1. Groups, subgroups, morphisms

1.1. Groups. — In order to study an object provided with a structure, we determine its automorphism group, that is the group of transformations which preserves the object and its structure. It gives some precise information to describe or even characterize the object.
Group is the simplest of the algebraic structures and the most important: the reasons will be clear along the lecture. The name group is due to Galois (1832) and the modern definition is due to Cayley (1854).

Definition 1.1.1. — *A group is a set G together with binary operation*

$$G \times G \longrightarrow G \ \ (g_1, g_2) \mapsto g_1 g_2$$

satisfying the following conditions:
1. **Associativity***: for all $g_1, g_2, g_3 \in G$,*

$$(g_1 g_2) g_3 = g_1 (g_2 g_3),$$

2. **Existence of a neutral element***: there exists an element $e \in G$ such that for all $g \in G$,*

$$ge = eg = g,$$

3. **Existence of inverse***: for each element $g \in G$, there exists $g^{-1} \in G$, such that*

$$gg^{-1} = g^{-1}g = e.$$

The group G is said to be abelian (or commutative) if for all $g_1, g_2 \in G$, one has $g_1 g_2 = g_2 g_1$. In this case, we denote in general the binary operation $g_1 + g_2$ and $-g_1$ for the inverse of g_1. We may also denote $\circ$, $*$ or $\cdot$ the binary operation. The order $|G|$ of a group G is its cardinality. If $|G| < \infty$, the group G is said to be finite. A finite group whose order is a power of a prime $p \in \mathbb{N}^*$, is called a p-group.

Example 1.1.2. — *A group of order 1, $G = \{e\}$ is denoted 1.*

Example 1.1.3. — *If k is a field, $(k, +)$, $(k^*, \cdot)$ are groups. In this note, the fields are commutative (in French, fields are always commutative). For example, if $k = \mathbb{C}$ is the field of complex numbers, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \cdot)$ are groups.*
More generally, for $n \in \mathbb{N}^*$, the $n \times n$ matrices with coefficients in k and nonzero determinant form a group $\mathrm{GL}_n(k)$. For $n \geq 2$, the group $\mathrm{GL}_n(k)$ is not abelian.
In the same way, if A is a ring, $(A, +)$ is an abelian group. Let $A^\times$ denote the set of invertible elements of A. Then $(A^\times, \cdot)$ is a group. If A is a commutative ring, we may consider the group $\mathrm{GL}_n(A)$ of invertible matrices of order $n \in \mathbb{N}^*$ with coefficients in A, i.e. with determinant in $A^\times$.

Example 1.1.4. — *If G, H are two groups, we can construct a new group $G \times H$ called the direct product of G and H. As a set, it is the cartesian product of G*

and H and the multiplication is defined by $(g,h)(g',h') = (gg',hh')$. If moreover G, H are finite, then $G \times H$ is finite of order $|G||H|$.

The main groups in this lecture will be the permutation group and the linear group, that is groups of bijective applications with binary operation given by the composition. Indeed, they allows to describe all finite groups (Corollary 1.3.8,1.3.9) and groups representations (Part III).

Example 1.1.5. — *Let S be a set and $Bij(S)$ be the set of bijections $\varphi : S \longrightarrow S$. We define the product of two elements of S to be their composite.Then* $\mathrm{Bij}(S)$ *is a group called the group of symmetries of S. For example the permutation group on n letters $\mathfrak{S}_n$ is defined to be the group of symmetries of the set $\{1,\dots,n\}$. It has order $n!$ and is non abelian if $n \geq 3$.*

Example 1.1.6. — *Let k be a field. For a finite dimensional k-vector space V, the k-linear automorphisms of V form a group* $\mathrm{GL}(V)$ *called the linear group of V.*

Other groups emerge naturally by considering bijections on set with additional structure.

Example 1.1.7. — *Let V be a finite dimensional vector space over a field k. A bilinear form on V is a mapping $\varphi : V \times V \longrightarrow k$ that is linear in each variable. An automorphism of (V,φ) is a k-linear automorphism $\alpha \in \mathrm{GL}(V)$ such that*

$$\varphi(\alpha u, \alpha v) = \varphi(u,v), u, v \in V.$$

The automorphisms of (V,φ) form a group $Aut(\varphi)$. When φ is symmetric

$$\varphi(u,v) = \varphi(v,u), u, v \in V$$

and non-degenerate (if $\varphi(u,v) = 0$ for all $v \in V$, then $u = 0$), $Aut(\varphi)$ is called the orthogonal group of φ.
When φ is alternate

$$\varphi(u,u) = 0, u \in V$$

and non-degenerate, $Aut(\varphi)$ is called the symplectic group of φ.

Let us discuss the hypotheses defining a group.

