z}$  in  $\mathbb{R}$ .

**Theorem 1.5. (Lagrange's Theorem).** *If  $H$  is a subgroup of  $G$ , then  $|G| = |H|[G : H]$ . In particular, if  $G$  is finite then  $|H|$  divides  $|G|$  and  $[G : H] = |G|/|H|$ .*

*Proof.* Let us start by recalling that the left cosets of  $H$  forms a partition of  $G$ , that is

$$G = \sqcup gH,$$

where  $g$  runs through a set of representatives (one for each coset). Let us look at the cardinality of  $G$ :

$$|G| = |\sqcup gH| = \sum |gH|$$

since we have a disjoint union of cosets, and the sum is again over the set of representatives. Now

$$\sum |gH| = \sum |H|$$

since we have already noted that each coset contains  $|H|$  elements. We then conclude that

$$|G| = \sum |H| = [G : H]|H|.$$

□

**Example 1.14.** Consider  $G = \mathbb{Z}$ ,  $H = 3\mathbb{Z}$ , then  $[G : H] = 3$ .

Of course, Lagrange did not prove Lagrange's theorem! The modern way of defining groups did not exist yet at his time. Lagrange was interested in polynomial equations, and in understanding the existence and nature of the roots (does every equation has a root? how many roots?...). What he actually proved was that if a polynomial in  $n$  variables has its variables permuted in all  $n!$  ways, the number of different polynomials that are obtained is always a



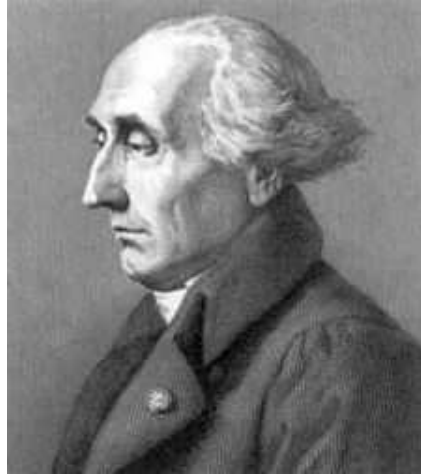


Figure 1.1: Joseph-Louis Lagrange (1736-1813)

factor of  $n!$ . Since all the permutations of  $n$  elements are actually a group, the number of such polynomials is actually the index in the group of permutations of  $n$  elements of the subgroup  $H$  of permutations which preserve the polynomial. So the size of  $H$  divides  $n!$ , which is exactly the number of all permutations of  $n$  elements. This is indeed a particular case of what we call now Lagrange's Theorem.

**Corollary 1.6.** 1. Let  $G$  be a finite group. If  $a \in G$ , then  $|a|$  divides  $|G|$ . In particular,  $a^{|G|} = 1$ .

2. If  $G$  has prime order, then  $G$  is cyclic.

*Proof.* 1. If  $a \in G$  has order say  $m$ , then the subgroup  $H = \{1, a, \dots, a^{m-1}\}$  is a cyclic subgroup of  $G$  with order  $|H| = m$ . Thus  $m$  divides  $|G|$  by the theorem.

2. Since  $|G|$  is prime, we may take  $a \neq 1$  in  $G$ , and since the order of  $a$  has to divide  $|G|$ , we have  $|a| = |G|$ . Thus the cyclic group generated by  $a$  coincides with  $G$ .

□

**Example 1.15.** Using Lagrange's Theorem and its corollaries, we can already determine the groups of order from 1 to 5, up to isomorphism (see Table 1.1). If  $|G|$  is prime, we now know that  $G$  is cyclic.

Let us look at the case where  $G$  is of order 4. Let  $g \in G$ . We know that the order of  $g$  is either 1, 2 or 4. If the order of  $g$  is 1, this is the identity. If  $G$  contains an element  $g$  of order 4, then that means that  $g$  generates the whole group, thus  $G$  is cyclic. If now  $G$  does not contain an element of order 4, then

$ G $	$G$
1	$\{1\}$
2	$C_2$
3	$C_3$
4	$C_4, C_2 \times C_2$
5	$C_5$

Table 1.1: Groups of order from 1 to 5.  $C_n$  denotes the cyclic group of order  $n$ .

apart the identity, all the elements have order 2. From there, it is easy to obtain a multiplication table for  $G$ , and see that it coincides with the one of the group

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x, y) \mid x, y \in \mathbb{Z}_2\}$$

with binary operation  $(x, y) + (x', y') = (x + x', y + y')$ . This group is called the **Klein group**, and it has several interpretations, for example, it is the group of isometries fixing a rectangle.

*Remark.* The above example also shows that the converse of Lagrange's Theorem is not true. If we take the group  $G = C_2 \times C_2$ , then 4 divides the order of  $G$ , however there is no element of order 4 in  $G$ .

Once Lagrange's Theorem and its corollaries are proven, we can easily deduce Euler's and Fermat's Theorem.

**Theorem 1.7. (Euler's Theorem).** *If  $a$  and  $n$  are relatively prime positive integers, with  $n \geq 2$ , then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

*Proof.* Since  $a$  and  $n$  are relatively prime, we know from Proposition 1.2 that  $a$  has an inverse modulo  $n$ , and by its corollary that the group of invertible elements has order  $\varphi(n)$ . Thus

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

by Lagrange's Theorem first corollary. □

**Corollary 1.8. (Fermat's Little Theorem).** *If  $p$  is a prime and  $a$  is a positive integer not divisible by  $p$ , then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is particular case of Euler's Theorem when  $n$  is a prime, since then  $\varphi(n) = p - 1$ .

## 1.4 Normal subgroups and quotient group

Given a group  $G$  and a subgroup  $H$ , we have seen how to define the cosets of  $H$ , and thanks to Lagrange's Theorem, we already know that the number of cosets  $[G : H]$  is related to the order of  $H$  and  $G$  by  $|G| = |H|[G : H]$ . A priori, the set of cosets of  $H$  has no structure. We are now interested in a criterion on  $H$  to give the set of its cosets a structure of group.

In what follows, we may write  $H \leq G$  for  $H$  is a subgroup of  $G$ .

**Definition 1.10.** Let  $G$  be a group and  $H \leq G$ . We say that  $H$  is a **normal** subgroup of  $G$ , or that  $H$  is **normal** in  $G$ , if we have

$$cHc^{-1} = H, \text{ for all } c \in G.$$

We denote it  $H \trianglelefteq G$ , or  $H \triangleleft G$  when we want to emphasize that  $H$  is a proper subgroup of  $G$ .

The condition for a subgroup to be normal can be stated in many slightly different ways.

**Lemma 1.9.** *Let  $H \leq G$ . The following are equivalent:*

1.  $cHc^{-1} \subseteq H$  for all  $c \in G$ .
2.  $cHc^{-1} = H$  for all  $c \in G$ , that is  $cH = Hc$  for all  $c \in G$ .
3. Every left coset of  $H$  in  $G$  is also a right coset (and vice-versa, every right coset of  $H$  in  $G$  is also a left coset).

*Proof.* Clearly 2. implies 1., now  $cHc^{-1} \subseteq H$  for all  $c \in G$  if and only if  $cH \subseteq Hc$ . Let  $x \in Hc$ , that is  $x = hc$  for some  $h \in H$ , so that

$$x = (cc^{-1})hc = c(c^{-1}hc) = ch'$$

for some  $h' \in H$  since  $cHc^{-1} \subset H$  for all  $c$  and thus in particular for  $c^{-1}$ . This shows that  $Hc$  is included in  $cH$  or equivalently that  $H \subseteq cHc^{-1}$ .

Also 2. clearly implies 3. Now suppose that  $cH = Hd$ . This means that  $c$  belongs to  $Hd$  by assumption and to  $Hc$  by definition, which means that  $Hd = Hc$ .  $\square$

**Example 1.16.** Let  $GL_n(\mathbb{R})$  be the group of  $n \times n$  real invertible matrices, and let  $SL_n(\mathbb{R})$  be the subgroup formed by matrices whose determinant is 1. Let us see that  $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ .

For that, we have to check that  $ABA^{-1} \in SL_n(\mathbb{R})$  for all  $B \in SL_n(\mathbb{R})$  and  $A \in GL_n(\mathbb{R})$ . This is clearly true since

$$\det(ABA^{-1}) = \det(B) = 1.$$

**Proposition 1.10.** *If  $H$  is normal in  $G$ , then the cosets of  $H$  form a group.*

*Proof.* Let us first define a binary operation on the cosets:  $(aH, bH) \mapsto (aH)(bH) = \{(ah)(bh'), ah \in aH, bh' \in bH\}$ . We need to check that the definition of group is satisfied.

- **closure.** This is the part which asks a little bit of work. Since  $cH = Hc$  for all  $c \in G$ , then

$$(aH)(bH) = a(Hb)H = a(bH)H = abHH = abH.$$

Note that this product does not depend on the choice of representatives.

- **Associativity** comes from  $G$  being associative.
- The **identity** is given by the coset  $1H = H$ .
- The **inverse** of the coset  $aH$  is  $a^{-1}H$ .

□

**Definition 1.11.** The group of cosets of a normal subgroup  $N$  of  $G$  is called the **quotient group** of  $G$  by  $N$ . It is denoted by  $G/N$ .

Let us finish this section by discussing the connection between normal subgroups and homomorphisms. The first normal subgroup of interest will be the kernel of a group homomorphism.

Recall that if  $f : G \rightarrow H$  is a group homomorphism, the **kernel** of  $f$  is defined by

$$\text{Ker}(f) = \{a \in G, f(a) = 1\}.$$

It is easy to see that  $\text{Ker}(f)$  is a normal subgroup of  $G$ , since

$$f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)f(a)^{-1} = 1$$

for all  $b \in \text{Ker}(f)$  and all  $a \in G$ .

The converse is more interesting.

**Proposition 1.11.** *Let  $G$  be a group. Every normal subgroup of  $G$  is the kernel of a homomorphism.*

*Proof.* Suppose that  $N \trianglelefteq G$  and consider the map

$$\pi : G \rightarrow G/N, a \mapsto aN.$$

To prove the result, we have to show that  $\pi$  is a group homomorphism whose kernel is  $N$ . First note that  $\pi$  is indeed a map from group to group since  $G/N$  is a group by assuming that  $N$  is normal. Then we have that

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$$

where the second equality comes from the group structure of  $G/N$ . Finally

$$\text{Ker}(\pi) = \{a \in G \mid \pi(a) = N\} = \{a \in G \mid aN = N\} = N.$$

□

**Definition 1.12.** Let  $N \trianglelefteq G$ . The group homomorphism

$$\pi : G \rightarrow G/N, a \mapsto aN$$

is called the **natural** or **canonical** map or projection.

Recall for further usage that for  $f$  a group homomorphism, we have the following characterization of injectivity: a homomorphism  $f$  is injective if and only if its kernel is trivial (that is, contains only the identity element). Indeed, if  $f$  is injective, then  $\text{Ker}(f) = \{a, f(a) = 1\} = \{1\}$  since  $f(1) = 1$ . Conversely, if  $\text{Ker}(f) = \{1\}$  and we assume that  $f(a) = f(b)$ , then

$$f(ab^{-1}) = f(a)f(b)^{-1} = f(a)f(a)^{-1} = 1$$

and  $ab^{-1} = 1$  implying that  $a = b$  and thus  $f$  is injective.

**Terminology.**

**monomorphism**=injective homomorphism

**epimorphism**=surjective homomorphism

**isomorphism**=bijective homomorphism

**endomorphism**=homomorphism of a group to itself

**automorphism**=isomorphism of a group with itself

We have looked so far at the particular subgroup of  $G$  which is its kernel. The proposition below describes more generally subgroups of  $G$  and  $H$ .

**Proposition 1.12.** *Let  $f : G \rightarrow H$  be a homomorphism.*

1. *If  $K$  is a subgroup of  $G$ , then  $f(K)$  is a subgroup of  $H$ . If  $f$  is an epimorphism and  $K$  is normal, then  $f(K)$  is normal.*
2. *If  $K$  is a subgroup of  $H$ , then  $f^{-1}(K) = \{x \in G, f(x) \in K\}$  is a subgroup of  $G$ . If  $K$  is normal, so is  $f^{-1}(K)$ .*

*Proof.* 1. To prove that  $f(K)$  is a subgroup of  $H$ , it is enough to show that  $f(a)f(b)^{-1} \in f(K)$  by Proposition 1.1, which is clear from

$$f(a)f(b)^{-1} = f(ab^{-1}) \in f(K).$$

If  $K$  is normal, we have to show that  $cf(K)c^{-1} = f(K)$  for all  $c \in H$ . Since  $f$  is an epimorphism, there exists  $d \in G$  such that  $f(d) = c$ , so that

$$cf(K)c^{-1} = f(d)f(K)f(d)^{-1} = f(dKd^{-1}) = f(K)$$

using that  $K$  is normal.

2. As before, to prove that  $f^{-1}(K)$  is a subgroup of  $G$ , it is enough to showing that  $ab^{-1} \in f^{-1}(K)$  for  $a, b \in f^{-1}(K)$ , which is equivalent to show that  $f(ab^{-1}) \in K$ . This is now true since  $f(ab^{-1}) = f(a)f(b)^{-1}$  with  $a, b \in f^{-1}(K)$  and  $K$  a subgroup.

For the second claim, we have to show that

$$cf^{-1}(K)c^{-1} = f^{-1}(K)$$

or equivalently

$$f(cf^{-1}(K)c^{-1}) = K, \quad c \in G.$$

For  $c \in G$  and  $a \in f^{-1}(K)$ , then

$$f(cac^{-1}) = f(c)f(a)f(c)^{-1} \in K$$

since  $K$  is normal. □

## 1.5 The isomorphism theorems

This section presents different isomorphism theorems which are important tools for proving further results. The first isomorphism theorem, that will be the second theorem to be proven after the factor theorem, is easier to motivate, since it will help us in computing quotient groups.

But let us first start with the so-called factor theorem. Assume that we have a group  $G$  which contains a normal subgroup  $N$ , another group  $H$ , and  $f : G \rightarrow H$  a group homomorphism. Let  $\pi$  be the canonical projection (see Definition 1.12) from  $G$  to the quotient group  $G/N$ :

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \bar{f} & \\ G/N & & \end{array}$$

We would like to find a homomorphism  $\bar{f} : G/N \rightarrow H$  that makes the diagram commute, namely

$$f(a) = \bar{f}(\pi(a))$$

for all  $a \in G$ .

**Theorem 1.13. (Factor Theorem).** *Any homomorphism  $f$  whose kernel  $K$  contains  $N$  can be factored through  $G/N$ . In other words, there is a unique homomorphism  $\bar{f} : G/N \rightarrow H$  such that  $\bar{f} \circ \pi = f$ . Furthermore*

1.  $\bar{f}$  is an epimorphism if and only if  $f$  is.
2.  $\bar{f}$  is a monomorphism if and only if  $K = N$ .

3.  $\bar{f}$  is an isomorphism if and only if  $f$  is an epimorphism and  $K = N$ .

*Proof. Unicity.* Let us start by proving that if there exists  $\bar{f}$  such that  $\bar{f} \circ \pi = f$ , then it is unique. Let  $\tilde{f}$  be another homomorphism such that  $\tilde{f} \circ \pi = f$ . We thus have that

$$(\bar{f} \circ \pi)(a) = (\tilde{f} \circ \pi)(a) = f(a)$$

for all  $a \in G$ , that is

$$\bar{f}(aN) = \tilde{f}(aN) = f(a).$$

This tells us that for all  $bN \in G/N$  for which there exists an element  $b$  in  $G$  such that  $\pi(b) = bN$ , then its image by either  $\bar{f}$  or  $\tilde{f}$  is determined by  $f(b)$ . This shows that  $\bar{f} = \tilde{f}$  by surjectivity of  $\pi$ .

**Existence.** Let  $aN \in G/N$  such that  $\pi(a) = aN$  for  $a \in G$ . We define

$$\bar{f}(aN) = f(a).$$

This is the most natural way to do it, however, we need to make sure that this is indeed well-defined, in the sense that it should not depend on the choice of the representative taken in the coset. Let us thus take another representative, say  $b \in aN$ . Since  $a$  and  $b$  are in the same coset, they satisfy  $a^{-1}b \in N \subset K$ , where  $K = \text{Ker}(f)$  by assumption. Since  $a^{-1}b \in K$ , we have  $f(a^{-1}b) = 1$  and thus  $f(a) = f(b)$ .

Now that  $\bar{f}$  is well defined, let us check this is indeed a group homomorphism. First note that  $G/N$  is indeed a group since  $N \trianglelefteq G$ . Then, we have

$$\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$$

and  $\bar{f}$  is a homomorphism.

1. The fact that  $\bar{f}$  is an epimorphism if and only if  $f$  is comes from the fact that both maps have the same image.
2. First note that the statement  $\bar{f}$  is a monomorphism if and only if  $K = N$  makes sense since  $K = \text{Ker}(f)$  is indeed a normal subgroup, as proved earlier.

To show that  $\bar{f}$  is a monomorphism is equivalent to show that  $\text{Ker}(\bar{f})$  is trivial. By definition, we have

$$\begin{aligned} \text{Ker}(\bar{f}) &= \{aN \in G/N, \bar{f}(aN) = 1\} \\ &= \{aN \in G/N, \bar{f}(\pi(a)) = f(a) = 1\} \\ &= \{aN \in G/N, a \in K = \text{Ker}(f)\}. \end{aligned}$$

So the kernel of  $\bar{f}$  is exactly those cosets of the form  $aN$  with  $a \in K$ , but for the kernel to be trivial, we need it to be equal to  $N$ , that is we need  $K = N$ .

3. This is just a combination of the first two parts.

□

We are now ready to state the first isomorphism theorem.

**Theorem 1.14. (1st Isomorphism Theorem).** *If  $f : G \rightarrow H$  is a homomorphism with kernel  $K$ , then the image of  $f$  is isomorphic to  $G/K$ :*

$$\text{Im}(f) \simeq G/\text{Ker}(f).$$

*Proof.* We know from the Factor Theorem that

$$\bar{f} : G/\text{Ker}(f) \rightarrow H$$

is an isomorphism if and only if  $f$  is an epimorphism, and clearly  $f$  is an epimorphism on its image, which concludes the proof. □

**Example 1.17.** We have seen in Example 1.16 that  $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ . Consider the map

$$\det : GL_n(\mathbb{R}) \rightarrow (\mathbb{R}^*, \cdot),$$

which is a group homomorphism. We have that  $\text{Ker}(\det) = SL_n(\mathbb{R})$ . The 1st Isomorphism Theorem tells that

$$\text{Im}(\det) \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R}).$$

It is clear that  $\det$  is surjective, since for all  $a \in \mathbb{R}^*$ , one can take the diagonal matrix with all entries at 1, but one which is  $a$ . Thus we conclude that

$$\mathbb{R}^* \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R}).$$

The 1st Isomorphism Theorem can be nicely illustrated in terms of exact sequences.

**Definition 1.13.** Let  $F, G, H, I, \dots$  be groups, and let  $f, g, h, \dots$  be group homomorphisms. Consider the following sequence:

$$\dots \quad F \xrightarrow{f} G \xrightarrow{g} H \xrightarrow{h} I \quad \dots$$

We say that this sequence is **exact in one point** (say  $G$ ) if  $\text{Im}(f) = \text{Ker}(g)$ . A sequence is **exact** if it is exact in all points.

A **short exact sequence** of groups is of the form

$$1 \xrightarrow{i} F \xrightarrow{f} G \xrightarrow{g} H \xrightarrow{j} 1$$

where  $i$  is the inclusion and  $j$  is the constant map 1.

**Proposition 1.15.** *Let*

$$1 \xrightarrow{i} F \xrightarrow{f} G \xrightarrow{g} H \xrightarrow{j} 1$$



be a short exact sequence of groups. Then  $\text{Im}(f)$  is normal in  $G$  and we have a group isomorphism

$$G/\text{Im}(f) \simeq H,$$

or equivalently

$$G/\text{Ker}(g) \simeq H.$$

*Proof.* Since the sequence is exact, we have that  $\text{Im}(f) = \text{Ker}(g)$  thus  $\text{Im}(f)$  is a normal subgroup of  $G$ . By the first Isomorphism Theorem, we have that

$$G/\text{Ker}(g) \simeq \text{Im}(g) = H.$$

since  $\text{Im}(g) = \text{Ker}(j) = H$ . □

The formulation in terms of exact sequences is useful to know, since it happens very often in the literature that an exact sequence is given exactly to be able to compute such quotient groups.

Let us state the second and third isomorphism theorem.

**Theorem 1.16. (2nd Isomorphism Theorem).** *If  $H$  and  $N$  are subgroups of  $G$ , with  $N$  normal in  $G$ , then*

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

There are many things to discuss about the statement of this theorem.

- First we need to check that  $HN$  is indeed a subgroup of  $G$ . To show that, notice that  $HN = NH$  since  $N$  is a normal subgroup of  $G$ . This implies that for  $hn \in HN$ , its inverse  $(hn)^{-1} = n^{-1}h^{-1} \in G$  actually lives in  $HN$ , and so does the product  $(hn)(h'n') = h(nh')n'$ .
- Note that by writing  $HN/N$ , we insist on the fact that there is no reason for  $N$  to be a subgroup of  $H$ . On the other hand,  $N$  is a normal subgroup of  $HN$ , since for all  $hn \in HN$ , we have

$$hnNn^{-1}h^{-1} = hNh^{-1} \subseteq N$$

since  $N$  is normal in  $G$ .

- We now know that the right hand side of the isomorphism is a quotient group. In order to see that so is the left hand side, we need to show that  $H \cap N$  is a normal subgroup of  $H$ . This comes by noticing that  $H \cap N$  is the kernel of the canonical map  $\pi : G \rightarrow G/N$  restricted to  $H$ .

Now that all these remarks have been done, it is not difficult to see that the 2nd Isomorphism Theorem follows from the 1st Isomorphism Theorem, as does the 3rd Isomorphism Theorem.

**Theorem 1.17. (3rd Isomorphism Theorem).** *If  $N$  and  $H$  are normal subgroups of  $G$ , with  $N$  contained in  $H$ , then*

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

## 1.6 Direct and semi-direct products

So far, we have seen how given a group  $G$ , we can get smaller groups, such as subgroups of  $G$  or quotient groups. We will now do the other way round, that is, starting with a collection of groups, we want to build larger new groups.

Let us start with two groups  $H$  and  $K$ , and let  $G = H \times K$  be the cartesian product of  $H$  and  $K$ , that is

$$G = \{(h, k), h \in H, k \in K\}.$$

We define a binary operation on this set by doing componentwise multiplication (or addition if the binary operations of  $H$  and  $K$  are denoted additively) on  $G$ :

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2) \in H \times K.$$

Clearly  $G$  is closed under multiplication, its operation is associative (since both operations on  $H$  and  $K$  are), it has an identity element given by  $1_G = (1_H, 1_K)$  and the inverse of  $(h, k)$  is  $(h^{-1}, k^{-1})$ . In summary,  $G$  is a group.

**Definition 1.14.** Let  $H, K$  be two groups. The group  $G = H \times K$  with binary operation defined componentwise as described above is called the **external direct product** of  $H$  and  $K$ .

- Examples 1.18.**
1. Let  $\mathbb{Z}_2$  be the group of integers modulo 2. We can build a direct product of  $\mathbb{Z}_2$  with itself, namely  $\mathbb{Z}_2 \times \mathbb{Z}_2$  with additive law componentwise. This is actually the Klein group, also written  $C_2 \times C_2$ . This group is not isomorphic to  $\mathbb{Z}_4$ !
  2. Let  $\mathbb{Z}_2$  be the group of integers modulo 2, and  $\mathbb{Z}_3$  be the group of integers modulo 3. We can build a direct product of  $\mathbb{Z}_2$  and  $\mathbb{Z}_3$ , namely  $\mathbb{Z}_2 \times \mathbb{Z}_3$  with additive law componentwise. This group is actually isomorphic to  $\mathbb{Z}_6$ !
  3. The group  $(\mathbb{R}, +) \times (\mathbb{R}, +)$  with componentwise addition is a direct product.

Note that  $G$  contains isomorphic copies  $\bar{H}$  and  $\bar{K}$  of respectively  $H$  and  $K$ , given by

$$\bar{H} = \{(h, 1_K), h \in H\}, \quad \bar{K} = \{(1_H, k), k \in K\},$$

which furthermore are normal subgroups of  $G$ . Let us for example see that  $\bar{H}$  is normal in  $G$ . By definition, we need to check that

$$(h, k)\bar{H}(h^{-1}, k^{-1}) \subseteq \bar{H}, \quad (h, k) \in G.$$

Let  $(h', 1_K) \in \bar{H}$ , we compute that

$$(h, k)(h', 1_K)(h^{-1}, k^{-1}) = (hh'h^{-1}, 1_K) \in \bar{H},$$

since  $hh'h^{-1} \in H$ . The same computation holds for  $\bar{K}$ .

If we gather what we know about  $G, \bar{H}$  and  $\bar{K}$ , we get that

- by definition,  $G = \bar{H}\bar{K}$  and  $\bar{H} \cap \bar{K} = \{1_G\}$ ,
- by what we have just proved,  $\bar{H}$  and  $\bar{K}$  are two normal subgroups of  $G$ .

This motivates the following definition.

**Definition 1.15.** If a group  $G$  contains normal subgroups  $H$  and  $K$  such that  $G = HK$  and  $H \cap K = \{1_G\}$ , we say that  $G$  is the **internal direct product** of  $H$  and  $K$ .

- Examples 1.19.**
1. Consider the Klein group  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , it contains the two subgroups  $H = \{(h, 0), h \in \mathbb{Z}_2\}$  and  $K = \{(0, k), k \in \mathbb{Z}_2\}$ . We have that both  $H$  and  $K$  are normal, because the Klein group is commutative. We also have that  $H \cap K = \{(0, 0)\}$ , so the Klein group is indeed an internal direct product. On the other hand,  $\mathbb{Z}_4$  only contains as subgroup  $H = \{0, 2\}$ , so it is not an internal direct product!
  2. Consider the group  $\mathbb{Z}_2 \times \mathbb{Z}_3$ , it contains the two subgroups  $H = \{(h, 0), h \in \mathbb{Z}_2\}$  and  $K = \{(0, k), k \in \mathbb{Z}_3\}$ . We have that both  $H$  and  $K$  are normal, because the group is commutative. We also have that  $H \cap K = \{(0, 0)\}$ , so this group is indeed an internal direct product. Also  $\mathbb{Z}_6$  contains the two subgroups  $H = \{0, 3\} \simeq \mathbb{Z}_2$  and  $K = \{0, 2, 4\} \simeq \mathbb{Z}_3$ . We have that both  $H$  and  $K$  are normal, because the group is commutative. We also have that  $H \cap K = \{0\}$ , so this group is indeed an internal direct product, namely the internal product of  $\mathbb{Z}_2$  and  $\mathbb{Z}_3$ . This is in fact showing that  $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$ .

The next result makes explicit the connection between internal and external products.

