PARTIE I

GROUPES

Download Sage: http://www.sagemath.org/index.html

1. Groupes, sous-groupes, morphismes

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:

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

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 sugroup 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 $< A >$:

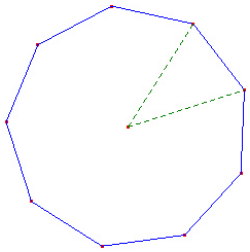
$$< A >= \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} | n \in \mathbb{N}, a_i \in A, \varepsilon_i \in \{1, -1\}, 1 \leq i \leq n\}.$$

□

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 counter-clockwise 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()
```
$(\cdots)$

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*

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

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.*

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

$$\begin{array}{cccccc} 6 & 1 & 3 & 4 & 5 & 2 \end{array}$$

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 sugroup $H =< h >$ 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 $G =< g_1, \ldots, g_n >$ et 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 of $R \subset S \times S$ 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 never 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 sugbroup 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 $\varphi : H \longrightarrow \operatorname{Aut} N$. 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 $\varphi : H \longrightarrow \operatorname{Aut}(N)$ 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

$$(g_1 H)(g_2 H) = g_1 g_2 H.$$

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

Exercise 2.3.6. — *Let G a group. The commutator or 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*

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

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*

$$1 \to \ker a \to \ker b \to \ker c \to \operatorname{Coker} a \to \operatorname{Coker} b \to \operatorname{Coker} c \to 1.$$

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. If the extension of G by N is split and central,

then $G \simeq N \times Q$.
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 if 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.

3. Structure des groupes abéliens de type fini

Nous disposons à présent des outils nécessaires à la classification des groupes abéliens de type fini. La démonstration développée ici est la plus élémentaire (d'autres stratégies de preuves sont évoquées dans les sections suivantes). Malgré le caractère élémentaire des arguments et des objets de cette section, plusieurs questions ouvertes se présentent à nous.

Dans §3, les groupes considérés sont abéliens, l'opération est notée additivement. En particulier, le groupe cyclique d'ordre n est noté $(\mathbb{Z}/n\mathbb{Z},+)$. Le groupe à un élément est noté 0 ou $\mathbb{Z}/n\mathbb{Z}$ avec $n = 1$.

3.1. Fonction indicatrice d'Euler et corps finis. — Le résultat clé, dit lemme chinois, est le suivant :

Lemme 3.1. — *Le produit (direct) de deux groupes cycliques d'ordre m et n respectivement, est un groupe cyclique d'ordre mn si et seulement si $(m,n)=1$:*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ si et seulement si } (m,n)=1.$$

Démonstration. — Dans un produit direct de groupes, l'ordre d'un élément est le ppcm des ordres des différents composants de l'élément.
Le morphisme $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ a pour noyau les éléments divisibles par n et m. Ce noyau s'identifie à $mn\mathbb{Z}$ si et seulement si $(m,n)=1$.
Si $(m,n)=1$), le morphisme f se factorise en un morphisme injectif $\bar{f} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui est un isomorphisme car les deux membres ont même cardinal. □

Exemple 3.2. — *Le groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (qui ne contient pas d'élément d'ordre 4) n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Le groupe $\mathbb{Z}/4\mathbb{Z}$ n'est pas non plus le produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ car le seul automorphisme de $\mathbb{Z}/2\mathbb{Z}$ est l'identité. La suite exacte*

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

n'est pas scindée.

Définition 3.3. — *La fonction indicatrice d'Euler est la fonction définie par*

$$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*, \varphi(n) = \#\{k | (k,n)=1, 0 \leq k \leq n-1\}.$$

Corollaire 3.4. — *Soit $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ un entier $n \geq 2$ décomposé en facteurs premiers distincts. Nous avons l'isomorphisme*

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}). \tag{1}$$

Le nombre de générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ est égal à

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{r} \Big(1 - \frac{1}{p_i}\Big),$$

Démonstration. — Soit $k \in \{0, \ldots, n-1\}$ et $\pi(k)$ l'image de k par la surjection $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. Alors $\pi(k)$ est générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $(k,n)=1$. Donc $\varphi(n)$ est le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.
D'après le lemme chinois, si $(m,n)=1$ alors $\varphi(mn) = \varphi(n)\varphi(m)$. De plus si p est premier et $\alpha \geq 1$, $\varphi(p^r) = p^r - p^{r-1}$ (le nombre d'entiers positifs strictement inférieurs à p^α - le nombre de multiples positifs de p strictement inférieurs à p^α). Nous en déduisons l'expression de $\varphi(n)$. □

Attardons-nous un peu sur la fonction indicatrice d'Euler, fonction combinatoire naturelle qui a diverses applications arithmétiques et donnons des quelques exemples de groupes cycliques utiles.

Lemme 3.5. — *(Formule de Möbius) Soit $n \in \mathbb{N}^*$, alors*

$$n = \sum_{d|n} \varphi(d).$$

Démonstration. — Pour $d|n$, le groupe $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe isomorphe à C_d qui est précisément l'ensemble

$$\{x \in \mathbb{Z}/n\mathbb{Z} | dx = 0\}.$$

Comme $C_d \sim \mathbb{Z}/d\mathbb{Z}$, il contient $\varphi(d)$ éléments d'ordre d. Donc $\mathbb{Z}/n\mathbb{Z}$ contient exactement $\varphi(d)$ éléments d'ordre d et nous obtenons le lemme en triant les éléments de $\mathbb{Z}/n\mathbb{Z}$ suivant leur ordre. □

Soit p un nombre premier. Il est usuel de munir le groupe additif $\mathbb{Z}/p\mathbb{Z}$ d'une structure d'anneau abélien dans lequel tous les éléments non nuls sont inversibles et de construire ainsi le corps à p éléments noté $\mathbb{F}_p$. Ces éléments non nuls sont les racines du polynome $x^{p-1} = 1$, ainsi le groupe multiplicatif $\mathbb{F}_p^*$ est un groupe cyclique d'ordre $p - 1$. Plus généralement,

Proposition 3.6. — *Soit k un corps et G un sous-groupe fini du groupe multiplicatif k^*. Alors G est cyclique.*

Démonstration. — Notons $n = |G|$ et supposons que G contienne un élément x d'ordre d. Alors le sous-groupe $< x > \simeq C_d$ est de cardinal d et tous ses éléments g vérifient $g^d = 1$. Mais dans le corps k, l'équation $X^d - 1$ a au plus d solutions, donc $< x >$ est l'ensemble de ces solutions. Comme il est cyclique d'ordre d, il contient $\varphi(d)$ éléments d'ordre d qui sont exactement les éléments d'ordre d de G. Donc pour tout d divisant n, G possède au plus $\varphi(d)$ éléments d'ordre d. Si G n'a pas d'élément d'ordre n, alors $n > \sum_{d|n, d\neq n} \varphi(d)$, ce qui est absurde. Donc G est cyclique d'ordre n. □

Remarque 3.7. — *Soit k un corps et le morphisme (d'anneaux)*

$$\psi : \mathbb{Z} \longrightarrow k, \quad n \mapsto \begin{cases} n \cdot 1 = 1 + \cdots + 1 & n > 0 \\ 0 & n = 0 \\ -(-n \cdot 1) & n < 0 \end{cases}$$

Son noyau est de la forme $p\mathbb{Z}$ avec $p \geq 0$. L'entier $p \geq 0$ ainsi défini est dit caractéristique du corps k. Si p est non nul, alors p est premier car le groupe multiplicatif k^* est intègre. Ainsi k contient un sous-corps isomorphe à $\mathbb{F}_p$ donc k est un $\mathbb{F}_p$-espace vectoriel. En particulier si k est fini, son ordre q est puissance de p et d'après la proposition 3.6, k^* est un groupe cyclique d'ordre $q - 1$. Remarquons que malgré la structure élémentaire de k^*, il est difficile de déterminer un générateur explicite de k. Cette difficulté est la garantie de la robustesse des algorithmes de cryptographie les plus utilisés.

Remarque 3.8. — *Soit p un nombre premier. Pour toute puissance $q = p^r > 1$, nous pouvons montrer qu'il existe un corps fini $\mathbb{F}_q$ d'ordre q unique à isomorphisme près. Le corps $\mathbb{F}_q$ se construit comme quotient de l'anneau quotient $\mathbb{F}_p[X]$ par l'idéal engendré par un polynôme irréductible sur $\mathbb{F}_p$ de degré r.*
Le groupe des automorphismes du corps $\mathbb{F}_q$ (i.e morphisme d'anneaux bijectif) est cyclique d'ordre r engendré par l'automorphisme de Frobenius $x \mapsto x^p$.
Il existe des corps de caractéristique $p > 0$ qui ne sont pas finis, par exemple le corps des fractions $\mathbb{F}_p(X)$ ou la cloture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$.

Remarque 3.9. — *Soit $n \geq 1$ et d un diviseur de n. Notons $\Phi_d \in \mathbb{C}[X]$ le polynôme, dit polynôme cyclotomique, unitaire de degré $\varphi(d)$ dont les racines sont les racines d'ordre d de $X^n - 1$. Ainsi par exemple*

$$\phi_1 = X - 1, \phi_2 = X + 1, \Phi_3 = X^2 + X + 1, \Phi_4 = X^2 + 1 \text{ et } X^n - 1 = \Pi_{d|n}\Phi_d.$$

En particulier, nous retrouvons l'égalité $n = \sum_{d|n} \varphi(d)$. Le polynôme Φ_n est à coefficients entiers (à démontrer). Nous le montrons par récurrence sur n en effectuant la division euclidienne de $X^n - 1$ par $\Pi_{d|n, d\neq n}\Phi_d$.

```
sage: from sage.rings.polynomial.cyclotomic import cyclotomic_coeffs
sage: R = QQ['x']
sage: R(cyclotomic_coeffs(30))
x^8 + x^7 - x^5 - x^4 - x^3 + x + 1
sage: R(cyclotomic_coeffs(105))
x^48 + x^47 + x^46 - x^43 - x^42 - 2*x^41 - x^40 - x^39 + x^36 + x^35 +
x^34 + x^33 + x^32 + x^31 - x^28 - x^26 - x^24 - x^22 - x^20 + x^17 + x^16 +
x^15 + x^14 + x^13 + x^12 - x^9 - x^8 - 2*x^7 - x^6 - x^5 + x^2 + x + 1
```

La première valeur de n pour laquelle Φ_n a un coefficient de valeur absolue supérieure à 2 est 105. Remarquons enfin (non évident) que les coefficients des polynomes cyclotomiques ne sont pas bornés.

Remarque 3.10. — *La fonction indicatrice d'Euler $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ tend vers l'infini quand n tend vers l'infini. En effet, pour tout $n \in \mathbb{N}^*$, $\varphi^{-1}(n)$ est un ensemble fini. Alors quel que soit $N > 0$, pour tout $n > \max \varphi^{-1}([1, N])$, nous avons $\varphi(n) > N$.*
Remarquons que la fonction indicatrice d'Euler n'est pas surjective, par exemple 14 n'a pas d'antécédent.
Le comportement de la fonction indicatrice d'Euler reste à ce jour mystérieux. Par exemple la conjecture de Carmichael énonce que pour tout $n > 0$, il existe $m \neq n$ tel que $\varphi(n) = \varphi(m)$.

3.2. Structure des groupes abéliens finis. — La structure des groupes abéliens finis est décrite dans le théorème suivant :

Théorème 3.11. — *Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe une suite finie décroissante d'entiers $(d_1, d_2, \ldots, d_r)$ telle que :*

i. $d_r|d_{r-1},\ldots,\ d_3|d_2,\ d_2|d_1$ *et* $d_r \geq 2$,
ii. $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z})$,
La suite $(d_1, d_2, \ldots, d_r)$ *est caractéristique de la classe d'isomorphie du groupe* G.

Pour démontrer ce théorème, nous avons besoin d'établir trois lemmes préliminaires.

Lemme 3.12. — *Soit* $x_1 \in G$ *un élément d'ordre maximal du groupe abélien fini* G. *Alors, pour tout* $y \in G$, *l'ordre de* y *est un diviseur de l'ordre de* x_1.

Démonstration. — Si $y_1, y_2 \in G$ ont des ordres premiers entre eux,

$$< y_1, y_2 >=< y_1 + y_2 >$$

est d'ordre le produit des ordres de y_1 et y_2. Donc tout diviseur premier p de l'ordre d'un élement y de G divise l'ordre de x_1. De plus si l'ordre de x_1 est $p^\alpha q$ avec $(p, q) = 1$ et si $y \in G$ est d'ordre $p^\beta q'$ avec $(p, q') = 1$ alors $\beta \leq \alpha$ (car sinon $p^\alpha x + q' y$ est d'ordre $p^\beta q > p^\alpha q$). □

Lemme 3.13. — *Soit* $x_1 \in G$ *un élément d'ordre maximal* d_1 *du groupe abélien fini* G *et* $H_1 =< x_1 >$. *Pour tout élément* $\bar{y} \in G/H_1$, *il existe un antécédent* $y \in G$ *de même ordre que* $\bar{y}$.

Démonstration. — Notons d l'ordre de $\bar{y}$. Soit $\tilde{y} \in G$ un relevé de $\bar{y}$ d'ordre δ. Comme $\delta\tilde{y} = 0$ implique $\delta\bar{y} = 0$, on a $d|\delta$. Posons $\delta = dd'$. Comme $d\bar{y} = 0$, on a $d\tilde{y} \in H_1$, donc il existe $k \in \mathbb{Z}$, tel que $d\tilde{y} = kx_1$ et $dd'\tilde{y} = 0 = d'kx_1$. Ainsi $d_1|d'k$ et $\delta|d_1$ (lemme 3.12), $d'k = \ell d_1 = \ell dd'd''$. Donc k est un multiple de d et $k = dk'$. Il suffit alors de prendre $y = \tilde{y} - k'x_1$. □

Lemme 3.14. — *Soit* $(d_1, d_2, \ldots, d_r)$ *et* $(\delta_1, \delta_2, \ldots, \delta_r)$ *deux suites décroissantes d'entiers positifs tels que* $d_{i+1}|d_i$, $1 \leq i \leq r-1$, $d_r \geq 2$ *et* $\delta_{j+1}|\delta_j$, $1 \leq j \leq s-1$, $\delta_s \geq 2$. *Pour que ces suites soient égales il faut et il suffit que pour tout entier* m *strictement positif, nous ayons*

$$\Pi_{i=1}^{r} pgcd(m, d_i) = \Pi_{j=1}^{s} pgcd(m, \delta_j).$$

Démonstration. — Il s'agit de montrer que cette condition est suffisante. Pour $m = d_1 \cdots d_r\delta_1 \cdots \delta_s$, nous déduisons que $d_1 \cdots d_r = \delta_1 \cdots \delta_s$. Pour $m = d_1$, nous déduisons que $\delta_j = pgcd(d_1, \delta_j)$, $1 \leq j \leq s$ donc $\delta_1|d_1$ et par symétrie $d_1|\delta_1$, donc $d_1 = \delta_1$. □

Ainsi le lemme 3.13 permet de montrer par récurrence sur l'ordre de G

$$G =< x_1 > \oplus < x_2 > \oplus \cdots \oplus < x_r >$$

avec x_i d'ordre d_i, $d_{i+1}|d_i$, $1 \leq i \leq r$ et $d_r \geq 2$. La classe d'isomorphie du groupe G caractérise la suite $(d_1, \ldots, d_r)$. Soit $(\delta_1, \ldots, \delta_s)$ une autre suite définissant

un groupe isomorphe à G. Si $x \in G$ est d'ordre d et $m \in \mathbb{N}$, mx est d'ordre $d/pgcd(m,d)$. Donc mG (image de G par la mulplication par m) est d'ordre

$$\prod_{i=1}^{r} \frac{d_i}{pgcd(m,d_i)} = \prod_{j=1}^{s} \frac{\delta_j}{pgcd(m,\delta_j)}.$$

Comme $|G| = \prod_{i=1}^{r} d_i = \prod_{j=1}^{s} \delta_j$, nous avons

$$\prod_{i=1}^{r} pgcd(m,d_i) = \prod_{j=1}^{s} pgcd(m,\delta_j).$$

Le lemme 3.14 permet de conclure.

Exemple 3.15. — *Du théorème de structure des groupes abéliens, nous déduisons aisément que si G est un groupe abélien fini et p premier divisant $|G|$. Alors G admet un élément d'ordre p.*

Exemple 3.16. — *Soit $G = \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ un groupe abélien fini avec $2 \geq d_s$ et $d_s|d_{s-1}|\cdots|d_1$. D'après le lemme de structure des groupes cycliques $G = \prod_{j\in J} \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$, où les p_j sont des nombres premiers éventuellement répétés.*
Réciproquement pour $G = \prod_{j\in J} \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$, nous récupèrons les d_i de la façon suivante : $d_1 = ppcm(p_j^{\alpha_j}, j \in J)$ et il s'écrit $d_1 = \prod_{j'\in J'} p_{j'}^{\alpha_{j'}}$. Puis d_2 est le ppcm des $p_j^{\alpha_j}$ pour $j \in J - J'$ etc...
Pour le groupe $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/2^3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z})$, nous obtenons ainsi $600, 60, 6, 2$.

```
sage:  J=AbelianGroup(9,[2,2,4,8,3,3,3,5,25]); J
Multiplicative Abelian group isomorphic to C2×C2×C4×C8×C3×C3×C3×C5×
C25
sage:  J.invariants()
(2, 2, 4, 8, 3, 3, 3, 5, 25)
sage:J.elementary_divisors()
(2, 6, 60, 600)
```

Exemple 3.17. — *Pour $n \geq 2$, il est facile d'écrire tous les groupes abéliens d'ordre n. Notons $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition de n en produit de puissances de nombres premiers distincts et* $\mathrm{Part}(\alpha)$ *le nombre de partitions de α en entiers naturels. Ainsi :*

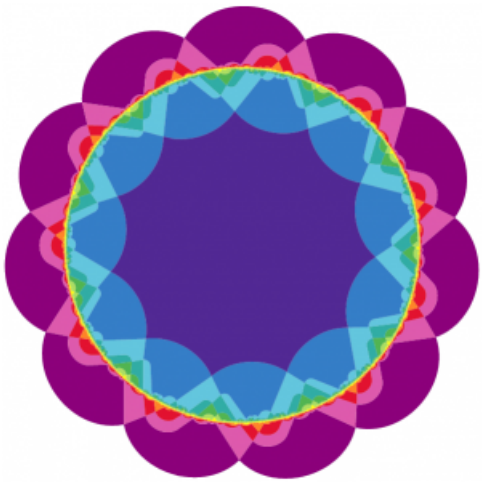
α	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathrm{Part}(\alpha)$	1	2	3	5	7	11	15	22	30	42	56	77	101	176	231

Alors, il y a

$$\mathrm{Part}(\alpha_1) \cdot \mathrm{Part}(\alpha_2) \cdots \mathrm{Part}(\alpha_k)$$

groupes abéliens d'ordre n distincts. Par exemple, il y a 42 groupes abéliens d'ordre 2^{10}. Nous pourrons chercher un algorithme efficace pour calculer le nombre de partitions.

Remarque 3.18. — *Soit X un ensemble fini et $P(X)$ l'ensemble de ses parties. Ainsi $|P(X)| = 2^{|X|}$. Notons l'ensemble vide $\emptyset \in P(X)$. Alors $P(X)$ muni de la différence symétrique $U + V = U \cup V / U \cap V$ (ensemble des éléments qui appartiennent à U ou à V mais pas les deux à la fois) est un groupe fini abélien d'élément neutre $\emptyset$ et chaque élément est son propre inverse.*
En 2012, K. Mamakani et F. Ruskey ont représenté les 2^{11} intersections possibles entre 11 régions symétriques du plan délimitées par des courbes fermées sans point double et sans point où trois courbes s'intersectent. Une telle représentation avec 13 régions n'est pas connue à ce jour.



http://images.math.cnrs.fr/

Exemple 3.19. — *Le groupe des automorphismes $\operatorname{Aut}\mathbb{Z}/n\mathbb{Z}$ du groupe additif $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe abélien multiplicatif fini $(\mathbb{Z}/n\mathbb{Z})^*$ à $\varphi(n)$ éléments. En effet l'application*

$$\Phi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \operatorname{Aut}\mathbb{Z}/n\mathbb{Z}, \quad a \mapsto (x \mapsto ax)$$

est un morphisme de groupes. Il est injectif car si $\Phi(a) = \mathrm{Id}$, alors $\Phi(a)(1) = a1 = 1$ donc $a = 1$. Il est surjectif : pour $\psi \in \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ posons $a = \psi(1)$. Alors pour tout $k \in \mathbb{N}$, $\psi(\bar{k}) = \psi(1 + \cdots + 1) = \bar{k}a$. De plus $a \in (\mathbb{Z}/n\mathbb{Z})^*$ car 1 doit avoir un antécédent par ψ.

Exemple 3.20. — *En constatant que l'isomorphisme (1) est un isomorphisme d'anneaux, nous obtenons l'isomorphisme de groupes abéliens (mutiplicatifs) finis*

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*.$$

Pour $p \neq 2$ premier, $r \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/p^r\mathbb{Z})^*$ est cyclique. En général, le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ n'est pas cyclique ; notamment pour $r \geq 3$, $(\mathbb{Z}/2^r\mathbb{Z})^*$ est isomorphe au groupe additif (non cyclique) $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{r-2}\mathbb{Z})$ (voir TD).

3.3. Groupes abéliens libres de rang fini. —

Définition 3.21. — *Un groupe abélien G est dit libre de rang r s'il est isomorphe à $\mathbb{Z}^r$, i.e il existe une famille d'éléments $x_1, \ldots, x_r$ de G tels que le morphisme de groupes*

$$\mathbb{Z}^r \longrightarrow G, \ \ (n_1, \ldots, n_r) \mapsto \sum_{i=1}^{r} n_i x_i$$

est bijectif. Une telle famille $(x_1, \ldots, x_r)$ est dite base de G.

La notion de rang est bien définie : les groupes abéliens $\mathbb{Z}^r$ et $\mathbb{Z}^s$ sont isomorphes si et seulement si $r = s$. En effet, par réduction modulo p, nous avons les surjections $\mathbb{Z}^r \longrightarrow (\mathbb{Z}/p\mathbb{Z})^r$, $\mathbb{Z}^s \longrightarrow (\mathbb{Z}/p\mathbb{Z})^s$, donc les groupes $(\mathbb{Z}/p\mathbb{Z})^r$ et $(\mathbb{Z}/p\mathbb{Z})^s$ ont le même cardinal $p^r = p^s$.

Lemme 3.22. — *Tout sous-groupe d'un groupe abélien libre de rang r est libre de rang s, $0 \leq s \leq r$.*

Démonstration. — Pour $r = 0$, le résultat est clair. Pour $r = 1$, les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ et sont libres de rang $0 \leq s \leq 1$.
Nous raisonnons ensuite par récurrence, en supposant le résultat vrai pour tout groupe abélien libre de rang $r-1$. Nous considérons un sous-groupe H non trivial de $\mathbb{Z}^r$ et la projection sur le dernier facteur

$$\pi : \mathbb{Z}^r \longrightarrow \mathbb{Z}, \ \ (x_1, x_2, \ldots, x_r) \mapsto x_r.$$

L'image de H par π est un sous-groupe de $\mathbb{Z}$ donc de la forme $n_r\mathbb{Z}$ avec $n_r \in \mathbb{N}$. Nous choisissons $h_r \in H$ avec $\pi(h_r) = n_r$. Or $\ker \pi = \mathbb{Z}^{r-1}$. Le sous-groupe $K = H \cap \ker \pi$ de $\mathbb{Z}^{r-1}$ est libre de rang au plus égal à $r-1$ (par induction) et $H = K \oplus \mathbb{Z}h_r$. □

D'un système de générateurs d'un groupe abélien libre de rang fini, nous ne pouvons pas nécéssairement extraire une base. Par exemple $2, 3$ engendre $\mathbb{Z}$ mais ni 2 ni 3 n'engendre $\mathbb{Z}$.
Dans $\mathbb{Z}^r$, nous avons les notions de famille libre sur $\mathbb{Z}$, cette notion est d'autant plus claire que nous avons l'inclusion $\mathbb{Z}^r \subset \mathbb{Q}^r$. Dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^r$, les notions d'indépendance linéaire sur $\mathbb{Z}$ ou sur $\mathbb{Q}$ sont équivalentes (à vérifier). Toute famille d'au moins $r+1$ éléments de $\mathbb{Z}^r$ est liée. Plus généralement

Définition 3.23. — *Une famille $y_1, \ldots, y_s$ d'élements d'un groupe abélien G est dite libre, si le morphisme de groupes*

$$\mathbb{Z}^s \longrightarrow G, \ \ (n_1, \ldots, n_s) \mapsto \sum_{i=1}^{s} n_i y_i$$

est injectif.

3.4. Groupes abéliens de type fini. —

Définition 3.24. — *Un groupe abélien G est dit de type fini s'il existe une famille d'éléments $x_1, \ldots, x_r$ de G telle que le morphisme de groupes*

$$\mathbb{Z}^r \longrightarrow G, \ \ (n_1, \ldots, n_r) \mapsto \sum_{i=1}^{r} n_i x_i$$

est surjectif.

Un groupe abélien de type fini est un quotient d'un groupe abélien libre de type fini. Il s'en suit qu'une famille libre d'un groupe abélien engendré par r générateurs a au plus r éléments.
Tout sous-groupe et tout groupe quotient d'un groupe abélien de type fini est un groupe abélien de type fini. En particulier, si G est un groupe abélien de type fini, le sous-groupe G_{tors} de torsion (des éléments d'ordre fini) de G est un sous-groupe abélien fini et le quotient G/G_{tors} est un groupe sans torsion (tout élément différent de l'élément neutre est d'ordre infini).

Lemme 3.25. — *Un groupe abélien G de type fini sans torsion est un groupe abélien libre de rang fini.*

Démonstration. — Soit $(x_1, \ldots, x_r)$ une famille génératrice et $(y_1, \ldots, y_s)$ une sous-famille libre de cardinal maximal de G. Notons H le sous groupe de G engendré par $y_1, \ldots, y_s$. Alors $s \leq r$ et pour tout i, il existe $n_i > 0$ tel que $n_i x_i \in H$ car $(x_i, y_1, \ldots, y_s)$ liée. Soit $n = \prod_{i=1}^{r} n_i$, et $nG < G$ l'image de G par le morphisme

$$G \longrightarrow G, g \mapsto ng = g + \cdots + g.$$

Nous avons $nG < H$. Le sous-groupe nG de H est donc libre de rang fini. Or $nG \simeq G$ car la multiplication par n est injective, donc G est libre de rang fini. □

Théorème 3.26. — *(Théorème de structure des groupes abéliens de type fini). Soit G un groupe abélien de type fini. Il existe des entiers r, s, $1 < d_s | d_{s-1} | \ldots | d_1$ tous déterminés par G tels que*

$$G \simeq \mathbb{Z}^r \times \Pi_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

Démonstration. — Le groupe quotient G/G_{tors} est sans torsion, donc

$$G/G_{\text{tors}} \simeq \oplus_{i=1}^{r} \mathbb{Z}\bar{x}_i.$$

Le sous-groupe H de G engendré par des antécédents x_i des $\bar{x}_i$, $1 \leq i \leq r$ est libre de rang r. Nous avons $H \cap G_{\text{tors}} = \{0\}$, $G = H + G_{\text{tors}}$, d'où le résultat. □

Remarque 3.27. — *Le théorème de structure des groupes abéliens de type fini est également une conséquence directe de la classification des matrices équivalentes à coefficients entiers (§5.1) ou de l'étude des caractères de G (§13).*

Remarque 3.28. — *Soit k un corps de caractéristique différente de 2 et 3. Une courbe elliptique est une courbe d'équation*

$$E : y^2 = x^3 + ax + b$$

pour a, b des coefficients dans k. L'ensemble $E(k)$ des points k-rationnels de la courbe elliptique est

$$E(k) = \{(x, y) \in k^2 | y^2 = x^3 + ax + b\} \cup \{O\}$$

où le point O est dit point à l'infini.
Nous définissons une loi de groupe abélien sur $E(k)$ de la façon suivante :
- O est l'élément neutre,
- l'opposé de $P = (x_1, y_1) \in E(k)$ est $-P = (x_1, -y_1)$,
- la somme de trois points alignés est nulle.

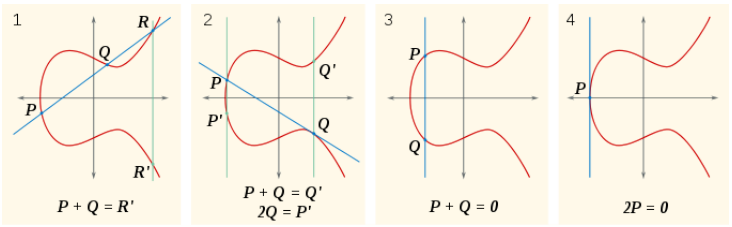


Illustration provenant de https://fr.wikipedia.org/wiki/Courbe_elliptique

Pour $P = (x_1, y_1)$ et $Q = (x_2, y_2)$, $P + Q = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1 \text{ et } \lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & si \quad P \neq Q, -Q \\ \frac{3x_1^2 + a}{2y_1} & si \quad P = Q. \end{cases}$$

Si k est fini, $E(k)$ est alors un groupe abélien fini, c'est toujours un groupe cyclique ou le produit de deux groupes cycliques.
Le théorème de Mordell-Weil établit que $E(\mathbb{Q})$ est un groupe abélien de type fini.
Le théorème de Mazur montre que le sous-groupe de torsion $E(\mathbb{Q})_{\text{tors}}$ appartient à l'ensemble des 15 groupes abéliens suivants : $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \{1, \ldots, 10, 12\}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $n \in \{2, 4, 6, 8\}$.
Le rang de $E(\mathbb{Q})$ est conjecturalement arbitrairement grand. En 2006, Elkies

a exhibé une courbe elliptique de rang supérieur à 28. Actuellement la courbe elliptique de rang connu maximum est de rang 19 :

$y^2 + xy + y = x^3 - x^2 + 31368015812338065133318565292206590792820353345x$
$+3020388026985660873356431884295434986245220416838744935551860625681598 47$
(Elkies 2009).

Par exemple pour la courbe elliptique définie sur $\mathbb{F}_7$ *par l'équation*

$$E : y^2 = x^3 + 3x - 1$$

le groupe $E(\mathbb{F}_7)$ *est cyclique d'ordre 4.*

```
sage:  E=EllipticCurve(GF(7),[3,-1]); E
Elliptic Curve defined by y^2 = x^3 + 3*x + 6 over Finite Field of
size 7
sage:  E.cardinality()
4
sage:  G=E.abelian_group(); G
Additive abelian group isomorphic to Z/4 embedded in Abelian group of
points on Elliptic Curve defined by y^2 = x^3 + 3*x + 6 over Finite
Field of size 7
```

Pour $E : y^2 = x^3 - x$*, nous avons*

$$E(\mathbb{F}_5) = \{O, (0,0), (2,1), (2,-1), (1,0), (-1,0), (-2,2), (-2,-2)\}.$$

```
sage:  E=EllipticCurve(GF(5),[-1,0]); E
Elliptic Curve defined by y^2 = x^3 + 4*x over Finite Field of size
5
sage:  G=E.abelian_group()
sage:  G
Additive abelian group isomorphic to Z/4+Z/2 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + 4*x over Finite
Field of size 5
sage:  P=E(2,-1); P
(2 :  4 :  1)
sage:  2*P
(0 :  0 :  1)
sage:  2*P
(0 :  0 :  1)
sage:  3*P
(2 :  1 :  1)
sage:  4*P
(0 :  1 :  0)
sage:  Q=E(1,0); Q
(1 :  0 :  1)
```