Lemma 1.1.8. — *i. If e' satisfies $ge' = e'g = g$, $g \in G$ then $e' = ee' = e$. In fact e is the unique element of G such that $ee = e$.*
ii. For all $g \in G$, the inverse g^{-1} is uniquely determined, indeed if $gg' = e = g''g$, then

$$g'' = g''e = g''(gg') = (g''g)g' = eg' = g'.$$

The existence of inverse implies that the concellation laws hold in groups

$$gg' = gg'' \Longrightarrow g' = g'', \;\; g'g = g''g \Longrightarrow g' = g''.$$

iii. The associativity property can be express through the following commutative diagram:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\cdot \times \mathrm{id}} & G \times G \\ \mathrm{id} \times \cdot \downarrow & \square & \downarrow \cdot \\ G \times G & \xrightarrow{\cdot} & G \end{array}$$

The associativity property gives that the product of any ordered n-tuple $g_1, g_2, \ldots, g_n$ of elements of G is unambigously defined (by induction).
The inverse of $g_1 g_2 \ldots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

A diagram is a collection of sets and arrows (maps); it is commutative if the final result does not depend on the path taken. A diagram with a single line is called a sequence. Other interesting structures would be obtained if underlying assymptions for definition of groups.

Remark 1.1.9. — *A set A together with a binary operation*

$$A \times A \longrightarrow A, \ \ (g, g') \mapsto gg'$$

is called a magma. When the binary operation is associative $(A, \cdot)$ is called a semi-group. A semi-group with a neutral element is called a monoid.

Questions 1.1.10. — *For group, as for any algebraic structure, there is an enumerative problem : for $n \in \mathbb{N}^*$, what are the groups of order n? How can we classify the group of order n?*
To set the problem properly, one needs first to state clearly when two finite groups are "equivalent" (isomorphic). The enumerative question is an open problem, althrough the abelian case is solved. We do not know a priori how many different groups of a given order there are. To gauge the complexity, there are 49487365422 groups (up to isomorphism) of order 1024.
How can we describe groups?
Where do groups appear? What are they for? Why do we need them?

Remark 1.1.11. — *A binary operation on a finite set can be described by its multiplication table. The element e is a neutral element if and only if the first row and column of the table simply repeat the elements. Inverses exists if and only if each element occurs exactly once in each row and in each column. If there are n elements, then verifying the associativity law requires checking n^3 equalities. This suggests an algorithm for finding all groups of a given finite order n, namely list all possible multiplication tables and check the axioms. That gives a total of n^{n^2} tables very few of which define groups. For example, it means 8^{64} binary operations on a set of 8 elements, but we will see that there is only five isomorphism classes of groups of order 8 (three abelian groups, the dihedral group and the quaternion group). For example, the following multiplication defines a non abelian group of order 8 (here, exceptionally, e does not denote the neutral*

element):

$\cdot$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	f	h	g	c	e	d
c	c	e	d	g	h	b	a	f
d	d	h	g	a	f	e	c	b
e	e	c	b	f	a	d	h	g
f	f	g	h	e	d	a	b	c
g	g	f	a	c	b	h	d	e
h	h	d	e	b	c	g	f	a

For an element g of a group G and $n \in \mathbb{Z}$, we define

$$g^n = \begin{cases} gg\cdots g & n > 0 \quad n \text{ copies of } g, \\ e & n = 0, \\ g^{-1}g^{-1}\cdots g^{-1} & n < 0 \quad |n| \text{ copies of } g^{-1}. \end{cases}$$

If $m, n \in \mathbb{Z}$, we have

$$g^{n+m} = g^n g^m, \ \ (g^m)^n = g^{mn},$$

hence the set $\{n \in \mathbb{Z} | g^n = e\}$ equals $m\mathbb{Z}$ for some integer $m \geq 0$. When $m = 0$, $g^n \neq e$ unless $n = 0$, and g is said to have infinite order. Moreover $\{g^n, n \in \mathbb{Z}\}$ is a group (with the binary operation induced by the binary operation of G) of infinite order contained in G.
When $m \neq 0$, it is the smallest integer $m > 0$ such that $g^m = e$, and g is said to have finite order. In this case $g^{-1} = g^{m-1}$ and

$$g^n = e \Longleftrightarrow m|n.$$

Moreover $\{g^n, 0 \leq n \leq m-1\}$ is a group of order m contained in G.

1.2. Subgroup. — An efficient way to construct groups, is to consider subgroups of a group.

Proposition 1.2.1. — *Let H be a nonempty subset of a group G. If*
i. $g, h \in H \Longrightarrow gh \in H$, and
ii. $g \in H \Longrightarrow g^{-1} \in H$,
then the binary operation on G makes H into a group.
A nonempty subset $H \subset G$ satisfying i. and ii. is called a subgroup of G and denoted $H < G$.

Proof. — The associative binary operation on G defines an associative binary operation on H (after $i.$). Since H is not empty, it contains an element h. Then H contains h^{-1} (after $ii.$) and $e = hh^{-1} \in H$ (after $i.$). Then $ii.$ shows that the inverses of elements of H lie in H. □

Considering a subset of elements of a group satisfying a given (stable) property, allows to construct useful subgroups.

