



# Contents

<b>1</b>	<b>Introduction to Group Theory</b>	<b>3</b>
1.1	Definitions and Examples . . . . .	3
1.2	Subgroups . . . . .	9
1.2.1	Cosets . . . . .	11
1.3	Normal Subgroups and Quotient Groups . . . . .	13
1.4	Direct products and finite abelian groups . . . . .	17
1.4.1	Direct products . . . . .	17
1.4.2	Cyclic groups . . . . .	18
1.4.3	Finite Abelian groups . . . . .	19
1.4.4	The Jordan-Hölder decomposition . . . . .	23
1.4.5	Commutators and commutator subgroups . . . . .	26
1.4.6	Solvable groups . . . . .	27

# **Foreword**

The course *FMA\_3F003\_EP* is a continuation of the Discrete Mathematics and of the second year Algebra courses. There the basic algebraic structures (groups, rings, fields) were introduced. In this course we will go deeper into the understanding of those structures and their relationships, and we will see some geometric and arithmetical situations in which they arise.

All pictures of mathematicians in these course notes are taken from Wikipedia.

# **Chapter 1**

## **Introduction to Group Theory**

### **1.1 Definitions and Examples**

### Definition 1.1.1

A **group** is a set  $G$  endowed with a binary operation:

$$\begin{aligned} G \times G &\rightarrow G \\ (g_1, g_2) &\mapsto g_1 g_2 \end{aligned}$$

called the **group law** of  $G$  and satisfying the following conditions:

(G1) *Associativity*:

$$\forall (g_1, g_2, g_3) \in G^3, \quad (g_1 g_2) g_3 = g_1 (g_2 g_3). \quad (1.1)$$

(G2) *Identity*: there is an element  $e \in G$  such that:

$$\forall g \in G, \quad g = eg = ge. \quad (1.2)$$

The element  $e$  is called the **identity element** of  $G$  and is often denoted by  $1_G$  or simply by 1.

(G3) *Inverse*: for each  $g \in G$ , there is an element  $h \in G$  such that:

$$e = gh = hg. \quad (1.3)$$

The element  $h$  is called an **inverse** of  $g$ .

A group  $G$  is said to be **abelian** (or **commutative**) if  $gh = hg$  for all  $g, h \in G$ . In that case, the operation on  $G$  is generally denoted additively and the identity element by  $0_G$ .

**Remark 1.1.2.** Let  $G$  be a group. As we saw in the previous courses (and/or in Tutorial 1),  $G$  has a unique identity, and every  $g \in G$  has a unique inverse. We will denote the inverse of  $g \in G$  by  $g^{-1}$ . If  $G$  is an abelian group, the inverse of  $g \in G$  is often denoted by  $-g$ .

### Example 1.1.3.

- (i) The pair  $(\mathbb{Z}, +)$  is an abelian group.
- (ii) For each  $n > 0$ , the pair  $(\mathbb{Z}/n\mathbb{Z}, +)$  is an abelian group.
- (iii) For each field  $K$  (e.g.  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ), the pairs  $(K, +)$  and  $(K^\times, \times)$  are abelian groups.
- (iv) Let  $K$  be a field and  $n$  a positive integer.

1. The set of invertible  $n \times n$  matrices with coefficients in  $K$  endowed with matrix multiplication is a group, called the **general linear group** and denoted  $GL_n(K)$  or  $GL(n, K)$ . This group is not abelian for  $n \geq 2$ . More generally, if  $K$  is a field and  $V$  is any  $K$ -vector space, the set of  $K$ -linear automorphisms  $GL(V)$  of  $V$  endowed with composition is a group.
  2. The  $\{A \in GL_n(K) \mid \det(A) = 1\}$  endowed with matrix multiplication is a group called the **special linear group** and denoted either by  $SL_n(K)$  or  $SL(n, K)$ .
- (v) Given a set  $X$ , the set  $\text{Sym}(X) := \{f : X \rightarrow X \mid f \text{ is a bijection}\}$  of bijections from  $X$  to  $X$  endowed with composition is a group. It is called the **symmetric group on  $X$** .
- (v') When  $X = X_n := \{1, \dots, n\}$ , the group  $\text{Sym}(X_n)$  is denoted by  $\mathcal{S}_n$  and is called the **symmetric group** of degree  $n$  or the symmetric group on  $n$  letters. Let us recall few facts about  $\mathcal{S}_n$  that we learned in the previous courses.

An element  $\sigma \in \mathcal{S}_n$  is called a **permutation** and is often denoted by:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Given  $r$  pairwise distinct integers  $a_1, \dots, a_r$  in  $\{1, 2, \dots, n\}$ , the permutation that sends  $a_i$  to  $a_{i+1}$  for  $1 \leq i \leq r-1$ , that sends  $a_r$  to  $a_1$ , and that fixes all other elements of  $\{1, 2, \dots, n\}$  is also denoted by:

$$(a_1 \ a_2 \ \dots \ a_r)$$

and is called an  **$r$ -cycle** or a cycle of length  $r$ . Its inverse is again an  $r$ -cycle,  $(a_r \ \dots \ a_2 \ a_1)$ .

- Any permutation in  $S_n$  can be written as a product of disjoint cycles (i.e., cycles with disjoint supports) in a unique way up to the order.
- For  $n \geq 3$ , the symmetric group  $\mathcal{S}_n$  is not abelian. For instance, we have:

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

**Notation 1.1.4.** Let  $G$  be a group and  $g \in G$ . We define  $g^0 = 1_G$ . For  $n \in \mathbb{N}$ ,  $n \geq 1$ , we define inductively  $g^1 = g$  and  $g^{n+1} = g^n g$ . Also, we define  $g^{-n}$  to be the inverse of  $g^n$ .

**Definition 1.1.5**

Let  $G$  be a group. If  $G$  is finite,  $|G|$  is the number of elements of  $G$  and is called the **order** of  $G$ .

Let  $g \in G$ . The **order** of  $g$  denoted by  $|g|$  or  $o(g)$  is the least positive integer  $n$  such that  $g^n = 1_G$ , if such  $n$  exists. If there is no such  $n$ , then  $g$  has an infinite order.

**Exercise 1.1.6.** If  $g \in G$ , prove that  $o(g) = 1$  if and only if  $g = 1_G$ .

**Example 1.1.7.** (1) The group  $(\mathbb{Z}, +)$  is infinite and if  $g \in \mathbb{Z} \setminus \{0\}$ , then  $g$  has infinite order.

(2) For each  $n > 0$ , the group  $(\mathbb{Z}/n\mathbb{Z}, +)$  is finite of order  $n$ .

(3) The group  $\mathcal{S}_n$  is finite of order  $n!$ .

(4) Let  $n \geq 3$  be an integer. In the plane  $\mathbb{R}^2$ , consider a regular  $n$ -gon  $P_n$  with center  $(0, 0)$ . The set  $D_{2n}$  of isometries of  $P_n$  (under the operation of composition) forms a group called the **dihedral group** of order  $2n$ . Let us find its elements.