```
sage:  P+Q
(3 :  2 :  1)
```
La notation de sage correspond au plongement dans l'espace projectif $E(\mathbb{F}_5) \subset \mathbb{P}^2(\mathbb{F}_5)$. *Ainsi le point* O *s'identifie au point* $[0:0:1]$.

Les courbes elliptiques sont un objet important en arithmétique. Leur application la plus célèbre est sans doute le théorème de Taylor-Wiles (1994), si p *premier,* $abc \neq 0$ *et* $a^p + b^p = c^p$, *alors* $y^2 = x(x - a^p)(x + b^p)$ *fournit une représentation sur le corps* $\mathbb{F}_p$ *dont les propriétés excluent l'existence.*

Revenons à la description de la structure des groupes généraux.

4. Structure des groupes

4.1. Suite de composition. —

Définition 4.1. — *Une suite de composition d'un groupe* G *est une suite finie*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$

de sous-groupes de G *où chaque groupe* G_{i+1} *et normal dans* G_i *et chaque quotient* G_i/G_{i+1} *est simple.*

Ainsi dans une suite de composition, pour tout i, G_{i+1} est un sous-groupe normal non trivial (i.e. différent de 1 et G_i) de G_i maximal pour l'inclusion.

Exemple 4.2. — *Soit* $n = \prod_{i=1}^{r} p_i$ *la décomposition d'un entier* n *en facteurs premiers (pas nécessairement distincts) alors*

$$C_n \rhd C_{n/p_1} \rhd \cdots \rhd C_{n/\prod_{i=1}^{j} p_i} \rhd \cdots \rhd 1$$

est une suite de composition.

Lemme 4.3. — *Si* $H_1 \lhd G$ *et* $K_1 \lhd G$ *sont des groupes normaux tels que* G/H_1 *et* G/K_1 *sont simples, alors* $H_1 \cap K_1$ *est normal dans* H_1 *et dans* K_1 *et*

$$G/H_1 \simeq K_1/(H_1 \cap K_1), \;\; G/K_1 \simeq H_1/(H_1 \cap K_1).$$

Démonstration. — Le morphisme $K_1 \longrightarrow G/H_1$ a pour noyau $H_1 \cap K_1$ et K_1 est normal dans G donc $K_1/(H_1 \cap K_1)$ est normal dans G/H_1. Comme G/H_1 est simple, nous avons $K_1/(H_1 \cap K_1) = G/H_1$ ou 1.
Si $K_1/(H_1 \cap K_1) = 1$ on a $K_1 \subset H_1$ et H_1/K_1 sous-groupe normal non trivial du groupe simple G/K_1. Comme G/H_1 est simple, il est non trivial donc $H_1 \neq G$ et H_1/K_1 est trivial ce qui est exclu par $H_1 \neq K_1$. □

Le théorème suivant indique l'existence l'unicité des suites de composition pour un groupe fini fixé : seuls les quotients successifs dépendent de G pas les termes d'une suite de composition. Ces quotients simples (comptés avec leur multiplicité) sont appelés les facteurs simples de G. Ainsi tous les groupes finis sont construits à partir des groupes simples. Cependant les facteurs simples ne caractérisent pas le groupe G : $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/24\mathbb{Z}$ (et même $\mathfrak{S}_4$) ont les mêmes facteurs simples mais ne sont pas isomorphes.

Théorème 4.4. — *(Théorème de Jordan-Hölder) Tout groupe fini admet une suite de composition. Deux telles suites*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = 1$$

sont équivalentes : $s = r$ et il existe une permutation $\sigma \in \mathfrak{S}_s$ telle que $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i+1)}$, $0 \leq i \leq s-1$.

Démonstration. — Par induction sur l'ordre de G, il est facile de voir que tout groupe fini admet une suite de composition.
Pour l'unicité, nous raisonnons par récurrence sur l'ordre de G si $H_1 = G_1$, nous avons deux suites de composition pour G_1. Nous pouvons conclure par récurrence. Si $H_1 \neq G_1$, d'après le lemme 4.3

$$G/G_1 \simeq H_1/G_1 \cap H_1 \text{ et } G/H_1 \simeq G_1/G_1 \cap H_1.$$

Posons $K_2 = G_1 \cap H_1$, c'est un sous-groupe normal maximal dans G_1 et H_1 et

$$G/G_1 \simeq H_1/K_2, G/H_1 \simeq G_1/K_2.$$

Considèrons une suite de composition

$$K_2 \rhd K_3 \rhd \cdots \rhd K_t = 1.$$

Ainsi par induction les deux suites de composition d'une part

$$G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1$$

$$G_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd K_t = 1,$$

et les deux suites de composition d'autre part

$$H_1 \rhd H_2 \rhd \cdots \rhd H_s = 1$$

$$H_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd K_t = 1,$$

sont équivalentes. Ce qui permet de conclure. □

Remarque 4.5. — *(Programme de Holder). La classification des groupes finis, se ramène donc d'une part, à la classification de tous les groupes simples finis et, d'autre part, à la classification des extensions de groupes finis.*
La classification complète des groupes simples finis a été achevée dans les années 90. Elle se compose
- des groupes cycliques d'ordre premier,
- des groupes alternés $\mathfrak{A}_n$ pour $n \geq 5$,

- de certaines familles infinies de groupes de matrices,
- de 26 groupes dits "sporadiques".
L'objet de ce cours est de présenter certains de ces groupes simples.

Les groupes simples les plus élémentaires sont les groupes cycliques d'ordre premier. L'étude des groupes finis, dits résolubles, admettant une suite de composition dont les quotients sont cycliques d'ordre premier, est naturellement plus aisée.

4.2. Groupes résolubles. —

Definition 4.2.1. — *Un groupe G est dit résoluble s'il admet une suite résoluble, i.e une suite finie*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$

de sous-groupes de G où chaque groupe G_{i+1} est normal dans G_i et chaque quotient G_i/G_{i+1} est abélien.

Si G est fini, il est facile de déduire d'une suite résoluble, une suite de composition dont tous les quotients sont (simples) de la forme C_p avec p premier.

Exemple 4.6. — *Les groupes abéliens, les groupes diédraux sont résolubles.*

Remarque 4.7. — *Soit $f \in \mathbb{Q}[X]$ de degré n. La théorie de Galois associe à f un sous-groupe G_f du groupe (fini) des permutations des racines de f et établit que les racines de f se déduisent des coefficients de f via des opérations algébriques (addition, soustraction, multiplication, division, racine m-ième) si et seulement si G_f est résoluble. Ceci justifie la terminologie.*
En particulier les équations algébriques de degré 2 (formule du trinôme), 3 (formule de Cardan) et 4 (formule de Ferrari) sont résolubles par radicaux.
Pour tout n, il existe des polynômes de degré n avec $G_f \simeq \mathfrak{S}_n$. Or $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$ (Corollaire 9.15), donc il existe des polynômes qui ne sont pas résolubles par radicaux.

Lemme 4.8. — *Soit H un sous-groupe normal de G. Alors G est résoluble si et seulement si H et G/H sont résolubles.*

Démonstration. — Si G est résoluble et si $G \rhd G_1 \rhd \cdots \rhd 1$ est une suite résoluble, alors en notant $\overline{G_i}$ l'image de G_i par la surjection $\pi : G \longrightarrow G/H$

$$H \rhd H \cap G_1 \rhd \cdots 1, G/H = \overline{G} \rhd \overline{G_1} \rhd \cdots \rhd \bar{1}$$

sont des suites résolubles car $G_i/G_{i+1} \simeq \overline{G_i}/\overline{G_{i+1}}$ abélien (voir Exercice 2.3.8).
Réciproquement si

$$H \rhd H_1 \rhd \cdots 1, G/H = \overline{G} \rhd \overline{G_1} \rhd \cdots \rhd \bar{1}$$

sont des suites résolubles, notons G_i l'image inverse de $\overline{G_i}$ dans G. Ainsi

$$G \rhd G_1 \rhd \cdots \rhd G_n = H \rhd H_1 \rhd \cdots \rhd 1$$

est une suite résoluble pour G. □

Définition 4.9. — *Deux éléments d'un groupe G commutent si leur commutateur $[x, y] = xyx^{-1}y^{-1}$ vaut e. Le sous-groupe de G*

$$D(G) =< [x, y] \ | x, y \in G >$$

engendré par tous les commutateurs est appelé sous-groupe dérivé de G. Nous définissons par induction $D^0(G) = G$, $D^{i+1}(G) = D^i(G)$ pour tout $i \geq 0$.

Lemme 4.10. — *Le groupe dérivé $D(G)$ est le plus petit sous-groupe normal de G tel que $G/D(G)$ est abélien.*

Démonstration. — L'image de $[x, y]$ par un automorphisme f de G est $[f(x), f(y)]$, donc $f(D(G)) = D(G)$ et $D(G)$ est normal.
Tous les commutateurs sont nuls dans le quotient $G/D(G)$, donc $G/D(G)$ est abélien. Enfin si G/H est abélien, alors pour tous $x, y \in G$, $[x, y] \in H$ donc $D(G) < H$. □

Lemme 4.11. — *Un groupe G fini est résoluble si et seulement si il existe $k \in \mathbb{N}$ avec $D^k(G) = 1$.*

Démonstration. — Si $D^k(G) = 1$, la suite des groupes dérivés $(D^i(G))_{0 \leq i \leq k}$ est une suite résoluble de G.
Si

$$G \rhd G_1 \rhd \cdots \rhd G_n = 1$$

est une suite résoluble de G. Le groupe G/G_1 est abélien donc $D(G) \subset G_1$. Nous avons (voir Exercice 2.3.8)

$$D(G)/D(G) \cap G_2 \xrightarrow{\simeq} D(G)G_2/G_2 \subset G_1/G_2$$

car $D(G)G_2$ est un sous-groupe de G_1. Comme G_1/G_2 est abélien, $D(G)G_2/G_2$ aussi et $D^2(G) \subset D(G) \cap G_2 \subset G_2$. Ainsi par induction, $D^i(G) \subset G_i$ pour tout $0 \leq i \leq n$ donc $D^n(G) = 1$. □

Remarque 4.12. — *Soit G un groupe et $S = \{[x, y] \ | x, y \in G\}$. Si S est fini, $D(G)$ est fini.*

Remarque 4.13. — *Les groupes non abéliens simples ne sont pas résolubles. Tout groupe d'ordre < 60 est résoluble car les seuls groupes simples d'ordre < 60 sont les groupes cycliques d'ordre premier.*
Feit et Thompson ont montré en 1963 que tout groupe fini d'ordre impair est résoluble.

4.3. Groupes nilpotents et croissance des groupes de type fini. —

Définition 4.14. — *Soit G un groupe. Nous notons*

$$C_0(G) \rhd C_1(G) \rhd \cdots \rhd C_i(G) \rhd \cdots$$

la suite décroissante de sous-groupes normaux de G définie par

$$C_0(G) = G, C_{i+1}(G) = \langle [g, x] | \forall g \in G, x \in C_i(G) \rangle.$$

Un groupe G est nilpotent s'il existe $n \in \mathbb{N}$ tel que $C_n(G) = 1$.

Les sous-groupes $C_n(G)$ sont normaux dans G par induction en remarquant que $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.

Exemple 4.15. — *Un groupe nilpotent est résoluble, car $D^n(G) \subset C_n(G)$, pour tout $n \in \mathbb{N}$.*
La réciproque est fausse. Par exemple si k est un corps

$$B = \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, a, b, d \in k, ad \neq 0 \}$$

alors B est résoluble car $D(B) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \lhd B$, $B/D(B) \simeq k^* \times k^*$ et $D^2(B) = 1$.
Mais B n'est pas nilpotent car $C_2(B) = C_1(B) = D(B)$.
Ce même exemple permet également de montrer que $U \lhd B$ nilpotent avec B/U nilpotent n'implique pas que B est nilpotent.

Remarque 4.16. — *Nous rappelons qu'une extension (suite exacte)*

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

est dite centrale si $\iota(N) \subset Z(G)$. Les groupes nilpotents sont les groupes qui s'obtiennent par une suite d'extensions centrales de groupes abéliens. Les groupes résolubles sont les groupes qui s'obtiennent par une suite d'extensions (pas forcément centrales) de groupes abéliens.

Remarque 4.17. — *(Voir TD). Soit G un groupe de type fini, engendré par une partie A finie. Pour tout entier $m \geq 0$, nous notons $B_{G,A}(m)$ l'ensemble des éléments de G qui peuvent s'écrire comme produits d'au plus m éléments de $A \cup A^{-1}$ et $\beta_{G,A}$ la fonction croissante :*

$$\beta_{G,A} : \mathbb{N} \longrightarrow \mathbb{N}, m \mapsto \#B_{G,A}(m).$$

La croissance de la fonction $\beta_{G,A}$ ne dépend pas du choix de la partie génératrice au sens suivant : nous définissons la relation d'ordre entre fonctions croissantes $N \longrightarrow \mathbb{R}^+$,

$$\beta_1 \preceq \beta_2 \Longleftrightarrow (\exists c > 0 \ \exists a \in \mathbb{N}^* \ \forall m \in \mathbb{N}^* \ \beta_1(m) \leq c\beta_2(am)).$$

Deux fonctions β_1, β_2 sont équivalentes si $\beta_1 \preceq \beta_2$ et $\beta_2 \preceq \beta_1$.
Ainsi si A, A' sont deux parties génératrices finies de G, les fonctions $\beta_{G,A}$ et $\beta_{G,A'}$ sont équivalentes.

Le groupe G est dit à croissance polynomiale (de degré au plus d) si $\beta_G(m) \preceq m^d$.
Le groupe G est dit à croissance exponentielle si $\beta_G(m) \equiv e^m$.
Les groupes abéliens de type fini sont à croissance polynomiale de degré au plus le nombre de générateurs. Wolf a montré en 1968 que les groupes nilpotents de type fini sont à croissance polynomiale. Gromov a établi en 1981 qu'un groupe de type fini est à croissance polynomiale si et seulement si il possède un sous-groupe nilpotent d'indice fini.

Les paragraphes (5.1,5.2) sont consacrés à l'étude des groupes $\mathrm{GL}_n(\mathbb{Z})$, $\mathrm{SL}_n(\mathbb{Z})$, $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ qui fournissent (pour $n \geq 2$, $|k| > 4$) des familles de groupes non résolubles et qui donnent une démonstration constructive du théorème de structure des groupes abéliens de type fini.

5. Groupe linéaire

5.1. Groupe $\mathrm{GL}_n(\mathbb{Z})$. — Nous notons E_{ij} la matrice carrée dont tous les coefficients sont nuls, sauf celui situé à la i-ème ligne et la j-ème colonne, qui vaut 1. Dans cette notation (et par abus), nous n'avons pas précisé la taille de la matrice ni l'anneau des coefficients. Ces informations se déduisent naturellement du contexte.

Définition 5.1. — *Une opération élémentaire est la multiplication à droite ou à gauche par une matrice carrée dite élémentaire :*
- la multiplication à gauche par la matrice $\mathrm{Id} + aE_{ij}$, permet d'ajouter à la i-ème ligne la j-ème ligne multipliée par $a \in \mathbb{Z}$;
- la multiplication à droite par la matrice $\mathrm{Id} + aE_{ij}$, permet d'ajouter à la j-ème colonne la i-ème colonne multipliée par $a \in \mathbb{Z}$.

Par une suite d'opérations élémentaires, nous pouvons échanger deux lignes ou deux colonnes quitte à changer le signe d'une d'elles :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} L_i \\ L_i + L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_i \\ L_i + L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix}.$$

Nous pouvons également changer le signe de deux colonnes ou de deux lignes :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_i \\ -L_j \end{pmatrix}$$

Par une suite d'opérations élémentaires, nous obtenons de façon moins immédiate un algorithme conduisant à la décomposition suivante :

Lemme 5.2. — *(Forme normale de Smith) Soit A une matrice $m \times n$ à coefficients dans $\mathbb{Z}$. Il existe des matrices $P \in \mathrm{GL}_m(\mathbb{Z})$ et $Q \in \mathrm{GL}_n(\mathbb{Z})$ telles que*

$$PAQ = \begin{pmatrix} d_1 & & & & & & \\ & \cdots & & & & & \\ & & d_r & & & & \\ & & & 0 & & & \\ & & & & \cdots & & \\ & & & & & 0 \quad \cdots & 0 \end{pmatrix}$$

où $d_1, \ldots, d_r$ sont des entiers positifs satisfaisants $d_1 | \cdots | d_r$, appelés facteurs invariants de la matrice A. Ils sont entièrement déterminés par A.

Démonstration. — La réduction s'effectue par récurrence sur la taille de la matrice A.
Etape 1 Soit α_1 le pgcd (positif) des coefficients de la première colonne. Nous appliquons des opérations élémentaires sur les lignes pour obtenir une première colonne C_1 dont tous les coefficients sont nuls, sauf le coefficient a_{11} qui sera égal à $\pm\alpha_1$. Faisons-le sur les deux premiers coefficients a_{11} et a_{21}. Quitte à échanger les deux premières lignes, nous pouvons supposer $|a_{11}| \geq |a_{21}|$.
Si $a_{21} = 0$, il n'y a rien à faire ;
sinon effectuons la division euclidienne $a_{11} = ba_{21} + c$ avec $0 \leq c < |a_{21}|$ et remplaçons C_1 par $C_1 - bC_2$;
Ainsi les coefficients (a_{11}, a_{21}) sont remplacés par (c, a_{21}) avec $|a_{21}| + |c| < |a_{11}| + |a_{21}|$. En itérant, l'algorithme d'Euclide garantit qu'en un nombre fini d'étape, nous avons remplacé (a_{11}, a_{21}) par $(\mathrm{pgcd}(a_{11}, a_{21}), 0)$. En répétant ce procédé sur chaque ligne, nous obtenons une matrice dont la première colonne est de la forme

$$\begin{pmatrix} \pm\alpha_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Etape 2 La même méthode peut être appliquée à la première ligne de telle façon à obtenir une matrice dont la première ligne est de la forme

$$\begin{pmatrix} \pm\alpha_2 & 0 & \cdots & 0 \end{pmatrix}$$

où α_2 est le pgcd des coefficients de la première ligne. Cependant, la première colonne a pu être modifiée par ces opérations successives. Néanmoins $0 \leq \alpha_2 \leq \alpha_1$. En réitérant ce processus, la suite $0 \leq \cdots \leq \alpha_3 \leq \alpha_2 \leq \alpha_1$ se stabilise : nous obtenons une matrice dont la première ligne est

$$\begin{pmatrix} \pm\delta_1 & 0 & \cdots & 0 \end{pmatrix}$$

où δ_1 est aussi un pgcd des coefficients de la première colonne, donc divise tous les coefficients de la première colonne. Il suffit alors de soustraire à chaque ligne

un multiple adéquat de la première ligne pour arriver à une matrice de la forme

$$\begin{pmatrix} \pm\delta_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}.$$

Etape 3 En appliquant la récurrence sur la matrice A', nous obtenons une matrice de la forme

$$\begin{pmatrix} \pm\delta_1 & & & & & & 0 \\ & \delta_2 & & & & & \\ & & \ddots & & & & \\ & & & \delta_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \end{pmatrix}$$

avec $\delta_2 | \cdots | \delta_r$. Nous pouvons enfin remplacer, via des opérations élémentaires le couple (δ_1, δ_2) par (d_1, m_2) avec $d_1 = \text{pgcd}(\delta_1, \delta_2)$,$m_2 = \text{ppcm}(\delta_1, \delta_2)$. En effet, d'après Bezout, il existe $u, v \in \mathbb{Z}$ avec $u\delta_1 + v\delta_2 = d_1$, puis nous effectuons des suites d'opérations élémentaires permettant de modifier les coefficients comme suit

$$\begin{pmatrix} \delta_1 & 0 \\ 0 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \delta_1 & 0 \\ -u\delta_1 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \delta_1 & 0 \\ -u\delta_1 - v\delta_2 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & -\delta_2 \\ \delta_1 & 0 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} d_1 & -\delta_2 \\ 0 & m_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & 0 \\ 0 & m_2 \end{pmatrix}.$$

Il suffit alors de procéder par induction sur les couples successivement modifiés

$$(m_2, \delta_3) \leftarrow (\text{pgcd}(m_2, \delta_3), \text{ppcm}(m_2, \delta_3))...$$

Ainsi nous obtenons une matrice de la forme voulue avec $d_1 | \ldots | d_r$.
Pour garantir la positivité des signes des d_i, nous pouvons changer les signes deux à deux via une suite d'opérations élémentaires. Seul d_r peut encore être négatif (et uniquement pour $m = n = r$). Si $d_r < 0$, il suffit de multiplier à droite par $\text{Id} - 2E_{rr}$ (c'est la seule fois que nous multiplions par une matrice de déterminant -1).
Les matrices P et Q du lemme 5.2 s'obtiennent comme produt de matrices correspondant aux opérations réalisées sur les lignes (resp. colonnes).
Enfin l'unicité des d_i s'obtient en constatant que pour $1 \leq k \leq r$,

$$d_1 \cdots d_k = \text{pgcd(mineurs d'ordre } k \text{ de } A).$$

En effet les pcgd des mineurs d'ordre fixé d'un matrice sont inchangés par multiplication à gauche ou à droite par une matrice élémentaire.

□

Remarque 5.3. — *La détermination de la forme normale de Smith est implémentée sous sage. Il est cependant raisonnable de chercher à l'implémenter directement*

sous Python.

```
sage:  A=matrix(ZZ,4,[1,2,3,4,5,6,7,8,9,10,11,12, 0,2,4,8])
sage:  A
[1 2 3 4]
[5 6 7 8]
[9 10 11 12]
[0 2 4  8]
sage:  [D,P,Q]=A.smith_form()
sage:  D,P,Q
(
[1 0 0 0] [0 2  − 1 0] [−3 2 4 1]
[0 2 0 0] [0 0 0 1] [4  − 3  − 4  − 2]
[0 0 4 0] [0  − 1 1 0] [0 0 0 1]
[0 0 0 0], [1  − 2 1 0], [−1 1 1 0]
)
```

Remarque 5.4. — *La démonstration constructive du lemme 5.2 s'adapte sans peine au cas des matrices à coefficients dans un corps (car nous pouvons diviser par tout élément non nul) et dans un anneau euclidien. Le résultat est plus généralement valable sur tout anneau principal.*

Cette décomposition sous forme normale de Smith permet de retrouver le théorème de structure des groupes abéliens de type fini comme corollaire du théorème suivant :

Corollaire 5.5. — *(Théorème de la base adaptée). Soit H un sous-groupe d'un groupe abélien G libre de rang fini s. Alors H est libre de rang fini $r \leq s$ et il existe une base $(e_1, \ldots, e_s)$ de G et des entiers $d_1, \ldots, d_r$ tels que*
- $(d_1 e_1, \ldots, d_r e_r)$ est une base de H,
- $d_1 | \cdots | d_r$.

Démonstration. — Soit $(x_1, \ldots, x_s)$ une base de G et $(y_1, \ldots, y_n)$ des générateurs de H. Ainsi il existe une matrice $A = (a_{ij})$ de taille $s \times n$ à coefficients dans $\mathbb{Z}$ telle que $y_j = \sum_{i=1}^{s} a_{ij} x_i$, $1 \leq j \leq n$.
Soient P, Q les matrices issues de la décomposition de A sous forme normale de Smith dans le lemme 5.2. Notons $(\varepsilon_1, \ldots, \varepsilon_n)$ la base standard de $\mathbb{Z}^n$ et $f : \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^s \xrightarrow{\Phi\sim} G$ le morphisme d'image H qui envoie ε_j sur y_j. Considérons la factorisation de $f \circ Q$:

$$\mathbb{Z}^n \xrightarrow{Q\sim} \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^s \xrightarrow{P\sim} \mathbb{Z}^s \xrightarrow{P^{-1}\sim} \mathbb{Z}^s \xrightarrow{\Phi\sim} G$$

L'isomorphisme $\Phi \circ P^{-1} : \mathbb{Z}^s \xrightarrow{\sim} G$ correspond à une nouvelle base $(e_1, \ldots, e_s)$ de G et $H = \mathrm{Im}(f \circ Q)$ est alors engendré par $(d_1 e_1, \ldots, d_r e_r)$. Comme ces éléments forment une famille libre, c'est une base de H. □

Corollaire 5.6. — *Soit G un groupe abélien de type fini. Il existe des entiers r et s et $1 < d_1 | \cdots | d_r$ tels que*

$$G \simeq \mathbb{Z}^s \times \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}.$$

Démonstration. — Comme G est de type fini, il existe un morphisme surjectif

$$\psi : \mathbb{Z}^t \longrightarrow G.$$

D'après le corollaire 5.5, il existe une base $(e_1, \ldots, e_t)$ de $\mathbb{Z}^t$ telle que $(d_1 e_1, \ldots, d_r e_r)$ soit une base de $\ker \psi$. D'où

$$G \simeq \mathbb{Z}^t / \ker \psi = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{t-r}.$$

En retirant les d_i égaux à 1, nous obtenons l'existence de la décomposition de G. □

Si $A \in \mathrm{GL}_n(\mathbb{Z})$, le lemme 5.2 donne une écriture sous la forme $A = P\,\mathrm{Id}\,Q$ avec P, Q produits de matrices correspondant aux opérations réalisées sur les lignes (resp. colonnes). Ces opérations sont de deux types :
- la mutiplication à gauche (à droite) par la matrice élémentaire $\mathrm{Id} + aE_{ij}$ et
- l'échange de deux lignes ou colonnes $\mathrm{Id} + E_{ij} - E_{ii} - E_{jj}$, pour $1 \leq i, j \leq n$, $i \neq j$.

Les opérations élémentaires du premier type ne changent pas le déterminant, au contraire de celles du deuxième type. Nous remplaçons les secondes par l'échange de deux lignes ou colonnes, suivi du changement de l'une d'elles en son opposé, soit la mutiplication par $\mathrm{Id} - 2E_{ij}$. L'algorithme du lemme 5.2 fonctionne toujours de même, mais nous ne pouvons plus assurer que d_r soit positif. Lorsque $A \in \mathrm{GL}_n(\mathbb{Z})$, la matrice finale obtenue est

$$A = P \begin{pmatrix} 1 & & & \\ & \cdots & & \\ & & 1 & \\ & & & \det(A) \end{pmatrix} Q.$$

Corollaire 5.7. — *Le groupe $\mathrm{SL}_n(\mathbb{Z})$ est de type fini. Il est engendré par les matrices élémentaires $\mathrm{Id} + E_{ij}$, $1 \leq i, j \leq n$, $i \neq j$.*
Le groupe $\mathrm{GL}_n(\mathbb{Z})$ est de type fini. Il est engendré par
- les matrices élémentaires $\mathrm{Id} + E_{ij}$, $1 \leq i, j \leq n$, $i \neq j$,
- et la matrice $\mathrm{Id} - 2E_{nn}$.

Démonstration. — Pour tout $a \in \mathbb{Z}$, $\mathrm{Id} + aE_{ij} = (\mathrm{Id} + E_{ij})^a \in < \mathrm{Id} + E_{ij} >$. □

Exemple 5.8. — *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par les deux matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Exemple 5.9. — *Supposons* $n \geq 2$. *En calculant les produits de la forme* $A(\mathrm{Id}+E_{ij})$ *et* $(\mathrm{Id}+E_{ij})A$, *nous établissons aisément :*
Le centre de $\mathrm{GL}_n(\mathbb{Z})$ *est réduit aux homothéties,* $Z(\mathrm{GL}_n(\mathbb{Z})) \simeq \{\pm \mathrm{Id}\}$. *Le centre de* $\mathrm{SL}_n(\mathbb{Z})$ *est réduit à l'identité si* n *impair et* $\{\pm \mathrm{Id}\}$ *si* n *pair.*

Remarque 5.10. — *En utilisant les matrices élémentaires, nous pouvons montrer que* $\mathrm{SL}_n(\mathbb{Z})$ *n'est pas résoluble pour* $n \geq 2$ *(voir Exemple 5.13). De plus, pour* $n \geq 3$, *le groupe dérivé* $D(\mathrm{SL}_n(\mathbb{Z}))$ *est* $\mathrm{SL}_n(\mathbb{Z})$. *En revanche, pour* $n = 2$, $[\mathrm{SL}_2(\mathbb{Z}) : D(\mathrm{SL}_2(\mathbb{Z}))] = 12$.

5.2. Le groupe linéaire. — Soit k un corps. D'après le lemme 5.2, nous avons

Corollaire 5.11. — *Le groupe* $\mathrm{GL}_n(k)$ *est engendré par les matrices élémentaires* $\mathrm{Id}+\alpha E_{ij}$, $1 \leq i, j \leq n$, $i \neq j$, $\alpha \in k$ *et les matrices* $Id + (\beta - 1)E_{nn}$, $\beta \in k^\times$. *De plus* $Z(\mathrm{GL}_n(k)) \simeq k^\times$.
Le groupe $\mathrm{SL}_n(k)$ *est engendré par les matrices élémentaires* $\mathrm{Id}+\alpha E_{ij}$, $1 \leq i, j \leq n$, $i \neq j$, $\alpha \in k$. *De plus* $Z(\mathrm{SL}_n(k)) \simeq \mu_n(k) = \{\lambda \in k | \lambda^n = 1\}$.

Proposition 5.12. — *Soit* k *un corps et* $n \geq 2$.
i. On a $D(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$ *sauf si* $n = 2$ *et* $k = \mathbb{F}_2$ *ou* $\mathbb{F}_3$.
ii. On a $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$ *sauf si* $n = 2$ *et* $k = \mathbb{F}_2$.

Démonstration. — Le déterminant d'un commutateur est 1, donc le groupe dérivé de $\mathrm{GL}_n(k)$ est toujours inclus dans $\mathrm{SL}_n(k)$. Pour montrer qu'il est égal, on montre que le groupe dérivé contient toutes les matrices élémentaires $\mathrm{Id}+\alpha E_{ij}$, $1 \leq i, j \leq n$, $i \neq j$, $\alpha \in k$.
Si $n \geq 3$, pour $1 \leq i, j, k \leq n$ distincts, vu que $(\mathrm{Id}+\alpha E_{ij})^{-1} = \mathrm{Id}-\alpha E_{ij}$, nous avons

$$(I_n + \alpha E_{ij})(\mathrm{Id}+\beta E_{jk})(\mathrm{Id}+\alpha E_{ij})^{-1}(\mathrm{Id}+\beta E_{jk})^{-1} = \mathrm{Id}-\alpha\beta E_{ik}$$

Lorsque $n = 2$, il suffit de montrer que $\mathrm{Id}+\alpha E_{12}$ (et $I_2 + \alpha E_{21}$ par symétrie) est un commutateur. Pour $\beta \notin \{0, 1, -1\}$ (donc $|k| > 3$), on a

$$\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}\begin{pmatrix} 1 & \frac{\alpha}{\beta^2-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \frac{\alpha}{\beta^2-1} \\ 0 & 1 \end{pmatrix}^{-1} = \mathrm{Id}+\alpha E_{12}.$$

Donc $D(\mathrm{SL}_n(k)) = \mathrm{SL}_n(k)$.
Pour $\beta \notin \{0, 1\}$, donc $|k| > 2$, on a

$$\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \frac{\alpha}{\beta-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & \frac{\alpha}{\beta-1} \\ 0 & 1 \end{pmatrix}^{-1} = \mathrm{Id}+\alpha E_{12}.$$

Donc $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$.

□

Exemple 5.13. — *Pour $n \geq 3$ et ou $n = 2$ et $|k| \geq 4$, les groupes $\mathrm{SL}_n(k)$ et $\mathrm{GL}_n(k)$ ne sont pas résolubles. Lorsque k est fini, il s'agit de groupes finis non résolubles. Ils admettent donc des facteurs simples non cycliques dans leurs suites de composition.*
Pour $n \geq 2$, le groupe $\mathrm{SL}_n(\mathbb{Z})$ n'est pas résoluble. En effet l'application de réduction modulo 5

$$\mathrm{SL}_n(\mathbb{Z}) \longrightarrow \mathrm{SL}_n(\mathbb{Z}/5\mathbb{Z})$$

est surjective et le groupe $\mathrm{SL}_n(\mathbb{Z}/5\mathbb{Z})$ n'est pas résoluble.

Remarque 5.14. — *Nous verrons plus loin que $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ dont le groupe dérivé est $\mathfrak{A}_3$. Par ailleurs $D(\mathrm{SL}_2(\mathbb{F}_3))$ est le groupe des quaternions d'ordre 8, il est d'indice 3 dans $\mathrm{SL}_2(\mathbb{F}_3)$.*

Remarque 5.15. — *Le groupe $\mathrm{GL}_n(\mathbb{R})$ (resp. $\mathrm{SL}_n(\mathbb{R})$) est une variété différentiable de dimension n^2 (resp. $n^2 - 1$).*
Le groupe $\mathrm{GL}_n(\mathbb{C})$ (resp. $\mathrm{SL}_n(\mathbb{C})$) est une variété complexe de dimension n^2 (resp. $n^2 - 1$).

6. Présentation par générateurs et relations

Le théorème de structure des groupes abéliens de type fini, donne une présentation très simple de

$$G \simeq \mathbb{Z}^r \times \Pi_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$$

via une famille de générateurs $(a_i)_{1 \leq i \leq r+s}$ satisfaisant les relations

$$a_i^{d_i} = e, 1 \leq i \leq s, \;\; a_i a_j a_i^{-1} a_j^{-1} = e, 1 \leq i, j \leq s + r.$$

De même l'éude du groupe linéaire est facilitée par la connaissance d'un système de générateurs. L'objet de cette section est de formaliser et généraliser ces descriptions explicites des groupes.

6.1. Générateurs et relations. —

Définition 6.1. — *Soit $\mathcal{A}$ un ensemble dit alphabet. Les éléments de $\mathcal{A}$ sont appelés lettres. Le groupe libre $\mathcal{L}(\mathcal{A})$ est défini de la façon suivante :*
- les éléments de $\mathcal{L}(\mathcal{A})$ sont les suites finies (dites mots) d'éléments de la forme a ou a'^{-1} pour $a, a' \in \mathcal{A}$,
- l'opération sur $\mathcal{L}(\mathcal{A})$ est donnée par la concaténation des mots. Elle est associative (mais pas abélienne), l'élément neutre noté e est le mot vide.
Soit $\mathcal{R}$ un sous-ensemble du groupe $\mathcal{L}(\mathcal{A})$, et $\mathcal{H}$ le sous-groupe normal engendré par $\mathcal{R}$. Le groupe quotient $\mathcal{L}(\mathcal{A})/\mathcal{H}$ est le groupe défini par les générateurs $\mathcal{A}$ et les relations $\mathcal{R}$; il est noté $\mathcal{L}(\mathcal{A})/\mathcal{R}$.
Si $\mathcal{A}$ est fini, le groupe $\mathcal{L}(\mathcal{A})/\mathcal{R}$ est dit de type fini. Si, de plus $\mathcal{R}$ est fini, le groupe $\mathcal{L}(\mathcal{A})/\mathcal{R}$ est dit de présentation finie.

Exemple 6.2. — *Pour $\mathcal{A} = \{a\}$, le groupe libre à un générateur est $\mathcal{L}(a) = \mathbb{Z}$. Si $\mathcal{R} = \{a^n\}$ pour $n \in \mathbb{N}^*$, alors $\mathcal{L}(\mathcal{A})/\mathcal{R} = C_n$.*
Le groupe diédral $D_n = \mathcal{L}(r,s)/\{r^n, s^2, srsr\}$.
Le groupe des quaternions généralisés est $Q_n = \mathcal{L}(a,b)/\{a^{2^{n-1}}, a^{2^{n-2}}b^{-2}, bab^{-1}a\}$. Pour $n = 3$, c'est le groupe classique des quaternions. En général, il est d'ordre 2^n.

Exemple 6.3. — *Le groupe abélien libre de générateurs $a_1, \ldots, a_n$ a pour relations $[a_i, a_j]$, $i \neq j$.*

Exemple 6.4. — *Un groupe fini G est de présentation finie. En effet pour $\mathcal{A} = G$ et $\mathcal{R} = \{abc^{-1} | ab = c \in G\}$, alors G est isomorphe à $\mathcal{L}(\mathcal{A})/\mathcal{R}$.*

Exemple 6.5. — *Soit G un groupe et $\mathcal{L}(\mathcal{A})$ un groupe libre. Pour définir un morphisme de groupes $\mathcal{L}(\mathcal{A}) \longrightarrow G$, il suffit de déterminer l'image des générateurs $a \in \mathcal{A}$.*
Soit $\mathcal{R}$ un ensemble de relations. Pour tout groupe G et pour toute application $f : \mathcal{A} \longrightarrow G$ qui envoie tout élément de $\mathcal{R}$ sur e_G, il existe un unique morphime de groupes $\bar{f} : \mathcal{L}(\mathcal{A})/\mathcal{R} \longrightarrow G$ qui factorise f.

Remarque 6.6. — *Soit $G = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$ et soit S, T les éléments of G:*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Alors $G = \mathcal{L}(S, ST)/\{S^2, (ST)^3\}$.

Il n'est pas toujours aisé de reconnaître un groupe, ou même de décrire certaines de ses propriétés à partir de sa présentation par générateurs et relations.

Remarque 6.7. — *Soit $G = \mathcal{L}(x,y)/\{x^m, y^n\}$. Alors x est d'ordre m, y est d'ordre n et xy est d'ordre infini.*
Soit $G = \mathcal{L}(x,y)/\{x^m, y^n, (xy)^r\}$ avec $m, n, r > 1$. Alors G est fini ou infini suivant le triplet (m,n,r) (voir les groupes de von Dyck).

```
sage:  F.<x,y> = FreeGroup()
sage:  G = F / [x^2, y^4, x*y*x*y*x*y]
sage:  G
Finitely presented group < x, y | x^2, y^4, (x*y)^3 >
sage:  G.order()
24
```

Remarque 6.8. — *(Le problème des mots). Soit $G = \mathcal{L}(\mathcal{A})/\mathcal{R}$ avec $\mathcal{A}$ fini. Le problème des mots pour G est le suivant : existe-t-il un algorithme pour décider si un mot (non vide) de $\mathcal{A}$ représente e dans G. La réponse négative est due à Novikov et Boone. Plus généralement, nous pouvons nous poser les questions suivantes : existe-t-il un algorithme qui détermine pour une presentation finie*

si le groupe correspondant est trivial, abélien, résoluble, simple, de torsion, sans torsion, libre ?...

Remarque 6.9. — *(Problème de Burnside). Un groupe est d'exposant t si $g^t = e$ pour tout $g \in G$ et $t > 0$ est le plus petit entier satisfaisant cette propriété. Il existe des groupes infinis engendrés par un nombre fini d'éléments d'ordre fini. Existe-t-il des groupes infinis de type fini et d'exposant fini ?*
Le groupe de Burnside d'exposant t à r générateurs $B(r,t)$ est le quotient du groupe libre à r générateurs par le sous-groupe engendré par toutes les puissances t-ièmes. Le problème de Burnside consiste à déterminer quand $B(r,t)$ est fini.

Remarque 6.10. — *(Groupes de Coxeter) Un système de Coxeter est une paire G, S composée d'un groupe et d'un ensemble de générateurs S de G soumis aux relations de la forme $(ss')^{m(s,s')} = e$, où*

$$\begin{cases} m(s,s) = 1 & s \in S, \\ m(s,s') \geq 2 & s \neq s' \in S, \\ m(s,s') = m(s',s). \end{cases}$$

S'il n'y a pas de relation entre s et s', nous posons $m(s,s') = \infty$. Soit $\mathcal{R} = \{(ss')^{m(s,s')} | m(s,s') < \infty\}$. Un groupe de la forme $\mathcal{L}(S)/\mathcal{R}$ est dit groupe de Coxeter. Le rang du système de Coxeter est défini comme le cardinal de S.
La finitude d'un groupe de Coxeter peut-être déterminée via la théorie des graphes.

6.2. Systèmes générateurs d'un groupe : Applications. — Nous donnons dans ce paragraphe deux exemples illustrant le lien entre groupe et topologie. D'une part, nous pouvons associer un groupe à un espace topologique. D'autre part nous pouvons définir une structure métrique sur un groupe via le choix d'un système de générateurs. Nous omettons les démonstrations (pourtant accessibles) des résultats présentés ici.

6.2.1. Groupe d'homotopie. —

Remarque 6.11. — *En topologie, nous considérons les chemins fermés orientés, dits lacets, dans le plan privé de n points $\mathfrak{E} = \mathbb{R}^2 - \{M_1, \ldots, M_n\}$, partant et revenant à l'origine O. Nous définissons une relation d'équivalence, dite d'homotopie, sur les lacets : deux chemins obtenus par déformation continue dans $\mathfrak{E}$ sont dits homotopes. Nous pouvons inverser un chemin en le parcourant en sens inverse et composer deux lacets en les parcourant consécutivement, opérations compatibles avec l'homotopie. Ceci munit l'ensemble des classes d'homotopie d'une structure de groupe, dit groupe d'homotopie $\pi_1(\mathfrak{E})$. Le groupe d'homotopie $\pi_1(\mathfrak{E})$ est un groupe libre engendré par les lacets élémentaires $\ell_1, \ldots, \ell_n$ n'inserant respectivement que $M_1, \ldots, M_n$.*
De façon analogue, nous définissons le groupe d'homotopie du tore T qui est engendré par deux générateurs a, b et une relation $ab = ba$. Ainsi $\pi_1(T) = \mathbb{Z} \times \mathbb{Z}$.

6.2.2. Graphe de Cayley. —

Définition 6.12. — *Un système S de générateurs d'un groupe G est dit symétrique si tout élément de S a son inverse dans S.*
Soit G un groupe et S un système de générateurs symétrique de G. La longueur $\ell_S(g)$ d'un élément g de G est la plus petite longueur d'une suite $s_1, \ldots, s_n$ d'éléments de S tels que $g = s_1 \cdots s_n$, avec par convention $\ell_S(e) = 0$.
Nous définissons une distance d_S, dite distance des mots, sur G :

$$d_S : G \times G \longrightarrow \mathbb{R}, (g, h) \mapsto \ell_S(g^{-1}h).$$

Il s'agit alors de vérifier que (G, d_S) est un espace métrique : $\forall f, g, h \in G$
- $d_S(g, h) \geq 0$ avec égalité si et seulement si $g = h$,
- $d_S(g, h) = d_S(h, g)$,
- $d_S(g, h) \leq d_S(g, f) + d_S(f, h)$.

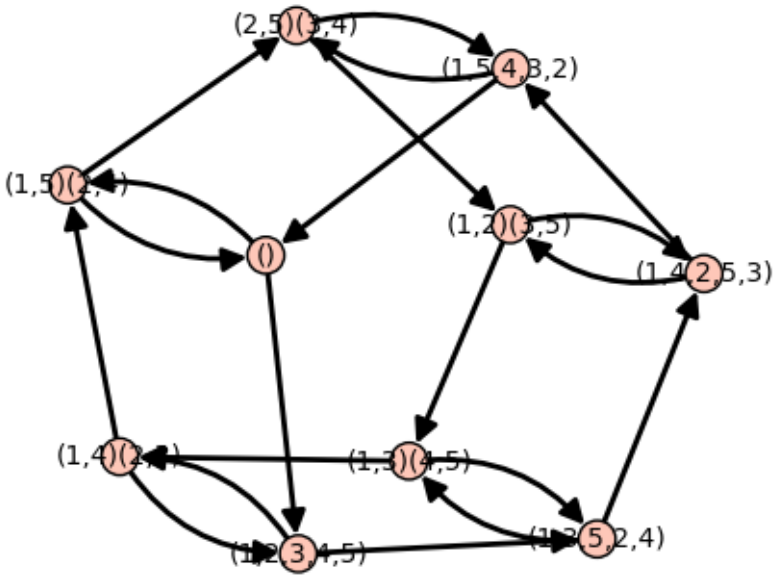
Définition 6.13. — *Soit G un groupe et S un sytème de générateurs symétrique. Le graphe de Cayley de (G, S) est le graphe dont les sommets sont les éléments de G, avec une arête entre g et h si et seulement si, $d_S(g, h) = 1$.*

Un groupe peut avoir deux graphes de Cayley différents et deux groupes différents peuvent avoir le même graphe de Cayley. Ces objets mathématiques interviennent notamment dans le cadre des marches aléatoires.

