Université de Paris VI 2ème semestre 2007-2008

Master de Mathématiques

GROUPES FINIS

(M 14)

Daniel BERTRAND

.

Plan

1. *Généralités.*
   - Groupes, sous-groupes, quotients.
   - Groupes cycliques, groupes d'unités, groupe symétrique.
   - Groupes opérant sur un ensemble. Produits semi-directs.

2. *Exemples*
   - Quelques groupes classiques.
   - Groupes abéliens finis.
   - Groupes d'isométrie.

3. *Structure des groupes finis*
   - Les théorèmes de Sylow.
   - Groupes nilpotents et résolubles.
   - Extensions de groupes (hors programme).

4. *Représentations linéaires des groupes finis.*
   - G-modules. Produits tensoriels. Lemme de Schur.
   - Théorie des caractères.

Prérequis: notions de base d'algèbre linéaire.

Références

J. Fresnel: *Groupes*; Hermann, Paris, 2001.

J-P. Serre: *Représentations linéaires des groupes finis*; Hermann, Paris 1967.

Le cours est également proposé en télé-enseignement.

.

CHAPITRE I

GÉNÉRALITÉS

§1. Rappels sur les groupes.

Un *groupe* est la donnée d'un ensemble G muni d'une loi de composition interne: $G \times G \to G$ [notée $(x, y) \mapsto xy$] associative [$(xy)z = x(yz)$, qu'on peut donc noter xyz], admettant un élément neutre e [$\forall x \in G, ex = xe = x$], et telle que tout élément de G admette un inverse [$\forall x \in G, \exists y \in G, xy = yx = e$]. L'élément neutre est alors unique, et souvent noté 1; l'inverse de x est unique, et noté x^{-1}.

On dit que deux éléments x, y de G commutent si $xy = yx$, et que le groupe G est abélien (ou commutatif) si c'est le cas pour tout $x, y \in G$; on pourra alors noter la loi de groupe additivement: $(x, y) \mapsto x + y$, élément neutre 0, inverse $-x$.

Le nombre (éventuellement infini) d'éléments de G s'appelle l'*ordre* de G, et est noté $|G|$.

Un *homomorphisme* d'un groupe G vers un groupe G' est une application $f : G \to G'$ telle que $f(xy) = f(x)f(y)$ pour tout $(x, y) \in G \times G$. (Alors $f(e) = e'; f(x^{-1}) = f(x)^{-1}$.) On parle d'endomorphisme si $G = G'$, d'isomorphisme s'il existe un homomorphisme g de G' dans G tel que $f \circ g = id_{G'}, g \circ f = id_G$, d'automorphisme si f est à la fois un endomorphisme et un isomorphisme.

Un *sous-groupe* H de G (notation : $H < G$) est une partie H contenant e , stable sous la loi de groupe de G et sous l'inversion, ou, de façon équivalente, telle que $xy^{-1} \in H$ pour tout $x, y \in H$. Comme une intersection de sous-groupes est un sous-groupe, on peut parler du plus petit sous-groupe $< S >$ de G contenant une partie S de G, qu'on appelle aussi sous-groupe engendré par S. On dit que G est monogène s'il est engendré par un élément, et que G est *cyclique* s'il est monogène et d'ordre fini. .

Soient G un groupe et x un élément de G. L'ordre du sous-groupe $< x >:=< \{x\} >$ engendré par x s'appelle l'ordre de x, et est noté $ord(x)$.

Soient A et B deux parties de G. On note AB (resp. A^{-1}) la *partie* de G formée des éléments de la forme $ab, a \in A, b \in B$ (resp. $a^{-1}, a \in A$). Par exemple, A est un

sous-groupe de G si et seulement si $A.A^{-1} = A$. Si A et B sont des sous-groupes de G, AB est un sous-groupe de G si et seulement si $AB = BA$.

On appelle *classe à gauche modulo* H toute partie de G de la forme $xH := \{xh; h \in H\}$ pour un élément x de G, appelé représentant dans G de la classe en question (chacun de ses éléments en est donc un représentant). Deux classes distinctes sont disjointes. Le nombre, éventuellement infini, d'éléments de l'ensemble G/H des classes à gauche modulo H, qu'on appelle *indice* de H dans G et qu'on note $[G : H]$, vérifie donc la relation :

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

Ainsi, si G est fini, $|H|$ divise $|G|$; en particulier, *l'ordre de tout élément de* G *divise l'ordre de* G.

On définit de même l'ensemble $H \setminus G$ des classes à droite Hx; il a encore $[G : H]$ éléments (considérer l'application $g \mapsto g^{-1}$). On dit que H est *distingué* dans G (ou *normal*; notation: $H \triangleleft G$), si $\forall x \in G, xH = Hx$, i.e. $\forall h \in H, xhx^{-1} \in H$. L'ensemble G/H est alors naturellement muni d'une structure de groupe, appelée *quotient* de G par H , telle que la surjection canonique $\pi : G \to G/H : x \mapsto (x) = xH$ est un homomorphisme de groupes. Rappelons les classiques

Proposition 1: (décomposition canonique d'un homomorphisme) : *Soit* $f : G \to G'$ *un homomorphisme de groupes. Alors :*

i) $Ker(f)$ = *noyau de* $f := \{x \in G : f(x) = e'\}$ *est un sous groupe distingué de* G . *Notons* π *la surjection canonique de* G *sur* $G/Ker(f)$*;*

ii) $Im(f)$ = *image def* $:= \{f(x), x \in G\}$ *est un sous-groupe de* G' . *Notons* i *l'injection canonique de* $Im(f)$ *dans* G' .

iii) il existe un unique isomorphisme $\overline{f}$ *de* $G/Ker(f)$ *sur* $Im(f)$ *tel que* $f = i \circ \overline{f} \circ \pi$.

Proposition 2: *Soient* G *un groupe,* H *un sous-groupe distingué de* G*, et* K *un sous-groupe de* G*. Alors,* $KH = HK$ *est un sous-groupe de* G*,* H *est un sous-groupe distingué de* KH*,* $H \cap K$ *est un sous-groupe distingué de* K*, et l'application* $x \mapsto \pi(x) = xH$ *induit un isomorphisme* $K/K \cap H \simeq KH/H$.

Proposition 3: *Soient* G *un groupe,* H *un sous-groupe distingué de* G*. L'application* $\pi : G \to G/H$ *établit une bijection entre l'ensemble des sous groupes* A *de* G *contenant* H *et l'ensemble des sous-groupes* A/H *de* G/H*, pour laquelle on a* $A \triangleleft G \Leftrightarrow A/H \triangleleft G/H$*; dans ce cas, l'application* $xH \mapsto xA$ *induit un isomorphisme* $(G/H)/(A/H) \simeq G/A$.

Soit I un ensemble, et $\{G_i; i \in I\}$ une collection de groupes. On définit une structure de groupe, appelée *produit (direct)* et notée $\prod_{i \in I} G_i$) sur le produit des ensembles G_i, en

posant $(x_i)_{i\in I}.(y_i)_{i\in I} = (x_i y_i)_{i\in I}$. Si tous les G_i sont égaux à un G , ce groupe, noté G^I (ou G^n si $card(I) = n$ est fini), s'identifie au groupe des applications de I dans G. La notion duale de coproduit fournit, lorsque les G_i sont abéliens, celle de *somme directe*: c'est le le sous-groupe $\oplus_{i\in I} G_i$ de, $\prod_{i\in I} G_i$ formé par les $(x_i)_{i\in I}$ tels que $x_i = e_i$ sauf pour un nombre fini d'indices $i \in I$.

Soit G un groupe. L'ensemble des automorphismes de G, muni de la loi de composition des applications, forme un groupe, noté $Aut(G)$. Pour tout $h \in G$, l'application

$$Int(h) : G \to G; g \mapsto Int(h)(g) := hgh^{-1}$$

est un automorphisme de G, dit *intérieur*. L'application $Int : G \to Aut(G) : h \mapsto Int(h)$ est un homomorphisme de groupes, dont le noyau

$$Z(G) := \{h \in G,\ \forall g \in G, hg = gh\}$$

s'appelle le *centre* de G. L'image $Int(G) \simeq G/Z(G)$ de Int est un sous-groupe distingué de $Aut(G)$, puisque $\forall h \in G, f \in Aut(G), f \circ Int(h) \circ f^{-1} = Int(f(h))$. Les éléments du groupe quotient $Out(G) := Aut(G)/Int(G)$ s'appellent les automorphismes extérieurs de G.

Un sous-groupe H de G est ainsi distingué si $f(H) = H$ pout tout $f \in Int(G)$. On dit que H est *caractéristique* si $f(H) = H$ pour tout $f \in Aut(G)$. Par exemple, le centre de G est un sous-groupe caractéristique. On dit qu'un groupe G est *simple* s'il n'admet pas de sous-groupe distingué propre (i.e. distinct de $\{1\}$ et de G).

§2 Premiers exemples

Groupes cycliques

L'ensemble $\mathbf{Z}$ des entiers rationnels, muni de la loi d'addition, est un groupe abélien, dont tout sous-groupe *non nul* H est de la forme $n\mathbf{Z}$, pour un unique entier rationnel $n > 0$ (effectuer des divisions euclidiennes par le plus petit élément > 0 de H). Le groupe quotient $\mathbf{Z}/n\mathbf{Z}$ des classes de congruence d'entiers rationnels modulo n est alors un groupe cyclique (engendré par exemple par la classe de 1), d'ordre n. Inversément, tout groupe cyclique G d'ordre n est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ (considérer l'homomorphisme $\mathbf{Z} \to G : m \mapsto x^m$, où x est un générateur de G; cf. feuille d'exercices).

Soit n un entier > 0. L'ensemble des classes de congruence modulo n des entiers k premiers à n forme un groupe pour la loi de multiplication. On le note $(\mathbf{Z}/n\mathbf{Z})^*$. D'après le théorème de Bézout ($(k, n) = 1 \Leftrightarrow \exists a, b \in \mathbf{Z}, ak + bn = 1$), il coïncide avec l'ensemble des générateurs du groupe additif $\mathbf{Z}/n\mathbf{Z}$. Son ordre est noté $\phi(n)$ ($\phi :=$ *fonction indicatrice*

d'Euler, avec $\phi(1) = 1$). Pour tout nombre premier p et tout entier $n > 0$, $\phi(p) = p - 1$, $\phi(p^n) = p^{n-1}(p-1)$. On déduit du lemme chinois (voir infra) que $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$ pour tout couple d'entiers m_1, m_2 *premiers entre eux*, de sorte que pour tout entier $n > 0$:

$$\phi(n) = n \prod_{p \text{ premier}, p|n} (1 - \frac{1}{p}).$$

Puisque l'ordre d'un élément divise l'ordre du groupe, on a pour tout entier x premier à n, $x^{\phi(n)} \equiv 1 \pmod{n}$, et en particulier (petit théorème de Fermat):

$$\forall\ p \text{ premier}, \forall\ x \text{ t.q. } p \not| x\ :\ x^{p-1} \equiv 1 \bmod p.$$

Soient G un groupe cyclique, et n son ordre. Alors, tout sous-groupe de G est cyclique (et son ordre divise n). Inversément, pour tout diviseur d de n, G admet un unique sous-groupe (forcément cyclique) d'ordre d. En particulier, un groupe cyclique (ou, plus généralement, un groupe fini et abélien) est simple si et seulement son ordre est un nombre premier. Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique (voir feuille d'exercices).

Groupes d'unités

Un anneau (unitaire) A est un groupe abélien (de loi notée additivement), muni d'une loi de composition interne $A \times A \to A : (x, y) \mapsto xy$ associative, distributive par rapport à la loi $+$, admettant un élément neutre noté 1 . On appelle *unité* de A tout élément x de A tel qu'il existe $y \in A$ vérifiant $xy = yx = 1$ (y est alors unique, et noté x^{-1}). L'ensemble des unités d'un anneau non nul A forme un groupe (pour la loi multiplicative), noté A^*.

Par exemple, le groupe $\mathbf{Z}^*$ des unités de l'anneau $\mathbf{Z}$ est réduit à $\{\pm 1\}$. C'est un groupe cyclique, d'ordre 2. Le groupe des unités de l'anneau $\mathbf{Z}[i]$ est cyclique d'ordre 4. En revanche, le groupe des unités de l'anneau $\mathbf{Z}[\sqrt{2}]$ est infini. Un *corps* est un anneau non nul K tel que $K^* = K \setminus \{0\}$.

Soient K un corps commutatif, n un entier > 0 et $M_n(K)$ l'anneau des matrices carrées d'ordre n à coefficients dans K. Son groupe des unités $(M_n(K))^* := GL_n(K)$ est formé des matrices de déterminant non nul. Plus généralement, pour tout anneau commutatif A, le groupe $GL_n(A)$ des unités de l'anneau $M_n(A)$ des matrices carrées d'ordre n à coefficients dans A est formé des matrices x de déterminant $det(x) \in A^*$. Le quotient de $GL_n(A)$ par le sous-groupe $A^*\mathbf{I}_n$ des matrices scalaires (qui en forme le centre) est noté $PGL_n(A)$. L'application $det : GL_n(A) \to A^*$ est un homomorphisme de groupes, dont on note $SL_n(A) = \{x \in M_n(A), det(x) = 1\}$ le noyau. Par exemple, $SL_n(\mathbf{Z})$ est un

sous-groupe (normal) d'indice 2 de $GL_n(\mathbf{Z})$. On note $PSL_n(A)$ l'image de $SL_n(A)$ dans $PGL_n(A)$.

Le groupe $\mathbf{Z}/n\mathbf{Z}$ est naturellement muni d'une structure d'anneau, dont le groupe des unités est le groupe déja noté $(\mathbf{Z}/n\mathbf{Z})^*$ plus haut. Pour $n = p$ premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps, noté $\mathbf{F}_p$. On montre en théorie des corps que pour toute puissance q d'un nombre premier p, il existe, à isomorphisme près, un unique corps $\mathbf{F}_q$ de cardinal q (par exemple, $\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2 + X + 1)$), et que $\mathbf{F}_q$ est commutatif. Les groupes $L_n(q) := PSL_n(\mathbf{F}_q)$ sont simples (sauf pour $n = 2, q = 2, 3$).

Si A_1 et A_2 sont deux anneaux, on munit (en calculant coordonnée par coordonnée comme pour les groupes) le produit $A_1 \times A_2$ d'une structure d'anneau. On a: $(A_1 \times A_2)^* = (A_1)^* \times (A_2)^*$.