Observe first that the (counterclockwise) rotation  $r$  through the angle  $\frac{2\pi}{n}$  about  $(0, 0)$  is in  $D_{2n}$ . Hence we get  $n$  rotations in  $D_{2n}$ :

$$1, r, r^2, \dots, r^{n-1}$$

Let  $A$  be a fixed vertex of  $P$ , the reflection  $s$  with respect to the line passing through  $A$  and the center of  $P$  is in  $D_{2n}$ . Then  $D_{2n}$  also contains the following  $n$  symmetries:

$$s, rs, r^2s, \dots, r^{n-1}s.$$

Let's check that  $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$ .

To do so, denote by  $A_0 = A, A_1, \dots, A_{n-1}$  the vertices of  $P$  in clockwise order and fix an element  $\sigma \in D_{2n}$ . Let  $i \in \{0, \dots, n-1\}$  be such that  $\sigma(A_0) = A_i$  and set  $\tau := r^i \sigma$ . We have  $\tau(A_0) = A_0$ . Since  $\tau$  preserves distances,

$$\tau(A_1) \in \{A_1, A_{n-1}\}.$$

If  $\tau(A_1) = A_1$ , then  $\tau$  fixes both  $A_0$  and  $A_1$ : hence  $\tau = 1$  and  $\sigma = r^{-i}$ .

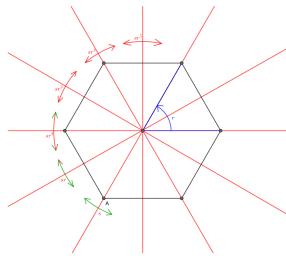
If  $\tau(A_1) = A_{n-1}$ , then  $s\tau$  fixes both  $A_0$  and  $A_1$ : hence  $s\tau = 1$  and  $\sigma = r^{-i}s$ .

Since  $o(r) = n$ , in all cases,  $\sigma \in \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$ , and hence:

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

Observe that  $r^i r^{n-i} = 1$ ,  $r^i s = sr^{n-i}$  and  $(r^i s)^2 = r^i s r^i s = r^i s s r^{n-i} = 1$ . One can conclude that  $D_{2n}$  is indeed a group of order  $2n$ . Also remark that  $o(r^i s) = 2$  and  $r^i s$  is a reflection for all  $0 \leq i < n$ .

- (4a) If  $n = 6$ ,  $P_n$  is a regular hexagon.



In this case the group  $D_{12}$  contains six rotations and six reflections.

#### Definition 1.1.8

A group  $G$  is called **cyclic** if there exists  $g \in G$  such that for every  $h \in G$ ,  $h = g^k$  for some  $k \in \mathbb{Z}$ . In this case  $g$  is called a generator of  $G$ .

**Example 1.1.9.** 1. The group  $(\mathbb{Z}, +)$  is an infinite cyclic group,  $g_1 = 1$  is a generator of  $\mathbb{Z}$ ,  $g_2 = -1$  is a generator of  $\mathbb{Z}$ .

2. For  $n \geq 1$ ,  $(\mathbb{Z}/n\mathbb{Z}, +)$  is a cyclic group of order  $n$ .

#### Definition 1.1.10

Let  $G$  and  $H$  be two groups.

A **group homomorphism** (or a **group morphism**) from  $G$  to  $H$  is a map  $f: G \rightarrow H$  such that:

$$\forall (g_1, g_2) \in G^2, f(g_1 g_2) = f(g_1) f(g_2).$$

If  $f$  is bijective, then its inverse is also a homomorphism and we say that  $f$  is an **isomorphism**. Two groups  $G$  and  $H$  are called **isomorphic** if there exists an isomorphism between them. In this case we write  $G \cong H$ .

Finally, if  $G = H$  and  $f : G \rightarrow G$  is an isomorphism, we say that  $f$  is an **automorphism** of  $G$ .

**Exercise 1.1.11.** If  $f : G \rightarrow H$  is a group homomorphism, show that  $f(1_G) = 1_H$  and for all  $g \in G$ ,  $f(g^{-1}) = f(g)^{-1}$ .

The following proposition gives a useful criterion to check whether a homomorphism is injective:

**Proposition 1.1.12**

Let  $G$  and  $H$  be two groups, and let  $f : G \rightarrow H$  be a homomorphism. Define the **kernel** of  $f$  by

$$\ker(f) := f^{-1}(\{1_H\}) = \{g \in G \mid f(g) = 1_H\}.$$

Then  $f$  is injective if, and only if,  $\ker(f) = \{1\}$ .

*Proof.* Assume that  $\ker(f) = \{1\}$  and let  $x$  and  $y$  be elements of  $G$  such that  $f(x) = f(y)$ . Then  $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1$  and so  $xy^{-1} \in \ker(f)$ . Then  $xy^{-1} = 1$  and  $x = y$ . This settles the injectivity of  $f$ . The converse follows immediately from the definition of injectivity and the fact that  $f(1) = 1$ .  $\square$

**Exercise 1.1.13.** Prove that any two infinite cyclic groups are isomorphic. Moreover, prove that if  $G$  and  $H$  are two cyclic groups with  $|G| = |H| = n$ ,  $n \geq 1$ , then  $G \cong H$ .

**Example 1.1.14.**

1. The exponential map:

$$\begin{aligned}\exp : \mathbb{C} &\rightarrow \mathbb{C}^\times \\ z &\mapsto e^z\end{aligned}$$

is a surjective group homomorphism. Its kernel is  $2\pi i\mathbb{Z}$ .

2. For  $n \geq 2$ , the signature map  $\text{sign} : \mathcal{S}_n \rightarrow \{-1, 1\}$  is a surjective group homomorphism. Its kernel is the **alternating group**  $\mathcal{A}_n$ .
3. Let  $K$  be a field and let  $n \geq 1$  be an integer. The determinant map

$$\det : GL_n(K) \rightarrow K^\times$$

is a surjective group homomorphism. Its kernel is  $SL_n(K)$ .

4. The group homomorphisms from  $\mathbb{Z}$  to  $\mathbb{Z}$  are the maps  $n \mapsto an$  for  $a \in \mathbb{Z}$ .

5. Let  $G$  be a group and let  $n \in \mathbb{Z}$  be an integer. The map:

$$\begin{aligned} G &\rightarrow G \\ g &\mapsto g^n \end{aligned}$$

is a group homomorphism if  $G$  is abelian, but not in general.

6. Let  $G$  be a group. Given  $g \in G$ , the map  $\phi_g : G \rightarrow G$  such that

$$\phi_g(h) = ghg^{-1}$$

for  $h \in G$ , is a group automorphism. Such an automorphism is called an **inner** automorphism of  $G$  (Tutorial Sheet 1).

## 1.2 Subgroups

### Definition 1.2.1

Let  $G$  be a group. A **subgroup** of  $G$  is a subset  $H$  of  $G$  such that the group law  $G \times G \rightarrow G$  restricts to a group law  $H \times H \rightarrow H$ .  
If  $H$  is a subgroup of  $G$ , we will write  $H \leq G$ .