```
sage:  D5 = DihedralGroup(5)
sage:  D5.gens()
```

$[(1, 2, 3, 4, 5), (1, 5)(2, 4)]$

```
sage:  C = [D5.gen(0), D5.gen(1)]
sage:  CD5 = D5.cayley_graph( generators = C)
CD5.show()
```


(2,5)(3,4)
(1,5)(4,3,2)
(1,5)(2,4)
()
(1,2)(3,5)
(1,4,2,5,3)
(1,4)(2,5)
(1,3)(4,5)
(1,2,3,4,5)
(1,5,2,4)

PARTIE II

ACTIONS DE GROUPES

7. Groupes opérant sur un ensemble

7.1. Définitions. — "Les groupes sont faits pour agir." (P. Colmez). Faire agir un groupe G sur un ensemble E muni d'une certaine structure est un moyen efficace d'obtenir des informations sur la structure du groupe G et sur celle de l'ensemble E considéré.

7.2. Définitions et exemples. —

Définition 7.1. — *Un groupe G opère sur un ensemble E si nous disposons d'un morphisme de groupes*

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

Lorsque ρ est injectif, nous disons que G opère fidèlement fidèle.

Si G opère fidèlement sur E alors nous pouvons décrire le groupe abstrait G de façon concrète comme sous-groupe de $\mathrm{Bij}(E)$.

Exemple 7.2. — *Pour tout ensemble E, le groupe $\mathrm{Bij}(E)$ opère fidèlement sur E. En particulier le groupe symétrique $\mathfrak{S}_n$ opère sur l'ensemble $\{1, \ldots, n\}$.*

Exemple 7.3. — *Soit k un corps et $n \geq 1$. Le groupe $\mathrm{GL}_n(k)$ opère fidèlement sur k^n.*

Exemple 7.4. — *Soit G un groupe, H un sous-groupe de G. Le groupe H opère fidèlement sur G par translation à gauche :*

$$\rho : H \longrightarrow \mathrm{Bij}(G),\ h \mapsto \rho(h)(g) = hg.$$

Si G est fini, nous en déduisons un morphisme injectif $G \longrightarrow \mathfrak{S}_{|G|}$ (qui dépend de la façon dont nous numérotons les éléments de G).

Exemple 7.5. — *Le groupe des automorphismes $\mathrm{Aut}(G)$ opère fidèlement sur le groupe G.*

Exemple 7.6. — *Le groupe $\mathrm{SL}_2(\mathbb{R})$ opère sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$ par*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Le groupe $\mathrm{SL}_2(\mathbb{R})$ n'opère pas fidèlement car le noyau de $\mathrm{SL}_2(\mathbb{R}) \longrightarrow \mathrm{Bij}(\mathcal{H})$ est $\{\pm \mathrm{Id}\}$.

Remarque 7.7. — *Une action à gauche d'un groupe G sur un ensemble E est la donnée d'une application*

$$L : G \times E \longrightarrow E, (g, x) \mapsto g \cdot x$$

telle que $e \cdot x = x$, $x \in E$ et pour tous $x \in E$, $g_1, g_2 \in G$ nous avons $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$.
Une action à droite d'un groupe G sur une ensemble E est la donnée d'une application

$$R : G \times E \longrightarrow E, (g, x) \mapsto x \cdot g$$

telle que $e \cdot x = x, x \in E$ et pour tous $x \in E$, $g_1, g_2 \in G$ nous avons $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$.
Une groupe G opère sur un ensemble E, si et seulement si, il définit une action à gauche (ou à droite) sur E (il suffit de poser $x \cdot g^{-1} = L(g)(x)$, le passage à l'inverse permet de replacer les éléments dans le bon ordre).

Définition 7.8. — *L'orbite d'un point $x \in E$ sous l'action de G est*

$$\mathcal{O}_x = \{\rho(g)(x), g \in G\}.$$

S'il n'y a qu'une seule orbite ($\mathcal{O}_x = E$) i.e. si pour tout couple $(x, y) \in E \times E$ il existe $g \in G$ avec $\rho(g)(x) = y$, alors G opère transitivement sur E.

Remarquons que si G opère transitivement sur E, pour tout $x, y \in E$, $\mathcal{O}_x = \mathcal{O}_y = E$.

Remarque 7.9. — *Pour $n > 0$, une action de G sur E est dite n-transitive si pour tous n-uplets d'éléments distincts de E, $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$, il existe $g \in G$ avec $\rho(g)(x_i) = y_i$, $1 \leq i \leq n$.*

Définition 7.10. — *Le groupe G opère sur lui-même par conjugaison :*

$$\rho : G \longrightarrow \mathrm{Bij}(G) : g \mapsto \rho(g)(x) = gxg^{-1}.$$

Les orbites sont appelées classes de conjugaison de G.

Un groupe est abélien si et seulement si ses classes de conjugaison sont des singletons. De façon générale, les classes de conjugaison joue un rôle important en théorie des représentations (Partie III) car donnent des informations fines sur la structure du groupe.

Définition 7.11. — *Le stabilisateur d'un point $x \in E$ sous l'action de G est*

$$\mathrm{Stab}(x) = \{g \in G | \rho(g)(x) = x\}.$$

Proposition 7.12. — *Soit G un groupe opérant sur un ensemble E. Soit $x \in E$. Alors* $\mathrm{Stab}(x)$ *est un sous-groupe de G et l'ensemble des classes à gauche* $G/\mathrm{Stab}(x)$ *est en bijection avec $\mathcal{O}_x$. En particulier, si G est fini*

$$[G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)| = |\mathcal{O}_x|.$$

Démonstration. — Le stabilisateur $\mathrm{Stab}(x)$ est clairement un sous-groupe de G. L'application $G \longrightarrow \mathcal{O}_x$, $g \mapsto \rho(g)(x)$ est surjective et deux éléments g_1, g_2 de G ont la même image si et seulement si ils appartiennent à la même classe à gauche de G modulo le sous-groupe $\mathrm{Stab}(x)$. □

En particulier si G fini agit transitivement sur E, alors $|E|$ divise $|G|$.
Le sous-groupe $\mathrm{Stab}(x)$ n'est pas forcément normal (en général $G/\mathrm{Stab}(x)$ n'est pas un groupe). Précisément, pour $y \in \mathcal{O}_x$, il existe $h \in G$ tel que $y = \rho(h)(x)$ et

$$\mathrm{Stab}(y) = h\,\mathrm{Stab}(x)h^{-1}.$$

Exemple 7.13. — *Soit G un groupe et H un sous-groupe de G. Le groupe G opère sur l'ensemble des classes à gauche de H dans G :*

$$\rho : G \longrightarrow \mathrm{Bij}(G/H), \rho(g)(g'H) = gg'H.$$

Pour tout $g \in G$,

$$\mathrm{Stab}(gH) = g\,\mathrm{Stab}(H)g^{-1} = gHg^{-1}$$

et le noyau de ρ est le plus grand sous-groupe normal de G contenu dans H:

$$\ker \rho = \cap_{g\in G} gHg^{-1}.$$

De ces définitions et propriétés élementaires sur les opérations de groupes, il faut retenir cet échange d'informations entre le groupe (objet algébrique qui permet de faire des calculs) et les orbites (objets géométriques).

Remarque 7.14. — *Soit k un corps. Le groupe $k^\times$ opère sur $k^n - \{0\}$*

$$k^* \longrightarrow \mathrm{Bij}(k^n - \{0\}), \;\; \lambda \mapsto (x_1, \ldots, x_n) \mapsto (\lambda x_1, \ldots, \lambda x_n).$$

L'ensemble des orbites (i.e un système de représentant des orbites)

$$\mathbb{P}^{n-1}(k) = \{\textit{droites vectorielles de } k^n\}$$

est appelé espace projectif.
En particulier $\mathbb{P}^1(k) \simeq k \cup \{\infty\}$. Pour $k = \mathbb{R}$, $\mathbb{P}^1(\mathbb{R})$ est isomorphe au cercle unité S^1. Pour $k = \mathbb{C}$, $\mathbb{P}^1(\mathbb{C}) \simeq \mathbb{C} \cup \{\infty\} \simeq \mathbb{R}^2 \cup \{\infty\} \simeq \mathrm{S}^2$.

http://images.math.cnrs.fr/

Pour $n \geq 2$, $\mathbb{P}^n(\mathbb{R}) = \mathrm{S}^n/\{x \sim -x\}$ est une variété analytique réelle compacte de dimension n.

7.3. Équation aux classes. —

Proposition 7.15. — *(Équation aux classes). Soit G un groupe opérant sur un ensemble E. Les orbites de E sous l'action de G forment une partition de E, $E = \coprod_{x \in X} \mathcal{O}_x$, où X désigne un système de représentants des différentes orbites de E. Ainsi, lorsque E est fini,*

$$|E| = \sum_{x \in X} |\mathcal{O}_x|.$$

Corollaire 7.16. — *(Théorème de Cauchy). Si un nombre p divise $|G|$, alors G contient un élément d'ordre p.*

Démonstration. — En effet G opère sur lui-même par conjugaison. L'équation aux classes s'écrit

$$|G| = |Z(G)| + \sum_{x \in X'} |\mathcal{O}_x|$$

où X' est un système de représentants des classes de conjugaison non réduite à un élément. Si pour $y \notin Z(G)$, p ne divise pas $|\mathcal{O}_y| = |G|/|\operatorname{Stab}(y)|$ alors p divise $|\operatorname{Stab}(y)|$ et nous pouvons raisonner par récurrence et chercher un élément d'ordre p dans $\operatorname{Stab}(y)$. Ainsi, nous pouvons supposer que G' est un sous-groupe de G d'ordre divisible par p qui agit sur lui-même par conjugaison avec

$$|G'| = |Z(G')| + \sum_{x \in X''} |\mathcal{O}_x|$$

et p divise tous les termes $|\mathcal{O}_x|$, donc p divise $|Z(G')|$. Ainsi $Z(G')$ est un groupe abélien d'ordre divisible par p donc contient un élément d'ordre p. Donc G',

sous-groupe de G admet un élément d'ordre p. Donc G admet un élément d'ordre p. □

Remarquons que l'élément d'ordre de p de G construit dans la preuve du théorème de Cauchy n'appartient pas forcément au centre $Z(G)$ (mais au centre d'un sous-groupe de G). En revanche, lorsque G est un p-groupe, il existe un élément d'ordre p dans $Z(G)$ (voir lemme 8.2).

Exemple 7.17. — *Un groupe d'ordre $2p$ avec p premier impair est cyclique ou diédral.*
En effet d'après le théorème de Cauchy, G contient un élément s d'ordre 2 et un élément r d'ordre p. Le sous-groupe $H =< r >$ est d'indice 2 donc normal et $s \notin H$. Donc $G = H \coprod Hs$ et comme H est normal, il existe $i \in \mathbb{N}$, $srs^{-1} = r^i$. Or $s^2 = e$, $r = s^2rs^{-2} = s(srs^{-1})s^{-1} = r^{i^2}$ donc $i^2 \equiv 1 \mod p$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, ses seuls éléments de carré 1 sont ± 1. Si $i = 1$, alors G est abélien d'ordre $2p$, $(2, p) = 1$ donc cyclique (lemme chinois). Si $i = -1$ alors G est le groupe diédral.

Exemple 7.18. — *Un groupe fini G est un p-groupe si et seulement si tous ses éléments sont d'ordre une puissance de p.*
En effet, si $|G|$ est une puissance de p, alors le théorème de Lagrange montre que les ordres des éléments de G sont des puissances de p. La réciproque vient du théorème de Cauchy.
D'autres conséquences de l'équation aux classes conduisant à décrire la structure d'un p-groupe via ses actions sont présentées dans le paragraphe suivant (§8.1).

Corollaire 7.19. — *(Théorème de Wedderburn). Toute algèbre à division finie est un corps.*

Démonstration. — Il s'agit d'une application directe de l'équation de classes. En effet, soit A une algèbre à division finie. Son centre $k = Z(A)$ est un corps fini de cardinal $q = |k|$. Ainsi A est un k-espace vectoriel de dimension finie n et $|A| = q^n$. Le groupe $A^\times$ opère sur lui-même par conjugaison et $k^\times$ est l'ensemble des points fixes pour cette action. Soit $x \in A - k$, alors $\mathrm{Stab}(x)$ est le groupe multiplicatif d'une sous-algèbre à division de A contenant k, donc il existe $m > 0$ avec $|A| = |\mathrm{Stab}(x) \cup \{0\}|^m$. Ainsi $|\mathrm{Stab}(x)| = q^{d_x} - 1$ avec $0 < d_x < n$ et d_x divise n. L'orbite de x a pour cardinal :

$$|\mathcal{O}_x| = \frac{q^n - 1}{q^{d_x} - 1}.$$

Si x_i, $1 \leq i \leq t$ désigne un système de représentants des différentes orbites de $A^\times$ non réduites à un point :

$$A^\times = k^\times \cup \cup_{i=1}^r \mathcal{O}_{x_i}.$$

L'équation aux classes donne

$$q^n - 1 = q - 1 + \sum_{1 \leq i \leq t} \frac{q^n - 1}{q^{d_i} - 1}.$$

Or $X^n - 1 = \Pi_{d|n} \Phi_d(X)$, avec $\Phi_n(X) = \Pi_{j=1}^{\varphi(n)}(X - \zeta_j) \in \mathbb{Z}[X]$ avec ζ_i racine primitive n-ième de l'unité (voir Remarque 3.9). De même pour $d_i | n$, $X^{d_i} - 1 = \prod_{d|d_i} \Phi_d(X)$. Donc

$$\frac{X^n - 1}{X^{d_i} - 1} = \prod_{d|n, d \not| d_i} \Phi_d(X).$$

En ávluant en $X = q$, l'entier $\Phi_n(q)$ divise chacun des entiers $\frac{q^n-1}{q^{d_i}-1}$, $d_i < n$ diviseur (positif) de n, donc divise $q - 1$. Or si $n > 1$, chacun des facteurs $q - \zeta_j$ a un module supérieur à $q - 1$. D'où l'absurdité. □

8. Théorème de Sylow

8.1. p-groupes. — L'ordre d'un groupe donne déjà beaucoup d'informations sur sa structure : abélien, existence de sous-groupes normaux...

Lemme 8.1. — *Si un p-groupe G (fini) agit sur un ensemble fini E. Notons E^G, le sous-ensemble de E des éléments fixes par G. Alors*

$$|E^G| \equiv |E| \mod p.$$

En particulier si p ne divise pas $|E|$, l'action de G a au moins un point fixe.

Démonstration. — D'après l'équation aux classes

$$|E| = |E^G| + \sum_{x \in X} |\mathcal{O}_x|,$$

où X est un système de représentants des orbites non triviales. Si $x \in X$, $|\mathcal{O}_x| > 1$ et divise $|G|$ qui est une puissance de p. D'où le résultat. □

Lemme 8.2. — *Tout p-groupe non trivial a un centre non réduit à l'élément neutre.*

Démonstration. — Le groupe G agit sur lui-même par conjugaison et $Z(G)$ est l'ensemble des points fixes pour cette action. Comme $|G|$ est une puissance de p, $|\mathcal{O}_x| = |G|/|\operatorname{Stab}(x)|$ est une puissance de p ($\neq 1$) pour tout x n'appartenant pas au centre de G. D'après l'équation aux classes, p divise alors $|Z(G)|$ qui n'est donc pas trivial. □

Exemple 8.3. — *Tout p-groupe G est résoluble. Pour le montrer, nous raisonnons par récurrence sur l'ordre de $|G|$. Comme $Z(G) \neq 1$, $G/Z(G)$ est un p-groupe d'ordre strictement inférieur à G donc résoluble. Le groupe abélien $Z(G)$ est résoluble. Donc, d'après le lemme 4.8, G est résoluble.*

Lemme 8.4. — *Supposons que G contient un sous-groupe $H \subset Z(G)$ (alors H est normal) tel que G/H cyclique. Alors G est abélien.*
Plus généralement, si $H \subset Z(G)$ et G contient un système de représentants de G/H d'éléments qui commutent, alors G est abélien.

Démonstration. — Soit $a \in G$ avec $G/H =< \bar{a} >$. Alors tout élément de G est de la forme $g = a^i h$ pour $h \in H$ et $i \in \mathbb{Z}$. Or $a^i h a^{i'} h' = a^i a^{i'} hh' = a^{i'} a^i h' h = a^{i'} h' a^i h$, donc G est abélien. □

Exemple 8.5. — *Tout groupe d'ordre p^2 est abélien et donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*
En effet, si le centre de G n'est pas trivial, donc $G/Z(G)$ est d'ordre 1 ou p, donc cyclique. D'après le lemme 8.4, G est abélien (absurde).

8.2. Théorème de Sylow. —

Définition 8.6. — *Soit G un groupe d'ordre $|G| = p^\alpha m$, $\alpha \geq 1$, p premier et $(p, m) = 1$. Un sous-groupe de G d'ordre p^α est appelé sous-groupe de p-Sylow.*

Exemple 8.7. — *Le sous-groupe des matrices triangulaires supérieures n'ayant que des 1 sur la diagonale est un sous-groupe de p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. L'ensemble des p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ est décrit dans l'exemple 8.17.*

Lemme 8.8. — *Si S est un p-Sylow de G et H est un sous-groupe de G, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. — Le groupe H agit à gauche sur l'ensemble G/S des classes à gauche via $h(gS) = (hg)S$, $h \in H$. Le stabilisateur d'une classe gS est

$$\mathrm{Stab}(gS) = gSg^{-1} \cap H.$$

Comme p ne divise pas $|G/S|$, l'équation aux classes ($|G/S| = \sum |\mathcal{O}_{gS}|$) assure qu'il existe au moins une classe gS telle que

$$p \text{ ne divise pas } |\mathcal{O}_{gS}| = |H|/|\mathrm{Stab}(gS)|.$$

Or $\mathrm{Stab}(gS) \subset gSg^{-1}$, qui est un p-groupe, donc $\mathrm{Stab}(gS)$ est un p-groupe, donc un p-Sylow de H. □

Théorème 8.9. — *(Théorème de Sylow). Soit G un groupe d'ordre $|G| = p^\alpha m$, $\alpha \geq 1$, p premier et $(p, m) = 1$.*
i. Il existe dans G un sous-groupe de p-Sylow.
ii. Tout sous-groupe de G d'ordre p^β, $1 \leq \beta \leq \alpha$ est inclus dans un sous-groupe

de p-Sylow.
iii. Le groupe G opère par conjugaison, transitivement sur l'ensemble des sous-groupes de p-Sylow.
iv. Le nombre des sous-groupes de p-Sylow de G est congru à 1 modulo p et divise m.

Démonstration. — i. Le groupe G opère sur l'ensemble

$$E = \{ \text{ sous-ensembles de } G \text{ ayant } p^\alpha \text{ éléments } \}.$$

via $gA = \{ga | a \in A\}$, $g \in G$, $A \in E$. Pour $A \in E$, notons

$$H = \mathrm{Stab}(A) = \{g \in G | gA = A\}.$$

Pour tout $a \in A$, $\phi_a : H \longrightarrow A, h \mapsto ha$ est injective donc $|H| \leq |A| = p^\alpha$. Or

$$|\mathcal{O}_A| = |G|/|\mathrm{Stab}(A)| \text{ et } |G| = p^\alpha m.$$

S'il existe A avec p ne divise pas $|\mathcal{O}_A|$ alors $H = \mathrm{Stab}\, A$ est d'ordre p^α.
Or le cardinal de E,

$$E = \binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)(p^\alpha m - 1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{(p^\alpha)(p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}.$$

Si $i < p^\alpha$ la puissance de p divisant $p^\alpha m - i$ (resp. $p^\alpha - i$) est la puissance de p divisant i, donc p ne divise pas $|E|$. Or les orbites sous l'action de G forment une partition de E, donc

$$|E| = \sum |\mathcal{O}_i|, \mathcal{O}_i \text{ parcourant l'ensemble des orbites distinctes.}$$

Donc au moins une orbite est d'ordre non divisible par p.
ii. Si H est un p-sous-groupe de G et si S est un p-Sylow de G, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H (Lemme 8.8) , donc égal à H car H est un p-groupe. Donc $H \subset gSg^{-1}$ qui est un p-Sylow de G.
iii. Si H, S sont deux p-Sylow de G, il existe $g \in G$ tel que $H \subset gSg^{-1}$ (Lemme 8.8) . Les deux groupes gSg^{-1} et H sont de même ordre, d'où $H = gSg^{-1}$.
iv. Le groupe G opère transitivement par conjugaison sur l'ensemble X des p-Sylow de G, donc $|X|$ divise $|G|$. Soit S un p-Sylow. Montrons que S est le seul point fixe de l'action de S sur X, car alors nous pourrons conclure d'après le lemme 8.1, $|X| \equiv |X^S| \equiv 1 \mod p$.
Soit $S' \in X^S$, i.e $sS's^{-1} = S'$, pour tout $s \in S$. Alors S est un sous-groupe du groupe $\mathrm{Stab}(S') = \{g \in G | gS'g^{-1} = S'\}$ et S' sous-groupe normal de $\mathrm{Stab}(S')$. Ainsi S et S' sont des p-Sylow de $\mathrm{Stab}(S')$, donc conjugués dans N. Or S' normal dans $\mathrm{Stab}(S')$ donc $S = S'$ et $|X| \equiv 1 \mod p$.
De plus $|X| = |G|/|\mathrm{Stab}(S')|$ avec p^α divisant $|\mathrm{Stab}(S')|$. Donc $|X|$ divise m. □

Corollaire 8.10. — *Un p-groupe de Sylow est normal si et seulement si c'est le seul p-Sylow.*

Exemple 8.11. — *Soit G un groupe simple, p nombre premier divisant strictement $|G| > p$ et n_p le nombre de sous-groupes de p-Sylow de G. Alors G s'identifie à un sous-groupe de $\mathfrak{S}_{n_p}$.*
En effet, $n_p > 1$ car sinon l'unique sous-groupe de p-Sylow de G est normal dans G simple donc $G = C_p$ ce qui est exclu. Le groupe G opère transitivement par conjugaison sur l'ensemble de ses n_p sous-groupes de p-Sylow. Ceci induit un morphisme de groupes $\varphi : G \longrightarrow \mathfrak{S}_{n_p}$. Si G est simple, le noyau de φ sous-groupe normal (distinct de G) est trivial : $\ker\varphi = 1$. *Donc G s'identifie à un sous-groupe de $\mathfrak{S}_{n_p}$.*

Exemple 8.12. — *Si G est fini abélien, il admet un unique p-Sylow S qui s'identifie au sous-groupe de p-torsion de G :*

$$G^{(p)}_{\text{tors}} = \{g \in G | \exists n \in \mathbb{N}, p^n g = 0\}.$$

En effet $G^{(p)}_{\text{tors}}$ est un groupe car G est abélien. Tous les éléments de S sont d'ordre une puissance de p, donc $S \subset G^{(p)}_{\text{tors}}$. Tous les éléments de $G^{(p)}_{\text{tors}}$ sont d'ordre une puissance de p donc $|G^{(p)}_{\text{tors}}|$ est une puissance de p. Donc $S = G^{(p)}_{\text{tors}}$.

Corollaire 8.13. — *Soit G un groupe n'admettant qu'un seul p-Sylow pour tout nombre premier p divisant son ordre. Alors G est produit direct de ses sous-groupes de Sylow.*

Démonstration. — Soit $P_1, \ldots, P_k$ les sous-groupes de Sylow de G d'ordre respectifs $p_i^{r_i}$ avec $(p_i, p_j) = 1$, $1 \leq i < j \leq k$. Le produit direct $P = \prod_{i=1}^k P_i$ des sous-groupes normaux P_i est normal dans G. Nous montrons par récurrence sur k qu'il est d'ordre $\Pi_{i=1}^k p_i^{r_i}$. Pour $k = 1$, le résultat est clair. Supposons $k \geq 2$. Les sous-groupes $\prod_{i=1}^{k-1} P_i$ et P_k sont normaux dans G et $\left(\prod_{i=1}^{k-1} P_i\right) \cap P_k = 1$ donc le produit direct $\prod_{i=1}^k P_i$ est un sous-groupe normal de G. □

Exemple 8.14. — *Si G est un groupe d'ordre 99, alors G est produit direct de ses sous-groupes de Sylow qui sont abéliens, donc G est abélien.*

Exemple 8.15. — *Soit G d'ordre pq avec p et q deux nombres premiers $p < q$. Le nombre n_q de q-Sylow de G satisfait $n_q \equiv 1 \mod q$ et n_q divise p. Donc $n_q = 1$ et l'unique q-Sylow Q de G est normal. Soit P un p-Sylow de G, $P \cap Q = \{e\}$, $Q \lhd G$ et $PQ = G$, donc $G = Q \rtimes_\varphi P$. Il s'agit de d'eterminer $\varphi : P \longrightarrow \operatorname{Aut} Q$. Or* $\operatorname{Aut} Q = (\mathbb{Z}/q\mathbb{Z})^*$. *Si p ne divise pas $q-1$, alors φ est trivial et G est cyclique. Si p divise $q-1$, alors G est cyclique ou est décrit par les générateurs $\{a, b\}$ et les relations*

$$a^p = 1, b^q = 1, aba^{-1} = b^i$$

avec i élément d'ordre p dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$ (la classe d'isomorphie de G ne dépend pas du choix de $i \neq 1$).

Remarque 8.16. — *Soit p, q deux nombres premiers distincts. Les groupes d'ordre pq, p^2q, p^3q ne sont pas simples. Si, de plus, $p < q$, les groupes d'ordre*

$p^m q^n$, $1 \leq m \leq 2$, $n \geq 1$ ne sont pas simples (voir TD). Plus généralement, Burnside a prouvé que si G est non-abélien et simple alors $|G|$ est divisible par trois nombres premiers distincts.

Exemple 8.17. — *Soit $G = \mathrm{GL}(V)$ où V est un espace vectoriel de dimension n sur $\mathbb{F}_p$, le corps à p éléments. Nous donnons une description géométrique des p-Sylow de G.*
Un drapeau maximal F dans V est une suite de sous-espaces

$$\{0\} \subset V_1 \subset \cdots \subset V_{n-1} \subset V_n = V$$

avec $\dim V_i = i$. Autrement dit, un drapeau maximal est une suite de composition de V.
Etant donné un drapeau maximal F de V, nous notons $U(F)$ l'ensemble des applications linéaires $\alpha : V \longrightarrow V$ telles que
a. $\alpha(V_i) \subset V_i$, $1 \leq i \leq n$,
b. l'endomorphisme induit par α sur V_i/V_{i-1} est l'identité.
Alors $U(F)$ est un p-Sylow de G.
En effet, nous pouvons construire une base $\{e_1, \ldots, e_n\}$ de V, telle que $\{e_1, \ldots, e_i\}$ est une base de V_i pour tout $1 \leq i \leq n$. Relativement à cette base, les matrices des éléments de $U(F)$ sont exactement les matrices triangulaires supérieures avec des 1 sur la diagonale. Elles forment un sous-groupe U d'ordre $p^{n(n-1)/2}$ de $\mathrm{GL}_n(\mathbb{F}_p)$ d'ordre $(p^n - 1)\cdots(p^n - p^{n-1})$, donc U est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ et $U(F)$ est un p-Sylow de G.
Soit $g \in G$, alors $gF = \{gV_i, 1 \leq i \leq n\}$ est un drapeau maximal et $U(gF) = gU(F)g^{-1}$. Donc les p-Sylow de G sont précisément les sous-groupes de la forme $U(F)$ pour F un drapeau maximal.

9. Groupe symétrique

9.1. Générateurs et classes de conjugaison du groupe symétrique. — Le groupe symétrique $\mathfrak{S}_n$ opère transitivement sur $\{1, \ldots, n\}$, le stabilisateur d'un point est $\mathfrak{S}_{n-1}$, donc $|\mathfrak{S}_n| = n|\mathfrak{S}_{n-1}|$ et par récurrence $|\mathfrak{S}_n| = n!$.

Définition 9.1. — *Un cycle est une permutation de la forme*

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_r \mapsto i_1, \text{ avec } i_i \neq i_j, i \neq j.$$

Nous le notons $(i_1, \ldots, i_r)$ et r est dit longueur du cycle. Un cycle de longueur 2 est dit transposition. Le support du cycle $(i_1, \ldots, i_r)$ est l'ensemble $\{i_1, \ldots, i_r\}$. Deux cycles sont dits disjoints si leurs supports sont disjoints.

La longueur d'un cycle est aussi son ordre comme élément de $\mathfrak{S}_n$. Deux cycles de supports disjoints commutent, donc si $\sigma \in \mathfrak{S}_n$ se décompose en cycles de

supports disjoints

$$\sigma = (i_1, \ldots, i_r)(j_1, \ldots, j_s) \cdots (\ell_1, \ldots, \ell_u)$$

$$\sigma^m = (i_1, \ldots, i_r)^m (j_1, \ldots, j_s)^m \cdots (\ell_1, \ldots, \ell_u)^m, m \in \mathbb{Z},$$

donc σ a pour ordre le ppcm$(r, s, \ldots, u)$.

Lemme 9.2. — *Toute permutation se décompose (de manière unique à l'ordre près) comme produit de cycles à supports disjoints (qui commutent deux à deux).*

Démonstration. — Soit $\sigma \in \mathfrak{S}_n$. Alors $< \sigma >$ opère sur $\{1, \ldots, n\}$ qui est réunion disjointe de ses orbites :

$$\{1, \ldots, n\} = \coprod_{i=1}^{r} \mathcal{O}_i.$$

En posant

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{si } x \in \mathcal{O}_i \\ x & \text{si } x \notin \mathcal{O}_i \end{cases}$$

alors nous obtenons des cycles σ_i de support $\mathcal{O}_i$, $\sigma_i \sigma_j = \sigma_j \sigma_i$, $1 \leq i, j \leq r$ tels que

$$\sigma = \sigma_1 \cdots \sigma_r.$$

□

Corollaire 9.3. — *Toute permutation $\sigma \in \mathfrak{S}_n$ est produit de transpositions. Le nombre de ces transpositions est pair ou impair suivant la valeur de la signature σ.*

Démonstration. — Le cycle de longueur r s'écrit comme produit de transpositions

$$(i_1 i_2 \cdots i_r) = (i_1 i_2) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r).$$

La signature est un homomorphisme de groupes (exemple 1.3.4) et la signature d'une transposition est égale à -1, donc $\varepsilon(\sigma) = (-1)^{|transpositions|}$. □

Corollaire 9.4. — *Le groupe $\mathfrak{S}_n$ est engendré par les tranpositions.*

Lemme 9.5. — *Si $\sigma = (a_1 \cdots a_k) \in \mathfrak{S}_n$ est un k-cycle et $\tau \in \mathfrak{S}_n$, on a*

$$\tau \sigma \tau^{-1} = (\tau(a_1) \cdots \tau(a_k))$$

Tous les k-cycles sont conjugués dans $\mathfrak{S}_n$.

Démonstration. — En effet si $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$, alors $\tau^{-1}(x) \notin \{a_1, \ldots, a_k\}$ donc $\tau \sigma \tau^{-1}(x) = x$. Si $x = \tau(a_i)$ alors $\tau \sigma \tau^{-1}(x) = \tau \sigma(a_i) = \tau(a_{i+1})$. □

Lemme 9.6. — *Les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n :*

$$n = k_1 + \cdots + k_r, r \in \mathbb{N}, 1 \leq k_1 \leq \cdots \leq k_r.$$

Démonstration. — En effet écrivons $\sigma = \sigma_1 \cdots \sigma_r$ comme produits de cycles à supports disjoints de longueur $1 \leq k_1 \leq \ldots \leq k_r$, alors

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1})$$

est encore un produit de cycles disjoints de mêmes longueurs $k_1, \ldots, k_r$. Réciproquement toutes les permutations correspondant à la même partition sont conjuguées. □

Exemple 9.7. — *Les 2 partitions de 2 sont 1+1 et 2, les classes de conjugaison correspondantes dans* $\mathfrak{S}_2$ *sont* $\{\mathrm{Id}\}$ *et* $\{(12)\}$.
Les 3 partitions de 3 sont 1+1+1, 1+2 et 3, les classes de conjugaison correspondantes dans $\mathfrak{S}_3$ *sont* $\{\mathrm{Id}\}$, $\{(12), (23), (13)\}$ *et* $\{(123), (132)\}$.
Les 5 partitions de 4 sont 1+1+1+1,1+1+ 2, 2+2, 1+3 et 4 les classes de conjugaison correspondant dans $\mathfrak{S}_4$ *sont* $\{\mathrm{Id}\}$, *les 6 transpositions, les 3 doubles transpositions, les 8 3-cycles et les 6 4-cycles.*

Exercice 9.8. — *Nous pouvons définir une classe de conjugaison de* $\mathfrak{S}_n$ *par la longueur de ses cycles : pour* $1 \leq k \leq n$ *soit* μ_k *le nombre de cycles de longueur* k. *Ainsi* $\sum_{k=1}^{n} k\mu_k = n$. *De plus le nombre de permutations distinctes dans cette classe de conjugaison est*

$$n_\mu = \frac{n!}{\prod_{k=1}^{n} \mu_k! k^{\mu_k}}.$$

9.2. Groupe alterné. — Le groupe alterné $\mathfrak{A}_n$ est le noyau de la signature (exemple 1.3.4)

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

Le sous-groupe normal $\mathfrak{A}_n$ de $\mathfrak{S}_n$ d'indice 2 pour $n \geq 2$ est de cardinal $n!/2$.

Exemple 9.9. — *D'après l'exemple 9.7,*
- le groupe alterné $\mathfrak{A}_2$ *est trivial,*
- le groupe alterné $\mathfrak{A}_3$ *d'ordre 3 est cyclique et simple,*
- le groupe $\mathfrak{A}_4$, *d'ordre 12, contient exactement 3 éléments d'ordre 2, les doubles transpositions, qui avec* Id *forment un sous-groupe d'ordre 4, réunion de classes de conjugaison donc normal dans* $\mathfrak{A}_4$, *qui n'est pas simple.*

Exercice 9.10. — *Grâce au théorème de Sylow, nous pouvons montrer qu'il existe exactement 3 groupes non commutatifs (dont* $\mathfrak{A}_4$*) et 2 groupes commutatifs d'ordre 12 non isomorphes.*

Corollaire 9.11. — *Le groupe* $\mathfrak{A}_n$ *est engendré par les cycles de longueur 3.*

Démonstration. — Tout $\sigma \in \mathfrak{A}_n$ est produit (éventuellement vide) d'un nombre pair de transpositions : $\sigma = t_1 t'_1 \cdots t_m t'_m$. Or le produit de deux transpositions peut toujours s'écrire comme produit de 3-cycles :

$$(ij)(kl) = \begin{cases} (ijl) & \text{si } j = k, \\ (ijk)(jkl) & \text{si } i, j, k, l \text{ distincts}, \\ 1 & \text{si } (ij) = (kl). \end{cases}$$

□

Lemme 9.12. — *Soit N un sous-groupe normal de $\mathfrak{A}_n$ avec $n \geq 5$. Si N contient un cycle de longueur 3, alors il contient tous les cycles de longueur 3 et est égal à $\mathfrak{A}_n$.*

Démonstration. — Soit σ, γ deux cycles de longueur 3 de $\mathfrak{A}_n$ avec $\gamma \in N$. Il existe $g \in \mathfrak{S}_n$, tel que $\sigma = g\gamma g^{-1}$. Si $g \in \mathfrak{A}_n$, alors $\sigma \in N$. Sinon, comme $n \geq 5$, il existe une transposition $t \in \mathfrak{S}_n$ disjointe de σ. Alors $tg \in \mathfrak{A}_n$ et

$$\sigma = t\sigma t^{-1} = tg\gamma g^{-1} t^{-1} \in N.$$

□

Lemme 9.13. — *Tout sous-groupe normal N non trivial de $\mathfrak{A}_n$, $n \geq 5$ contient un cycle de longueur 3.*

Démonstration. — Pour $E = \{1, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$, notons $E^\sigma = \{x \in E, \sigma(x) = x\}$. Si $\sigma \in N - \{e\}$ n'est pas un 3-cycle, construisons $\sigma' \in N - \{e\}$ avec E^σ strictement inclus dans $E^{\sigma'}$. Ainsi en un nombre fini d'étapes nous obtenons un 3-cycle dans N. La décomposition en cycles disjoints de σ est de la forme

$$\sigma = (i_1 i_2 i_3 \cdots) \cdots \text{ ou } \sigma = (i_1 i_2)(i_3 i_4) \cdots .$$

Dans le premier cas, comme $\sigma \neq (i_1 i_2 i_3), (i_1 i_2 i_3 i_4)$ nous avons au moins cinq éléments i_1, i_2, i_3, i_4, i_5 distincts n'appartenant pas à E^σ. Posons $\gamma = (i_3 i_4 i_5)$, $\sigma_1 = \gamma\sigma\gamma^{-1} = (i_1 i_2 i_4 \cdots) \cdots \neq \sigma$ (car σ_1 et σ agissent différemment sur i_2) et $\sigma_1 \in N$ car $N \lhd \mathfrak{A}_n$. Alors $\sigma' = \sigma_1\sigma^{-1} = \gamma\sigma\gamma^{-1}\sigma^{-1} \in N$, $\sigma' \neq e$, fixe i_2 et tous les éléments distincts de $i_1, \ldots, i_5$ fixés par σ. Donc, $|E^\sigma| + 1 \leq |E^{\sigma'}|$.
Dans le second cas, choisissons i_5 distincts de $i_1, \ldots, i_4$. Soit $\gamma = (i_4 i_5)$ et $\sigma_1 = \gamma\sigma\gamma^{-1} = (i_1 i_2)(i_5 i_3) \cdots$. Alors $\sigma_1 \in N$, $\sigma_1 \neq \sigma$ et $\sigma' = \sigma_1\sigma^{-1} \in N - \{e\}$ fixe i_1, i_2 et tous les éléments $\neq i_1, \ldots, i_5$ fixé par σ, d'où $|E^\sigma| + 1 \leq |E^{\sigma'}|$. □

Des deux lemmes précédents, nous déduisons

Théorème 9.14. — *(Galois). Le groupe $\mathfrak{A}_n$ est simple si $n \geq 5$.*

Corollaire 9.15. — *Pour $n \geq 5$, les seuls sous-groupes normaux de $\mathfrak{S}_n$ sont $1, \mathfrak{A}_n, \mathfrak{S}_n$.*

Démonstration. — Si N est normal dans $\mathfrak{S}_n$, alors $N \cap \mathfrak{A}_n$ est normal dans $\mathfrak{A}_n$, donc égal à 1 ou $\mathfrak{A}_n$. Dans le premier cas $N \longrightarrow \mathfrak{S}_n/\mathfrak{A}_n$, $x \mapsto x\mathfrak{A}_n$ est injective donc N est d'ordre 1 ou 2, mais il ne peut pas être d'ordre 2 car $\mathfrak{S}_n$ n'a pas de classe de conjugaison non triviale réduite à un élément. Dans le second cas $\mathfrak{A}_n \subset N$ et $\mathfrak{A}_n$ d'indice 2 dans $\mathfrak{S}_n$ donc $N = \mathfrak{A}_n$ ou $\mathfrak{S}_n$. □

Exemple 9.16. — *Pour $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$ car $D(\mathfrak{A}_n)$ est normal dans $\mathfrak{A}_n$ et $\mathfrak{A}_n$ est simple non abélien, donc non résoluble.*
Pour $n \geq 2$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$. En effet, la signature d'un commutateur est triviale donc $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$. Par ailleurs $[(ab),(abc)] = (abc) \in D(\mathfrak{A}_n)$, donc $D(\mathfrak{A}_n)$ contient tous les 3-cycles donc $\mathfrak{A}_n$ pour tout $n \geq 3$. Le cas $n = 2$ est élémentaire.

Exercice 9.17. — *Grâce au théorème de Sylow, nous déduisons que le seul groupe simple d'ordre 60 est $\mathfrak{A}_5$. C'est le plus petit groupe simple non cyclique (voir TD).*

Remarque 9.18. — *Si $p < n$ premier, les sous-groupes de p-Sylow de $\mathfrak{S}_n$ sont d'ordre p et engendrés par les cycles d'ordre p. Pour $p \geq n$, les p-Sylow sont d'ordre p^α avec*

$$\alpha = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Leur description peut s'avérer fastidueuse.

9.3. Groupes d'isométries des polyèdres réguliers de l'espace $\mathbb{R}^3$. — Les symétries d'un objet forment un groupe. Comprendre l'action de ce groupe sur l'objet est une approche fructueuse à la compréhension de l'objet. Compter permet de faire une liste exhaustive des objets satisfaisant certaines propriétés. Ceci permet de classifier les objets.

Définition 9.19. — *Le groupe des isométries de $\mathbb{R}^3$ est le groupe, dit orthogonal,*

$$\mathrm{O}_3(\mathbb{R}) = \{M \in M_3(\mathbb{R}) | M^t M = \mathrm{Id}\}.$$

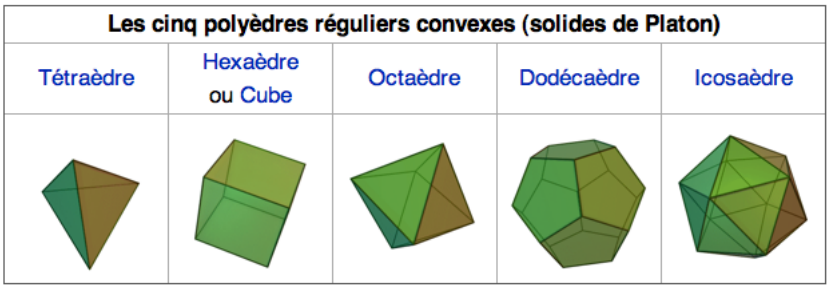
Le groupe des isométries positives de $\mathbb{R}^3$ est le groupe, dit spécial orthogonal,

$$\mathrm{SO}_3(\mathbb{R}) = \{M \in \mathrm{O}_3(\mathbb{R}) | \det M = 1\}.$$

Toute matrice de $\mathrm{O}_3(\mathbb{R})$ est semblable à une matrice de la forme

$$\begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad \theta \in [0, 2\pi[, \varepsilon \in \{-1, 1\}.$$

Définition 9.20. — *Un polyèdre de $\mathbb{R}^3$ est dit régulier si toutes ses faces sont des polygones réguliers de même type et si tous ses sommets sont de même degré.*



http://images.math.cnrs.fr/

Définition 9.21. — *Nous appelons polyèdre dual d'un polyèdre P le polyèdre dont les sommets sont les centres de gravité des faces de P.*

Le tétraèdre est auto-dual. Le cube et l'octaèdre sont duaux. Le dodécaèdre et l'icosaèdre sont duaux.

	tétraèdre	cube	octaèdre	dodécaèdre	icosaèdre
sommets	4	8	6	20	12
arêtes	6	12	12	30	30
faces	4	6	8	12	20

Exemple 9.22. — *Dans un polyèdre régulier, comme dans tout polyèdre convexe, nous avons la relation d'Euler qui relie les nombres de sommets ($|S|$), d'arêtes ($|A|$) et de faces ($|F|$)*

$$|S| - |A| + |F| = 2.$$

Pour une surface polyèdre convexe et ouverte, dont le contour est une ligne brise plane ou gauche, par induction sur le nombre de faces $|F| + |S| = |A| + 1$. De manière intuitive, si nous retirons une face à un polyèdre convexe, nous obtenons une surface polyèdre.

Une similitude de $\mathbb{R}^3$ est la composée d'une isométrie et d'une homothétie. Dans la proposition suivante, nous déterminons les classes de similitude de polyèdres.

Proposition 9.23. — *Il existe exactement cinq classes de polyèdres réguliers : tétraèdre, cube, octaèdre, dodécaèdre et icosaèdre.*

Démonstration. — Considèrons un polyèdre régulier P de $\mathbb{R}^3$ dont nous notons S (resp. A, F) l'ensemble des sommets (resp. des arêtes, des faces). Les faces de P sont des polygones réguliers identiques ayant p sommets. Nous notons q le nombre de faces qui contiennent un sommet fixé. Ainsi $p \geq 3$ et $q \geq 3$. En considérant la sommes des angles autour d'un sommet du polyèdre, nous obtenons

$$2\pi > q(\pi - 2\pi/p) \text{ soit encore } p < \frac{2q}{q-2}.$$

La fonction $f : x \mapsto \frac{2x}{x-2}$ est strictement croissante sur $[3, +\infty[$ et $f(6) = 3$, donc $p \in \{3, 4, 5\}$ et

$$(p, q) \in \{(5, 3), (4, 3), (3, 3), (3, 4), (3, 5)\}.$$

De plus les liens entre sommets/arêtes et arêtes/faces conduisent aux égalités

$$2|A| = \sum_{a \in A} \#\{s \in S | s \in a\} = \#\{(s, a) \in S \times A | s \in a\} = \sum_{s \in S} \#\{a \in A | s \in a\} = q|S|$$

$$2|A| = \sum_{a \in A} \#\{f \in F | a \in f\} = \#\{(a, f) \in A \times F | a \in f\} = \sum_{f \in F} \#\{a \in A | a \in f\} = p|F|$$

La relation d'Euler $|S| - |A| + |F| = 2$ implique alors

$$|S| = \frac{4p}{2p + 2q - pq},\ |A| = \frac{2pq}{2p + 2q - pq},\ |F| = \frac{4q}{2p + 2q - pq}.$$

Nous vérifions alors que les cinq triplets $(|S|, |A|, |F|)$ obtenus définissent cinq classes de similitude de polyèdres et qu'ils correspondent aux cinq polyèdres réguliers tétraèdre, cube, octaèdre, dodécaèdre et icosaèdre. □

Nous décrivons les groupes d'isomètries des polyèdres réguliers. Remarquons que :
- la dualité des polyèdres est une involution sur les classes de similitude de polyèdres,
- deux polyèdres duaux ont le même groupe d'isométries.

Il suffit donc de déterminer le groupe d'isométrie du tétrèdre, du cube/octaèdre et du dodécaèdre/icosaèdre.