Lemme chinois : *Soient m_1 et m_2 deux entiers > 0 premiers entre eux. Alors, le morphisme naturel d'anneaux $\mathbf{Z}/m_1m_2\mathbf{Z} \to (\mathbf{Z}/m_1\mathbf{Z})\times(\mathbf{Z}/m_2\mathbf{Z})$ est un isomorphisme. En particulier, les groupes d'unités de ces anneaux sont isomorphes, et $\phi(m_1m_2) = \phi(m_1)\phi(m_2)$.*

Groupe symétrique.

Soit X un ensemble. L'ensemble des bijections de X sur lui-même (appelées aussi *permutations* de X) forme un groupe pour la composition des applications: c'est le *groupe symétrique* S_X de X. Si, comme nous le supposons maintenant, X est de cardinal fini n, ou, de façon équivalente, $X = \{1, 2, ..., n\}$, on le note simplement S_n. Il a pour ordre $n!$. Ses éléments généraux se notent $\sigma : \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$.

Un cycle de longueur $k \leq n$ (ou k-cycle) est un élement σ de S_n laissant fixes $n - k$ éléments de X et induisant une permutation circulaire $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ sur les k autres éléments; on note alors $\sigma = (i_1, ..., i_k)$. Deux cycles $(i_1, ..., i_k)$ et $(j_1, ..., j_k)$ coïncident si et seulement s'il existe $t \in \mathbf{N}$ tel que $\forall s, j_s = i_{s+t}$, où les indices s sont lus dans $\mathbf{Z}/k\mathbf{Z}$. Un 2-cycle s'appelle une transposition. Il est clair que tout élément de S_n s'écrit comme produit de transpositions. Par exemple, pour i, j, k distincts: $(ijk) = (k, j)(k, i)$. [Attention à l'ordre: on compose des applications, donc on fait d'abord (k, i), puis (k, j).] On en déduit (voir feuille d'exercices) que tout élément de S_n s'écrit comme produit de transpositions $(1, i), i = 2, ..., n$, ou encore comme produit de transpositions $(i, i + 1), i = 1, ..., n - 1$.

On appelle support d'une permutation σ le complémentaire de l'ensemble des éléments de X laissés fixes par σ. Deux permutations de supports disjoints commutent. On voit aisément que toute permutation s'écrit comme produit de cycles de supports disjoints, et qu'une telle écriture est unique à l'ordre des cycles près.

On appelle *signature* $sgn(\sigma)$ d'un élément σ de S_n le nombre $\Pi_{1\leq i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j} = \pm 1$. On dit que σ est paire (resp. impaire) si sa signature vaut 1 (resp. -1). Par exemple, une transposition est une permutation impaire, un cycle de longueur k a pour signature $(-1)^{k+1}$. L'application $sgn : S_n \to \{\pm 1\}$ est un homomorphisme de groupes. Son noyau, dont les éléments sont donc les permutations paires, s'appelle le *groupe alterné* A_n. Pour $n \geq 2$, c'est un sous-groupe (normal) d'indice 2 de S_n. Les groupes A_n sont simples dès que $n \geq 5$ (voir feuille d'exercices).

§3 Action d'un groupe sur un ensemble.

Soient G un groupe, et X un ensemble. Un action (à gauche) de G sur X est une application $G \times X \to X : (g, x) \mapsto g.x$ (aussi noté simplement gx) telle que pour tout $x \in X, (g, h) \in G \times G$, $g.(h.x) = (gh).x$ et $1.x = x$. La donnée d'une action de G sur X équivaut donc à celle d'un homomorphisme τ de G dans le groupe S_X des permutations de X: poser $\tau(g)(x) = g.x$ et noter que $\tau(g^{-1}) = (\tau(g))^{-1}$. On dit alors que G opère (à gauche) sur X (par τ). On définit de même ce qu'est une action à droite de G sur X: $(g, x) \mapsto xg$, avec la condition $x(gh) = (xg)h$.

Soit G un groupe agissant sur un ensemble X (quand on ne précise pas, cela veut dire "à gauche"). Si A (resp. Y) est une partie de G (resp. X), on note AY l'ensemble des éléments de X de la forme $ay, a \in A, y \in Y$. Pour tout $x \in X$, la partie $G.x := G\,x := G\{x\} = \{gx, g \in G\}$ de X s'appelle l'*orbite* sous G (ou G-orbite) de x. Alors, $G\,x = G\,y$ si et seulement si $y \in G\,x$, et l'ensemble $G \setminus X$ des G-orbites forme un partition de X. Si l'action de G sur X est à droite, on le note X/G.

On dit que G agit *transitivement* sur un ensemble X si $G \setminus X$ n'a qu'un élément. Par exemple, G agit transitivement sur chaque orbite.

Soient x un point de X, et H un sous-groupe de G. On dit que x est fixé par H si $\forall h \in H, hx = x$. On note X^H l'ensemble des points de X fixés par H. Inversément, pour tout $x \in X$, on appelle *stabilisateur* (ou fixateur) de x le sous-groupe $G_x := \{g \in G, gx = x\}$. On dit que G agit *fidèlement* sur X si $\cap_{x\in X} G_x = \{1\}$, c'est-à-dire si l'homomorphisme τ est injectif. Plus généralement, pour toute partie Y de X, le fixateur $Fix_G(Y)$ de Y est le sous-groupe $\cap_{x\in Y} G_x$ de G formé des éléments qui fixent Y point par point. En général, l'ensemble $\{g \in G, gY \subset Y\}$ des éléments de G qui laissent stable Y globalement est seulement un sous-monoïde de G (partie stable par la loi de groupe et contenant 1). Néanmoins, il coïncide souvent (par exemple si Y est fini) avec le sous-groupe $G_Y := \{g \in G, gY = Y\}$ de G, qu'on appelle alors le stabilisateur de Y.

Exemples: soit H un sous-groupe de G. Alors, H agit à gauche sur G par translation:

$(h,g) \mapsto hg$, et une orbite Hg n'est autre qu'une classe à droite modulo H. Les deux notations $H \setminus G$ (§§ 1 et 3) sont donc compatibles. Idem avec G/H, pour l'action de H sur G par translation à droite. Pour chacune de ces actions, le fixateur de tout élément est réduit à $\{1\}$.

l'action (à gauche) $(g,x) \mapsto gxg^{-1}$ de G sur $X = G$ donnée par l'homomorphisme $\tau = Int$ s'appelle l'action par conjugaison de G sur G. Deux éléments de G sont dit conjugués s'ils sont dans une même orbite. Les orbites $C_x := \{gxg^{-1}, g \in G\}$ s'appellent les *classes de conjugaison* (des éléments) de G. L'ensemble des classes de conjugaison de G sera noté $C\ell(G)$, ou encore G/adG; son cardinal $c\ell(G)$ s'appelle le nombre de classes de G. Pour toute partie Y de G, le fixateur $Z_G(Y) = \{g \in G, \forall\, x \in Y, gx = xg\}$ de Y s'appelle le *centralisateur* (ou commutant) de Y (dans G). Le sous-groupe $N_G(Y) = \{g \in G, gY = Yg\}$ s'appelle le *normalisateur* de Y (dans G). Le centralisateur de G lui-même est le centre $Z(G) = Z_G(G)$ de G.

soit $S(G)$ l'ensemble des sous-groupes de G. Pour tout $g \in G, H \in S(G)$, $H' = gHg^{-1}$ est encore un sous-groupe de G, et cela munit $S(G)$ d'une action de G. Deux sous-groupes de G sont dit conjugués s'ils sont dans une même orbite. Les orbites s'appellent les classes de conjugaison de sous-groupes de G. Pour $H \in S(G)$, le fixateur de H n'est autre que son normalisateur $N_H(G)$; c'est le plus grand sous-groupe de G dans lequel H est normal. Par exemple, $H \lhd G \Leftrightarrow N_H(G) = G$..

Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, l'application $g \mapsto gx$ induit une bijection de G/G_x sur $G.x$ (dans laquelle la classe de 1 s'envoie sur x). En particulier,

$$|G.x| = [G : G_x].$$

Si on remplace x par $x' = gx \in G.x$, alors G_x est remplacé par le sous-groupe $G_{x'} = gG_xg^{-1}$, et inversément. Donc la donnée de X où G agit transitivement équivaut à celle de la classe de conjugaison d'un stabilisateur dans G. Par exemple, pour tout corps K, le groupe $G = Aff^1(K)$ des similitudes $x \mapsto ax + b, a \in K^*, b \in K$ de la droite affine $X = \mathbf{A}^1(K)$ agit transitivement sur X; pour tout $x \in X$, le stabilisateur de x est le sous-groupe des homothéties centrées en x, et on peut identifier X à la classe de conjugaison du sous-groupe $GL_1(K) = K^*$ de G.

Soient G un groupe fini agissant sur un ensemble fini X, et $x_1, ..., x_m$ un système de représentants des orbites de X sous G. Autrement dit, m est le cardinal de $G \setminus X$, et

$X = \cup_{i=1,...m} Gx_i$ (réunion disjointe). Donc $|X| = \Sigma_{i=1,...,m}[G : G_{x_i}] = \Sigma_{i=1,...,m} \frac{|G|}{|G_{x_i}|}$ et

$$\frac{|X|}{|G|} = \sum_{i=1}^{m} \frac{1}{|G_{x_i}|}.$$

Appliquons cette "*formule des classes*" à l'action de G sur lui-même par conjugaison. Dans ce cas, $m = c\ell(G)$ est le nombre de classes de conjugaison de G, chaque G_{x_i} est le centralisateur $Z_G(x_i)$ de x_i dans G (par exemple, la classe de $x_1 = 1$, qui est réduite à un élément, vérifie $Z_G(1) = G$), et on obtient

$$1 = \sum_{i=1}^{c\ell(G)} \frac{1}{|Z_G(x_i)|}.$$

Produits semi-directs

Soient A et C deux groupes. On dit qu'une action (à gauche) de C sur A est compatible avec la structure de groupe de A si l'homomorphisme correspondant $\tau : C \to S_A$ est à valeurs dans $Aut(A)$, autrement dit, en notant ${}^c a = \tau(c)(a)$ cette action, si ${}^c(a_1 a_2) = {}^c a_1 . {}^c a_2$ pour tous c, a_1, a_2. Dans ces conditions, on appelle

produit semi-direct de C par A relativement à $\tau : C \to Aut(A)$,

et on note $A \times_\tau C$, l'ensemble $A \times C$, muni de la loi de composition interne

$$(a, c), (a', c') \to (a.{}^c a', c.c'),$$

qui en fait un groupe, d'élement neutre $(1, 1)$ (avec $(a, c)^{-1} = ({}^{c^{-1}} a^{-1}, c^{-1})$).

Les applications $i : A \to A \times_\tau C : i(a) = (a, 1)$ et $s : C \to A \times_\tau C : s(c) = (1, c)$ sont alors des homomorphismes de groupes injectifs, qui permettent d'identifier A et C à des sous-groupes de $A \times_\tau C$. Avec cette identification, A est normal dans G, et l'action de G sur A par conjugaison induit précisément τ sur C : ${}^c a = cac^{-1}$. En revanche, C n'est en général pas normal dans G: il l'est si et seulement si l'action est triviale ($\tau = id_A$), auquel cas le produit semi-direct n'est autre que le produit direct $A \times C$ des groupes A et C. L'application $\phi : A \times C \to A \times_\tau C : (a, c) \mapsto ac$ (c-à-d. $i(a)s(c)$) est toujours une bijection ensembliste, mais n'est un isomorphisme de groupes que si τ est triviale.

Inversement, soient G un groupe, et H, K deux sous-groupes de G tels que l'application $\phi : H \times K \to G : (h, k) \mapsto hk$ soit une bijection ensembliste. Cela entraîne en particulier que $H \cap K = \{1\}$, et pour G fini, cela équivaut à la conjonction de cette condition et de la relation $|G| = |H|.|K|$. Si H et K commutent, c'est-à-dire si $kh = hk$ pour tout

$(h,k) \in H \times K$, l'application ϕ est un isomorphisme de groupes (pour la loi de produit sur $H \times K$), et G est le produit direct de H et K.

Les sous-groupes H et K commutent si et seulement si K est contenu dans le centralisateur $Z_G(H)$ de H. Supposons maintenant seulement que K soit contenu dans le normalisateur $N_G(H)$ de H (comme $HK = G$, cela équivaut à demander que H soit normal dans G). Alors, K agit sur H par conjugaison: $(k,h) \mapsto \tau(k)(h) := khk^{-1}$, et G est isomorphe au produit semi-direct $H \times_\tau K$ de K par H relativement à $\tau = (Int_{|K})_{|H}$. (Voir aussi chap. III, Prop. 3.ii.)

Voici deux exemples standard: avec les notations du §2, le sous-groupe triangulaire supérieur B de $GL_n(k)$ est produit semi-direct du sous-groupe $D \simeq (k^*)^n$ (formé des matrices diagonales) par le sous-groupe triangulaire supérieur strict S (l'action de D sur S est donnée par la conjugaison dans $GL_n(k)$). Avec les notations du chap. I, §2, le groupe $Aff^1(k)$ est produit semi-direct du sous-groupe multiplicatif $\simeq k^*$ formé des homothéties centrées en 0, par le sous-groupe additif $\simeq k$ formé des translations (l'action de k^* sur k par conjugaison dans $Aff^1(k)$ est simplement donnée par la multiplication).

Exercices:

1. Soient p un nombre premier, m un entier > 0 et G un groupe d'ordre p^m (voir chap. IV). Alors, p divise $|Z(G)|$. (Noter que pour tout x_i central, la classe de x_i est réduite à un élément, et que $Z_G(x_j)$ divise p^{m-1} si x_j n'est pas central.)

2. Soient p un nombre premier, et G un groupe d'ordre p^2. Montrer que $G \simeq (\mathbf{Z}/p\mathbf{Z})^2$ ou que $G \simeq \mathbf{Z}/p^2\mathbf{Z}$. Montrer qu'en revanche, il existe des groupes d'ordre p^3 non abéliens.

3. Soient K un corps et n un entier ≥ 1. On note $\mathbf{P}_n(K)$ l'ensemble des orbites de $X := K^{n+1} - \{0\}$ sous l'action du groupe K^* par homothéties $((\lambda, x) \in K^* \times X \mapsto \lambda x \in X)$. De l'action naturelle de $GL_{n+1}(K)$ sur K^{n+1}, on déduit par passage au quotient une action de $PGL_{n+1}(K)$ sur $\mathbf{P}_n(K)$. On a les isomorphismes (voir feuille d'exercices):

$PGL_2(\mathbf{F}_2) \simeq S_3, PGL_2(\mathbf{F}_3) \simeq S_4, PGL_2(\mathbf{F}_5) \simeq S_5$;

$PSL_2(\mathbf{F}_3) \simeq A_4, PSL_2(\mathbf{F}_5) \simeq A_5$.