**Proposition 1.18.** *If  $G$  is the internal direct product of  $H$  and  $K$ , then  $G$  is isomorphic to the external direct product  $H \times K$ .*

*Proof.* To show that  $G$  is isomorphic to  $H \times K$ , we define the following map

$$f : H \times K \rightarrow G, f(h, k) = hk.$$

First remark that if  $h \in H$  and  $k \in K$ , then  $hk = kh$ . Indeed, we have using that both  $K$  and  $H$  are normal that

$$(hkh^{-1})k^{-1} \in K, h(kh^{-1}k^{-1}) \in H$$

implying that

$$hkh^{-1}k^{-1} \in K \cap H = \{1\}.$$

We are now ready to prove that  $f$  is a group isomorphism.

1. This is a group homomorphism since

$$f((h, k)(h', k')) = f(hh', kk') = h(h'k)k' = h(kh')k' = f(h, k)f(h', k').$$

2. The map  $f$  is injective. This can be seen by checking that its kernel is trivial. Indeed, if  $f(h, k) = 1$  then

$$hk = 1 \Rightarrow h = k^{-1} \Rightarrow h \in K \Rightarrow h \in H \cap K = \{1\}.$$

We have then that  $h = k = 1$  which proves that the kernel is  $\{(1, 1)\}$ .

3. The map  $f$  is surjective since by definition  $G = HK$ .

□

Note that the definitions of external and internal product are surely not restricted to two groups. One can in general define them for  $n$  groups  $H_1, \dots, H_n$ . Namely

**Definition 1.16.** If  $H_1, \dots, H_n$  are arbitrary groups, the **external direct product** of  $H_1, \dots, H_n$  is the cartesian product

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

with componentwise multiplication.

If  $G$  contains normal subgroups  $H_1, \dots, H_n$  such that  $G = H_1 \cdots H_n$  and each  $g$  can be represented as  $h_1 \cdots h_n$  uniquely, we say that  $G$  is the **internal direct product** of  $H_1, \dots, H_n$ .

We can see a slight difference in the definition of internal product, since in the case of two subgroups, the condition given was not that each  $g$  can be represented uniquely as  $h_1 h_2$ , but instead that the intersection of the two subgroups is  $\{1\}$ . The next proposition shows the connection between these two points of view.

**Proposition 1.19.** *Suppose that  $G = H_1 \cdots H_n$  where each  $H_i$  is a normal subgroup of  $G$ . The following conditions are equivalent.*

1.  $G$  is the internal direct product of the  $H_i$ .
2.  $H_1 H_2 \cdots H_{i-1} \cap H_i = \{1\}$ , for all  $i = 1, \dots, n$ .

*Proof.* Let us prove 1.  $\iff$  2.

1.  $\Rightarrow$  2. Let us assume that  $G$  is the internal direct product of the  $H_i$ , which means that every element in  $G$  can be written uniquely as a product of elements in  $H_i$ . Now let us take  $g \in H_1 H_2 \cdots H_{i-1} \cap H_i = \{1\}$ . We have that  $g \in H_1 H_2 \cdots H_{i-1}$ , which is uniquely written as  $g = h_1 h_2 \cdots h_{i-1} 1_{H_i} \cdots 1_{H_n}$ ,  $h_j \in H_j$ . On the other hand,  $g \in H_i$  thus  $g = 1_{H_1} \cdots 1_{H_{i-1}} g$  and by unicity of the representation, we have  $h_j = 1$  for all  $j$  and  $g = 1$ .
2.  $\Rightarrow$  1. Conversely, let us assume that  $g \in G$  can be written either

$$g = h_1 h_2 \cdots h_n, \quad h_j \in H_j,$$

or

$$g = k_1 k_2 \cdots k_n, \quad k_j \in H_j.$$

Recall that since all  $H_j$  are normal subgroups, then

$$h_i h_j = h_j h_i, \quad h_i \in H_i, \quad h_j \in H_j.$$

(If you cannot recall the argument, check out the proof of Proposition 1.18). This means that we can do the following manipulations:

$$\begin{aligned} h_1 h_2 \cdots h_n &= k_1 k_2 \cdots k_n \\ \iff h_2 \cdots h_n &= \underbrace{(h_1^{-1} k_1)}_{\in H_1} k_2 \cdots k_n \\ \iff h_3 \cdots h_n &= (h_1^{-1} k_1)(h_2^{-1} k_2) k_3 \cdots k_n \end{aligned}$$

and so on and so forth till we reach

$$h_n k_n^{-1} = (h_1^{-1} k_1) \cdots (h_{n-1}^{-1} k_{n-1}).$$

Since the left hand side belongs to  $H_n$  while the right hand side belongs to  $H_1 \cdots H_{n-1}$ , we get that

$$h_n k_n^{-1} \in H_n \cap H_1 \cdots H_{n-1} = \{1\},$$

implying that  $h_n = k_n$ . We conclude the proof by iterating this process. □

Let us get back to the case of two groups. We have seen above that we can endow the cartesian product of two groups  $H$  and  $K$  with a group structure by considering componentwise binary operation

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2) \in H \times K.$$

The choice of this binary operation of course determines the structure of  $G = H \times K$ , and in particular we have seen that the isomorphic copies of  $H$  and  $K$  in  $G$  are normal subgroups. Conversely in order to define an internal direct product, we need to assume that we have two normal subgroups.

We now consider a more general setting, where the subgroup  $K$  does not have to be normal (and will not be in general), for which we need to define a new binary operation on the cartesian product  $H \times K$ . This will lead us to the definition of internal and external semi-direct product.

Recall that an automorphism of a group  $H$  is a bijective group homomorphism from  $H$  to  $H$ . It is easy to see that the set of automorphisms of  $H$  forms a group with respect to the composition of maps and identity element the identity map  $\text{Id}_H$ . We denote it by  $\text{Aut}(H)$ .

**Proposition 1.20.** *Let  $H$  and  $K$  be groups, and let*

$$\rho : K \rightarrow \text{Aut}(H), \quad k \mapsto \rho_k$$

*be a group homomorphism. Then the binary operation*

$$(H \times K) \times (H \times K) \rightarrow (H \times K), \quad ((h, k), (h', k')) \mapsto (h\rho_k(h'), kk')$$

*endows  $H \times K$  with a group structure, with identity element  $(1, 1)$ .*

*Proof.* First notice that the closure property is satisfied.

**(Identity).** Let us show that  $(1, 1)$  is the identity element. We have

$$(h, k)(1, 1) = (h\rho_k(1), k) = (h, k)$$

for all  $h \in H, k \in K$ , since  $\rho_k$  is a group homomorphism. We also have

$$(1, 1)(h', k') = (\rho_1(h'), k') = (h', k')$$

for all  $h' \in H, k' \in K$ , since  $\rho$  being a group homomorphism, it maps  $1_K$  to  $1_{\text{Aut}(K)} = \text{Id}_H$ .

**(Inverse).** Let  $(h, k) \in H \times K$  and let us show that  $(\rho_k^{-1}(h^{-1}), k^{-1})$  is the inverse of  $(h, k)$ . We have

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

We also have

$$\begin{aligned} (\rho_k^{-1}(h^{-1}), k^{-1})(h, k) &= (\rho_k^{-1}(h^{-1})\rho_{k^{-1}}(h), 1) \\ &= (\rho_{k^{-1}}(h^{-1})\rho_{k^{-1}}(h), 1) \end{aligned}$$

using that  $\rho_k^{-1} = \rho_{k^{-1}}$  since  $\rho$  is a group homomorphism. Now

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

using that  $\rho_{k^{-1}}$  is a group homomorphism for all  $k \in K$ .

**Associativity.** This is the last thing to check. On the one hand, we have

$$\begin{aligned} [(h, k)(h', k')](h'', k'') &= (h\rho_k(h'), kk')(h'', k'') \\ &= (h\rho_k(h')\rho_{kk'}(h''), (kk')k''), \end{aligned}$$

while on the other hand

$$\begin{aligned} (h, k)[(h', k')(h'', k'')] &= (h, k)(h'\rho_{k'}(h''), k'k'') \\ &= (h\rho_k(h'\rho_{k'}(h'')), k(k'k'')). \end{aligned}$$

Since  $K$  is a group, we have  $(kk')k'' = k(k'k'')$ . We now look at the first component. Note that  $\rho_{kk'} = \rho_k \circ \rho_{k'}$  using that  $\rho$  is a group homomorphism, so that

$$h\rho_k(h')\rho_{kk'}(h'') = h\rho_k(h')\rho_k(\rho_{k'}(h'')).$$

Furthermore,  $\rho_k$  is a group homomorphism, yielding

$$h\rho_k(h')\rho_k(\rho_{k'}(h'')) = h\rho_k(h'\rho_{k'}(h''))$$

which concludes the proof.  $\square$

We are now ready to define the first semi-direct product.

**Definition 1.17.** Let  $H$  and  $K$  be two groups, and let

$$\rho : K \rightarrow \text{Aut}(H)$$

be a group homomorphism. The set  $H \times K$  endowed with the binary operation

$$((h, k), (h', k')) \mapsto (h\rho_k(h'), kk')$$

is a group  $G$  called an **external semi-direct product** of  $H$  and  $K$  by  $\rho$ , denoted by  $G = H \times_\rho K$ .

**Example 1.20.** Let us consider the group  $\mathbb{Z}_2$  of integers modulo 2. Suppose we want to compute the semi-direct product of  $\mathbb{Z}_2$  with itself, then we need to first determine  $\text{Aut}(\mathbb{Z}_2)$ . Since an automorphism of  $\mathbb{Z}_2$  must send 0 to 0, it has no other choice than send 1 to 1, and thus  $\text{Aut}(\mathbb{Z}_2)$  is only the identity map, in which case the semi-direct product is just the direct product, since  $\rho_k$  is the identity for every  $k$ . To have a bigger automorphism group, let us consider  $H = \mathbb{Z}_3$ . In that case, apart the identity map, we also have the map  $x \mapsto x^{-1}$ , that is  $0 \mapsto 0$ ,  $1 \mapsto 2$ ,  $2 \mapsto 1$ . Thus  $\rho(0) = \rho_0$  is the identity,  $\rho(1) = \rho_1$  is the inverse map, and we can form the external semi-direct product  $G = \mathbb{Z}_3 \times_\rho \mathbb{Z}_2$ .

In fact, this example holds for  $\mathbb{Z}_n$ ,  $n \geq 3$ .

**Example 1.21.** Let  $H = \mathbb{Z}_n$  be the group of integers mod  $n$ ,  $K = \mathbb{Z}_2$  be the group of integers mod 2, and let  $\rho : K \rightarrow \text{Aut}(H)$  be the homomorphism that sends 0 to the identity, and 1 to the inverse map of  $H$ , given by  $x \mapsto x^{-1}$ , which is indeed a group homomorphism of  $H$  since  $H$  is abelian. Since the subgroup of  $\text{Aut}(H)$  generated by the inverse map is of order 2, it is isomorphic to  $K$ . We can thus define the external semi-direct product  $G = \mathbb{Z}_n \times_\rho \mathbb{Z}_2$ .

We can make observations similar to what we did for direct products. Namely, we can identify two isomorphic copies  $\bar{H}$  and  $\bar{K}$  of respectively  $H$  and  $K$ , given by

$$\bar{H} = \{(h, 1_K), h \in H\}, \quad \bar{K} = \{(1_H, k), k \in K\},$$

and look at the properties of these subgroups.

- The subgroup  $\bar{H} = \{(h, 1), h \in H\}$  is normal in  $H \times_\rho K$ , this can be seen by writing down the definition of normal subgroup. (We cannot claim the same for  $\bar{K}$ !).
- We have  $\bar{H}\bar{K} = H \times_\rho K$ , since every element  $(h, k) \in H \times_\rho K$  can be written as  $(h, 1)(1, k)$  (indeed  $(h, 1)(1, k) = (h\rho_1(1), k) = (h, k)$ ).
- We have  $\bar{H} \cap \bar{K} = \{1_G\}$ .

This motivates the definition of internal semi-direct products.

**Definition 1.18.** Let  $G$  be a group with subgroups  $H$  and  $K$ . We say that  $G$  is the **internal semi-direct product** of  $H$  and  $K$  if  $H$  is a normal subgroup of  $G$ , such that  $HK = G$  and  $H \cap K = \{1_G\}$ . It is denoted by

$$G = H \rtimes K.$$

**Example 1.22.** The dihedral group  $D_n$  is the group of all reflections and rotations of a regular polygon with  $n$  vertices centered at the origin. It has order  $2n$ . Let  $a$  be a rotation of angle  $2\pi/n$  and let  $b$  be a reflection. We have that

$$D_n = \{a^i b^j, 0 \leq i \leq n-1, j = 0, 1\},$$

with

$$a^n = b^2 = (ba)^2 = 1.$$

We thus have that  $\langle a \rangle = C_n$  and  $\langle b \rangle = C_2$ , where  $C_n$  denotes the cyclic group of order  $n$ .

The geometric interpretation of  $D_n$  as symmetries of a regular polygon with  $n$  vertices holds for  $n \geq 3$ , however, note that when  $n = 2$ , we can still look at the relations defined above: we then have  $a^2 = b^2 = (ba)^2 = 1$ , thus  $D_2$  contains only 4 elements, the identity and 3 elements of order 2, showing that it is isomorphic to the Klein group  $C_2 \times C_2$ .

To prove, for  $n \geq 3$ , that

$$D_n \simeq C_n \rtimes C_2,$$

we are left to check that  $\langle a \rangle \cap \langle b \rangle = \{1\}$  and that  $\langle a \rangle$  is normal in  $D_n$ . The former can be seen geometrically (a reflection cannot be obtained by possibly successive rotations of angle  $2\pi/n$ ,  $n \geq 3$ ). For the latter, we first show that

$$bab^{-1} \in \langle a \rangle,$$

which can be easily checked, since  $(ba)^2 = baba = 1$ , thus  $bab = a^{-1} = bab^{-1}$  using that  $b^2 = 1$ . This also shows that  $ba = a^{-1}b$  from which we have:

$$ba^2b^{-1} = baab^{-1} = a^{-1}(bab^{-1}) \in \langle a \rangle,$$

similarly

$$ba^3b^{-1} = baa^2b^{-1} = a^{-1}(ba^2b^{-1}) \in \langle a \rangle.$$

Again similarly to the case of direct products, these assumptions guarantee that we can write uniquely elements of the internal semi-direct product. Let us repeat things explicitly.

**Lemma 1.21.** Let  $G$  be a group with subgroups  $H$  and  $K$ . Suppose that  $G = HK$  and  $H \cap K = \{1_G\}$ . Then every element  $g$  of  $G$  can be written uniquely in the form  $hk$ , for  $h \in H$  and  $k \in K$ .

*Proof.* Since  $G = HK$ , we know that  $g$  can be written as  $hk$ . Suppose it can also be written as  $h'k'$ . Then  $hk = h'k'$  so  $h^{-1}h' = k'k^{-1} \in H \cap K = \{1\}$ . Therefore  $h = h'$  and  $k = k'$ .  $\square$



The internal and external direct products were two sides of the same objects, so are the internal and external semi-direct products. If  $G = H \times_{\rho} K$  is the external semi-direct product of  $H$  and  $K$ , then  $\bar{H} = H \times \{1\}$  is a normal subgroup of  $G$  and it is clear that  $G$  is the internal semi-direct product of  $H \times \{1\}$  and  $\{1\} \times K$ . This reasoning allows us to go from external to internal semi-direct products. The result below goes in the other direction, from internal to external semi-direct products.

**Proposition 1.22.** *Suppose that  $G$  is a group with subgroups  $H$  and  $K$ , and  $G$  is the internal semi-direct product of  $H$  and  $K$ . Then  $G \simeq H \times_{\rho} K$  where  $\rho : K \rightarrow \text{Aut}(H)$  is given by  $\rho_k(h) = khk^{-1}$ ,  $k \in K$ ,  $h \in H$ .*

*Proof.* Note that  $\rho_k$  belongs to  $\text{Aut}(H)$  since  $H$  is normal.

By the above lemma, every element  $g$  of  $G$  can be written uniquely in the form  $hk$ , with  $h \in H$  and  $k \in K$ . Therefore, the map

$$\varphi : H \times_{\rho} K \rightarrow G, \quad \varphi(h, k) = hk$$

is a bijection. It only remains to show that this bijection is a homomorphism.

Given  $(h, k)$  and  $(h', k')$  in  $H \times_{\rho} K$ , we have

$$\varphi((h, k)(h', k')) = \varphi((h\rho_k(h'), kk')) = \varphi(hkh'hk^{-1}, kk') = hkh'hk' = \varphi(h, k)\varphi(h', k').$$

Therefore  $\varphi$  is a group isomorphism, which concludes the proof.  $\square$

In words, we have that every internal semi-direct product is isomorphic to some external semi-direct product, where  $\rho$  is the conjugation.

**Example 1.23.** Consider the dihedral group  $D_n$  from the previous example:

$$D_n \simeq C_n \rtimes C_2.$$

According to the above proposition,  $D_n$  is isomorphic to an external semi-direct product

$$D_n \simeq C_n \times_{\rho} C_2,$$

where

$$\rho : C_2 \rightarrow \text{Aut}(C_n),$$

maps to the conjugation in  $\text{Aut}(C_n)$ . We have explicitly that

$$1 \mapsto \rho_1 = \text{Id}_{C_n}, \quad b \mapsto \rho_b, \quad \rho_b(a) = bab^{-1} = a^{-1}.$$

In fact, we are back to Example 1.21!

Before finishing this section, note the following distinction: the external (semi-)direct product of groups allows to construct new groups starting from different abstract groups, while the internal (semi-)direct product helps in analyzing the structure of a given group.

$ G $	$G$ abelian	$G$ non-abelian
1	$\{1\}$	-
2	$C_2$	-
3	$C_3$	-
4	$C_4, C_2 \times C_2$	-
5	$C_5$	-
6	$C_6 = C_3 \times C_2$	$D_3 = C_3 \rtimes C_2$
7	$C_7$	-
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	$D_4 = C_4 \rtimes C_2$

Table 1.2:  $C_n$  denotes the cyclic group of order  $n$ ,  $D_n$  the dihedral group

**Example 1.24.** Thanks to the new structures we have seen in this section, we can go on our investigation of groups of small orders. We can get two new groups of order 6 and 4 of order 8:

- $C_3 \times C_2$  is the direct product of  $C_3$  and  $C_2$ . You may want to check that it is actually isomorphic to  $C_6$ .
- The dihedral group  $D_3 = C_3 \rtimes C_2$  is the semi-direct product of  $C_3$  and  $C_2$ . We get similarly  $D_4 = C_4 \rtimes C_2$ .
- The direct product  $C_4 \times C_2$  and the direct product of the Klein group  $C_2 \times C_2$  with  $C_2$ .

The table actually gives an exact classification of groups of small order (except the missing non-abelian quaternion group of order 8), though we have not proven it. The reason why the quaternion group of order 8 is missing is exactly because it cannot be written as a semi-direct product of smaller groups (see Exercises).

## 1.7 Permutations and Group action

Since we introduced the definition of group as a set with a binary operation which is closed, we have been computing things internally, that is inside a group structure. This was the case even when considering cartesian products of groups, where the first thing we did was to endow this set with a group structure.

In this section, we wonder what happens if we have a group and a set, which may or may not have a group structure. We will define a group action, that is a way to do computations with two objects, one with a group law, not the other one.

As a first result, we will prove the so-called Cayley's theorem, whose proof will motivate the introduction of group action. Since the statement of this theorem uses permutation groups, we start by recalling the necessary definitions. We will give enough background on permutations to define the alternating group, a group which is useful as an illustration of many concepts!

**Definition 1.19.** A **permutation** of a set  $S$  is a bijection on  $S$ . The set of all such functions (with respect to function composition) is a group called the **symmetric group** on  $S$ . We denote by  $S_n$  the symmetric group on  $n$  elements.

**Example 1.25.** Consider the symmetric group  $S_3$  of permutations on 3 elements. It is given by (note here that by  $ab$  we mean that we first apply the permutation  $b$ , then  $a$ )

$$\begin{aligned} e & : 123 \rightarrow 123 \text{ or } () \\ a & : 123 \rightarrow 213 \text{ or } (12) \\ b & : 123 \rightarrow 132 \text{ or } (23) \\ ba & : 123 \rightarrow 312 \text{ or } (132) \\ ab & : 123 \rightarrow 231 \text{ or } (123) \\ aba & : 123 \rightarrow 321 \text{ or } (13) \end{aligned}$$

One can check that this is indeed a group. The notation  $(132)$  means that the permutation sends 1 to 3, 3 to 2, and 2 to 1.

We can generally write a permutation on  $m$  elements as  $(i_1, \dots, i_m)$ , which is called a cycle notation. The permutation  $(i_1, \dots, i_m)$  is called an  $m$ -**cycle**. When  $m = 2$ , a 2-cycle is called a **transposition**. Note that several different cycles can represent the same permutation (e.g.,  $(132) = (321) = (213)$ ), and not every permutation is a cycle. For example, if we consider  $1 \mapsto 2$ ,  $2 \mapsto 1$ ,  $3 \mapsto 4$ ,  $4 \mapsto 3$ , this permutation is not a cycle. However, it is clearly the product of two disjoint cycles, namely  $(12)(34)$ . Formally, we say that two cycles  $(i_1, \dots, i_s)$  and  $(j_1, \dots, j_t)$  are disjoint if and only if  $\{i_1, \dots, i_s\} \cap \{j_1, \dots, j_t\}$  is empty. Such a decomposition of a permutation into product of disjoint cycles is true in general.

**Proposition 1.23.** *Every element of  $S_n$  can be expressed uniquely as a product of disjoint cycles, up to ordering of the cycles, and notational redundancy within each cycle. Furthermore, every cycle can be written as a product of transpositions.*

*Proof.* Let  $\sigma$  be an element of  $S_n$ . Choose any index  $i_1 \in \{1, \dots, n\}$ . By applying  $\sigma$  repeatedly on  $i_1$ , we construct a sequence of elements of  $\{1, \dots, n\}$ :  $i_1, i_2, \dots$ , where  $i_j = \sigma(i_{j-1})$  for  $j \geq 2$ . If we let  $j$  grow, this sequence necessarily contains repetitions: suppose that the  $k$ th term is the first one which is repeated, that is  $i_k = i_j$  with  $j < k$ . But this means that both  $i_{k-1}$  and  $i_{j-1}$  are mapped to  $i_k$  by  $\sigma$ , and since  $\sigma$  is a bijection, two elements cannot be mapped to  $i_k$ , thus it must be that  $i_k = i_1$  (the only element which has not yet a preimage). We then see that  $\sigma$  defines a  $k - 1$ -cycle

$$(i_1, \dots, i_{k-1}).$$

If  $k - 1 = n$ , we are done. If not, we take  $i'_1$  another index not covered by the first cycle, and iterate. This second cycle has to be disjoint from the first one, since  $\sigma$  is a bijection. We then obtain a disjoint cycle representation for  $\sigma$ .

Now take an  $l$ -cycle  $(i_1, \dots, i_l)$ . It can be rewritten as

$$(i_1, \dots, i_l) = (i_1 \ i_2)(i_2 \ i_3) \cdots (i_{l-1} \ i_l).$$

Indeed, start with the right hand-side:  $i_l$  and  $i_{l-1}$  are swapped. Thus  $(i_1, \dots, i_l)$  is mapped to an  $l$ -tuple whose last 2 terms are  $i_l, i_{l-1}$ . The next transposition is  $(i_{l-2}, i_{l-1})$ , thus both terms are swapped, and we now have as last 3 terms  $i_{l-1}, i_l, i_{l-2}$ . The next swap will yield

$$i_{l-2}, i_{l-1}, i_l, i_{l-3}$$

and by iterating this process, we reach the last swap  $(i_1, i_2)$ , that is

$$i_2, i_3, \dots, i_l, i_1$$

as we wanted to prove.  $\square$

The representation has a product of transpositions is not unique, for example

$$(2, 5, 3, 6) = (2, 6)(2, 3)(2, 5) = (5, 2)(3, 5)(6, 3) = (1, 7)(2, 6)(2, 3)(2, 5)(1, 7).$$

We can however define an invariant of a permutation, called the parity.

**Definition 1.20.** An element of  $S_n$  is said to be **even** if it can be expressed as a product of an even number of transpositions. It is said **odd** otherwise.

For this definition to make sense, parity of an element of  $S_n$  should be unique, which it is.

**Theorem 1.24.** For  $n \geq 2$ , every element of  $S_n$  has a unique parity, even or odd.

*Proof.* To prove this, we need to introduce some ordering on the permutations. We call the switching number of a permutation  $\sigma$  the number of ordered pairs  $(i, j)$  with  $i < j$  but  $\sigma(i) > \sigma(j)$ . The switching number is an invariant of a permutation. Let  $t$  be the switching number of  $\sigma$ , and let  $\tau$  be an arbitrary transposition, say  $\tau = (i \ j)$ . Without loss of generality, we may assume that  $i$  comes before  $j$  in the permutation

$$\sigma(1), \dots, \sigma(n).$$

By applying  $\tau$  to  $\sigma$ , we switch  $i$  and  $j$ , and the picture now looks like

$$\begin{aligned} (1, 2, \dots, \sigma^{-1}(i), \dots, \sigma^{-1}(j), \dots, n) &\xrightarrow{\sigma} (\sigma(1), \sigma(2), \dots, i, \dots, j, \dots, \sigma(n)) \\ &\xrightarrow{\tau} (\sigma(1), \sigma(2), \dots, \tau(i), \dots, \tau(j), \dots, \sigma(n)) \end{aligned}$$

(where the first vector is ordered, but not the second and the third).