Proposition 9.24. — *Le groupe des isométries positives (resp. isométries) du tétraèdre est isomorphe à $\mathfrak{A}_4$ (resp $\mathfrak{S}_4$).*

Démonstration. — Le groupe des isométries conserve l'ensemble des sommets du tétraèdre donc s'injecte dans $\mathfrak{S}_4$. La symétrie par rapport au plan contenant les sommets 1 et 2 et le milieu des sommets 3 et 4 induit la transposition (34). Comme les transpositions engendrent $\mathfrak{S}_4$, le groupe des isométries est $\mathfrak{S}_4$. Une transformation est directe si et seulement si la permutation est positive. □

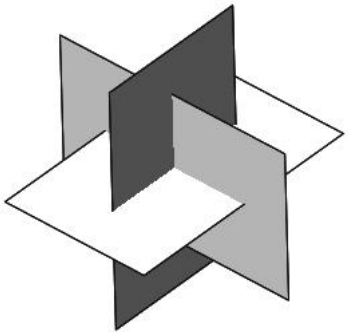
Proposition 9.25. — *Le groupe des isométries positives (resp. isométries) du cube (et de l'octaèdre) est isomorphe à $\mathfrak{S}_4$ (resp $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$).*

Démonstration. — Le groupe des isométries G permute les quatre grandes diagonales non orientées. En considérant les symétries (isométries positives) par rapport aux plans contenant deux grandes diagonales, nous montrons qu'il contient toutes les transpositions. Donc $\phi : G \longrightarrow \mathfrak{S}_4$ est surjectif. Si deux sommets d'une grande diagonale sont échangés par une isométrie, ces deux sommets et les sommets d'une autre grande diagonale forment un rectangle non carré, donc

l'isométrie est la symétrie centrale. Le noyau de ϕ est donc engendré par la syimétrie centrale (qui n'est pas une isométrie positive). □

Proposition 9.26. — *Le groupe des isométries positives (resp. isométries) de l'icosaèdre (et du dodécaèdre) est isomorphe à* $\mathfrak{A}_5$ *(resp* $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$*).*

Démonstration. — Le groupe des isométries positives G de l'icosaèdre contient l'identité, les 24 rotations d'ordre 5 (4 par couple de sommets opposés), les 20 rotations d'ordre 3 (2 par couple de faces opposées) et les 15 rotations d'ordre 2 (une par couple d'arêtes opposées). Il est donc d'ordre au moins 60.
L'icosaèdre contient 5 systèmes de 6 arêtes, formés de trois couples d'arêtes parallèles, les directions des couples étant deux à deux orthogonales.



http://images.math.cnrs.fr/

Le groupe G permute ces 5 systèmes et un élément de G qui fixe globalement un sytème est l'identité. Donc $\varphi : G \longrightarrow \mathfrak{S}_5$ est injective. Le sous-groupe de G qui fixe un système est un sous-groupe des isométries positives $\mathfrak{S}_4$ d'un octaèdre régulier (composé des milieux des 6 arêtes du système). C'est un sous-groupe strict car il ne contient pas les quart de tour. Donc φ n'est pas surjective. D'où $G \simeq \mathfrak{A}_5$. □

Remarque 9.27. — *(Pavage de la sphère). Un problème de pavage périodique est la donnée d'un ensemble X (souvent muni d'une structure), d'un groupe de symétries G (groupe de transformations de X qui préservent sa structure) et d'une tuile $T \subset X$ union disjointe d'un intérieur $\overset{\circ}{T}$ et d'un bord δT. Le problème de pavage périodique consiste à savoir si X peut être pavé par la tuile T avec le groupe de symétries G, i.e. s'il existe un sous-groupe, dit groupe de pavage $H < G$ avec*

$$X = \cup_{g \in H} gT \text{ et } g, h \in H, g \neq h \Longrightarrow g\overset{\circ}{T} \cap h\overset{\circ}{T} = \emptyset.$$

La sphére unité S^2 *d'équation* $x^2 + y^2 + z^2 = 1$ *hérite de son espace ambiant* $\mathbb{R}^3$ *une métrique* $ds^2 = dx^2 + dy^2 + dz^2$ *et les isométries de* $\mathbb{R}^3$ *induisent sur* S^2

des bijection préservant cette métrique. Le groupe des isométries de S^2 *s'identifie à* $\mathrm{O}_3(\mathbb{R})$*. Les groupes de pavages périodiques directs de* S^2 *sont les sous-groupes finis de* $\mathrm{SO}_3(\mathbb{R})$*, c'est-à-dire, les groupes cycliques, les groupes diédraux,* $\mathfrak{A}_4$*,* $\mathfrak{S}_4$ *ou* $\mathfrak{S}_5$*. Nous avons vu que tous ces groupes étaient atteints, pour montrer que ce sont les seuls, la finitude de l'inéquation*

$$1/n + 1/m + 1/r > 1, n, m, r \text{ entiers supérieurs à } 2$$

joue un rôle clef dans la preuve ; elle reflète le fait qu'en géométrie sphérique, la somme des angles d'un triangle est $> \pi$*.*

Remarque 9.28. — *(Théorème de Polya). Soit* X *un ensemble fini à* n *éléments muni de l'action d'un groupe fini* G*. Soit* L *un ensemble fini à* ℓ *éléments. Nous appelons coloriage de* X *à* ℓ *couleurs toute application* $\gamma : X \longrightarrow L$*. Nous notons* Γ *l'ensemble des coloriages de* X *à* ℓ *couleurs. Nous disposons d'une action de* G *sur* Γ *via* $g\gamma = \gamma \circ g^{-1}$*,* $\gamma \in \Gamma$*,* $g \in G$*. L'objet du théorème de Polya est de dénombrer les coloriages de* X *à l'action de* G *près. En particulier, il existe 11 coloriages d'un dodécaèdre avec une face rose, deux faces bleues et neuf faces jaunes à rotation près.*

Remarque 9.29. — *Il s'avère pertinent, en chimie notamment, d'étudier le groupe d'isométrie de polyèdres plus généraux. Par exemple, le groupe de symétrie de l'icosaèdre tronqué, modèle de la molécule de fullerène, composé de 20 hexagones et 12 pentagones est* $\mathfrak{A}_5 \times C_2$*.*

Paige Johnson

10. Groupe projectif linéaire

Pour k un corps, les groupes linéaires $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ agissent sur l'ensemble des droites vectorielles de k^n, dit espace projectif. Les noyaux de ces actions

sont les homothéties. Les groupes quotient $\mathrm{PGL}_n(k)$ et $\mathrm{PSL}_n(k)$ sont les groupes projectifs linéaires. L'objet de cette section (§10) est d'établir, grâce au théorème d'Iwasawa, la simplicité de $\mathrm{PSL}_n(k)$ pour $n \geq 3$ ou $n \geq 2$ et $|k| > 4$.

10.1. Définitions. —

Définition 10.1. — *Soit $n \geq 2$ et k un corps. Le groupe $k^\times$ agit naturellement sur $k^n - \{0\}$ et le système de représentants des orbites est*

$$\mathbb{P}^{n-1}(k) = \{ \text{ droites vectorielles de } k^n \},$$

appelé l'espace projectif (sur k).

Exemple 10.2. — *Soit k un corps à q éléments. Le nombre de points de $\mathbb{P}^{n-1}(k)$ est $(q^n - 1)/(q - 1)$.*
En effet, k^n contient q^n vecteurs ; les $q^n - 1$ vecteurs non nuls engendrent $q^n - 1$ sous-espaces de rang 1. Chaque sous-espace de dimension 1 contient $q-1$ vecteurs non nuls qui l'engendrent.

Exemple 10.3. — *i. Le nombre de sous-espaces de rang $m - 1$ de $\mathbb{P}^{n-1}(k)$ est*

$$\left[\begin{array}{c} n \\ m \end{array} \right]_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^m)}{(q^m - 1)(q^m - q) \cdots (q^m - q^{m-1})}.$$

En effet, il s'agit de compter le nombre de m-uplets de vecteurs linéairement indépendants. Le j-ème vecteur doit être choisi en dehors du sous-espace de rang $j - 1$ engendré par les vecteurs précédents. D'où $q^n - q^j$ choix. Ensuite le même argument (en remplaçant n par m) donne le nombre de m-uplets de vecteurs linéairement indépendants qui engendrent le même sous-espace de rang m.
ii. Le nombre de sous-espaces de $\mathbb{P}^{n-1}(k)$ de rang $m-1$ contenant un sous-espace de rang $l-1$ fixé est égal au nombre de sous-espaces de rang $m-l-1$ de $\mathbb{P}^{n-l-1}(k)$. En effet soit U un sous-espace vectoriel de rang l d'un espace vectoriel de rang m. D'après le théorème d'isomorphisme, il y a une bijection entre les sous-espaces de V de rang m contenant U et les sous-espaces de rang $m-l$ de l'espace vectoriel V/U de rang $n - l$.

Exercice 10.4. — *(Théorème du q-binome). Pour $n \geq 1$,*

$$\prod_{i=0}^{n-1} (1 + q^i x) = \sum_{k=0}^{n} q^{k(k-1)/2} \left[\begin{array}{c} n \\ k \end{array} \right]_q x^k.$$

En effet, il s'agit d'abord d'établir

$$\left[\begin{array}{c} n \\ k \end{array} \right]_q + q^{n-k+1} \left[\begin{array}{c} n \\ k-1 \end{array} \right]_q = \left[\begin{array}{c} n+1 \\ k \end{array} \right]_q.$$

Nous représentons l'élément de $\mathbb{P}^{n-1}(k)$ correspondant à la droite vectorielle engendrée par le vecteur (non nul) $(x_1, \ldots, x_n)$ de k^n par ses coordonnées homogènes $[x_1 : \cdots : x_n]$. Ainsi, nous avons $[x_1 : \cdots : x_n] = [\lambda x_1 : \cdots : \lambda x_n]$, pour tout $\lambda \in k^\times$.

Exemple 10.5. — *Pour $n = 2$, la droite projective*

$$\mathbb{P}^1(k) = \{k(x,1) | x \in k\} \cup \{k(1,0)\} \xrightarrow{\sim} k \cup \{\infty\},\ [x_1 : x_2] \mapsto \begin{cases} x_1/x_2 & si\ x_2 \neq 0, \\ \infty & si\ x_2 = 0. \end{cases}$$

est constituée d'une copie de k et d'un point à l'infini.

L'action de $\mathrm{GL}_2(k)$ sur k^2 induit une action sur $\mathbb{P}^1(k)$. L'action de $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ sur $\mathbb{P}^1(k)$ s'écrit

$$A \cdot [x_1 : x_2] = [ax_1 + bx_2 : cx_1 + dx_2]$$

ou encore si $bc \neq 0$,

$$k \cup \{\infty\} \longrightarrow k \cup \{\infty\}, x \mapsto \begin{cases} \frac{ax+b}{cx+d} & si\ x \neq -d/c, \\ \infty & si\ x = -d/c, \\ a/c & si\ x = \infty. \end{cases}$$

Lemme 10.6. — *L'action de $\mathrm{GL}_n(k)$ sur k^n induit une action sur $\mathbb{P}^{n-1}(k)$ de noyau les homothéties.*

Démonstration. — En effet le noyau de l'action de $\mathrm{GL}_n(k)$ sur $\mathbb{P}^{n-1}(k)$ est constitué des automorphismes u linéaires qui fixent chaque droite de $V = k^n$. Ainsi pour tout $x \in V$, il existe $\lambda_x \in k^\times$, tel que $u(x) = \lambda_x x$. Par linéarité, pour tous $x, y \in V$, $\lambda_{x+y}(x + y) = \lambda_x x + \lambda_y y$ donc $\lambda_{x+y} = \lambda_x = \lambda_y$ donc u est une homothétie. □

Définition 10.7. — *Soit $n \geq 2$, nous définissons le groupe projectif linéaire*

$$\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/Z(\mathrm{GL}_n(k)).$$

L'action de $\mathrm{GL}_n(k)$ sur $\mathbb{P}^{n-1}(k)$ a pour noyau $Z(\mathrm{GL}_n(k)) = k^* \,\mathrm{Id}$. Le groupe projectif linéaire $\mathrm{PGL}_n(k)$ opère ainsi fidèlement sur $\mathbb{P}^{n-1}(k)$.

Exemple 10.8. — *Pour tout $n \geq 2$, $\mathrm{GL}_n(\mathbb{F}_2) = \mathrm{SL}_n(\mathbb{F}_2) = \mathrm{PGL}_n(\mathbb{F}_2)$.*

Exemple 10.9. — *Si $|k| = q$, $|\mathrm{PGL}_n(k)| = q^{n(n-1)/2}(q^n - 1) \cdots (q^2 - 1)$.*

Remarque 10.10. — *Nous avons les isomorphismes exceptionnels avec des groupes symétriques*

$$\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4,\ \ \mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5,\ \ \mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5.$$

Notamment $\mathrm{PGL}_2(\mathbb{F}_3)$ opère fidèlement sur $\mathbb{P}^1(\mathbb{F}_3)$ qui a quatre éléments, donc nous avons un morphisme injectif entre deux groupes de même cardinal

$$\mathrm{PGL}_2(\mathbb{F}_3) \longrightarrow \mathfrak{S}_4.$$

La notation $\mathbb{F}_4$ désigne le corps à quatre éléments qui est unique à isomorphisme près $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$.

Définition 10.11. — *Soit $n \geq 2$, nous définissons le groupe projectif spécial linéaire*

$$\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/Z(\mathrm{SL}_n(k)).$$

Exemple 10.12. — *Le groupe dérivé $D(\mathrm{PSL}_n(k)) = \mathrm{PSL}_n(k)$ pour $n \geq 3$ ou $|k| \geq 4$ (i.e sauf si $n = 2$ et $k = \mathbb{F}_2$ ou $\mathbb{F}_3$, voir Proposition 5.12).*
Si k est fini d'ordre q, son groupe multiplicatif est cyclique d'ordre $q-1$ et

$$|\mathrm{PSL}_n(k)| = \frac{|\mathrm{SL}_n(k)|}{\mathrm{pgcd}(n, q-1)}.$$

En effet, $Z(\mathrm{SL}_n(k)) = \{r\,\mathrm{Id}, r \in k^*, r^n = 1\}$.

Remarque 10.13. — *Nous avons les isomorphismes exceptionnels (et ce sont les seuls)*

$$\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3, \mathrm{PSL}_4(\mathbb{F}_2) \simeq \mathfrak{A}_8, \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4,$$

$$\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5, \mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5, \mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{PSL}_3(\mathbb{F}_2), \mathrm{PSL}_2(\mathbb{F}_9) \simeq \mathfrak{A}_6$$

où $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$, $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.
L'isomorphisme $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{PSL}_3(\mathbb{F}_2)$ découlent du fait que tous les groupes simples d'ordre 168 sont isomorphes. C'est le plus petit groupe simple qui n'est ni cyclique, ni alterné. Le plus petit groupe simple qui n'est ni cyclique, ni alterné ni linéaire spécial projectif est $\mathrm{PSU}_3(\mathbb{F}_9)$ qui est d'ordre 6048 (voir §20).

10.2. Théorème d'Iwasawa. — Le théorème d'Iwasawa met en place une stratégie efficace pour démontrer qu'un groupe est simple. Nous le mettons en œuvre ici pour établir la simplicité du groupe spécial projectif linéaire (§10.3). Cette stratégie permet également de démontrer la simplicité d'autres groupes classiques (Partie IV).
Nous commençons ce paragraphe par quelques compléments sur les actions primitives.

Définition 10.14. — *Un sous-groupe H de G est maximal si $H \neq 1, G$ et pour tout sous-groupe H' de G contenant H, $H' = H$ ou $H' = G$.*

Définition 10.15. — *Une action transitive d'un groupe G sur un ensemble X est dite primitive si pour tout point $x \in X$, le stabilisateur $\mathrm{Stab}(x)$ est un sous-groupe maximal de G.*

Exemple 10.16. — *Le groupe $\mathfrak{S}_n$ opère primitivement sur $\{1, \ldots, n\}$. En effet le stabilisateur de tout point est $\mathfrak{S}_{n-1}$ qui est un sous-groupe maximal de $\mathfrak{S}_n$.*

Lemme 10.17. — *Une action de G sur X 2-transitive est primitive.*

Démonstration. — En effet soit $x \in X$ et $\mathrm{Stab}(x) < H < G$, supposons $H \neq \mathrm{Stab}(x)$. Soit $h \in H - \mathrm{Stab}(x)$ et $g \in G - \mathrm{Stab}(x)$. Par 2-transitivité, il existe $g' \in G$ avec $g'(x, gx) = (x, hx)$, i.e $g' \in \mathrm{Stab}(x)$ et $g'gx = hx$. Donc $h^{-1}g'g \in \mathrm{Stab}(x) < H$. Comme $h, g' \in H$, pour tout élément $g \in G - \mathrm{Stab}(x)$, $g \in H$, donc $H = G$. □

Théorème 10.18. — *(Théorème d'Iwasawa). Supposons que G opère primitivement sur X et notons*

$$G_X = \{g \in G, gx = x, x \in X\}$$

le sous-groupe normal de G des éléments qui agissent trivialement sur X. Supposons, de plus, que pour tout $x \in X$, il existe un sous-groupe T_x de G satisfaisant
- T_x abélien,
- $T_{gx} = gT_xg^{-1}$, $g \in G$, $x \in X$,
- $< \cup_{x \in X} T_x >= G$.
Alors,
i. pour tout sous-groupe $H \lhd G$, nous avons $H < G_X$ ou $D(G) < H$;
ii. si $G = D(G)$, alors G/G_X est simple.

Démonstration. — i. Soit $H \lhd G$ agissant non trivialement sur X ($H \not< G_X$) et soit $x \in X$. Comme $\mathrm{Stab}(x)$ est maximal, le sous-groupe $H\,\mathrm{Stab}(x)$ de G est égal à $\mathrm{Stab}(x)$ ou à G.
Si $H\,\mathrm{Stab}(x) = \mathrm{Stab}(x)$, alors $H < \mathrm{Stab}(x)$ et pour tout $g \in G$, $H = gHg^{-1} < g\,\mathrm{Stab}(x)g^{-1} = \mathrm{Stab}(gx)$. Or G agit transitivement sur X,

$$H < \cap_{y \in G}\,\mathrm{Stab}(y) = G_X.$$

Ce qui est absurde car H n'agit pas trivialement sur X ($H \not< G_X$).

Donc $H\,\mathrm{Stab}(x) = G$. Comme l'action de G sur X est transitive

$$X = Gx = H\,\mathrm{Stab}(x)x = Hx,$$

donc l'action de H sur X est transitive. Montrons que $G = HT_x$. Si $h \in H$, nous avons

$$T_{hx} = hT_xh^{-1} \subset HT_xH = HT_x$$

car $H \lhd G$. Comme H agit transitivement sur X, $T_y < HT_x$ pour tout $y \in X$, donc $G = HT_x$ puisque $G = \cup_{y \in X} T_y$. Enfin comme T_x abélien, $G/H = HT_x/H \simeq T_x/(H \cap T_x)$ est abélien et $D(G) \subset H$.
ii. Soit $\overline{N} \lhd G/G_X$. Nous relevons $\overline{N}$ en $N \lhd G$ avec $G_X \subset N$. D'après i., $N < G_X$ ou $D(G) < N$. Si $N < G_X$, alors $N = G_X$ et $\overline{N} = 1$. Si $D(G) < N$, alors $N = G = D(G)$ donc $\overline{N} = G/G_X$. Donc G/G_X est simple. □

10.3. Groupe projectif spécial linéaire. —

Définition 10.19. — *Soit V un k-espace vectoriel de dimension n. Une transvection de $\mathrm{GL}(V)$ est une application de la forme*

$$\tau_{\varphi,a} = \mathrm{Id} + a\varphi$$

avec $\varphi \in V^* = \mathrm{Hom}(V,k)$ une forme linéaire et $a \in \ker\varphi$.

Lemme 10.20. — *i. Les transvections de vecteur $a \in V$ forment un sous-groupe abélien de $\mathrm{GL}(V)$:*

$$\tau_{0,a} = \mathrm{Id}_V, \quad \tau_{\varphi,a} \circ \tau_{\varphi',a} = \tau_{\varphi+\varphi',a}.$$

ii. Les transvections de forme linéaire $\varphi \in V^*$ forment un sous-groupe abélien de $\mathrm{GL}(V)$:

$$\tau_{\varphi,0} = \mathrm{Id}_V, \quad \tau_{\varphi,a} \circ \tau_{\varphi,b} = \tau_{\varphi,a+b}.$$

iii. Pour $t \in \mathrm{GL}(V)$,

$$t \circ \tau_{\varphi,a} \circ t^{-1} = \tau_{\varphi \circ t^{-1}, t(a)}.$$

iv. Les transvections engendrent $\mathrm{SL}(V)$.

Démonstration. — iv. Pour $\varphi \neq 0$ et $a \in \ker\varphi$, nous pouvons compléter une base $(a, e_2, \ldots, e_{n-1})$ de $\ker\varphi$ en une base $(a, e_2, \ldots, e_n)$ de V et la matrice de $\tau_{\varphi,a}$ dans cette base est la matrice élémentaire $\mathrm{Id} + \varphi(e_n)E_{1n}$. De la même façon, toutes les matrices élémentaires définissent des transvections. Comme les matrices élémentaires engendrent $\mathrm{SL}_n(k)$, les transvections engendrent $\mathrm{SL}(V)$. □

Lemme 10.21. — *Soit $n \geq 2$. Le groupe $\mathrm{PSL}_n(k)$ agit 2-transitivement sur $\mathbb{P}^{n-1}(k)$.*

Démonstration. — La preuve se déduit directement de la 2-transitivité de $\mathrm{SL}_n(k)$. En effet, soit $[v_1] \neq [v_2]$ et $[u_1] \neq [u_2]$ des points de $\mathbb{P}^{n-1}(k)$. Comme v_1 et v_2 (resp. u_1, u_2) sont linéairement indépendants, nous pouvons compléter v_1, v_2 (resp. u_1, u_2) en une base $(v_1, v_2, \ldots, v_n)$ (resp. $(u_1, \ldots, u_n)$) de k^n. Soit $A \in \mathrm{GL}_n(k)$ définie par $Av_j = u_j$, $1 \leq j \leq n$. Nous définissons

$$S : k^n \longrightarrow k^n, v_j \mapsto \begin{cases} u_j & \text{si } 1 \leq j < n \\ \frac{u_n}{\det A} & \text{si } j = n. \end{cases}$$

Ainsi $S \in \mathrm{SL}_n(k)$ et son image $\overline{S} \in \mathrm{PSL}_n(k)$ envoie $[v_i]$ sur $[u_i]$, $i = 1, 2$. □

Théorème 10.22. — *Le groupe $\mathrm{PSL}_n(k)$ est simple pour $n \geq 3$ ou $n = 2$ et $|k| \geq 4$.*

Démonstration. — L'action de $\mathrm{PSL}_n(k)$ sur $\mathbb{P}^{n-1}(k)$ est 2-transitive, donc primitive (lemme 10.17). Pour $x = [x_1 : \cdots : x_n] \in \mathbb{P}^{n-1}(k)$, posons $u = (x_1, \ldots, x_n)$. Le sous-groupe T_x de $\mathrm{PSL}_n(k)$ image du sous-groupe abélien de $\mathrm{SL}_n(k)$ des transvections de vecteur u

$$T_x = \{\overline{\tau}_{\varphi,u} | \varphi : k^n \longrightarrow k \text{ tel que } u \in \ker\varphi\} < \mathrm{PSL}_n(k)$$

ne dépend pas du choix de u (avec $[u] = x$) et la famille de sous-groupes de $\mathrm{PSL}_n(k)$, $(T_x)_{x\in\mathbb{P}^{n-1}(k)}$ satisfait les hypothèses de la proposition 10.18. Comme $\mathrm{PSL}_n(k)$ agit fidèlement (le sous-groupe des éléments agissant trivialement est réduit à 1), tout sous-groupe normal de $\mathrm{PSL}_n(k)$ non trivial doit contenir $D(\mathrm{PSL}_n(k))$. Pour $n \geq 3$ ou $n = 2$ et $|k| \geq 4$, $D(\mathrm{PSL}_n(k)) = \mathrm{PSL}_n(k)$ (voir exemple 10.12). Donc $\mathrm{PSL}_n(k)$ est simple. □

Exercice 10.23. — *Les cas exclus dans le théorème 10.22 ne sont pas des groupes simples car*

$$\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3, \quad \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4.$$

Nous avons donc décrit trois familles infinies de groupes simples (cycliques, alternés et projectifs spéciaux linéaires). Pour en décrire d'autres, nous considérons des groupes agissant sur des ensembles munis de structures supplémentaires. Nous commençons par une étude des représentations, i.e. des actions de G sur un espace vectoriel.

PARTIE III

REPRÉSENTATIONS DES GROUPES

Soit k un corps. Soit G un groupe agissant sur un ensemble X. Soit $\mathcal{F}(X)$ le k-espace vectoriel des fonctions sur X à valeurs dans k. L'ensemble $\mathcal{F}(X)$ est muni d'une action de G via

$$\rho : G \longrightarrow \mathrm{Bij}(\mathcal{F}(X)), \quad \rho(g)(f)(x) = f(g^{-1}x)$$

Cette nouvelle action contient autant d'informations que l'action de G sur X, mais présente néanmoins l'avantage de pouvoir utiliser les techniques d'algèbre linéaire. Ce point de vue extrêmement fertile est l'objet de ce chapitre d'étude des actions linéaires de groupes, dites représentations.

11. Représentations

11.1. Définitions. —

Définition 11.1. — *Soit G un groupe, k un corps et V un k-espace vectoriel. Une représentation linéaire de G dans V est un morphisme de groupes*

$$\rho : G \longrightarrow \mathrm{GL}(V).$$

Une représentation linéaire de G dans V est une action de G sur V qui préserve sa structure de k-espace vectoriel. Ainsi une représentation linéaire est dite fidèle si elle est injective.

Si V est de dimension n, une représentation linéaire de G dans V est dite de dimension n. Le choix d'une base de V permet d'écrire la représentation sous forme matricielle $\rho : G \longrightarrow \mathrm{GL}_n(k)$.

Exemple 11.2. — *Une représentation linéaire de dimension 1 est un morphisme $\rho : G \longrightarrow k^*$. Si G est fini, l'image de ρ est un groupe cyclique inclus dans $\mu_{|G|}(k) = \{\lambda \in k | \lambda^{|G|} = 1\}$.*
La représentation triviale notée triv *de G est la représentation de dimension 1 qui à tout $g \in G$ associe $1 \in \mathrm{GL}_1(k) = k^*$.*
La représentation nulle $G \longrightarrow \mathrm{GL}(\{0\})$ est de dimension 0.

Exemple 11.3. — *Le groupe G des rotations dans le plan réel $\mathbb{R}^2$ admet une représentation de dimension 2 :*

$$G \longrightarrow \mathrm{GL}_2(\mathbb{R}), r_\theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Définition 11.4. — *Si $G < \mathrm{GL}(V)$, l'inclusion $G \longrightarrow \mathrm{GL}(V)$ est appelée la représentation standard.*

Définition 11.5. — *Si $(e_1, \ldots, e_n)$ est une base de k^n, nous définissons une représentation de $\mathfrak{S}_n$ dans k^n via $\rho(\sigma)(e_i) = e_{\sigma(i)}$, $1 \leq i \leq n$. Cette représentation est dite représentation de permutation et les matrices $\rho(\sigma)$ sont dites matrices de permutation.*

Définition 11.6. — *Soit G un groupe fini et $\mathcal{F}(G)$ est l'espace vectoriel des applications de G dans k. Si $\delta_g : G \longrightarrow k$ est la fonction caractéristique de l'élément g de G, la famille $(\delta_g)_{g \in G}$ forme une base du k-espace vectoriel $\mathcal{F}(G)$ de dimension $|G|$.*
Le groupe G agit sur $\mathcal{F}(G)$ via la représentation dite régulière $(\mathcal{F}(G), \rho_{\mathrm{reg}})$:

$$\rho_{\mathrm{reg}} : G \longrightarrow \mathrm{GL}(\mathcal{F}(G)), \rho_{\mathrm{reg}}(g)(f)(x) = f(g^{-1}x), g \in G, f \in \mathcal{F}(G), x \in G.$$

La représentation régulière est la composée de l'inclusion $G \longrightarrow \mathfrak{S}_{|G|}$ avec la représentation de permutation.

Exemple 11.7. — *Le groupe $\mathfrak{S}_4$ s'identifie au sous-groupe de $\mathrm{O}_3(\mathbb{R})$ formé des isométries de $\mathbb{R}^3$ qui laissent invariantes un tétraèdre régulier centré à l'origine (proposition 9.24). Il s'identifie également au groupe des isométries positives de $\mathbb{R}^3$ qui laissent invariant le cube (proposition 9.25). Il s'agit de deux représentations linéaires du groupe $\mathfrak{S}_4$ de natures différentes. Par exemple les isométries du tétraèdre ne sont pas toutes de déterminant 1, contrairement aux isométries positives du cube. La notion de représentations équivalentes précice cette observation.*

Définition 11.8. — *Un morphisme (ou opérateur d'entrelacement) entre des représentations (V, ρ) et (V', ρ') est une application linéaire $f : V \longrightarrow V'$ telle que*

$$\forall g \in G, f \circ \rho(g) = \rho'(g) \circ f.$$

L'espace des morphismes entre (V, ρ) et (V', ρ') est noté $\mathrm{Hom}_G(V, V')$.
Si l'opérateur d'entrelacement f entre (V, ρ) et (V', ρ') est inversible, les représentations ρ et ρ' sont dites équivalentes.

Exemple 11.9. — *En dimension finie, si (V, ρ) et (V', ρ') sont équivalentes, en identifiant V et V', les matrices représentatives de ρ et ρ' sont reliées par une transformation de similitude et peuvent être considérées comme différant par un changement de base. Il n'y a donc pas lieu de distinguer fondamentalement deux représentations équivalentes.*

11.2. Représentations irréductibles. —

Définition 11.10. — *Une sous-représentation de (V, ρ) est un sous-espace vectoriel $W \subset V$ stable sous G, dit sous-espace G-invariant. Dans ce cas nous disposons canoniquement de représentations induites sur W et sur le quotient V/W.*

Exemple 11.11. — *Soit (V, ρ) une représentation de G. Le sous-espace vectoriel des vecteurs fixes sous G*

$$V^G = \{v \in V | \forall g \in G, \rho(g)v = v\}$$

est un sous-espace G-invariant.

Exemple 11.12. — *Si $V = k^n$ est la représentation de permutation du groupe $\mathfrak{S}_n$, l'hyperplan*

$$V_0 = \left\{ (x_1, \ldots, x_n) \in V | \sum_{i=1}^{n} x_i = 0 \right\}$$

est une sous-représentation de V ainsi que la droite supplémentaire $V_1 = k(1, \ldots, 1)$.

Exemple 11.13. — *Si f est un morphisme de (V, ρ) dans (V', ρ') alors* $\ker f$ *(resp.* $\operatorname{im} f$*) est une sous-représentation de V (resp. V') et f induit une équivalence de représentations*

$$f : V/\ker f \longrightarrow \operatorname{im} f.$$

Exemple 11.14. — *Si (V_1, ρ_1), (V_2, ρ_2) sont deux représentations de G, nous pouvons construire une représentation $(V_1 \oplus V_2, \rho)$, via $\rho(g) = (\rho_1(g), \rho_2(g))$. Les sous-espaces V_1 et V_2 de $V = V_1 \oplus V_2$ sont invariants par (V, ρ).*
Réciproquement si le sous-espace V_1 de (V, ρ) est G-invariant et admet un supplémentaire V_2 G-invariant alors (V, ρ) est équivalente à $V_1 \oplus V_2$.
Si V est de dimension finie, cela se traduit simplement sur les matrices de la représentation, qui sont diagonales par blocs.

Si W est une sous-représentation de V, il n'existe pas en général de supplémentaire G-invariant de W dans V.

Exemple 11.15. — *Le groupe $G < \mathrm{GL}_2(k)$ des matrices triangulaires supérieures se représente dans $V = k^2$ par la représentation standard. La droite $W = ke_1$ est une sous-représentation dépourvue de suppémentaire G-invariant.*
Si $k = \mathbb{F}_p$, cela fournit un exemple avec un groupe G fini de cardinal $p(p-1)^2$.

Définition 11.16. — *Une représentation V est irréductible si elle est non nulle et si ses seules sous-représentations sont 0 et V.*

Exemple 11.17. — *Pour $n \geq 3$ la représentation standard du groupe diédral D_n dans $\mathbb{R}^2$ (ou $\mathbb{C}^2$) est irréductible car aucune droite n'est laissée stable par tous les éléments de D_n.*

Exemple 11.18. — *Si G est abélien et k est algébriquement clos ($k = \mathbb{C}$ par exemple), les seules représentations irréductibles V de dimension finie de G sont de dimension 1. En effet, soit $g \in G$ et $W \subset V$ un sous-espace propre (non nul) de $\rho(g)$, pour la valeur propre $\lambda \in k$ (qui existe car k algébriquement clos). Comme G est abélien, pour tout $h \in G$ et $w \in W$,*

$$\rho(g)(\rho(h)(w)) = \rho(h)(\rho(g)(w)) = \rho(h)(\lambda w) = \lambda \rho(h)(w).$$

Le sous-espace W est G-stable, donc $W = V$, car V irréductible. Donc $\rho(g)$ est une homothétie pour tout $g \in G$. Toute droite D est alors G-stable, donc $V = D$ est de dimension 1.
En particulier, nous disposons de n représentations complexes irréductibles de $\mathbb{Z}/n\mathbb{Z}$:

$$\rho_j : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^\times, \bar{\ell} \mapsto \exp(2\ell j\pi i/n).$$

Exemple 11.19. — *Il faut souligner l'importance du corps de base dans la discussion de l'irréductibilité. La représentation de l'exemple 11.3 est irréductible sur un $\mathbb{R}$-espace vectoriel, mais pas sur un $\mathbb{C}$-espace vectoriel. Après changement de base, nous pouvons l'écrire*

$$r_\theta \mapsto \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Exemple 11.20. — *Soit $H \lhd G$, $\pi : G \longrightarrow G/H$ le morphisme quotient et $\bar{\rho} : G/H \longrightarrow \mathrm{GL}(V)$ une représentation irréductible. Alors $\rho = \bar{\rho} \circ \pi : G \longrightarrow \mathrm{GL}(V)$ est une représentation irréductible de G.*

Remarque 11.21. — *Si $\dim V \geq 2$, les représentations standard de $\mathrm{GL}(V), \mathrm{SL}(V)$ (et du groupe symplectique $\mathrm{Sp}(V)$ que nous étudierons en §19) sont irréductibles puisque ces groupes opèrent transitivement sur $V - \{0\}$. C'est également le cas pour le groupe orthogonal $\mathrm{O}_n(\mathbb{R})$ qui opère transitivement sur la sphère unité $\mathbf{S}^{n-1}$, qui engendre $\mathbb{R}^n$ (voir §21).*

11.3. Représentations des groupes finis. — L'objet de ce paragraphe est la décomposition des représentations des groupes finis en somme de représentations irréductibles sous de bonnes hypothèses sur le corps k (la caractéristique du corps k ne divise pas $|G|$, i.e car$k$ $\not|\,|G|$).
Pour les groupes finis, la pluspart des résultats que nous obtenons repose sur la sommation sur les éléments du groupe. Ces résultats peuvent se géneraliser à des groupes infinis pourvu que nous puissions donner un sens à cette sommation. Sauf mention contraire, nous supposons dorénavant que G est un groupe fini.

Lemme 11.22. — *(Théorème de Maschke). Si G est un groupe fini tel que* car$k$ *ne divise pas $|G|$ et (V, ρ) est une représentation de G, tout sous-espace G-invariant de V admet un supplémentaire G-invariant.*

Démonstration. — Soit W_1 un supplémentaire quelconque dans V d'un sous-espace G-invariant W et p_1 la projection sur le sous-espace W parallèlement à W_1. Alors

$$p_2 = \frac{1}{|G|} \sum_{g \in G} \rho(g) p_1 \rho(g)^{-1}$$

est un projecteur ($p_2 \circ p_2 = p_2$) d'image W dont le noyau est stable par G (si $p_2(y) = 0$, $p_2(\rho(h)(y)) = \rho(h)^{-1}(p_2(y)) = 0$). □

D'après l'exemple 11.15, dans le cas où la caractéristique de k divise l'ordre $|G|$, la conclusion du théorème de Maschke n'est plus valable.
Le théorème suivant se déduit du théorème de Maschke par récurrence sur la dimension de la représentation.

Théorème 11.23. — *Soit G un groupe fini avec* car$k \not| |G|$. *Toute représentation de G de dimension finie est somme directe de représentations irréductibles.*

La caractérisation de cette décomposition en somme directe de représentations irréductibles (Corollaire 11.27) se déduit du lemme technique mais important suivant :

Lemme 11.24. — *(Lemme de Schur). Soit G un groupe fini. Soit (V, ρ) et (V', ρ') deux représentations irréductibles de G et $f : V \longrightarrow V'$ un morphisme (opérateur d'entrelacement) de l'une dans l'autre. Alors*
i. $f = 0$ ou les représentations sont équivalentes (f isomorphisme).
ii. Si $\rho = \rho'$ et k algébriquement clos, l'application f est une homothétie.

Démonstration. — En effet $\ker f$ et $\operatorname{im} f$ sont G-invariants (d'où i). Comme k est algébriquement clos, le morphisme f admet une valeur propre λ. De plus, $\ker(f - \lambda Id_V) \neq \{0\}$ est G-invariant (d'où ii). □

Exemple 11.25. — *Si les représentations (V, ρ) et (V', ρ') ne sont pas irréductibles, les conclusions du lemme de Schur ne sont plus valables : la représentation $\rho : \mathbb{R} \longrightarrow \mathrm{GL}_2(\mathbb{R}), a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ commute avec le morphisme non injectif défini par $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.*

Corollaire 11.26. — *Soit G un groupe fini avec* car$k \not| |G|$. *La représentation régulière de G se décompose en une somme finie de représentations irréductibles*

$$\mathcal{F}(G) = \oplus R_i$$

et pour toute représentation irréductible (V, ρ) de G, il existe i pour lequel (V, ρ) équivalente à (R_i, ρ_i).
Par conséquent il n'y a, à isomorphisme près, qu'un nombre fini de représentations irréductibles de G et chacune est de dimension $\leq |G|$.

Démonstration. — Soit (V, ρ) une représentation irréductible de G. Pour $v_0 \in V$, nous définissons une application linéaire

$$f : \mathcal{F}(G) \longrightarrow V, \ \ (u : G \longrightarrow k) \mapsto \sum_{g \in G} u(g)\rho(g)(v_0).$$

C'est un opérateur d'entrelacement de $(\mathcal{F}(G), \rho_{\text{reg}})$ dans (V, ρ), car pour tout $h \in G$, $u \in \mathcal{F}(G)$,

$$f(\rho_{\text{reg}}(h)(u)) = \sum_{g\in G} \rho_{\text{reg}}(h)(u)(g)\rho(g)(v_0) = \sum_{g\in G} u(h^{-1}g)\rho(g)(v_0)$$
$$= \sum_{g'\in G} u(g')\rho(hg')(v_0) = \rho(h)(f(u)).$$

Si $v_0 \neq 0$ l'application f n'est pas nulle (car $f(\delta_e) = v_0$). Comme V est irréductible f est surjective, donc il existe au moins un i tel que $f_{|R_i}$ est non nul. Par le lemme de Schur, $f_{|R_i}$ est un isomorphisme. □

Corollaire 11.27. — *Soit G un groupe fini avec* car$k \not| |G|$ *et soient $\rho_1, \ldots, \rho_\ell$ les représentations irréductibles de G. Toute représentation de G de dimension finie se décompose en $\oplus \rho_i^{n_i}$ où les entiers naturels n_i sont uniquement déterminés par la représentation.*

Démonstration. — Nous raisonnons par récurrence sur la dimension de la représentation V. Soit $V = \oplus_{i\in I} V_i \simeq \oplus_{j\in J} W_j$ deux décompositions de la représentation V en représentations irréductibles. Nous montrons qu'à permutation près les $(V_i)_{i\in I}$ et $(W_j)_{j\in J}$ sont la même collection de représentations. Nous disposons d'un isomorphisme

$$f : \oplus_{i\in I} V_i \longrightarrow \oplus_{j\in J} W_j$$

et de projections $p_i : V \longrightarrow V_i$, $i \in I$ et $q_j : V \longrightarrow W_j$, $j \in J$. Pour $j \in J$, posons

$$u_j : V_1 \longrightarrow V_1, u_j = p_1 \circ {f^{-1}}_{|W_j} \circ q_j \circ f_{|V_1}.$$

Ainsi

$$\sum_{j\in J} u_j = p_1 \circ \left(\sum_{j\in j} {f^{-1}}_{|W_j} \circ q_j \right) \circ f_{|V_1} = p_1 \circ f^{-1} \circ f_{|V_1} = \text{id}_{V_1}.$$

Donc un des u_j est non nul, quitte à renuméroter J, nous pouvons supposer que c'est u_1 et en appliquant le lemme de Schur, nous obtenons des isomorphismes $q_1 \circ f_{|V_1} : V_1 \longrightarrow W_1$ et $p_1 \circ {f^{-1}}_{|W_1} : W_1 \longrightarrow V_1$.
Pour appliquer l'hypothèse de récurrence, il suffit de montrer que le morphisme de représentations

$$\psi = (\text{Id}_V - q_1) \circ f_{|\oplus_{i\in I-\{1\}} V_i} \oplus_{i\in I-\{1\}} V_i \longrightarrow \oplus_{j\in J-\{1\}} W_j$$

entre représentations de même dimension est encore un isomorphisme. Ce qui est le cas car il est injectif : si $x \in \ker \psi$, $f(x) \in W_1$, $p_1(f^{-1}(f(x))) = p_1(x) = 0$ et comme $p_1 \circ {f^{-1}}_{|W_1}$ est bijectif, $f(x) = 0$ et $x = 0$. □

Exemple 11.28. — *La somme directe en représentations irréductibles*

$$V = \oplus V_i$$

n'est pas unique. Par exemple la représentation constante $\rho : G \longrightarrow \text{GL}_n(k)$, $g \mapsto \text{Id}$ se décompose en somme directe de n droites linéairement indépendantes.

12. Tenseur

Une méthode efficace pour construire des représentations irréductibles consiste à faire le produit tensoriel de représentations connues et à le décomposer en représentations irréductibles.

Remarque 12.1. — *C'est la situation rencontrée en mécanique quantique quand la transformation des composantes d'un système est connue et que nous étudions comment le système entier se transforme (système de deux particules de spin j_1 et j_2 par exemple).*

12.1. Produit tensoriel. — Commençons par une courte introduction sur le produit tensoriel.

Définition 12.2. — *Soit k un corps et V, W des k-espaces vectoriels. Un produit tensoriel de V et W est la donnée d'un k-espace vectoriel T et d'une application bilinéaire $t : V \times W \longrightarrow T$ satisfaisant la propriété universelle : si $b : V \times W \longrightarrow U$ est une application bilinéaire, il existe une unique application linéaire $\hat{b} : T \longrightarrow U$ telle que que $b = \hat{b} \circ t$.*

Notons $E \subset k^{V \times W}$, le k-espace vectoriel des combinaisons à support fini à coefficients dans k de la forme

$$E = \left\{ \sum_{v \in V, w \in W} a_{v,w} e_{(v,w)}, a_{v,w} \in k \text{ presque tous nuls} \right\}.$$

Soit F le sous-k-espace vectoriel de E engendré par

$$e_{(v+v',w)} - e_{(v,w)} - e_{(v',w)}, \quad e_{(v,w+w')} - e_{(v,w)} - e_{(v,w')}$$