Example 1.2.2. — *The additive subgroups of relative numbers* $\mathbb{Z}$*, rational numbers* $\mathbb{Q}$*, real numbers* $\mathbb{R}$ *are subgroup of* $\mathbb{C}$*.*

Example 1.2.3. — *The centre of a group* G *is the subgroup*

$$Z(G) = \{g \in G \mid \ gx = xg, x \in G\}.$$

The group G *is abelian if and only if* $G = Z(G)$*. The centre of* $\mathrm{GL}_n(k)$ *is the set of non zero homotheties. The centre of* $\mathfrak{S}_n$ *is* $\{e\}$ *if* $n > 2$*.*

Example 1.2.4. — *The set* $\mu_n(k)$ *of* n*-root of unity in a field* k *forms a subgroup of* $k^\times$*.*
More generally, in an abelian group G*, the elements of finite order form a subgroup* G_{tors} *of* G *called the torsion subgroup.*
If G *is non abelian, the elements of finite order do not necessary form a subgroup of* G*. For example*

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

The elements A, B *are finite order elements of* $\mathrm{SL}_2(\mathbb{Z})$ *but* AB *has infinite order.*

Example 1.2.5. — *Assume* k *is a finite field of order* q*. The* $n \times n$ *matrices in* $\mathrm{GL}_n(k)$ *are those whose columms form a basis of* k^n*. The first column can be any nonzero vector in* k^n*, of which there are* $q^n - 1$ *; the second column can be any vector not in the span of the first column, of which there are* $q^n - q$*; and so on. Therefore, the order of* $\mathrm{GL}_n(k)$ *is* $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$*. The upper triangular matrices with 1's down the diagonal form a subgroup of order* $q^{n(n-1)/2}$*.*

The following property gives not only an efficient way to construct subgroup, but also to describe a group.

Proposition 1.2.6. — *For any subset* A *of a group* G*, there exists a smallest subgroup of* G *containing* A*. It is called the subgroup of* G *generated by* A *and denoted* $< A >$*.*
If $< A >= G$*, we say that* A *generates* G*.*

Proof. — The intersection of all subgroups of G containing A is again a subgroup containing A, and it is the smallest. It consists of all finite products of elements of A and their inverses. The set of such products satisfies the properties $i.$ and $ii.$ of proposition 1.2.1. Then it is a subgroup containing A, and therefore equals $< A >$:

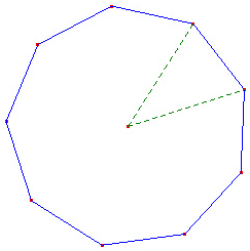
$$< A >= \left\{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} | n \in \mathbb{N}, a_i \in A, \varepsilon_i \in \{1, -1\}, 1 \leq i \leq n\right\}.$$

□

Example 1.2.7. — *A group is said to be cyclic if it is generated by a single element,* $G =< r >$ *for some* $r \in G$. *If* r *has finite order* n, *then*

$$G = \{e, r, r^2, \ldots, r^{n-1}\}$$

is denoted C_n, *cyclic group of order* n *and can be thought as the group of rotational symmetries about the center of a regular polygon with* n*-sides. It is a subgroup of* $\mathfrak{S}_n$ *by permuting the* n *vertices of the polygon.*



Example 1.2.8. — *For* $n \geq 3$, *the dihedral group* D_n *is the group of symmetries of a regular polygon with* n*-sides. Number the vertices* $1, \ldots, n$ *in the counterclockwise direction. Let* r *the rotation through* $2\pi/n$ *about the centre of polygon* $(i \mapsto i+1 \mod n)$ *and let* s *be the reflection in the line through the vertex 1 and the centre of the polygon* $(i \mapsto n+2-i \mod n)$. *Then*

$$r^n = e,\ s^2 = e,\ srs = r^{-1} \text{ and } D_n = \{e, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}.$$

Hence D_n *is a subgroup of* $\mathfrak{S}_n$ *of order* $2n$. *For example, using sage, we obtain the multiplication table of the dihedral group* D_4 *given in example 1.1.11. Remark that sage gives another family of generators.*

```
sage:  D4=DihedralGroup(4)
sage:  D4
Dihedral group of order 8 as a permutation group
sage:  D4.order()
8
sage:  D4.gens()
[(1,2,3,4), (1,4)(2,3)]
sage:  D4.is_abelian()
False
sage:  D4.cayley_table()
(···)
```

Example 1.2.9. — *The quaternion group* Q.
Let $a = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ *and* $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. *Then*

$$a^4 = e, a^2 = b^2, bab^{-1} = a^3 (so\ ba = a^3 b).$$

The subgroup of $\mathrm{GL}_2(\mathbb{C})$ *generated by* a *and* b *is*

$$Q = \{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\}.$$

```
sage:  Q = groups.presentation.Quaternion(); Q
Finitely presented group < a, b|a^4, b^2 * a^ - 2, a * b * a * b^ - 1 >
sage:Q.order(); Q.is_abelian()
8
False
```