(Noter d'ailleurs que $SL_2(\mathbf{F}_2) = PSL_2(\mathbf{F}_2) = GL_2(\mathbf{F}_2) = PGL_2(\mathbf{F}_2)$, et que $SL_2(\mathbf{F}_4) = PSL_2(\mathbf{F}_4)$ est aussi isomorphe à A_5.)

4. Pour tout entier $n \geq 1$, on note $p(n)$ (p = *fonction de partitions*) le nombre d'écritures de n comme somme $k_1 + ... + k_m$ d'entiers $k_i > 0$ (aux permutations des k_i près). Ainsi, $\Pi_{k \geq 1} \frac{1}{(1-x^k)} = 1 + \Sigma_{n \geq 1} p(n) x^n$. Alors, $c\ell(S_n) = p(n)$. (Associer à la partition $k_1 + ... + k_m$ la classe de conjugaison du produit de cycles disjoints de longueurs $k_1, ..., k_m$.)

5. Le groupe symétrique S_n agit sur l'anneau $X_n = \mathbf{C}[x_1, ..., x_n]$ des polynômes en n variables par la loi $(\sigma.P)(x_1, ..., x_n) = P(x_{\sigma(1)}, ..., x_{\sigma(n)})$. L'ensemble $(X_n)^{S_n}$ des polynômes invariants sous l'action de S_n (qu'on appelle "polynômes symétriques") est le sous-anneau $Y_n = \mathbf{C}[s_1, ..., s_n]$ engendré par les polynômes symétriques élémentaires, définis par l'identité $\Pi_{i=1,..,n}(T - x_i) = T^n - s_1 T^{n-1} + ... + (-1)^n s_n$, i.e. $s_1 = x_1 + ..., +x_n, ..., s_n = x_1 ... x_n$. Le sous-groupe A_n est le fixateur du polynôme $\delta = \Pi_{1 \leq i < j \leq n}(x_i - x_j)$.

6. La plupart des groupes sont définis à partir d'une action sur un ensemble, et leurs sous-groupes "classiques" comme stabilisateurs de parties remarquables. Ainsi, le sous-groupe $O_n(\mathbf{R})$ de $G = GL_n(\mathbf{R})$ formé par les matrices orthogonales réelles est le groupe G_Y associé à la sphère unité $Y = \mathbf{S}^{n-1}$ de $\mathbf{R}^n$. Son sous-groupe $SO_n(\mathbf{R}) = O_n(\mathbf{R}) \cap SL_n(\mathbf{R})$ est le groupe des rotations de $\mathbf{R}^n$. Le groupe fini S_4 (resp. A_4) est isomorphe au sous-groupe de $O_3(\mathbf{R})$ (resp. de $SO_3(\mathbf{R})$ formé des isométries (resp. des rotations) laissant stable un tétraèdre régulier de centre de gravité placé en l'origine (voir chap. II).

CHAPITRE II

EXEMPLES

§1. Quelques groupes classiques.

Outre les exemples déjà rencontrés au chapitre I, comme les groupes cycliques $C_n = \mathbf{Z}/n\mathbf{Z}$, les groupes symétriques et alternés S_n, A_n, et quelques sous-quotients du groupe de matrices $GL_n(k)$, on peut citer:

les groupes diédraux: soit n un entier ≥ 2. Le groupe diédral D_n est le stabilisateur dans $O_2(\mathbf{R})$ d'un polygone régulier à n sommets (un segment si $n = 2$), centré à l'origine. Son intersection avec $SO_2(\mathbf{R})$ est le groupe cyclique C_n d'ordre n engendré par la rotation r d'angle $2\pi/n$. L'indice de ce sous-groupe divise $[O_2(\mathbf{R}) : SO_2(\mathbf{R})] = 2$, et vaut 2 puisque D_n contient l'une quelconque, soit s, des symétries par rapport aux droites joignant l'origine à un sommet. On a

$$r^n = 1, s^2 = 1, srs = srs^{-1} = r^{-1},$$

d'où $sr^{-k}s = r^k$ pour tout entier k. Ainsi, D_n est un groupe d'ordre $2n$, isomorphe au produit semi-direct $C_n \times_\tau \{\pm 1\}$, pour l'action de $\{\pm 1\}$ sur C_n donnée par $\tau(-1)(a) := a^{-1}$. Les éléments d'ordre 2 de D_n sont les n symétries sr^k, ainsi que, pour n pair, la rotation $r^{n/2}$. Pour $n = 2$, le produit est direct, et le groupe D_2, isomorphe à $C_2 \times C_2$, est souvent noté $\mathbf{V}$ (Vierergruppe; il apparaît comme sous-groupe distingué d'indice 3 de A_4, qui est donc résoluble). Le groupe D_3 est isomorphe au groupe symétrique S_3.

le groupe quaternionien: considérons le corps des quaternions de Hamilton $\mathbf{H} = \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$, dont la loi de multiplication est définie par $\mathbf{R}$-bilinéarité à partir des relations $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$ (on vérifie qu'elle est bien associative). Le groupe quaternionien H_8 est le sous groupe

$$H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

du groupe multiplicatif $\mathbf{H}^*$. Il est d'ordre 8, admet exatement trois sous-groupes cycliques $< i >, < j >, < k >$ d'ordre 4 (contrairement au groupe diédral D_4, qui n'en admet qu'un)

et un seul élément d'ordre 2 (alors que D_4 en a 5). L'injection de C_4 dans H_8 définie par l'élément i munit H_8 d'une structure d'extension de C_2 par C_4. Cette extension n'est pas scindée, puisque le seul élément de H_8 d'ordre 2 est -1. L'injection de ± 1 dans H_8 munit également H_8 d'une structure d'extension (centrale, et non scindée) de $\mathbf{V}$ par C_2.

Remarque: voici une façon commode (mais d'un usage subtil) pour décrire les groupes, et plus particulièrement les groupes finis. À tout ensemble non vide X, on associe formellement un ensemble $X^{-1} = \{x^{-1}, x \in X\}$, et on appelle *groupe libre* sur X l'ensemble $F(X)$ des mots construits sur l'alphabet $X \cup X^{-1}$, où on convient de supprimer les couples de lettres adjacentes du type xx^{-1} et $x^{-1}x, x \in X$, et que l'on munit de la loi de groupe définie par concaténation des mots: l'élément neutre est le mot vide, noté 1; pour $x \in X$, l'inverse de x (resp. x^{-1}) est x^{-1} (resp. x), l'inverse d'un mot quelconque $y_1...y_n$ (avec $y_i \in X \cup X^{-1}$ pour tout i) est $y_n^{-1}...y_1^{-1}$. Pour tout groupe G et toute application ϕ de X dans G, il existe alors un unique homomorphisme de groupes $F_\phi : F(X) \to G$ tel que $F_\phi(x) = \phi(x)$ pour tout $x \in X$. En particulier, si S est une partie de G telle que $< S >= G$, il existe un unique homomophisme surjectif $\pi : F(S) \to G$ induisant l'identité sur S, et G est isomorphe à $F(S)/Ker(\pi)$. Soit de plus R une partie de $Ker(\pi)$ telle que le plus petit sous-groupe *distingué* de $F(X)$ contenant R soit $Ker(\pi)$. Alors G est à isomorphisme près entièrement déterminé par S et R. On dit dans ces conditions que $(S \mid R)$ est une présentation de G, d'ensemble générateur S, d'ensemble de relations R. Par exemple, $(\{a\} \mid \{a^n\})$ est une présentation de C_n; $(\{a, b\} \mid \{a^n, b^2, abab\})$ est une présentation de D_n; $(\{a, b\} \mid \{a^4, a^2b^2, ab^{-1}ab\})$ est une présentation de H_8.

Le groupe modulaire: c'est le sous-groupe d'ordre infini $PSL_2(\mathbf{Z}) = SL_2(\mathbf{Z})/\{\pm \mathbf{1}_2\}$ de $PSL_2(\mathbf{R})$. Le groupe $SL_2(\mathbf{Z})$ est engendré par les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (d'ordre 4) et $U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ (d'ordre 6). Le groupe $PSL_2(\mathbf{Z})$ admet pour présentation $(\{a, b\} \mid \{a^2, b^3\})$.

Groupes n-transitifs: soient E un ensemble, n un entier $\leq card(E)$, et G un sous-groupe du groupe symétrique S_E. On dit que G est n-transitif (ou mieux: agit n fois transitivement sur E) si pour tout couple de parties $\{x_1, ..., x_n\}, \{y_1, ..., y_n\}$ de E à n éléments, il existe un élément g de G tel que $g.x_i = y_i$ pour tout $i = 1, ..., n$. Par définition, G est $1-$transitif si l'action de G sur E est transitive. Le groupe S_n est n-transitif, donc A_n est $(n-2)$-transitif (si $n \geq 3$). Pour tout corps k, le groupe $PGL_2(k)$ (resp. $PSL_2(k)$) agit 3 fois (resp. 2 fois) transitivement sur $\mathbf{P}_1(k)$. Et $PGL_2(k)$ n'est pas 4-transitif (si $k \neq \mathbf{F}_3$), puisque le *birapport* $(x_1 : x_2 : x_3 : x_4) := \frac{x_3 - x_1}{x_3 - x_2} : \frac{x_4 - x_1}{x_4 - x_2}$ d'un quadruplet est invariant sous son action, et que $(\infty : 0 : 1 : x) = x$. Hors de A_n, S_n eux-mêmes, on connait peu de groupes 4 ou 5 -transitifs (groupes de Mathieu), et on conjecture qu'aucun n'est 6-transitif.

Passons à quelques nouveaux groupes de type matriciel.

Groupes symplectiques et orthogonaux: soient k un corps commutatif, n un entier > 0, et $J = \begin{pmatrix} 0_n & \mathbf{1}_n \\ -\mathbf{1}_n & 0_n \end{pmatrix}$ la matrice carrée d'ordre $2n$ représentant la forme bilinéaire alternée sur l'espace vectoriel k^{2n} : $(\underline{x}, \underline{y}) \mapsto \Sigma_{i=1,..,n} x_i y_{n+i} - x_{n+i} y_i$. Le groupe symplectique est le groupe $Sp_{2n}(k) = \{P \in GL_{2n}(k), {}^t PJP = J\}$. Ainsi, $Sp_2(k) = SL_2(k)$. Plus généralement, on démontre que le déterminant d'une matrice symplectique vaut toujours 1, de sorte que pour tout n, $Sp_{2n}(k)$ est un sous-groupe de $SL_{2n}(k)$.

Le groupe orthogonal est le groupe $O_n(k) = \{P \in GL_n(k), {}^t P.P = \mathbf{1}_n\}$. Ses éléments représentent les "transformations orthogonales" de l'espace k^n, muni de la forme bilinéaire symétrique $(\underline{x}, \underline{y}) \mapsto \Sigma_{i=1,..,n} x_i y_i$). Son intersection avec $SL_n(k)$ est notée $SO_n(k)$.

Groupes unitaires: soit k un corps commutatif muni d'une involution non triviale $x \mapsto \overline{x}$ (exemple: $k = \mathbf{C}, {}^- =$ la conjugaison complexe; ou encore: $k = \mathbf{F}_{p^2}, {}^- =$ le Frobenius $x \mapsto x^p$). Pour tout entier $n > 0$, le groupe unitaire $U_n(k)$ est le sous-groupe de $GL_n(k)$ formé des matrices P telles que ${}^t\overline{P}.P = \mathbf{1}_n$. Son intersection avec $SL_n(k)$ est notée $SU_n(k)$.

Soient $\mathbf{H}$ le corps des quaternions de Hamilton, σ l'anti-involution de $\mathbf{H}$ définie par $\sigma(x + yi + zj + tk) = x - yi - zj - tk$, de sorte que $||u|| := \sqrt{\sigma(u).u}$ définit une structure euclidienne sur $\mathbf{H}$, et U le sous-groupe du groupe multiplicatif $\mathbf{H}^*$ formé par les quaternions de norme 1. On peut voir $\mathbf{H} = \mathbf{C} \oplus \mathbf{C}j \simeq \mathbf{C}^2$ comme un $\mathbf{C}$-espace vectoriel de dimension 2 , et $||.||$ comme un produit hermitien. Alors, l'application $\rho : U \to GL_2(\mathbf{C})$ qui attache à $u \in U$ l'automorphisme $\mathbf{C}$-linéaire de $\mathbf{H} : h \to \rho(u)(h) := hu^{-1}$ est un homomorphisme de groupes injectif. Comme $||hu|| = ||h||.||u|| = ||h||$ pour tout $h \in \mathbf{H}$, son image est contenue dans $U_2(\mathbf{C})$. En fait, pour $u^{-1} = \alpha + \beta j \in \mathbf{C} \oplus \mathbf{C}j$ de norme $\alpha\overline{\alpha} + \beta\overline{\beta} = 1$, la matrice représentative de $\rho(u)$ dans la base $\{1, j\}$ de $\mathbf{H}$ est donnée par $\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix}^{-1}$, de sorte que ρ établit un isomorphisme de U sur $SU_2(\mathbf{C})$.

L'espace $\mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$ des quaternions purs, muni de $||.||$, s'identifie à l'espace euclidien usuel $\mathbf{R}^3$. Pour tout $u \in U$, l'application $Int(u) : h \mapsto uhu^{-1}$ de $\mathbf{H}$ induit une isométrie de $\mathbf{R}^3$, d'où un homomorphisme de groupe $\pi : U \to SO_3(\mathbf{R})$, appliquant u sur $\pi(u) = (Int(u))|_{\mathbf{R}^3}$, de noyau $U \cap Z(\mathbf{H}^*) = \{\pm 1\}$. On peut montrer que π est surjective, de sorte que $SO_3(\mathbf{R}) \simeq SU_2(\mathbf{C})/\{\pm \mathbf{1}_2\}$ [(*)].

Groupes de réflexions: soit G un sous-groupe *fini* de $GL_n(\mathbf{C})$. On verra au chapitre 3 que chacun de ses éléments est diagonalisable, et que G est conjugué à un sous-groupe du groupe unitaire $U_n(\mathbf{C})$. On dit que G est un groupe de réflexions s'il est engendré par des

[(*)] Plus généralement, pour tout $n \geq 3$, le groupe $SO_n(\mathbf{R})$ admet un revêtement simplement connexe de degré 2: le groupe spinoriel $Spin_n\mathbf{R}$ (voir cours "Algèbres de Lie").

réflexions, i.e. des matrices P ayant $n-1$ valeurs propres égale à 1 (la dernière est alors une racine de l'unité). On dit qu'un groupe de réflexions G est un groupe de Coxeter s'il est conjugué à un sous-groupe de $GL_n(\mathbf{R})$ (on montre que c'est le cas si et seulement si G est conjugué à un sous-groupe de reflexions de $O_n(\mathbf{C})$; les générateurs de G sont alors des symétries hyperplanes).