$$e_{(av,w)} - a e_{(v,w)}, \quad e_{(v,aw)} - a e_{(v,w)}$$

pour $v, v' \in V$, $w, w' \in W$ et $a \in k$. Le k-espace vectoriel E/F muni de l'application bilinéaire canonique

$$\varphi : V \times W \longrightarrow E/F, (v, w) \mapsto \overline{e_{(v,w)}}$$

est un produit tensoriel de V par W, il est noté $V \otimes W$. L'image par φ d'un élément $(v, w) \in V \times W$ est appelé tenseur pur et noté $v \otimes w$.

Théorème 12.3. — *Soit k un corps et V, W des k-espaces vectoriels. Il existe un produit tensoriel de V et W, noté $V \otimes_k W$ (ou s'il n'y a pas d'ambiguité $V \otimes W$). Il est unique à unique isomorphisme près.*

Démonstration. — L'existence est obtenue par la construction de $(V \otimes W, \varphi)$. Par propriété universelle, le produit tensoriel est unique à unique isomorphisme près. En effet notons $((V \otimes W)', \psi)$ un autre produit tensoriel. Il existe des

applications uniques $\alpha : V \otimes W \longrightarrow (V \otimes W)'$ et $\beta : (V \otimes W)' \longrightarrow V \otimes W$ avec $\psi = \alpha \circ \varphi$ et $\varphi = \beta \circ \psi$. Donc

$$\varphi = \beta \circ \psi = \beta \circ (\alpha \circ \varphi) = (\beta \circ \alpha) \circ \varphi.$$

Comme $\varphi = \mathrm{Id}_{V\otimes} \circ \varphi$, par unicité $\beta \circ \alpha = \mathrm{Id}_{V\otimes W}$, et de même $\alpha \circ \beta = \mathrm{Id}_{(V\otimes W)'}$. □

Exemple 12.4. — *(Fonctorialité). Si nous avons des applications linéaires*

$$f : V \longrightarrow V', \;\; g : W \longrightarrow W',$$

il existe une et une seule application linéaire

$$f \otimes g : V \otimes W \longrightarrow V' \otimes W'$$

telle que

$$(f \otimes g)(v \otimes w) = f(v) \otimes g(w) \text{ pour tous } v \in V, w \in W.$$

De plus $(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$.

Exemple 12.5. — *(Commutativité, associativité, élément neutre, distributivité par rapport à la somme directe) Soit V_1, V_2, V_3 des k-espaces vectoriels, nous avons les isomorphismes canoniques*

$$V_1 \otimes V_2 \simeq V_2 \otimes V_1, v_1 \otimes v_2 \mapsto v_2 \otimes v_1,$$

$$(V_1 \otimes V_2) \otimes V_3 \simeq V_1 \otimes (V_2 \otimes V_3), (v_1 \otimes v_2) \otimes v_3 \mapsto v_1 \otimes (v_2 \otimes v_3),$$

$$V_1 \simeq V_1 \otimes k, v \mapsto v \otimes 1, \;\; V_1 \simeq k \otimes V_1, v \mapsto 1 \otimes v,$$

$$(V_1 \oplus V_2) \otimes V_3 \simeq (V_1 \otimes V_3) \oplus (V_2 \otimes V_3), (v_1 + v_2) \otimes v_3 \mapsto v_1 \otimes v_3 + v_2 \otimes v_3.$$

Toutes ces applications, définies sur les tenseurs purs, s'étendent par linéarité à tous les éléments du produit tensoriel.
En particulier en dimension finie, nous en déduisons que si $(v_i)_{i\in I}$ est une base de V et $(w_j)_{j\in J}$ est une base de W, alors $(v_i \otimes w_j)_{(i,j)\in I\times J}$ est une base de $V \otimes W$ et $\dim_k V \otimes W = \dim_k V \dim_k W$.
Si V a pour base $(v_i)_{i\in I}$, V' a pour base $(v'_{i'})_{i'\in I'}$, W a pour base $(W_j)_{j\in J}$ et W' a pour base $(w'_{j'})_{j'\in J'}$ et $f : V \longrightarrow V'$, $g : W \longrightarrow W'$ de matrices respectives $A = (a_{ii'})_{(i,i')\in I\times I'}$, $B = (b_{jj'})_{(j,j')\in J\times J'}$ dans ces bases, alors

$$(f \otimes g)(v_i \otimes w_j) = \sum_{i'\in I', j'\in J'} a_{ii'} b_{jj'} v'_{i'} \otimes w'_{j'}.$$

Donc la matrice de $f \otimes g$ dans les bases $(v_i \otimes w_j)$ de $V \otimes W$ et $(v'_{i'} \otimes W'_{j'})$ de $V' \otimes W'$ est

$$A \otimes B = (a_{ii'} b_{jj'})_{(i,j)\in I\times J, (i',j')\in I'\times J'}.$$

Par exemple si tous ces espaces sont de dimension 2 :

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{12}b_{11} & a_{12}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{12}b_{21} & a_{12}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

En particulier $\mathrm{rg}(A \otimes B) = \mathrm{rg}(A)\mathrm{rg}(B)$ *et si* A *et* B *sont carrées de taille respective* a *et* b, $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\,\mathrm{tr}(B)$, $\det A \otimes B = (\det A)^b (\det B)^a$.

Exemple 12.6. — *Soit* V *un* k*-espace vectoriel et* k' *un sur-corps de* k, $k \subset k'$. *Comme* k' *est un* k*-espace vectoriel, nous pouvons former le* k*-espace vectoriel*

$$V' = k' \otimes_k V$$

et donner à V' *une structure de* k'*-espace vectoriel canonique. Le* k'*-espace vectoriel* V' *est obtenu à partir de* V *par extension des scalaires de* k *à* k'. *Si* $(v_i)_{i\in I}$ *est une* k*-base de* V, $(1 \otimes v_i)_{i\in I}$ *est une* k'*-base de* V' *et* $\dim_k V = \dim_{k'} V'$.

Exemple 12.7. — *La construction ci-dessus s'adapte sans peine pour définir le produit tensoriel d'un nombre fini de* k*-espaces vectoriels : nous définissons* $V_1 \otimes \cdots \otimes V_n$ *comme le quotient de* $V_1 \times \cdots \times V_n$ *par le* k*-espace vectoriel qui doit être annulé par toute application* n*-linéaire.*
De même, si nous avons des applications linéaires $f_i : V_i \longrightarrow W_i$, *nous obtenons une application linéaire unique*

$$f_1 \otimes \cdots \otimes f_n : V_1 \otimes \cdots \otimes V_n \longrightarrow W_1 \otimes \cdots \otimes W_n,$$
$$(f_1 \otimes \cdots \otimes f_n)(v_1 \otimes \cdots \otimes v_n) = f_1(v_1) \otimes \cdots \otimes f_n(v_n).$$

Remarque 12.8. — *Soient* $V_1, \ldots, V_n$ *des espaces vectoriels de dimension finie. Tout élément de* $V_1 \otimes \cdots \otimes V_n$ *s'écrit comme somme de tenseurs purs. En général, nous ne savons pas quel est le nombre nécessaire de tenseurs purs.*

Introduisons encore quelques définitions afin de faire un premier pont entre le langage algébrique et la physique ou le calcul différentiel. Nous notons V un espace vectoriel de dimension finie n sur un corps k et $V^* = \mathrm{Hom}(V, k)$ son dual. Soit $r \in \mathbb{N}$, nous définissons le produit tensoriel

$$T^r V = \underbrace{V \otimes \cdots \otimes V}_{r \text{ fois}}, \quad T^0 V = k$$

Remarque 12.9. — *La somme* $\oplus_{r\geq 0} T^r V$ *a une structure de* k*-algèbre.*

La somme

Définition 12.10. — *Soit* $r, s \in \mathbb{N}$. *Un tenseur* r *fois covariant et* s *fois contravariant est un élément*

$$T \in T^r V^* \otimes T^s V.$$

Soit $(e_i)_{1\leq i\leq n}$ une base de V de base duale $(e^i)_{1\leq i\leq n}$, un tenseur $T\in T^rV^*\otimes T^sV$ s'écrit

$$T = \sum_{i_1,\dots i_s,j_1,\dots,j_r} T^{i_1\dots i_s}_{j_1\dots j_r} e^{j_1}\otimes\cdots\otimes e^{j_r}\otimes e_{i_1}\otimes\cdots\otimes e_{i_s},$$
$$T^{i_1\dots i_s}_{j_1\dots j_r} e^{j_1}\otimes\cdots\otimes e^{j_r}\otimes e_{i_1}\otimes\cdots\otimes e_{i_s}.$$

Avec la convention usuelle en physique de sommation sur les indices répétés en haut et en bas.

Exemple 12.11. — *Soit $P=(P^j_i)_{1\leq i,j\leq n}$, la matrice de passage de la base $(e_i)_{1\leq i\leq n}$ à la base $(e'_i)_{1\leq i\leq n}$: $e'_i = P^j_i e_j$. Pour un tenseur $T=(T^{i_1\dots i_s}_{j_1\dots j_r})$, r fois covariant et s fois contravariant, ses coordonnés dans la base (e'_i) sont*

$$T'^{i'_1\dots i'_s}_{j'_1\dots j'_r} = (P^{-1})^{i'_1}_{i_1}\cdots(P^{-1})^{i'_s}_{i_s} P^{j_1}_{j'_1}\cdots P^{j_r}_{j'_r} T^{i_1\dots i_s}_{j_1\dots j_r}.$$

Revenons à présent à la théorie des représentations.

Définition 12.12. — *Si $\rho_i : G\longrightarrow \mathrm{GL}(V_i)$ $i=1,2$ sont deux représentations du groupe G, nous définissons leur produit tensoriel*

$$\rho=\rho_1\otimes\rho_2 : G\longrightarrow \mathrm{GL}(V_1\otimes V_2),$$

$$\rho(g)(v_1\otimes v_2)=\rho_1(g)(v_1)\otimes\rho_2(g)(v_2), g\in G, v_1\in V_1, v_2\in V_2.$$

Exemple 12.13. — *Soient (V,ρ_V) et (W,ρ_W) deux représentations de G et $V^*=\mathrm{Hom}(V,k)$ le dual de V. Ainsi $V^*\otimes W=\mathrm{Hom}_k(V,W)$ et nous pouvons former la représentation $(V^*\otimes W,\rho)$ via $\rho(g)(f)=\rho_W(g)\circ f\circ\rho_V(g)^{-1}$. En particulier l'espace des morphismes de représentations de V dans W est*

$$\mathrm{Hom}_G(V,W)=\mathrm{Hom}_k(V,W)^G.$$

Exemple 12.14. — *Si (ρ_1,V_1) est une représentation du groupe G_1 et (ρ_2,V_2) est une représentation du groupe G_2, nous pouvons munir l'espace $V_1\otimes V_2$ d'une représentation notée $\rho_1\square\rho_2$ de $G_1\times G_2$ définie par*

$$(\rho_1\square\rho_2)(g_1,g_2)(v_1\otimes v_2)=\rho_1(g_1)(v_1)\otimes\rho_2(g_2)v_2, v_i\in V_i, g_i\in G_i, i\in\{1,2\}.$$

Remarque 12.15. — *Le produit tensoriel de deux copies de l'espace euclidien de dimension trois ne forme pas une représentation irréductible du groupe des rotations. Il se décompose en la somme directe de trois représentations irréductibles de dimensions respectives $1,3,5$.*
Plus généralement, il est utile de décomposer en somme de représentations irréductibles, les produits tensoriels multiples. Pour cela, nous introduisons les produits extérieurs et les tenseurs symétriques et anti-symétriques (§12.2,12.3).

12.2. Produit extérieur. — Nous construisons le produit extérieur d'espaces vectoriels de façon analogue au produit tensoriel :

Définition 12.16. — *Soit k un corps, $r \in \mathbb{N}$ et V un k-espace vectoriel. La puissance extérieure r-ième $\Lambda^r V$ de V est le quotient de $T^r V$ par le sous-espace vectoriel I^r engendré par les éléments $x_1 \otimes \cdots \otimes x_r$ où $x_i = x_j$ pour deux indices distincts $i \neq j$. La classe de l'élement $x_1 \otimes \cdots \otimes x_r$ dans le quotient $\Lambda^r V$ est notée*

$$x_1 \wedge \cdots \wedge x_r.$$

Exemple 12.17. — *La puissance extérieure satisfait la propriété universelle suivante : pour toute application r-linéaire alternée $\rho : V^r \longrightarrow W$, il existe une unique application linéaire $f : \Lambda^r V \longrightarrow W$ telle que*

$$\begin{array}{ccc} V^r & & \\ c\downarrow & \searrow^{\rho} & \\ \Lambda^r V & \xrightarrow{f} & W \end{array}$$

où c est l'application r-linéaire alternée définie par $c(x_1, \ldots, x_r) = x_1 \wedge \cdots \wedge x_p$.

Exemple 12.18. — *Si $r > n$, $\Lambda^r V = 0$. Plus généralement*

$$\dim_k \Lambda^r V = \binom{n}{r}.$$

Exemple 12.19. — *Il existe une application bilinéaire non dégénérée*

$$\begin{array}{ccc} \Lambda^r(V^*) \times \Lambda^r V & \longrightarrow & k \\ (u_1 \wedge \cdots \wedge u_r, v_1 \wedge \cdots \wedge v_r) & \mapsto & \det(u_i(v_j))_{1 \leq i,j \leq r}. \end{array}$$

12.3. Tenseurs anti-symétriques et symétriques. — Dans ce paragraphe, nous supposons car$k = 0$ et V est un k-espace vectoriel de dimension finie n.
Une permutation $\sigma \in \mathfrak{S}_r$ induit un endomorphisme $\tilde{\sigma}$, k-linéaire de $T^r V$ défini par

$$\tilde{\sigma}(x_1 \otimes \cdots \otimes x_r) = x_{\sigma(1)} \otimes \cdots x_{\sigma(r)}.$$

Définition 12.20. — *Un tenseur $t \in T^r V$ est dit anti-symétrique si $\tilde{\sigma}(t) = \varepsilon(\sigma) t$ pour tout $\sigma \in \mathfrak{S}_r$.*
Un tenseur $t \in T^r V$ est dit symétrique si $\tilde{\sigma}(t) = t$ pour tout $\sigma \in \mathfrak{S}_r$.

Notons $A^r V \subset T^r V$ le sous-espace vectoriel des tenseurs anti-symétriques et $S^r V \subset T^r V$ le sous-espace vectoriel des tenseurs symétriques.

Exercice 12.21. — *Soit V un k-espace vectoriel de dimension n et $r \in \mathbb{N}$. Alors*

$$\dim S^r V = \binom{n+r-1}{r}, \dim A^r V = \binom{n}{r}.$$

Nous définissons l'application linéaire d'antisymétrisation (ici nous utilisons l'hypothèse car$k = 0$ ou car$k > r$)

$$p : T^r V \longrightarrow T^r V, \quad t \mapsto \frac{1}{r!} \sum_{\sigma \in \mathfrak{S}_r} \varepsilon(\sigma) \tilde{\sigma}(t),$$

et l'application de symétrisation

$$q : T^r V \longrightarrow T^r V, \quad t \mapsto \frac{1}{r!} \sum_{\sigma \in \mathfrak{S}_r} \tilde{\sigma}(t).$$

L'application d'antisymétrisation permet de réaliser $\Lambda^r V$ comme sous-espace vectoriel de $T^r V$. En effet,

Lemme 12.22. — *Supposons* car$k = 0$ *ou* car$k > r$. *L'application p est un projecteur de noyau I^r et d'image $A^r V$. Elle induit donc un isomorphisme $A^d V \simeq \Lambda^r V$.*

Démonstration. — Nous vérifions que $\mathrm{Im} p \subset A^r V$ et p induit l'identité sur $A^r V$, donc $\mathrm{Im} p = A^r V$. En remarquant que $N =< t - \varepsilon(\sigma)\tilde{\sigma}(t), t \in T^r V, \sigma \in \mathfrak{S}_r >$ est inclus dans $\ker p$ et

$$t = p(t) + t - p(t), \text{ avec } t - p(t) \in N.$$

nous obtenons $T^r V = A^r V \oplus N$, donc $N = \ker p$. Ainsi $A^r V \simeq T^r V / \ker p \simeq \Lambda^r V$. □

De même, nous établissons :

Lemme 12.23. — *Supposons* car$k = 0$ *ou* car$k > r$. *L'application q est un projecteur d'image $S^r V$. Elle induit donc un isomorphisme $S^r V \simeq T^r V / \ker q$.*

Remarque 12.24. — *Soit V une k-représentation du groupe G. Alors pour tout $r \geq 1$, $\Lambda^r V$ et $S^r V$ sont des représentations de G.*
De plus si car$k \neq 2$, *le produit tensoriel $V \otimes V$ se décompose*

$$T^2 V = V \otimes V = \Lambda^2 V \oplus S^2 V$$

avec $\Lambda^2 V$ espace engendré par $x \wedge y = \frac{1}{2} x \otimes y - y \otimes x$, dit carré extérieur et $S^2 V$ engendré par $xy = \frac{1}{2}(x \otimes y + y \otimes x)$, dit carré symétrique. De plus (en notant χ_V la trace de la représentation (V, ρ), $\chi_V(g) = \mathrm{tr}\, \rho(g), g \in G$),

$$\chi_{S^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)), \quad \chi_{\Lambda^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)).$$

Remarque 12.25. — *Pour $r = 3$, l'inclusion $T^r V \subset \Lambda^r V \oplus S^r V$ est stricte. En effet,*

$$\dim T^3 V = n^3 > \dim \Lambda^3 V + \dim S^3 V = \binom{n}{3} + \binom{n+2}{3}.$$

En général, nous avons une décomposition sous la forme

$$T^dV = \oplus_{\substack{\lambda_1 \geq \cdots \geq \lambda_n \geq 0,\\ \lambda_1+\cdots+\lambda_r}} (S_{(\lambda_1,\ldots,\lambda_n)}V)^{m_\lambda}$$

où $m_\lambda > 0$ *et*
- $S_{(1,\ldots,1)}V \simeq \Lambda^r V$,
-$S_{(r)}V \simeq S^r V$,
- $S_{(\lambda_1,\ldots,\lambda_n)}V$ *est une représentation irréductible de* $\mathrm{GL}(V)$ *de dimension*

$$\prod_{1\leq i<j\leq r} \frac{\lambda_i - \lambda_j + j - i}{j-i}.$$

Lorsque le corps k est algébriquement clos, la théorie des caractères donne un moyen efficace pour déterminer les représentations irréductibles d'un groupe fini et la décomposition des représentations en somme de représentations irréductibles.

13. Caractères des représentations

Dans cette partie, sauf mention contraire explicite, k désigne un algébriquement clos (nous le notons parfois $\bar{k}$ pour rappeler qu'il est supposé algébriquement clos et que cette hypothèse joue un rôle important dans le résultat ou la preuve présentés), G un groupe fini d'ordre $|G|$, la caractéristique de $\bar{k}$ ne divisant pas $|G|$. Le lecteur peu familier avec la théorie des corps, peut supposer que $\bar{k} = \mathbb{C}$ dans cette partie §13.

13.1. Définitions. —

Définition 13.1. — *Le caractère d'une représentation de dimension finie* (V,ρ) *de* G*, est l'application* $\chi : G \longrightarrow k$ *donnée par la trace de la représentation* $\chi(g) = \operatorname{tr}\rho(g)$*. Le degré d'un caractère est la dimension de la représentation associée.*

Nous notons χ, χ_ρ ou χ_V le caractère associé à la représentation (V,ρ) suivant le contexte. Il est indépendant du choix de la base de V.
Le caractère évalué en $e \in G$ est la dimension de ρ :

$$\chi_\rho(e) = \dim\rho = \dim V.$$

L'énoncé suivant s'obtient directement à partir des propriétés de la trace matricielle.

Proposition 13.2. — *Soient* (V,ρ) *et* (W,ρ') *deux représentations de dimension finie* G*.*
i. Si V *et* W *sont équivalentes, elles ont même caractère,*
ii. $\chi_{V\oplus W} = \chi_V + \chi_W$*,*

iii. Si $W \subset V$ est une sous-représentation, $\chi_V = \chi_W + \chi_{V/W}$,
iv. $\chi_{V\otimes W} = \chi_V \chi_W$.

Exemple 13.3. — *Soit $\sigma \in \mathfrak{S}_n$ alors le caractère de la représentation standard de $\mathfrak{S}_n$ dans $\mathbb{C}^n$ est le nombre de points fixes de σ.*

Exemple 13.4. — *Considérons le caractère d'une représentation de permutation ρ définie à partir d'une opération d'un groupe fini G sur un ensemble fini E. Pour $g \in G$, nous interprètons $\chi_\rho(g)$ comme le nombre $|E^g|$ des éléments de E stables par g.*
En particulier, le caractère de la représentation régulière est

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & si\ g = e, \\ 0 & si\ g \neq e. \end{cases}$$

Exemple 13.5. — *Le caractère de la représentation standard de D_n dans $\mathbb{C}^2$ est donné par*

$$\chi(r^j) = 2\cos 2j\pi/n,\ \chi(r^j s) = 0, 0 \leq j \leq n-1.$$

Remarque 13.6. — *Si G est abélien, ses représentations irréductibles sont de dimension 1, donc coïncident avec leur caractère. Considérons le groupe abélien infini $U(1)$ des rotations du cercle unité $\mathbf{S}^1$. Les représentations irréductibles sont*

$$\chi_n(\phi) = \frac{1}{2\pi} e^{in\phi}, n \in \mathbb{Z}.$$

Toute fonction complexe (continue) $f : \mathbf{S}^1 \longrightarrow \mathbb{C}$, s'écrit

$$f(\phi) = \sum_{n\in\mathbb{Z}} c_n \chi_n(\phi)$$

où $c_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(\phi)e^{-in\phi}d\phi$. La théorie des caractères est une version finie (et non abélienne) des séries/transformations de Fourier.

13.2. Fonctions centrales. — Le caractère prend la même valeur dans une classe de conjugaison de G :

$$\chi(g) = \chi(hgh^{-1}), \chi(gh) = \chi(hg),\ \ g, h \in G.$$

Le caractère est une fonction centrale de G au sens suivant :

Définition 13.7. — *Une fonction centrale de G est une fontion $f : G \longrightarrow k$ invariante par conjugaison :*

$$\forall g, h \in G,\ f(hgh^{-1}) = f(g).$$

Le k-espace vectoriel des fonctions centrales est noté $\mathcal{C}(G)$. Il est de dimension le nombre de classes de conjugaison de G.

Le k-espace vectoriel $\mathcal{F}(G)$ est muni d'une forme bilinéaire symétrique

$$< f, f' >= \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) f'(g) =< f', f > .$$

Comme $< f, \delta_g >= \frac{1}{|G|} f(g^{-1})$, cette forme est non dégénérée :

$$\forall f \in \mathcal{F}(G) - \{0\}, \exists f' \in \mathcal{F}(G), < f, f' > \neq 0.$$

Soit (V, ρ_V) et (W, ρ_W) deux représentations de G, nous posons

$$\pi : \mathrm{Hom}(V, W) \longrightarrow \mathrm{Hom}(V, W), \;\; u \mapsto \frac{1}{|G|} \sum_{g \in G} \rho_W(g) \circ u \circ \rho_V(g)^{-1}.$$

Lemme 13.8. — *L'endomorphisme* π *de* $\mathrm{Hom}(V, W)$ *est un projecteur d'image* $\mathrm{Hom}_G(V, W)$ *et*

$$\mathrm{tr}(\pi) =< \chi_V, \chi_W > .$$

Démonstration. — Par définition,

$$\mathrm{Hom}_G(V, W) = \{u \in \mathrm{Hom}(V, W) | \forall h \in G, u \circ \rho_V(h) = \rho_W(h) \circ u\}.$$

L'endomorphisme π est un projecteur d'image $\mathrm{Hom}_G(V, W)$. En effet, si $u \in \mathrm{Hom}_G(V, W)$, $\pi(u) = u$, donc $\mathrm{Hom}_G(V, W) \subset \mathrm{Im}\pi$. Pour $h \in H$, $v \in \mathrm{Hom}(V, W)$,

$$\begin{array}{rcl} \rho_W(h) \circ \pi(v) \circ \rho_V(h)^{-1} & = & \frac{1}{|G|} \sum_{g \in G} \rho_W(h) \circ \rho_W(g) \circ v \circ \rho_V(g)^{-1} \circ \rho_V(h)^{-1} \\ & = & \frac{1}{|G|} \sum_{g \in G} \rho_W(hg) \circ v \circ \rho_V(g^{-1} h^{-1}) \\ & = & \frac{1}{|G|} \sum_{g' \in G} \rho_W(g') \circ v \circ \rho_V(g')^{-1} \\ & = & \pi(v). \end{array}$$

D'où $\mathrm{Im}\pi = \mathrm{Hom}_G(V, W)$ et comme $\pi^2(v) = \pi(v)$, $v \in \mathrm{Hom}(V, W)$, π est un projecteur d'image $\mathrm{Hom}_G(V, W)$. Choisissons des bases de V et de W et notons E_{ij} l'élément de $\mathrm{Hom}(V, W)$ dont la matrice dans ces bases a tous ses coefficients nuls sauf celui situé à la i-ème ligne et la j-ème colonne, qui vaut 1. Les (E_{ij}) forment une base de $\mathrm{Hom}(V, W)$ et nous avons

$$(\rho_W(g) \circ E_{ij} \circ \rho_V(g)^{-1})_{kl} = \rho_W(g)_{ki} \rho_V(g^{-1})_{jl}.$$

Par conséquent,

$$\begin{array}{rcl} \mathrm{tr}(\pi) = \sum_{ij} \pi(E_{ij})_{ij} & = & \sum_{ij} \frac{1}{|G|} \sum_{g \in G} \rho_W(g)_{ii} \rho_V(g^{-1})_{jj} \\ & = & \frac{1}{|G|} \sum_{g \in G} \Big(\sum_i \rho_W(g)_{ii} \Big) \Big(\sum_j \rho_V(g^{-1})_{jj} \Big) \\ & = & \frac{1}{|G|} \sum_{g \in G} \chi_W(g) \chi_V(g^{-1}) \\ & = & < \chi_V, \chi_W > . \end{array}$$

□

Proposition 13.9. — *La famille des* χ_V *pour* V *décrivant l'ensemble des classes d'isomorphisme de représentations irréductibles de* G *est orthonormale.*

Démonstration. — Si V et W sont irréductibles, d'après le lemme de Schur

$$\mathrm{Hom}_G(V,W) = \begin{cases} 0 & \text{si } V \text{ et } W \text{ ne sont pas isomorphes,} \\ \overline{k} & \text{si } V \text{ et } W \text{ sont isomorphes.} \end{cases}$$

Comme la trace d'un projecteur est son rang, le lemme 13.8 implique

$$< \chi_V, \chi_W >= \mathrm{tr}(\pi) = \begin{cases} 0 & \text{si } V \text{ et } W \text{ ne sont pas isomorphes,} \\ 1 & \text{si } V \text{ et } W \text{ sont isomorphes.} \end{cases}$$

□

Lemme 13.10. — *Soit (V,ρ) une représentation de G. Si $f : G \longrightarrow \bar{k}$ est une fonction centrale, $f \in \mathcal{C}(G)$, posons*

$$f_\rho = \frac{1}{|G|} \sum_{g \in G} f(g)\rho(g^{-1}) \in \mathrm{End}(V).$$

i. Nous avons $f_\rho \in \mathrm{End}_G(V)$ et $\mathrm{tr}(f_\rho) =< f, \chi_g >$.
ii. Si (V,ρ) est irréductible, $\dim(V)$ est inversible dans $\bar{k}$ et f_ρ est l'homothétie de V de rapport $\frac{<f,\chi_g>}{\dim V}$.

Démonstration. — i. Pour tout $h \in G$, $f_\rho \in \mathrm{End}_G(V)$ car :

$$\begin{array}{rcll} \rho(h) \circ f_\rho \circ \rho(h)^{-1} & = & \frac{1}{|G|} \sum_{g \in G} f(g)\rho(hg^{-1}h^{-1}) & \\ & = & \frac{1}{|G|} \sum_{g' \in G} f(h^{-1}g'h)\rho(g'^{-1}) & \\ & = & \frac{1}{|G|} \sum_{g' \in G} f(g')\rho(g'^{-1}) & \text{car } f \text{ centrale,} \\ & = & f_\rho. & \end{array}$$

De plus $\mathrm{tr}(f_\rho) = \frac{1}{|G|} \sum_{g \in G} f(g)\chi_\rho(g^{-1}) =< f, \chi_\rho >$.
ii. Si ρ est irréductible, le lemme de Schur appliqué à la fonction centrale χ_ρ, montre que $(\chi_\rho)_\rho$ est une homothétie. Son rapport λ vérifie (d'après la proposition 13.9) :

$$\mathrm{tr}(\chi_\rho)_\rho = \lambda \dim V =< \chi_\rho, \chi_\rho >= 1.$$

Si f est une fonction centrale quelconque, f_ρ est une homothétie de trace $< f, \chi_\rho >$ et donc de rapport $\frac{<f,\chi_\rho>}{\dim V}$. □

Théorème 13.11. — *Les caractères des représentations irréductibles de dimension finie forment une base orthomormale du $\bar{k}$-espace vectoriel $\mathcal{C}(G)$ des fonctions centrales sur G.*
En particulier toute fonction centrale $f \in \mathcal{C}(G)$ s'écrit $f = \sum_{\rho \,\mathrm{irr}} < f, \chi_\rho > \chi_\rho$.

Démonstration. — Soit $f \in \mathcal{C}(G)$, fonction centrale orthogonale à tous les caractères χ_ρ, pour ρ irréductible. Alors $f_\rho = 0$ pour toute représentation irréductible ρ, puis toute représentation car $f_{\rho \oplus \rho'} = f_\rho \oplus f_{\rho'}$. Pour la représentation régulière, nous obtenons $f_{\rho_{\mathrm{reg}}} \in \mathrm{End}_G(\mathcal{F}(G))$ et $f_{\rho_{\mathrm{reg}}} = 0$. En évaluant $f_{\rho_{\mathrm{reg}}}$ en $\delta_e \in \mathcal{F}(G)$,

$$0 = f_{\rho_{\mathrm{reg}}}(\delta_e) = \frac{1}{|G|} \sum_{g \in G} f(g)\rho_{\mathrm{reg}}(g^{-1})(\delta_e) = \frac{1}{|G|} \sum_{g \in G} f(g)\delta_{g^{-1}}$$

dans $\mathcal{F}(G)$, ce qui entraîne que $f = 0$ car les δ_g forment une base de $\mathcal{F}(G)$. □

Corollaire 13.12. — *Rappelons que $\bar{k}$ est algébriquement clos de caractéristique première à l'ordre de G.*
i. Le nombre de représentations irréductibles de G est égal au nombre de classes de conjugaison de G.
ii. Soient $\chi_1, \ldots, \chi_s$ les caractères des représentations irréductibles de G, soient $C = [g]$ et $C' = [g']$ des classes de conjugaison dans G. Nous avons

$$\sum_{i=1}^{s} \chi_i(g^{-1})\chi_i(g') = \begin{cases} \frac{|G|}{|C|} & \text{si } C = C', \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. — i. La dimension de $\mathcal{C}(G)$ est égale au nombre de classes de conjugaison dans G.
ii. Soit δ_C la fonction caractéristique de C, c'est une fonction centrale qui se décompose sur la base orthonormale des caractères χ_i des représentations irréductibles :

$$\delta_C = \sum_{i=1}^{s} < \delta_C, \chi_i > \chi_i, \quad < \delta_C, \chi_i >= \frac{1}{|G|}|C|\chi_i(g^{-1}).$$

□

13.3. Décomposition des représentations. —

Définition 13.13. — *Soit $V = \oplus V_i$ une décomposition d'une représentation V de dimension finie d'un groupe fini G en représentations irréductibles. La décomposition de V en composantes isotypiques, s'obtient en regroupant tous les V_i isomorphes à la même représentation irréductible.*

Nous retrouvons le résultat de décomposition des représentations en somme directe de représentations irréductibles.

Proposition 13.14. — *Soit (V, ρ) une représentation de dimension finie du groupe fini G. La projection de V sur la composante isotypique correspondant à une représentation irréductible (V', ρ') est donnée par*

$$p_{V'} = \frac{\dim V'}{|G|} \sum_{g \in G} \chi_{\rho'}(g)\rho(g^{-1}).$$

En particulier, la décomposition en composantes isotypiques ne dépend que de la représentation (V, ρ).

Démonstration. — Soit f une fonction centrale sur G. L'endomorphisme f_ρ de V laisse stable toute sous-représentation (V_i, ρ_i) de (V, ρ) et se restreint à V_i en f_{ρ_i}. Si V_i est irréductible, alors f_{ρ_i} est l'homothétie de V_i de rapport $\frac{<f,\chi_i>}{\dim V_i}$ (lemme 13.10).

Pour $f = \chi_{\rho'}$, caractère d'une représentation irréductible (V', ρ'), l'endomorphisme $(\chi_{\rho'})_{\rho|V_i}$ est donc $\frac{1}{\dim V_i}\mathrm{Id}_{V_i}$ si $V_i \simeq V'$ ou 0 sinon. Comme $p_{V'} = (\dim V')(\chi_{\rho'})_\rho$ sa restriction à V_i est donc l'identité si $V_i \simeq V'$ et 0 sinon. □

Proposition 13.3.1. — *Notons $\rho_1, \ldots, \rho_s$ les représentations irréductibles (non équivalentes deux à deux) du groupe fini G. Soit $\rho = \oplus_{i=1}^s \rho_i^{n_i}$ une représentation de G. Nous avons*

$$< \chi_\rho, \chi_{\rho_i} >= n_i \cdot 1_{\bar{k}}, \quad < \chi_\rho, \chi_\rho >= \sum_{i=1}^{\ell} n_i^2 \cdot 1_{\bar{k}}.$$

Supposons de plus $\mathrm{car}\bar{k} = 0$,
- des représentations de G sont isomorphes si et seulement si elles ont le même caractère,
- ρ est irréductible si et seulement si $< \chi_\rho, \chi_\rho >= 1$,
- la représentation régulière se décompose en $\mathcal{F}(G) = \oplus_{i=1}^s \rho_i^{\dim \rho_i}$; en particulier $\sum_{i=1}^s (\dim \rho_i)^2 = |G|$.

Démonstration. — Pour la représentation régulière

$$\chi_{\mathrm{reg}} = |G|\delta_e, \quad < \chi_{\mathrm{reg}}, \chi_i >= \chi_i(e) = \dim \rho_i.$$

Donc $\rho_{\mathrm{reg}} = \oplus_{i=1}^s \rho_i^{\dim \rho_i}$. □

Si $\mathrm{car}k = p \neq 0$, le caractère ne détermine pas la représentation. Par exemple, pour toute représentation V, le caractère de V^p est nul.
Nous verrons plus loin qu'en caractéristique zéro (sur un corps algébriquement clos), la dimension d'une représentation irréductible divise l'ordre $|G|$. Ceci donne une contrainte importante sur les dimensions des représentations irréductibles.

Exemple 13.15. — *Supposons* $\mathrm{car}\bar{k} = 0$ *(algébriquement clos). Le groupe G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1.*
En effet un groupe abélien G a exactement $|G|$ classes de conjugaison, donc $|G|$ représentations irréductibles. Or $|G| = \sum_{i=1}^s (\dim \rho_i)^2$ donc $\ell \leq |G|$ avec égalité si et seulement si toutes les représentations irréductibles sont de dimension 1.

Exemple 13.16. — *La représentation de $\mathfrak{S}_n$ sur*

$$V_0 = \{(x_1, \ldots, x_n) \in \mathbb{C}^n | x_1 + \ldots + x_n = 0\}$$

est irréductible.
En effet la représentation de permutation est somme de V_0 et de la représentation triviale de dimension 1 (avec $< \chi_{\mathrm{triv}}, \chi_{\mathrm{triv}} >= 1$). Il suffit donc de montrer que le caractère χ de la représentation de permutation vérifie $< \chi, \chi >= 2$. Or $\chi(g)$ est

le nombre de points fixes de la permutation $g \in \mathfrak{S}_n$. Pour $a \in \{1, \dots, n\}$, nous posons

$$g_a = \begin{cases} 0 & si\ g(a) \neq a, \\ 1 & si\ g(a) = a. \end{cases}$$

Ainsi $\chi(g) = \chi(g^{-1}) = \sum_{a=1}^{n} g_a$ et

$$\begin{aligned} < \chi, \chi > &= \tfrac{1}{\mathfrak{S}_n} \textstyle\sum_{g \in \mathfrak{S}_n} \chi(g^{-1})\chi(g) \\ &= \tfrac{1}{n!} \textstyle\sum_{g \in \mathfrak{S}_n} \Big(\sum_{a=1}^{n} g_a \Big)^2 \\ &= \tfrac{1}{n!} \textstyle\sum_{1 \leq a,b \leq n} \sum_{g \in \mathfrak{S}_n} g_a g_b \\ &= \tfrac{1}{n!} \textstyle\sum_{1 \leq a \leq n} \sum_{g \in \mathfrak{S}_n} g_a + \tfrac{2}{n!} \sum_{1 \leq a < b \leq n} \sum_{g \in \mathfrak{S}_n} g_a g_b \\ &= \tfrac{1}{n!} \textstyle\sum_{1 \leq a \leq n} (n-1)! + \tfrac{2}{n!} \sum_{1 \leq a < b \leq n} (n-2)! = 2. \end{aligned}$$

Remarque 13.17. — *(Théorie de jauge sur réseau, d'après notes de cours de Jean-Bernard Zuber). En mécanique statistique, nous définissons un modèle sur un réseau carré dans lequel les degrés de liberté sont attachés aux liens entre sites voisins et prennent leur valeur dans un groupe fini G. A chaque lien orienté $\ell = \overrightarrow{ij}$, on associe l'élément g_ℓ, à $-\ell = \overrightarrow{ji}$, on associe g_ℓ^{-1}. A chaque carré (ou plaquette) $p = ijkl$, nous associons le produit des éléments des liens :*

$$g_p = g_{ij} g_{jk} g_{kl} g_{lj}$$

et l'énergie d'une configuation de ces variables est donnée par

$$E = - \sum_{plaquettes\ p} \Re_\chi(g_p)$$

où χ est le caractère d'une représentation unitaire du groupe ($\overline{\rho(g)} = \rho(g)^{-1}$, $g \in G$). La fonction de partition s'écrit

$$Z = \prod_{liens \ell} \Big(\frac{1}{n} \sum_{g_\ell \in G} \Big) \prod_{plaquettes} e^{\beta \Re_\chi(g_p)},$$

pour $\beta = \frac{1}{kT}$.
Nous pouvons montrer que l'energie E est invariante par la redéfinition des g_{ij} selon $g_{ij} \mapsto g_i g_{ij} g_j^{-1}$ où $g_i \in G$ et que E ne dépend pas de l'orientation des plaquettes. Nous pouvons calculer la fonction de partition Z pour un réseau fini de N plaquettes enserrées dans une courbe fermée du réseau fini.

14. Caractères complexes

Dans ce paragraphe, $k = \mathbb{C}$. Rappelons les résultats obtenus dans le paragraphe précédent en spécifiant la structure complexe.

14.1. Tables de caractères complexes. — Pour toute représentation (V,ρ) d'un groupe fini, nous avons $\rho(g)^{|G|} = \mathrm{Id}_V$, donc les valeurs propres de $\rho(g)$ sont des racines de l'unité et celles de $\rho(g^{-1})$ sont leurs conjugués. Nous avons donc

$$\chi_\rho(g^{-1}) = \mathrm{tr}(\rho(g^{-1})) = \overline{\mathrm{tr}(\rho(g))} = \overline{\chi_\rho(g)}.$$

Nous avons ainsi

$$< \chi_\rho, \chi_{\rho'} >= \frac{1}{|G|}\sum_{g\in G} \overline{\chi_\rho(g)}\chi_{\rho'}(g).$$

Pour $\chi_1,\ldots,\chi_s$ les caractères des représentations irréductibles de G et $C = [g], C' = [g']$ des classes de conjugaison de G :

$$\sum_{i=1}^{s} \overline{\chi_i(g)}\chi_i(g') = \begin{cases} \frac{|G|}{|C|} & \text{si } C = C', \\ 0 & \text{sinon.} \end{cases}$$

Définition 14.1. — *La table des caractère de G donne la valeur de chaque caractère sur chaque classe de conjugaison. Les lignes correspondent aux caractères et les colonnes aux classes de conjugaison. C'est une table carrée de taille s, le nombre de classes de conjugaison.*

Nous portons dans la première ligne du tableau un représentant de chaque classe de conjugaison du groupe et en indice de ce représentant le nombre d'éléments dans sa classe de conjugaison.
- Les lignes sont orthogonales car les caractères irréductibles constituent une base orthonormale des fonctions centrales $\mathcal{C}(G)$ de G.
- Les colonnes sont orthogonales pour le produit scalaire usuel de $\mathbb{C}^s$ et de plus

$$\sum_{i=1}^{s} \chi_i(e)^2 = \sum_{i\in S} (\dim \rho_i)^2 = |G|.$$

Plus généralement, en notant $|C|$ le cardinal de la classe de conjugaison de $g \in G$,

$$\sum_{i=1}^{s} |\chi_i(g)|^2 = \frac{|G|}{|C|}.$$

Exemple 14.2. — *Nous connaissons déja deux représentations irréductibles de $D_3 = \mathfrak{S}_3$ de dimension 1 : la représentation triviale* triv, *la signature ε. Le groupe $\mathfrak{S}_3$ a trois classes de conjugaison, et $|\mathfrak{S}_3| = 6 = 1+1+2^2$. La dimension de la dernière représentation irréductible est donc 2. Nous pouvons dresser la table des caractères en complétant la dernière ligne par orthogonalité ou en introduisant le caractère de la représentation régulière $\chi_{\mathrm{reg}} = 6\cdot\delta_{\{e\}} = \chi_{\mathrm{triv}} + \chi_\varepsilon + 2\chi_2$.*

$\mathfrak{S}_3$	e	$(12)_3$	$(123)_2$
χ_{triv}	*1*	*1*	*1*
χ_ε	*1*	*-1*	*1*
χ_2	*2*	*0*	*-1*

Il s'agit à présent de décrire explicitement la représentation irréductible de dimension 2. Nous en connaissons une réelle. Les éléments de $\mathfrak{S}_3$ s'identifient aux symétries d'un triangle équilatéral situé dans un plan horizontal. Par identification, nous pouvons en déduire la représentation complexe : la réalisation géométrique de $\mathfrak{S}_3$ comme stabilisateur dans le groupe orthogonal du plan euclidien d'un triangle équilatéral. L'irréductibilité de cette représentation tient au fait qu'il n'existe pas de direction propre commune au six isométries. Son caractère χ_2 se calcule en identifiant une transposition à une symétrie droite par rapport à la médiatrice de l'un des côtés et un 3-cycle à une rotation de $\pm 2\pi/3$ autour du centre de gravité du triangle.
Nous savons également que $\mathfrak{S}_3$ a une représentation ρ dans le plan complexe $V_0 = \{(x_1, x_2, x_3) \in \mathbb{C}^3 | x_1 + x_2 + x_3 = 0\}$ dont la somme directe avec la représentation triviale de dimension 1 est la représentation de permutation, de caractère de valeurs $3, 1, 0$ qui est donc la somme $\chi_{\text{triv}} + \chi_2$.
Les sous-groupes normaux de $\mathfrak{S}_3$ sont : $\mathfrak{S}_3$, noyau de χ_{triv}, $\mathfrak{A}_3 = \{1\} \cup \{(123)\}$ noyau de χ_ε et 1, noyau de χ_2.
Notons V la représentation irréductible de dimension 2. Le caractère de $V \otimes V$ est χ_2^2 de valeurs $4, 0, 1$, donc $\chi_2^2 = \chi_{\text{triv}} + \chi_\varepsilon + \chi_2$ et

$$V \otimes V = V_{\text{triv}} \oplus V_\varepsilon \oplus V.$$

Remarque 14.3. — *La table des caractères du groupe $D_3 = \mathfrak{S}_3$ est utile aux chimistes. Elle apparait avec des notations différentes :*

$\mathfrak{S}_3$	E	$3s_\nu$	$2C_3$
A_1	1	1	1
A_2	1	-1	1
E	2	0	-1

La notation $3s_\nu$ signifie qu'il y a trois éléments dans la classe de conjugaison et s_ν signifie qu'elle contient des symétries par rapport à un plan vertical. La notation $2C_3$ signifie qu'il y a deux éléments dans la classe de conjugaison et C_m correspond à des rotations d'angle $2\pi/m$. Les lettres A et B désignent des représentations irréductibles de dimension 1, E des représentations de dimension 2 et T des représentations de dimension 3.

Exemple 14.4. — *Le groupe diédral D_4 admet la présentation à deux générateurs, un élément d'ordre 4, r et un élément d'ordre 2, s avec les relations*

$$s^2 = e, r^4 = e, sr^k s = r^{-k}, rsr^{-1} = sr^2.$$

Il y a donc 5 classes de conjugaison $\{e\}, \{r^2\}, \{r, r^3\}, \{s, r^2 s\}, \{rs, r^3 s\}$. Le sous-groupe $\mathbb{Z}/2\mathbb{Z} =< r^2 >$ est normal et dans le quotient les trois éléments r, s, rs sont d'ordre deux ; donc

$$D_4/(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ceci donne quatre représentations de dimension 1 correspondant aux quatre morphismes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^*$. La cinquième représentation doit être de dimension 2, avec pour table de caractères

D_4	e	$(r^2)_1$	$(r)_2$	$(s)_2$	$(rs)_2$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_1'	1	1	1	-1	-1
$\chi_1\chi_1'$	1	1	-1	-1	1
χ_2	2	-2	0	0	0

La représentation de dimension 2 est la représentation standard de $\mathbb{C}^2$. Les sous-groupes normaux de D_4 sont D_4, $\{e, r^2, s, r^2s\}$ noyau de χ_1, $\{e, r, r^2, r^3\}$ noyau de χ_1', $\{e, r^2, rs, r^3s\}$ noyau de $\chi_1\chi_1'$, $\{e\}$ et leurs intersections. Le sous-groupe dérivé est $\{e, r^2\}$ ($\ker\chi_1 \cap \ker\chi_1'$) et c'est aussi le centre

$$Z(D_4) = \{g \in D_4, \forall \chi \textit{ irréductible}, |\chi(g)| = \chi(e)\}.$$