Example 1.2.10. — *A group G is said to be of finite type if there exists a finite subset $A \subset G$, such that $< A >= G$.*
A finite group is of finite type. A group of finite type is countable. The converse is false, for example the countable group $(\mathbb{Q}, +)$ is not generated by a finite set.
A subgroup of a group of finite type is not always of finite type. Indeed let G be the subgroup of $\mathrm{Bij}(\mathbb{Z})$ *generated by the transposition* (01) *and $\sigma : \ell \mapsto \ell + 1$. Then G contains all transpositions of $\mathbb{Z}$. The group of permutations of $\mathbb{Z}$ with finite support is a subgroup of G, but is not of finite type.*

Remark 1.2.11. — *We have seen in the proof of Proposition 1.2.6 that an intersection of subgroups of G is a subgroup of G. More generally, an intersection of subobjects of an algebraic object (rings, modules, fields, vectors spaces, algebras...) is a subobject.*

1.3. Group Homomorphism. — The notion of group homomorphism is useful not only in order to construct subgroups but also to compare and identify groups and to understand the structure of groups.

Definition 1.3.1. — *A group (homo)morphism from a group G to a group G' is a map*

$$\varphi : G \longrightarrow G', \text{ such that } \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2), \quad g_1, g_2 \in G.$$

If $\varphi : G \longrightarrow G'$ is a morphism of groups, the kernel and the image of φ

$$\ker \varphi = \{g \in G | \varphi(g) = e'\} \text{ and } \operatorname{im} \varphi = \{\varphi(g), g \in G\}$$

are subgroups of G and G' respectively.
The morphism φ is injective if and only if $\ker \varphi = \{e\}$.
The morphism φ is surjective if and only if $\operatorname{im} \varphi = G'$.
An isomorphism is a bijective -injective and surjective- morphism of groups.
An automorphism is an isomorphism with $G = G'$.

Group homomorphisms are not only efficient way to construct subgroup, but also to identify two groups by isomorphisms.

Example 1.3.2. — *Let k a field. The choice of a basis of a k-vector space V of dimension n, determines an isomorphism* $\mathrm{GL}(V) \to \mathrm{GL}_n(k)$.
The determinant $\det : \mathrm{GL}_n(k) \longrightarrow k^*$ *is a surjective group morphism. Its kernel* $\ker \det = \mathrm{SL}_n(k)$ *is the special linear group of matrices with determinant 1.*

Example 1.3.3. — *We say that a group G acts on a set X, if there is a group homomorphism:*

$$G \longrightarrow \mathrm{Bij}(X).$$

Assume $X = V$ is a k-vector space. A representation of the group G is a group homomorphism in the linear group:

$$G \longrightarrow \mathrm{GL}(V)$$

These groups homomorphisms appear in many different contexts in mathematics whose importance justifies specific terminology and study (Part II, Part III).

Example 1.3.4. — *The signature*

$$\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}, \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

is a group morphism, surjective if $n \geq 2$ and its kernel is called the alternate group $\mathfrak{A}_n$.
In order to prove that ε is a group morphism, consider the polynomial in n variables

$$p(z_1, \ldots, z_n) = \prod_{1 \leq i < j \leq n} (z_i - z_j)$$

and for any $\sigma \in \mathfrak{S}_n$, define

$$\sigma(p) = p(z_{\sigma(1)}, \ldots, z_{\sigma(n)}).$$

Then $\sigma(p) = \varepsilon(\sigma)p$, and for any $\sigma, \tau \in \mathfrak{S}_n$,

$$\sigma(\tau p) = (\sigma\tau)p \Longrightarrow \varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\sigma\tau).$$

Remark 1.3.5. — *To compute the signature of σ, connect (by a line) each element i in the top row to the element i in the bottom row, and count the number of times that the lines cross ; σ is even or odd according as this number is even or odd. This works because there is one crossing for each inversion.*

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$$

$$6 \quad 1 \quad 3 \quad 4 \quad 5 \quad 2$$

The braid group on n strands is a generalization of permutation group.

Remark 1.3.6. — *Groups with small order. For each prime p, there is only one group of order p up to isomorphism, namely C_p. For $n \leq 12$ (not prime), up to isomorphism, groups of order n are given by the following table*

$\lvert G\rvert$	Groups
4	$C_4, C_2 \times C_2$
6	$C_6, \mathfrak{S}_3$
8	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, D_4, Q$
9	$C_9, C_3 \times C_3$
10	C_{10}, D_5
12	$C_{12}, C_2 \times C_6, C_2 \times \mathfrak{S}_3, \mathfrak{A}_4, C_3 \rtimes C_4$