§2 Groupes abéliens finis.

Un produit (direct) de groupes cycliques, ou plus généralement abéliens, est évidemment abélien. La réciproque est vraie: tout groupe abélien fini est isomorphe à un produit de groupes cycliques. Plus précisément:

Théorème et définition: *soit G un groupe abélien fini $\neq \{0\}$. Il existe une unique famille d'entiers $a_1, ..., a_s \geq 2$, vérifiant les propriétés suivantes:*

i) pour tout $i = 1, ..., s-1$, a_i divise a_{i+1};

ii) G est isomorphe au produit $(\mathbf{Z}/a_1\mathbf{Z}) \times ... \times (\mathbf{Z}/a_s\mathbf{Z})$.

On appelle ces entiers a_i les facteurs invariants *de G.*

La preuve directe qui suit repose sur le lemme suivant, où l'*exposant* du groupe fini G désigne le ppcm des ordres de ses éléments ; de façon équivalente, le pgcd des entiers n (ou encore : le plus petit des entiers $n \geq 1$) tels que $\forall x \in G, nx = 0$.

Lemme: *Soient G un groupe abélien fini, et r l'exposant de G. Alors, G possède un élément d'ordre r.*

Preuve: il suffit par induction de montrer que si x et y sont deux éléments de G d'ordres respectifs n et m, il existe un élément de G d'ordre $r = ppcm(n, m)$. En décomposant n et m en produit de puissances de nombres premiers, on voit qu'ils admettent des diviseurs n', m' premiers entre eux tels que $n'm' = r$. Alors, $x' = \frac{n}{n'}x$ est d'ordre n', $y' = \frac{m}{m'}y$ est d'ordre m', et $x'y'$ est d'ordre $ppcm(n', m') = r$.

Existence des a_i (par récurrence sur $|G|$). Soient a_s l'exposant de G, x_s un élément de G d'ordre a_s, et G' le groupe quotient $G/ < x_s >$. D'après l'hypothèse de récurrence, il existe des entiers $a_1, ..., a_{s-1}$ se divisant successivement, et des éléments $x'_1, ..., x'_{s-1}$ de G' d'ordres respectifs $a_1, ..., a_{s-1}$, tels que $G' =< x'_1 > \times ... \times < x'_{s-1} >$; noter que a_{s-1} est l'exposant de G', qui divise l'exposant a_s de G. Montrons que pour tout $i = 1, ..., s-1$, il existe un élément x_i de G d'ordre a_i dont l'image dans G' soit x'_i. Soit y_i un représentant de x'_i dans G. Alors, $a_i y_i \in < x_s >$, et il existe un entier k_i tel que $a_i y_i = k_i x_s$. Je dis que a_i divise k_i, et que $x_i := y_i - \frac{k_i}{a_i}x_s$ répond à la question. En effet, $0 = a_s y_i = \frac{a_s}{a_i}a_i y_i = (\frac{a_s}{a_i}k_i)x_s$,

donc a_s divise $\frac{a_s}{a_i}k_i$ et $a_i|k_i$. Alors, $a_i(y_i - \frac{k_i}{a_i}x_s) = 0$, donc l'ordre de x_i divise a_i, et lui est égal puisque l'image x'_i de x_i dans G' est déjà d'ordre a_i.

Dans ces conditions, le sous-groupe $H =< x_1 > \times ... \times < x_{s-1} >$ de G ne rencontre $K =< x_s >$ qu'en 0 ($n_1x_1 + ... + n_{s-1}x_{s-1} = n_sx_s \Rightarrow n_1x'_1 + ... + n_{s-1}x'_{s-1} = 0 \Rightarrow a_1|n_1, ..., a_{s-1}|n_{s-1} \Rightarrow n_1x_1 = ... = n_{s-1}x_{s-1} = 0$), et $|G| = |G'|.|K| = |H|.|K|$. Le groupe abélien G est donc produit direct de H et K, d'où la décomposition recherchée.

Unicité des a_i. Le plus grand facteur invariant étant l'exposant de G, son unicité est claire, mais c'est par celle de a_1 (et de s) qu'on va débuter. Pour tout entier d, posons $\Phi(d) = card\{x \in G, dx = 0\}) = \prod_{i=1,...,s}(pgcd(d, a_i)) \leq d^s$. Alors, s est le plus petit des entiers k tels que $\Phi(d) \leq d^k$ pour tout $d \geq 1$, et ne dépend donc que de G. De plus, a_1 est le plus grand des entiers d tels que $\Phi(d) \geq d^s$, et ne dépend donc que de G.

On conclut par une récurrence sur $|G|$: soit $G[a_1]$ le sous-groupe de G formé des éléments d'ordre divisant a_1. Pour tout $i \geq 1$, $(\mathbf{Z}/a_i\mathbf{Z})[a_1] = \frac{a_i}{a_1}\mathbf{Z}/a_i\mathbf{Z}$, donc $G/G[a_1]$ admet pour facteurs invariants $(\frac{a_2}{a_1}, ..., \frac{a_s}{a_1})$. L'hypothèse de récurrence entraîne qu'ils ne dépendent que de G. Il en est donc de même des facteurs invariants $(a_1, ..., a_s)$ de G.

Comme il est bien connu, les sous-groupes discrets de $\mathbf{R}$ sont de la forme $\mathbf{Z}u$, où u est un élément (éventuellement nul) de $\mathbf{R}$. Nous aurons besoin d'une description similaire en dimension 2.

Proposition et définition: *soit G un sous-groupe discret de $\mathbf{R}^2$. Alors, ou bien $G = \{0\}$, ou bien il existe un élément non nul u de $\mathbf{R}^2$ tel que $G = \mathbf{Z}u$, ou bien il existe deux éléments u_1 et u_2 de $\mathbf{R}^2$, linéairement indépendants sur $\mathbf{R}$, tels que $G = \mathbf{Z}u_1 \oplus \mathbf{Z}u_2$; dans ce dernier cas, on dit que G est un* réseau *de $\mathbf{R}^2$.*

Démonstration: si G est contenu dans une droite, il s'identifie à un sous-groupe de $\mathbf{R}$, et est donc de la forme $\mathbf{Z}u$. Sinon, soit u_1 un des éléments non nuls de norme minimale de G, de sorte que $G \cap \mathbf{R}u_1 = \mathbf{Z}u_1$, et soit u_2 un des éléments de G, non contenu dans cette droite, de norme minimale. (L'existence de u_2, comme celle de u_1, résulte de la discrétion de G, en vertu de laquelle G ne possède qu'un nombre fini d'éléments de norme bornée.) Au signe près, l'angle (u_1, u_2) est alors compris entre $\pi/3$ et $2\pi/3$. Montrons que le sous-groupe G' engendré par u_1 et u_2 coïncide avec G. En effet, tout élément g de G est congru modulo G' à un élément de G de la forme $u = xu_1 + yu_2$, où x et y sont deux nombres réels compris entre $-1/2$ et $1/2$. Alors, $||u||^2 \leq \frac{1}{4}(||u_1||^2 + ||u_1||.||u_2|| + ||u_2||^2) \leq \frac{3}{4}||u_2||^2$, donc $u \in \mathbf{Z}u_1$ par définition de u_2, donc $u = 0$, et $g \in G'$.

[On montre, de façon générale, que tout sous groupe discret de $\mathbf{R}^n$ est engendré sur $\mathbf{Z}$ par un famille $\mathbf{R}$-libre de $m \leq n$ vecteurs de $\mathbf{R}^n$.]

§3 Groupes d'isométries.

Pavages du plan.

Commençons par quelques rappels de géométrie euclidienne. Soient E un espace affine euclidien orienté, V l'espace vectoriel euclidien orienté sous-jacent, $O(V)$ le groupe des transformations orthogonales de V, $SO(V)$, également noté $O^+(V)$, le sous-groupe des rotations de V, et $T(V) = \{t_v, v \in V\}$ le groupe des translations sur E (qui est isomorphe au groupe additif sous-jacent à V). Le groupe $O(V)$ agit naturellement sur V, et cela définit une action τ de $\overline{f} \in O(V)$ sur $t_v \in T(V) : \tau(\overline{f})(t_v) := t_{\overline{f}(v)}$. On appelle *isométrie* de E toute bijection de E sur lui-même préservant les distances. Elles forment un groupe $Isom(E)$, admettant $T(V)$ comme sous-groupe distingué: plus précisément, pour tout $f \in Isom(E)$ il existe un unique élément $\overline{f}$ de $O(V)$ tel que pour tout $w \in V$, $ft_wf^{-1} = t_{\overline{f}(w)}$, et l'application $\{f \in Isom(E)\} \mapsto \{\overline{f} \in O(V)\}$ est un homomorphisme surjectif, de noyau $T(V)$. Ainsi, $Isom(E)$ est le *produit semi-direct* de $O(V)$ par $T(V)$ relativement à l'action τ de $O(V)$ sur $T(V)$. De même, les déplacements (= isométries préservant l'orientation) forment un sous-groupe $Isom^+(E) \simeq T(V) \times_\tau SO(V)$, d'indice 2 dans $Isom(E)$. Si E est un plan, tout élément f de $Isom^+(E)$ n'appartenant pas à $T(V)$ admet un unique point fixe a_f, et est une rotation de centre a_f.

Le groupe $Isom^+(E)$ agit naturellement sur l'ensemble des parties de E. Un *pavage* (direct) de E est la donnée d'un sous-groupe G de $Isom^+(E)$ et d'une partie compacte connexe P de E, dont l'intérieur P^o admette P pour adhérence, tels que l'orbite $G.P$ de P sous G soit un recouvrement de E et que l'orbite $G.P^o$ de P^o soit constituée de parties de E disjointes (ou confondues). Admettant que pour tout point x de E, l'orbite $G.x$ de x est alors discrète dans E, nous allons montrer que quand E est un *plan*, un tel groupe G vérifie les propriétés suivantes:

i) l'intersection $T(L)$ de G avec $T(V)$ est formée par les translations associées aux éléments d'un *réseau* L de $V \simeq \mathbf{R}^2$ (pour la notion de réseau, voir le chapitre 5);

ii) l'image $\overline{G} = G/T(L)$ de G dans $SO(V) \simeq SO_2(\mathbf{R})$ est un groupe fini d'ordre $n = 1$, 2, 3, 4, ou 6. Comme $SO_2(\mathbf{R})$ est isomorphe au sous-groupe $\{z \in \mathbf{C}^*, |z| = 1\}$ du groupe multiplicatif du corps $\mathbf{C}$, il revient au même de dire que $\overline{G}$ est un groupe cyclique d'ordre $n \leq 6, n \neq 5$ (engendré par la rotation d'angle $2\pi/n$). Ainsi:

tout groupe de pavage (direct) du plan euclidien est isomorphe à $\mathbf{Z}^2 \times_\tau C_n$, *où* $n = 1, 2, 3, 4$ *ou* 6. On montre d'ailleurs que chacun de ces 5 groupes donne bien naissance à un pavage, cf. M. Berger, *Géométrie*, tome 1.

Démonstration: i) L'intersection de G avec $T(V)$ est de la forme $T(L)$, où L est un sous-groupe de V, nécessairement discret, puisque l'orbite sous G de tout point est discrète.

D'après la proposition précédente, il suffit donc de montrer que L contient deux éléments linéairement indépendants sur $\mathbf{Z}$. Dans le cas contraire, $L = \{0\}$ ou $\mathbf{Z}v$. Si $L = \{0\}$, tout élément g de G aurait un point fixe a_g. Si deux éléments g, g' de G avaient deux points fixes distincts, leur commutateur serait une translation non nulle, donc G est formé de rotations autour d'un même point. L'orbite $G.P$ du pavé P est donc bornée, contradiction. Si $L = \mathbf{Z}v$, $\overline{g}(v)$ appartient à L pour tout $g \in G$, donc tous les points fixes $a_g, g \in G - L$ sont situés sur une même droite, de direction v. L'orbite $G.P$ de P est alors contenue dans une bande de largeur bornée de E, contradiction.

ii) La relation $ft_w f^{-1} = t_{\overline{f}(w)}$ et la discrétion montre que les éléments de $\overline{G}$ sont d'ordre fini, et il s'agit de borner ces ordres. Si tous sont d'ordre ≤ 2, $\overline{G}$ est trivial ou engendré par la symétrie de centre 0. S'il a un élément d'ordre $n \geq 3$, G contient une rotation g de E, d'angle $2\pi/n$. Soit h un élément de $G - L$ et de point fixe a_h aussi proche que possible du centre a_g de g; quitte à en considérer une puissance, on peut supposer que l'angle de h est $2\pi/m$ avec m entier ≥ 2. Alors, $k = (gh)^{-1} \in G$ est une rotation d'angle $2\pi\frac{s}{r}, r, s \in \mathbf{N}, (r, s) = 1$, de centre a_k donné par la géométrie élémentaire, et comme la rotation k_0 de centre a_k et d'angle $2\pi/r$ appartient encore à G, la minimalité de $|a_g a_h|$ montre que nécessairement, $k = k_0$. La somme des angles du triangle $a_g a_h a_k$ valant π, on a finalement $\frac{1}{n} + \frac{1}{m} + \frac{1}{r} = 1$, où $n \geq 3, m \geq 2, r \geq 2$ sont des entiers. Cette équation impose à chaque n, m, r d'être ≤ 6, et différent de 5. Ainsi, $\overline{G}$ est un groupe fini, donc cyclique, d'ordre $1, 2, 3, 4$, ou 6.

[La fin de ce chapitre est hors programme.]

Pavages de la sphère

La sphère unité $\mathbf{S}^2$, d'équation $x^2 + y^2 + z^2 = 1$, hérite de son espace ambiant $\mathbf{R}^3$ une métrique $ds^2 = dx^2 + dy^2 + dz^2$ (en coordonnées sphériques: $ds^2 = d\theta^2 + cos^2\theta d\phi^2$), et les transformations orthogonales de $\mathbf{R}^3$ induisent sur $\mathbf{S}^2$ des bijections préservant cette métrique. En fait (voir cours " Géométrie différentielle"), le groupe des isométries de $\mathbf{S}^2$ s'identifie à $O_3(\mathbf{R})$. Comme $\mathbf{S}^2$ est compacte, les groupes de pavages (directs) de la sphère sont des sous-groupes finis de $SO_3(\mathbf{R})$, pour lesquels on a:

tout sous-groupe fini de $SO_3(\mathbf{R})$ est isomorphe au groupe cyclique C_n ou au groupe diédral D_n, avec n entier arbitraire, ou à l'un des groupes A_4, S_4, A_5. (Et tous sont effectivement atteints.) La finitude des solutions de l'inéquation $\frac{1}{n} + \frac{1}{m} + \frac{1}{r} > 1, n, m > 2$ joue un rôle clef dans la preuve; elle reflète le fait qu'en géométrie sphérique, la somme des angles d'un triangle est $> \pi$.