**Remark 1.2.2.** Equivalently, a subset  $H$  of  $G$  is a subgroup of  $G$  if

$$\begin{aligned} 1_G &\in H, \\ \forall (h_1, h_2) \in H^2, \quad h_1 h_2 &\in H, \\ \forall h \in H, \quad h^{-1} &\in H. \end{aligned}$$

**Example 1.2.3.**

1. The subgroups of  $\mathbb{Z}$  are the subsets of the form  $n\mathbb{Z}$  for some  $n \in \mathbb{Z}$ .
2. The subgroups of  $\mathbb{Z}/n\mathbb{Z}$  are the subsets of form  $\{[0], [d], [2d], \dots, [n-d]\}$  with  $d$  a divisor of  $n$ .
3. If  $K$  is a field and  $n \in \mathbb{N}^*$ ,  $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ .
4. Let  $G$  and  $M$  be two groups and  $f : G \rightarrow M$  a homomorphism.  
Then  $\ker(f) \leq G$  and  $\text{im}(f) \leq M$ .

For instance, the special linear group  $SL_n(K)$  is a subgroup of  $GL_n(K)$  since it is the kernel of the determinant map, and the alternating group  $\mathcal{A}_n$  is a subgroup of  $\mathcal{S}_n$  since it is the kernel of the signature map.

5. Let  $f : G \rightarrow M$  be a group homomorphism. If  $H \leq G$ , then  $f(H) \leq M$ . Also, if  $K \leq M$ , then  $f^{-1}(K) = \{g \in G \mid f(g) \in K\}$  is a subgroup of  $G$ .
6. Let  $(G_i)_{i \in I}$  be a family of subgroups of a group  $G$ . Then the intersection of all the  $G_i$  is a subgroup of  $G$ . Note however that the union need not be a subgroup of  $G$ .

The following lemma gives us a quicker way to check whether a non-empty subset of a group is a subgroup.

**Lemma 1.2.4**

Let  $G$  be a group. If  $H$  is a non-empty subset of  $G$ , then  $H$  is a subgroup of  $G$  iff for all  $a, b \in H$ ,  $ab \in H$  and  $a^{-1} \in H$ .

**Proposition 1.2.5**

Let  $G$  be a group and let  $A$  be a subset of  $G$ . There exists a smallest subgroup  $H$  of  $G$  containing  $A$ . It is called the **subgroup generated by  $A$**  and it is usually denoted by  $\langle A \rangle$ .

*Proof.* Let  $H$  be the intersection of all subgroups of  $G$  containing  $A$ . It is a subgroup of  $G$  containing  $A$  and every other subgroup of  $G$  containing  $A$  contains  $H$ . Hence it is the smallest subgroup of  $G$  containing  $A$ .  $\square$

**Remark 1.2.6.** More explicitly, if  $A \neq \emptyset$ , the subgroup  $\langle A \rangle$  can be described as the set  $S$  of elements of  $G$  that can be written as  $g_1^{\epsilon_1} \dots g_r^{\epsilon_r}$  for some  $r \in \mathbb{N}$ , some  $\epsilon_1, \dots, \epsilon_r \in \{-1, 1\}$  and some  $g_1, \dots, g_r \in A$ . If  $A = \emptyset$ ,  $\langle A \rangle = \{1_G\}$ .

**Example 1.2.7.**

1. If  $G$  is a cyclic group and  $g$  is a generator of  $G$ , then  $G = \langle g \rangle$ .
2. Let  $a_1, \dots, a_r$  be  $r$  integers. The subgroup of  $\mathbb{Z}$  generated by  $a_1, \dots, a_r$  is:

$$a_1\mathbb{Z} + \dots + a_r\mathbb{Z} = \gcd(a_1, \dots, a_r)\mathbb{Z}.$$

3. The group  $\mathcal{S}_3$  is generated by the elements:

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

Indeed, one can easily check that  $\mathcal{S}_3 = \{\text{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ . More generally, the following sets generate the symmetric group  $\mathcal{S}_n$ :

- the set of all transpositions;
- the set  $\{(1\ 2), (2\ 3), \dots, ((n-1)\ n)\}$ .
- the transposition  $(1\ 2)$  and the cycle  $(1\ 2 \dots n)$ .

The alternating group  $\mathcal{A}_n$  is generated by the set of 3-cycles. See Tutorial Sheet 2 for more details.

4. The dihedral group  $D_{2n}$  is generated by the rotation  $r$  and a reflection  $s$ . These two generators satisfy the relations  $r^n = s^2 = 1$  and  $srs^{-1} = r^{-1}$ .
5. Consider the following complex matrices:

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Observe that:

$$A^4 = I_2, \quad A^2 = B^2, \quad BA = A^3B.$$

The subgroup of  $GL_2(\mathbb{C})$  generated by  $A$  and  $B$  is:

$$\{I_2, A, A^2, A^3, B, AB, A^2B, A^3B\}.$$

It is called the **quaternion group** and will be denoted by  $Q_8$ . It can also be described as the 8-element group  $\{\pm 1, \pm i, \pm j, \pm k\}$  subject to the following relations:

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

### 1.2.1 Cosets

Let  $G$  be a group and  $H$  a subgroup of  $G$ . Define a relation  $\mathcal{R}$  on  $G$  by:

$$x \mathcal{R} y \Leftrightarrow x^{-1}y \in H.$$

We have checked in class that this is an equivalence relation and that given  $x \in G$ , the equivalence class of  $x$  is the set

$$xH = \{xh | h \in H\},$$

which is called a **left coset** of  $H$  in  $G$ . The set of all left cosets of  $H$  in  $G$  is usually denoted by  $G/H$ . The number of distinct left cosets is denoted by  $|G : H|$  and is called the **index** of  $H$  in  $G$ .

**Remark 1.2.8.** One can also define an equivalence relation:

$$x\mathcal{R}'y \Leftrightarrow xy^{-1} \in H.$$

In this case, the equivalence class of an element  $x \in G$  for  $\mathcal{R}'$  is

$$Hx = \{hx \mid h \in H\}$$

called a **right coset** of  $H$  in  $G$ . The set of all right cosets of  $H$  in  $G$  is usually denoted by  $H\backslash G$ .

One can define a bijection between  $G/H$  and  $H\backslash G$  by:

$$\begin{aligned} G/H &\rightarrow H\backslash G \\ xH &\mapsto Hx^{-1}. \end{aligned}$$

**Exercise 1.2.9.** Check that this is indeed a bijection.

**Theorem 1.2.10 – Lagrange's theorem**

Let  $G$  be a finite group and let  $H$  be any subgroup of  $G$ . Then:

$$|G| = |H| \cdot |G : H|.$$

*Proof.* The left cosets form a partition of  $G$ , so that:

$$|G| = \sum_{Y \in G/H} |Y|.$$

But, for each  $x \in G$ , there is a bijection:

$$\begin{aligned} H &\rightarrow xH \\ h &\mapsto xh, \end{aligned}$$

and hence each left coset has  $|H|$  elements. We deduce that:

$$|G| = \sum_{Y \in G/H} |H| = |G : H| \cdot |H|.$$

□



*Joseph-Louis Lagrange (Turin 1736 - Paris 1813)*

**Corollary 1.2.11**

Let  $G$  be a finite group and let  $x \in G$ . The order of  $x$  divides  $|G|$ .