To understand the effect of the transposition  $\tau$  on the switching number of  $\sigma$  (that is we are computing the switching number of  $\tau\sigma$  and see how it differs from that of  $\sigma$ ), we need to remember that we are looking at all the ordered pairs  $(k, l)$ ,  $k < l$ , in  $(1, 2, \dots, n)$ :

1. For the ordered pair  $(\sigma^{-1}(i), \sigma^{-1}(j))$ , when applying  $\sigma$ , either (a) the ordering is preserved (i.e.,  $i < j$ ), the switching number thus does not change, however when applying  $\tau$ , the ordering is reversed, and thus  $t$  increases by 1, or (b) the ordering is changed, but  $\tau$  changes again the ordering, so that  $t$  decreases by 1.
2. Let us now assume that  $i < j$  (if not do the same with  $j > i$ ). Then for every index  $l$  such  $i < l < j$ , we can look at the non-ordered pairs  $(i, l)$  and  $(l, j)$ . It might be that  $\sigma^{-1}(i)$  is either greater or smaller than  $\sigma^{-1}(l)$ , yielding one ordered pair or the other, and similarly for  $\sigma^{-1}(j)$  and  $\sigma^{-1}(l)$ . Thus each ordered pair might or not contribute to the switching number of  $\sigma$ , but after  $\tau$  is applied,  $i$  and  $j$  are reversed, and thus both  $(i, l)$  and  $(l, j)$  are changed at once. Thus the switching number increases by 2, decreases by 2, or does not change. We can write down the cases explicitly:

$$(\sigma^{-1}(i), \sigma^{-1}(l)), (\sigma^{-1}(l), \sigma^{-1}(j)) \xrightarrow{\sigma} (i, l), (l, j) \xrightarrow{\tau} (j, l), (l, i), \quad i < l < j$$

thus the switching number of  $\sigma$  is  $t$  including no switch for these 2 pairs, and that of  $\tau\sigma$  has two switches for these 2 paires, thus is of  $t + 2$ .

$$(\sigma^{-1}(i), \sigma^{-1}(l)), (\sigma^{-1}(j), \sigma^{-1}(l)) \xrightarrow{\sigma} (i, l), (j, l) \xrightarrow{\tau} (j, l), (i, l), \quad i < l < j$$

and the switching number of  $\sigma$  is here  $t$  including one switch for the second pair, and that of  $\tau\sigma$  has one switch for the first pair, but none for the second, thus a total of  $t$ . The case  $(\sigma^{-1}(l), \sigma^{-1}(i)), (\sigma^{-1}(l), \sigma^{-1}(j))$  also gives  $t$ , and finally

$$(\sigma^{-1}(l), \sigma^{-1}(i)), (\sigma^{-1}(j), \sigma^{-1}(l)) \xrightarrow{\sigma} (l, i), (j, l) \xrightarrow{\tau} (l, j), (i, l), \quad i < l < j$$

has a switching number of  $t$  for  $\sigma$  including two switches for these 2 pairs, and  $\tau\sigma$  has no switch, thus a total of  $t - 2$ .

3. All the non-ordered pairs  $(k, l)$ , where  $l < i < j$  and  $k < l$  or  $k > l$ , or  $l > j > i$  and  $k < l$  or  $k > l$  (that is all the cases not considered so far) do not induce any change in the switching number, since by swapping  $i$  and  $j$ , we do not change the ordering of the pairs.

This shows that given a permutation  $\sigma$  with switching number  $t$ , composing with one transposition always changes the parity of the switching number. Since the switching number is invariant, this means that it always takes an even number of transpositions applied to  $\sigma$  to have a chance to keep the same switching number. This establishes that the parity of a permutation is either even or odd, but not both.  $\square$

**Definition 1.21.** The set of even permutations forms a subgroup of  $S_n$  called the [alternating group](#), denoted by  $A_n$ .

Note that if  $\tau$  is any odd permutation, then the coset  $\tau A_n$  consists entirely of odd permutations, and conversely, if  $\sigma$  is an odd permutation, then  $\tau^{-1}\sigma$  is even, so  $\sigma \in \tau A_n$ . This shows that  $|A_n| = |S_n|/2$ .

We will encounter the alternating group in the future, but for now, we only need to recall the definition of the symmetric group  $S_n$  to prove Cayley's Theorem.

**Theorem 1.25. (Cayley's Theorem.)** *Every group is isomorphic to a group of permutations.*

*Proof.* Let  $S_G$  be the group of permutations of  $G$ . We will prove that every group is isomorphic to a subgroup of  $S_G$ . The idea is that each element  $g \in G$  corresponds to a permutation of  $G$ , namely we need to define a map from  $G$  to  $S_G$ :

$$\lambda : G \rightarrow S_G, g \mapsto \lambda(g) = \lambda_g$$

and since  $\lambda_g$  is a bijection on  $G$ , we need to define what  $\lambda_g$  does:

$$\lambda_g : G \rightarrow G, \lambda_g(x) = gx.$$

For justifying that  $\lambda_g$  is indeed a bijection, it is enough to see that  $g^{-1}$  exists since  $G$  is a group (try to write down the definition of injection and surjection).

We are left to check that  $\lambda$  is an injective group homomorphism. Injectivity again comes from  $G$  being a group, for if  $\lambda_g(x) = \lambda_h(x)$  for all  $x \in G$ , then it has to be true that  $gx = hx$  when  $x = 1$ .

Now

$$(\lambda(a) \circ \lambda(b))(x) = (\lambda_a \circ \lambda_b)(x) = a(bx) = \lambda_{ab}(x) = \lambda(ab)(x)$$

for all  $x$ , so that  $\lambda(a) \circ \lambda(b) = \lambda(ab)$  which concludes the proof.  $\square$

**Examples 1.26.** 1. Consider the group  $\{0, 1\}$  of integers modulo 2. The group element 0 corresponds to the identity permutation, while the group element 1 corresponds to the permutation (12).

2. Let us consider the group  $\{0, 1, 2\}$  of integers modulo 3 to get a less simple example. Again 0 corresponds to the identity permutation, 1 corresponds to the permutation (123), and 2 to the permutation (132). To see that it makes sense, you may want to check that the arithmetic works similarly on both sides. For example, we can say that  $1 + 1 = 2$  on the one hand, now on the other hand, we have  $(123)(123) = (132)$ .

3. One can check that the dihedral group  $D_3$  of order 6 is isomorphic to  $S_3$  (this can be done for example by working out the multiplication table for each group).

The key point in the proof of Cayley's Theorem is the way the function  $\lambda_g$  is defined. We see that for  $x \in G$ ,  $g$  "acts" (via  $\lambda_g$ ) on  $x$  by multiplication.

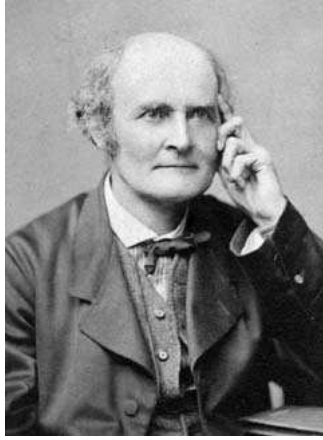


Figure 1.2: Arthur Cayley (1821-1895): he was the first to define the concept of a group in the modern way. Before him, groups referred to permutation groups.

**Definition 1.22.** The group  $G$  **acts** on the set  $X$  if for all  $g \in G$ , there is a map

$$G \times X \rightarrow X, (g, x) \mapsto g \cdot x$$

such that

1.  $h \cdot (g \cdot x) = (hg) \cdot x$  for all  $g, h \in G$ , for all  $x \in X$ .
2.  $1 \cdot x = x$  for all  $x \in X$ .

The first condition says that we have two laws, the group law between elements of the group, and the action of the group on the set, which are compatible.

**Examples 1.27.** Let us consider two examples where a group  $G$  acts on itself.

1. Every group acts on itself by left multiplication. This is called the regular action.
2. Every group acts on itself by conjugation. Let us write this action as

$$g \cdot x = gxg^{-1}.$$

Let us check the action is actually well defined. First, we have that

$$h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = hgxg^{-1}h^{-1} = (hg)xg^{-1}h^{-1} = (hg) \cdot x.$$

As for the identity, we get

$$1 \cdot x = 1x1^{-1} = x.$$

Similarly to the notion of kernel for a homomorphism, we can define the kernel of an action.

**Definition 1.23.** The **kernel** of an action  $G \times X \rightarrow X$ ,  $(g, x) \mapsto g \cdot x$  is given by

$$\text{Ker} = \{g \in G, g \cdot x = x \text{ for all } x\}.$$

This is the set of elements of  $G$  that fix everything in  $X$ . When the group  $G$  acts on itself, that is  $X = G$  and the action is the conjugation, we have

$$\text{Ker} = \{g \in G, gxg^{-1} = x \text{ for all } x\} = \{g \in G, gx = xg \text{ for all } x\}.$$

This is called the **center** of  $G$ , denoted by  $Z(G)$ .

**Definition 1.24.** Suppose that a group  $G$  acts on a set  $X$ . The **orbit**  $B(x)$  of  $x$  under the action of  $G$  is defined by

$$B(x) = \{g \cdot x, g \in G\}.$$

This means that we fix an element  $x \in X$ , and then we let  $g$  act on  $x$  when  $g$  runs through all the elements of  $G$ . By the definition of an action,  $g \cdot x$  belongs to  $X$ , so the orbit gives a subset of  $X$ .

It is important to notice that orbits partition  $X$ . Clearly, one has that  $X = \cup_{x \in X} B(x)$ . But now, assume that one element  $x$  of  $X$  belongs to two orbits  $B(y)$  and  $B(z)$ , then it means that  $x = g \cdot y = g' \cdot z$ , which in turn implies, due to the fact that  $G$  is a group, that

$$y = g^{-1}g' \cdot z, z = (g')^{-1}g \cdot y.$$

In words, that means that  $y$  belongs to the orbit of  $z$ , and vice-versa,  $z$  belongs to the orbit of  $y$ , and thus  $B(y) = B(z)$ . We can then pick a set of representatives for each orbit, and write that

$$X = \sqcup B(x),$$

where the disjoint union is taken over a set of representatives.

**Definition 1.25.** Suppose that a group  $G$  acts on a set  $X$ . We say that the action is **transitive**, or that  $G$  **acts transitively** on  $X$  if there is only one orbit, namely, for all  $x, y \in X$ , there exists  $g \in G$  such that  $g \cdot x = y$ .

**Definition 1.26.** The **stabilizer** of an element  $x \in X$  under the action of  $G$  is defined by

$$\text{Stab}(x) = \{g \in G, g \cdot x = x\}.$$

Given  $x$ , the stabilizer  $\text{Stab}(x)$  is the set of elements of  $G$  that leave  $x$  fixed. One may check that this is a subgroup of  $G$ . We have to check that if  $g, h \in \text{Stab}(x)$ , then  $gh^{-1} \in \text{Stab}(x)$ . Now

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x)$$



by definition of action. Since  $h \in \text{Stab}(x)$ , we have  $h \cdot x = x$  or equivalently  $x = h^{-1} \cdot x$ , so that

$$g \cdot (h^{-1} \cdot x) = g \cdot x = x,$$

which shows that  $\text{Stab}(x)$  is a subgroup of  $G$ .

**Examples 1.28.** 1. The regular action (see the previous example) is transitive, and for all  $x \in X = G$ , we have  $\text{Stab}(x) = \{1\}$ , since  $x$  is invertible and we can multiply  $g \cdot x = x$  by  $x^{-1}$ .

2. Let us consider the action by conjugation, which is again an action of  $G$  on itself ( $X = G$ ):  $g \cdot x = gxg^{-1}$ . The action has no reason to be transitive in general, and for all  $x \in X = G$ , the orbit of  $x$  is given by

$$B(x) = \{gxg^{-1}, g \in G\}.$$

This is called the **conjugacy class** of  $x$ . Let us now consider the stabilizer of an element  $x \in X$ :

$$\text{Stab}(x) = \{g \in G, gxg^{-1} = x\} = \{g \in G, gx = xg\},$$

which is the **centralizer** of  $x$ , that we denote by  $C_G(x)$ .

Note that we can define similarly the centralizer  $C_G(S)$  where  $S$  is an arbitrary subset of  $G$  as the set of elements of  $G$  which commute with everything in  $S$ . The two extreme cases are: if  $S = \{x\}$ , we get the centralizer of one element, if  $S = G$ , we get the center  $Z(G)$ .

**Theorem 1.26. (The Orbit-Stabilizer Theorem).** *Suppose that a group  $G$  acts on a set  $X$ . Let  $B(x)$  be the orbit of  $x \in X$ , and let  $\text{Stab}(x)$  be the stabilizer of  $x$ . Then the size of the orbit is the index of the stabilizer, that is*

$$|B(x)| = [G : \text{Stab}(x)].$$

If  $G$  is finite, then

$$|B(x)| = |G|/|\text{Stab}(x)|.$$

In particular, the size of an orbit divides the order of the group.

*Proof.* Recall first that  $[G : \text{Stab}(x)]$  counts the number of left cosets of  $\text{Stab}(x)$  in  $G$ , that is the cardinality of

$$G/\text{Stab}(x) = \{g\text{Stab}(x), g \in G\}.$$

Note that cosets of  $\text{Stab}(x)$  are well-defined since we saw that  $\text{Stab}(x)$  is a subgroup of  $G$ . The idea of the proof is to build a function between the sets  $B(x)$  and  $G/\text{Stab}(x)$  which is a bijection. That the cardinalities are the same will then follow.

Take  $y \in B(x)$ , that is  $y = g \cdot x$  for some  $g \in G$ . We define a map

$$f : B(x) \rightarrow G/\text{Stab}(x), y = g \cdot x \mapsto g\text{Stab}(x).$$

Before checking that this map is a bijection, we need to check that it is well defined. Indeed, for a given  $y$ , there is no reason for the choice of  $g$  to be unique (there is in general no bijection between  $G$  and  $B(x)$ ). Suppose that

$$y = g_1 \cdot x = g_2 \cdot x$$

then

$$g_2^{-1}g_1 \cdot x = x \iff g_1\text{Stab}(x) = g_2\text{Stab}(x).$$

The equivalence is the characterization of having two equal cosets. This is exactly what we wanted: the image by  $f$  does not depend on the choice of  $g$ , and if we choose two different  $g$ 's, their image falls into the same coset.

The surjectivity of  $f$  is immediate.

We conclude the proof by showing the injectivity. Let us assume that  $f(y_1) = f(y_2)$  for  $y_1 = g_1 \cdot x \in B(x)$ ,  $y_2 = g_2 \cdot x \in B(x)$ . Thus

$$g_1\text{Stab}(x) = g_2\text{Stab}(x) \iff g_2^{-1}g_1 \in \text{Stab}(x) \iff g_2^{-1}g_1 \cdot x = x \iff g_1 \cdot x = g_2 \cdot x.$$

□

Let  $G$  be a finite group. We consider again as action the conjugation ( $X = G$ ), given by:  $g \cdot x = gxg^{-1}$ . Recall that orbits under this action are given by

$$B(x) = \{gxg^{-1}, g \in G\}.$$

Let us notice that  $x$  always is in its orbit  $B(x)$  (take  $g = 1$ ). Thus if we have an orbit of size 1, this means that

$$gxg^{-1} = x \iff gx = xg$$

and we get an element  $x$  in the center  $Z(G)$  of  $G$ . In words, elements that have an orbit of size 1 under the action by conjugation are elements of the center.

Recall that the orbits  $B(x)$  partition  $X$ :

$$X = \sqcup B(x)$$

where the disjoint union is over a set of representatives. We get

$$\begin{aligned} |G| &= \sum |B(x)| \\ &= |Z(G)| + \sum |B(x)| \\ &= |Z(G)| + \sum [G : \text{Stab}(x)], \end{aligned}$$

where the second equality comes by splitting the sum between orbits with 1 element and orbits with at least 2 elements, while the third follows from the Orbit-Stabilizer Theorem. By remembering that  $\text{Stab}(x) = C_G(x)$  when the action is the conjugation, we can alternatively write

$$|G| = |Z(G)| + \sum [G : C_G(x)].$$

This formula is called the [class equation](#).

**Example 1.29.** Consider the dihedral  $D_4$  of order 8, given by

$$D_4 = \{1, s, r, r^2, r^3, rs, r^2s, r^3s\},$$

with  $s^2 = 1$ ,  $r^4 = 1$  and  $sr = r^{-1}s$ . We have that the center  $Z(D_4)$  of  $D_4$  is  $\{1, r^2\}$  (just check that  $r^2s = sr^2$ ). There are three conjugacy classes given by

$$\{r, r^3\}, \{rs, r^3s\}, \{s, r^2s\}.$$

Thus

$$|D_4| = 8 = |Z(D_4)| + |B(r)| + |B(rs)| + |B(s)|.$$

The following result has many names: Burnside's lemma, Burnside's counting theorem, the Cauchy-Frobenius lemma or the orbit-counting theorem. This result is not due to Burnside himself, who only quoted it. It is attributed to Frobenius.

**Theorem 1.27. (Orbit-Counting Theorem).** *Let the finite group  $G$  act on the finite set  $X$ , and denote by  $X^g$  the set of elements of  $X$  that are fixed by  $g$ , that is  $X^g = \{x \in X, g \cdot x = x\}$ . Then*

$$\text{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

that is the number of orbits is the average number of points left fixed by elements of  $G$ .

*Proof.* We have

$$\begin{aligned} \sum_{g \in G} |X^g| &= |\{(g, x) \in G \times X, g \cdot x = x\}| \\ &= \sum_{x \in X} |\text{Stab}(x)| \\ &= \sum_{x \in X} |G|/|B(x)| \end{aligned}$$

by the Orbit-Stabilizer Theorem. We go on:

$$\begin{aligned} \sum_{x \in X} |G|/|B(x)| &= |G| \sum_{x \in X} 1/|B(x)| \\ &= |G| \sum_{B \in \text{set of orbits}} \sum_{x \in B} \frac{1}{|B|} \\ &= |G| \sum_{B \in \text{set of orbits}} 1 \end{aligned}$$

which concludes the proof. Note that the second equality comes from the fact that we can write  $X$  as a disjoint union of orbits.  $\square$

## 1.8 The Sylow theorems

We look at orders of groups again, but this time paying attention to the occurrence of prime factors. More precisely, we will fix a given prime  $p$ , look at the partial factorization of the group order  $n$  as  $n = p^r m$  where  $p$  does not divide  $m$ , and study the existence of subgroups of order  $p$  or a power of  $p$ . In a sense, this is trying to establish some kind of converse for Lagrange's Theorem. Recall that Lagrange's Theorem tells that the order of a subgroup divides the order of the group. Here we conversely pick a divisor of the order of the group, and we try to find a subgroup with order the chosen divisor.

**Definition 1.27.** Let  $p$  be a prime. The group  $G$  is said to be a  $p$ -group if the order of each element of  $G$  is a power of  $p$ .

**Examples 1.30.** We have already encountered several 2-groups.

1. We have seen in Example 1.15 that the cyclic group  $C_4$  has elements of order 1, 2 and 4, while the direct product  $C_2 \times C_2$  has elements of order 1 and 2.
2. The dihedral group  $D_4$  is also a 2-group.

**Definition 1.28.** If  $|G| = p^r m$ , where  $p$  does not divide  $m$ , then a subgroup  $P$  of order  $p^r$  is called a **Sylow  $p$ -subgroup** of  $G$ . Thus  $P$  is a  $p$ -subgroup of  $G$  of maximum possible size.

The first thing we need to check is that such a subgroup of order  $p^r$  indeed exists, which is not obvious. This will be the content of the first Sylow theorem. Once we have proven the existence of a subgroup of order  $p^r$ , it has to be a  $p$ -group, since by Lagrange's Theorem the order of each element must divide  $p^r$ .

We need a preliminary lemma.

**Lemma 1.28.** If  $n = p^r m$  where  $p$  is prime, then  $\binom{n}{p^r} \equiv m \pmod{p}$ . Thus if  $p$  does not divide  $m$ , then  $p$  does not divide  $\binom{n}{p^r}$ .

*Proof.* We have to prove that

$$\binom{n}{p^r} \equiv m \pmod{p},$$

after which we have that if  $p$  does not divide  $m$ , the  $m \not\equiv 0 \pmod{p}$  implying that  $\binom{n}{p^r} \not\equiv 0 \pmod{p}$  and thus  $p$  does not divide  $\binom{n}{p^r}$ .

Let us use the binomial expansion of the following polynomial

$$(x+1)^{p^r} = \sum_{k=0}^{p^r} \binom{p^r}{k} x^{p^r-k} 1^k \equiv x^{p^r} + 1 \pmod{p}$$

where we noted that all binomial coefficients but the first and the last are divisible by  $p$ . Thus

$$(x+1)^{p^r m} \equiv (x^{p^r} + 1)^m \pmod{p}$$



Figure 1.3: Ludwig Sylow (1832-1918)

which we can expand again into

$$\sum_{k=0}^{p^r m} \binom{p^r m}{k} x^{p^r m - k} \equiv \sum_{k=0}^m \binom{m}{k} (x^{p^r})^{m-k} \pmod{p}.$$

We now look at the coefficient of  $x^{p^r}$  on both sides:

- on the left, take  $k = p^r(m - 1)$ , to get  $\binom{p^r m}{p^r}$ ,
- on the right, take  $k = m - 1$ , to get  $\binom{m}{m-1} = m$ .

The result follows by identifying the coefficients of  $x^{p^r}$ . □

We are ready to prove the first Sylow Theorem.

**Theorem 1.29. (1st Sylow Theorem).** *Let  $G$  be a finite group of order  $p^r m$ ,  $p$  a prime such that  $p$  does not divide  $m$ , and  $r$  some positive integer. Then  $G$  has at least one Sylow  $p$ -subgroup.*

*Proof.* The idea of the proof is to actually exhibit a subgroup of  $G$  of order  $p^r$ . For that, we need to define a clever action of  $G$  on a carefully chosen set  $X$ . Take the set

$$X = \{\text{subsets of } G \text{ of size } p^r\}$$

and for action that  $G$  acts on  $X$  by left multiplication. This is clearly a well-defined action. We have that

$$|X| = \binom{p^r m}{p^r}$$

which is not divisible by  $p$  (by the previous lemma). Recall that the action of  $G$  on  $X$  induces a partition of  $X$  into orbits:

$$X = \sqcup B(S)$$

where the disjoint union is taken over a set of representatives. Be careful that here  $S$  is an element of  $X$ , that is  $S$  is a subset of size  $p^r$ . We get

$$|X| = \sum |B(S)|$$

and since  $p$  does not divide  $|X|$ , it does not divide  $\sum |B(S)|$ , meaning that there is at least one  $S$  for which  $p$  does not divide  $|B(S)|$ . Let us pick this  $S$ , and denote by  $P$  its stabilizer.

The subgroup  $P$  which is thus by choice the stabilizer of the subset  $S \in X$  of size  $p^r$  whose orbit size is not divisible by  $p$  is our candidate: we will prove it has order  $p^r$ .

$|P| \geq p^r$ . Let us use the Orbit-Stabilizer Theorem, which tells us that

$$|B(S)| = |G|/|P| = p^r m/|P|.$$

By choice of the  $S$  we picked,  $p$  does not divide  $|B(S)|$ , that is  $p$  does not divide  $p^r m/|P|$  and  $|P|$  has to be a multiple of  $p^r$ , or equivalently  $p^r$  divides  $|P|$ .

$|P| \leq p^r$ . Let us define the map  $\lambda_x$ ,  $x \in S$ , by

$$\lambda_x : P \rightarrow S, g \mapsto \lambda_x(g) = gx.$$

In words, this map goes from  $P$ , which is a subgroup of  $G$ , to  $S$ , which is an element of  $X$ , that is a subset of  $G$  with cardinality  $p^r$ . Note that this map is well-defined since  $gx \in S$  for any  $x \in S$  and any  $g \in P$  by definition of  $P$  being the stabilizer of  $S$ . It is also clearly injective ( $gx = hx$  implies  $g = h$  since  $x$  is an element of the group  $G$  and thus is invertible). If we have an injection from  $P$  to  $S$ , that means  $|P| \leq |S| = p^r$ .

□

**Example 1.31.** Consider the general group  $G = GL_n(\mathbb{F}_p)$  of  $n \times n$  invertible matrices with coefficients in  $\mathbb{F}_p$ , which denotes integers mod  $p$ ,  $p$  a prime. Let us compute a Sylow  $p$ -subgroup of  $G$ . For that, we first need to know the cardinality of  $G$ . This is a classical combinatorial computation: to build an invertible matrix with coefficients in  $\mathbb{F}_p$ , the first column can be anything but the whole zero vector, thus  $p^n - 1$  choices, the 2nd column can be anything but a multiple of the first column, thus  $p^n - p$  choices, the 3rd column can be anything but a linear combination of the first 2 columns, thus  $p^n - p^2$  choices, ..., thus the cardinality is

$$\begin{aligned} |G| = |GL_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}) \\ &= (p^n - 1)p(p^{n-1} - 1)p^2(p^{n-2} - 1) \cdots p^{n-1}(p - 1) \\ &= p^{n(n-1)/2} \prod_{k=1}^n (p^k - 1). \end{aligned}$$



Figure 1.4: Augustin Louis Cauchy (1789-1857)

Clearly  $p^{n(n-1)/2}$  is the highest power of  $p$  that divides  $G$ , we thus have to find a subgroup of  $G$  of that order. Consider the set  $U(p, n)$  of  $n \times n$  upper triangular matrices with every diagonal coefficient at 1 and elements of  $\mathbb{F}_p$  above. This is clearly a subgroup of  $G$ , since such matrices are invertible and form a group. Its cardinality is  $p^{n(n-1)/2}$  as wanted (there are  $n(n-1)/2$  coefficients above the diagonal, which can take any value mod  $p$ ).

**Corollary 1.30. (Cauchy Theorem).** *If the prime  $p$  divides the order of  $G$ , then  $G$  has an element of order  $p$ .*

*Proof.* Let  $P$  be a Sylow  $p$ -subgroup of  $G$  (which exists by the 1st Sylow Theorem), and pick  $x \neq 1$  in  $P$ . The order  $|x|$  of  $x$  is a power of  $p$  by definition of a  $p$ -group, say  $|x| = p^k$ . Then  $x^{p^{k-1}}$  has order  $p$ .  $\square$

The above corollary gives some converse to Lagrange's Theorem. The one below gives an alternative definition of a finite  $p$ -group. It is tempting to use it as a definition of  $p$ -group, however it cannot be used for infinite groups.

**Corollary 1.31.** *A finite group  $G$  is a  $p$ -group if and only if the order of  $G$  is a power of  $p$ .*

*Proof.* If the order of  $G$  is not a power of  $p$ , then it is divisible by some other prime  $q$ , in which case  $G$  contains an element of order  $q$  by Cauchy's Theorem, which contradicts the definition of  $p$ -group.

The converse is clear using Lagrange's Theorem.  $\square$

**Example 1.32.** Let us consider again the group  $H = U(p, n)$  of  $n \times n$  upper triangular matrices with every diagonal coefficient at 1 and elements of  $\mathbb{F}_p$  above computed in Example 1.31. We know that  $|H| = p^{n(n-1)/2}$ , thus it is a  $p$ -group. Now let us consider the union

$$G = \bigcup_{n \geq 1} U(p, n).$$

This forms an infinite  $p$ -group, since every element has order a power of  $p$ .

Now that we know that at least one Sylow  $p$ -subgroup exists, let us derive a result on the number  $n_p$  of Sylow  $p$ -subgroups in a group  $G$ .

We need again a preliminary lemma.

**Lemma 1.32.** *Let  $H$  and  $K$  be arbitrary finite subgroups of a group  $G$ . Then*

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

Note that if  $K$  is further assumed to be normal in  $G$ , then this result can be deduced from the second isomorphism Theorem.