```
sage: G=PermutationGroup([[(1,2),(3,4)],[(1,2,3,4)]])
sage: G.character_table()
```

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & 0 & 0 & 0 & -2 \end{bmatrix}$$

Nous pouvons utiliser cette table pour obtenir des informations sur la structure du groupe G.

Lemme 14.5. — *Soit ρ une représentation de G et $g \in G$. Alors*

$$\chi_\rho(g) = \chi_\rho(e) \textit{ si et seulement si } \rho(g) = \mathrm{Id}\,.$$

Ainsi $\{g \in G, \chi_\rho(g) = \chi_\rho(e)\} = \ker\rho \lhd G$.

Démonstration. — Comme $\chi_\rho(g)$ est somme des valeurs propres de $\rho(g)$,

$$\forall g \in G, |\chi_\rho(g)| \leq \chi_\rho(e) = \dim V.$$

Ainsi $|\chi_\rho(g)| = \chi_\rho(e)$ si et seulement $\rho(g)$ est une homothétie (inégalité triangulaire). En particulier, $\chi_\rho(g) = \chi_\rho(e)$ si et seulement si $\rho(g) = \mathrm{Id}$. □

Pour tout caractère χ d'une représentation ρ de G, nous notons

$$G_\chi = \ker\rho = \{C, \chi(C) = \chi(e)\} \lhd G.$$

Lemme 14.6. — *Tout sous-groupe normal s'obtient comme intersection de G_{χ_i} où χ_i décrit une sous-famille des caratères des représentations irréductibles de G (non équivalentes deux à deux).*

Démonstration. — Soit $N \lhd G$ et $\bar{\rho} : G/N \longrightarrow \mathrm{GL}(\mathcal{F}(G/N))$ la représentation régulière (injective) de G/N. Alors en composant avec la projection $\pi : G \longrightarrow G/N$, nous obtenons une représentation

$$\rho : G \longrightarrow \mathrm{GL}(\mathcal{F}(G/N))$$

de noyau $\ker \rho = N$. En décomposant ρ en somme directe de représentations irréductibles $\rho = \oplus \rho_i$, nous obtenons $\ker \rho = \cap \ker \rho_i$. □

En particulier, G est simple si tous les G_χ sont triviaux pour $\chi \neq \chi_{\mathrm{triv}}$, autrement dit si et seulement si dans chaque ligne exceptée celle correspondant à la représentation triviale, la valeur $\chi(e)$ n'apparait qu'une seulement fois (dans la colonne correspondant à la classe $\{e\}$).

Lemme 14.7. — *Le groupe dérivé $D(G)$ est l'intersection des G_χ pour tous les caractères de dimension 1.*

Démonstration. — Les représentations de dimension 1 sont des morphismes

$$G \longrightarrow \mathbb{C}^*.$$

Ainsi $G/\ker \rho$, isomorphe à un sous-groupe fini de $\mathbb{C}^*$, est abélien et $D(G) < \ker \rho$. Donc $D(G)$ inclus dans l'intersection des noyaux des représentations de dimension 1.
Réciproquement la représentation régulière $\bar{\rho} : G/D(G) \longrightarrow \mathrm{GL}(\mathcal{F}(G/D(G))$ admet une décomposition en représentations irréductibles $\bar{\rho}_i$ de $G/D(G)$. Comme $G/D(G)$ est abélien les représentations $\bar{\rho}_i$ sont de dimension 1. Notons ρ (resp. ρ_i) la représentation $\rho : G \longrightarrow G/D(G) \longrightarrow \mathrm{GL}(\mathcal{F}(G/D(G))$ obtenu par composition de la projection $G \longrightarrow G/D(G)$ avec $\bar{\rho}$ (resp. $\bar{\rho}_i$). La représentation $\bar{\rho}$ est injective donc $\ker \rho = D(G) = \cap \ker \rho_i$ où ρ_i sont des représentations de G de dimension 1. Par conséquent $D(G)$ contient l'intersection des noyaux des représentations de dimension 1. □

Lemme 14.8. — *Le centre de G est la réunion des classes de conjugaison C pour lesquelles $|\chi_i(C)| = \chi_i(e)$ pour tout i.*

Démonstration. — En effet si $g \in Z(G)$, alors $\rho_i(g)$ commute avec ρ_i, c'est donc (d'après le lemme de Schur) une homothétie de rapport une racine de l'unité et $|\chi_i(g)| = \chi_i(e)$ pour tout i. Réciproquement si $|\chi_i(g)| = \chi_i(e)$, $\rho_i(g)$ est une homothétie donc commute avec ρ_i, donc $\rho(g)$ commute avec toute représentation ρ. Choisissons pour ρ la représentation régulière. Ainsi

$$\rho_{\mathrm{reg}}(gh) = \rho_{\mathrm{reg}}(g)\rho_{\mathrm{reg}}(h) = \rho_{\mathrm{reg}}(h)\rho_{\mathrm{reg}}(g) = \rho_{\mathrm{reg}}(hg), h \in H.$$

Comme la représentation régulière est injective $gh = hg$ pour tout $h \in G$ donc $g \in Z(G)$. □

La table de caractères peut également être utilisée pour calculer la décomposition en composantes irréductibles d'une représentation donnée.

Exemple 14.9. — *Le groupe $\mathfrak{S}_4$ admet deux caractères de degré 1 : le caractère trivial et le caractère de la signature ε. Ce sont les seuls car $D(\mathfrak{S}_4) = \mathfrak{A}_4$. Il admet 5 classes de conjugaison. Le groupe $\mathfrak{S}_4$ possède un sous-groupe normal engendré par les bi-transpositions et le quotient par ce groupe est isomorphe à $\mathfrak{S}_3$. Nous obtenons par passage au quotient une représentation irréductible de dimension 2 à partir de celle connue de gS_3. Nous notons χ_2 son caractère. L'écriture $|\mathfrak{S}_4| = 24 = 1+1+4+n^2+m^2$ avec $m, n > 2$, implique qu'il existe deux autres representations irréductibles de degré 3. Or nous avons une représentation de degré 3 de $\mathfrak{S}_4$ dans $V_0 = \{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 | x_1 + x_2 + x_3 + x_4 = 0\}$. Le caractère de la représentation de permutation χ de $V_0 \oplus V_{\text{triv}}$ a pour valeurs $4, 2, 1, 0, 0$; donc χ_{V_0} a pour valeurs $3, 1, 0, -1, -1$ et*

$$< \chi_{V_0}, \chi_{V_0} >= \frac{1}{|G|}\chi_{V_0}(g)^2 = 1$$

donc V_0 est irrréductible. On pose $\chi_3 = \chi_{V_0}$. Nous obtenons ainsi la table

$\mathfrak{S}_4$	e	$(12)_6$	$(123)_8$	$(1234)_6$	$(12)(34)_3$
χ_{triv}	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
$\chi_3 = \chi_{V_0}$	3	11	0	-1	-1
χ'_3	3	-1	0	1	-1

Le caractère χ'_3 correspond à la représentation $V \otimes \chi_{\text{triv}}$ qui est donc irréductible (comme tout produit tensoriel d'une représentation irréductible et d'une représentation de dimension 1).
Les sous-groupes normaux de $\mathfrak{S}_4$ sont $\mathfrak{S}_4$ noyau de χ_{triv}, $\mathfrak{A}_4$ noyau de χ_ε, le groupe de Klein noyau de χ_2 et le groupe 1. Le groupe dérivé $D(\mathfrak{S}_4) = \mathfrak{A}_4$ et le centre est trivial car $\{\sigma \in \mathfrak{S}_4, ||\chi_{V_0}(\sigma)| = \chi_{V_0}(e) = 3\} = \{e\}$.

Comme représentations réelles, χ_3 le caractère des déplacements qui préservent le cube et χ'_3 le caractère des isométries qui stabilisent un trétraèdre régulier.

Nous en déduisons la table de $\mathfrak{A}_4$:

$\mathfrak{A}_4$	e	$(123)_4$	$(132)_4$	$(12)(34)_3$
χ_{triv}	*1*	*1*	*1*	*1*
χ	*1*	ω	ω^2	*1*
χ^2	*1*	ω^2	ω	*1*
χ_{V_0}	*3*	*0*	*0*	*-1*