The group $C_3 \rtimes C_4$ is defined in Remark 2.2.9. We will also show that the dihedral group D_3, of order 6, is isomorphic to the permutation group $\mathfrak{S}_3$ as expressed with sage.

```
sage:  S3 = SymmetricGroup(3);S3
Symmetric group of order 3!  as a permutation group
sage:  D3=DihedralGroup(3); D3
Dihedral group of order 6 as a permutation group
sage:  D3.is_isomorphic(S3)
True
```

Theorem 1.3.7. — *(Cayley) There is a canonical injective group homomorphism*

$$\varphi : G \longrightarrow \mathrm{Bij}(G).$$

Proof. — For $g \in G$, we define $\alpha_g \in \mathrm{Bij}(G)$ to be the map $\alpha_g : x \mapsto gx$. Then $G \longrightarrow \mathrm{Bij}(G)$, $g \mapsto \alpha_g$ is an injective group homomorphism. □

Corollary 1.3.8. — *A finite group of order n can be realized as a subgroup of the permutation group $\mathfrak{S}_n$.*

Proof. — List the elements of the group as $g_1, \ldots, g_n$ and apply Cayley's Theorem. □

In general a group G of order n can be embedded in a permutation group of much smaller order than $n!$.

Corollary 1.3.9. — *Let k be a field. A finite group of order n can be realized as a subgroup of* $\mathrm{GL}_n(k)$.

Proof. — Indeed there is an injective group homomorphism

$$\mathfrak{S}_n \longrightarrow \mathrm{GL}_n(k),\ \sigma \mapsto P_\sigma$$

where P_σ is the matrix defined by the application defined on the canonical basis by $e_i \mapsto e_{\sigma(i)}$, $1 \leq i \leq n$. □

Example 1.3.10. — *A sequence of group homomorphisms*

$$\cdots \xrightarrow{\varphi_{n+2}} G_{n+1} \xrightarrow{\varphi_{n+1}} G_n \xrightarrow{\varphi_n} G_{n-1} \xrightarrow{\varphi_{n-1}} \cdots$$

is said to be exact if and only if $\forall n, \operatorname{im}\varphi_{n+1} = \ker\varphi_n$.
For example, the sequence $G' \xrightarrow{\varphi} G'' \longrightarrow 1$ *is exact if and only if* φ *is surjective; the sequence* $1 \longrightarrow G \xrightarrow{\psi} G'$ *is exact if and only if* ψ *is injective.*
For example, the following sequences are exact

$$1 \longrightarrow \mathfrak{A}_n \longrightarrow \mathfrak{S}_n \longrightarrow \{1,-1\} \longrightarrow 1$$

$$1 \longrightarrow \mathrm{SL}_n(k) \longrightarrow \mathrm{GL}_n(k) \longrightarrow k^* \longrightarrow 1.$$

2. Quotients

2.1. Cosets. —

Definition 2.1.1. — *Let* H *a subgroup of a group* G. *For* $g \in G$, *we denote*

$$gH = \{gh | h \in H\} \text{ and } Hg = \{hg | h \in H\}.$$

The subsets of G *of the forms* gH *are called the left cosets of* H *in* G *and the subsets de* G *of the forms* Hg *are called the right cosets of* H *in* G.
The set of left cosets of H *in* G *is denoted* G/H. *The set of right cosets of* H *in* G *is denoted* $H\backslash G$.
The index $[G : H]$ *of* H *in* G *is defined to be the number of left cosets of* H *in* G.

The inverse map

$$G \to G, g \mapsto g^{-1}$$

sends gH on Hg^{-1}, hence induces a bijection $G/H \longrightarrow H\backslash G$. Hence the index $[G : H]$ is also the number of right cosets of H in G. But, in general, a left coset is not a right coset, the quotient set does not have a group structure.

Let H a subgroup of a group G, two left cosets of H in G are either disjoint or equal. For $a, b \in G$, $aH = bH$ if and only if $a^{-1}b \in H$. The left cosets form a partition of G.

Theorem 2.1.2. — *(Lagrange) Let* H *be a subgroup of a finite group* G. *Then*

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

Proof. — For $g \in G$, the map

$$H \longrightarrow G, \quad h \mapsto gh$$

induces a bijection $H \longrightarrow gH$. Hence if H is finite, the cardinality of gH equals $|H|$. The left cosets of H in G form a partition of G by cosets of same cardinality. □

Corollary 2.1.3. — *i. The order of a subgroup divides the order of the group. ii. The order of each element of a finite group divides the order of the group.*

Proof. — i. follows from Lagrange's theorem.
ii. Let $h \in G$. Apply Lagrange's theorem to the subgroup $H =< h >$ of G. □

Example 2.1.4. — *If G has order p, a prime, then every element of G has order 1 or p. But only e has order 1, so G is generated by any element $g \neq e$. In particular G is cyclic isomorphic to C_p (see Example 1.3.6).*