*Proof.* Apply Lagrange's theorem to  $H = \langle x \rangle$ . □

### 1.3 Normal Subgroups and Quotient Groups

**Definition 1.3.1**

Let  $G$  be a group and let  $N$  be a subgroup of  $G$ . Then  $N$  is called a **normal** subgroup of  $G$  if for all  $g \in G$ ,

$$gN = Ng$$

If  $N$  is a normal subgroup of  $G$ , we will write either  $N \triangleleft G$  or  $N \trianglelefteq G$ .

**Example 1.3.2.** 1. If  $G$  is a group, the subgroups  $\{1_G\}$  and  $G$  are both normal subgroups of  $G$ .

2. If  $G$  is an abelian group and  $N$  is a subgroup of  $G$ , then  $N \trianglelefteq G$ .
3. Let  $G = S_3$ . Then  $N = \{1, (1, 2, 3), (3, 2, 1)\} \triangleleft G$ , while subgroup  $H = \{1, (1, 2)\}$  is not normal in  $G$ .

In fact, there is a different way to decide whether a given subgroup is normal or not.

**Proposition 1.3.3**

Let  $G$  be a group and  $N$  a subgroup of  $G$ . Then  $N$  is a normal subgroup of  $G$  if and only if for all  $g \in G$  and  $n \in N$ ,  $gng^{-1} \in N$ .

*Proof.* Let  $N$  be a normal subgroup of  $G$ . Take any  $g \in G$  and  $n \in N$ . Then  $gN = Ng$ , and so  $gn \in gN = Ng$ . Thus there exists  $n' \in N$  such that  $gn = n'g$ , and so  $gng^{-1} = n' \in N$ .

Assume now that  $gng^{-1} \in N$  for all  $g \in G$  and  $n \in N$ . Then for any  $gn \in gN$ , as  $gng^{-1} \in N$ , there exists  $n_1 \in N$  with  $gng^{-1} = n_1$ . Hence,  $gn = n_1g \in Ng$ , and so  $gN \subseteq Ng$ . Now,  $g^{-1}ng \in N$  and so there exists  $n_2 \in N$  such that  $g^{-1}ng = n_2$ . Hence,  $ng = gn_2 \in gN$ , and so  $Ng \subseteq gN$ . Thus  $gN \subseteq Ng$  and  $Ng \subseteq gN$ , and so  $gN = Ng$ .  $\square$

**Example 1.3.4.** 1. For  $n \in \mathbb{N}$ ,  $n \geq 1$ ,  $A_n \trianglelefteq S_n$ .

2. Let  $n \in \mathbb{N}$ ,  $n \geq 1$ . Then  $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$ .

These examples can be generalised in the following way.

**Lemma 1.3.5**

Let  $f : G \rightarrow M$  be a group homomorphism. Then  $\ker(f) \trianglelefteq G$ .

*Proof.* Let  $f : G \rightarrow M$  be a group homomorphism. We have seen last time that a kernel of a homomorphism is a subgroup of  $G$ . Now take any  $g \in G$  and any  $k \in \ker(f)$  and consider  $gkg^{-1}$ . Since  $f(k) = 1$ , we have

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(k)f(g)^{-1} = f(g)1_M f(g)^{-1} = 1_M,$$

and so  $gkg^{-1} \in \ker(f)$ . Using Proposition 1.3.3, we obtain that  $\ker(f) \trianglelefteq G$ .  $\square$

**Notation 1.3.6.** Let  $G$  be a group and  $A \subseteq G$  and  $B \subseteq G$ . Then

$$AB := \{ab \mid a \in A, b \in B\}$$

**Lemma 1.3.7**

Let  $G$  be a group and  $N$  a normal subgroup of  $G$ . Then for  $x, y \in G$ ,

$$(Nx)(Ny) = N(xy)$$

*Proof.* Take any  $x, y \in G$  and  $n, n_1, n_2 \in N$ . Then  $(n_1x)(n_2y) = n_1(xn_2)y$ . Now  $xn_2 \in xN = Nx$  (as  $N \triangleleft G$ ), and so there exists  $n'_2 \in N$  such that  $xn_2 = n'_2x$ . Therefore  $n_1(xn_2)y = n_1(n'_2x)y = (n_1n'_2)(xy)$ . We conclude that  $(Nx)(Ny) \subseteq N(xy)$ .

Now  $n(xy) = (nx)(1_Gy) \in (Nx)(Ny)$ , and so  $N(xy) \subseteq (Nx)(Ny)$ .

We may now conclude that  $(Nx)(Ny) = N(xy)$ .  $\square$

**Remark 1.3.8.** Observe that in the proof Lemma 1.3.7, we used the fact that  $N$  was a normal subgroup of  $G$ . Can you think of an example of a group and a subgroup for which Lemma 1.3.7 does not hold?

**Theorem 1.3.9**

Let  $G$  be a group and let  $N$  be a normal subgroup of  $G$ . Then the set of cosets of  $N$  in  $G$  forms a group under the operation of multiplication of cosets. We denote this group by  $G/N$  and call it the **quotient group** of  $G$  by  $N$ .

*Proof.* As we in Lemma 1.3.7, the set  $G/N$  of cosets of  $N$  in  $G$  is indeed closed under the operation of multiplication of cosets. Now it is easy to check that this operation is associative (check!). Also, as  $N = N1_G$ , for all  $x \in G$ , we have

$$(N1_G)(Nx) = N(1_Gx) = Nx = N(x1_G) = (Nx)(N1_G)$$

and

$$(Nx)(Nx^{-1}) = N(xx^{-1}) = N = N(x^{-1}x) = (Nx^{-1})(Nx).$$

Therefore,  $G/N$  is a group under multiplication of cosets with

$$1_{G/N} = N \text{ and } (Nx)^{-1} = Nx^{-1}.$$

$\square$

**Remark 1.3.10.** If  $G$  is a finite group and  $N \triangleleft G$ , Lagrange's Theorem implies that that  $|G/N| = |G : N| = \frac{|G|}{|N|}$ .

### Theorem 1.3.11 – First Isomorphism Theorem

Let  $f : G \rightarrow M$  be a group homomorphism with kernel  $\ker(f) := K$ . Then  $K \trianglelefteq G$  and

$$G/K \cong \text{Im}(f)$$

More precisely, there is an isomorphism  $\bar{f} : G/K \rightarrow \text{Im}(f)$  defined by  $\bar{f}(Kg) = f(g)$  for all  $g \in G$ .