*Proof.* Consider the map

$$f : H \times K \rightarrow HK, (h, k) \mapsto hk.$$

Since  $f$  is surjective,  $|HK| \leq |H \times K| < \infty$  since  $H$  and  $K$  are finite, and thus  $HK$  is finite. Let  $h_1k_1, \dots, h_dk_d$  be the distinct elements of  $HK$ . Then  $H \times K$  is the disjoint union of the  $f^{-1}(h_ik_i)$ ,  $i = 1, \dots, d$ . Now we can check that

$$f^{-1}(hk) = \{(hg, g^{-1}k), g \in H \cap K\}$$

and this set has cardinality

$$|f^{-1}(hk)| = |H \cap K|.$$

Thus

$$|H \times K| = d|H \cap K|$$

which concludes the proof.  $\square$

**Theorem 1.33. (2nd Sylow Theorem).** *Let  $G$  be a finite group of order  $p^r m$ ,  $p$  a prime such that  $p$  does not divide  $m$ , and  $r$  some positive integer. Denote by  $n_p$  the number of Sylow  $p$ -subgroups of  $G$ . Then*

$$n_p \equiv 1 \pmod{p}.$$

*Proof.* Consider the set

$$X = \{ \text{all Sylow } p\text{-subgroups of } G \}$$

whose cardinality  $|X|$  is denoted by  $n_p$ . By the 1st Sylow Theorem, this set is non-empty and there exists at least one Sylow  $p$ -subgroup  $P$  in  $X$ , whose order is  $p^r$ . We can thus let  $P$  act on  $X$  by conjugation, i.e.,  $g \cdot Q = gQg^{-1}$ ,  $g \in P$ ,  $Q \in X$ . Note that in the case where  $P$  is the only Sylow  $p$ -subgroup, then we can take  $Q = P$ .

By the Orbit-Stabilizer Theorem, we have that the orbit  $B(Q)$  of any Sylow  $p$ -subgroup  $Q$  in  $X$  has cardinality

$$|B(Q)| = |P|/|\text{Stab}(Q)| = p^r/|\text{Stab}(Q)|.$$



In particular, the size of an orbit of any Sylow  $p$ -subgroups divides  $p^r$ , meaning it has to be either 1 or a power of  $p$ .

Let us recall that the set  $X$  is partitioned by the orbits  $B(Q)$  under the action of  $P$ , so that the cardinality of  $X$  is:

$$|X| = \sum |B(Q)| = \sum |B(Q')| + \sum |B(Q'')|$$

where  $Q'$  and  $Q''$  denote subgroups whose orbit has respectively one element or at least two elements. Since  $p$  divides the second sum, we have

$$|X| \equiv \text{number of orbits of size 1} \pmod{p}.$$

To conclude the proof, we thus have to show that there is only one Sylow  $p$ -subgroup whose orbit has size 1, namely  $P$  itself (it is clear that  $P$  has an orbit of size 1, since conjugating  $P$  by itself will not give another subgroup).

Let us assume there is another Sylow  $p$ -subgroup  $Q$  whose orbit has only one element, namely (recall that one element is always in its orbit):

$$gQg^{-1} = Q, \quad g \in P,$$

which translates into

$$gQ = Qg \text{ for all } g \in P \iff PQ = QP.$$

This easily implies that  $PQ$  is a subgroup of  $G$ , and by the previous lemma

$$|PQ| = \frac{p^r p^r}{|P \cap Q|}$$

implying that  $|PQ|$  is a power of  $p$ , say  $p^c$  for some  $c$  which cannot be bigger than  $r$ , since  $|G| = p^r m$ . Thus

$$p^r = |P| \leq |PQ| \leq p^r$$

so that  $|PQ| = p^r$  and thus  $|P| = |PQ|$ , saying that  $Q$  is included in  $P$ . But both  $Q$  and  $P$  have same cardinality of  $p^r$ , so  $Q = P$ .  $\square$

The third of the Sylow Theorems tells us that all Sylow  $p$ -subgroups are conjugate.

**Theorem 1.34. (3rd Sylow Theorem).** *Let  $G$  be a finite group of order  $p^r m$ ,  $p$  a prime such that  $p$  does not divide  $m$ , and  $r$  some positive integer. Then all Sylow  $p$ -subgroups are conjugate.*

*Proof.* Let  $P$  be a Sylow  $p$ -subgroup of  $G$  and let  $R$  be a  $p$ -group of  $G$ . We will prove that  $R$  (being a  $p$ -group in general) is contained in a conjugate of  $P$ .

Let  $R$  act by multiplication on the set  $Y$  of left cosets of  $P$ :

$$Y = \{gP, g \in G\}.$$

It is a well-defined action (it is multiplication in the group  $G$ ).

We want to prove that there is an orbit of size 1 under this action. By Lagrange's Theorem, we know that

$$|Y| = |G|/|P| = \frac{p^r m}{p^r} = m$$

and thus  $p$  does not divide  $|Y|$  by assumption on  $m$ . By writing that we have a partition of  $Y$  by its orbits, we get

$$|Y| = \sum |B(y)|$$

and there exists one orbit  $B(y)$  whose size is not divisible by  $p$ . By the Orbit-Stabilizer Theorem, we have that the size of every orbit divides  $|R|$ , which has order a power of  $p$  (by a corollary of the 1st Sylow Theorem), so every orbit size must divide  $p$ , which gives as only possibility that there is an orbit of size 1.

Let  $gP \in Y$  be the element whose orbit size is 1. We have

$$h \cdot gP = gP$$

for  $h \in R$ , since  $gP$  belongs to its orbit. Thus

$$g^{-1}hg \in P \iff h \in gPg^{-1}$$

for all  $h$  in  $R$ . We have just proved that the  $p$ -group  $R$  is contained in a conjugate of  $P$ .

All we needed for the proof is that  $R$  is a  $p$ -group, so the same proof holds for the case of a Sylow  $p$ -subgroup, for which we get that  $R$  is contained in a conjugate of  $P$ , and both have same cardinality, which concludes the proof.

We will use the fact that the proof works for  $R$  a  $p$ -group in general for proving one corollary.  $\square$

**Corollary 1.35.** 1. Every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup.

2. The number  $n_p$  of Sylow  $p$ -subgroups divides  $m$ .

*Proof.* 1. Now we know that if  $P$  is a Sylow  $p$ -subgroup, then so is  $gPg^{-1}$ ,  $g \in G$ , by the above theorem. The proof of the theorem itself shows that any  $p$ -group is included in  $gPg^{-1}$  and we are done.

2. Let the group  $G$  act by conjugation on the set of its subgroups. In particular,  $G$  acts on the Sylow  $p$ -subgroup  $P$ , and the orbit of  $P$  has size the number of Sylow  $p$ -subgroups in  $G$ , denoted by  $n_p$ . By the Orbit-Stabilizer Theorem,  $n_p$  divides  $|G| = p^r m$ . But  $p$  cannot be a prime factor of  $n_p$  since  $n_p \equiv 1 \pmod{p}$ , from which it follows that  $n_p$  must divide  $m$ .  $\square$

## 1.9 Simple groups

We will now see a few applications of the Sylow Theorems, in particular to determine the structure of so-called simple groups.

**Definition 1.29.** A group  $G$  is **simple** if  $G \neq \{1\}$  and the only normal subgroups of  $G$  are  $G$  itself and  $\{1\}$ .

Finite simple groups are important because in a sense they are building blocks of all finite groups, similarly to the way prime numbers are building blocks of the integers. This will be made clearer in the coming section by the Jordan-Hölder Theorem. Infinite simple groups exist and can be found for example among Lie groups, but we will concentrate here on finite groups.

The case of simple abelian groups is easy to understand. Suppose that  $G$  is a simple abelian group. Note that  $G$  cannot be  $\{1\}$ . Now  $G$  being abelian, all its subgroups are normal. On the other hand,  $G$  being simple, its only normal subgroups are  $\{1\}$  and itself, leaving as only solution that  $G$  has only two subgroups, namely  $\{1\}$  and  $G$ . Thus  $G$  has to be a cyclic group of prime order.

We now start looking at non-abelian simple groups. We start with some preliminary results.

**Proposition 1.36.** *If  $P$  is a non-trivial finite  $p$ -group, then  $P$  has a non-trivial center.*

*Proof.* Let  $P$  act on itself by conjugation. The orbits of this action are the conjugacy classes of  $P$ , and we have that  $x$  belongs to an orbit of size 1 if and only if  $x$  belongs to the center  $Z(P)$ .

By the Orbit-Stabilizer, the size of any orbit must divide  $|P|$ , which is a power of  $p$  by a corollary of the 1st Sylow Theorem.

If it were true that the center is trivial, that is  $Z(P) = \{1\}$ , then that means there is only one orbit of size 1, and thus all the other orbits must have size that divides  $p$ , namely they are congruent to 0 mod  $p$ . Thus

$$|P| = |Z(P)| + \sum |B| \equiv 1 \pmod{p},$$

where the sum is over orbits of size at least 2. This is clearly a contradiction, which concludes the proof.  $\square$

**Lemma 1.37.** *The group  $P$  is a normal Sylow  $p$ -subgroup of a group  $G$  if and only if  $P$  is the unique Sylow  $p$ -subgroup of  $G$ .*

*Proof.* We know from the 3rd Sylow Theorem that the Sylow  $p$ -subgroups form a single conjugacy class. Then  $P$  is the unique Sylow  $p$ -subgroup means that  $P$  is the only element in the conjugacy class, and thus it satisfies

$$gPg^{-1} = P,$$

for every  $g \in G$ , which exactly means that  $P$  is a normal subgroup of  $G$ . Conversely, if  $P$  is normal, then  $gPg^{-1} = P$  for all  $g \in G$ , which means that

when we conjugate  $P$  by any element of  $G$ ,  $P$  is the only Sylow  $p$ -subgroup in its conjugacy class. Since all the Sylow  $p$ -subgroups belong to the same conjugacy class,  $P$  is the only Sylow  $p$ -subgroup.  $\square$

Thanks to the two above results, we can now prove that a non-abelian simple group must have more than one Sylow  $p$ -subgroup.

**Proposition 1.38.** *Let  $G$  be a finite group which is non-abelian and simple. If the prime  $p$  divides  $|G|$ , then the number  $n_p$  of Sylow  $p$ -subgroups is strictly bigger than 1.*

*Proof.* Let us look at the prime factors appearing in the order of  $G$ .

- If  $p$  is the only prime factor of  $|G|$ , then  $|G|$  must be a power of  $p$ , that is  $G$  is a non-trivial  $p$ -group (it is non-trivial by definition of simple and a  $p$ -group by a corollary of the 1st Sylow Theorem). Now the above proposition tells us that its center  $Z(G)$  is non-trivial as well. Since  $Z(G)$  is a normal subgroup of  $G$  and  $G$  is simple, it must be that  $G = Z(G)$ , which contradicts the assumption that  $G$  is non-abelian.
- We then know that  $|G|$  is divisible by at least two distinct primes. So if  $P$  is a Sylow  $p$ -subgroup, then

$$\{1\} < P < G,$$

where the second inclusion is strict since the order of  $G$  is divisible by two primes.

If there were only one Sylow  $p$ -subgroup, namely  $n_p = 1$ , then this Sylow  $p$ -subgroup would be normal by the above lemma, which contradicts the simplicity of  $G$ .

$\square$

Let us see if we can be more precise by refining the assumptions on the order of the group  $G$  we consider. The group  $G$  can be either abelian or non-abelian, though the results on simplicity are more interesting for non-abelian groups.

**Proposition 1.39.** *Let  $G$  be a group of order  $pq$ , where  $p$  and  $q$  are distinct primes.*

1. *If  $q \not\equiv 1 \pmod{p}$ , then  $G$  has a normal Sylow  $p$ -subgroup.*
2. *If both  $q \not\equiv 1 \pmod{p}$  and  $p \not\equiv 1 \pmod{q}$ , then  $G$  is cyclic.*
3.  *$G$  is not simple.*

*Proof.* 1. By Lemma 1.37, saying that  $G$  has a normal Sylow  $p$ -subgroup is the same as saying that there is a unique Sylow  $p$ -subgroup. This is now indeed the case, since the number  $n_p$  of Sylow  $p$ -subgroups has to satisfy both  $n_p \equiv 1 \pmod{p}$  and  $n_p \mid q$  by the Sylow Theorems. Since  $q$  is prime,  $n_p$  is either 1 or  $q$ . It cannot be that  $n_p = q$ , since it would imply that  $q \equiv 1 \pmod{p}$  which contradicts the assumption.

2. By the previous point, the group  $G$  has a normal Sylow  $p$ -subgroup  $P$  and a normal Sylow  $q$ -subgroup  $Q$ , both of them cyclic (since they are of prime order). Let us write them respectively  $P = \langle x \rangle$  and  $Q = \langle y \rangle$ . Since both  $P$  and  $Q$  are normal, with  $P \cap Q = \{1\}$ , we have that  $xy = yx$  (we have seen that before, but the argument goes like that: take the element  $xyx^{-1}y^{-1}$  and show that it belongs to  $P \cap Q$  by normality of  $P$  and  $Q$ ). Thanks to this commutativity property, we have that  $(xy)^n = x^n y^n$  and the order of  $xy$  is  $pq$ , showing that  $G$  is cyclic with generator  $xy$ .
3. Without loss of generality, we can assume that  $p > q$  so that  $p$  does not divide  $q - 1$  which can be rewritten as

$$q \not\equiv 1 \pmod{p}.$$

By the first point, we know that  $G$  has a normal Sylow  $p$ -group, and thus  $G$  cannot be simple. □

Here is another family of groups which are not simple. The proof contains an interesting combinatorial argument!

**Proposition 1.40.** *Let  $G$  be a group of order  $|G| = p^2q$  where  $p$  and  $q$  are two distinct primes. Then  $G$  contains either a normal Sylow  $p$ -subgroup or a normal Sylow  $q$ -subgroup. In particular,  $G$  is not simple.*

*Proof.* Recall that having a normal Sylow  $p$ -subgroup (resp.  $q$ -subgroup) is the same as saying there is a unique Sylow  $p$ -subgroup (resp.  $q$ -subgroup). Suppose that the claim is not true, that is both the number of Sylow  $p$ -subgroups  $n_p$  and the number of Sylow  $q$ -subgroups  $n_q$  are bigger than 1. Let us start this proof by counting the number of elements of order  $q$  in  $G$ .

If a Sylow  $q$ -subgroup has order  $q$ , it is cyclic and can be generated by any of its elements which is not 1. This gives  $q - 1$  elements of order  $q$  per Sylow  $q$ -subgroup of  $G$ . Conversely, if  $y$  has order  $q$ , then the cyclic group it generates is a Sylow  $q$ -subgroup, and any two distinct Sylow  $q$ -subgroups have trivial intersection. Thus

$$\text{number of elements of order } q = n_q(q - 1).$$

Now we know from the Sylow Theorems that  $n_q \mid p^2$ , thus  $n_q$  is either  $p$  or  $p^2$  ( $n_q = 1$  is ruled out by the fact that we do a proof by contradiction).

- $n_q = p^2$ : then the number of elements of order NOT  $q$  is

$$p^2q - p^2(q - 1) = p^2.$$

On the other hand, if  $P$  is a Sylow  $p$ -subgroup, then it also contains  $p^2$  elements, and all of them have order not  $q$ , so that we can conclude that  $P$  actually contains all elements of order not  $q$ , which implies that we have only one Sylow  $p$ -subgroup, yielding the wanted contradiction.

$ G $	abelian	non-abelian
$p$	$C_p$ simple	not possible
$p^r$	not simple	not simple since $ Z(G)  > 1$
$pq$	not simple	not simple
$p^2q$	not simple	not simple

Table 1.3:  $C_p$  refers to a cyclic group of prime order.

- $n_q = p$  : We know from Sylow Theorems that

$$n_q \equiv 1 \pmod{q} \Rightarrow p \equiv 1 \pmod{q} \Rightarrow p > q,$$

but also that

$$n_p \mid q$$

and since  $q$  is prime, that leaves  $n_p = 1$  or  $n_p = q$  and thus  $n_p = q$ . As before

$$n_p \equiv 1 \pmod{p} \Rightarrow q \equiv 1 \pmod{p} \Rightarrow q > p.$$

This concludes the proof.

□

We have thus shown that the situation is easy for simple abelian groups. For non-abelian groups, we have seen two cases ( $|G| = pq$  and  $|G| = p^2q$ ) where groups are not simple. To find a non-abelian group which is simple, one has to go to groups of order at least 60. Indeed, it has been proven that the smallest non-abelian simple group is the alternating group  $A_5$  of order 60, this is the group of even permutations of a finite set. This result is attributed to Galois (1831). It is not an easy task to determine the list of simple groups, and in fact, the classification of finite simple groups was only accomplished in 1982 (there has been some controversy as to whether the proof is correct, given its length - tens of thousands of pages - and complexity).

## 1.10 The Jordan-Hölder Theorem

We have mentioned when introducing simple groups in the previous section that they can be seen as building blocks for decomposing arbitrary groups. This will be made precise in this section.

**Definition 1.30.** Let  $G$  be a group, and let  $G_0, \dots, G_n$  be subgroups of  $G$  such that

1.  $G_n = \{1\}$  and  $G_0 = G$ ,
2.  $G_{i+1} \trianglelefteq G_i$ ,  $i = 0, \dots, n-1$ .

Then the series

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

is called a **subnormal series** for  $G$ .

Suppose that  $G_{i+1}$  is not a maximal normal subgroup of  $G_i$ , then we can refine the subnormal series by inserting a group  $H$  such that  $G_{i+1} \triangleleft H \triangleleft G_i$ , and we can repeat this process hoping it will terminate (it will if  $G$  is finite, it may not otherwise).

**Definition 1.31.** Let  $G$  be a group, and let  $G_0, \dots, G_n$  be subgroups of  $G$  such that

1.  $G_n = \{1\}$  and  $G_0 = G$ ,
2.  $G_{i+1} \triangleleft G_i$ ,  $i = 0, \dots, n-1$ , such that  $G_{i+1}$  is a maximal normal subgroup of  $G_i$ .

Then the series

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$$

is called a **composition series** for  $G$ . The factor groups  $G_i/G_{i+1}$  are called the **factors** of the composition series, whose length is  $n$ .

Another way of stating the condition  $G_{i+1}$  is a maximal normal subgroup of  $G_i$  is to say that  $G_i/G_{i+1}$  is simple,  $i = 0, \dots, n-1$ . To see that asks a little bit of work. This result is sometimes called the 4rth isomorphism theorem.

**Theorem 1.41. (Correspondence Theorem).** Let  $N$  be a normal subgroup of  $G$  and let  $H$  be a subgroup of  $G$  containing  $N$ . Then the map

$$\psi : \{\text{subgroups of } G \text{ containing } N\} \rightarrow \{\text{subgroups of } G/N\}, H \mapsto \psi(H) = H/N$$

is a bijection. Furthermore,  $H$  is a normal subgroup of  $G$  if and only if  $H/N$  is a normal subgroup of  $G/N$ .

*Proof.* We first prove that  $\psi$  is a bijection.

**Injectivity.** If  $H_1/N = H_2/N$ , then cosets in each subgroup are the same, that is for any  $h_1 \in H_1$ , we have  $h_1N = h_2N$  for some  $h_2 \in H_2$ , implying that  $h_2^{-1}h_1 \in N \subset H_2$  and thus  $h_1 \in H_2$ , showing that  $H_1 \subseteq H_2$ . By repeating the same argument but reverting the role of  $H_1$  and  $H_2$ , we get  $H_2 \subseteq H_1$  and thus  $H_1 = H_2$ .

**Surjectivity.** Let  $Q$  be a subgroup of  $G/N$  and let  $\pi : G \rightarrow G/N$  be the canonical projection. Then

$$\pi^{-1}(Q) = \{a \in G, aN \in Q\}.$$

This is a subgroup of  $G$  containing  $N$  and

$$\psi(\pi^{-1}(Q)) = \{aN, aN \in Q\} = Q.$$

We are left to prove that  $H \trianglelefteq G \iff H/N \trianglelefteq G/N$ . Assume thus that  $H \trianglelefteq G$ . For any  $a \in G$ , we have to show that

$$(aN)(H/N)(aN)^{-1} = H/N.$$

Now for any  $hN \in H/N$ , we have

$$(aN)(hN)(aN)^{-1} = (aha^{-1})N \in H/N$$

and we are done.

Conversely, suppose that  $H/N \trianglelefteq G/N$ . Consider the homomorphism

$$a \mapsto (aN)(H/N)$$

which is the composition of the canonical projection  $\pi$  of  $G$  onto  $G/N$ , and the canonical projection of  $G/N$  onto  $(G/N)/(H/N)$  (the latter makes sense since  $H/N \trianglelefteq G/N$ ). We now want to show that  $H$  is the kernel of this map, which will conclude the proof since the kernel of a group homomorphism is normal.

An element  $a$  is in the kernel if and only if  $(aN)(H/N) = H/N$ , that is if and only if  $aN \in H/N$ , or equivalently  $aN = hN$  for some  $h \in H$ . Since  $N$  is contained in  $H$ , this means  $aN$  is in  $H$  and thus so is  $a$ , which is what we wanted to prove.  $\square$

Let us now go back to the composition series of  $G$ . If  $G/N$  is simple, then by definition it has only trivial normal subgroups, namely  $N$  and  $G/N$ . Now using the Correspondence Theorem, the normal subgroups  $N$  and  $G/N$  exactly correspond to the normal subgroups  $N$  and  $G$  in  $G$ , which shows that  $N$  is the maximal normal subgroup of  $G$ .

The Jordan-Hölder Theorem will tell us that if  $G$  has a composition series, then the resulting composition length  $n$  and the simple composition factors  $G_i/G_{i+1}$  are unique up to isomorphism and rearrangement. This for example shows that if  $G_1$  and  $G_2$  are two groups with different composition factors, then they cannot be isomorphic.

**Lemma 1.42.** *Let  $G$  be a group with composition series*

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G.$$

*Then for any normal subgroup  $K$  of  $G$ , if we remove the duplicates from the series*

$$\{1\} = K \cap G_n \trianglelefteq K \cap G_{n-1} \trianglelefteq \cdots \trianglelefteq K \cap G_0 = K,$$

*the result is a composition series for  $K$  of length at most  $n$ .*

*Proof.* We need to show that  $K \cap G_{i+1} \triangleleft K \cap G_i$  and that the group  $(K \cap G_i)/(K \cap G_{i+1})$  is simple for all  $i$ .

Let  $x \in K \cap G_i$  and  $g \in K \cap G_{i+1}$ . Then  $xgx^{-1} \in K$  since by assumption  $K$  is a normal subgroup of  $G$ , and  $xgx^{-1} \in G_{i+1}$  since  $G_{i+1} \triangleleft G_i$ . Thus  $xgx^{-1} \in K \cap G_{i+1}$  which proves that  $K \cap G_{i+1} \triangleleft K \cap G_i$ .



We now look at the quotient group  $(K \cap G_i)/(K \cap G_{i+1})$ . Since  $G_i/G_{i+1}$  is simple,  $G_{i+1}$  is a maximal normal subgroup of  $G_i$ , and thus the only normal subgroups of  $G_i$  that contain  $G_{i+1}$  are  $G_i$  and  $G_{i+1}$ .

Recall that  $K \cap G_i$  is normal in  $G_i$  (it is the kernel of the canonical projection of  $G$  to  $G/K$  restricted to  $G_i$ ), so that we get

$$G_{i+1} \triangleleft (K \cap G_i)G_{i+1} \triangleleft G_i.$$

For the first normal inclusion, compute that for  $kg \in (K \cap G_i)G_{i+1}$  we have

$$kgG_{i+1}g^{-1}k^{-1} = kG_{i+1}k^{-1} \subseteq G_{i+1}$$

since  $k \in G_i$  and  $G_{i+1}$  is normal in  $G_i$ . For the second normal inclusion, we have for  $g \in G_i$  that

$$g(K \cap G_i)G_{i+1}g^{-1} = (K \cap G_i)gG_{i+1}g^{-1}$$

since  $K \cap G_i$  is normal in  $G_i$  and

$$(K \cap G_i)gG_{i+1}g^{-1} \subseteq (K \cap G_i)G_{i+1}$$

since  $G_{i+1} \triangleleft G_i$ .

Thus either  $G_{i+1} = (K \cap G_i)G_{i+1}$  or  $(K \cap G_i)G_{i+1} = G_i$ . Using the second isomorphism theorem (with  $G_{i+1} \triangleleft G_i$  and  $(K \cap G_i) \leq G_i$ ), we have

$$(K \cap G_i)G_{i+1}/G_{i+1} \simeq (K \cap G_i)/(K \cap G_i \cap G_{i+1}) = (K \cap G_i)/(K \cap G_{i+1}).$$

We can see that if  $G_{i+1} = (K \cap G_i)G_{i+1}$ , then  $K \cap G_i = K \cap G_{i+1}$  and we have a duplicate to remove. If  $(K \cap G_i)G_{i+1} = G_i$ , then

$$G_i/G_{i+1} \simeq (K \cap G_i)/(K \cap G_{i+1})$$

and thus  $(K \cap G_i)/(K \cap G_{i+1})$  is simple.  $\square$

**Theorem 1.43. (Jordan-Hölder Theorem).** *Let  $G$  be a group that has a composition series. Then any two composition series for  $G$  have the same length. Moreover, if*

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$$

and

$$\{1\} = H_n \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_0 = G$$

are two composition series for  $G$ , there exists a permutation  $\tau$  such that  $G_i/G_{i+1} \simeq H_{\tau(i)}/H_{\tau(i)+1}$ .

*Proof.* The proof will be on induction on the length of a composition series. Suppose that  $G$  is a group with a composition series of length 1. Then the subnormal series

$$G \triangleright \{1\}$$

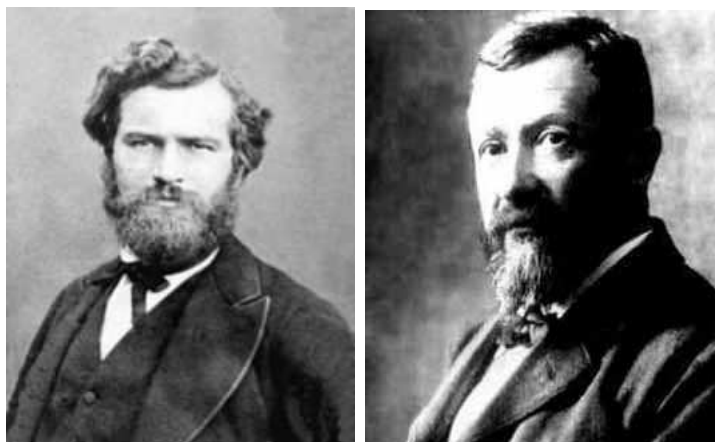


Figure 1.5: Camille Jordan (1838–1922) and Otto Hölder (1859–1937)

cannot be refined, so it must be a composition series. In particular  $G \simeq G/\{1\}$  is simple. This is also the only composition series for  $G$  and so all the assertions are true for length 1.

Suppose now that  $n > 1$  and that the claims are true for composition series of length up till  $n - 1$ . Let  $G$  be a group with composition series of length  $n$ , say

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$$

(so that  $G_i \neq G_{i+1}$  for each  $i$ ). Now let

$$\{1\} = H_m \triangleleft H_{m-1} \triangleleft \cdots \triangleleft H_0 = G$$

be a composition series for  $G$  (again  $H_i \neq H_{i+1}$  for each  $i$ ).

We first have to show that  $m = n$  after which we discuss the unicity of the decomposition.