Exercise 2.1.5. — *Let G a group of finite type and H a subgroup of G of finite index. Then H has finite type. Indeed, assume $G =< g_1, \ldots, g_n >$ and denote $g'_1H, \ldots, g'_rH$ the left cosets. Then the finite set $H \cap \{g_i'^{-1} g_k g'_j | 1 \leq k \leq n, 1 \leq i, j \leq r\}$ generates H.*

Remark 2.1.6. — *Let S be a set. An equivalence relation on S is a binary relation denoted $\sim$ (i.e a subset $R \subset S \times S$ and $\forall (a, b) \in S \times S$, $a \sim b$ if and only if $(a, b) \in R$) which is reflexive ($a \sim a$, $a \in S$), symmetric ($a \sim b \Longleftrightarrow b \sim a$) and transitive ($a \sim b$ and $b \sim c \Longrightarrow a \sim c$). A subset $T \subset S$ such that $a \sim b$ holds for all $a, b \in T$ and $a \sim b$ never holds if $a \in T$ and $b \in S - T$, is said to be an equivalence class. The equivalence classes form a partition of S (A partition of a set S is a set P of nonempty subsets of S, such that every element of S is an element of a single element of P). The quotient set of S by $\sim$ is the set of all equivalence classes. There is a canonical surjection $\pi : S \longrightarrow S/\sim$. It satisfies the following universal property: let S' be a set. For any map $f : S \longrightarrow S'$, there exists a map $\bar{f} : S/\sim \longrightarrow S'$ such that $f = \bar{f} \circ \pi$ if and only if f is constant on any equivalence class.*
In particular, let H be an subgroup of G. We define an equivalence relation on G (reflexive, symmetric and transitive) by

$$g_1 \sim g_2 \Longleftrightarrow \exists h \in H \text{ such that } g_2 = g_1 h.$$

The left cosets and the right cosets of H in G are equal if and only if for any $g \in G$, $gHg^{-1} = H$. Indeed, $gH = Hg$ for any $g \in G$ implies $G/H = H\backslash G$. In this case, we are able to define a group structure on the set G/H. This is the main motivation of the following sections (2.2,2.3).

2.2. Normal subgroup. —

Definition 2.2.1. — *A subgroup H of a group G is said to be normal if*

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H.$$

If H is normal in G, we denote $H \lhd G$.
If G and 1 are the unique normal subgroups of G, the group G is said to be simple.

The subgroup H of G is normal if and only if $gH = Hg$, for all $g \in G$. The intersection of two normal subgroups is normal.

Example 2.2.2. — *If G is an abelian group, all its subgroups are normal.*
For $m \geq 1$, the cyclic group C_m is simple if and only if m is prime.

Example 2.2.3. — *If $\varphi : G \longrightarrow G'$ is a group morphism, then* $\ker \varphi$ *is a normal subgroup of G.*
The alternate group $\mathfrak{A}_n$, kernel of the signature, is normal in $\mathfrak{S}_n$. For k a field, the special linear group $\mathrm{SL}_n(k)$*, kernel of the determinant, is normal in* $\mathrm{GL}_n(k)$*. More generally for $H' \lhd G'$, $\varphi^{-1}(H')$ is a normal subgroup of G. Be careful, in general* $\mathrm{im}\,\varphi$ *is not normal.*

Example 2.2.4. — *The centre $Z(G)$ of a group G is a normal subgroup of G.*

Example 2.2.5. — *If H is a subgroup of index 2 in the group G, then $H \lhd G$. Indeed let $g \in G - H$, then gH is the complement of H in G. Similarly Hg is the complement of H in G, hence $gH = Hg$.*

Example 2.2.6. — *The normal subgroup generated by a subset A of a group G is*

$$N = \left\langle \cup_{g \in G}\, gAg^{-1} \right\rangle.$$

Example 2.2.7. — *Let G a group and* $\mathrm{Aut}\, G$ *its automorphisms group. For $h \in G$, we denote* $\mathrm{Inn}(h)$ *the element of* $\mathrm{Aut}\, G$ *defined by* $\mathrm{Inn}(h) : g \mapsto hgh^{-1}$*. The set*

$$\mathrm{Inn}\, G = \{\mathrm{Inn}(h), h \in G\}$$

is a normal subgroup of $\mathrm{Aut}\, G$*. Moreover*

$$\mathrm{Inn} : G \longrightarrow \mathrm{Aut}\, G, \quad h \mapsto \mathrm{Inn}(h)$$

defines a group homomorphism of kernel the (normal) subgroup $Z(G)$, centre of G and image $\mathrm{Inn}\, G$*. To summarize, the following sequence is exact*

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow \mathrm{Inn}\, G \longrightarrow 1$$

Normal subgroups can be used to reconstruct the whole group from subgroups in some cases.

Exercise 2.2.8. — *(Direct Product) Let H_1, H_2 two subgroups of the group G. Then $G = H_1 \times H_2$ if and only if H_1 and H_2 are normal in G, $< H_1, H_2 >= G$ and $H_1 \cap H_2 = \{e\}$.*
Indeed $H_1 \times H_2 \longrightarrow G$, $(h_1, h_2) \mapsto h_1 h_2$ should be a group isomorphism.