*Proof.* Let us first show that  $\bar{f}$  is well-defined. Take any  $x, y \in G$  with  $Kx = Ky$ . Then  $\bar{f}(Kx) = f(x)$  and  $\bar{f}(Ky) = f(y)$ . Since  $Kx = Ky$ ,  $x = ky$  for some  $k \in K$ . Hence,  $f(x) = f(ky) = f(k)f(y) = 1_M f(y) = f(y)$  and so, indeed,  $\bar{f}(Kx) = \bar{f}(Ky)$ . Now

$$\bar{f}((Kx)(Ky)) = \bar{f}(K(xy)) = f(xy) = f(x)f(y) = \bar{f}(Kx)\bar{f}(Ky)$$

for all  $Kx, Ky \in G/K$ , and so  $\bar{f}$  is a homomorphism. Since  $\text{Im}(\bar{f}) = \text{Im}(f)$ ,  $\bar{f}$  is surjective, and as  $\ker(\bar{f}) = \{Kx \mid f(x) = 1_M\} = \{Kx \mid x \in K\} = \{1_{G/K}\}$ ,  $\bar{f}$  is injective. Thus  $\bar{f}$  is an isomorphism.  $\square$

### Lemma 1.3.12

Let  $G$  be a group and  $N$  a normal subgroup of  $G$ . Then the map

$$\pi : G \rightarrow G/N$$

defined by  $\pi(g) = Ng$  is a surjective homomorphism with kernel  $N$ . This map is called the **natural homomorphism** from  $G$  to  $G/N$ .

*Proof.* Take any  $x, y \in G$ . Then  $\pi(xy) = N(xy) = (Nx)(Ny) = \pi(x)\pi(y)$  and so  $\pi$  is a homomorphism. Finally,

$$\ker(\pi) = \{g \in G \mid \pi(g) = 1_{G/N}\} = \{g \in G \mid Ng = N\} = N.$$

$\square$

### Theorem 1.3.13 – Second Isomorphism Theorem

Let  $G$  be a group,  $N \trianglelefteq G$  and  $H \leq G$ . Then the following conditions hold:

1.  $NH \leq G$ ,
2.  $N \cap H \trianglelefteq H$ , and

3.  $NH/N \cong H/(N \cap H)$ .

*Proof.* As  $N \subseteq NH$ ,  $NH \neq \emptyset$ . Take any  $n_1 h_1, n_2 h_2 \in NH$ . Then

$$(n_1 h_1)(n_2 h_2) \in Nh_1 Nh_2 = N(h_1 h_2) \subseteq NH$$

and

$$(n_1 h_1)^{-1} = h_1^{-1} n_1^{-1} = (h_1^{-1} n_1^{-1} h_1) h_1^{-1} \in Nh_1^{-1} \subseteq NH$$

proving that  $NH \leq G$ .

Take the natural map  $\pi : G \rightarrow G/N$ , and consider its restriction to  $H$ :

$$\pi_H : H \rightarrow G/N.$$

Then  $\pi_H$  is a homomorphism,  $Im(\pi_H) = \{Nh \mid h \in H\} = NH/N$ . Finally,

$$\ker(\pi_H) = \ker(\pi) \cap H = N \cap H.$$

Therefore, by the First Isomorphism Theorem,  $N \cap H \trianglelefteq H$  and  $H/(N \cap H) \cong NH/H$ .  $\square$

## 1.4 Direct products and finite abelian groups

### 1.4.1 Direct products

Let  $G_1$  and  $G_2$  be two groups. Consider the set

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_i \in G_i\}$$

and let us define an operation on this set by

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \text{ for all } a_1, b_1 \in G_1 \text{ and } a_2, b_2 \in G_2.$$

It is easy to see that this operation is associative (check!). Moreover, for all  $(g_1, g_2) \in G_1 \times G_2$ ,  $(1_{G_1}, 1_{G_2})(g_1, g_2) = (g_1, g_2)$  and  $(g_1^{-1}, g_2^{-1})(g_1, g_2) = (1_{G_1}, 1_{G_2})$ . Hence, by Question 1 of Tutorial 1,  $G_1 \times G_2$  together with the operation defined above is a group. This group is called the *direct product* of  $G_1$  and  $G_2$ .

**Remark 1.4.1.** Let  $G_1$  and  $G_2$  be two groups. It is easy to check that the following hold:

1. The group  $G_1 \times G_2$  is abelian if and only if  $G_1$  is abelian and  $G_2$  is abelian.

2. The group  $G_1 \times G_2$  is finite if and only if  $G_1$  is finite and  $G_2$  is finite.
3. If  $G_1 \times G_2$  is finite, then  $|G_1 \times G_2| = |G_1| \cdot |G_2|$ .
4. Finally, if  $n \in \mathbb{N}$  with  $n \geq 2$ , and  $G_1, \dots, G_n$  are  $n$  groups, we can define a direct product of  $G_1, G_2, \dots, G_n$ .  
If  $G_1 = G_2 = \dots = G_n = G$ , we will denote the direct product of  $G_1, \dots, G_n$  by  $G^n$ .

**Lemma 1.4.2**

Let  $G$  be a group,  $N \trianglelefteq G$  and  $K \trianglelefteq G$ . Suppose further that  $NK = G$  and  $N \cap K = \{1\}$ . Then  $G \cong N \times K$ .

*Proof.* Consider a map  $\phi : N \times K \rightarrow G$  defined by  $\phi((n, k)) = nk$  for  $(n, k) \in N \times K$ . Take any two elements  $(n_1, k_1), (n_2, k_2) \in N \times K$ . Then

$$\begin{aligned}\phi((n_1, k_1)(n_2, k_2)) &= \phi((n_1 n_2, k_1 k_2)) = n_1 n_2 k_1 k_2 = \\ &= n_1 n_2 k_1 (n_2^{-1} k_1^{-1} k_1 n_2) k_2 = n_1 (n_2 k_1 n_2^{-1} k_1^{-1}) k_1 n_2 k_2\end{aligned}$$

Now  $n_2 k_1 n_2^{-1} k_1^{-1} = (n_2 k_1 n_2^{-1}) k_1^{-1} \in K$  as  $k_1 \in K$  and  $K \trianglelefteq G$ .

Similarly,  $n_2 k_1 n_2^{-1} k_1^{-1} = n_2 (k_1 n_2^{-1} k_1^{-1}) \in N$  as  $n_2 \in N$  and  $N \trianglelefteq G$ , and so  $n_2 k_1 n_2^{-1} k_1^{-1} \in N \cap K = \{1_G\}$ . Therefore

$$\phi((n_1, k_1)(n_2, k_2)) = n_1 (n_2 k_1 n_2^{-1} k_1^{-1}) k_1 n_2 k_2 = n_1 k_1 n_2 k_2 = \phi((n_1, k_1)) \phi((n_2, k_2)),$$

and so  $\phi$  is a homomorphism.

Clearly,  $\phi$  is surjective as  $G = NK$ . Finally, if  $\phi((n_1, k_1)) = \phi((n_2, k_2))$  for some  $(n_1, k_1), (n_2, k_2) \in N \times K$ , then  $n_1 k_1 = n_2 k_2$ , and so  $n_2^{-1} n_1 = k_2 k_1^{-1} \in N \cap K = \{1_G\}$ . Thus  $n_1 = n_2$ ,  $k_1 = k_2$ , and  $\phi$  is injective. The result now follows.  $\square$

### 1.4.2 Cyclic groups

Recall that we proved (see Tutorial 2) that any two infinite cyclic groups are isomorphic. In particular, every infinite cyclic group is isomorphic to  $(\mathbb{Z}, +)$ . We also proved that any two finite cyclic groups of the same order are isomorphic. In particular, every cyclic group of order  $n$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z}, +)$ . Let us now look at some properties of cyclic groups.