L'isomorphisme $SU_2(\mathbf{C})/\{\pm \mathbf{1}_2\} \simeq SO_3(\mathbf{R})$ du §1 permet d'en déduire la liste des sous-groupes finis de $SU_2(\mathbf{C})$, donc aussi de $GL_2(\mathbf{C})$, puisque tout sous-groupe fini de $GL_2(\mathbf{C})$ est conjugué à un sous-groupe de $SU_2(\mathbf{C})$. En quotientant par le centre, on peut enfin montrer que tout sous-groupe fini de $PGL_2(\mathbf{C})$ est isomorphe à l'un des groupes C_n, D_n, A_4, S_4 , A_5 précédents.

Pavages du disque

Le disque unité $\mathbf{D} = \{\zeta \in \mathbf{C}, |\zeta| < 1\}$ est naturellement muni d'une métrique $d\sigma^2 = 4\frac{|d\zeta|^2}{(1-|\zeta|^2)^2}$. La transformation conforme $z = -i\frac{\zeta+1}{\zeta-1}$ l'envoie bijectivement sur le demi-plan de Poincaré $\mathcal{H} = \{z = x + iy \in \mathbf{C}, y > 0\}$, muni de la métrique $ds^2 = \frac{dx^2+dy^2}{y^2}$. L'action de $SL_2(\mathbf{R})$ sur $\mathcal{H}$ donnée par $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$ induit une action fidèle de $PSL_2(\mathbf{R})$ sur $\mathcal{H}$, qui préserve cette métrique. En fait (voir cours "Analyse complexe"), le groupe des isométries directes de $\mathcal{H}$ s'identifie à $PSL_2(\mathbf{R})$, et l'étude des pavages de $\mathbf{D}$, ou de façon équivalente, de $\mathcal{H}$, s'identifie à celle des sous-groupes discrets de $PSL_2(\mathbf{R})$ (on autorise ici des pavés non compacts, pourvu qu'ils soient d'aire finie relativement à la mesure $PSL_2(\mathbf{R})$-invariante $\frac{dxdy}{y^2}$).

La classification des sous-groupes discrets de $PSL_2(\mathbf{R})$ est beaucoup plus complexe que les précédentes (en géométrie hyperbolique, la somme des angles d'un triangle est $< \pi$, et l'inéquation $\frac{1}{n} + \frac{1}{m} + \frac{1}{r} < 1$ ne permet pas de borner n, m, r). Signalons simplement l'exemple du groupe modulaire $\Gamma = PSL_2(\mathbf{Z})$ et de ses "sous-groupes de congruences" , qui jouent un rôle fondamental en théorie des nombres. Un pavage de $\mathcal{H}$ correspondant à Γ est donné par $P = \{z \in \mathcal{H}, |x| \leq 1/2, |z| \geq 1\}$. Voir J-P. Serre, *Cours d'arithmétique*, G. Shimura *Arithmetic theory of automorphic functions*, et pour d'autres applications, M. Yoshida, *Fuchsian differential equations*.

CHAPITRE III

STRUCTURE DES GROUPES FINIS

§1. Les théorèmes de Sylow.

Dans tout ce paragraphe, p désigne un nombre premier, et G un groupe fini. On dit que G est un p-groupe si son ordre est une puissance p^n de p (avec $n \geq 0$). Plus généralement, écrivons $|G| = p^n m$ avec m premier à p. On dit qu'un sous-groupe S de G est un p-sous-groupe de Sylow de G (ou plus simplement: un p-Sylow de G) si $|S| = p^n$, autrement dit si S est un p-groupe d'ordre premier à $[G : S]$. Alors, tout sous-groupe conjugué à S est un p-Sylow de G. On va voir que l'ensemble $\mathcal{S}$ des p-sous-groupes de Sylow de G forme une classe de conjugaison non vide de sous-groupes de G (réduite bien sûr à $\{1\}$ si p ne divise pas $|G|$). On en déduit que dès que p divise $|G|$, il existe des éléments x de G d'ordre égal à une puissance $p^\nu, \nu > 0$ de p, et donc, en considérant $x^{p^{\nu-1}}$:

Corollaire 1: i) (Cauchy) *pour tout nombre* premier p *divisant* $|G|$, G *admet des éléments d'ordre* p.

ii) G *est un* p*-groupe si et seulement si tous ses éléments sont d'ordre une puissance de* p.

Exemple: soit k un corps fini, de cardinal $q = p^f$. Le groupe $G = GL_n(k)$ est d'ordre $p^{fn(n-1)/2}m$, où $m = \Pi_{i=1,..,n}(q^i - 1)$, qui est premier à p. Le sous-groupe S de G formé par les matrices triangulaires supérieures strictes (i.e. n'ayant que des 1 sur la diagonale) est un p-Sylow de G.

Lemme 1: *soient* G *un groupe fini,* H *un sous-groupe de* G *et* S *un* p*-Sylow de* G. *Alors il existe* $g \in G$ *tel que* $H \cap gSg^{-1}$ *soit un* p*-Sylow de* H.

Démonstration: soit $X = G/S$ l'ensemble des classes à gauche de G modulo S, sur lequel le groupe H agit par translation à gauche. Le fixateur de tout point gS de X sous l'action de H est l'intersection de H avec le conjugué gSg^{-1} de S; c'est donc un p-groupe. Comme p ne divise pas $card(X) = [G : S]$, l'une au moins des orbites, soit $H.gS$, de X sous H a un cardinal $[H : (H \cap gSg^{-1})]$ premier à p. Donc $H \cap gSg^{-1}$ est un p-sous-groupe de H d'ordre premier à son indice dans H, i.e. un p-Sylow de H.

Théorème 1: *soient G un groupe fini, et p un nombre premier. Alors,*

i) G possède des p-Sylow;

ii) deux p-Sylow de G sont conjugués l'un de l'autre;

iii) tout p-sous-groupe de G est contenu dans un p-Sylow de G.

Démonstration: i) D'après le Lemme 1, il suffit de plonger G (c'est-à-dire de construire un homomorphisme injectif de G) dans un groupe $\mathbf{G}$ admettant un p-Sylow. Or si $n = |G|$, G se plonge dans le groupe symétrique S_n, et ce dernier se plonge dans $\mathbf{G} = GL_n(\mathbf{F}_p)$ par l'homomorphisme ρ qui attache à $\sigma \in S_n$ l'automorphisme $\rho(\sigma)$ du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p^n$ défini par $\rho(\sigma)(x_1, ..., x_n) = (x_{\sigma^{-1}(1)}, ..., x_{\sigma^{-1}(n)})$. D'après l'exemple, $\mathbf{G}$ admet un p-Sylow, donc G aussi.

ii) (resp. iii) Appliquer le lemme au cas où H est un p-Sylow (resp. un p-sous-groupe) de G. [NB: le Corollaire 1.i et ii *supra* découle immédiatement de i).]

Proposition 1: *si $|G| = p^n m$ avec $(p, m) = 1$, le nombre $s = card(\mathcal{S})$ de p-sous-groupes de Sylow de G divise m, et vérifie $s \equiv 1$ mod p.*

Démonstration: D'après le Théorème 1, G agit par conjugaison sur $\mathcal{S}$, et ce de façon transitive. Or le fixateur dans G d'un élément S de $\mathcal{S}$ est $N_G(S)$, qui contient S. Par conséquent, $s = [G : N_G(S)]$, qui divise $[G : S] = m$. Faisons maintenant agir S sur $\mathcal{S}$ par conjugaison, et montrons que la seule orbite à un élément est celle de S lui-même: si $sS's^{-1} = S'$ pour tout $s \in S$, alors SS' est un sous-groupe de G, dont tous les éléments sont d'ordre une puissance de p; d'après le corollaire 1.ii, c'est donc un p-groupe, d'où par maximalité des p-Sylow: $SS' = S = S'$. Les autres orbites ont un cardinal distinct de 1 et diviseur de $|S|$, donc divisible par p. Ainsi, $s \equiv 1$ mod p.

§2 Groupes résolubles et groupes nilpotents.

Dans un groupe G, on appelle commutateur de deux éléments x, y l'élément $[x, y] := x^{-1}y^{-1}xy$ de G , et pour deux sous-groupes A, B de G, on note $[A, B]$ le sous-groupe de G *engendré* par les commutateurs $[a, b], a \in A, b \in B$. Si $B \triangleleft G$, $[A, B]$ est contenu dans B et $[A, B]$ est distingué dans G (resp. caractéristique) dès que A *et* B le sont. En particulier, le *groupe dérivé* $DG := [G, G]$ est caractéristique. Par sa définition même, DG est le plus petit sous-groupe distingué N de G tel que G/N soit abélien, et on peut interpréter G/DG (souvent noté G^{ab}) comme "le plus grand quotient" abélien de G: tout homomorphisme de G vers un groupe abélien se factorise de manière unique à travers G/DG.

Posons $D^0G = G$ et pour tout entier $i \geq 0, D^{i+1}G = [D^iG, D^iG]$. Les D^iG forment une suite décroissante de sous-groupes caractéristiques de G, dont les quotients successifs

$D^iG/D^{i+1}G$ sont abéliens, et qu'on appelle la *suite dérivée* de G. Elle vérifie clairement la propriété de minimalité suivante:

Lemme 2: *Soit* $\{G_i, i = 0, 1, ...\}$ *une suite décroissante de sous-groupes tels que* $G_0 = G, G_{i+1} \triangleleft G_i$ *et que* G_i/G_{i+1} *soit abélien pour tout* i. *Alors,* D^iG *est contenu dans* G_i *pour tout* i.

On dit que G est *résoluble* s'il existe un entier n tel que $D^nG = \{1\}$. Le plus petit de ces entiers s'appelle alors la classe de résolubilité de G. Par exemple, un groupe abélien est résoluble de classe 1. Le groupe diédral D_n (stabilisateur dans $O_2(\mathbf{R})$ d'un polygone régulier à n côtés) est résoluble de classe 2. Plus généralement (exercice), il résulte du Lemme 2 et des théorèmes d'isomorphisme du chap. I. §1 que:

i) tout sous-groupe (resp. tout quotient) d'un groupe résoluble est résoluble;

ii) soit H un sous-groupe distingué d'un groupe G; si H et G/H sont résolubles (de classes de résolubilité n_1, n_2), G est résoluble (de classe de résolubilité $\leq n_1 + n_2$).

Un peu d'histoire: pour $n \geq 5$, le groupe alterné A_n est simple et non abélien, de sorte que le groupe S_n n'est pas résoluble; en revanche, S_2, S_3, S_4 sont résolubles. On montre en théorie de Galois qu'une équation algébrique est résoluble par radicaux si et seulement si son groupe de Galois est résoluble; on en déduit que pour $n \geq 5$, l'équation générale de degré n n'est pas résoluble par radicaux, tandis qu'elle l'est pour $n = 2$ (formule du trinôme), $n = 3$ (formules de Cardan), $n = 4$ (formules de Ferrari).

Posons $C^0G = G$ et pour tout entier $i \geq 0, C^{i+1}G = [G, C^iG]$. Les C^iG forment une suite décroissante de sous-groupes caractéristiques de G, qu'on appelle la *suite centrale descendante* de G. Pour tout $i > 0$, on a $C^i(G) \supset D^i(G)$, et $C^{i+1}(G)$ est le plus petit sous-groupe distingué N de G contenu dans $C^i(G)$ et tel que $C^i(G)/N$ soit contenu dans le centre $Z(G/N)$ de G/N.

On dit que G est *nilpotent* s'il existe un entier n tel que $C^n(G) = \{1\}$. Le plus petit de ces entiers n s'appelle la classe de nilpotence de G. Un groupe abélien est nilpotent. Un groupe nilpotent est résoluble. Mais S_3 est résoluble sans être nilpotent. De même, pour tout corps commutatif k, le sous-groupe B de $G = GL_n(k)$ formé par les matrices triangulaires supérieures (à coefficients diagonaux quelconques) est résoluble, mais (si $k \neq \mathbf{F}_2$) pas nilpotent. Le sous-groupe S de B formé par les matrices triangulaires supérieures strictes est, lui, nilpotent.

Un groupe G est nilpotent si et seulement s'il admet une suite de sous-groupes $G_0 = G \supset G_1 \supset ... \supset G_m = \{1\}$ telle que $[G, G_i] \subset G_{i+1}$ pour tout i (puisqu'alors, $C^i(G) \subset G_i$ pour tout i). Donc tout sous-groupe et tout quotient d'un groupe nilpotent est nilpotent.

Inversément, si H est un sous-groupe de G *contenu dans le centre* $Z(G)$ de G et si G/H est nilpotent, alors G est nilpotent.

Proposition 2: *i) tout p-groupe G est nilpotent.*

ii) Soit G un groupe nilpotent. Tout sous-groupe propre H de G est strictement inclus dans son normalisateur $N_G(H)$; en particulier, tout sous-groupe de G d'indice premier est distingué dans G.

iii) Soient G un groupe fini, et S un p-Sylow de G. Pour tout sous-groupe H de G contenant $N_G(S)$, on a $H = N_G(H)$.

Démonstration: i) d'après l'application 1 du chap. I, §3, le centre Z de G est non trivial (si $|G| > 1$). On conclut par une récurrence sur $|G|$. On peut aussi montrer cet énoncé en plongeant, pour n assez grand, G dans $GL_n(\mathbf{F}_p)$, puis en notant que les p-Sylow de G sont conjugués au groupe triangulaire strict S, qui est nilpotent.

ii) Récurrence sur la classe de nilpotence n de G. L'énoncé est clair si $n = 1$. Si $n > 1$, le sous-groupe $A = C^{n-1}(G)$ de G est contenu dans le centre de G, et G/A est nilpotent de classe $n-1$. Alors, $N_G(H)$ contient A, et on a gagné si H ne contient pas A. Sinon, l'hypothèse de récurrence entraîne que H/A est strictement inclus dans $N_{G/A}(H/A)$, donc $H \neq N_G(H)$.

iii) Soit n un élément de $N_G(H)$. Alors, S et $nSn^{-1} \subset nHn^{-1} = H$ sont des p-Sylow de H, donc sont conjugués dans H: il existe $h \in H$ tel que $hSh^{-1} = nSn^{-1}$. Donc $h^{-1}n \in N_G(S) \subset H$, et $n \in H$.