Exercise 2.2.9. — *(Semidirect product) Let N, H two groups and a group morphism $\varphi : H \longrightarrow \mathrm{Aut}\, N$. The semidirect product $G = N \rtimes H$ of N by H is the set $N \times H$ provided with the binary operation given by*

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2), \quad (n_i, h_i) \in N \times H, i = 1, 2.$$

If $G = N \rtimes H$, then N is identified with the normal subroup $N \times \{e_H\}$ of G and H is identified to the subgroup $\{e_N\} \times H$.
Let N, H two subgroup of the group G. Then $G = N \rtimes H$ if and only if $N \lhd G$, $N \cap H = \{e\}$ and $NH = \{nh | n \in N, h \in H\} = G$. Moreover the operation $\varphi : H \longrightarrow \mathrm{Aut}(N)$ is given by $\varphi(h)(n) = hnh^{-1}$, $h \in H$ and $n \in N$.
For example, the dihedral group is a semidirect product $D_n = C_n \rtimes C_2$, $C_2 =< s >$,

$C_n =< r >$, $\varphi : C_2 \longrightarrow \operatorname{Aut} C_n$, $s \mapsto (r^i \mapsto r^{-i})$.
A cyclic group of order p^2 and the quaternion group can not be written as a semidirect product in a non trivial fashion.
The non trivial semidirect product $C_3 \rtimes C_4$ is given on the generators $< x >= C_3$, $< y >= C_4$ by $\varphi : C_4 \longrightarrow \operatorname{Aut}(C_3)$, $\varphi(y)(x) = x^{-1}$.

Normal subgroups are also used to define groups by quotient.

2.3. Quotient. — Let H be a subgroup of a group G. In this section, we define a group structure on the set G/H such that the surjective map

$$\pi : G \longrightarrow G/H, \quad g \mapsto gH$$

becomes a group morphism. Since $\pi(e) = eH$ should be the neutral element of G/H, $\ker \pi = H$, hence H should be a normal subgroup of G.

Theorem 2.3.1. — *Let H be a normal subgroup of the group G. There exists an unique group structure on G/H such that the surjective map*

$$\pi : G \longrightarrow G/H, \quad g \mapsto gH$$

is a group morphism.
The induced sequence is exact

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1.$$

Proof. — To ensure that π is a group morphism, the binary operation on G/H should verify

$$(g_1H)(g_2H) = g_1g_2H.$$

So we have to prove that this equality induces a well-defined group structure on the set G/H. In particular, it is independant of the choice of g_1 and g_2 in their left cosets. Indeed, if $g_1 = g_1'h_1$ and $g_2 = g_2'h_2$, one has

$$g_1g_2 = g_1'h_1g_2'h_2 = g_1'g_2'(g_2'^{-1}h_1g_2')h_2.$$

Since $H \lhd G$, $g_2'^{-1}h_1g_2' \in H$, hence $g_1g_2H = g_1'g_2'H$.
It remains to prove that this binary operation on G/H satisfies the properties associativity, existence of a neutral element and inverse. □

Let us begin with quotient groups of abelian groups (in this case any abelian subgroup is normal).

Example 2.3.2. — *The subgroups of $(\mathbb{Z}, +)$ are $m\mathbb{Z}$ for $m \in \mathbb{N}$ (and normal since $\mathbb{Z}$ is abelian). For $m \geq 1$, the quotient group $(\mathbb{Z}/m\mathbb{Z}, +)$ is isomorphic to $(C_m, \cdot)$ cyclic of order m.*

Example 2.3.3. — *The multiplicative group $\mu(\mathbb{C})$ of complex roots of unity is isomorphic to the quotient group $(\mathbb{Q}/\mathbb{Z}, +)$.*

Example 2.3.4. — *If V is a k-vector space and W is a subvector space of V, then W is a normal subgroup of V (abelian) and the quotient V/W is not only a group but also a k-vector space.*

Remark 2.3.5. — *A chain complex is a sequence of abelian group homomorphisms*

$$\cdots \xrightarrow{\varphi_{n+2}} G_{n+1} \xrightarrow{\varphi_{n+1}} G_n \xrightarrow{\varphi_n} G_{n-1} \xrightarrow{\varphi_{n-1}} \cdots$$

with $\varphi_n\varphi_{n+1} = 0$ for all n. The nth homology group in the chain complex is defined to be the quotient

$$H_n(G_\bullet) = \ker \varphi_n / \operatorname{im} \varphi_{n+1}.$$

The homology measures "how far" the chain complex associated to $G_\bullet$ is from being exact.