**(Proof that  $m = n$ ).** The idea of the proof goes as follows: to use the induction hypothesis, we need to get a composition series of length smaller than  $n$ , that is, we need to identify the first composition factors, which we will use the above lemma. Concretely, we first exclude the case when  $G_1 = H_1$ , then compute a composition series of length  $n - 2$  for  $H_1 \cap G_1$ , which will indeed be the second composition factor. We then use the second composition series of  $G$  to get another composition series for  $H_1 \cap G_1$  whose length depends on  $m$ , that we can compare to the known one.

If  $G_1 = H_1$ , then by the induction hypothesis applied to  $G_1$ , we have  $n - 1 = m - 1$ , we have a suitable permutation  $\tau$  of the  $n - 1$  factors, and we are done.

Suppose then that  $H_1 \neq G_1$ . Since both  $G_1$  and  $H_1$  are maximal normal in  $G$ , we see that  $H_1 \triangleleft G_1 H_1 \triangleleft G$  with  $H_1 \neq G_1 H_1$  since we assumed  $H_1 \neq G_1$ . Thus  $G_1 H_1 = G$ , from which we conclude by the 2nd isomorphism theorem that

$$G_1 H_1 / H_1 \simeq G / H_1 \simeq G_1 / (H_1 \cap G_1).$$

Since  $G/H_1$  is simple, we get that  $G_1/(H_1 \cap G_1)$  is simple as well. Now by the above lemma, upon removing duplicates from the series

$$\{1\} = H_1 \cap G_n \trianglelefteq \cdots \trianglelefteq H_1 \cap G_0 = H_1,$$

we get a composition series for  $H_1$  of length at most  $n$  and thus upon removing duplicates

$$\{1\} = H_1 \cap G_n \trianglelefteq \cdots \trianglelefteq H_1 \cap G_1$$

is a composition series for  $H_1 \cap G_1$  of length at most  $n - 1$ . Since  $G_1/(H_1 \cap G_1)$  is simple, it follows that upon removing duplicates

$$\{1\} = H_1 \cap G_n \trianglelefteq \cdots \trianglelefteq H_1 \cap G_1 \triangleleft G_1$$

is a composition series for  $G_1$ . But then

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}$$

and

$$G_1 \triangleright H_1 \cap G_1 \triangleright H_1 \cap G_2 \triangleright \cdots \triangleright H_1 \cap G_n = \{1\}$$

are both composition series for  $G_1$ , with the first series of length  $n - 1$ . By induction hypothesis, both series have the same length. Since  $G_1 \neq H_1 \cap G_1$  (recall that we assumed  $H_1 \neq G_1$ ), any duplication must occur later in the series. Let

$$G_1 = K_1 \triangleright K_2 = H_1 \cap G_1 \triangleright K_3 \triangleright \cdots \triangleright K_n = \{1\}$$

denote the composition series for  $G_1$  of length  $n - 1$  that results from removing the duplicates. By hypothesis, there exists a permutation  $\alpha$  such that  $G_i/G_{i+1} \simeq K_{\alpha(i)}/K_{\alpha(i)+1}$  for each  $i = 1, \dots, n - 1$ . Set  $\alpha$  not to move the index 0, then

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}$$

and

$$G = K_0 \triangleright G_1 = K_1 \triangleright K_2 = H_1 \cap G_1 \triangleright K_3 \triangleright \cdots \triangleright K_n = \{1\}$$

are composition series of length  $n$  for  $G$  and  $\alpha$  is a permutation such that  $G_i/G_{i+1} \simeq K_{\alpha(i)}/K_{\alpha(i)+1}$  for each  $i = 0, \dots, n - 1$ . Moreover, we have found a composition series for  $H_1 \cap G_1$  of length  $n - 2$ .

Let us now repeat similar computations for the composition series

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = \{1\}$$

and the normal subgroup  $G_1$  of  $G$ . Again by the above lemma, upon removing the duplicates from the series

$$G_1 = H_0 \cap G_1 \triangleright H_1 \cap G_1 \triangleright \cdots \triangleright H_m \cap G_1 = \{1\}$$

we obtain a composition series for  $G_1$ , so that upon removing the duplicates

$$H_1 \cap G_1 \triangleright \cdots \triangleright H_m \cap G_1 = \{1\}$$

yields a composition series for  $H_1 \cap G_1$ . Now since  $H_1 \cap G_1$  has a composition series of length  $n - 2$ , namely

$$K_2 = H_1 \cap G_1 \triangleright \cdots \triangleright K_n = \{1\},$$

we apply the induction hypothesis to  $H_1 \cap G_1$  to conclude that all composition series of  $H_1 \cap G_1$  have length  $n - 2$ , and so in particular the preceding composition series

$$H_1 \cap G_1 \supseteq \cdots \supseteq H_m \cap G_1 = \{1\}$$

has length  $n - 2$ . We cannot conclude yet, since we do not know how many terms there are in function of  $m$  in the above composition series (we need to get rid of the duplicates).

Since we know from the 2nd isomorphism theorem that  $H_1/(H_1 \cap G_1) \simeq H_1 G_1/G_1 = G_0/G_1$ , which is a simple group, it follows that  $H_1/(H_1 \cap G_1)$  is simple. Thus upon the removal of the duplicates from

$$H_1 \triangleright H_1 \cap G_1 \supseteq \cdots \supseteq H_m \cap G_1 = \{1\}$$

the result is a composition series for  $H_1$  of length  $n - 1$  (we added the term  $H_1$  to the composition series for  $H_1 \cap G_1$  of length  $n - 2$ ). Also

$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_m = \{1\}$$

is another composition series for  $H_1$ . Since the first series has length  $n - 1$ , by our induction hypothesis, the second series must also have length  $n - 1$ . Since its length is  $m - 1$ , it follows that  $m = n$ .

**(Unicity of the composition factors).** Again by induction hypothesis on  $H_1$ , we have a permutation  $\beta$  of the  $n - 1$  composition factors (which can be extended to  $n$  factors by setting  $\beta(0) = 0$ .) Namely, let  $L_i$ ,  $i = 1, 2, \dots, n$  denote the distinct terms in the series

$$H_1 \triangleright H_1 \cap G_1 \triangleright H_2 \cap G_1 \triangleright \cdots \triangleright H_n \cap G_1 = \{1\}$$

so that  $L_1 = H_1$  and  $L_2 = H_1 \cap G_1$ . Then we have composition series

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{1\} \text{ and } G = L_0 \triangleright L_1 \triangleright \cdots \triangleright L_n = \{1\}$$

of length  $n$  for  $G$  and there exists a permutation  $\beta$  of  $\{0, 1, \dots, n - 1\}$  such that  $H_i/H_{i+1} \simeq L_{\beta(i)}/L_{\beta(i)+1}$  for each  $i = 0, 1, \dots, n - 1$ .

We are almost done but for the fact that we need an isomorphism between  $H_i/H_{i+1}$  and  $G_{\beta(i)}/G_{\beta(i)+1}$  instead of having  $H_i/H_{i+1} \simeq L_{\beta(i)}/L_{\beta(i)+1}$ . We recall that we already have a permutation  $\alpha$  such that  $G_i/G_{i+1} \simeq K_{\alpha(i)}/K_{\alpha(i)+1}$ . We are thus left to find one between  $L_i/L_{i+1}$  and  $K_i/K_{i+1}$ .

Finally, since  $K_2 = L_2 = H_1 \cap G_1$ , we have two composition series for  $G$ :

$$\begin{array}{ccccccc} G \triangleright & G_1 \triangleright & H_1 \cap G_1 \triangleright & K_3 \triangleright & \cdots & K_{n-1} \triangleright & K_n = \{1\} \\ G \triangleright & H_1 \triangleright & H_1 \cap G_1 \triangleright & L_3 \triangleright & \cdots & L_{n-1} \triangleright & L_n = \{1\}. \end{array}$$

We may apply the induction hypothesis to  $H_1 \cap G_1$  to obtain the existence of a permutation  $\gamma$  of  $\{2, 3, \dots, n-1\}$  such that for each  $i$  in this set we have  $K_i/K_{i+1} \simeq L_{\gamma(i)}/L_{\gamma(i)+1}$ . We have already seen that  $G/G_1 \simeq H_1/(H_1 \cap G_1)$  and  $G/H_1 \simeq G_1/(H_1 \cap G_1)$ , so we may extend  $\gamma$  to a permutation of  $\{0, 1, \dots, n-1\}$  by setting  $\gamma(0) = 1$  and  $\gamma(1) = 0$ . Then since

$$K_0 = G = L_0, \quad K_1 = G_1, \quad L_1 = H_1, \quad K_2 = L_2 = H_1 \cap G_1,$$

we have

$$K_i/K_{i+1} \simeq L_{\gamma(i)}/L_{\gamma(i)+1}, \quad i = 0, \dots, n-1.$$

In summary, we have  $m = n$ , and for  $\tau = \beta^{-1}\gamma\alpha$ , we have

$$G_i/G_{i+1} \simeq H_{\tau(i)}/H_{\tau(i)+1}, \quad i = 0, \dots, n-1.$$

This concludes the proof.  $\square$

**Example 1.33.** The cyclic group  $C_{12}$  has three composition series

$$C_1 \triangleleft C_2 \triangleleft C_6 \triangleleft C_{12}, \quad C_1 \triangleleft C_2 \triangleleft C_4 \triangleleft C_{12}, \quad C_1 \triangleleft C_3 \triangleleft C_6 \triangleleft C_{12}$$

and all of them have the same length. Furthermore, the factor groups appearing are

$$\{C_2, C_3, C_2\}, \{C_2, C_2, C_3\}, \{C_3, C_2, C_2\}$$

which are indeed the same up to permutation.

**Corollary 1.44. (Fundamental Theorem of arithmetic).** *Let  $n > 1$  be a positive integer. Then there exist unique primes  $p_1 < p_2 < \dots < p_k$  and unique positive integers  $r_1, \dots, r_k$  such that  $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ .*

*Proof.* Let  $G = \langle g \rangle$  be a cyclic group of order  $n$ . Then every subgroup of  $G$  is normal, and there is a unique subgroup of size  $d$  for each positive divisor  $d$  of  $n$ . Let  $d$  be the largest proper divisor of  $n$ , and let  $G_1$  be the unique subgroup of  $G$  of size  $d$ . Then  $G/G_1$  is simple and cyclic, hence of prime order. We may repeat this construction on the cyclic subgroup  $G_1$ , so by induction, we obtain a composition series

$$G = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_m = \{1\}$$

for  $G$  with  $G_i/G_{i+1}$  of prime order  $p_i$  for each  $i$ . Thus

$$\begin{aligned} n &= |G| \\ &= |G/G_1||G_1| \\ &= |G/G_1||G_1/G_2| \cdots |G_{m-1}/G_m||G_m| \\ &= p_1 p_2 \cdots p_{m-1}. \end{aligned}$$

The uniqueness of the prime decomposition of  $n$  follows from the Jordan-Hölder Theorem applied to  $G$ .  $\square$

## 1.11 Solvable and nilpotent groups

Let us start by introducing a notion stronger than normality.

**Definition 1.32.** A subgroup  $H$  of the group  $G$  is called **characteristic** in  $G$  if for each automorphism  $f$  of  $G$ , we have

$$f(H) = H.$$

We may write  $H \text{ char } G$ .

This is stronger than normal since normality corresponds to choose for  $f$  the conjugation by an element of  $G$ .

Note that  $f$  restricted to  $H$  a characteristic subgroup (denoted by  $f|_H$ ) is an automorphism of  $H$  (it is an endomorphism by definition of  $H$  being characteristic).

Here are a few immediate properties of characteristic subgroups.

**Lemma 1.45.** *Let  $G$  be a group, and let  $H, K$  be subgroups of  $G$ .*

1. *If  $H$  is characteristic in  $K$  and  $K$  is characteristic in  $G$ , then  $H$  is characteristic in  $G$  (being characteristic is transitive).*
2. *If  $H$  is characteristic in  $K$ , and  $K$  is normal in  $G$ , then  $H$  is normal in  $G$ .*

*Proof.* 1. Note that by assumption  $H \leq K \leq G$ . Let  $\phi$  be an automorphism of  $G$ . Since  $K$  is characteristic in  $G$ , then  $\phi(K) = K$  by definition, and thus  $\phi|_K$  is an automorphism of  $K$ . Now  $\phi|_K(H) = H$  since  $H$  is characteristic in  $K$ . But  $\phi|_K$  is just the restriction of  $\phi$  (recall  $H \leq K$ ), so  $\phi(H) = H$ .

2. Consider the automorphism of  $K$  given by  $k \mapsto gkg^{-1}$ ,  $g \in G$ , which is well defined since  $K$  is normal in  $G$ . For any choice of  $g$ , we get a different automorphism of  $K$ , which will always preserve  $H$  since  $H$  is characteristic in  $K$ , and thus  $gHg^{-1} \subset H$  which proves that  $H$  is normal in  $G$ . □

Let us introduce a new definition, that will give us an example of characteristic subgroup.

**Definition 1.33.** The **commutator subgroup**  $G'$  of a group  $G$  is the subgroup generated by all commutators

$$[x, y] = xyx^{-1}y^{-1}.$$

It is also called the **derived subgroup** of  $G$ .

Let us make a few remarks.

- By the subgroup generated by all commutators, we mean that by definition we take the smallest subgroup of  $G$  containing all the commutators. It is thus closed by construction.

- The product of two or more commutators need not be a commutator. It is known that the least order of a finite group for which there exists two commutators whose product is not a commutator is 96.
- Note that the inverse  $[x, y]^{-1}$  of  $[x, y]$  is given by  $[x, y]^{-1} = [y, x] = yxy^{-1}x^{-1}$ .

Here are a list of properties of the commutator subgroup  $G'$ .

**Lemma 1.46.** *Let  $G'$  be the commutator subgroup of  $G$ .*

1.  $G'$  is characteristic in  $G$ .
2.  $G$  is abelian if and only if  $G'$  is trivial.
3.  $G/G'$  is abelian.
4. If  $N$  is normal in  $G$ , then  $G/N$  is abelian if and only if  $G' \leq N$ .

*Proof.* 1. To show that  $G'$  is characteristic in  $G$ , we have to show that  $f(G') = G'$  for  $f$  any automorphism of  $G$ . Now

$$f([x, y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)].$$

2. We have that  $G'$  is trivial if and only if  $xyx^{-1}y^{-1} = 1$  which exactly means that  $xy = yx$ .
3. Since  $G'$  is characteristic, it is also normal in  $G$ , and  $G/G'$  is a group. We are left to prove it is an abelian group. Take two elements (that is two cosets)  $G'x$  and  $G'y$  in  $G/G'$ . We have that  $G'xG'y = G'yG'x \iff G'xy = G'yx$  by definition of the law group on  $G/G'$ . Now

$$G'xy = G'yx \iff xy(yx)^{-1} \in G' \iff xyx^{-1}y^{-1} \in G',$$

which holds by definition.

4. Let us assume that  $N$  is normal in  $G$ . We have that  $G/N$  is a group, and  $G/N$  is abelian if and only if for  $Nx, Ny$  two cosets we have

$$NxNy = NyNx \iff Nxy = Nyx \iff xy(yx)^{-1} \in N \iff xyx^{-1}y^{-1} \in N$$

which exactly tells that each commutator must be in  $N$ . □

We can iterate the process of taking commutators:

$$G^{(0)} = G, G^{(1)} = G', G^{(2)} = (G')', \dots, G^{(i+1)} = (G^{(i)})', \dots$$

The process may or may not reach  $\{1\}$ .

**Definition 1.34.** The group  $G$  is said to be **solvable** if  $G^{(r)} = 1$  for some  $r$ . We then have a **normal series**

$$\{1\} = G^{(r)} \trianglelefteq G^{(r-1)} \trianglelefteq \dots \trianglelefteq G^{(0)} = G$$

called the **derived series** of  $G$ . The term “solvable” historically refers to Galois theory and the question of “solvability” of quintic equations, as we will see later.

We have already seen the notion of subnormal series in the previous section. By normal series, we mean a serie where not only each group is normal in its successor, but also each group is normal in the whole group, namely each  $G^{(i)}$  is normal in  $G$ . We have indeed such series here using the fact that the commutator subgroup is a characteristic subgroup, which is furthermore a transitivity property.

Let us make a few remarks about the definition of solvable group.

**Lemma 1.47.** 1. *Every abelian group is solvable.*

2. *A group  $G$  both simple and solvable is cyclic of prime order.*

3. *A non-abelian simple group  $G$  cannot be solvable.*

*Proof.* 1. We know that  $G$  is abelian if and only if  $G'$  is trivial. We thus get the normal series

$$G^{(0)} = G \triangleright G^{(1)} = \{1\}.$$

2. If  $G$  is simple, then its only normal subgroups are  $\{1\}$  and  $G$ . Since  $G'$  is characteristic and thus normal, we have either  $G' = \{1\}$  or  $G' = G$ . The latter cannot possibly happen, since then the derived serie cannot reach  $\{1\}$  which contradicts the fact that  $G$  is solvable. Thus we must have that  $G' = \{1\}$ , which means that  $G$  is abelian. We conclude by remembering that an abelian simple group must be cyclic of order a prime  $p$ .

3. If  $G$  is non-abelian, then  $G'$  cannot be trivial, thus since  $G$  is simple, its only normal subgroups can be either  $\{1\}$  or  $\{G\}$ , thus  $G'$  must be either one of the other, and it cannot be  $\{1\}$ , so it must be  $G$ . Thus the derived series never reaches  $\{1\}$  and  $G$  cannot be solvable. □

There are several ways to define solvability.

**Proposition 1.48.** *The following conditions are equivalent.*

1.  *$G$  is solvable, that is, it has a derived series*

$$\{1\} = G^{(r)} \trianglelefteq G^{(r-1)} \trianglelefteq \dots \trianglelefteq G^{(0)} = G.$$

2.  *$G$  has a normal series*

$$\{1\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \dots \trianglelefteq G_0 = G$$

*where all factors, that is all quotient groups  $G_i/G_{i+1}$  are abelian.*



3.  $G$  has a subnormal series

$$\{1\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

where all factors, that is all quotient groups  $G_i/G_{i+1}$  are abelian.

*Proof.* That 1.  $\Rightarrow$  2. is clear from Lemma 1.46 where we proved that  $G/G'$  is abelian, where  $G'$  is the commutator subgroup of  $G$ .

That 2.  $\Rightarrow$  3. is also clear since the notion of normal series is stronger than subnormal series.

What we need to prove is thus that 3.  $\Rightarrow$  1. Starting from  $G$ , we can always compute  $G'$ , then  $G^{(2)}, \dots$ . To prove that  $G$  has a derived series, we need to check that  $G^{(s)} = \{1\}$  for some  $s$ . Suppose thus that  $G$  has a subnormal series

$$1 = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

where all quotient groups  $G_i/G_{i+1}$  are abelian. For  $i = 0$ , we get  $G_1 \trianglelefteq G$  and  $G/G_1$  is abelian. By Lemma 1.46, we know that  $G/G_1$  is abelian is equivalent to  $G' \leq G_1$ . By induction, let us assume that  $G^{(i)} \leq G_i$ , that is taking  $i$  times the derived subgroup of  $G$  is a subgroup which is contained in the  $i$ th term  $G_i$  of the subnormal series, and see what happens with  $G^{(i+1)}$ . We have that  $G^{(i+1)} = (G^{(i)})' \leq G'_i$  by induction hypothesis (and noting that if  $H \subset G$  then  $H' \subset G'$ , since all the commutators in  $H$  surely belong to those of  $G$ ). Furthermore,  $G'_i \leq G_{i+1}$  since  $G_i/G_{i+1}$  is abelian. Thus  $G^{(r)} \leq G_r = \{1\}$ .  $\square$

Let us see what are the properties of subgroups and quotients of solvable groups.

**Proposition 1.49.** *Subgroups and quotients of a solvable group are solvable.*

*Proof.* Let us first consider subgroups of a solvable groups. If  $H$  is a subgroup of a solvable group  $G$ , then  $H$  is solvable because  $H^{(i)} \leq G^{(i)}$  for all  $i$ , and in particular for  $r$  such that  $H^{(r)} \leq G^{(r)} = \{1\}$  which proves that the derived series of  $H$  terminates.

Now consider  $N$  a normal subgroup of a solvable group  $G$ . The commutators of  $G/N$  are cosets of the form  $xNyNx^{-1}Ny^{-1}N = xyx^{-1}y^{-1}N$ , so that the commutator subgroup  $(G/N)'$  of  $G/N$  satisfies  $(G/N)' = G'N/N$  (we cannot write  $G'/N$  since there is no reason for  $N$  to be a subgroup of  $G'$ ). Inductively, we have  $(G/N)^{(i)} = G^{(i)}N/N$ . Since  $G$  is solvable,  $G^{(r)} = \{1\}$  and thus  $(G/N)^{(r)} = N/N = \{1\}$  which shows that  $G/N$  is solvable.  $\square$

**Example 1.34.** Consider the symmetric group  $S_4$ . It has a subnormal series

$$\{1\} \triangleleft C_2 \times C_2 \triangleleft A_4 \triangleleft S_4,$$

where  $A_4$  is the alternating group of order 12 (given by the even permutations of 4 elements) and  $C_2 \times C_2$  is the Klein group of order 4 (corresponding to the permutations 1, (12)(34), (13)(24), (14)(23)). The quotient groups are

$$\begin{aligned} C_2 \times C_2 / \{1\} &\simeq C_2 \times C_2 && \text{abelian of order 4} \\ A_4 / C_2 \times C_2 &\simeq C_3 && \text{abelian of order 3} \\ S_4 / A_4 &\simeq C_2 && \text{abelian of order 2.} \end{aligned}$$

We finish by introducing the notion of a nilpotent group. We will skip the general definition, and consider only finite nilpotent groups, for which the following characterization is available.

**Proposition 1.50.** *The following statements are equivalent.*

1.  $G$  is the direct product of its Sylow subgroups.
2. Every Sylow subgroup of  $G$  is normal.

*Proof.* If  $G$  is the direct product of its Sylow subgroups, that every Sylow subgroup of  $G$  is normal is immediate since the factors of a direct product are normal subgroups.

Assume that every Sylow subgroup of  $G$  is normal, then by Lemma 1.37, we know that every normal Sylow  $p$ -subgroup is unique, thus there is a unique Sylow  $p_i$ -subgroup  $P_i$  for each prime divisor  $p_i$  of  $|G|$ ,  $i = 1, \dots, k$ . Now by Lemma 1.32, we have that  $|P_1 P_2| = |P_1| |P_2|$  since  $P_1 \cap P_2 = \{1\}$ , and thus  $|P_1 \cdots P_k| = |P_1| \cdots |P_k| = |G|$  by definition of Sylow subgroups. Since we work with finite groups, we deduce that  $G$  is indeed the direct product of its Sylow subgroups, having that  $G = P_1 \cdots P_k$  and  $P_i \cap \prod_{j \neq i} P_j$  is trivial.  $\square$

**Definition 1.35.** A finite group  $G$  which is the product of its Sylow subgroups, or equivalently by the above proposition satisfies that each of its Sylow subgroup is normal is called a **nilpotent group**.

**Corollary 1.51.** *Every finite abelian group and every finite  $p$ -group is nilpotent.*

*Proof.* A finite abelian group surely has the property that each of its Sylow subgroup is normal, so it is nilpotent.

Now consider  $P$  a finite  $p$ -group. Then by definition  $P$  has only one Sylow subgroup, namely itself, so it is the direct product of its Sylow subgroups and thus is nilpotent.  $\square$

Finite nilpotent groups are also nicely described with respect to their normalizer.

**Proposition 1.52.** *If  $G$  is a finite nilpotent group, then no proper subgroup  $H$  of  $G$  is equal to its normalizer  $N_G(H) = \{g \in G, gH = Hg\}$ .*

*Proof.* Let  $H$  be a proper subgroup of  $G$ , and let  $n$  be the largest index such that  $G_n \subseteq H$  (such index exists since  $G$  is nilpotent). There exists  $a \in G_{n+1}$  such that  $a \notin H$  (since  $H$  is a proper subgroup). Now for every  $h \in H$ , the cosets  $aG_n$  and  $hG_n$  commute (since  $G_{n+1}/G_n \subseteq Z(G/G_n)$ ), namely:

$$G_n ah = (G_n a)(G_n h) = (G_n h)(G_n a) = G_n ha$$

and thus there is some  $h' \in G_n \subseteq H$  for which

$$ah = h'ha$$

that is

$$aha^{-1} = h'h \in H.$$

Thus  $a \in N_G(H)$  and  $a \notin H$ .  $\square$

Here is the definition for possibly infinite nilpotent groups.

**Definition 1.36.** A **central series** for a group  $G$  is a normal series

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

such that  $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$  for every  $i = 0, \dots, n-1$ . An arbitrary group  $G$  is said to be **nilpotent** if it has a central series. The smallest  $n$  such that  $G$  has a central series of length  $n$  is called the **nilpotency class** of  $G$ , and  $G$  is said to be nilpotent of class  $n$ .

**Example 1.35.** Abelian groups are nilpotent of class 1, since

$$\{1\} = G_1 \trianglelefteq G_0 = G$$

is a normal series for  $G$  and for  $i = 0$  we have  $G/\{1\} \simeq G \subseteq Z(G)$ .

Nilpotent groups in general are discussed with solvable groups since they can be described with normal series, and one can prove that they are solvable. Indeed, if  $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ , then the elements of  $G_i/G_{i+1}$  commute with each other, since they commute with everything in  $G/G_{i+1}$ , thus  $G_i/G_{i+1}$  is abelian. It is not true that solvable groups are necessarily nilpotent (see Exercises for an example).

The main definitions and results of this chapter are

- **(1.1-1.2).** Definitions of: group, subgroup, group homomorphism, order of a group, order of an element, cyclic group.
- **(1.3-1.4).** Lagrange's Theorem. Definitions of: coset, normal subgroup, quotient group
- **(1.5).** 1st, 2nd and 3rd Isomorphism Theorems.
- **(1.6).** Definitions of: external (semi-)direct product, internal (semi-)direct product.
- **(1.7).** Cayley's Theorem, the Orbit-Stabilizer Theorem, the Orbit-Counting Theorem. Definitions of: symmetric group, group action, orbit, transitive action, stabilizer, centralizer. That the orbits partition the set under the action of a group
- **(1.8).** Definition:  $p$ -group, Sylow  $p$ -subgroup. The 3 Sylow Theorems, Cauchy Theorem
- **(1.9).** Definition: simple group. Applications of the Sylow Theorems.
- **(1.10).** Definitions: subnormal series, composition series. Jordan-Hölder Theorem.
- **(1.11).** Definitions: characteristic subgroup, commutator subgroup, normal and derived series, solvable group, finite nilpotent group.

# Chapter 2

## Exercises on Group Theory

Exercises marked by (\*) are considered difficult.

### 2.1 Groups and subgroups

**Exercise 1.** Let  $G$  be a group and let  $H$  be a nonempty subset of  $G$ . We have seen that the two following statements are equivalent:

- a)  $H$  is a subgroup of  $G$ ,
- b)  $b_1) x, y \in H \Rightarrow xy \in H$   
 $b_2) x \in H \Rightarrow x^{-1} \in H$ .