Théorème 2: *soit G un groupe fini. Les conditions suivantes sont équivalentes:*

i) G est nilpotent;

ii) pour tout sous-groupe propre H de G, $H \neq N_G(H)$;

iii) deux éléments de G d'ordres premiers entre eux commutent;

iv) G est isomorphe au produit direct de ses sous-groupes de Sylow;

v) pour tout nombre premier p, G admet un unique p-Sylow.

Démonstration: comme $C^i(G_1 \times G_2) = C^i(G_1) \times C^i(G_2)$ et que *iii)* $\Leftrightarrow$ *iv)* $\Leftrightarrow$ *v)* est clair (voir la Proposition 3.i *infra*), seul *ii)* $\Rightarrow$ *iv)* reste à vérifier. Soit S un p-Sylow de G. D'après l'hypothèse ii) et la Prop. 2.iii, $N_G(S) = G$, i.e. S est distingué dans G, et le théorème 1.ii entraîne que pour tout p, G n'a qu'un p-Sylow S_p; leur normalité dans G entraîne de plus que, pour tout couple p, ℓ de nombres premiers distincts, $[S_p, S_\ell] \subset S_p \cap S_\ell = \{1\}$, d'où en vertu de la Proposition 3.i, $G \simeq \Pi_p S_p$.

Si G est abélien, son unique p-Sylow s'appelle la composante p-primaire $G^{(p)}$ de G. On peut énoncer:

Corollaire 2: *tout groupe abélien fini G est isomorphe au produit direct $\Pi_p\ G^{(p)}$ de ses composantes p-primaires, où p parcourt l'ensemble des diviseurs premiers de $|G|$.*

Il est d'ailleurs facile de déduire cet énoncé de la décomposition de G donnée par ses facteurs invariants (voir chap. II, §2).

§**3 Extensions de groupes.** (hors programme)

Soient A et C deux groupes. Une *extension* E de C par A est la donnée d'un triplet (B, i, p), où B est un groupe, et $i : A \to B, p : B \to C$ sont deux homomorphismes tels que $Ker(i) = \{1\}, Im(p) = C$ et $Im(i) = Ker(p)$. On dit encore que la suite

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$$

est exacte. C'est le cas si et seulement si B possède un sous-groupe distingué $A' \simeq A$, tel que $B/A' \simeq C$, et on dit alors par abus de langage que B est une extension de C par A. Un extension est dite *centrale* si $i(A)$ est inclus dans le centre $Z(B)$ de B (ce qui impose bien entendu que A soit commutatif).

On appelle *section* (resp. rétraction) d'une extension $E : 1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$ tout homomorphisme $s : C \to B$ (resp. $r : B \to A$) tel que $p \circ s = id_C$ (resp. $r \circ i = id_A$). On dit qu'une extension est *scindée* si elle admet une section s. L'image $C' = s(C)$ de s est alors un sous-groupe de B. Posant $i(A) = A'$, on a $A' \cap C' = \{1\}, B = A'.C'$, et on dit que C' est un complément de A' dans B. Noter qu'en général, une extension n'est pas scindée: par exemple, dans $1 \longrightarrow \mathbf{Z}/3\mathbf{Z} \xrightarrow{i} \mathbf{Z}/9\mathbf{Z} \xrightarrow{p} \mathbf{Z}/3\mathbf{Z} \longrightarrow 1$, où p est la projection canonique, $Im(i) = 3\mathbf{Z}/9\mathbf{Z}$ n'admet pas de complément.

Soient $E : 1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$ et $E' : 1 \longrightarrow A \xrightarrow{i'} B' \xrightarrow{p'} C \longrightarrow 1$ deux extensions de C par A. Un morphisme de E vers E' est la donnée d'un morphisme de groupes $f : B \to B'$ tel que $f \circ i = i', p' \circ f = p'$, i.e. tel que le diagramme

$$\begin{array}{ccccc} & & B & & \\ & i\nearrow & | & \searrow p & \\ A & & f & & C \\ & i'\searrow & \downarrow & \nearrow p' & \\ & & B' & & \end{array}$$

soit commutatif. Alors, f est automatiquement un isomorphisme. On notera par ailleurs que les groupes B, B' sous-jacents à deux extensions E, E' peuvent être isomorphes sans que les extensions le soient.

Le *produit direct* $A \times C$ est naturellement muni d'une structure d'extension E_1 de C par A, et on dit qu'une extension E est *triviale* si elle est isomorphe à E_1. Cela équivaut (vérification immédiate) à demander que E admette une rétraction, ou encore que E admette une section s telle que $C' := s(C)$ soit *contenu dans le centralisateur* $Z_G(i(A))$ de $i(A)$. En particulier:

Proposition 3.i: *soit G un groupe et H, K deux sous-groupes de G tels que $H \cap K = \{1\}, G = HK$* et *$K \subset Z_G(H)$. Alors, l'application $(h,k) \mapsto hk$ établit un isomorphisme du produit direct $H \times K$ sur G.*

NB: i) les conditions $K \subset Z_G(H)$ et $H \subset Z_G(K)$ sont équivalentes; on dit alors que H et K commutent, ou encore qu'ils se centralisent mutuellement.

ii) supposons G fini; sous l'hypothèse $H \cap K = \{1\}$, la condition $G = HK$ équivaut à demander que $|G| = |H|.|K|$.

Soit maintenant $\tau : C \to Aut(A)$ un homomorphisme (autrement dit: une action de C sur A compatible à la structure de groupe de A). Pour tout $(a,c) \in A \times C$, écrivons ${}^c a$ pour $\tau(c)(a)$. Rappelons qu'on appelle *produit semi-direct* $A \times_\tau C$ de C par A relativement à τ l'ensemble $A \times C$, muni de la loi de composition interne

$$(a,c),(a',c') \to (a.{}^c a', c.c'),$$

qui en fait un groupe, d'élement neutre $(1,1)$ (avec $(a,c)^{-1} = ({}^{c^{-1}}a^{-1}, c^{-1})$). De plus, les applications naturelles $i : A \to A \times C$ et $p : A \times C \to C$ munissent $A \times_\tau C$ d'une structure d'extension E_τ de C par A. Pour l'action triviale $\tau = 1$ de C sur A (i.e. $\tau(c) = id_A$ pour tout $c \in C$), on retrouve le produit direct $E_1 \simeq A \times C$.

Soit $E : 1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$ une extension scindée, et s une section. Puisque $A' = i(A) \lhd B$, $C' = s(C)$ est trivialement inclus dans le normalisateur $N_B(A')$, et l'action de B sur A' par conjugaison définit par restriction à C' un homomorphisme τ_s de C dans $Aut(A)$. (Par exemple, $\tau_s = 1$ si l'extension est centrale.) Dans ces conditions, les extensions E et $E' = E_{\tau_s}$ sont isomorphes: en effet, l'application $f' : E' \to E : (a,c) \mapsto i(a).s(c)$ vérifie $f'(a_1,c_1).f'(a_2,c_2) = i(a_1)Int(s(c_1))(i(a_2)).s(c_1c_2) = f'(a_1\tau_s(c_1)(a_2), c_1c_2)$, et définit bien un morphisme d'extensions. En particulier:

Proposition 3.ii: *soient G un groupe et H, K deux sous-groupes de G tels que $H \cap K = \{1\}, G = HK$* et *$K \subset N_G(H)$, et soit τ l'homomorphisme de K dans $Aut(H)$ défini par $\tau(k)(h) = khk^{-1}$ pour tout $(k,h) \in K \times H$. Alors, l'application $(h,k) \mapsto hk$ établit un isomorphisme du produit semi-direct $H \times_\tau K$ sur G.*

NB: i) sous l'hypothèse $G = HK$, la condition $K \subset N_G(H)$ équivaut à $H \lhd G$.

ii) Soit E une extension centrale de C par A. Alors, E est triviale si et seulement si elle est scindée.

Rudiments de cohomologie des groupes

Nous supposons désormais que A **est commutatif**, de sorte que pour toute extension $E : 1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$, l'homomorphisme de B dans $Aut(i(A)) \simeq Aut(A)$ défini par la conjugaison admet $i(A)$ dans son noyau, et induit donc par passage au quotient un homomorphisme $\tau : C \to Aut(A)$. On fixe dans ce qui suit un tel homomorphisme τ et on note $Ext_\tau(C, A)$ l'ensemble des classes d'isomorphismes d'extensions de C par A induisant τ; par exemple, si τ est l'identité, i.e. si l'action de C sur A est triviale, $Ext_\tau(C, A)$ est l'ensemble $Ext(C, A)$ des classes d'isomorphisme d'extensions *centrales* de C par A. Les groupes de cohomologie définis plus bas permettent de mesurer l'obstruction au scindage de E, de reconstruire B à partir de C, A, τ et de cette obstruction, et de s'assurer de l'unicité d'un scindage s'il en existe.

$\bullet H^2$. - Notons additivement la loi de groupe de A, et reprenons la notation ${}^c a = \tau(c)(a)$ pour tout $(c, a) \in C \times A$. Un 2-cocycle de C à valeurs dans A (relativement à τ) est une application $f : C \times C \to A$ telle que $f(c, c'c'') + {}^c f(c', c'') = f(cc', c'') + f(c, c')$ pour tout $c, c', c'' \in C$. La loi de groupe de A munit l'ensemble $Z^2(C, A)$ des 2-cocyles d'une structure de groupe abélien, qui contient comme sous-groupe l'ensemble $B^2(C, A)$ des 2-cobords, c'est-à-dire des applications $dF : C \times C \to A$ de la forme $dF(c, c') = F(c) + {}^c F(c') - F(cc')$, où F est une application de C dans A. Le quotient $H^2(C, A) = Z^2(C, A)/B^2(C, A)$ s'appelle le *2e groupe de cohomologie* de C à valeurs dans A (τ est ici sous-entendu).

Soit E une extension dans $Ext_\tau(C, A)$. Considérons une "section ensembliste" de E, c'est-à-dire une application $\sigma : C \to B$ telle que $p \circ \sigma = id_C$; autrement dit, $\sigma(C)$ est un système de représentants de l'ensemble $G/i(A)$ des classes à gauche modulo $i(A)$. Pour tous $c, c' \in C$, $\sigma(cc')$ et $\sigma(c)\sigma(c')$ sont dans la même classe, et il existe $f(c, c') \in A$ unique tel que $\sigma(c)\sigma(c') = i(f(c, c'))\sigma(cc')$. L'associativité de la loi de groupe de B montre que l'application f ainsi définie est un 2-cocycle. En outre, si on remplace σ par une autre section ensembliste σ', il existe pour tout $c \in C$ un unique élément $F(c) \in A$ tel que $\sigma'(c) = F(c)\sigma(c)$, et le 2-cocycle f' associé à σ' vérifie $f'(c, c') = f(c, c') + dF(c, c')$. Ainsi, la classe de f dans $H^2(C, A)$ ne dépend que de la classe d'isomorphisme de E dans $Ext_\tau(C, A)$.

Inversément, soit $f : C \times C \to A$ un 2-cocycle. Alors la loi $(a, c).(a', c') = (a + {}^c a' + f(c, c'), cc')$ munit l'ensemble $A \times C$ d'une structure de groupe B, d'élément neutre

$(-f(1,1),1)$, qui est naturellement une extension de C par A (poser $i(a) = (a - f(1,1),1)$), et cette construction est inverse de la précédente. On peut donc identifier $Ext_\tau(C,A)$ et $H^2(C,A)$, et munir ainsi $Ext_\tau(C,A)$ d'un structure de groupe (*)

L'élément neutre E^τ de $Ext_\tau(C,A)$ correspond aux cocycles f de classe nulle dans H^2, i.e. aux cobords dF. Étant donné une section ensembliste σ de E^τ, on peut donc trouver une application $F : C \to A$ telle que $\sigma' := F \,.\, \sigma$ vérifie $\sigma'(cc') = \sigma'(c)\sigma'(c')$. Ainsi, σ' est une "vraie" section, et l'extension E^τ est scindée, donc isomorphe au produit semi-direct $A \times_\tau C$.

•H^1.- Un 1-cocycle de C à valeurs dans A (relativement à τ) est une application $f : C \to A$ telle que $\forall\ c, c' \in C\ ,\ f(cc') = f(c) + {}^c f(c')$. La loi de groupe de A munit l'ensemble $Z^1(C,A)$ des 1-cocyles d'une structure de groupe abélien, qui contient comme sous-groupe l'ensemble $B^1(C,A)$ des 1-cobords, c'est-à-dire des applications $da : C \to A$ de la forme $da(c) = {}^c a - a$, où a est un élément de A. Le quotient $H^1(C,A) = Z^1(C,A)/B^1(C,A)$ s'appelle le *1er groupe de cohomologie* de C à valeurs dans A (τ est ici sous-entendu).

Soient s et s' deux sections (de groupe) de l'extension scindée E_τ. Alors, il existe une unique application f de C dans A telle que $s'(c) = f(c)s(c)$ pour tout c, et on vérifie aisément que f est un 1-cocycle. De plus, si s' se déduit de s au moyen d'une conjugaison par un élément a de A, i.e. si $s'(c) = as(c)a^{-1}$ pour tout c, alors $f = d(-a)$. Ainsi, $H^1(C,A)$ décrit l'ensemble des classes de conjugaison (sous A) de sections de E_τ, ou encore: dans un produit semi-direct $G = H \times_\tau K$, l'ensemble des classes de conjugaison sous A des compléments K' de H dans G est en bijection avec le groupe $H^1(K,H)$.

• Exemple: supposons que $|A|$ et $|C|$ soient des nombres premiers entre eux. On peut montrer qu'alors $H^i(C,A) = 0$ pour $i = 1, 2$ (et tout choix de τ). Traduction concrète ?

(*) Voici, au moins dans le cas des extensions centrales, un procédé plus direct pour construire cette structure: pour toute $E \in Ext(C,A)$ et tout morphisme $g : C' \to C$, le groupe $\{(b,c') \in B \times C', p(b) = g(c')\}$ fournit un élément $g^*(E)$ de $Ext(C',A)$. Pour tout morphisme $f : A \to A'$, le groupe $A' \times B/\{(-a, f(a)), a \in A\}$ fournit un élément $f_*(E)$ de $Ext(C,A')$. Dans ces conditions, soient E_1 et E_2 dans $Ext(C,A)$. Alors, $E_1 \times E_2$ définit un élément de $Ext(C \times C, A \times A)$. Si $d : C \to C \times C$ et $s : A \times A \to A$ désignent l'application diagonale et la loi de A, la loi de groupe sur $Ext(C,A)$ est donnée par $E_1 + E_2 := d^* s_*(E_1 \times E_2)$.