Exercise 2.3.6. — *Let G a group. The derived subgroup of G is the subgroup $D(G)$ of G generated by the elements of the form $ghg^{-1}h^{-1}$, $g, h \in G$. Then $D(G)$ is normal*

$$g'(ghg^{-1}h^{-1})g'^{-1} = (g'g)h(g'g)^{-1}g'h^{-1}g'^{-1} = (g'g)h(g'g)^{-1}h^{-1} \cdot hg'h^{-1}g'^{-1}$$

and $G/D(G)$ is abelian

$$\bar{g}\bar{h} = \bar{h}\bar{g}\overline{g^{-1}h^{-1}gh}.$$

If H is any normal subgroup of G with G/H abelian, then $D(G) \subset H$.

Exercise 2.3.7. — *Let H be a normal subgroup of the group G. If G is of finite type, then G/H is of finite type. If H and G/H are of finite type, then G is of finite type.*

Exercise 2.3.8. — *i. (First theorem of isomorphism). Let $\varphi : G \to G'$ a group morphism and $H = \ker \varphi$. Then φ factorizes through G/H and defines an isomorphism $\bar{\varphi} : G/H \longrightarrow \operatorname{im} \varphi$.*
ii. (Second theorem of isomorphism). Let H, K two normal subgroups of a group G such that $K \subset H$. Then $H/K \lhd G/K$ and

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

iii. Let H, K be subgroups of G with $H \lhd G$. Then

$$HK = \{hk | h \in H, k \in K\} = KH = HKH$$

is a subgroup of G, $H \cap K \lhd K$ and

$$HK/H \simeq K/(H \cap K).$$

(voir TD).

Proposition 2.3.9. — *Let N a normal subgroup of a group G. There is a bijection between*

$$\{ \text{ Subgroups of } G \text{ containing } N\} \longleftrightarrow \{ \text{ Subgroups of } G/N\}, H \longleftrightarrow \bar{H}.$$

Moreover H is normal in G if and only if $\bar{H}$ is normal in G/N.

Proof. — Let $\pi : G \longrightarrow G/N$. If $\bar{H}$ is a subgroup of G/N, then $\pi^{-1}(\bar{H})$ is a subgroup of G containing N. If H is a subgroup of G, $\pi(H)$ is a subgroup of G/N. Since $\pi^{-1}\pi(H) = HN$, $HN = H$ if and only if $N \subset H$ and $\pi\pi^{-1}(\bar{H}) = \bar{H}$. Therefore, the two operations give the required bijection. The remaining statement are easily verified. □

Remark 2.3.10. — *(Snake lemma) Consider the two exact sequences of group homomorphisms*

$$\begin{array}{ccccccccc} & & A & \underset{f}{\longrightarrow} & B & \underset{g}{\longrightarrow} & C & \longrightarrow & 1 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 1 & \longrightarrow & A' & \underset{f'}{\longrightarrow} & B' & \underset{g'}{\longrightarrow} & C' & & \end{array}$$

where $a(A), b(B)$ and $c(C)$ are normal subgroups. Denote $\operatorname{Coker} a = A'/a(A)$, $\operatorname{Coker} b = B'/b(B)$, $\operatorname{Coker} c = C'/c(C)$. *Then the following sequence is exact*

$$\ker a \to \ker b \to \ker c \to \operatorname{Coker} a \to \operatorname{Coker} b \to \operatorname{Coker} c.$$

Remark 2.3.11. — *An exact sequence*

$$1 \longrightarrow N \underset{\iota}{\longrightarrow} G \underset{\pi}{\longrightarrow} Q \longrightarrow 1$$

is called an extension of Q by N.
The extension of Q by N is said to be central if $\iota(N) \subset Z(G)$.
The extension of Q by N is said to be split if there exists a group homomorphism $s : Q \longrightarrow G$ such that $\pi \circ s = \mathrm{Id}$; This is equivalent to G is isomorphic to a semidirect product of Q by N.
For example, the following two sequences are split

$$1 \longrightarrow \mathfrak{A}_n \longrightarrow \mathfrak{S}_n \xrightarrow{\varepsilon} \{1, -1\} \longrightarrow 1$$

for $s : \{1, -1\} \longrightarrow \mathfrak{S}_n$, $1 \mapsto \mathrm{Id}$, $-1 \mapsto \tau$, where τ is any transposition;

$$1 \longrightarrow \mathrm{SL}_n(k) \longrightarrow \mathrm{GL}_n(k) \xrightarrow{\det} k^* \longrightarrow 1$$

for $s : k^* \longrightarrow \mathrm{GL}_n(k)$, $\lambda \mapsto \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$.

In general an extension is not split, for example

$$1 \longrightarrow C_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$$

is not split.
An extension of finite groups of relatively prime order is split (Schur-Zassenhaus).
Two extensions of Q by N are said to be isomorphic if there exists a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \\ & & \| & & \downarrow\sim & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \end{array}$$

The isomorphic classes of extensions of Q by N are described by the group $Ext^1(Q, N)$.

The problem of classifying all finite groups falls into two parts:
- Classify all finite simple groups,
- Classify all extensions of finite groups.

The case of finite abelian groups is the simplest.