```
sage: G=PermutationGroup([[(1,2),(3,4)],[(1,2,3)]])
sage: G.character_table()
```

$$\begin{array}{[cccc]} 1 & 1 & 1 & 1 \\ 1 & -zeta3-1 & zeta3 & 1 \\ 1 & zeta3 & -zeta3-1 & 1 \\ 3 & 0 & 0 & -1 \end{array}$$

Exemple 14.10. — *(Caractères des quaternions) Nous considèrons le groupe des quaternions formé des 8 matrices*

$$\mathcal{D} = \left\{ \pm \mathrm{Id}, \pm I = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm J = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm K = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

Le sous-groupe $\{\pm \mathrm{Id}\}$ *est le groupe dérivé* $D(\mathcal{D})$ *et le quotient* $\mathcal{D}/D(\mathcal{D})$ *est isomorphe au groupe* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Nous en déduisons les quatre caractères de degré 1. La représentation des quaternions par des matrices* 2×2 *fournit une représentation irréductible de dimension 2 de* $\mathcal{D}$, *d'où le caractère irréductible* χ_2 *de degré 2. La table des caractères est donc*

$\mathcal{D}$	*1*	*-1*	$(I)_2$	$(J)_2$	$(K)_2$
χ_{triv}	*1*	*1*	*1*	*1*	*1*
χ_1	*1*	*1*	*-1*	*-1*	*1*
χ_1'	*1*	*1*	*1*	*-1*	*-1*
χ_1''	*1*	*1*	*-1*	*1*	*-1*
χ_2	*2*	*-2*	*0*	*0*	*0*

Nous observons l'égalité des tables de caractères des groupes non isomorphes $\mathcal{D}_4$ *et* $\mathcal{D}$. *La table des caractères irréductibles d'un groupe fini ne caractérise pas ce groupe.*

Remarque 14.11. — *Soit* G *un groupe fini d'ordre* n. *Le déterminant* Δ *de la table des caractères de* G *est de la forme*

$$\Delta = \epsilon \Big(\frac{n^N}{n_1 \cdots n_N} \Big)^{1/2}$$

où n_i *désigne le cardinal d'une des* N *classes de conjugaison de* G *et* ϵ *est une racine quatrième de l'unité.*

14.2. Propriétés d'intégralité des caractères. — Soit $k = \bar{k}$ un corps algébriquement clos de caractéristique zéro (ainsi $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{C} \subset \bar{k}$). Nous rappellons qu'un anneau est un groupe commutatif muni d'une seconde loi interne associative, admettant un élément neutre et distributive par rapport à l'addition. Nous notons $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers.

Définition 14.12. — *Un élément $x \in k$ est dit entier algébrique, s'il est racine d'un polynôme unitaire de $\mathbb{Z}[X]$.*
Pour $x \in k$, nous notons $\mathbb{Z}[x]$ le sous-groupe additif de k engendré par les puissances positives de x : $\mathbb{Z}[x] = \{P(x), P \in \mathbb{Z}[X]\}$.

Exemple 14.13. — *Les entiers algébriques $x \in \mathbb{Q} \cap k$ sont les entiers. En effet si $x = r/s$ avec $(r, s) = 1$ annule $r^n + a_1 r^{n-1} s + \cdots a_n s^n = 0$ alors $s | r^n$ donc $s = \pm 1$.*

Lemme 14.14. — *Les trois propriétés suivantes sont équivalentes :*
i. $x \in k$ est un entier algébrique,
ii. le groupe abélien $\mathbb{Z}[x]$ est de type fini,
iii. Il existe un sous-groupe abélien de type fini de k contenant $\mathbb{Z}[x]$.

Démonstration. — i.$\Longrightarrow$ii. car $x^n + a_1 x^{n-1} + \cdots + a_0 = 0 \in \mathbb{Z}[x]$ implique que $\mathbb{Z}[x]$ est engendré par $\{1, x, \ldots, x^{n-1}\}$.
ii.$\Longrightarrow$ iii. est clair. Montrons iii.$\Longrightarrow$i. $\mathbb{Z}[x]$ sous-groupe d'un groupe abélien de type fini est de type fini. Soit $\{P_1(x), \ldots, P_r(x)\}$ une famille génératrice et $d = \max_{1 \leq i \leq r} \deg P_i$. Ainsi $\{1, \ldots, x^d\}$ engendre aussi $\mathbb{Z}[x]$, donc x^{d+1} s'écrit comme combinaison linéaire à coefficients entiers de $1, \ldots, x^d$. D'où x entier algébrique. □

Corollaire 14.15. — *L'ensemble des entiers algébriques de $\bar{k}$ est un sous-anneau de k.*
En particulier, les valeurs de caractères, somme de racines de l'unité sont des entiers algébriques.

Démonstration. — Si x, y sont deux entiers algébriques, il existe r, s tels que $\mathbb{Z}[x, y]$ est engendré par $x^i y^j$, $0 \leq i \leq r$, $0 \leq j \leq s$. Or $\mathbb{Z}[x - y] < \mathbb{Z}[x, y]$ et $\mathbb{Z}[xy] < \mathbb{Z}[x, y]$, donc $x - y$ et xy sont des entiers algébriques. □

Lemme 14.16. — *Soit $C = [g]$ une classe de conjugaison du groupe fini G et (V, ρ) une représentation irréductible (de dimension finie). Alors $\frac{|C| \chi_\rho(g)}{\dim V}$ est un entier algébrique*

Démonstration. — Notons $C^{-1} = \{g^{-1}, g \in C\}$ et $f = \delta_{C^{-1}}$ la fonction centrale caractéristique de la classe C^{-1}. L'endomorphisme $\nu = |G| f_\rho = \sum_{g \in C} \rho(g)$ commute à ρ, donc est une homothétie de rapport

$$\lambda = \frac{|G| < f, \chi_\rho >}{\dim V} = \frac{|G| \chi_\rho(g)}{\dim V}.$$

Dans la base canonique δ_g de $\bar{k}^G$, la matrice de $\rho_{\text{reg}}(g)$ est une matrice de permutation pour tout $g \in G$, donc est à coefficients entiers. L'endomorphisme $u = \sum_{g \in C} \rho_{\text{reg}}(g) \in \mathcal{F}(G)$ est donc à coefficients entiers. La restriction de u à V (V irréductible est facteur direct de $\bar{k}^G$) est l'endomorphisme ν, homothétie de rapport λ. Donc λ, valeur propre de u est racine d'un polynôme à coefficients entiers, donc est un entier algébrique. □

Théorème 14.17. — *Soit G un groupe fini et $\bar{k}$ un corps algébriquement clos de caractéristique 0. Si V est une représentation irréductible de G alors* $\dim V$ *divise* $|G|$.

Démonstration. — Notons χ le caractère de V. Comme V est irréductible,

$$< \chi, \chi >= \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\chi(g) = 1.$$

Notons $C_1, \ldots, C_s$ les classes de conjugaison de G. Ainsi

$$\begin{array}{rl} \frac{|G|}{\dim V} & = \frac{1}{\dim V} \sum_{g \in G} \chi(g^{-1})\chi(g) \\ & = \frac{1}{\dim V} \sum_{i=1}^{s} |C_i| \chi(C_i^{-1})\chi(C_i) \\ & = \sum_{i=1}^{s} \frac{|C_i|\chi(C_i)}{\dim V} \chi(C_i^{-1}) \end{array} .$$

Comme les $\chi(C_i^{-1})$, $\frac{|C_i|\chi_\rho(C_i)}{\dim V}$ sont des entiers algébriques, $\frac{|G|}{\dim V}$ est un entier algébrique et comme il est rationnel, il est entier. □

Remarque 14.18. — *Il existe une représentation de $\mathbb{Z}/3\mathbb{Z}$ comme groupe des rotations de $\mathbb{R}^2$ préservant un triangle équilatéral centré à l'origine, de dimension 2 irréductible sur $\mathbb{R}$ qui ne divise pas $3 = |\mathbb{Z}/3\mathbb{Z}|$. Cela ne contredit pas le théorème (!) car le corps des réels n'est pas algébriquement clos.*
Il existe une représentation irréductible de dimension 5 sur $\overline{\mathbb{F}}_{13}$ de $\mathrm{SL}_2(\mathbb{F}_{13})$, d'ordre $2^3 \cdot 3 \cdot 7 \cdot 13$ divisible par 13 mais pas par 5.

Exemple 14.19. — *Un groupe d'ordre p^2 ne peut avoir que des représentations irréductibles de dimension 1, donc est abélien.*

15. Représentations induites

15.1. Définitions. — Jusqu'à présent, nous nous sommes intéressés aux propriétés d'une représentation d'un groupe G fixé et aux représentations obtenues par restriction à un sous-espace vectoriel stable ou par passage au quotient par un sous-groupe normal de G. Maintenant, nous procédons dans l'autre sens : nous partons d'une représentation d'un sous-groupe H de G et nous l'étendons au groupe G. Il s'agit d'un outil très puissant pour fabriquer des représentations de groupe.

Dans ce paragraphe, nous supposons encore que G est un groupe fini, en revanche il n'est pas nécessaire de supposer que k est algébriquement clos ou de caractéristique 0. Pour $H < G$, nous notons

$$G = \cup_{i=1}^{r} g_i H$$

la partition de G en classes à gauche modulo H.
Pour (V, ρ) une représentation de G et $W \subset V$ un sous-espace vectoriel de V stable par les automorphismes $\rho(h)$, $h \in H$, nous notons

$$\rho_{|H,W} : H \longrightarrow \mathrm{GL}(W)$$

la restriction de ρ au sous-groupe H et au sous-espace W.

Définition 15.1. — *Soit $W \subset V$, un sous-espace vectoriel d'un espace vectoriel V de dimension finie, $H < G$ un sous-groupe de G d'indice r d'un groupe fini G, $\rho_1 : H \longrightarrow \mathrm{GL}(W)$ et $\rho : G \longrightarrow \mathrm{GL}(V)$ deux représentations. La représentation ρ est dite induite par la représentation ρ_1 si $\rho_1 = \rho_{|H,W}$ et $V = \oplus_{i=1}^{r} g_i W$. Nous notons alors*

$$\rho = \mathrm{Ind}_H^G \rho_1.$$

Exemple 15.2. — *La représentation régulière de G est induite par la représentation régulière de H pour tout $H < G$. En effet*

$$\mathcal{F}(G) = \oplus_{g \in G} k\delta_g = \oplus_{i=1}^{r} \oplus_{h \in H} k\delta_{g_i h} \oplus_{i=1}^{r} \rho_{\mathrm{reg},G}(g_i)\Big(\oplus_{h \in H} k\delta_h \Big)$$

car $\rho_{\mathrm{reg},G}(g_i)(\delta_h)(x) = \delta(g_i^{-1}x) = 1$ si et seulement $g_i^{-1}x = h$, i.e. $x = g_i h$.

Exemple 15.3. — *(Construction d'une représentation induite I). Soit $H < G$ et $\rho_1 : H \longrightarrow \mathrm{GL}(W)$ une représentation de H. Soit*

$$V = \oplus_{i=1}^{r} W_i$$

l'espace vectoriel somme directe de $r = [G : H]$ copies de W. Nous identifions W_1 et W. Nous définissons une opération de $G = \cup_{i=1}^{r} g_i H$ ($g_1 = e$) sur V via les formules suivantes :

$$\rho(h)(w, 0, \ldots, 0) = (\rho_1(h)(w), 0, \ldots, 0) \in W_1,$$

$$\rho(g_i)(w, 0, \ldots, 0) = (0, \ldots, 0, w, 0, \ldots, 0) \in W_i, \ w \text{ est à la } i\text{-ème coordonnée}$$

et si $g \in G$ avec $g g_i = g_j h$ pour $h \in H$,

$$\rho(g)(0, \ldots, \underset{\uparrow}{w}, \ldots, \underset{\uparrow}{0}, \ldots, 0) = (0, \ldots, \underset{\uparrow}{0}, \ldots, \underset{\uparrow}{\rho_1(h)(w)}, \ldots, 0)$$
$$\qquad\qquad\qquad\quad i \qquad\quad j \qquad\qquad\qquad\quad i \qquad\quad j$$

Ainsi, nous avons défini une représentation induite

$$\rho = \mathrm{Ind}_H^G \rho_1.$$

Exemple 15.4. — *(Construction d'une représentation induite II). Soit* (W, ρ_1) *une représentation d'un sous-groupe* H *de* G. *Posons*

$$V = \mathrm{Ind}_H^G(W) = \{g : G \longrightarrow W, \forall h \in H, \forall x \in G, f(hx) = \rho_1(h)f(x)\}.$$

Nous munissons cet espace vectoriel de l'action par translations à droite $(gf)(x) = f(xg)$. *Nous obtenons ainsi une représentation induite* $\mathrm{Ind}_H^G \rho_1$.

Exemple 15.5. — *Le groupe diédral* D_n *est engendré par deux éléments* r, s *satisfaisant*

$$r^n = s^2 = (rs)^2 = e.$$

Les éléments de D_n *s'écrivent donc* $\{r^\alpha s^\beta, 0 \leq \alpha \leq n-1, \beta = 0, 1\}$. *Les formules suivantes pour* $0 \leq i, j \leq n-1$ *permettent de déterminer les classes de conjugaison de* D_n *:*

$$r^i r^j r^{-i} = r^j, r^i(sr^j)r^{-i} = sr^{j-2i}, (sr^i)r^j(sr^i)^{-1} = r^{-j}, (sr^i)sr^j(sr^i)^{-1} = sr^{2j-1}.$$

Ainsi si $n = 2m$ *est pair,* D_n *a* $m+3$ *classes de conjugaison*

$$\{e\}, \{r^j, r^{n-j}\}_{\{1 \leq j \leq m-1\}}, \{r^m\}, \{sr^j, j \text{ pair}\}, \{sr^j, j \text{ impair}\}.$$

Si $n = 2m+1$ *est impair,* D_n *a* $m+2$ *classes de conjugaison*

$$\{e\}, \{r^j, r^{n-j}\}_{\{1 \leq j \leq m\}}, \{sr^j, 0 \leq j \leq n-1\}.$$

Les caractères de degré 1 sont donnés par

$$r \mapsto \pm 1, s \mapsto \pm 1 \text{ si } n \text{ pair},$$

$$r \mapsto 1, s \mapsto \pm 1 \text{ si } n \text{ impair}.$$

Par induction, nous construisons les représentations irréductibles de dimension 2 de D_n. *Les caractères complexes du sous-groupe abélien normal cyclique d'ordre* n, $C_n =< r >$, *de* D_n *sont connus : pour* $\rho_\ell^1 : r \mapsto \omega^\ell$ *pour* $\omega = \exp(2i\pi/n)$. *Nous en déduisons* $\rho_\ell = \mathrm{Ind}_{C_n}^{D_n} \rho_\ell^1$ *représentation de dimension 2 de* D_n *:*

$$\rho_\ell(r) = \begin{pmatrix} \omega^\ell & 0 \\ 0 & \omega^{-\ell} \end{pmatrix}, \rho_\ell(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Nous en déduisons la table des valeurs du caractère de ρ_ℓ *:*

D_n	e	r^α	s	$r^\alpha s$
χ_ℓ	2	$\omega^{\alpha\ell} + \omega^{-\alpha\ell}$	0	0

Pour $1 \leq \ell \leq m$, *ces caractères sont deux à deux distincts. De plus*

$$< \chi_\ell, \chi_\ell >= \begin{cases} 1 & \text{si } 2\ell \neq 0 \mod n, \\ 2 & \text{si } 2\ell = 0 \mod n. \end{cases}$$

Ainsi si $n = 2m+1$, D_n *a* $m+2$ *classes de conjugaison, deux caractères de degré 1 et* m *représentations irréductibles de dimension 2 ;*
si $n = 2m$, D_n *a* $m+3$ *classes de conjugaison, quatre caractères de degré 1 et* $m-1$ *représentations irréductibles de dimension 2.*

Exemple 15.6. — *Soit $H < G$ et $\rho = \mathrm{Ind}_H^G \rho_1$ une représentation induite de $\rho_1 : H \longrightarrow \mathrm{GL}(W)$. Si $W = W_1 \oplus W_2$ est une décomposition de W en sous-espaces stables par ρ_1. Alors*

$$V = \oplus_{i=1}^r g_i W = \Big(\oplus_{i=1}^r g_i W_1 \Big) \oplus \Big(\oplus_{i=1}^r g_i W_2 \Big),$$

$$\mathrm{Ind}_H^G(\rho_{1|W_1} \oplus \rho_{1|W_2}) = \mathrm{Ind}_H^G \rho_{1|W_1} \oplus \mathrm{Ind}_H^G \rho_{1|W_2}.$$

De même si U est un sous-espace stable par ρ_1, alors

$$\mathrm{Ind}_H^G \rho_{1|U} = \rho_{|\oplus_{i=1}^r g_i U}.$$

Exemple 15.7. — *Soient (V, ρ), (V', ρ') deux représentations du groupe G. Notons $\mathrm{Hom}_G(V, V')$ l'ensemble des applications linéaires de V dans V' compatibles à l'action de G. Supposons $\rho = \mathrm{Ind}_H^G \rho_1$, pour $\rho_1 : H \longrightarrow \mathrm{GL}(W)$. Nous avons*

$$\mathrm{Hom}_G(V, V') = \mathrm{Hom}_H(W, V').$$

En effet tout élément $f \in \mathrm{Hom}_H(W, V')$ se prolonge de façon unique en $\tilde{f} \in \mathrm{Hom}_G(V, V')$ via

$$\tilde{f}(w_i) = \rho'(g_i) f(w), \text{ pour tout } w_i = g_i w \in g_i W.$$

Nous en déduisons l'unicité de la représentation induite : si $\rho' = \mathrm{Ind}_H^G \rho_1$, nous avons le diagramme commutatif

$$\begin{array}{ccc} & & V \\ & \nearrow & \downarrow \varphi \\ W & \longrightarrow & V' \end{array}$$

L'application φ qui prolonge l'injection $W \longrightarrow V'$ est surjective et comme les espaces V et V' ont même dimension, les deux représentations ρ et ρ' sont équivalentes.

Nous calculons le caractère χ de la représentation induite $\rho = \mathrm{Ind}_H^G \rho_1$ (avec les notations précédentes). Soit $g \in G$. L'automorphisme $\rho(g)$ permute les sous-espaces vectoriels $g_i W$. Pour calculer la trace de $\rho(g)$, il suffit de se restreindre aux sous-espaces $g_i W$ qui sont stables sous l'action de la permutation (penser à l'écriture de $\rho(g)$ sous forme de blocs), i.e. aux sous-espaces tels que $g g_i W = g_i W$:

$$\chi(g) = \mathrm{tr}\, \rho(g) = \sum_{i | g_i^{-1} g g_i \in H} \mathrm{tr}\, \rho(g)_{|g_i W} = \sum_{i | g_i^{-1} g g_i \in H} \mathrm{tr}\, \rho(g_i^{-1} g g_i)_{|W}$$

$$\chi(g) = \sum_{i | g_i^{-1} g g_i \in H} \mathrm{tr}\, \rho_1(g_i^{-1} g g_i)$$

L'avant-dernière égalité met en œuvre l'invariance de la trace par changement de base. D'où

$$\chi(g) = \sum_{i | g_i^{-1} g g_i \in H} \chi_1(g_i^{-1} g g_i) = \frac{1}{|H|} \sum_{g' \in G, g'^{-1} g g' \in H} \chi_1(g'^{-1} g g'), \quad g \in G.$$

Plus généralement,

Définition 15.8. — *Pour $\varphi : H \longrightarrow \mathbb{C}$, fonction définie sur $H < G$, constante sur les classes de conjugaison de H, nous définissons la fonction $\mathrm{Ind}_H^G \varphi$ définie sur G constante sur les classes de conjugaison de G :*

$$\mathrm{Ind}_H^G \varphi(g) = \frac{1}{H} \sum_{g' \in G, g'^{-1} g g' \in H} \varphi(g'^{-1} g g'), g \in G.$$

Si $\psi : G \longrightarrow \mathbb{C}$ est une fonction constante sur les classes de conjugaison de G, nous notons $\mathrm{res}_H \psi = \psi_{|H}$ sa restriction à H.

Le théorème de réciprocité de Frobenius établit que la multiplicité avec laquelle une représentation irréductible ρ' apparait dans une représentation induite $\mathrm{Ind}_H^G \rho$ est égale à celle avec laquelle la représentation ρ apparait dans la restriction de ρ' à H.

Théorème 15.9. — *(Formule de réciprocité de Frobenius) Soit $\varphi : H \longrightarrow \mathbb{C}$ constante sur les classes de conjugaison de H et $\psi : G \longrightarrow \mathbb{C}$ constante sur les classes de conjugaison de G, nous avons :*

$$< \varphi, \mathrm{res}_H(\psi) >_H = < \mathrm{Ind}_H^G \varphi, \psi >_G .$$

Démonstration. — Les caractères irréductibles constituent une base de l'espace vectoriel des fonctions constantes sur les classes de conjugaison. Il suffit donc de montrer la formule de réciprocité sur les caractères. Nous utilisons la formule donnant le caractère induit, en remarquant que si nous posons $h = g'^{-1} g g'$:

$$\mathrm{Ind}_H^G \varphi(g) = \frac{1}{|H|} \sum_{g' \in G, g'^{-1} g g' \in H} \varphi(g'^{-1} g g') = \frac{1}{|H|} \sum_{h \in H} |\{g' \in G, g'^{-1} g g' = h\}| \varphi(h).$$

Ainsi

$$< \mathrm{Ind}_H^G \varphi, \psi >_G = \frac{1}{|G||H|} \sum_{g \in G} \sum_{g' \in G, g'^{-1} g g' \in H} \varphi(g'^{-1} g g') \psi(g^{-1}).$$

Avec le changement de variable $g'^{-1} g g' = h$, nous obtenons (en notant $\mathcal{O}_h$ l'orbite de h par conjugaison dans G)

$$\begin{aligned}
< \mathrm{Ind}_H^G \varphi, \psi >_G &= \tfrac{1}{|G||H|} \textstyle\sum_{g \in G} \sum_{h \in H} |\{g' \in G, g'^{-1} g g' = h\}| \varphi(h) \psi(h^{-1}), \\
&= \tfrac{1}{|G||H|} \textstyle\sum_{h \in H} \varphi(h) \psi(h^{-1}) \sum_{g \in G} |\{g' \in G, g'^{-1} g g' = h\}|, \\
&= \tfrac{1}{|G||H|} \textstyle\sum_{h \in H} \varphi(h) \psi(h^{-1}) \sum_{g \in \mathcal{O}_h} |\{g' \in G, g'^{-1} g g' = h\}|, \\
&= \tfrac{1}{|G||H|} \textstyle\sum_{h \in H} \varphi(h) \psi(h^{-1}) \sum_{g \in \mathcal{O}_h} |\operatorname{Stab}(h)|, \\
&= \tfrac{1}{|G||H|} \textstyle\sum_{h \in H} \varphi(h) \psi(h^{-1}) |\mathcal{O}_h| |\operatorname{Stab}(h)|, \\
&= \tfrac{1}{|H|} \textstyle\sum_{h \in H} \varphi(h) \psi(h^{-1}), \\
&= < \varphi, \mathrm{res}_H(\psi) >_H .
\end{aligned}$$

□

Exemple 15.10. — *Supposons $k = \mathbb{C}$. Soit (V, ρ) une représentation irréductibles du groupe G et $\mathrm{Ind}_H^G \rho_1$ la représentation induite de H à G de $\rho_1 : H \to \mathrm{GL}(W)$. Alors la multiplicité de ρ dans $\mathrm{Ind}_H^G \rho_1$ est égale à $< \chi_\rho, \chi_{\rho_1} >_H$.*

Pour $H < G$, $\rho_1 : H \longrightarrow \mathrm{GL}(W)$ et $g \in G$, nous notons $H_g = H \cap gHg^{-1}$ et $\rho_g : H_g \longrightarrow \mathrm{GL}(W)$, la représentation définie par $\rho_g(h) = \rho_1(g^{-1}hg), h \in H$.

Corollaire 15.11. — *(Critère d'irréductibilité de Mackey). Supposons que $k = \mathbb{C}$. Pour que $\rho = \mathrm{Ind}_H^G \rho_1$ soit irréductible, il faut et il suffit que ρ_1 le soit et que pour tout $g \in G\backslash H$, les représentations $\mathrm{res}_{H_g} \rho_1$ et ρ_g soient sans composante irréductible commune.*
En particulier, si $H \lhd G$, $\rho = \mathrm{Ind}_H^G \rho_1$ est irréductible, si et seulement si ρ_1 est irréductible et pour tout $g \in G\backslash H$, les représentations ρ_1 et ρ_g ne sont pas équivalentes.

Démonstration. — L'irréductibilité de ρ implique celle de ρ_1. Le corollaire découle de la formule de réciprocité de Frobenius :

$$< \chi, \chi >_G = < \chi, \mathrm{Ind}_H^G \chi_1 >_G = < \mathrm{res}_H \chi, \chi_1 >_H .$$

Introduisons la partition de G en double classes modulo H :

$$G = \cup_{i=1}^t H g_i H.$$

Nous avons $\mathrm{res}_H \chi = \sum_{i=1}^t \mathrm{Ind}_{H_{g_i}}^H \chi_{g_i}$. D'où

$$< \chi, \chi >_G = < \chi_1, \chi_1 >_H + \sum_{i=2}^{t} < \chi_i, \mathrm{res}_{H_{g_i}} \chi_1 >_{H_{g_i}} .$$

□

16. Représentations du groupe symétrique

Dans ce paragraphe, nous étudions spécifiquement les représentations complexes du groupe symétrique $\mathfrak{S}_n$. En effet c'est un domaine d'applications fertiles des notions étudiées, notamment lié à des problèmes de Mécanique Quantique impliquant des particules identiques. Par ailleurs, elles illustrent de façon élémentaire l'intéret de considérer l'algèbre d'un groupe fini dans le cadre de la théorie des représentations.

16.1. Algèbre d'un groupe fini. —

Définition 16.1. — *Soit k un corps. Une k-algèbre A (associative unitaire) est un k-espace vectoriel muni d'une application bilinéaire $A \times A \longrightarrow A$ qui lui confère une structure d'anneau (unitaire). Un morphisme d'algèbres $f : A \longrightarrow B$*

est un endomorphisme compatible avec les applications bilinéaires.
L'agèbre A est dite graduée si elle est munie d'une décomposition

$$A = \oplus_{d\in\mathbb{N}} A_d$$

en somme d'espaces vectoriels telle que

$$\forall d, e \in \mathbb{N}, A_d A_e \subset A_{d+e}.$$

Un élément non nul $x \in A$ est dit homogène s'il existe $d \in \mathbb{N}$ tel que $x \in A_d$. Alors x est dit de degré d.
Un morphisme d'algèbres graduées est un morphisme d'algèbres $f : A \longrightarrow A'$ qui préserve la graduation $f(A_d) \subset A'_d$ pour tout $d \in \mathbb{N}$.

Définition 16.2. — *Soit G un groupe fini et k un corps, nous notons $k[G]$ la k-algèbre du groupe G, définie comme le k-espace vectoriel*

$$\{\sum_{g\in G} \lambda_g g, \lambda_g \in k\}$$

muni de l'application bilinéaire,

$$\forall a, b \in k[G], a \cdot b = \sum_{g,h\in G} a(g)b(h)gh.$$

En particulier, la composante sur $h \in G$ du produit $a \cdot b$ est le produit de convolution

$$\delta_h((a \cdot b)) = \sum_{g\in G} a(g)b(g^{-1}h) = \sum_{g\in G} a(hg^{-1})b(g).$$

Comme k-espace vectoriel, $k[G]$ est isomorphe à l'espace vectoriel des fonctions de G dans k :

$$k[G] \longrightarrow \mathcal{F}(G),\ g' = \sum_{g\in G} \lambda_g g \mapsto f_{g'} = \sum_{g\in G} \lambda_g \delta_g.$$

Nous pouvons donc identifier g' et $f_{g'}$, ce qui définit une loi de multiplication sur les $f_{g'}$:

$$f_{g'} f_g = g' \cdot f_g = f_{g'g}$$

La représentation régulière est une réalisation explicite de la multiplication dans cette algèbre :

$$\forall g, h \in G, g' \in k[G],\ \ \rho_{\text{reg}}(g)(f_{g'})(h) = f_{g'}(g^{-1}h) = f_{gg'}(h).$$

La puissance des raisonnements basés sur cette algèbre de groupe $k[G]$ tient à cette double interprétation de ses éléments comme vecteurs et comme opérateur sur l'algèbre.
L'algèbre $k[G]$ jouit, par construction de propriétés universelles :

Lemme 16.3. — *Soit (ρ, V) une représentation de G. Le diagramme de factorisation suivant où les flêches verticales sont des inclusions est commutatif :*

$$\begin{array}{ccc} G & \stackrel{\rho}{\longrightarrow} & \mathrm{GL}(V) \\ \downarrow & & \downarrow \\ k[G] & \stackrel{\tilde{\rho}}{\longrightarrow} & \mathrm{End}(V) \end{array}$$

Les notions de représentations équivalentes ou irréductibles, de décomposition en somme directe de sous-espaces stables passent naturellement de ρ à $\tilde{\rho}$.

L'espace de la représentation régulière se décompose en sous-espaces invariants correspondant aux représentations irréductibles :

$$k[G] = \oplus_\rho \mathrm{II}_\rho$$

Chacun des sous-espaces II_ρ est stable par multiplication à gauche :

$\forall f \in \mathrm{II}_\rho, g, h \in G, g'g \cdot f = g'\rho(g)(f) = \rho(g'g)(f) = \rho(g')\rho(g)(f) \Longrightarrow \rho(g)(f) \in \mathrm{II}_\rho.$

En outre, la propriété d'irréductibilité se traduit par le fait que l'idéal est minimal, c'est-à-dire qu'il ne contient pas d'idéal plus petit.

Exemple 16.4. — *Soit $k[G] = \oplus \mathrm{II}_\rho$, une décomposition en idéaux minimaux. Ainsi pour tout $x \in k[X]$ et pour l'élément neutre $e \in G$, nous avons des décompositions uniques :*

$$x = \sum_\rho x_\rho, e = \sum_\rho j_\rho, \;\; x_\rho, j_\rho \in \mathrm{II}_\rho.$$

Donc

$$x = xe = \sum_\rho x j_\rho$$

avec $xj_\rho \in \mathrm{II}_\rho$ qui est un idéal à gauche ; donc par unicité de la décomposition $x_\rho = xj_\rho$. En particulier pour $x = j_\rho$, nous obtenons

$$j_\rho = ej_\rho = i_\rho e = \mathrm{J}_\rho \sum_\sigma j_\sigma = j_\rho^2 + \sum_{\sigma \neq \rho} j_\rho j_\sigma$$

Ainsi par unicité $j_\rho j_\sigma = \delta_{\rho\sigma} j_\rho$.

Définition 16.5. — *Un idempotent $j \in k[G]$ est un élément de l'algèbre $k(G]$ satisfaisant $j^2 = j$.*

Pour tout idempotent $j \in k[G]$, il existe un idéal à gauche II telle que la multiplication à droite par j projette sur II :

$$\mathrm{II} = \{x \cdot j | x \in k[G]\}.$$

En effet $x \cdot j = x \Longrightarrow x \in \mathrm{II}$ et $x \in \mathrm{II} \Longrightarrow \exists y, x = y \cdot j, x \cdot j = y \cdot j^2 = x$.
Un idempotent est dit minimal s'il engendre un idéal minimal.

Exemple 16.6. — *La décomposition de la représentation régulière en représentations irréductibles permet de définir un ensemble d'idempotents orthogonaux* (j_ρ) *:*

$$j_\rho j_\sigma = \delta_{\rho\sigma} j_\rho.$$

Exemple 16.7. — *Soit* II *un idéal à gauche de* $k[G]$ *engendré par un idempotent* j*. Nous considèrons la représentation*

$$\rho : G \longrightarrow \mathrm{GL}(\mathrm{II}), \quad \rho(g)(aj) = gaj$$

et nous souhaitons calculer sa trace. Pour cela, nous remarquons que

$$\rho(g) \text{ et } \phi(g) : k[G] \longrightarrow k[G], x \mapsto gxj$$

ont même trace car $\mathrm{im}(g) \subset \mathrm{im}\,\rho(g)$ *et* $\phi(g)_{\mathrm{II}} = \rho(g)$*. Dans la base naturelle de* $k[G]$ *:*

$$\phi(g)(h) = ghj = \sum_{g' \in G} j(g')ghg' = \sum_{\ell \in G} j(h^{-1}g^{-1}\ell)\ell.$$

La composante sur h *est alors* $j(h^{-1}g^{-1}h)$*. D'où*

$$\chi_\rho(g) = \sum_{h \in G} j(h^{-1}g^{-1}h).$$

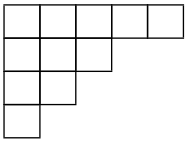
Lemme 16.8. — *Supposons* k *algébriquement clos.*
i. Un idempotent $j \in k[G]$ *est minimal si et seulement si pour tout* $x \in k[G]$*, il existe* $\lambda_x \in k$ *tel que* $jxj = \lambda_x j$*.*
ii. Deux idempotents minimaux j_1, j_2 *de* $k[G]$ *engendrent des représentations équivalentes si et seulement si il existe* $x \in k[G]$ *tel que* $j_1 x j_2 \neq 0$*.*

Démonstration. — i. Soit j non minimal avec $jxj = \lambda_x j$ pour tout $x \in k[G]$. Comme j n'est pas minimal, on a une décomposition en idéaux $\mathrm{II} = \mathrm{II}_1 \oplus \mathrm{II}_2$ et $j = j_1 + j_2$ avec $j_a j_b = \delta_{ab} j_a$. Ainsi $\lambda j = j j_1 j = j_1$ donc j_1 ou $j_2 = 0$.
Si l'idéal engendré par j est minimal, II est une représentation irréductible de G et pour tout $x \in k[G]$, $f(g) = gjxj \in \mathrm{II}$ commute avec la représentation II, donc, par le lemme de Schur, $f(g) = \lambda_x j$.
ii. Supposons qu'il existe $x \in k[G]$ avec $y = j_1 x j_2 \neq 0$. La multiplication à droite par y réalise une application linéaire de II_1 dans II_2 qui commute avec la représentation. Ainsi y est un entrelacement et d'après le lemme de Schur les représentations sont équivalentes. Réciproquement si les représentations sont équivalentes, il existe $Y : \mathrm{II}_1 \longrightarrow \mathrm{II}_2$, $Y\rho_1 = \rho_2 Y$ commutant sur II_1 avec tout $x \in k[G]$. Soit $y = Yj_1 \in \mathrm{II}_1 \cap \mathrm{II}_2$. On a $y = Yj_1 = (Yj_1)j_1 = j_1 Y j_2 = j_1 y$. Par ailleurs $y \in \mathrm{II}_2$ donc $yj_2 = y$ donc $y = j_1 y = j_1 y j_2$. □

16.2. Idempotent associé à un tableau de Young. — William Henry Young est un mathématicien anglais (1863-1942) qui a introduit au début du vingtième siècle les formes, les tableaux et le symétriseur qui portent son nom pour décrire les représentations irréductibles du groupe symétrique $\mathfrak{S}_n$.

Définition 16.9. — *Une forme de Young est un tableau formé de n cases disposées en lignes de longueur décroissante* $(\alpha_i)_{1\leq i\leq r}$. *Une forme de Young est définie par une partition* $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r$ *de l'entier* $n = \sum_{i=1}^{r} \alpha_i$. *Il y a bijection entre l'ensemble des formes de Young et les classes de conjugaison du groupe symétrique* $\mathfrak{S}_n$.
A partir d'une forme de Young, on fabrique des tableaux, dits de Young, en rpartissant les entiers $\{1, \ldots, n\}$ *dans les différentes cases de la forme. Chaque ligne représente alors un cycle et un tableau un e permutation, produit de ces cycles à supports disjoints. Nous notons* $\mathcal{T}_n$ *l'ensemble des tableaux de Young à n cases.*
Le tableau de Young correspondant à une forme de Young dont les cases sont numérotées en ordre croissant de gauche à droite puis de bas en haut est dit tableau de Young standard.

Exemple 16.10. — *Pour* $n = 11 = 5 + 3 + 2 + 1$, *la forme de Young associée s'illustre*



Pour la permutation $(135117)(1086)(49)(2) \in \mathfrak{S}_{11}$ *s'écrit grâce au tableau de Young suivant :*

1	3	5	11	7
10	8	6		
4	9			
2				

Le tableau de Young standard associé à la même forme de Young correspond à la permutation $(12345)(678)(910)(11)$ *:*

1	2	3	4	5
6	7	8		
9	10			
11				

Exemple 16.11. — *Soit* $p(n)$ *le nombre de forme de Young à n cases. Une fonction génératrice des* $p(n)$ *est donnée par le produit d'Euler*

$$\frac{1}{\Pi_{\ell=1}^{\infty}(1-x^{\ell})} = \sum_{n=0}^{\infty} p(n)x^n.$$

Nous montrons dans ce paragraphe que les représentations irréductibles de $\mathfrak{S}_n$ sont en correspondance avec les $p(n)$ formes de Young à n cases.
Nous munissons $\mathcal{T}_n$ de l'ordre lexicographique : pour $\alpha = (\alpha_1, \ldots, \alpha_r)$ et $\beta = (\beta_1, \ldots, \beta_s)$ deux partitions décroissantes de n, nous disons que $\alpha > \beta$ si nous pouvons trouver k avec $0 \leq k \leq r_1$, tel que

$$\alpha_i = \beta_i, 1 \leq i \leq k \text{ et } \alpha_{k+1} > \beta_{k+1} \text{ ou } k+1 > s.$$

C'est un ordre total sur l'ensemble $\mathcal{T}_n$ des tableaux de Young : $\forall \alpha \neq \beta \in \mathcal{T}_n$, $\alpha > \beta$ ou $\beta > \alpha$.
Le groupe symétrique $\mathfrak{S}_n$ agot sur $\mathcal{T}_n$ de la façon suivante : soit $\sigma \in \mathfrak{S}_n$ et $T \in \mathcal{T}_n$, on définit σT comme le tableau de Young ayant la même forme de Young que T et que l'on a rempli en remplaçant i par $\sigma(i)$ dans chaque case. Par exemple pour $\sigma = (1234567)$

$$T \qquad \mapsto \qquad \sigma T$$