1. Show that  $b_1)$  is not sufficient to show that  $H$  is a subgroup of  $G$ .
2. Show that however, if  $G$  is a finite group, then  $b_1)$  is sufficient.

**Answer.**

1. Consider for example the group  $G = \mathbb{Q}^*$  with multiplication. Then the set  $\mathbb{Z}$  with multiplication satisfies that if  $x, y \in \mathbb{Z}$  then  $xy \in \mathbb{Z}$ . However,  $\mathbb{Z}$  is not a group with respect to multiplication since  $2 \in \mathbb{Z}$  but  $1/2$  is not in  $\mathbb{Z}$ .
2. Let  $x \in H$ . Then take the powers  $x, x^2, x^3, \dots$  of  $x$ . Since  $G$  is finite, there is some  $n$  such that  $x^n = 1$ , and by  $b_1)$ ,  $x^n \in H$  thus  $1 \in H$ , and  $x^{n-1} = x^{-1} \in H$ .

**Exercise 2.** Let  $G$  be a finite group of order  $n$  such that all its non-trivial elements have order 2.

1. Show that  $G$  is abelian.

2. Let  $H$  be a subgroup of  $G$ , and let  $g \in G$  but not in  $H$ . Show that  $H \cup gH$  is a subgroup of  $G$ .
3. Show that the subgroup  $H \cup gH$  has order twice the order of  $H$ .
4. Deduce from the previous steps that the order of  $G$  is a power of 2.

**Answer.**

1. Let  $x, y \in G$ ,  $x, y$  not 1. By assumption,  $x^2 = y^2 = 1$ , which also means that  $x, y$  and  $xy$  are their own inverse. Now

$$(xy)(xy) = 1 \Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

2. First note that  $H \cup gH$  contains 1 since  $1 \in H$ . Let  $x, y \in H \cup gH$ . Then  $x \in H$  or  $x \in gH$ , and  $y \in H$  or  $y \in gH$ . If both  $x, y \in H$ , then clearly  $xy \in H$  since  $H$  is a subgroup. If both  $x, y \in gH$ , then  $x = gh, y = gh'$  and  $xy = ghgh' = hh' \in H$  since  $G$  is commutative and  $g^2 = 1$ . If say  $x \in H$  and  $y \in gH$  (same proof vice-versa), then  $xy = xgh = g(xh) \in gH$  since  $G$  is commutative. For the inverse, if  $x \in H$ , then  $x^{-1} \in H$  since  $H$  is a subgroup. If  $x \in gH$ , then  $x = gh$ , and  $x^{-1} = h^{-1}g^{-1} = gh$  since  $G$  is commutative and all elements have order 2.
3. It is enough to show that the intersection of  $H$  and  $gH$  is empty. Let  $x \in H$  and  $x \in gH$ . Then  $x = gh$  for  $h \in H$ , so that  $xh = gh^2 = g$ , which is a contradiction, since  $xh \in H$  and  $g$  is not in  $H$  by assumption.
4. Take  $h$  an element of order 2 in  $G$ , and take  $H = \{1, h\}$ . If  $G = H$  we are done. If not, there is a  $g$  not in  $H$ , and by the previous point  $H \cup gH$  has order 4. We can now iterate. If  $G = H \cup gH$  we are done. Otherwise,  $H \cup gH = H'$  is a subgroup of  $G$ , and there exists a  $g'$  not in  $H'$ , so that  $H' \cup g'H'$  has order 8. One can also write a nice formal proof by induction.

**Exercise 3.** Let  $G$  be an abelian group, and let  $x, y \in G$  of finite order. Show that  $|xy|$  divides  $lcm(|x|, |y|)$ , where  $lcm$  stands for “least common multiple”. Give an example to illustrate that  $|xy| \neq lcm(|x|, |y|)$  in general.

**Answer.** Let  $x \in G$  be of order  $n$  and let  $y \in G$  be of order  $m$ . Since  $G$  is an abelian group, we have that

$$(xy)^k = x^k y^k$$

for any  $k$ . Thus by definition, the order  $|xy|$  is the smallest positive  $k$  such that  $x^k y^k = 1$ . Also by definition, the  $lcm(|x|, |y|) = lcm(n, m) = N$  satisfies that  $N = nn' = mm'$ , so that

$$x^N y^N = (x^n)^{n'} (y^m)^{m'} = 1.$$

Finally  $(xy)^k = (xy)^N = 1$  and since  $k$  is the smallest such positive integer with this property, it must divide  $N$ . (If you are not yet convinced, you can add that  $k$  is smaller than  $N$ , thus you can divide  $N$  by  $k$  and write  $N = kq + r$ ,  $r < k$ , which implies that  $1 = (xy)^{kq+r} = (xy)^r$ , a contradiction to the definition of  $k$ .) An easy counter-example is: take  $y = x^{-1}$ ,  $x \neq 1$ , then  $|1| \neq lcm(|x|, |x^{-1}|)$ .

**Exercise 4.** Let  $G$  be a group and let  $H$  and  $K$  be two subgroups of  $G$ .

1. Is  $H \cap K$  a subgroup of  $G$ ? If your answer is yes, prove it. If your answer is no, provide a counterexample.
2. Is  $H \cup K$  a subgroup of  $G$ ? If your answer is yes, prove it. If your answer is no, provide a counterexample.

**Answer.**

1. This is true. It is enough to check that  $xy^{-1} \in H \cap K$  for  $x, y \in H \cap K$ . But since  $x, y \in H$ , we have  $xy^{-1} \in H$  since  $H$  is a subgroup, and likewise,  $xy^{-1} \in K$  for  $x, y \in K$  since  $K$  is a subgroup.
2. This is false. For example, take the groups of integers modulo 3 and 2, namely  $\mathbb{Z}/3\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z}$ . Then 2 and 3 are in their union, but 5 is not.

**Exercise 5.** Show that if  $G$  has only one element of order 2, then this element is in the center of  $G$  (that is the elements of  $G$  which commute with every element in  $G$ ).

**Answer.** Let  $x$  be the element of order 2. Then  $xyx^{-1}$  has also order 2. Thus it must be either 1 or  $x$ . If  $xyx^{-1} = 1$ , then  $x = 1$  a contradiction. Thus  $xyx^{-1} = x$ .

**Exercise 6.** Let  $G$  be a group and  $H$  be a subgroup of  $G$ . Show that

$$N_G(H) = \{g \in G, gH = Hg\}$$

and

$$C_G(H) = \{g \in G, gh = hg \text{ for all } h \in H\}$$

are subgroups of  $G$ .

**Answer.** Take  $x, y \in N_G(H)$ . We have to check that  $xy^{-1} \in N_G(H)$ , that is, that  $xy^{-1}H = Hxy^{-1}$ . But  $Hxy^{-1} = xHy^{-1}$  since  $x \in N_G(H)$ , and  $xHy^{-1} = xy^{-1}H$  since  $yH = Hy \iff y^{-1}H = Hy^{-1}$ .

Now take  $x, y \in C_G(H)$ . We have to check that  $xy^{-1}h = hxy^{-1}$  for all  $h \in H$ . But  $hxy^{-1} = xhy^{-1}$  because  $x \in C_G(H)$ , and  $xhy^{-1} = xy^{-1}h$  since  $yh = hy \iff y^{-1}h = hy^{-1}$ .

## 2.2 Cyclic groups

**Exercise 7.** Let  $G = \mathbb{Z}_{24}^*$  be the group of invertible elements in  $\mathbb{Z}_{24}$ . Find all cyclic subgroups of  $G$ .

**Answer.** We have that the size of  $G$  is

$$|G| = \varphi(24) = \varphi(3)\varphi(2^3) = 2 \cdot 4 = 8.$$

$G$  is given by the elements that are invertible mod 24, that is, those that are coprime to 24:

$$G = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

Now

$$\begin{aligned} \langle 1 \rangle &= \{1\}, \\ \langle 5 \rangle &= \{5, 5^2 = 1\}, \\ \langle 7 \rangle &= \{7, 7^2 = 49 = 1\}, \\ \langle 11 \rangle &= \{11, 11^2 = 121 = 1\} \\ \langle 13 \rangle &= \{13, 13^2 = 169 = 1\} \\ \langle 17 \rangle &= \{17, 17^2 = (-7)^2 = 1\} \\ \langle 19 \rangle &= \{19, 19^2 = (-5)^2 = 1\} \\ \langle 23 \rangle &= \{23, 23^2 = (-1)^2 = 1 \end{aligned}$$

and there are 8 cyclic subgroups of  $G$ , including the trivial subgroup  $\{1\}$ .

**Exercise 8.** Let  $G = \mathbb{Z}_{20}^*$  be the group of invertible elements in  $\mathbb{Z}_{20}$ . Find two subgroups of order 4 in  $G$ , one that is cyclic and one that is not cyclic.

**Answer.** As in the exercise above,  $G$  contains

$$|G| = \varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8.$$

These 8 elements are coprime to 20, that is

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

The subgroup

$$\langle 3 \rangle = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 21 = 1\}$$

is cyclic of order 4. We have that

$$11, 11^2 = 121 = 1, 19, 19^2 = (-1)^2 = 1, 11 \cdot 19 = (-11) = 9, 9^2 = 81 = 1$$

and

$$\{1, 11, 19, 9\}$$

is a group of order 4 which is not cyclic.

**Exercise 9.** Let  $\varphi$  be the Euler totient function. Let  $G$  be a cyclic group of order  $n$ .

1. First show that the order of  $g^k$  is

$$|g^k| = n/\gcd(k, n).$$

2. Show that if  $m|n$ , then  $\langle g^{n/m} \rangle$  is the unique subgroup of  $G$  of order  $m$ .
3. Prove that for every factor  $m$  of  $n$ , the number of elements in  $G$  with order  $m$  is exactly  $\varphi(m)$ .



4. Furthermore, show that  $\sum_{m|n} \varphi(m) = n$ .

**Answer.** Let  $G = \langle g \rangle$  be a cyclic group of order  $n$ , so that every element in  $G$  is of the form

$$g^k, \quad 1 \leq k \leq n.$$

1. Set  $m = \gcd(k, n)$ , so that  $k = mk'$ ,  $n = mn'$ . If  $(g^k)^r = 1$ , then  $n|kr$ , and

$$\frac{n}{m} \mid \frac{kr}{m}.$$

By definition of  $m$ ,  $n/m$  and  $k/m$  are coprime, so that  $n/m$  divides  $r$ . Hence  $n/m$  is the smallest power of  $g^k$  such that  $(g^k)^{n/m} = 1$  showing that  $n/m = |g^k|$ .

2. Let  $H$  be a subgroup of order  $m$ , then  $H = \langle g^k \rangle$  with  $|H| = m$  and some  $k > 0$ . We will show first that  $H$  can be also generated by an element  $g^d$  where  $d = \gcd(k, n)$ , and in particular, we can always write

$$H = \langle g^d \rangle, \quad d|n.$$

Since  $d|k$ ,  $k = dq$  and  $g^k = g^{dq} \in \langle g^d \rangle$  and  $\langle g^k n \rangle \subseteq \langle g^d \rangle$ . Conversely,  $d = \gcd(k, n) = kr + ns$  for some  $r, s$  and

$$g^d = g^{kr+ns} = g^{kr} \in \langle g^k \rangle$$

and  $\langle g^d \rangle \subseteq \langle g^k \rangle$ . Now  $m = |H| = |g^k| = |g^d| = n/\gcd(d, n)$  by the above, and since  $d|n$ , we get that  $m = n/d$ , or  $d = m/n$ .

3. Now for  $m|n$ , an element is of order  $m$  if and only if it is the generator of the only subgroup of  $G$  of order  $m$ . Now there are as many generators for this subgroup as elements coprime to  $m$ , that is  $\varphi(m)$ .
4. To show that  $\sum_{m|n} \varphi(m) = n$ , we can sort the elements of  $G$  according to their order. Since the order of each element divides  $n$ , we have

$$n = \sum_{m|n} \text{nb of elements of order } m = \sum_{m|n} \varphi(m).$$

### 1.3 Cosets and Lagrange's Theorem

**Exercise 10.** Let  $G = S_3$  be the group of permutations of 3 elements, that is

$$G = \{(1), (12), (13), (23), (123), (132)\}$$

and let  $H = \{(1), (12)\}$  be a subgroup. Compute the left and right cosets of  $H$ .

**Answer.** We have

$g$	$gH$	$Hg$
(1)	$\{(1), (12)\}$	$\{(1), (12)\}$
(12)	$\{(1), (12)\}$	$\{(1), (12)\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(13), (123)\}$	$\{(23), (123)\}$
(132)	$\{(23), (132)\}$	$\{(13), (132)\}$

For example,  $H(23)$  is  $\{(1)(23), (12)(23)\}$ . Clearly  $(1)(23) = (23)$ . Now  $(12)(23)$  sends  $123 \mapsto 132$  via  $(23)$ , and then sends  $132 \mapsto 231$  via  $(12)$ , so that finally we have  $123 \mapsto 231$  which can be written  $(123)$ .

**Exercise 11.** Let  $G$  be a finite group and let  $H$  and  $K$  be subgroups with relatively prime order. Then  $H \cap K = \{1\}$ .

**Answer.** Since  $H \cap K$  is a subgroup of both  $H$  and  $K$ , we have

$$|H \cap K| \mid |H|, |H \cap K| \mid |K|$$

by Lagrange's Theorem. Since  $(|H|, |K|) = 1$ , it must be that  $|H \cap K| = 1$  implying that  $H \cap K = \{1\}$ .

## 2.3 Normal subgroups and quotient group

**Exercise 12.** Consider the following two sets:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}, U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{R} \right\}.$$

1. Show that  $T$  is a subgroup of  $GL_2(\mathbb{R})$ .
2. Show that  $U$  is a normal subgroup of  $T$ .

**Answer.**

1. It is enough to show that if  $X, Y \in T$ , then  $XY^{-1} \in T$ . Let

$$X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, Y = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

then

$$XY^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} = \frac{1}{a'c'} \begin{pmatrix} ac' & -ab' + a'b \\ 0 & a'c \end{pmatrix} \in T$$

2. We have to show that  $XYX^{-1} \in U$  when  $Y \in U$  and  $X \in T$ . We have

$$\begin{aligned} XYX^{-1} &= \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \begin{pmatrix} a' & a'b + b' \\ 0 & c' \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \frac{1}{a'c'} \begin{pmatrix} a'c' & -b'a' + a'(a'b + b') \\ 0 & a'c' \end{pmatrix} \in U. \end{aligned}$$

**Exercise 13.** Let  $G$  be a group, and let  $H$  be a subgroup of index 2. Show that  $H$  is normal in  $G$ .

**Answer.** If  $H$  is of index 2, that means by definition that there are only 2 cosets, say  $H$  and  $g_1H$  for some  $g_1$  not in  $H$ . Note that if  $g_1 \neq g_2 \in G$  are not in  $H$ , then  $g_1g_2 \in H$ . Indeed, we have that either  $g_1g_2 \in H$  or  $g_1g_2 \in g_1H$  (recall that the cosets partition the group), and  $g_1g_2 \in g_1H$  is not possible since  $g_2$  is not in  $H$ . In other words, if both  $g_1, g_2$  are not in  $H$ , then  $(g_1g_2)H(g_1g_2)^{-1} \in H$ .

Now let  $h \in H, g \in G$ . If  $g \in H$ , then  $ghg^{-1} \in H$  and we are done. If  $g$  is not in  $H$ , then  $gh$  is not in  $H$  and by the above remark we have that  $ghg^{-1} = (gh)g^{-1} \in H$  (take  $g_1 = gh, g_2 = g^{-1}$ ). Alternatively by the same above remark, since  $(g_1g_2)H(g_1g_2)^{-1} \in H$  for every  $g_1, g_2$  not in  $H$ , it is enough to write  $g$  as  $g_1g_2$ , say  $g_1 = g$  ( $g$  is not in  $H$ ) and  $g_2 = g^{-1}h$  (which is not in  $H$  either).

**Exercise 14.** If  $G_1$  is normal in  $G_2$  and  $G_2$  is normal in  $G_3$ , then  $G_1$  is normal in  $G_3$ . True or false?

**Answer.** This is wrong (we need the notion of characteristic to get transitivity, this is introduced in the section "Solvable and Nilpotent Groups"). An example is the dihedral group  $D_4$ :

$$D_4 = \langle r, f \mid f^2 = 1, r^4 = 1, fr = r^{-1}f \rangle.$$

The subgroup

$$H = \langle rf, fr \rangle = \{1, rf, r^2, fr\} \simeq C_2 \times C_2$$

is isomorphic to the Klein group. We have that  $H \triangleleft G$ . Finally

$$K = \langle rf \rangle = \{1, rf\} \triangleleft H$$

but  $K$  is not normal in  $G$ , since  $f \cdot rf \cdot f^{-1} = f \cdot rf \cdot f = fr$  which is not in  $K$ .

**Exercise 15.** Let  $G$  be a group and let  $Z(G)$  be its center (that is the elements of  $G$  which commute with every element in  $G$ ). Show that if  $G/Z(G)$  is cyclic then  $G$  is abelian. Give an example to show that if  $G/Z(G)$  is only abelian, then  $G$  does not have to be abelian.

**Answer.** If  $G/Z(G)$  is cyclic, then  $G/Z(G) = \langle gZ(G) \rangle$ . Let  $x, y \in G$ , then their corresponding cosets are  $xZ(G), yZ(G)$  which can be written

$$xZ(G) = (gZ(G))^k = g^k Z(G), \quad yZ(G) = (gZ(G))^l = g^l Z(G)$$

and

$$x = g^k z_1, \quad y = g^l z_2, \quad z_1, z_2 \in Z(G).$$

Now

$$xy = g^k z_1 g^l z_2 = yx$$

since  $z_1, z_2 \in Z(G)$ . For example, consider the dihedral group  $D_4 = \langle r, f \mid f^2 = 1, r^4 = 1, fr = r^{-1}f \rangle$ . Its center is  $Z(D_4) = \{1, r^2\}$ . Thus  $D_4/Z(D_4)$  is a group of order 4, it contains 4 cosets:  $Z(D_4), rZ(D_4), fZ(D_4), rfZ(D_4)$ , which is isomorphic to the Klein group, which is abelian but not cyclic.

**Exercise 16.** 1. Let  $G$  be a group. Show that if  $H$  is a normal subgroup of order 2, then  $H$  belongs to the center of  $G$ .

2. Let  $G$  be a group of order 10 with a normal subgroup  $H$  of order 2. Prove that  $G$  is abelian.

**Answer.**

1. Since  $H$  is of order 2, then  $H = \{1, h\}$ . It is furthermore normal, so that  $gHg^{-1} = \{1, ghg^{-1}\}$  is in  $H$ , thus  $ghg^{-1} = h$  and we are done, since this is saying that  $h$  commutes with every  $g \in G$ .

2. Since  $H$  is normal in  $G$ ,  $G/H$  has a group structure, and  $|G/H| = |G|/|H| = 10/2 = 5$ . Thus the quotient group  $G/H$  is a group of order 5, implying that it is cyclic. Now take  $x, y$  in  $G$ , with respective coset  $xH, yH$ . Since the quotient group is cyclic, there exists a coset  $gH$  such that  $xH = (gH)^k = g^k H$ , and  $yH = (gH)^l = g^l H$  for some  $k, l$ . Thus  $x = g^k h, y = g^l h'$  for some  $h, h' \in H$ . We are left to check that  $xy = yx$ , that is  $g^k h g^l h' = g^l h' g^k h$ , which is true since we know that  $h, h' \in H$  which is contained in the center of  $G$  (by the part above).

## 2.4 The isomorphism theorems

**Exercise 17.** Consider  $A$  the set of affine maps of  $\mathbb{R}$ , that is

$$A = \{f : x \mapsto ax + b, \quad a \in \mathbb{R}^*, \quad b \in \mathbb{R}\}.$$

1. Show that  $A$  is a group with respect to the composition of maps.

2. Let

$$N = \{g : x \mapsto x + b, \quad b \in \mathbb{R}\}.$$

Show that  $N$  is a normal subgroup of  $A$ .

3. Show that the quotient group  $A/N$  is isomorphic to  $\mathbb{R}^*$ .

**Answer.**

1. Let  $f, g \in A$ . Then

$$(f \circ g)(x) = f(ax + b) = a'(ax + b) + b' = a'ax + a'b + b',$$

where  $a'a \in \mathbb{R}^*$  thus the closure property is satisfied. The composition of maps is associative. The identity element is given by the identity map since

$$\text{Id} \circ f = f \circ \text{Id} = f.$$

Finally, we need to show that every  $f \in A$  is invertible. Take  $f^{-1}(x) = a^{-1}x - a^{-1}b$ . Then

$$f^{-1} \circ f(x) = f^{-1}(ax + b) = a^{-1}(ax + b) - a^{-1}b = x.$$

2. Let  $g \in N$  and let  $f \in A$ . We have to show that

$$f \circ g \circ f^{-1} \in N.$$

We have

$$f \circ g(a^{-1}x - a^{-1}b) = f(a^{-1}(x) - a^{-1}b + b') = x - b + ab' + b \in N.$$

3. Define the map

$$\varphi : A \rightarrow \mathbb{R}^*, f(x) = ax + b \mapsto a.$$

It is a group homomorphism since

$$\varphi(f \circ g) = a'a = \varphi(f)\varphi(g).$$

The kernel of  $\varphi$  is  $N$  and its image is  $\mathbb{R}^*$ . By the 1st isomorphism theorem, we thus have that

$$A/N \simeq \mathbb{R}^*.$$

**Exercise 18.** Use the first isomorphism theorem to

1. show that

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

2. show that

$$\mathbb{C}^*/U \simeq \mathbb{R}_+^*,$$

where

$$U = \{z \in \mathbb{C}^* \mid |z| = 1\}.$$

3. compute

$$\mathbb{R}/2\pi\mathbb{Z}.$$

**Answer.**

1. Consider the map:

$$\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*, X \mapsto \det(X).$$

It is a group homomorphism. Its kernel is  $SL_n(\mathbb{R})$ , its image is  $\mathbb{R}^*$  and thus by the 1st isomorphism theorem, we have

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

2. Consider the map

$$\exp : \mathbb{C}^* \rightarrow \mathbb{R}_+^*.$$

It is a group homomorphism. Its kernel is  $U$ , and its image is  $\mathbb{R}_+^*$  and thus by the 1st isomorphism theorem, we have

$$\mathbb{C}^*/U \simeq \mathbb{R}_+^*.$$

3. Define the map

$$f : \mathbb{R} \rightarrow \mathbb{C}^*, x \mapsto e^{ix}.$$

It is a group homomorphism. Its kernel is  $2\pi\mathbb{Z}$ . Its image is  $\{e^{ix}, x \in \mathbb{R}\} = U$ . Thus by the 1st isomorphism theorem

$$\mathbb{R}/2\pi\mathbb{Z} \simeq U.$$

**Exercise 19.** Let  $G = \langle x \rangle$  be a cyclic group of order  $n \geq 1$ . Let  $h_x : \mathbb{Z} \rightarrow G$ ,  $m \mapsto x^m$ .

- Show that  $h_x$  is surjective and compute its kernel.
- Show that  $G \simeq \mathbb{Z}/n\mathbb{Z}$ .

**Answer.**

- Let  $g \in G$ . Since  $G = \langle x \rangle$ ,  $g = x^k$  for some  $0 \leq k \leq n-1$  and thus  $h_x$  is surjective. Its kernel is the set of  $m$  such that  $x^m = 1$ , thus  $m$  must be a multiple of  $n$  and  $\text{Ker}(h_x) = n\mathbb{Z}$ .
- By the 1st isomorphism theorem, since  $h_x$  is a group homomorphism, we have

$$G \simeq \mathbb{Z}/n\mathbb{Z}.$$

**Exercise 20.** Prove the second isomorphism theorem for groups, namely that if  $H$  and  $N$  are subgroups of  $G$ , with  $N$  normal in  $G$ , then

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

**Answer.** Let  $\pi$  be the canonical epimorphism from  $G$  to  $G/N$ , and let  $\pi_0$  be the restriction of  $\pi$  to  $H$ . Then the kernel of  $\pi_0$  is  $H \cap N$ , so by the 1st isomorphism theorem for groups, we have that  $H/(H \cap N)$  is isomorphic to the image of  $\pi_0$  which is  $\{hN, h \in H\} = HN/N$ .

**Exercise 21.** Prove the third isomorphism theorem for groups, namely that if  $N$  and  $H$  are normal subgroups of  $G$ , with  $N$  contained in  $H$ , then

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

**Answer.** This follows from the 1st isomorphism theorem for groups, if we can find an epimorphism of  $G/N$  into  $G/H$  with kernel  $H/N$ : take  $f(aN) = aH$ . Now  $f$  well-defined, since if  $aN = bN$ , then  $a^{-1}b \in N \subset H$  so  $aH = bH$ . Since  $a$  is arbitrary in  $G$ ,  $f$  is surjective. By definition of coset multiplication,  $f$  is a homomorphism. The kernel is

$$\{aN, aH = H\} = \{aN, a \in H\} = H/N.$$

**Exercise 22.** Consider the short exact sequence of groups

$$1 \xrightarrow{i} A \xrightarrow{u} B \xrightarrow{v} C \xrightarrow{j} 1$$

where  $i$  is the inclusion and  $j$  is the constant map 1.

1. Show that  $Im(u) = Ker(v) \iff v \circ u = 1$ , and  $Ker(v) \subset Im(u)$  (1 denotes the constant map here).
2. Show that in the short exact sequence, we have that  $u$  is injective and  $v$  is surjective.
3. Show that  $u(A)$  is normal in  $B$  and that we have a group isomorphism

$$B/u(A) \simeq C.$$

**Answer.**

1. If  $Im(u) = Ker(v)$ , then clearly  $Ker(v) \subset Im(u)$ . Then  $v \circ u(x) = v(u(x)) = 1$  since  $u(x)$  is in the kernel of  $v$ . Conversely, we have to show that  $Im(u) \subset Ker(v)$ . Let  $u(x) \in Im(u)$ . Now  $v(u(x)) = 1$  and thus  $u(x)$  is in  $Ker(v)$ .
2. To show that  $u$  is injective, we compute its kernel. Now  $Ker(u) = Im(i) = \{1\}$  and  $u$  is injective. To show that  $v$  is surjective, we have to see that  $Im(v) = C$ , but  $Im(v) = Ker(j) = C$ .
3. Since  $Im(u) = Ker(v)$ ,  $u(A)$  is normal in  $B$ , and we conclude by the 1st isomorphism theorem.

## 2.5 Direct and semi-direct products

**Exercise 23.** The *quaternion group*  $Q_8$  is defined by

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

with product  $\cdot$  computed as follows:

$$\begin{aligned} 1 \cdot a &= a \cdot 1 = a, \quad \forall a \in Q_8 \\ (-1) \cdot (-1) &= 1, \quad (-1) \cdot a = a \cdot (-1) = -a, \quad \forall a \in Q_8 \\ i \cdot i &= j \cdot j = k \cdot k = -1 \\ i \cdot j &= k, \quad j \cdot i = -k, \\ j \cdot k &= i, \quad k \cdot j = -i, \\ k \cdot i &= j, \quad i \cdot k = -j. \end{aligned}$$

Show that  $Q_8$  cannot be isomorphic to a semi-direct product of smaller groups.