**Notation 1.4.3.** We will denote a cyclic group of order  $n$  by  $C_n$ .

**Lemma 1.4.4**

Every subgroup of a cyclic group is cyclic.

*Proof.* Let  $G$  be a cyclic group with generator  $g$ . Let  $H \leq G$ . If  $H = \{1\}$ ,  $H$  is obviously cyclic. Let  $H$  be a non-trivial subgroup of  $G$  and let  $m$  be the smallest positive integer such that  $g^m \in H$ . Take any  $1 \neq h \in H$ . Since  $G$  is generated by  $g$ , there exists  $a \in \mathbb{Z}$  such that  $h = g^a$ . But then there exist  $q, r \in \mathbb{Z}$  such that  $a = mq + r$  and  $0 \leq r \leq m - 1$ . Hence,

$$h = g^a = g^{mq+r} = (g^m)^q g^r$$

As  $h \in H$  and  $g^m \in H$ ,  $(g^m)^q \in H$  and so  $(g^m)^{-1}h = g^r \in H$ . But  $0 \leq r \leq m - 1$ , and so  $r = 0$  because of our choice of  $m$ . Therefore  $m$  divides  $a$ , and so  $h = g^{mq}$  and  $H = \langle g^m \rangle$ .  $\square$

**Lemma 1.4.5**

Let  $n \in \mathbb{N}$ ,  $n \geq 1$ , and let  $G$  be a cyclic group of order  $n$ . Then there exists a unique subgroup of  $G$  of order  $d$  for every divisor  $d$  of  $n$ .

### 1.4.3 Finite Abelian groups

**Lemma 1.4.6**

Let  $m, n \in \mathbb{N}^*$ . Then  $m$  and  $n$  are co-prime if and only if  $C_{nm} \cong C_n \times C_m$ .

*Proof.* Suppose  $\gcd(m, n) = 1$ . Let  $G$  be a cyclic group of order  $mn$  and let  $g$  be a generator of  $G$ . Consider subgroups  $N := \langle g^n \rangle$  and  $M := \langle g^m \rangle$  of  $G$ . By Lemma 1.4.4,  $N \cong C_n$  and  $M \cong C_m$ . Since  $G$  is abelian,  $N \trianglelefteq G$  and  $M \trianglelefteq G$ . By the Second Isomorphism Theorem,  $NM \leq G$ . Hence,  $N \leq NM$  and  $M \leq NM$ , and so, by Lagrange's Theorem,  $n \mid |NM|$  and  $m \mid |NM|$ . Since  $\gcd(m, n) = 1$ ,  $nm \leq |NM|$ , and so  $nm \leq |NM| \leq |G| = nm$ . Thus  $G = NM$ . Again using Lagrange's Theorem, we obtain that  $N \cap M = \{1_G\}$  (for  $N \cap M \leq N$  and  $N \cap M \leq M$ ). By Lemma 1.4.2, we conclude that  $G \cong C_n \times C_m$ .

For the rest of the proof, see Tutorial 3.  $\square$

### Theorem 1.4.7 – Classification of finite abelian groups

Any finite abelian group  $G$  can be written as:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$$

for some  $n_1, \dots, n_k > 1$ . Moreover:

- (i) the integers  $n_1, \dots, n_k$  can be chosen to be powers of prime numbers, and then they are uniquely determined by  $G$  up to permutation.

Alternatively:

- (ii) the integers  $n_1, \dots, n_k$  can be chosen so that  $n_k|n_{k-1}| \dots |n_1$ , and then they are uniquely determined by  $G$ .



Leopold Kronecker (Liegnitz 1823 - Berlin 1891)

We proceed in four steps:

**Step 1:** Let  $G$  be an abelian group and let  $g_1, \dots, g_k$  be generators of  $G$ . Let  $n_1, \dots, n_k$  be non-negative integers such that  $\gcd(n_1, \dots, n_k) = 1$ . Then one can

find generators  $h_1, \dots, h_k$  of  $G$  with  $h_1 = n_1 g_1 + \dots + n_k g_k$ .

*Proof.* We proceed by induction on  $s := n_1 + \dots + n_k$ . If  $s = 1$ , there is nothing to prove. Assume now that  $s > 1$ . Without loss of generality, we can assume that  $n_1 \geq n_2 \geq \dots \geq n_k$ , so that  $n_2 > 0$ . Observe that:

$$\begin{cases} G = \langle g_1, g_1 + g_2, g_3, \dots, g_k \rangle, \\ \gcd(n_1 - n_2, n_2, \dots, n_k) = 1, \\ (n_1 - n_2) + n_2 + \dots + n_k = s - n_2 < s. \end{cases}$$

Hence, by the inductive assumption, we can find generators  $h_1, \dots, h_k$  of  $G$  with:

$$h_1 = (n_1 - n_2)g_1 + n_2(g_1 + g_2) + n_3g_3 + \dots + n_kg_k = n_1g_1 + \dots + n_kg_k.$$

□

**Step 2:** Any finite abelian group is a direct product of cyclic groups.

*Proof.* Let  $G$  be an abelian group and let  $k$  be the minimal number of generators of  $G$ . We proceed by induction on  $k$ . For  $k = 1$ , the group  $G$  is cyclic and therefore there is nothing to prove. Now assume that  $k \geq 2$  and consider the set  $\mathcal{E}$  of  $k$ -tuples  $(g_1, \dots, g_k) \in G$  such that:

$$\begin{cases} G = \langle g_1, \dots, g_k \rangle, \\ \text{ord}(g_1) \leq \dots \leq \text{ord}(g_k) \end{cases}.$$

Fix an element  $(g_1, \dots, g_k)$  of  $\mathcal{E}$  for which  $\text{ord}(g_1)$  is minimal. By the inductive assumption, we know that  $\langle g_2, \dots, g_k \rangle$  is a product of cyclic groups. Hence it is enough to prove that:

$$G = \langle g_1 \rangle \times \langle g_2, \dots, g_k \rangle.$$

To do so, we proceed by contradiction and assume that the previous equality is not true. We can therefore find integers  $m_1, \dots, m_k$  such that:

$$m_1g_1 = m_2g_2 + \dots + m_kg_k \neq 0.$$

We may and do assume that  $0 < m_1 < \text{ord}(g_1)$  and that  $m_i < 0$  for  $i \geq 2$ . Set  $d := \gcd(m_1, \dots, m_k)$ . By step 1, we can find  $h_1, \dots, h_k \in G$  such that  $G = \langle h_1, \dots, h_k \rangle$  and

$$h_1 = \frac{m_1}{d}g_1 - \frac{m_2}{d}g_2 - \dots - \frac{m_k}{d}g_k.$$

But then  $dh_1 = 0$  and hence  $\text{ord}(h_1) < \text{ord}(g_1)$ . This contradicts the minimality of  $\text{ord}(g_1)$ . □