CHAPITRE IV

REPRÉSENTATIONS LINÉAIRES

§1. Lexique des représentations.

Soient G un groupe, et K un corps commutatif. Une *représentation linéaire* de G sur un K-espace vectoriel V est la donnée d'une action à gauche de G sur V, respectant la structure K-linéaire de V; autrement dit, c'est la donnée d'un homomorphisme de groupes $\rho = \rho_V : G \to GL(V)$ de G dans le groupe des automorphismes K-linéaires de V. Par abus de langage, on sous-entend parfois ρ , et on dit que V est une représentation de G; au lieu de $\rho(g)(v)$, on note $g.v$, ou même gv, l'image d'un vecteur v de V sous l'action (via ρ) d'un élément g de G. On a donc $g(\lambda v + v') = \lambda gv + gv', (gg')v = g(g'v), 1_G v = v$ pour tout $g, g' \in G, v, v' \in V, \lambda \in K$. La dimension $\dim V$ de l'espace de la représentation s'appelle le *degré* de ρ, et on dit que v est un *invariant* de la représentation si $gv = v$ pour tout g dans G; notation: $v \in V^G$.

On dit qu'une représentation ρ est *fidèle* si l'action correspondante l'est, i.e. si l'homomorphisme ρ est injectif. A l'extrême opposé, on trouve la représentation triviale $\mathbf{1}_V$ sur V, définie par $\mathbf{1}_V(g) = id_V$ pour tout $g \in G$. Pour $V = K$, la représentation triviale $\mathbf{1}_K$ s'appelle la *représentation unité* de G (relativement au corps K).

Exemples: i) quand G est déjà défini comme un sous-groupe de $GL(V)$, V est une représentation de G, dite souvent représentation naturelle (ou standard).

ii) Soit X un ensemble muni d'une action à gauche de G. La *représentation de permutation* associée est le K-espace vectoriel $V = K.X$ de base $\{e_x, x \in X\}$, muni de l'action définie par K-linéarité à partir des conditions $g.e_x = e_{g.x}$. On peut aussi voir $K.X$ comme l'espace vectoriel des fonctions $\mathcal{F}_0(X, K)$ sur X à valeurs dans K, de support fini (i.e. nulles hors d'une partie finie de X). Dans l'identification avec des fonctions, e_x correspond à la fonction de Dirac centrée en x: $\delta_x : y \mapsto \delta_x(y) = 0$ si $x \neq y, \delta_x(x) = 1$. En terme de fonctions $f \in \mathcal{F}_0(X, K)$, l'action de G est donc donnée par $g.f : x \mapsto f(g^{-1}x)$. Si X est fini, l'élément $\Sigma_{x \in X} e_x$ (i.e. la fonction constante 1 sur X) est un invariant de V.

iii) Pour $X = G$, muni de l'action par translation à gauche de G, la représentation de permutation $V = K.G \simeq \mathcal{F}_0(G, K)$ s'appelle la *représentation régulière* R de G. Elle est

donc définie par

$$R(g)(\Sigma_{h\in G}\ x_h e_h) = \Sigma_{h\in G}\ x_h e_{gh} = \Sigma_{h\in G}\ x_{g^{-1}h} e_h,$$

où pour tout $h \in G$, x_h est un élément de K, avec $x_h = 0$ pour tout h en dehors d'une partie finie de G.

Une K-ss-ev W de V stable (on dit aussi : invariant) sous G, i.e. tel que gv appartient à W pour tout $(g, v) \in G \times W$, s'appelle une *sous-représentation* de ρ. L'espace vectoriel quotient V/W est alors naturellement muni d'une structure de représentation de G, appelée *représentation quotient* de V par W. On dit que ρ est *irréductible* si elle n'admet pas de sous-représentation propre (i.e. distincte de $\{0\}$ et de V). Si V et W sont deux représentations de G, leur somme directe est la représentation $V \oplus W$ définie par $g.(v \oplus w) = gv \oplus gw$. Si une représentation V est somme directe de deux sous-représentations propres, on dit qu'elle est *décomposable*. Noter qu'une représentation indécomposable n'est pas forcément irréductible.

Un *morphisme* entre deux représentations V et W de G est un homomorphisme K-linéaire $\phi : V \to W$ tel que $\phi(g.v) = g.\phi(v)$ pour tout $(g, v) \in G \times V$. On dit aussi que ϕ est G-linéaire, ou que c'est un G-morphisme. Les représentations V et W sont dites *équivalentes* (ou isomorphes, ou, quand $V = W$, *conjuguées*) s'il existe un G-morphisme bijectif de l'une vers l'autre (son inverse est encore un G-morphisme). Exemple : la sous-représentation $W = K.v$ de V engendrée par un vecteur invariant v de V est isomorphe à la représentation unité $\mathbf{1}_K$ de G.

Remarque 1: le K-espace vectoriel $K.G$ de la représentation régulière est muni d'un loi de produit $(e, e') \to e.e'$, définie par K-bilinéarité à partir des relations $e_g.e_h := e_{gh}$ pour tout g, h dans G, qui fait de $K.G$ une K-algèbre associative unitaire (= K-espace vectoriel A muni d'une application K-bilinéaire $A \times A \to A$ qui fait de A un anneau unitaire; K est alors isomorphe au sous-anneau $K.1_A$ de A). En terme de $\mathcal{F}_0(X, K)$, ce produit s'identifie au produit de convolution $(f, f') \mapsto f * f'$, où $f * f'(g) := \Sigma_{h\in G} f(h)f'(h^{-1}g)$. On note $K[G]$ cette structure d'algèbre sur $K.G$, et on l'appelle l'**algèbre du groupe** G sur le corps K. Soit alors M un $K[G]$-module à gauche. L'application $g \to \{\rho(g) : m \to \rho(g)(m) := e_g m\}$ munit le K-espace vectoriel sous-jacent à M d'une structure de représentation de G. Inversément, l'espace V d'une représentation ρ de G est muni par la loi $e_g.v := \rho(g)(v)$ d'une structure naturelle de $K[G]$-module à gauche. On vérifie immédiatement que la catégorie des représentations de G est ainsi équivalente à la catégorie des modules sur l'algèbre $K[G]$.

Si A est une K-algèbre, un A-module à gauche M est dit simple s'il n'a pas de sous-A-module autre que $\{0\}$ et M. Un A-module est dit semi-simple s'il est somme directe (éventuellement réduite à un élément) de sous-modules simples. Un $K[G]$-module simple (resp. semi-simple) correspond donc à une représentation irréductible de G (resp. à une représentation irrédutible ou décomposable en somme directe de représentations irréductibles). Comme tout anneau, l'algèbre de groupe $K[G]$ est un module sur elle-même (pour la multiplication à gauche). La représentation correspondante n'est autre que la représentation régulière de G; ses sous-représentations sont données par les idéaux à gauche de $K[G]$.

Soient (V, ρ) une représentation de G, et $V^* = Hom(V, K)$ le dual du K-espace vectoriel V. On munit V^* d'une structure de représentation de G en posant, pour toute forme linéaire f sur V et tout g dans G: $\rho^*(g)(f) = f \circ \rho(g^{-1})$ (en abrégé : $g.f = fg^{-1}$), de sorte que pour tout $(g, f, v) \in G \times V^* \times V$, on a: $< g.f|g.v >:=< \rho^*(g)(f)|\rho(g)(v) > = < f|v >$; autrement dit, $\rho^*(g) \in End_K(V^*)$ est la transposée de $\rho(g^{-1}) \in End_K(V)$. On dit que ρ^* est la représentation duale , ou *contragrédiente*, de ρ. Soient maintenant V et W deux représentations de G. L'espace $Hom(V, W)$ des homomorphismes K-linéaires de V dans W est naturellement muni d'une structure de représentation de G: poser, pour tout g dans G et tout K-homom. ϕ de V dans W: $g.\phi = g\phi g^{-1}$. Un G-morphisme s'identifie ainsi à un invariant de la représentation $Hom(V, W)$; l'ensemble $(Hom(V, W))^G$ des G-morphismes est noté $Hom_G(V, W)$. La représentation V^* s'identifie à $Hom(V, \mathbf{1}_K)$; de même, la représentation W s'identifie à $Hom(\mathbf{1}_K, W)$.

Plus généralement, *toutes les constructions de l'algèbre (multi)linéaire s'étendent à la catégorie des représentations de G.* Partons ainsi de deux K-espaces vectoriels V, W. On peut former leur **produit tensoriel** $V \otimes_K W$: c'est un K-espace vectoriel $\mathcal{E}$ muni d'une application K-bilinéaire $\beta := \otimes : V \times W \to \mathcal{E}$, qui est solution du problème universel suivant: pour toute application K-bilinéaire b de $V \times W$ vers un K-espace vectoriel E quelconque, il existe une *unique application K-linéaire* $f : \mathcal{E} \to E$ telle que pour tout $v, w \in V \times W, b(v, w) = f(v \otimes w)$ (i.e. $b = f \circ \beta$). En particulier, pour tout scalaire λ, $(\lambda v) \otimes w = v \otimes (\lambda w) = \lambda(v \otimes w)$; si $\{e_i; i \in I\}, \{\epsilon_j; j \in J\}$ sont des bases de V, W, alors $\{e_i \otimes \epsilon_j, (i, j) \in I \times J\}$ est une base de $V \otimes W$, et donc $\dim(V \otimes W) = \dim(V) \dim(W)$.

Soit V^* le dual de V. L'application bilinéaire $W \times V^* \to Hom(V, W) : (w, f) \mapsto \{\phi : v \mapsto \phi(v) := f(v)w\}$ définit un homomorphisme canonique de $W \otimes V^*$ vers $Hom(V, W)$. Cet homomorphisme est injectif, mais en général pas surjectif: son image est formée des homomorphismes $\phi : V \to W$ de rang fini, i.e. tels que $\phi(V)$ soit un sous-espace de

dimension finie de W. On a donc un isomorphisme canonique

$$\iota : W \otimes V^* \simeq Hom(V, W)$$

dès que V ou W est de dimension finie. Par exemple, pour $\dim(V)$ finie, $V \otimes V^* \simeq End_K(V)$, l'image inverse de id_V étant donnée par le tenseur $\Sigma_{i\in I} e_i \otimes e_i^*$, où $\{e_i\}$ désigne une base quelconque de V, de base duale $\{e_i^*\}$. Si un endomophisme ϕ de V est représenté par un tenseur $\Sigma_\ell v_\ell \otimes f_\ell \in V \otimes V^*$, sa trace est donnée par la formule $Tr(\phi) = \Sigma_\ell f_\ell(v_\ell) \in K$.

L'inversion des facteurs induit un isomorphisme $V \otimes W \simeq W \otimes V$, d'où, pour $V = W$, une involution $\theta \in GL(V \otimes V)$. On appelle tenseurs symétriques (resp. antisymétriques) les élements t de $V \otimes V$ tels que $\theta(t) = t$ (resp. $-t$). Ils forment des sous-espaces vectoriels $Sym^2(V)$ (resp. $Alt^2(V)$), qui, pour K de caractéristique $\neq 2$, sont supplémentaires dans $V \otimes V$. – Dans le cas général, il vaut mieux introduire les quotients S^2V (resp. $\Lambda^2 V$) de $V \otimes V$ par le sous-espace engendré par les tenseurs de type $\theta(t) - t$ (resp. $v \otimes v$); ce sont les solutions de problèmes universels du même type que $\otimes$, où on impose aux formes bilinéaires d'être symétriques (resp. alternées).

Supposons maintenant que V, W soient les espaces de représentations ρ, σ du groupe G. Alors, $V \otimes W$ est l'espace d'une représentation de G, notée $\rho \otimes \sigma$ et définie par la condition $(\rho \otimes \sigma)(g)(v \otimes w) := \rho(g)(v) \otimes \sigma(g)(w) = gv \otimes gw$ pour tout $(g, v, w) \in G \times V \times W$. On l'appelle *produit tensoriel* des représentations ρ et σ. Ainsi, les espaces vectoriels $Hom(V, W)$ et $W \otimes V^*$ portent tous deux des représentations naturelles, et on vérifie aisément que pour V, W de dimension finie, l'isomorphisme de K-espaces vectoriels $\iota : W \otimes V^* \simeq Hom(V, W)$ défini plus haut est en fait un G-isomorphisme: en effet, si $\iota(w \otimes f) = \phi$, l'image sous ι de $g.(w \otimes f) := gw \otimes gf = gw \otimes fg^{-1}$ est l'homomorphisme $v \mapsto f(g^{-1}v)gw = g\phi(g^{-1}v) := (g.\phi)(v)$, d'où $\iota g = g\iota$. On pourra donc noter $\sigma \otimes \rho^*$ la représentation sous-jacente à $Hom(V, W)$. De même, $Sym^2(V)$, $Alt^2(V)$ sont des sous-représentations de la représentation $V \otimes V$, et en caractéristique $\neq 2$, $\otimes^2 \rho \simeq Sym^2(\rho) \oplus Alt^2(\rho)$.

Remarque 2 (hors programme): soit A une K-algèbre, et M un A-module à gauche. On munit l'espace $M^* = Hom(M, K)$ des formes K-linéaires sur M d'une structure de A-module à droite par la loi $(a, f) \mapsto f.a : \{m \mapsto f.a(m) = f(am)\}$. Pour $A = k[G]$, on retrouve une structure de $k[G]$-module à gauche pour M^* en posant $(\Sigma_g x_g e_g).f = f.(\Sigma_g x_g e_{g^{-1}})$. Si maintenant M (resp. N) est un A-module *à droite* (resp. à gauche), on définit le produit tensoriel *sur* A de M et N, noté $M \otimes_A N$ comme le quotient du K-ev $M \otimes_K N$ par le K-ssev engendré par les tenseurs $ma \otimes n - m \otimes an$, où m, n, a parcourent

M, N, A. C'est la solution d'un problème universel du même type que supra, pour les formes bilinéaires vérifiant $b(ma, n) = b(m, an)$ pour tout $a \in A$.

Concluons cette avalanche de définitions (qu'il est recommandé de ne lire qu'en parallèle avec le §2) par un résultat essentiellement tautologique, mais fondamental:

Lemme de Schur: *Soient V et W deux représentations* irréductibles *d'un groupe G , et ϕ un G-morphisme non identiquement nul de V vers W . Alors,*

i) ϕ est un isomorphisme;

ii) si de plus $V = W$ est de dimension finie, et si K est algébriquement clos (par ex. si $K = \mathbf{C}$), il existe un scalaire non nul λ tel que $\phi = \lambda.id_V$.