**Answer.** By definition, a semi direct product must contain two smaller subgroups of trivial intersection  $\{1\}$ . Now the smaller subgroups of  $Q_8$  are  $\{1, -1\}$ ,  $\{1, i, -i, -1\}$ ,  $\{1, j, -j, -1\}$ ,  $\{1, k, -k, -1\}$ , and each contains  $-1$  so that it is not possible that  $Q_8$  is a semi-direct product.

**Exercise 24.** Consider the set of matrices

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, a \neq 0, a, b \in \mathbb{F}_p \right\}$$

(where  $\mathbb{F}_p$  denotes the integers mod  $p$ ).

1. Show that  $G$  is a subgroup of  $SL_2(\mathbb{F}_p)$ .
2. Write  $G$  as a semi-direct product.

**Answer.**

1. That  $G$  is a subset of  $SL_2(\mathbb{F}_p)$  is clear because the determinant of every matrix in  $G$  is 1. We have to show that for  $X, Y \in G$ ,  $XY^{-1} \in G$ . This is a straightforward computation:

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} c^{-1} & -d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac^{-1} & -da + bc \\ 0 & a^{-1}c \end{pmatrix} \in G.$$

2. Take

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, a \neq 0, a \in \mathbb{F}_p \right\}$$

and

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{F}_p \right\}.$$

Both  $K$  and  $H$  are subgroups of  $G$ . Their intersection is the 2-dimensional identity matrix, and  $HK = G$ , since

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a & ba^{-1} \\ 0 & a^{-1} \end{pmatrix}$$



and  $ba^{-1}$  runs through every possible element of  $\mathbb{F}_p$  (since  $b$  does). Also  $H$  is normal in  $G$ , since

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2b \\ 0 & 1 \end{pmatrix} \in H.$$

Note that  $K$  is not normal, which can be seen by doing the same computation. Thus  $G$  is the semi-direct product of  $H$  and  $K$ .

**Exercise 25.** Show that the group  $\mathbb{Z}_n \times \mathbb{Z}_m$  is isomorphic to  $\mathbb{Z}_{mn}$  if and only if  $m$  and  $n$  are relatively prime. Here  $\mathbb{Z}_n$  denotes the integers modulo  $n$ .

**Answer.** If  $m$  and  $n$  are relatively prime, then for a multiple of  $(1, 0)$  to be zero, it must be a multiple of  $n$ , and for a multiple of  $(0, 1)$  to be zero, it must be a multiple of  $m$ . Thus for a multiple  $k$  of  $(1, 1)$  to be zero, it must be a multiple of both  $n$  and  $m$ , and since they are coprime, the smallest possible value of  $k$  is  $mn$ . Hence  $\mathbb{Z}_n \times \mathbb{Z}_m$  contains an element of order  $mn$ , showing that  $\mathbb{Z}_m \times \mathbb{Z}_n$  is isomorphic to  $\mathbb{Z}_{mn}$ . Conversely, suppose that  $\gcd(m, n) > 1$ . Then the least common multiple of  $m$  and  $n$  is smaller than  $mn$ , let us call it  $d$ . This shows that every element of  $\mathbb{Z}_m \times \mathbb{Z}_n$  has order at most  $d$  and thus none of them can generate the whole group, so that it cannot be cyclic, and thus cannot be isomorphic to  $\mathbb{Z}_{mn}$ .

Note that one can also prove this result by the definition of direct product: we have that  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  are both normal subgroups of  $\mathbb{Z}_{mn}$  because this is an abelian group. We are thus left to look at the intersection of  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$ . Recall that  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  are embedded into  $\mathbb{Z}_{mn}$  as respectively

$$\mathbb{Z}_m = \{0, n, 2n, \dots, (m-1)n\}, \quad \mathbb{Z}_n = \{0, m, 2m, \dots, (n-1)m\}.$$

If  $m$  and  $n$  are coprime, then  $\mathbb{Z}_m \cap \mathbb{Z}_n = \{0\}$ . Conversely, if  $x$  belongs to the intersection and is non-zero, then  $x$  must be a multiple of both  $n$  and  $m$  which is not congruent to 0 modulo  $mn$ , and thus  $m$  and  $n$  cannot be coprime.

**Exercise 26.** Let  $\mathbb{Z}_3$  denote the group of integers modulo 3.

1. Show that the map

$$\sigma : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3, (x, y) \mapsto (x + y, y)$$

is an automorphism of  $\mathbb{Z}_3 \times \mathbb{Z}_3$  of order 3.

2. Show that the external semi-direct product of  $\mathbb{Z}_3 \times \mathbb{Z}_3$  and  $\mathbb{Z}_3$  by  $\rho, \rho : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3), i \mapsto \sigma^i$ , is a non-abelian group  $G$  satisfying that

$$a^3b^3 = (ab)^3$$

for any  $a, b$  in  $G$ .

**Answer.**

1. So to be an automorphism,  $\sigma$  has to be a group homomorphism, but

$$\sigma((x+x', y+y')) = (x+x'+y+y', y+y') = (x+y, y) + (x'+y', y') = \sigma(x, y) + \sigma(x', y').$$

It clearly goes from the group to itself, and it is a bijection. It is an injection

$$\sigma(x, y) = \sigma(x', y') \Rightarrow (x + y, y) = (x' + y', y') \Rightarrow y = y', x = x',$$

and thus it is a surjection since the group is finite. It is of order 3, since

$$\sigma(x, y) = (x + y, y), \sigma^2(x, y) = (x + 2y, y), \sigma^3(x, y) = (x + 3y, y) = (x, y).$$

2. An element in the external semi-direct product is of the form  $((x, y), i)$ , and we have

$$((x, y), i)((x, y), i) = ((x, y) + \sigma^i(x, y), 2i),$$

$$\begin{aligned} ((x, y), i)^3 &= ((x, y) + \sigma^i(x, y) + \sigma^{2i}(x, y), 3i) \\ &= ((x, y) + (x + iy, y) + (x + 2iy, y), 3i) \\ &= ((3x + 3iy, 3y), 3i) \\ &= ((0, 0), 0). \end{aligned}$$

This shows that for any element  $a$  of the semi-direct product  $a^3 = 0$ , thus  $b^3 = 0$ ,  $ab$  is another element of the group thus  $(ab)^3 = 0$  which shows that  $a^3b^3 = 0 = (ab)^3$ , though the group is non-abelian (because  $\sigma$  is not the identity).

## 2.6 Permutations and Group action

**Exercise 27. (\*)** In a group  $G$  of order  $n$ , for all divisors  $d$  of  $n$ , there exists at least one subgroup of order  $d$ . True or false? [Though the statement only involves the order of a group, there were not enough examples of groups seen in the lecture notes earlier to come up with a counter-example.]

**Answer.** This is false. The smallest counterexample is the alternating group  $G = A_4$  of even permutation on 4 elements, given explicitly by

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123),$$

$$(132), (124), (142), (134), (143), (234), (243)\}.$$

It has 12 elements. We will now show that it has no subgroup of order 6. Let  $H$  denote a subgroup of order 6, that is,  $H$  has index 2 in  $A_4$  and there are only two cosets, satisfying

$$A_4 = H \cup Ha,$$

for all  $a \in A_4$  but not in  $H$ . Consider the coset  $Ha^2$ . We have that either  $Ha^2 = H$  or  $Ha^2 = Ha$ . If  $Ha^2 = Ha$ , then  $Ha = H$  and  $a \in H$ , a contradiction. Thus

$$Ha^2 = H,$$

for all  $a \in A_4$  but not in  $H$ . But those  $a \in H$ , because  $H$  is a subgroup, also satisfy that  $Ha^2 = H$ , so that we deduce that

$$Ha^2 = H, \forall a \in A_4.$$

This in turn implies that

$$a^2 \in H \forall a \in A_4.$$

Let now  $b \in A_4$  be an element of order 3, that is  $b^3 = e$ . Then  $b^2 = b^{-1}$  and  $b^2 \in H$  showing that  $b^{-1} \in H$  and finally  $b \in H$ . We have just shown that every element of order 3 in  $A_4$  are in  $H$ , which is contradiction, since  $A_4$  contains 8 elements of order 3. (If you are not satisfied with this proof, please check “Variations on a Theme:  $A_4$  Definitely Has No Subgroup of Order Six!” by M. Brennan and D. Machale, available online, where 12 different proofs are provided.)

**Exercise 28.** 1. Let  $G = GL_n(\mathbb{C})$  and  $X = \mathbb{C}^n - \{0\}$ . Show that  $G$  acts on  $X$  by  $G \times X \rightarrow X, (M, \nu) \mapsto M\nu$ .

2. Show that the action is transitive.

**Answer.**

1. We have to show that

$$M \cdot (M' \cdot \nu) = (MM') \cdot \nu, 1_G \cdot \nu = \nu.$$

The first point is clear by properties of matrix vector multiplication. The second is also clear since  $1_G$  is the identity matrix.

2. We have to show that there is only one orbit (which is why we have to remove the whole zero vector from  $\mathbb{C}^n$ ). For that, we need to show that for any two vectors  $\nu, \nu' \in X$ , there is a matrix  $M \in G$  such that  $M\nu = \nu'$ . We thus have a system of  $n$  linear equations for  $n^2$  unknowns, so that we have enough degrees of freedom to find such a matrix. Alternatively, if  $\nu = (a_1, \dots, a_n)$ ,  $\nu' = (b_1, \dots, b_n)$ , where  $a_i, b_i$  are all non-zero, take the matrix

$$\text{diag}(a_1^{-1}, \dots, a_n^{-1})$$

and notice that

$$\text{diag}(b_1, \dots, b_n) \text{diag}(a_1^{-1}, \dots, a_n^{-1}) \nu = \nu'.$$

The case where some  $a_i, b_j$  are zero can be done similarly.

**Exercise 29.** Let  $G$  be group, and  $H$  be a subgroup of  $G$ . Show that

$$g \cdot g'H = gg'H$$

defines an action of  $G$  on the set  $G/H$  of cosets of  $H$ . Find the stabilizer of  $gH$ .

**Answer.** To show that the action is well defined we have to check that it does not depend on the choice of the representative, and that it satisfies the definition of group action. First suppose that  $g'H = g''H$ . We have to show that  $g \cdot g'H = gg'H$ . But  $g'H = g''H \iff (g'')^{-1}g' \in H \iff (gg'')^{-1}(gg') \in H \iff gg'H = gg''H$ . The definition of group action can be checked easily:

$$g_1 \cdot (g_2 \cdot g'H) = g_1 \cdot g_2g'H = g_1g_2g'H = g_1g_2 \cdot g'H, \quad 1 \cdot g'H = g'H.$$

The stabilizer of  $gH$  is formed by  $g'$  such that  $g'gH = gH$  that is  $g^{-1}g'g \in H$ . Thus  $g^{-1}g'g = h$ , for some  $h \in H$ , or equivalently  $g' = ghg^{-1}$ , thus the stabilizer is  $gHg^{-1}$ .

**Exercise 30.** Consider the *dihedral group*  $D_8$  given by

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

(that is  $s^2 = 1$ ,  $r^4 = 1$  and  $(rs)^2 = 1$ ).

1. Divide the elements of the dihedral group  $D_8$  into conjugacy classes.
2. Verify the class equation.

**Answer.**

1. There are 5 conjugacy classes

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

2. We have that  $\{1\}$  and  $\{r^2\}$  are in the center. Thus

$$|D_8| = 8 = |Z(D_8)| + |B(r)| + |B(rs)| + |B(s)|.$$

**Exercise 31.** The *quaternion group*  $Q_8$  is defined by

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

with product  $\cdot$  computed as follows:

$$\begin{aligned} 1 \cdot a &= a \cdot 1 = a, \quad \forall a \in Q_8 \\ (-1) \cdot (-1) &= 1, \quad (-1) \cdot a = a \cdot (-1) = -a, \quad \forall a \in Q_8 \\ i \cdot i &= j \cdot j = k \cdot k = -1 \\ i \cdot j &= k, \quad j \cdot i = -k, \\ j \cdot k &= i, \quad k \cdot j = -i, \\ k \cdot i &= j, \quad i \cdot k = -j. \end{aligned}$$

1. Show that if  $x \notin Z(Q_8)$ , then  $|C_{Q_8}(x)| = 4$ .
2. Show that as a consequence, the class of conjugacy of  $x \notin Z(D_8)$  has only two elements.

**Answer.**

1. The center  $Z(Q_8)$  is  $Z(Q_8) = \{1, -1\}$ . We have by definition that

$$C_{Q_8}(x) = \{g \in Q_8, gx = xg\}.$$

Thus

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

2. When the action is defined by conjugation, we have that  $\text{Stab}(x) = C_{Q_8}(x)$ . Thus by the Orbit-Stabilizer, the size of an orbit, which is a conjugacy class, is

$$|B(x)| = |Q_8|/|C_{Q_8}(x)| = 8/4 = 2.$$

**Exercise 32.** Let  $G$  be a group and let  $H$  and  $K$  be two subgroups of  $G$ .

1. Show that the subgroup  $H$  acts on the set of left cosets of  $K$  by multiplication.
2. Consider the coset  $1K = K$ . Compute its orbit  $B(K)$  and its stabilizer  $\text{Stab}(K)$ .
3. Compute the union of the cosets in  $B(K)$  and deduce how many cosets are in the orbit.
4. Use the Orbit-Stabilizer Theorem to get another way of counting the number of cosets in  $B(K)$ . By comparing the two expressions to count the cardinality of  $B(K)$ , can you recover a known result on the cardinality of  $HK$ ?

**Answer.**

1. Let  $X = \{gK, g \in G\}$  be the set of left cosets of  $K$ . We have to check that  $h' \cdot (h \cdot gK) = (h'h) \cdot gK$  which clearly holds, as does  $1_H \cdot gK = gK$ .
2. We have that  $B(K) = \{h \cdot K, h \in H\}$  and  $\text{Stab}(K) = \{h \in H, h \cdot K = K\} = H \cap K$ .
3. The union of the cosets in  $B(K)$  is  $HK$ , the cosets in  $B(K)$  are disjoint and each has cardinality  $K$ , so that we have  $|HK|/|K|$  cosets in  $B(K)$ .

4. By the Orbit-Stabilizer Theorem, we have

$$|B(K)| = |H|/|\text{Stab}(K)| \Rightarrow |HK|/|K| = |H|/|H \cap K|$$

and thus

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

**Exercise 33.** Let  $G$  be a finite group, and let  $p$  be the smallest prime divisor of the order of  $G$ .

1. Let  $H$  be a normal subgroup of  $G$ . Show that  $G$  acts on  $H$  by conjugation.
2. Let  $H$  be a normal subgroup of  $G$  of order  $p$ .
  - Show that the orbits of  $H$  under the action of  $G$  are all of size 1.
  - Conclude that a normal subgroup  $H$  of order  $p$  is contained in the center of  $G$ .

**Answer.**

1. We check the definition, that is, the group  $G$  acts on  $H$  if for the map  $(g, x) \mapsto g \cdot x = gxg^{-1}$ ,  $x \in H$ , defined from  $G \times H \rightarrow H$  (note that we need here  $H$  normal to guarantee that  $gxg^{-1} \in H$ !), we have
  - $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = h(gxg^{-1})h^{-1} = (hg) \cdot x$
  - $1 \cdot x = x$  for all  $x \in H$
2.
  - By the orbit stabilizer theorem, the size of an orbit  $B(x), x \in H$  divides the size of  $G$ , the group that acts on  $H$ , thus if  $|B(x)|$  is not 1, it must be at least  $p$ , since  $p$  is the smallest divisor of the order of  $G$ . Now the orbits partition  $H$ , that is  $H = \cup B(x)$  and thus  $|H| = \sum |B(x)|$ , that is the sum of the cardinals of the orbits is  $|H| = p$ . Among all the  $B(x)$ , we can take  $x = 1 \in H$  since  $H$  is a subgroup. The orbit  $B(1) = \{g \cdot 1, g \in G\} = \{g1g^{-1} = 1\}$  has only 1 element, there is at least one orbit of size 1, and thus no orbit can have size greater or equal to  $p$ , since then  $p + 1 > p$ . Thus all orbits of  $H$  are of size 1.
  - We have that  $B(x) = \{g \cdot x, g \in G\} = \{gxg^{-1}, g \in G\}$  is always of size 1, and since for  $g = 1 \in G$  we have  $x \in B(x)$ , we deduce that  $B(x) = \{x\}$ , that is  $gxg^{-1} = x$ , or  $gx = xg$  showing that for all  $x \in H$ ,  $x$  actually commutes with every  $g \in G$ , that is,  $H$  is contained in the center.

**Exercise 34.** Let  $G$  be a group acting on a finite set  $X$ .

1. We assume that every orbit contains at least 2 elements, that  $|G| = 15$ , and that  $|X| = 17$ . Find the number of orbits and the cardinality of each of them.

2. We assume that  $|G| = 33$  and  $|X| = 19$ . Show that there exists at least one orbit containing only 1 element.

**Answer.**

1. The cardinal of every orbit divides the order of  $G$ . Furthermore, the sum of the orbit cardinalities is equal to the cardinality of  $X$ . If  $|G| = 15$ ,  $|X| = 17$ , and there is no orbit of size 1, there is only one possibility: 4 orbits of length 3 and 1 of length 5. Indeed, we are looking for integers such that their sum is 17, but each integer must divide 15, that is we need to realize 17 as a sum of integers belonging to  $\{3, 5, 15\}$  (1 is excluded by assumption). Then 15 is not possible, and we can use only 3 and 5:  $15+2$  is not possible,  $10+7$  is not possible, so only  $5+12$  works.
2. Now  $|G| = 33$  and  $|X| = 19$ . The divisors of 33 are 1, 3, 11 and 33. We need to obtain as above 19 as a sum of these divisors. 33 is too big, and we cannot possibly use only 11 and 3. Thus there must be at least one orbit of size 1.

**Exercise 35.** Let  $G$  be a finite group of order  $n \geq 1$  and let  $p$  be a prime. Consider the set

$$X = \{x = (g_1, g_2, \dots, g_p) \in G^p \mid g_1 \cdot g_2 \cdots g_p = 1_G\}.$$

1. Compute the cardinality  $|X|$  of the set  $X$ .
2. Show that if  $(g_1, \dots, g_p) \in X$ , then  $(g_2, \dots, g_p, g_1) \in X$ . Denote by  $\sigma$  the corresponding permutation. Show that  $\langle \sigma \rangle$  acts on  $X$  as follows:

$$\sigma^k \cdot (g_1, \dots, g_p) = (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}), \quad k \in \mathbb{Z}$$

3. What is the cardinal of one orbit of  $X$ ?
4. What are the orbits with one element? Show that there is at least one such orbit.
5. Deduce that if  $p$  does not divide  $n$ , then

$$n^{p-1} \equiv 1 \pmod{p}.$$

6. Deduce Cauchy Theorem from the above, namely, if  $p \mid n$  then  $G$  has at least one element of order  $p$ .

**Answer.**

1. Since  $g_1, \dots, g_{p-1}$  can take any value in  $G$  (only  $g_p$  is constrained so as to have  $g_1 \cdot g_2 \cdots g_p = 1_G$ ), we have  $|X| = |G|^{p-1} = n^{p-1}$ .
2. Since  $(g_1, \dots, g_p) \in X$ , then  $g_1 \cdot g_2 \cdots g_p = 1_G$  and  $g_2 \cdots g_p \cdot g_1 = g_1^{-1} \cdot 1_G \cdot g_1$  showing that  $(g_2, \dots, g_p, g_1) \in X$ . To show that  $\langle \sigma \rangle$  acts on  $X$ , check the definition, namely  $\sigma^l \cdot (\sigma^k \cdot (g_1, \dots, g_p)) = \sigma^l \sigma^k \cdot (g_1, \dots, g_p)$  and  $\sigma^0 \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$ .

3. The answer is either 1 or  $p$ . There are two ways to do it: one can notice that  $\langle \sigma \rangle$  has order  $p$ , and thus by the Orbit-Stabilizer Theorem the size of the orbit divides  $p$ , so it can be either 1 or  $p$ . Also one can just write down the definition of one orbit: the orbit of  $(g_1, \dots, g_p)$  is formed by all the shifts of the components, and thus since  $p$  is prime, there will be  $p$  distinct shifts, apart if all the components are all the same, in which case there is only one element in the orbit.
4. Since an element always belongs to its orbit, we have that orbits with one element are of the form  $B(x) = \{x\}$ , and if there is only one element, that means that the shifts are doing nothing on  $x = (g_1, \dots, g_p)$  thus  $x = (g, \dots, g)$  and since  $x \in X$ , that further means that  $g^p = 1_G$ . To show one such orbit exists, take the orbit of  $(1, \dots, 1)$ .
5. Since the orbits partition  $X$ , we have

$$|X| = \sum |B(x)| + \sum |B(x')|$$

where the first sum is over orbits of size 1, and the second over orbits of size greater or equal to 2. By the above, if the size is at least 2, it is  $p$ , and thus  $|B(x')| \equiv 0 \pmod{p}$ . Then if there were more than  $(1, \dots, 1)$  with orbit of size 1, that means an element  $g$  such that  $g^p = 1$ , which would mean  $p|n$ , a contradiction. Thus only there is only one orbit of size 1, and

$$|X| = n^{p-1} \equiv 1 \pmod{p}.$$

6. Again, we have that

$$n^{p-1} = |X| = \sum |B(x)| + \sum |B(x')|$$

and if  $p|n$  then  $0 \equiv \sum |B(x)|$  and there must be at least another element with orbit size 1, that is an element  $g$  of order  $p$ .

## 2.7 The Sylow theorems

**Exercise 36.** Let  $G$  be a group of order 399.

1. Show that  $G$  has a unique Sylow 19-subgroup  $P$  which is normal in  $G$ .
2. Let  $Q$  be a Sylow 7-subgroup. Show that  $N = PQ$  is a subgroup of order 133 of  $G$ .

**Answer.**

1. The number  $n_{19}$  of Sylow 19-subgroups is  $\equiv 1 \pmod{19}$  and divides 21, thus it must be 1. Since it is unique, it has to be normal.



2. Since  $P$  is normal in  $G$ , we have that  $N = PQ$  is a subgroup of  $G$ . (The fact that  $P$  is normal can be used to check directly the definition of subgroup). By the 2nd isomorphism theorem for groups, we have

$$Q/(Q \cap P) \simeq PQ/P \Rightarrow Q \simeq PQ/P$$

since  $Q \cap P = \{1\}$  so that  $|PQ| = |P||Q| = 19 \cdot 7 = 133$ .

**Exercise 37.** Let  $G$  be a simple group of order 168.

1. Compute its number of Sylow 7-subgroups.
2. Deduce the number of elements of order 7 in  $G$ .

**Answer.**

1. Since  $168 = 2^3 \cdot 3 \cdot 7$ , the number of Sylow 7-subgroups must be  $\equiv 1 \pmod{7}$  and must divide 24. The only possibilities are thus 1 and 8. Since  $G$  is simple, it cannot be 1.
2. Elements of order 7 correspond to generators of the cyclic Sylow 7-subgroups, and there are 6 of them per Sylow 7-subgroup, that is  $6 \times 8 = 48$  elements of order 7.

**Exercise 38. (\*)** This exercise aims at classifying groups of order up to 8.

1. For  $p$  prime, show that any group  $G$  with cardinality  $p^2$  is abelian.
2. For  $p$  an odd prime, show that any non-abelian group  $G$  of order  $2p$  is isomorphic to the dihedral group  $D_p$ .
3. Determine all the finite groups of order at most 8 up to isomorphism.

**Answer.**

1. Let  $Z(G)$  be the center of  $G$ . We have by Lagrange Theorem that  $|Z(G)|$  divides  $p^2$ , thus we have 3 cases:
  - $|Z(G)| = 1$ : we know that the center of a  $p$ -group cannot be trivial, thus this case cannot happen.
  - $|Z(G)| = p^2$ : then clearly  $G$  is abelian.
  - $|Z(G)| = p$ : then  $|G/Z(G)| = p^2/p = p$ , and then quotient group is cyclic, and we already showed (see Exercise 15) that in this case it implies that  $G$  is abelian.
2. Let  $G$  be a group of order  $2p$ . Then  $G$  contains an element  $\alpha$  of order  $p$ , and an element  $\beta$  of order 2, by Cauchy Theorem. We will prove

$$\langle \alpha, \beta \rangle \simeq D_p.$$

- First we have that  $|\langle \alpha, \beta \rangle| = 2p$ . Indeed, it must divide  $2p$ , and it must be great than  $p$ , since  $\langle \alpha \rangle$  has already cardinality  $p$  and does not contain  $\beta$ .
- We now show that

$$\beta\alpha\beta^{-1} = \alpha^{-1}.$$

Since  $\langle \alpha \rangle$  is normal in  $G$ , then

$$\beta\alpha\beta^{-1} = \alpha^i$$

for some  $i$ . Since  $\beta^2 = 1$

$$\alpha = \beta^2\alpha\beta^{-2} = \beta(\beta\alpha\beta^{-1})\beta^{-1} = \beta\alpha^i\beta^{-1} = (\beta\alpha\beta^{-1})^i = \alpha^{i^2}$$

and  $i^2 \equiv 1 \pmod{p}$ . If  $i \equiv 1 \pmod{p}$ , then  $\alpha$  and  $\beta$  commute, so  $G$  cannot be non-abelian. Thus  $i \equiv -1 \pmod{p}$  as wanted.

- Finally, it is enough to conclude to show that

$$f(a^m b^e) = \alpha^m \beta^e$$

is an isomorphism, where  $a$  is a rotation of angle  $2\pi/p$  and  $b$  is a reflection. This map is surjective, and both sets have same size, so it is injective. It is also clear that  $f$  is a group homomorphism.

- For prime order  $|G|$ , we have that  $G$  is cyclic, so that gives  $C_2, C_3, C_5, C_7$ .
- For  $|G| = 4$ , we already know that either  $G$  contains an element of order 4, and  $G = C_4$ , or  $G$  has only elements of order 2 (except of course the identity), and then  $G = C_2 \times C_2$ .
- If  $|G| = 6$ , if  $G$  contains an element of order 6, then  $G = C_6$ . If not, then  $G$  must contain 1 element of order 3, and one of order 2, and by the above computations, we have  $G = D_6$ .
- If  $|G| = 8$ , then elements in  $G$  can have order 2,4 and 8. If there is an element of order 8, then  $G = C_8$ . If all elements have order 2, then  $G$  is abelian (namely  $C_2 \times C_2 \times C_2$ ), so for  $G$  to be non-abelian, we must have an element of order 4, say  $g$ . Now we have  $1, g, g^2, g^3 \in G$ . If there is an element  $h$  of order 2,  $h$  not in  $\langle g \rangle$ , then  $hah^{-1}$  has order 4, and repeating the above computations, we can see that  $G = D_8$ . If such an  $h$  does not exist, then all elements not in  $\langle g \rangle$  have order 4. Let  $k$  be such an element of order 4, then  $k^2$  has order 2 and must then be  $g^2$ . In this case, we obtain  $G = Q_8$ . Finally, if  $G$  has an element of order 4 and is abelian but not cyclic, then  $G = C_2 \times C_4$ .