**Step 3:** *Proof of (i).*

*Proof.* By the second step,  $G$  can be written as:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$$

for some  $n_1, \dots, n_k > 1$ . By Lemma 1.4.3, for any  $n > 1$ , we have:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z},$$

where  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  is the prime decomposition of  $n$ . This proves that  $n_1, \dots, n_k$  can be chosen to be powers of prime numbers. In other words,  $G$  can be written as:

$$G \cong \prod_p \prod_{i=1}^{\infty} (\mathbb{Z}/p^i\mathbb{Z})^{\beta_{p,i}},$$

where  $p$  runs through the set of prime numbers and each  $\beta_{p,i}$  is a non-negative integer. We then have, for each  $p$  and each  $i$ :

$$\beta_{p,i} = \dim_{\mathbb{F}_p}(p^i G / p^{i+1} G) - \dim_{\mathbb{F}_p}(p^{i-1} G / p^i G).$$

Hence  $n_1, \dots, n_k$  are uniquely determined by  $G$  up to permutation.  $\square$

**Step 4:** *Proof of (ii).*

*Proof.* By step 3, we can write:

$$G \cong \prod_{p \in \mathcal{P}} \prod_{j=1}^{+\infty} \mathbb{Z}/p^{\alpha_j^{(p)}}\mathbb{Z},$$

where  $\mathcal{P}$  is a finite set of prime numbers and for each  $p \in \mathcal{P}$ , the sequence  $(\alpha_j^{(p)})_{j \in \mathbb{N}}$  is a non-increasing sequence of non-negative integers that stabilizes to 0. Let  $k$  be the largest integer such that not all the  $\alpha_k^{(p)}$  are 0. By the Chinese remainder theorem, we then have:

$$G \cong \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$$

with  $n_i = \prod_{p \in \mathcal{P}} p^{\alpha_i^{(p)}}$  for each  $i$ . By construction,  $n_k | n_{k-1} | \dots | n_1$ . For the uniqueness, let  $\mathbb{P}$  be the set of all prime numbers and observe that:

$$k = \max\{\dim_{\mathbb{F}_p} G / pG | p \in \mathbb{P}\}.$$

The integer  $k$  is therefore uniquely determined by  $G$ . We denote it by  $k(G)$ . Now, for each positive integer  $n$ , we have:

$$nG \cong \prod_{i=1}^k \mathbb{Z}/(n_i \gcd(n_i, n)^{-1})\mathbb{Z}.$$

Hence, for each  $i \in \{1, \dots, k\}$ , we have  $n_i = \min\{n | k(nG) = i - 1\}$  and  $n_i$  is completely determined by  $G$ .  $\square$

#### 1.4.4 The Jordan-Hölder decomposition

##### Definition 1.4.8

We say that a group  $G$  is **simple** if it is not trivial and its only normal subgroups are  $\{1\}$  and  $G$ .

**Example 1.4.9.** Let  $p$  be a prime. A cyclic group of order  $p$  is simple.

##### Lemma 1.4.10

An abelian group is simple if, and only if, it is a cyclic group of prime order.

*Proof.* If  $G$  is a cyclic group of prime order, it is abelian and simple (see example above).

Assume that  $G$  is abelian and simple. If  $G$  is non-cyclic, for any  $g \in G \setminus \{1\}$ ,  $G \neq \langle g \rangle$ , and, as  $G$  is abelian,  $\langle g \rangle \triangleleft G$ , contradicting the simplicity of  $G$ . Thus  $G$  is cyclic.

If  $G$  is infinite,  $G \cong \mathbb{Z}$ . Since  $2\mathbb{Z}$  is a proper subgroup of  $G$  and  $G$  is abelian,  $G$  has a proper non-trivial normal subgroup, contradicting the simplicity of  $G$ .

Hence,  $G$  is a finite cyclic group. Let  $n = |G|$ . If  $n$  is not prime, take a non-trivial proper divisor  $d$  of  $n$ . By Lemmas 1.4.5,  $G$  has a non-trivial subgroup of order  $d$ . Since  $G$  is abelian, this subgroup is normal, a contradiction. The result now follows.  $\square$

##### Definition 1.4.11

(i) A **composition series** of a group  $G$  is a (finite) series of subgroups

$$G = G_0 \supset G_1 \supset \dots \supset G_r = \{1_G\}$$

such that for each  $i \in \{1, \dots, r\}$ ,  $G_i \trianglelefteq G_{i-1}$  and the quotient  $G_{i-1}/G_i$

is simple.

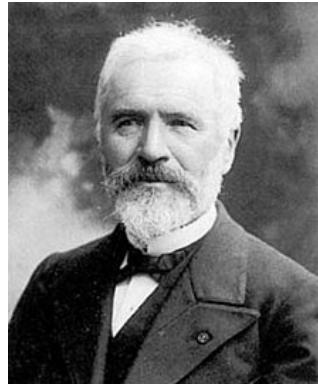
- (ii) Two composition series  $G = G_0 \supset G_1 \supset \dots \supset G_r = \{1_G\}$  and  $G = \tilde{G}_0 \supset \tilde{G}_1 \supset \dots \supset \tilde{G}_s = \{1_G\}$  are **equivalent** if  $r = s$  and there exists a permutation  $\sigma \in \mathcal{S}_r$  such that  $G_{i-1}/G_i \cong \tilde{G}_{\sigma(i)-1}/\tilde{G}_{\sigma(i)}$ .

**Example 1.4.12.** 1. If  $G = S_3$ , take  $G_1 = A_3$ . Then  $G > G_1 \{1_G\}$  is a composition series of  $G$ .

2. If  $G = \langle g \rangle \cong C_6$ , then  $G_1 := \langle g^2 \rangle \cong C_3$  and  $\tilde{G}_1 := \langle g^3 \rangle \cong C_2$ . Then  $G > G_1 > \{1_G\}$  is a composition series of  $G$  and  $G > \tilde{G}_1 > \{1_G\}$  is a composition series of  $G$ .

### Theorem 1.4.13 – Jordan-Hölder decomposition

Every finite group has a composition series, which is unique up to equivalence.