1	3	5	11	7
10	8	6		
4	9			
2				

2	4	6	11	1
10	8	7		
5	9			
3				

A un tableau de Young $T \in \mathfrak{S}_n$ de forme $(\alpha_i)_{1 \leq i \leq r}$, on associe deux sous-groupes de $\mathfrak{S}_n$:
- $\Lambda = \Pi_{1 \leq i \leq r} \mathfrak{S}_i$, le sous-groupe des permutations qui stabilisent globablement chaque ligne de T ;
- Δ le sous-groupe des permutations qui stabilisent globablement chaque colonne de T. C'est aussi un produit direct de groupes symétriques.

Lemme 16.12. — *i. Soit $T \in \mathcal{T}_n$ un tableau de Young et $\sigma_0 \in \mathfrak{S}_n$ la permutation associée. Soit σ une permutation de $\mathfrak{S}_n$.*
i. Le tableau σT est de la même forme que T et a pour permutation associée $\sigma \sigma_0 \sigma^{-1}$.
ii. Si Λ et Δ sont les sous-groupes associés à T alors $\sigma \Lambda \sigma^{-1}$ et $\sigma \Delta \sigma^{-1}$ sont les sous-groupes associés à σT.
En particulier, $\Lambda \cap \Delta = \{e\}$.

Démonstration. — Le lemme résulte de l'action de $\mathfrak{S}_n$ sur $\mathcal{T}_n$ et de la formule de conjugaison dans $\mathfrak{S}_n$. □

Exemple 16.13. — *Soit T, T' deux tabeaux de Young de forme respective $\alpha = (\alpha_i)_{1 \leq i \leq r}$ et $\alpha' = (\alpha'_i)_{1 \leq i \leq r'}$ avec $\alpha \geq \alpha'$. On suppose que deux éléments d'une même colonne de T' ne sont jamais dans une même ligne de T. Alors $\alpha = \alpha'$. De plus il existe $\ell \in \Lambda$ et $d \in \Delta$ tels que $T' = ldT$. En particulier, il n'existe pas de transposition dans $\Lambda \cap \Delta'$.*
Comme les éléments de la première ligne de T sont dans des colonnes distinctes de T', le tableau T' a au moins α_1 colonnes et comme $\alpha \geq \alpha'$, on a $\alpha_1 = \alpha'_1$.
On note Λ' et Δ' les sous-groupes associés à T'. Il existe $d'_1 \in \Delta'$ tel que la première ligne de $d'_1 T'$ coïncide à l'ordre près avec celle de T. Il existe donc $\ell_1 \in \Lambda$, tel que $\ell_1 T$ et $d'_1 T'$ aient la même première ligne. On itère cette opération (à première ligne fixée et on obtient enfin une égalité du type $\ell T = d' T'$ avec $\ell \in \Lambda$ et $d' \in \Delta'$, soit $T' = d'^{-1} \ell T$. Par conséquent les groupes Δ et Δ' sont conjugués via $\sigma = d'^{-1} \ell$. Il existe donc $d \in \Delta$, avec

$$d'^{-1} = d'^{-1} \ell d \ell^{-1} d'.$$

D'où $d'^{-1} = \ell d \ell^{-1}$ et $T' = \ell d T$.

Définition 16.14. — *Soit $T \in \mathcal{T}_n$ un tableau de Young, Λ, Δ les sous-groupes de $\mathfrak{S}_n$ associés à T. Les symétriseur s_T et antisymétriseur a_T attachés au tableau de Young T sont les éléments de $\mathbb{C}[\mathfrak{S}_n]$ définis par*

$$s_T = \sum_{\ell \in \Lambda} \ell, \quad a_T = \sum_{d \in \Delta} \varepsilon(d) d,$$

où ε désigne la signature de $\mathfrak{S}_n$.

Lemme 16.15. — *Les propriétés élémentaires suivantes sont satisfaites :*
- $s_T \neq 0$, $a_T \neq 0$ *et* $j_T = s_T a_T \neq 0$ *(car* $j_T(e) = e$ *car* $\Delta \cap \Lambda = \{e\}$*),*
- $\ell s_T = s_T \ell = s_T$, $\ell \in \lambda$,
- $\varepsilon(d) d a_T = a_T \varepsilon(d) d = a_T$, $d \in \Delta$,
- $s_T^2 = |\Lambda| s_T$,
- $a_T^2 = |\Delta| a_T$,
- $\ell j_T \varepsilon(d) d = j_T, \ell \in \lambda, d \in \Delta$.

Les éléments s_T et a_T sont donc à normalisation près des idempotents. Mais en général ils ne sont pas minimaux. En revanche nous allons montrer que j_T est un idempotent minimal à normalisation près.

Lemme 16.16. — *Soit T, T' deux tableaux de Young de forme $\alpha > \alpha'$.*
i. Les trois relations suivantes sont vérifiées pour tout $\sigma \in \mathfrak{S}_n$ et $a \in k[\mathfrak{S}_n]$:

$$s_T a_{T'} = 0, s_T \sigma a_{T'} \sigma^{-1} = 0, s_T a a_{T'} = 0.$$

ii. On a $j_T j_{T'} = 0$.
iii. Si un élément $a \in k[\mathfrak{S}_n]$ satisfait $\ell a \varepsilon(d) d = a$ pour tout $\ell \in \Lambda$ et $d \in \Delta$ alors il existe $c \in k$ tel que $a = c j_T$.
iv. Pour tout $a \in k[\mathfrak{S}_n]$, on a $j_T a j_T \in k j_Y$.

Démonstration. — i. Vu les hypothèses, il existe une transposition $\tau = (ij)$ telle que son support soit simultanément dans une même ligne de$T$ et une même colonne de T'. D'après le lemme 16.15,

$$s_T a_{T'} = s_T \tau \varepsilon(\tau) \tau a_{T'} = -s_T a_{T'} = 0.$$

Comme $\sigma T'$ et T' ont la même forme de Young, nuos en déduisons $s_T \sigma a_{T'} \sigma^{-1} = 0$. Pour $a = \sum_{g \in \mathfrak{S}_n} a(\sigma)\sigma \in k[\mathfrak{S}_n]$, nous avons

$$\forall \sigma \in \mathfrak{S}_n, s_T \sigma a_{T'} \sigma^{-1} = 0, s_T \sigma a(\sigma) a_{T'} \sigma^{-1} = 0, s_T \sigma a(\sigma) a_{T'} \sigma^{-1} \sigma = 0$$

donc $\sum_{\sigma \in \mathfrak{S}_n} s_T a(\sigma) \sigma a_{T'} = 0$; d'où $s_T a a_{T'} = 0$.
ii. $j_T j_{T'} = s_T (a_T s_{T'}) a_{T'} = 0$.
iii. Comparons les composantes de $a = \sum_{\sigma \in \mathfrak{S}_n} a(\sigma)\sigma$ avec celles de $\ell a \varepsilon(d) d$. La composante sur $\sigma = \ell d$, donne $\varepsilon(d) a(1) = a(\ell d)$ pour tout $\ell \in \Lambda$ et $d \in \Delta$.
Pour σ qui n'est pas de la forme ℓd, comparons les tableaux T et $T' = \sigma T$. Il existe une transposition τ de support sur une ligne de T et une colonne de $\sigma T'$. Ainsi τ stabilise les colonnes de T' et $\sigma^{-1} \tau \sigma$ stabilise les colonnes de T. Posons $\ell = \tau$

et $d = \sigma^{-1}\tau\sigma$, ainsi en regardant la composante sur σ de a, $a(\sigma) = \varepsilon(d)a(\sigma) = 0$.
iv. $j_T a j_T$ satisfait les hypothèses de iii. □

Nous montrons qu'on peut associer un idempotent minimal à chaque forme de Young. Si on peut montrer que les représentations associées ne sont pas équivalentes, vues qu'elles sont en nombre adéquat, nous aurons construit toutes les représentations irréductibles de $\mathfrak{S}_n$.
Le lemme suivant permet d'associer à un tableau de Young une représentation irréductible non réduite à $\{0\}$ du groupe symétrique $\mathfrak{S}_n$.

Proposition 16.17. — *Soit T un tableau et Young $j_T = s_T a_T$ le produit du symétriseur et de l'antisymétriseur associé. L'idéal à gauche* II *engendré dans* $\mathbb{C}[\mathfrak{S}_n]$ *par* j_T *est minimal.*

Démonstration. — Soit $J \subset$ II un idéal à gauche de $\mathbb{C}[\mathfrak{S}_n]$ inclus dans II. On a les inclusions (d'après le lemme16.16) : $j_T J \subset j_T$II $\subset \mathbb{C}j_T$. Comme $\mathbb{C}j_T$ est un espace vectoriel de dimension 1, on a :
- soit $j_T J = \mathbb{C}j_T$, donc II $= \mathbb{C}[\mathfrak{S}_n]j_T = \mathbb{C}[\mathfrak{S}_n](\mathbb{C}j_T) = \mathbb{C}[\mathfrak{S}_n]j_T J \subset J$. Donc II $= J$.
- Soit $j_T J = \{0\}$. D'où $J^2 \subset$ II$J = \mathbb{C}[\mathfrak{S}_n]j_T J = \{0\}$. Donc $J^2 = 0$. Or sur le corps de base $\mathbb{C}$, nous disposons d'une involution naturelle de $\mathbb{C}[\mathfrak{S}_n]$:

$$a = \sum_{g\in\mathfrak{S}_n} a(g)g \mapsto a^* = \sum_{g\in\mathfrak{S}_n} \overline{a(g)}g.$$

En particulier, $aa^* = 0 \iff a = 0$. Mais pour $a \in J$, on a $a^*a \in J$, donc $(a^*a)^2 = 0$. Or $(a^*a)^2 = (a^*a)(a^*a)^* = 0$ implique $a^*a = 0$ donc $a = 0$ et $J = 0$. □

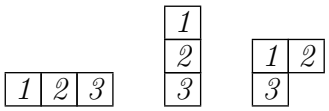
Proposition 16.2.1. — *Les représentations associées à deux tableaux de Young de formes différentes ne sont pas équivalentes.*

Démonstration. — Soient T, T' deux tableaux de Young associés à des formes $\alpha > \alpha'$. Sur l'espace vectoriel sous-jacent à l'idéal engendré par j_T, l'action de s_T n'est pas nulle car $s_T j_T = |\Lambda| j_T \neq 0$, tandis que l'action de s_T sur l'idéal engendré par $j_{T'}$ est nulle car $s_T j_{T'} = s_T s_{T'} a_{T'} = 0$. Donc les deux représentations ne sont pas équivalentes. □

Théorème 16.18. — *Les représentations irréductibles de $\mathfrak{S}_n$ sont en correspondance avec les formes de Young à n cases.*

Exemple 16.19. — *Considérons $\mathfrak{S}_3$. Nous disposons trois tableaux de Young standards ayant des formes différentes*

$$T_1 \qquad T_2 \qquad T_3$$



Pour chacun d'entre eux, nous calculons symétriseur, antisymétriseur et représentation irréductible associés :

$$s_{T_1} = \sum_{g\in\mathfrak{S}_n} g, a_{T_1} = e, \rho_1 = \text{triv}$$

$$s_{T_2} = e, a_{T_2} = \sum_{g\in\mathfrak{S}_n} g, \rho_2 = \varepsilon$$

Le calcul de la représentation associé au tableau T_3 est un peu moins direct

$$s_{T_3} = e + (12), a_{T_3} = e - (13), j_{T_3} = e + (12) - (13) - (132).$$

Ainsi $j_{T_3}j_{T_3} = 3j_{T_3}$. L'idéal à gauche de $\mathfrak{S}_3$ engendré par j_{T_3} est de dimension 2 sur $\mathbb{C}$ engendré, comme espace vectoriel par j_{T_3} et $(13)j_{T_3} = e+(23)-(13)-(123)$. Dans cette base, les matrices de la représentation s'écrivent

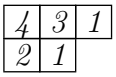
$$\rho((12)) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \rho((13)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \rho((23)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\rho(e) = \mathrm{Id}, \rho((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \rho((132)) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Remarque 16.20. — *Il peut être utile de connaître la dimension de la représentation irréductible associée à un tableau de Young T à ℓ lignes et n cases. Nous notons $f_1 \geq \cdots \geq f_\ell$ les longueurs de chaque ligne et on pose $\ell_i = f_i + \ell - i$, $0 \leq i \leq \ell$. Ainsi $\ell_1 > \ell_2 > \cdots > \ell_\ell$ et la dimension de la représentation associée à T est*

$$n_T = \frac{n!}{\Pi_i \ell_i!} \Pi_{i<j}(\ell_i - \ell_j).$$

Nous pouvons reformuler cette expression de la façon suivante : à chaque case, nous comptons le nombre de cases placées au-dessous ou à droite y compris la case elle-même. La dimension est donnée par $n!$ divisé par le produit de ces nombres pour toutes les cases. Considérons la forme de Young dans laquelle nous avons indiqué le nombre en question à l'intérieur de chaque case :



La représentation de $\mathfrak{S}_5$ associée est de dimension $\frac{5!}{4\cdot3\cdot1\cdot2\cdot1} = 5$.
En particulier des tableaux symétriques par rapport à la diagonale donnent des représentations duales de dimensions égales.

PARTIE IV

GROUPES CLASSIQUES

Il y a 18 familles infinies de groupes simples. Nous avons vu les groupes cycliques, les groupes alternés. Les autres familles s'obtiennent en considérant des quotients de sous-groupes du groupe linéaire. Nous avons ainsi construit la famille des groupes simples projectifs linéaires. Nous construisons dans ce chapitre les familles projectives symplectiques, projectives spéciales unitaires et de sous-groupes projectifs orthogonaux. La classification des groupes simples (achevée en 1980) nécessiterait également la description des 26 groupes sporadiques.

17. Formes sesquilinéaires

17.1. Premières définitions. — Dans ce paragraphe, V désigne un espace vectoriel de dimension finie $n \geq 2$ sur un corps k et $\theta : k \longrightarrow k$ un automorphisme de corps. Pour toute matrice M à coefficients dans k, nous notons $\theta(M)$ la matrice obtenue en appliquant θ composante par composante.

Définition 17.1. — *Une forme θ-sesquilinéaire sur V est une application*

$$b : V \times V \longrightarrow k$$

telle que pour tout $y \in V$, l'application $x \mapsto b(x, y)$ est linéaire et l'application $x \mapsto b(y, x)$ est θ-linéaire : $\forall \lambda_1, \lambda_2, \mu_1, \mu_2 \in k$, $\forall u_1, u_2, v_1, v_2 \in V$,

$$b(\lambda_1 u_1 + \lambda_2 u_2, \mu_1 v_1 + \mu_2 v_2) = \sum_{i=1}^{2} \sum_{j=1}^{2} \lambda_i \theta(\mu_j) b(u_i, v_j).$$

Le mot "sesquilinéaire" ("1 et demi"-linéaire) s'éclaire par le fait que la θ-linéarité est dit semi-linéarité. Lorsque $\theta = \mathrm{Id}_k$, une forme θ-sesquilinéaire est simplement une forme bilinéaire.

Lemme 17.2. — *Soit b une forme θ-sesquilinéaire. Nous notons M la matrice de b dans une base $(e_1, \ldots, e_n)$ de V :*

$$M = (b(e_i, e_j))_{1 \leq i,j \leq n}.$$

i. Si les éléments de V sont représentés par les vecteurs colonnes X et Y, alors $b(X, Y) = {}^t X M \theta(Y)$.
ii. Si P est la matrice de passage de la base (e_i) à la base (e'_i), la matrice de b dans la base (e'_i) est donnée par

$$M' = {}^t P M \theta(P).$$

Le rang de b est le rang de la matrice associée M (il est bien défini).

Démonstration. — i. Avec des notations naturelles,

$$b(X,Y) = b\Big(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i \theta(y_j) b(e_i, e_j) = {}^t X M \theta(Y).$$

ii. Pour tous $X = PX'$ et $Y = PY'$

$${}^t XM\theta(Y) = {}^t(PX')M\theta(PY') = {}^t X' {}^t P M \theta(P) Y' = {}^t X' M' Y',$$

d'où $M' = {}^t P M \theta(P)$. □

Définition 17.3. — *Une forme b θ-sesquilinéaire est dite*
- reflexive si $b(x,y) = 0 \Longleftrightarrow b(y,x) = 0$, $x, y \in V$.
Si, de plus, la forme est bilinéaire (i.e $\theta = \mathrm{Id}_k$), b est dite
- symétrique si $b(x,y) = b(y,x)$, $x, y \in V$,
- antisymétrique si $b(x,y) = -b(y,x)$, $x, y \in V$,
- alternée si $b(x,x) = 0$, $x \in V$.
Si, de plus, $\theta \neq \mathrm{Id}_k$, b est dite
- hermitienne si $b(x,y) = \theta(b(y,x))$, $x, y \in V$.

La forme b est (anti)symétrique si et seulement si la matrice M associée est (anti)symétrique. La forme b est hermitienne si et seulement si la matrice M associée est hermitienne : $M = {}^t\theta(M)$.
Une forme symétrique, antisymétrique ou hermitienne est réflexive.
Si la forme bilinéaire ($\theta = \mathrm{id}_k$) b est alternée, alors elle est antisymétrique. En effet, $b(x+y, x+y) = b(x,y) + b(y,x) + b(x,x) + b(y,y) = 0$. Donc

$$b(x,y) = -b(y,x), x, y \in V.$$

La réciproque est vraie si car$k \neq 2$, car alors $2b(x,x) = 0$ implique $b(x,x) = 0$.

Remarquons qu'en caractéristique 2, les définitions de forme symétrique et antisymétrique coïncident. La caractéristique 2 soulève des questions de nature différente du cas général. Nous en exhibons quelques unes, c'est pourquoi nous n'excluons pas a priori la caractéristique 2.

Exemple 17.4. — *Si* car$k \neq 2$, *une forme bilinéaire symétrique alternée est nulle. En effet*

$$2b(x,y) = b(x+y, x+y) - b(x,x) - b(y,y), \forall x, y \in V.$$

Si $V = \mathbb{F}_2^2$, $b(u,v) = u_1v_2 + u_2v_1$ est symétrique alternée et non nulle. Plus généralement, si V est de dimension finie sur un corps de caractéristique 2, une forme bilinéaire est alternée si et seulement si sa matrice est symétrique avec des coefficients diagonaux nuls.

Définition 17.5. — *Soit b une forme θ-sesquilinéaire reflexive sur V, $u, v \in V$. Les vecteurs u et v de V sont dits orthogonaux si $b(u,v) = 0$.*

Soit $X \subset V$ une partie de V Si $X \subset V$, le sous-espace vectoriel de V

$$X^{\perp} = \{w \in V \mid b(w,x) = 0, \text{ pour tout } x \in X\}$$

est dit orthogonal de X.
Si $V^{\perp} = \{0\}$, b est dite non dégénérée. Sinon, $V^{\perp} \neq \{0\}$ et b est dite dégénérée.

Nous disposons d'une caractérisation simple de la dégénérescence de b en termes d'inversibilité de sa matrice associée. Pour W un sous-espace vectoriel de V, nous notons l'espace vectoriel des formes linéaires sur W, $W^* = \mathrm{Hom}_k(W,k)$.

Définition 17.6. — *Soit b une forme θ-sesquilinéaire sur V. L'adjoint* $\mathrm{ad}(b)$ *de b est l'application définie par*

$$\mathrm{ad}(b) : V \longrightarrow V^*, \mathrm{ad}(b)(y)(x) = b(x,y), x, y \in V.$$

L'adjoint de b est θ-semilinéaire :

$$\mathrm{ad}(b)(\mu y + \mu' y') = \theta(\mu)\mathrm{ad}(b)(y) + \theta(\mu')\mathrm{ad}(b)(y').$$

Lemme 17.7. — *Soit b une forme θ-sesquilinéaire sur V de matrice M dans une base (e_i) fixée. Les assertions suivantes sont équivalentes :*
i. la forme b est non dégénérée,
ii. l'application $\mathrm{ad}(b) : V \longrightarrow V^*$ *est inversible,*
iii. la matrice M est inversible.

Démonstration. — i.$\Longleftrightarrow$ ii. Remarquons que $V^{\perp} = \ker \mathrm{ad}(b)$. Donc b est non dégénérée si et seulement $\mathrm{ad}(b)$ est inversible.
ii.$\Longleftrightarrow$ iii. Soit $y \in V$. La matrice de $\mathrm{ad}(b)(y)$ dans la base duale de (e_i) est $M\theta(y)$. Comme θ est bijectif, $\mathrm{ad}(b)$ est inversible si et seulement si l'application "multiplication par M" l'est. □

Comme première application de ce lemme, nous citons le résultat suivant :

Lemme 17.8. — *Soit b une forme θ-sesquilinéaire reflexive non dégénérée et X est un sous-espace vectoriel de V,*

$$\dim X + \dim X^{\perp} = \dim V.$$

En particulier si $X \cap X^{\perp}\{0\}$, alors $V = X \oplus X^{\perp}$.

Démonstration. — Notons X' le k-espace vectoriel obtenu en munissant le groupe additif X de la structure de k-espace vectoriel donnée par $\lambda \cdot x = \theta(\lambda)x$ pour $\lambda \in k$ et $x \in X$. Ainsi $\dim X' = \dim X$. L'application de restriction de $\mathrm{ad}(b)$ à X^*

$$\varphi : V \longrightarrow X^*, X' \mapsto b(x, \cdot)$$

est θ-linéaire surjective et $\ker \varphi = X^{\perp}$. L'application obtenue en changeant la structure de k-espace vectoriel $\varphi' : V \longrightarrow X'^*$ est alors linéaire surjective de noyau $X^{\perp}$. Ainsi

$$\dim V = \dim X^{\perp} + \dim X' = \dim X^{\perp} + \dim X.$$

□

17.2. Groupes d'isométries. —

Définition 17.9. — *Soit b une forme θ-sesquilinéaire sur V. Nous appelons groupe d'isométries de (V,b) le sous-groupe de* $\mathrm{GL}(V)$*,*

$$\mathrm{Isom}(V,b) = \{u \in \mathrm{GL}(V) \mid b(x,y) = b(u(x),u(y)),\ \textit{pour tous } x,y \in V\}.$$

Si b est reflexive dégénérée, $\mathrm{Isom}(V,b)$ laisse invariant le sous-espace $V^\perp$ et agit sur $V/V^\perp$ en préservant la forme induite $\bar{b}$:

$$\bar{b}(x+V^\perp, y+V^\perp) = b(x,y).$$

La forme $\bar{b}$ est non dégénérée et

$$\mathrm{Isom}(V,b) = \mathrm{Isom}(V/V^\perp, \bar{b}) \times \mathrm{GL}(V^\perp).$$

Quitte à retreindre b à $V/V^\perp$ et sauf mention explicite du contraire, nous supposons dorénavant que b est non dégénérée et reflexive.

Définition 17.10. — *Pour b symétrique, le groupe* $\mathrm{Isom}(V,b)$ *est dit groupe orthogonal et noté* $\mathrm{O}(V,b)$*.*
Pour b alternée, le groupe $\mathrm{Isom}(V,b)$ *est dit groupe symplectique et noté* $\mathrm{Sp}(V,b)$*.*
Pour b hermitienne, le groupe $\mathrm{Isom}(V,b)$ *est dit groupe unitaire et noté* $U(V,b)$*.*

Si M est la matrice de la forme b dans une base,

$$\mathrm{Isom}(V,b) = \{A \in \mathrm{GL}_n(k) \mid {}^tAM\theta(A) = M\}.$$

Plus généralement, il est utile de considérer des isométries entre deux espaces vectoriels différents munis de formes θ-sesquilinéaires :

Lemme 17.11. — *Soient $(V_1,b_1),(V_2,b_2)$ des espaces vectoriels munis de formes θ-sesquilinéaires. Une isométrie de V_1 dans V_2 est un isomorphisme d'espaces vectoriels $\varphi : V_1 \longrightarrow V_2$, tel que*

$$b_2(\varphi(x),\varphi(y)) = b_1(x,y), x,y \in V_1.$$

Soient U et U' deux sous-espaces de V_1 tels que $V_1 = U \oplus U'$ et $\varphi : U \longrightarrow V_2$, $\varphi' : U' \longrightarrow V_2$ des applications linéaires satisfaisant
i. $\varphi : U \longrightarrow \varphi(U)$ et $\varphi' : U' \longrightarrow \varphi'(U')$ sont des isométries,
ii. $V_2 = \varphi(U) \oplus \varphi'(U')$,
iii. $b_2(\varphi(u),\varphi'(u')) = b_1(u,u')$ et $b_2(\varphi'(u'),\varphi(u)) = b_1(u',u)$ pour tout $u \in U$ et $u' \in U'$.
Alors $\varphi \oplus \varphi'$ est une isométrie de V_1 dans V_2.

Démonstration. — Il suffit de vérifier que pour tous $u, v \in U$ et $u', v' \in U'$, nous avons :

$$b_2(\varphi(u) + \varphi'(u'), \varphi(v) + \varphi'(v')) = b_1(u + u', v + v').$$

□

17.3. Forme quadratique et polarisation. — Nous exhibons le lien entre forme bilinéaire symétrique et forme quadratique. Les formes quadratiques sont les objets qui apparaissent naturellement en géométrie pour mesurer des longueurs. Les groupes de transformations qui préservent les distances sont des groupes d'isométrie. En caractéristique différente de deux, les deux notions sont équivalentes. En revanche, pour car$k = 2$, la notion de forme quadratique est mieux adaptée.

Définition 17.12. — *Une forme quadratique sur V est une application $f : V \longrightarrow k$, telle que*

$$f(au + v) = a^2 f(u) + ab(u, v) + f(v), a \in k, u, v \in V,$$

où l'application $b : V^2 \longrightarrow k$ est une forme bilinéaire dite polarisation de f.

La polarisation d'une forme quadratique est une forme bilinéaire symétrique. Réciproquement, si car$k \neq 2$ et si b est une forme bilinéaire symétrique sur V, alors il existe une unique forme quadratique f sur V telle que

$$b(x, y) = f(x + y) - f(x) - f(y), x, y \in V;$$

en effet nous avons nécessairement, $f(v) = \frac{1}{2}b(v, v)$, $v \in V$.
En caractéristique 2, la polarisation b d'une forme quadratique f est alternée car

$$0 = f(2v) = f(v + v) = 2f(v) + b(v, v) = b(v, v).$$

En caractéristique 2, plusieurs formes quadratiques correspondent à la même forme bilinéaire symétrique alternée. C'est l'une des raisons pour laquelle, nous considérons les formes quadratiques plutôt que les formes bilinéaires symétriques en caractéristique 2 (et aussi en caractéristique différente de deux).

Définition 17.13. — *Une forme quadratique $f : V \longrightarrow k$ de polarisation b est dite non-dégénérée si*

$$f(x) = 0 \text{ et } \Big(\forall y \in V, b(x, y) = 0\Big) \Longrightarrow x = 0.$$

Remarque 17.14. — *Une forme quadratique est dite non singulière si le noyau de sa polarisation est réduit à $\{0\}$. La polarisation d'une forme quadratique non singulière peut être dégénérée (en toute caractéristique). En caractéristique différente de 2, une forme quadratique est non dégénérée si et seulement si sa polarisation l'est.*

Proposition 17.3.1. — *(Réduction de Gauss). Supposons* car$k \neq 2$. *Soit f une forme quadratique sur V. Alors il existe $(\alpha_i)_{1\leq i\leq n} \in k^n$ et une base de V dans laquelle la forme f s'écrit*

$$f(x_1, \ldots, x_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2,$$

le nombre de coefficient $\alpha_i \neq 0$ est dit rang de f. Il coïncide avec le rang de b.

Démonstration. — Si la forme bilinéaire symétrique b n'est pas nulle, il existe $x, y \in V$ avec $b(x, y) \neq 0$ donc il existe $x \in V$ avec $b(x, x) \neq 0$. Nous avons alors $V = kx \oplus x^\perp$ et par induction (en considérant la restriction de b à $x^\perp$), nous construisons une base orthogonale $(e_1, \ldots, e_n)$ de V, i.e telle que $b(e_i, e_j) = 0$, $i \neq j$. En posant $\alpha_i = \frac{1}{2}b(e_i, e_i)$, nous obtenons la réduction de Gauss. □

Lemme 17.15. — *(Théorème de Sylvester). Soit f une forme quadratique non dégénérée de V de dimension n. Si k est algébriquement clos (ou quadratiquement clos), il existe une base de V dans laquelle f s'écrit :*

$$f(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2.$$

Son groupe orthogonal (indépendant de f) est noté $\mathrm{O}_n(k)$.

Démonstration. — D'après la réduction de Gauss, il existe une base de V dans laquelle

$$f(x_1, \ldots, x_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2, \alpha_i \neq 0.$$

Si k est algébriquement clos (ou quadratiquement clos $k = k^2$), pour chaque $\alpha_i \in k$, il existe $a_i \in k$ avec $a_i^2 = 1/\alpha_i$. Dans la base $(a_1 e_1, \ldots, a_n e_n)$, la forme quadratique f s'écrit

$$f(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2.$$

□

Lemme 17.16. — *Soit f une forme quadratique non dégénérée de V de dimension n sur $k = \mathbb{R}$. Alors il existe une base dans laquelle*

$$f(x_1, \ldots, x_n) = x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_n^2.$$

Le couple $(r, n-r)$ est la signature de f, son groupe orthogonal est noté $\mathrm{O}_{r,n-r}(\mathbb{R})$ *(nous notons aussi* $\mathrm{O}_n(\mathbb{R})$ *pour* $\mathrm{O}_{n,0}(\mathbb{R})$*) et les groupes* $\mathrm{O}_{r,n-r}(\mathbb{R})$ *et* $\mathrm{O}_{n-r,r}(\mathbb{R})$ *sont isomorphes.*

Démonstration. — D'après la réduction de Gauss, il existe une base de V dans laquelle

$$f(x_1, \ldots, x_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2, \alpha_i \neq 0.$$

Pour chaque α_i, il existe $a_i \in \mathbb{R}$ avec $a_i^2 = \pm 1/\alpha_i$. □

Lemme 17.17. — *Soit f une forme quadratique non dégénérée de V de dimension n sur $k = \mathbb{F}_q$ (*car$k \neq 2$*), il existe une base dans laquelle f s'écrit sous l'une des deux formes suivantes :*

$$f(x_1, \ldots, x_n) = \begin{cases} x_1^2 + \cdots + x_n^2, \\ x_1^2 + \cdots + x_{n-1}^2 + \alpha x_n^2, \end{cases}$$

où $\alpha \in \mathbb{F}_q$ n'est pas un carré.

Démonstration. — D'après la réduction de Gauss, il existe une base orthogonale dans laquelle f s'écrit

$$f(x) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$$

Le morphisme $\mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$, $x \mapsto x^2$ a pour noyau $\{\pm 1\}$ (q impair), donc son image est de cardinal $(q-1)/2$, en ajoutant 0, il y a $(q+1)/2$ carrés dans $\mathbb{F}_q$. Pour $a, b \in \mathbb{F}_q^*$ et $c \in \mathbb{F}_q$, il existe $x, y \in \mathbb{F}_q$ tels que $ax^2 = c - by^2$ (en effet quand x, y décrivent $\mathbb{F}_q$, ax^2 et by^2 décrivent des sous-ensembles à $(q+1)/2$ éléments dans $\mathbb{F}_q$ d'ordre a, donc ces sous-ensembles sont non disjoints). Par conséquent, il existe $x_1, x_2 \in \mathbb{F}_q$ avec $f(x_1, x_2, 0 \ldots, 0) = \alpha_1 x_1^2 + \alpha_2 x_2^2 = 1$. Posons $e_1 = (x_1, x_2, 0, \ldots, 0)$. La décomposition $V = ke_1 \oplus e_1^\perp$ permet de conclure par induction. □

17.4. Formes sesquilinéaires reflexives non dégénérées. —

Lemme 17.18. — *Soit b une forme θ-sesquilinéaire reflexive non-dégénérée sur V. Alors*

$$\theta^2 = \mathrm{Id}_k \,.$$

Démonstration. — L'application $b : V^2 \longrightarrow k$ est surjective. En effet, soit $x \in V - \{0\}$, comme b est non dégénérée, il existe $y \in V$ avec $b(x, y) \neq 0$. Alors pour tout $t \in k$,

$$t = b\left(\frac{tx}{b(x,y)}, y\right),$$

d'où la surjectivité.

Soit $y_0 \in V - \{0\}$. Soit $\gamma \in V^*$ défini par

$$\gamma(x) = \theta^{-1}(b(y_0, x)), x \in V.$$

Les applications $\alpha_0 = \mathrm{ad}(b)(y_0)$ et γ sont non nulles car $\mathrm{ad}(b) : V \longrightarrow V^*$ est injectif et $y_0 \neq 0$. Comme b est reflexive,

$$\mathrm{ad}(b)(y_0)(x) = 0 \Longleftrightarrow \gamma(x) = 0$$

donc $\ker \alpha_0 = \ker \gamma$. La forme α_0 est donc un multiple scalaire (non nul) de γ. Posons $\alpha_0 = \lambda(y_0)\gamma$ où $\lambda(y_0) \in k^*$. Ainsi pour tout $x \in V$,

$$b(x, y_0) = \alpha_0(x) = \lambda(y_0)\gamma(x) = \lambda(y_0)\theta^{-1}(b(y_0, x))$$

Ainsi pour tout $y \in V$, il existe $\lambda(y) \in k^*$ tel que

$$b(x,y) = \lambda(y)\theta^{-1}(b(y,x)), x \in V.$$

Soient $y, y' \in V$ linéairement indépendants. Pour tout $x \in V$,

$$\begin{aligned} b(x, y+y') &= \lambda(y+y')\theta^{-1}b(y+y', x) \\ &= \lambda(y+y')\theta^{-1}b(y,x) + \lambda(y+y')\theta^{-1}b(y',x), \end{aligned}$$

$$\begin{aligned} b(x, y+y') &= b(x,y) + b(x,y') \\ &= \lambda(y)\theta^{-1}b(y,x) + \lambda(y')b(y',x) \end{aligned}.$$

Donc $(\lambda(y+y') - \lambda(y))\theta^{-1}b(y,x) + (\lambda(y+y') - \lambda(y'))\theta^{-1}b(y',x) = 0$;
puis comme θ est un automorphisme

$$\theta(\lambda(y+y') - \lambda(y))b(y,x) + \theta(\lambda(y+y') - \lambda(y'))b(y',x) = 0;$$

et par linéarité de b par rapport à la première variable :

$$b\Big(\theta(\lambda(y+y') - \lambda(y))y + \theta(\lambda(y+y') - \lambda(y'))y', x\Big) = 0, x \in V.$$

Donc, comme b est non dégénérée

$$\theta(\lambda(y+y') - \lambda(y))y + \theta(\lambda(y+y') - \lambda(y'))y' = 0.$$

Comme y et y' sont linéairement indépendants :

$$\lambda(y+y') = \lambda(y) = \lambda(y'), y, y' \in V.$$

Donc il existe $\lambda \in k^*$ tel que pour tout $x, y \in V$,

$$b(x,y) = \lambda\theta^{-1}(b(y,x)).$$

Choisissons $x, y \in V$ avec $b(x,y) = 1$, nous avons

$$1 = b(x,y) = \lambda\theta(b(y,x)) = \lambda\theta^{-1}(\lambda\theta^{-1}(b(x,y))) = \lambda\theta^{-1}(\lambda)\theta^{-2}b(x,y) = \lambda\theta^{-1}(\lambda).$$

D'où $b(x,y) = \theta^{-2}(b(x,y)), x, y \in V$ et $\theta^2 = \mathrm{Id}$. □

Théorème 17.19. — *Soit b une forme θ-sesquilinéaire reflexive non-dégénérée sur V. Alors l'une des assertions suivantes est vraie :*
i. $\theta = \mathrm{Id}_k$ et b est symétrique ou antisymétrique,
ii. $\theta \neq \mathrm{Id}_k$, $\theta^2 = \mathrm{Id}_k$ et il existe une forme hermitienne β sur V et $a \in k^*$ tels que $b = a\beta$.

Démonstration. — *i*. Supposons $\theta = \mathrm{Id}_k$. Avec les notations de la preuve du lemme 17.18, $\lambda^2 = 1$, donc $\lambda = \pm 1$. Si $\lambda = 1$, $b(x,y) = b(y,x)$ et b est symétrique. Si $\lambda = -1$, $b(x,y) = -b(y,x)$ donc b est antisymétrique.
ii. Supposons $\theta \neq \mathrm{Id}_k$. Montrons qu'il existe $t_0 \in k$ tel que $t_0 + \theta(\lambda)\theta(t_0) \neq 0$. En effet, si pour tout $t \in k$, $t + \theta(\lambda)\theta(t) = 0$ alors pour $t = 1$, $\theta(\lambda) = -1 = \lambda$ donc $t - \theta(t) = 0$ pour tout $t \in k$, donc $\theta = \mathrm{Id}_k$ absurde !
Posons $a = t_0 + \theta(\lambda)\theta(t_0) \neq 0$. Comme $\lambda\theta(\lambda) = 1$, nous avons

$$\theta(a) = \theta(t_0 + \theta(\lambda)\theta(t_0)) = \theta(t_0) + \lambda t_0 = \lambda(\theta(t_0)\theta(\lambda) + t_0) = \lambda a.$$

Et comme $a \neq 0$, $\lambda = \frac{\theta(a)}{a}$.
La forme

$$\beta(x, y) = ab(x, y), x, y \in V.$$

est alors hermitienne, d'après le calcul suivant :

$$\begin{aligned} \beta(x, y) &= ab(x, y) \\ &= b(ax, y) \\ &= a\lambda\theta^{-1}b(y, x) \\ &= \theta(ab(y, x)) \\ &= \theta(\beta(y, x)). \end{aligned}$$

□