**Exercise 39.** Consider the set of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where  $a, b, c$  are integers modulo 2. Show that this set forms a group and compute its cardinality. Can you identify this group?

**Answer.** This set forms a group under matrix multiplication. Matrix multiplication is clearly associative. One can check that the product of two such matrices still belongs to the set. The identity element is given by the identity matrix. Every matrix is clearly invertible with inverse

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Since  $a, b, c$  are integers modulo 2, there are 8 possible such matrices. Thus it is a group of order 8. It is not commutative, thus it is either  $D_4$  or  $Q_8$ . We note that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

thus

$$\begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

is an element of order 4, and the subgroup it generates is

$$\left\langle \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & b+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, I_3 \right\rangle.$$

So when  $a = 0$  and  $c = 1$ , or  $a = 1$  and  $c = 0$ , we see that we get elements of order 2 not in this subgroup, thus it must be  $D_4$ . (This line of argument comes from the above exercise where we did the classification of groups of order 8.) Alternatively, we can notice that

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is of order 2, and the intersection of this subgroup of order 2 with that above of order 4 is the identity. Again this cannot happen with  $Q_8$  since we know the intersection of any two subgroups cannot be trivial (this was the line of argument used to show that  $Q_8$  cannot be a semi-direct product).

**Exercise 40.** Let  $G$  be a finite  $p$ -group, and let  $H$  be a normal subgroup of  $G$ . Show that  $H \cap Z(G)$  cannot be trivial (where  $Z(G)$  denotes the center of  $G$ ). Is it still true when  $G$  is an infinite  $p$ -group?[this is harder!]

**Answer.** The subgroup  $H$  is normal, thus  $G$  acts by conjugation on  $H$ . Since  $|G| = p^r$  for some  $r$ , the size of the non-trivial orbits is divisible by  $p$ . Since

$G$  is a  $p$ -group,  $H$  is also a  $p$ -group, with say  $|H| = p^s$  for some  $s < r$ . We deduce that the union of orbits has size  $p^s$ , and since the orbits of size  $\geq 2$  are divisible by  $p$ , the union of trivial orbits, that is of orbits of fixed points, is also of cardinality divisible by  $p$ . But the union of orbits of fixed points is  $H \cap Z(G)$ . Since it contains the identity element, it at least contains  $p$  elements and cannot be trivial.

This is not true anymore when the group is infinite. Take for example the group

$$G = \bigcup_{n \geq 1} U(p, n),$$

where  $U(p, n)$  is the group of  $n \times n$  upper triangular matrices with every diagonal coefficient at 1 and elements of  $\mathbb{F}_p$  discussed in Example 1.31. This is an infinite  $p$ -group. Now the center  $Z(U(p, n))$  of  $U(p, n)$  is a cyclic group of order  $p$ , formed by matrices with every diagonal coefficient at 1, one element of  $\mathbb{F}_p$  in position  $(1, n)$  and zeros elsewhere. Thus the center of the infinite  $p$ -group  $G$  which is itself the limit of the  $U(p, n)$  when  $n$  grows will be contained in the limit of these centers, which is in fact the trivial group (that is the limit of the identity matrix when  $n$  tends to infinity).

**Exercise 41.** Let  $G$  be a group of order 57 which is not cyclic.

1. Compute the number of its Sylow 19-subgroups.
2. Deduce the number of elements of order 3 in  $G$ .

**Answer.**

1. Since  $57 = 3 \cdot 19$ ,  $n_{19} | 3$  and  $n_{19} \equiv 1 \pmod{19}$ , showing that  $n_{19} = 1$ .
2. Let  $a \neq 1$  be in  $G$ . Then  $|a| = 3$  or  $|a| = 19$  ( $|a| \neq 57$  since  $G$  is not cyclic and  $|a| \neq 1$  since  $a \neq 1$ ). Since there is only one Sylow 19-subgroup, which is cyclic, it contains 18 elements of order 19, which are all the elements of order 19 of  $G$ . Thus there are exactly 38 elements of order 3 in  $G$ .

**Exercise 42.** Let  $G$  be a group of order 231.

1. Show that  $G$  has a unique Sylow 11-subgroup  $M$ .
2. Compute the number  $n_7$  of its Sylow 7-subgroups.
3. Let  $P$  be a Sylow 3-subgroup and  $L$  be a Sylow 7-subgroup. Show that  $N := PL$  forms a subgroup of order 21.
4. Show that  $N$  is furthermore normal.\*
5. Deduce from the above that  $G$  can be written as  $MN$ .
6. Prove that the Sylow 11-subgroup  $M$  belongs to the center of  $G$ .

**Answer.**

1. We have that

$$231 = 11 \cdot 3 \cdot 7.$$

Thus  $n_{11} \equiv 1 \pmod{11}$  and  $n_{11} \mid 21$ . Thus it must be 1.

2. Again,  $n_7 \equiv 1 \pmod{7}$  and  $n_7$  divides 33. Thus it must be 1.
3. Notice first that since  $L$  is a unique Sylow 7-subgroup, it is normal. We have to see that  $PL$  is a subgroup. Let  $pl$  be an element of  $PL$ . Its inverse is  $(pl)^{-1} = l^{-1}p^{-1}$  and since  $L$  is normal, we know that  $gL = Lg$  for every  $g$  in  $G$ . Thus in particular  $l^{-1}p^{-1} \in Lp^{-1} = p^{-1}L$  and  $l^{-1}p^{-1} = p^{-1}l'$  showing that the inverse belongs to  $PL$ . The same argument works to show that  $plp'l' \in PL$ . We know that  $lp' = p'l''$  by normality of  $L$ , thus  $p(lp')l' = p(p'l'')l' \in PL$  and 1 is in  $PL$ . Now about the order of  $PL$ , since  $|P| = 3$  and  $|L| = 7$ , and  $P \cap L = \{1\}$  because they are groups of order respectively 3 and 7, we have that  $|PL| = |P||L|/|P \cap L| = 21$ .
4. This is the most difficult part. The most likely quickest way to do it is by using the normalizer  $N_G(N)$  of  $N$ . It is a subgroup of  $G$ , thus its order divides  $|G|$ . Since  $N$  is contained in its normalized,  $|N_G(N)| \geq 21$ . So if we can prove that  $|N_G(N)| > 21$ , we are done, because then  $|N_G(N)| = 231$  and the normalizer is  $G$ , which yields the desired conclusion. To show that  $|N_G(N)| > 21$ , it is enough to exhibit at least one element in the normalizer which is not in  $N$ . This is not the most economical way of doing it, but one way is to just get an element in the center. By Cauchy Theorem, we know  $G$  contains an element  $g$  of order 3, and since  $M$  is the unique Sylow 11-subgroup, it is a normal subgroup of  $G$ , which is furthermore cyclic, generated by say  $m$ . We thus have that  $gM = Mg$  that is  $gm = m^l g$  and we are left to show that  $l$  is one. Since  $g$  is of order 3, then  $m = g^3 m g^{-3} = g^2 (g m g^{-1}) g^{-2} = g^2 m^l g^{-2} = g (g m^l g^{-1}) g^{-1} = g (m^l)^l g^{-1} = m^{l^3}$ . This shows that  $l^3 \equiv 1 \pmod{11}$ . But this is possible only if  $l = 1$  ( $\gcd(3, 10) = 1$ ) and  $m$  belongs to the center.
5. That  $MN$  is a group works as above, because  $N$  is normal. That the cardinality is right also works as above, since  $|M| = 11$  and  $|N| = 21$ , thus their intersection is 1, and thus  $|MN| = 231$ , from which it follows that  $MN = G$ .
6. We first observe that  $M$  commutes with  $N$ , since if  $m \in M, n \in N$ , then by normality of  $M$  (it is a unique Sylow 11-subgroup) we have that  $mnm^{-1}n^{-1} \in M \cap N = \{1\}$  implying that  $mn = nm$ . To show that  $M$  commutes with  $G$ , we use the fact that  $G = MN$ , and thus every element  $g \in G$  can be written as  $g = m'n'$ . Now  $gm = (m'n')m = m'mn'$  since  $M$  and  $N$  commute, and  $m'mn' = mm'n' = mg$  since  $M$  is abelian (it is in fact cyclic).

## 2.8 Simple groups

**Exercise 43.** Show that no group of order 200 is simple.

**Answer.** The number of Sylow 5-subgroups of a group of order  $200 = 5^2 \cdot 2^3$  is  $\equiv 1 \pmod{5}$  and divides 8, thus it must be 1. Thus the unique Sylow 5-subgroup is normal and thus the group cannot be simple.

**Exercise 44. (\*)** Let  $G$  be a group such that  $|G| \leq 59$ . Show that if  $G$  is simple, then  $|G|$  is prime.

**Answer.** We know that if  $|G| = pq$ ,  $p, q$  two distinct primes, then  $G$  is not simple. This can be extended by noting that if  $|G| = p^k m$ , where  $k > 0$  and  $(m, p) = 1$ ,  $m < p$ . Indeed, in this case,  $n_p$  must divide  $mp^k$ , and thus must divide  $m$ . But also,  $n_p \equiv 1 \pmod{p}$ , so that if  $n_p \neq 1$  then  $n_p \geq p + 1 > m$ , which contradicts that  $n_p | m$ . We are thus left to check that groups of order

$$12, 24, 30, 36, 40, 45, 48, 56$$

are not simple. We know  $G$  with  $|G| = 45 = 5 \cdot 3^2$  is not simple since  $G$  is not simple when  $|G| = p^2 q$ . If  $|G| = 40$ , then the number  $n_5$  of Sylow 5-subgroups is congruent to 1 modulo 5 and divides 8. The only possibility is  $n_5 = 1$ , and  $G$  has a normal Sylow 5-subgroup. If  $|G| = 56 = 2^3 \cdot 7$ , then the number  $n_7$  of Sylow 7-subgroups must divide 8 and  $\equiv 1 \pmod{7}$ . If  $n_7 = 1$ ,  $G$  is not simple. If  $n_7 = 8$ , then we get  $6 \cdot 8 = 48$  elements of order 7, and only 8 elements are left in the group not of order 7, which correspond to the Sylow 2-subgroup of size 8. Similarly if  $|G| = 12$ , there are  $n_3 \equiv 1 \pmod{3}$  Sylow 3-subgroups, where  $n_3 | 12$ , so this can be 1 or 4. If  $n_3 = 1$   $G$  is not simple. If  $n_3 = 4$ , we get  $4 \cdot 2 = 8$  elements of order 3. The other 4 elements must be part of the Sylow 2-subgroup which is of order 4. We are thus left with

$$24, 30, 36, 48$$

One way to take care of 24, 36 and 48 at once is to prove that the order of  $G$  divides  $n_p!$ . Otherwise it can be done case by case.  $|G| = 30$  is done individually.

**Exercise 45.** Let  $G$  be a group of order 105. Prove that it is impossible that  $|Z(G)| = 7$ .

Suppose to the contrary that  $|Z(G)| = 7$ , then  $|G|/|Z(G)| = 15$  and thus  $G/Z(G)$  is a group of order 15. Since  $15 = 3 \cdot 5$ , that is  $p = 3$ ,  $q = 5$ , with  $p$  which does not divide  $q - 1 = 4$ , then  $G/Z(G)$  is cyclic (by Proposition 1.39) and thus  $G$  is abelian (by Exercise 15).

**Exercise 46.** Let  $G$  be a group,  $H$  a subgroup, and consider  $N_G(H) = \{g \in G, gH = Hg\}$ .

1. Show that the number of conjugates of  $H$  in  $G$  is equal to the index of  $N_G(H)$  in  $G$ .
2. Deduce a formula for the number of Sylow  $p$ -subgroups of  $G$ .
3. Use the above to show that a simple group  $G$  of order 60 cannot have a subgroup of order 20.

**Answer.** First recall that  $N_G(H)$  is a subgroup of  $G$  (see Exercise 6).

1. Let  $G$  act by conjugation on the set  $X$  of its subgroups. By the orbit-stabilizer theorem, we have that  $|B(H)| = |G|/|N_G(H)|$  since  $N_G(H)$  is the stabilizer of  $H$ . Now  $|B(H)|$  is the number of conjugates of  $H$ , which proves the claim.
2. Let  $H$  be a Sylow  $p$ -subgroup of  $G$ . We know by the Sylow theorems that all Sylow  $p$ -subgroups are conjugate, thus  $n_p = |B(H)|$  and  $n_p$  is the index of  $N_G(H)$ .
3. Assume by contradiction that  $K$  is a subgroup of order 20, then  $K$  has a unique Sylow 5-subgroup  $L$  which is then normal, and thus  $K \subset N_G(L)$ . Now the order of  $K$  must divide the order of  $N_G(L)$  and the order of  $G$ , and since  $|K| = 20$ , we have that  $|N_G(L)|$  is 20 or 60:
  - if it is 60, then the index of  $N_G(L)$  is 1, and there is a unique Sylow 5-subgroup in  $G$ , which is then normal, and contradicts the simplicity of  $G$ .
  - if it is 20, then the index is 3, and there are 3 Sylow 5-subgroups in  $G$ , that is  $n_5 = 3$  which contradicts the Sylow theorems:  $n_5 \equiv 1 \pmod{5}$

**Exercise 47. (\*)** Let  $G$  be a simple group of order 60, which thus cannot contain a subgroup of order 20.

1. Show that if  $G$  contains a subgroup  $K$  of order 12, then  $K$  contains 4 Sylow 3-subgroups.
2. Show that if  $H$  and  $K$  are two distinct subgroups of order 4 of  $G$ , then  $H \cap K = \{1\}$ .

**Answer.**

1.  $K$  is of order 12, thus its number  $n_3$  of Sylow 3-subgroups is congruent to 1 mod 3, so

$$n_3 = 1 \text{ or } n_3 = 4$$

(it cannot be more since  $K$  is of order 12). To show that it must be 4, we show that it cannot be 1. Let us assume that  $K$  has a unique Sylow 3-subgroup  $L$ , then  $L$  must be normal in  $K$ , then  $K$  must be contained in  $N_G(L) = \{g \in G, gL = Lg\}$ , and since  $N_G(L)$  is a subgroup of  $G$ , its

order must divide 60, and also be divisible by the order of  $K$  which is 12. Thus

$$|N_G(L)| = 12 \text{ or } 60.$$

Its index in  $G$  is then respectively 5 or 1. Since its index is also the number of Sylow 3-subgroups (because they are all conjugate, and using the Orbit Stabilizer theorem), that means that we have either 1 or 5 Sylow 3-subgroups in  $G$ , which is impossible: 1 is impossible since  $G$  is simple, and 5 is impossible since  $|G| = 60$ , and thus its number of Sylow 3-subgroups is congruent to 1 mod 3.

- The intersection of two subgroups is a subgroup, thus its order is either 1, 2 or 4. It cannot be 4 since they are distinct, to prove that it is 1, let us assume by contradiction that it is 2, thus a cyclic group of order 2:

$$H \cap K = \langle a \rangle$$

and  $a^2 = 1$ . Since the order of  $H$  is 4, the index of  $\langle a \rangle$  in  $H$  is 2, and  $\langle a \rangle$  is normal in  $H$ , that is  $hah^{-1} = a$  and  $H$  is contained in  $C_G(a) = \{g \in G, ga = ag\}$ . The same holds for  $K$  and since both  $H$  and  $K$  are in  $C_G(a)$ , so must be their union  $H \cup K$ . Now the size of  $H \cup K$  is 6, and thus  $|C_G(a)| \geq 6$  and must be divisible by 4. The possibilities are

$$12, 20, 60.$$

Now 20 is impossible, by what is mentioned in the statement of the exercise. 12 is also impossible by the previous question: then  $C_G(a)$  would have 4 Sylow 3-subgroups, showing that there should be only 1 Sylow 2-subgroup, but both  $H$  and  $K$  are in  $C_G(a)$ . This leaves 60: in that case, we would get that  $\langle a \rangle$  is a normal subgroup, and thus it should be the unique Sylow 2-subgroup, which is also a contradiction.

## 2.9 The Jordan-Hölder Theorem

**Exercise 48.** Prove that every finite group has a composition series.

**Answer.** Take the longest possible subnormal series of  $G$ , say

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$$

which is possible since  $G$  is finite. Then the composition factors are all simple. Indeed, if there exists a composition factor  $G_i/G_{i+1}$  which is not simple, then it has a non-trivial normal subgroup, which by the correspondence theorem gives a normal subgroup between  $G_i$  and  $G_{i+1}$ . This extends the subnormal series assumed to be the longest possible, thus a contradiction. The longest possible subnormal series is then a composition series.



**Exercise 49.** Prove that the infinite cyclic group  $G$  has no composition series.

**Answer.** Let  $G = \langle g \rangle$  where  $|g| = \infty$ . Suppose there exists a composition series for  $G$ , that is

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G.$$

It cannot be that  $n = 1$ , that is

$$\{1\} = G_0 \triangleleft G$$

because that would mean that  $G$  is simple, and clearly  $G$  is not simple, because for example  $\langle g^2 \rangle$  is a proper normal subgroup of  $G$ . Thus  $n \geq 2$ , and the composition series contains a subgroup  $G_{n-1}$  different than  $\{1\}$  and  $G$ . Then  $G_{n-1}$  is a non-trivial subgroup of  $G$ , which means it is of the form  $G_{n-1} = \langle g^k \rangle$  for some positive integer  $k$ . But then  $G_{n-1}$  is an infinite cyclic group, so it cannot be simple, which contradicts the definition of composition series.

**Exercise 50.** Show that the group  $GL_n(\mathbb{R})$  has a subnormal series, but no composition series.

**Answer.** The series

$$\{1\} \triangleleft Z(GL_n(\mathbb{R})) \triangleleft SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$$

is a subnormal series, however  $GL_n(\mathbb{R})$  cannot have a composition series, because it contains a normal subgroup isomorphic to the infinite cyclic group (look at matrices of the form a scalar times the identity matrix, which clearly commute with every matrix in  $GL_n(\mathbb{R})$ ).

## 2.10 Solvable and nilpotent groups

**Exercise 51.** Consider the general dihedral group

$$D_{2n} = \{a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1}\}.$$

Is  $D_{2n}$  solvable? Prove your answer.

**Answer.** We have seen several equivalent definitions of  $G$  solvable. One of them is that  $G$  is solvable if and only if there exists a normal series

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G$$

such that  $G_{i+1}/G_i$  is abelian. The rotations  $\langle a \rangle$  form a subgroup of order  $n$ , this is not the case of the reflections (composing two reflections gives a rotation). We have that  $\langle a \rangle$  is normal. So the series

$$\{1\} \triangleleft \langle a \rangle \triangleleft D_{2n}$$

is normal and the quotient  $D_{2n}/\langle a \rangle$  has order two hence is the cyclic group of order 2 which is abelian.

**Exercise 52.** Consider the dihedral group

$$D_6 = \{a, b \mid a^3 = b^2 = 1, b^{-1}ab = a^{-1}\},$$

which was shown to be solvable in the previous exercise. Is  $D_6$  nilpotent? Prove your answer.

**Answer.** It is not, because the number  $n_2$  of its Sylow 2-subgroups is 3. Indeed, we know that  $n_2 \equiv 1 \pmod{2}$ , and  $n_2 \equiv 0 \pmod{3}$ . This contradicts the fact that a finite nilpotent group must have a unique Sylow  $p$ -subgroup for every  $p$ .

**Exercise 53.** Show that the nilpotency class of the quaternion group  $Q_8$  is 2.

**Answer.** A central series for  $Q_8$  is

$$\{1\} = G_2 \triangleleft G_1 = \{1, -1\} \triangleleft G_0 = Q_8.$$

Indeed, we notice that  $G_1$  is the center of  $Q_8$ , thus it is normal in  $Q_8$ , which shows that this is a normal series. Now for  $i = 1$ , we have that  $G_1/G_2 \simeq \{1, -1\} \subseteq Z(G/G_2) \simeq \{1, -1\}$ . For  $i = 0$ , we have that  $G_0/G_1 \simeq G/Z(G)$ , since  $G/Z(G)$  is of order 4 and cannot be cyclic (otherwise  $Q_8$  would be abelian) it must be the Klein group, which is commutative (anyway knowing that the quotient group is of order 4 is enough to conclude the commutativity). Thus  $G/Z(G) \subseteq Z(G/Z(G))$ . Finally, the central series cannot be shortened, since  $Q_8$  is not abelian, thus the nilpotency class of  $Q_8$  is 2.

**Exercise 54. (\*)** Let  $G$  be a group of order 16, which contains an element  $g$  of order 4. Show that  $\langle g^2 \rangle$  is normal in  $G$ .

**Answer.** There are two cases:

1. If  $\langle g \rangle$  is normal in  $G$ , then  $\langle g^2 \rangle$  is also normal in  $G$ , since it is characteristic in  $G$  (this can be checked by the definition, take any automorphism  $f$  of  $\langle g \rangle$ , it thus maps some  $g^i$  to some  $g^j$  and thus  $f((g^2)^i) = f(g^i)^2 = (g^j)^2 \in \langle g^2 \rangle$ ).
2. If  $\langle g \rangle$  is not normal in  $G$ , then the subgroup

$$H = \{h \in G, h\langle g \rangle = \langle g \rangle h\}$$

(called the normalizer of  $\langle g \rangle$ ) will be order 8. Indeed  $H$  is a subgroup of  $G$ , thus  $|H|$  divides 16, that is  $|H| = 1, 2, 4, 8, 16$ , and  $|H| \geq |\langle g \rangle|$ , so that  $|H| = 4, 8, 16$ . It cannot be 16, since otherwise  $\langle g \rangle$  would be normal in  $G$ . Finally, if  $|H| = 4$ , then that would mean that  $\langle g \rangle = H$ . This is not possible either (see result on nilpotent groups (currently Prop 1.50) in the lecture notes). If we can now prove that  $\langle g^2 \rangle$  is characteristic in  $H$ , then we are done, since then  $\langle g^2 \rangle$  is characteristic in  $H$  which is normal in  $G$  (it is of index 2 in  $G$ ) thus  $\langle g^2 \rangle$  is normal in  $G$ .

We are thus left to prove that if  $H$  is a group of order 8, with a cyclic group  $\langle g \rangle$  of order 4, then  $\langle g^2 \rangle$  is characteristic in  $H$ .

1. If  $H$  is abelian, then  $H$  is isomorphic to  $C_8$  or to  $\langle g \rangle \times C_2$ . In both cases it is characteristic (in the first case,  $\langle g^2 \rangle$  is a subgroup of a cyclic group, thus it is characteristic).
2. If  $H$  is not abelian, then its center  $Z(H)$  is of order 2 (the order of the center has to divide  $|H|$ , if it were 4 or 8, then  $H/Z(H)$  would be of order 2 or 1, thus cyclic, which implies that  $H$  is abelian). Furthermore, the center intersects non trivially every non-trivial normal subgroup of  $H$ . Thus  $Z(H) = \langle g^2 \rangle$  since this is the only subgroup of  $\langle g \rangle$  of order 2 and  $\langle g \rangle$  is normal in  $H$  (it is of index 2). Finally  $Z(H)$  is a characteristic subgroup of  $H$  which concludes the proof.

**Exercise 55. True/False.**

- Q1.** There are 3 kinds of groups of order 4, up to isomorphism.
- Q2.** Let  $H$  and  $K$  be two subgroups of  $G$ . Then  $HK$  is a subgroup of  $G$ .
- Q3.** Let  $G$  be a group, and let  $X$  be a set. Then the orbit  $B(x)$  of  $x$  in  $X$  under the action of  $G$  is a subgroup of  $G$ .
- Q4.** The dihedral group  $D_{10}$  of order 20 is simple.
- Q5.** The dihedral group  $D_3$  is isomorphic to the symmetric group  $S_3$ .
- Q6.** Let  $H$  and  $N$  be two subgroups of  $G$ , with  $N$  normal in  $G$ . Then the following two quotient groups are isomorphic:  $HN/N \simeq H/N$ .
- Q7.** Every simple  $p$ -group  $G$  is abelian.
- Q8.** The number of elements in any conjugacy class of a finite group  $G$  divides the order of  $G$ .
- Q9.** The Klein group is a 2-group.
- Q10.** Let  $G$  be a cyclic group of order  $n$ . Then there is a subgroup of size  $d$  for each positive divisor  $d$  of  $n$ .

**Answer.**

- Q1.** False. There are only the Klein group  $C_2 \times C_2$  and the cyclic group  $C_4$ .
- Q2.** False. Indeed, you need the extra condition that  $HK = KH$  for it be true! If you try to find an inverse for  $hk$ , you will see you cannot find it. Of course, in  $G$  it should be  $k^{-1}h^{-1}$ , but without the assumption that  $HK = KH$ , this element has no reason to live in  $HK$ .
- Q3.** False. For  $B(x)$  to be a subgroup of  $G$ , then  $B(x)$  at least need to contain the identity element 1. However  $gx$  has no reason to be 1 in general, since  $x$  belongs to  $X$  which is an arbitrary set.

- Q4.** False. Remember that  $D_{10}$  has order  $2 \cdot 10 = 20$ . Now  $20 = (2^2) \cdot 5 = p^2q$  and we have seen that groups of such order cannot be simple.
- Q5.** True. One can for example check out the multiplication table for both groups.
- Q6.** False. In fact  $H/N$  is not even properly defined since  $N$  has no reason to be included in  $H$  to start with.
- Q7.** True.  $G$  is a  $p$ -group, thus its center is non-trivial (result proved in the lecture notes). The center of  $G$  is always normal in  $G$ . Now  $G$  is simple, thus its normal subgroups are only  $\{1\}$  and  $G$ . Thus either the center is  $\{1\}$  or it is  $G$ . It cannot be one since it's non-trivial, thus it is  $G$  and  $G$  is abelian.
- Q8.** True. Use the Orbit-Stabilizer theorem to deduce that the number of elements in an orbit divides the order of the group, and now notice that a conjugacy class is nothing else than an orbit when  $G$  acts on itself by conjugation.
- Q9.** True. The Klein group is of order 4, and is actually isomorphic to  $C_2 \times C_2$ . All its elements are order 2, so it is indeed a 2-group.
- Q10.** True. It is not true in general for an arbitrary group, but it is true for cyclic groups. Indeed, take  $g$  to be the generator of  $G$  of order  $n$ . Now if  $d$  divides  $n$ , then  $n = kd$  for some  $k$ . Take the subgroup generated by  $g^k$ . Clearly  $(g^k)^d = 1$  since  $g^n = 1$ . There cannot be a  $d' < d$  such that  $(g^k)^{d'} = 1$ , otherwise this would mean the order of  $G$  is  $< n$ .