Camille Jordan  
(Lyon 1838 - Paris 1922)



Otto Hölder  
(Stuttgart 1859 - Leipzig 1937)

*Proof of existence in theorem 1.4.13.* Let  $G$  be a finite group. Let us prove that  $G$  has a composition series by induction on the order of  $G$ . If  $G$  is simple, then  $G \supset \{1_G\}$  is a composition series of  $G$ . Otherwise, we can find a maximal normal proper subgroup  $G_1$  of  $G$ . By the inductive assumption, the group  $G_1$  has a composition series. Hence it suffices to check that the quotient  $G/G_1$  is simple. To do so, denote by  $\pi : G \rightarrow G/G_1$  the natural projection and let  $H$  be a normal subgroup of  $G/G_1$ . The pre-image  $\pi^{-1}(H)$  is then a normal subgroup of  $G$  that contains  $G_1$  (see Tutorial 3). By maximality of  $G_1$ , we deduce that  $\pi^{-1}(H) = G$  or  $\pi^{-1}(H) = G_1$ . Hence either  $H = G/G_1$  or  $H$  is trivial, as wished.  $\square$

**Lemma 1.4.14**

Let  $G$  be a group and let  $H$  and  $K$  be distinct normal subgroups of  $G$  such that  $G/H$  and  $G/K$  are simple. Then  $H \cap K$  is normal in  $H$  and there is an isomorphism:

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

*Proof.* The normality of  $H \cap K$  in  $H$  is straightforward. By composing the inclusion  $H \subseteq G$  with the projection  $G \rightarrow G/K$ , we get a morphism:

$$H \rightarrow G/K.$$

whose kernel is  $H \cap K$ . We can therefore see  $H/(H \cap K)$  as a subgroup of  $G/K$ . It is moreover a normal subgroup since  $H$  is normal in  $G$ . Hence, by simplicity of  $G/K$ , we get that  $H/(H \cap K) = G/K$  or  $H/(H \cap K) = \{1\}$ .

Assume that  $H/(H \cap K) = \{1\}$ . Then  $H \subseteq K$  and  $K/H$  is a normal subgroup of the simple group  $G/H$ . This implies that  $K = H$  or  $K = G$ : contradiction! Hence  $H/(H \cap K) \neq \{1\}$ , and the only remaining possibility is that  $H/(H \cap K) = G/K$ .  $\square$

*Proof of uniqueness in theorem 1.4.13.* Let  $G$  be a finite group. Let's prove the uniqueness of its composition series. To do so, let  $r(G)$  be the minimal length of a composition series of  $G$ , and let's proceed by induction on  $r(G)$ . If  $r(G) = 1$ , then  $G$  is simple and hence there is nothing to prove.

Now assume that  $r(G) \geq 2$  and consider two composition series:

$$\begin{aligned} G &= H_0 \triangleright H_1 \triangleright \dots \triangleright H_{r(G)} = 1, \\ G &= K_0 \triangleright K_1 \triangleright \dots \triangleright K_s = 1, \end{aligned}$$

with  $s \geq r(G)$ . We want to check that these two composition series are equivalent.

*First case.* Assume that  $H_1 = K_1$ . Then the sequences  $(H_i)_{i \geq 1}$  and  $(K_i)_{i \geq 1}$  are both composition series of  $H_1$  and hence, by the inductive assumption, they are equivalent. We deduce that the composition series  $(H_i)_{i \geq 0}$  and  $(K_i)_{i \geq 0}$  of  $G$  are also equivalent.

*Second case.* Assume now that  $H_1 \neq K_1$  and consider a composition series of  $H_1 \cap K_1$ :

$$H_1 \cap K_1 = L_2 \triangleright L_3 \triangleright \dots \triangleright L_t = 1.$$

By lemma 1.4.14, we have two isomorphisms:

$$H_1/(H_1 \cap K_1) \cong G/K_1 \quad \text{and} \quad K_1/(H_1 \cap K_1) \cong G/H_1. \quad (1.4)$$

In particular, the quotients  $H_1/(H_1 \cap K_1)$  and  $K_1/(H_1 \cap K_1)$  are simple, so that the four sequences:

$$G \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_{r(G)} = 1, \quad (1.5)$$

$$G \triangleright H_1 \triangleright H_1 \cap K_1 = L_2 \triangleright L_3 \triangleright \dots \triangleright L_t, \quad (1.6)$$

$$G \triangleright K_1 \triangleright H_1 \cap K_1 = L_2 \triangleright L_3 \triangleright \dots \triangleright L_t, \quad (1.7)$$

$$G \triangleright K_1 \triangleright K_2 \triangleright \dots \triangleright K_s = 1, \quad (1.8)$$

are all composition series of  $G$ . By the first case, the composition series (1.5) and (1.6) are equivalent, as well as (1.8) and (1.7). Moreover, the isomorphisms (1.4) show that (1.6) and (1.7) are also equivalent. Hence (1.5) and (1.8) are equivalent.  $\square$

#### Definition 1.4.15

Let  $G$  be a finite group with a composition series:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_r = \{1\}$$

Then  $r$  is called the *length* of the composition series, and the quotients  $G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$  are called the **composition factors** of  $G$ .

#### 1.4.5 Commutators and commutator subgroups

##### Definition 1.4.16

Let  $G$  be a group. For  $x \in G$  and  $y \in G$ , the **commutator** of  $x$  and  $y$  is the element  $[x, y] = xyx^{-1}y^{-1}$ .

The **derived subgroup** of  $G$  (or the **commutator subgroup** of  $G$ ) is the subgroup  $[G, G]$  generated by the set of all commutators of  $G$ , i.e.,

$$[G, G] = \langle \{[x, y] \mid x, y \in G\} \rangle$$

**Example 1.4.17.** 1. If  $G$  is a group and  $x, y \in G$ , then  $[x, y] = 1$  iff  $xy = yx$ .

2. A group  $G$  is abelian iff  $[G, G] = \{1\}$ .

3. If  $G = A_n$ ,  $n \geq 5$ ,  $[(1, 2, 4), (1, 3, 5)] = (1, 2, 3)$ .

**Lemma 1.4.18**

The commutator subgroup of a group is normal.

In fact, the following result holds.

**Lemma 1.4.19**

Let  $G$  be a group and  $N$  a normal subgroup of  $G$ . Then  $G/N$  is abelian if and only if  $[G, G] \leq N$ .

*Proof.* Take any  $x, y \in G$ . Then  $[Nx, Ny] = NxNyNx^{-1}Ny^{-1} = N[x, y]$ .

Then  $G/N$  is abelian iff  $[Nx, Ny] = 1_{G/N}$  for all  $x, y \in G$  iff  $[x, y] \in N$  for all  $x, y \in G$  iff  $[G, G] \leq N$ .  $\square$

### 1.4.6 Solvable groups

**Definition 1.4.20**

Let  $G$  be a group. Define the following series of subgroups:

$$G^{(0)} = G,$$

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}], \quad i \in \mathbb{N}^*.$$

This series is called the **derived series** of  $G$ .

**Exercise 1.4.21.** For each  $i \in \mathbb{N}$ ,  $G^{(i)} \trianglelefteq G$ .

**Definition 1.4.22**

A group  $G$  is solvable if there exists a positive integer  $n$  with  $G^{(n)} = \{1\}$ .

**Example 1.4.23.** 1. Every abelian group is solvable.

2. A dihedral group of order  $2n$  is solvable.

**Lemma 1.4.24**

If a group  $G$  is both solvable and simple, then  $G$  is cyclic of prime order.

*Proof.* Since  $G$  is solvable  $G^{(1)}$  is a proper normal subgroup of  $G$ . But  $G$  is simple, and so  $G^{(1)} = \{1\}$ . Now  $G/G^{(1)}$  is abelian, hence, by Lemma 1.4.10,  $G \cong C_p$  for some prime  $p$ .  $\square$