Démonstration: Le noyau (resp. l'image) de ϕ est un sous-espaces invariants de V (resp. W) . L'irréductibilité de ces représentations entraîne la première assertion. Sous les hypothèses de la seconde, ϕ admet au moins une valeur propre $\lambda \in K$, et il suffit d'appliquer la première assertion au G-morphisme $\phi - \lambda id_V$.

2. Théorie des caractères.

Nous supposons désormais que

a) *G est un groupe fini*;

b) *la caractéristique du corps K est nulle ou première à l'ordre $|G|$ de G.*

La proposition suivante exprime que sous ces hypothèses, les notions de représentation "irréductible" et "indécomposable" coïncident (autrement, dit, que tout sous-module d'un $K[G]$-module est facteur direct).

Lemme de Maschke. [sous a) et b)]: *Soit W une sous-représentation d'une représentation V de G. Alors, il existe une sous-représentation W' de V telle que $V \simeq W \oplus W'$.*

Démonstration: soit $\tilde{W}$ un supplémentaire (au sens des espaces vectoriels) de W dans V, et $\tilde{p}$ le projecteur correspondant de V sur W. C'est un élément de $Hom(V, W)$, mais, en général, pas un G-morphisme. Posons alors:

$$p = |G|^{-1}(\Sigma_{g \in G} g.\tilde{p}) = |G|^{-1}(\Sigma_{g \in G}\ g\tilde{p}g^{-1}).$$

On vérifie que p est toujours un projecteur de V sur W, et cette fois, qu'il est invariant sous G. Donc son noyau $W' = Ker(p)$ est un supplémentaire de W dans V stable sous G.

Par récurrence sur $\dim(V)$, on déduit de la proposition que sous a) et b), toute représentation de dimension finie de G est somme directe de représentations irréductibles

(i.e.: tout $K[G]$-module de dimension finie sur K est semi-simple). Le lemme de Schur permet de préciser dans quelle mesure une telle décomposition est unique.

Théorème 1: [sous a) et b)] *Soit V une représentation de dimension finie de G. Il existe une famille finie de représentations irréductibles et non isomorphes V_i $(i = 1, ..., k)$ de G et des entiers $a_1, ..., a_k$ tels que la représentation V soit isomorphe à la somme directe $V_1^{\oplus a_1} \oplus ... \oplus V_k^{\oplus a_k}$. De plus, les classes d'isomorphismes des représentations V_i et leurs "multiplicités d'apparition" a_i dans V ne dépendent que de la représentation V.*

Démonstration (de l'unicité): soient W une seconde représentation de dimension finie de G, $W_1^{\oplus b_1} \oplus ... \oplus W_{k'}^{\oplus b_{k'}}$ une décomposition de W en somme de sommes de représentations irréductibles non isomorphes, et ϕ un G-morphisme de V dans W. On déduit du lemme de Schur (appliqué au composé de ϕ par les projections de W sur les W_j) que $\phi(V_i^{\oplus a_i})$ est nul ou contenu dans l'unique facteur $W_i^{\oplus b_i}$ de W vérifiant (après réindexation) $W_i \simeq V_i$. En comparant les dimensions, on voit que si $V \simeq W$, $a_i = b_i$ pour tout i et $k = k'$.

Outre l'hypothèse a): $|G| < \infty$, nous supposons désormais que

b') $K = \mathbf{C}$ (de sorte que l'hypothèse b) et l'hypothèse ii) de Schur sont satisfaites),

et nous nous restreignons à des représentations de dimension finie. On note indifféremment $\overline{z}$ ou z^* le conjugué d'un nombre complexe z.

Soit donc (V, ρ) une représentation complexe de degré fini de G. On appelle *caractère* de ρ la fonction

$$\chi_\rho = \chi_V : G \to \mathbf{C} : g \mapsto \chi_V(g) = Tr(\rho(g))$$

qui associe à tout élément g de G la trace de l'automorphisme $\rho(g)$ de V, i.e. la somme de ses valeurs propres. Comme les valeurs propres de $\rho(g)$ sont des racines de l'unité (d'ordre divisant $|G|$), on a $\chi_V(g^{-1}) = \chi_V(g)^*$; en l'élément neutre de G, $\chi_V(1) = \dim(V)$. Pour tout (g, h) dans G, $\chi_V(hgh^{-1}) = \chi_V(g)$, donc $\chi_V(g)$ ne dépend que de la classe de conjugaison de g (de telles fonctions sur G sont dites *centrales*). De même, deux représentations isomorphes ont le même caractère.

Remarque 3: on donne souvent le nom de "caractères de G" aux homomorphismes de G dans le groupe multiplicatif K^*. Le caractère χ_V d'une représentation V est une fonction de G dans K, qui peut admettre 0 parmi ses valeurs, et qui n'est donc en général *pas* un caractère de G (sauf bien sûr si $\dim(V) = 1$).

Théorème 2. *Soient V et W deux représentations de degré fini de G. Alors :*

i) le caractère de la représentation $V \oplus W$ est donné par: $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$.

ii) le caractère de la repr. $H = Hom(V, W)$ est donné par: $\chi_H(g) = \chi_W(g)\chi_V(g)^*$.

iii) le caractère de la repr. contragrédiente V^* est donné par $\chi_{V^*}(g) = \chi_V(g)^*$;

iv) le caractère de la représentation $V \otimes W$ est donné par: $\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)$.

v) le caractère des représentations Sym^2V et Alt^2V sont respectivement donnés par $\chi_S(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$, $\chi_A(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$, *de sorte que* $\chi_V^2 = \chi_S + \chi_A$.

Démonstration (de ii): l'endomorphisme $\rho_W(g)$ de W est diagonalisable (appliquer Maschke au sous-groupe $G' =< g >$ de G; ou l'exercice 5.ii infra, puisque G' est abélien; ou encore, noter que le polynôme minimal de $\rho(g)$ divise $X^{ord(g)} - 1$, et n'a donc que des racines simples; ou enfin, appliquer l'exercice 4.ii infra, en se souvenant que toute matrice unitaire est diagonalisable). De même pour $\rho_V(g^{-1})$. Dans des bases de V et W formées de vecteurs propres, la matrice représentative de $\rho_H(g)$ est donc la matrice diagonale $diag\big(\lambda_i^*\mu_j; i = 1, ..., \dim V, j = 1, ..., dimW\big)$, où les λ_i, μ_j désignent les valeurs propres de $\rho_V(g), \rho_W(g)$, d'où ii).

Les autres formules se démontrent de la même manière. Pour v), noter que $\Sigma_{i\leq j}\lambda_i\lambda_j = \frac{1}{2}(\Sigma\lambda_i)^2 + \frac{1}{2}(\Sigma\lambda_i^2)$.

On notera que iii) est conséquence de ii) (prendre $W = \mathbf{1}_K$), et que ii) est conséquence de iii) et iv), puisque d'après le §1, les représentations $Hom(V, W)$ et $W \otimes V^*$ sont équivalentes.

Munissons l'espace $\mathbf{C}.G = \mathbf{C}[G] = \mathcal{F}(G, \mathbf{C})$ des fonctions complexes sur G de sa norme L^2, i.e. du produit scalaire :

$$(f, f') = |G|^{-1}\Sigma_{g\in G} f(g)f'(g)^*.$$

On considérera aussi son sous-espace $\mathcal{F}^{cent}(G, \mathbf{C}) = \{f \in \mathcal{F}(G, \mathbf{C}), \forall g, h \in G, f(hgh^{-1}) = f(g)\}$ des fonctions centrales, qu'on munit de la norme induite. (Comme G est ici fini, on a supprimé l'indice 0 de la notation $\mathcal{F}_0$.) Les **relations d'orthogonalité** suivantes sont la clef de la théorie des caractères.

Théorème 3: *soient V et W deux représentations* irréductibles *de G . Alors,*

i) si W n'est pas isomorphe à V : $(\chi_V, \chi_W) = 0$;

ii) si W est isomorphe à V : $(\chi_V, \chi_V) = 1$.

Démonstration: considérons le sous-espace $V' = V^G$ des vecteurs invariants de V. L'endomorphisme $p = |G|^{-1}\Sigma_{g\in G}\rho_V(g)$ de V est un projecteur de V sur V'. Sa trace vaut donc: $dim(V^G) = Tr(p) = |G|^{-1}\Sigma_{g\in G}Tr(\rho_V(g)) = |G|^{-1}\Sigma_{g\in G}\chi_V(g) = (\chi_V, \mathbf{1_C})$. Appliquons ce résultat à la représentation $H = Hom(V, W)$. D'après le lemme de Schur, $Hom(V, W)^G$ est de dimension 0 (resp. 1) si V et W ne sont pas (resp. sont) isomorphes. Ainsi $(\chi_H, \mathbf{1_C}) = 0$ ou 1 suivant qu'on est dans le cas i) ou le cas ii), et le théorème 2.ii permet de conclure.

Corollaire: *Soit V une représentation de G, et $V_1^{\oplus a_1} \oplus ... \oplus V_k^{\oplus a_k}$ sa décomposition en somme de sommes de représentations irréductibles non isomorphes.*

i) Pour tout $i = 1, ..., k$, la multiplicité a_i de V_i dans V est donnée par $a_i = (\chi_V, \chi_{V_i})$. En particulier, deux représentations sont isomorphes si et seulement si elles ont le même caractère.

ii) On a $(\chi_V, \chi_V) = \Sigma_{i=1,...,k} a_i^2$. En particulier, V est irréductible si et seulement si $(\chi_V, \chi_V) = 1$.

iii) Toute représentation irréductible W de G apparaît dans la représentation régulière de G avec une multiplicité égale à son degré $\dim(W)$. *En particulier, $|G| = \Sigma_W dim(W)^2$, où W parcourt l'ensemble des classes d'isomorphisme de représentations irréductibles de G.*

Démonstration: i) + ii) découle du thm. 2.i et des relations d'orthogonalité.
iii) Le caractère r de la représentation régulière R vérifie $r(1) = |G|$, et $r(g) = 0$ pour tout $g \neq 1$. Pour toute repr. W de G, on a donc : $(r, \chi_W) = |G|^{-1}(r(1)\chi_W(1)^* + 0) = \dim(W)$. Si W est irréductible, et si R est isomorphe à $W_1^{\oplus a_1} \oplus ... \oplus W_k^{\oplus a_k}$, on déduit alors des relations d'orthogonalité que W est isomorphe à l'un des W_i , avec $a_i = \dim(W)$.

Cette dernière conclusion montre que G n'a qu'un nombre fini de classes d'isomorphisme de représentations irréductibles. En fait, il y en a exactement $cl(G)$ (qui est la dimension de $\mathcal{F}^{cent}(G, \mathbf{C})$). En effet:

Théorème 4: *les caractères des différentes classes d'isomorphismes de représentations irréductibles de G forment une base de l'espace des fonctions centrales sur G. Il y en a donc autant que de classes de conjugaison du groupe G.*

Démonstration: il s'agit de voir que la seule fonction centrale f telle que $(f, \chi_V) = 0$ pour toute repr. irréd. V, est la fonction nulle. Pour une telle V, posons $\phi_V = \Sigma_{g \in G} f(g)\rho_V(g)$. Comme f est centrale, on voit que ϕ est un G-morphisme de V dans V, donc par Schur, une homothétie, et puisque sa trace $|G|(f, \chi_V^*)$ est nulle , $\phi_V = 0$. Donc l'endomorphisme $\Sigma_{g \in G} f(g)R(g)$ de l'espace $\mathcal{F}(G, \mathbf{C})$ de la représentation régulière est identiquement nul. Ses vecteurs $R(g)(e_1) = e_g$ étant $\mathbf{C}$-lináirement indépendantes, $f(g)$ est bien nul pour tout g dans G .

Exemples, exercices, etc

1. Montrer que la représentation régulière R est conjuguée à la représentation R' définie (en termes de fonctions sur G) par $R'(g)f : h \mapsto R'(g)(f)(h) := f(hg)$.
2. Soit V/K une représentation de degré fini d'un groupe G. Définir la représentation associée à l'espace $S^2(V^*)$ (resp. $\Lambda^2(V^*)$) des formes K-bilinéaires symétriques (resp.

alternées) sur V. Si $car(K) \neq 2$, montrer qu'une forme bilinéaire symétrique b est un invariant si et seulement si la forme quadratique associée $q(v) = b(v, v)$ vérifie : $q(g.v) = q(v)$ pour tout (g, v) dans $G \times V$.

3. i) Trouver un contre-exemple à la deuxième assertion de Schur lorsque $K = \mathbf{R}$.

ii) Soit L un corps gauche de centre K, de dimension finie sur K. Montrer que si K est algébriquement clos, L coïncide avec K. En déduire une "autre" preuve de Schur.

4. i) Démontrer Maschke en supposant que $K = \mathbf{C}$ et que V est muni d'un produit scalaire (i.e. d'une forme hermitienne définie positive) invariante sous G.

ii) Montrer par un procédé de moyenne que cette dernière condition est automatiquement vérifiée si V est de dimension finie. Ainsi, pour un choix convenable de base, l'image de toute repr. complexe de degré n est contenue dans le groupe unitaire $U_n(\mathbf{C})$.

iii) Soient $K = \mathbf{F}_p$ le corps à p éléments, et G le sous-groupe de $GL_2(\mathbf{F}_p)$ formé par les matrices triangulaires supérieures. Montrer que la représentation naturelle $V = \mathbf{F}_p^2$ de G est indécomposable, mais pas irréductible. Pourquoi ceci ne contredit-il pas Maschke ?

5. Soit (V, ρ) une représentation sur un corps K d'un groupe fini G.

i) Soit g un élément de G. Montrer que l'endomorphisme $\rho(g)$ de V est G-linéaire si (et lorsque ρ est fidèle, seulement si) g appartient au centre de G.

ii) Supposons que G est abélien, que $K = \mathbf{C}$ et que V est irréductible. Montrer que V est de dimension 1. Ainsi, les représentations complexes irréductibles d'un groupe abélien fini sont données par les homomorphismes de G dans $\mathbf{C}^*$ (i.e. par les caractères de G).

iii) Montrer qu'un groupe fini non abélien admet des représentations complexes irréductibles de dimension > 1 .

6 Soient V une représentation complexe irréductible de dimension finie d'un groupe G , et b une forme bilinéaire sur $V \times V$, invariante sous G et non nulle.

i) Montrer que b est non dégénérée.

ii) Soit b' une seconde forme bilinéaire sur $V \times V$, invariante sous G . Montrer qu'il existe $\ell \in \mathbf{C}$ tel que $b' = \ell b$.

iii) Montrer que b est ou bien symétrique, ou bien alternée.