Groupes finis et leurs représentations

Antoine Ducros

Guide du cours de M1 dispensé à l'Université Paris 6

Année universitaire 2011-2012

Introduction

Ce cours va illustrer, autour d'une notion fondamentale que vous connaissez déjà – celle de groupe – , un principe très général en mathématiques : celui du va-et-vient permanent entre les points de vue ≪abstrait≫ et ≪concret≫ sur une même classe d'objets. C'est une démarche que vous avez par exemple rencontrée en algèbre linéaire, avec l'opposition entre les espaces vectoriels abstraits et les sous-espaces vectoriels de k^n (ou, si vous préférez, le calcul en coordonnées), et que vous retrouverez également en géométrie différentielle, où vous travaillerez tantôt avec des variétés différentielles ≪intrinsèques≫ (point de vue abstrait) tantôt avec des sous-variétés de $\mathbb{R}^n$ (point de vue concret).

Expliquons maintenant plus en détail ce qu'il en est concernant les groupes.

Les groupes de transformation

Les premiers groupes que les mathématiciens ont considérés, avant que la définition axiomatique que nous connaissons aujourd'hui ne soit dégagée, étaient des *groupes de transformations*, c'est-à-dire que l'on considérait un ensemble X, et un ensemble G de bijections de X dans X possédant les propriétés suivantes : l'identité de X appartient à G ; si g et h sont deux éléments de G alors $g \circ h$ appartient à G ; et si g est un élément de G sa bijection réciproque g^{-1} appartient à G.

De tels groupes de transformations sont apparus dans différents contextes : en géométrie par exemple, avec le groupe des applications linéaires ou des isométries du plan ou de l'espace, ou avec celui des isométries fixant un cube ou un tétraèdre... ; mais aussi en algèbre, où Galois a introduit, un polynôme P étant donné (disons à coefficients dans $\mathbb{Q}$), un certain groupe de permutations de l'ensemble des racines complexes de P (que l'on appelle aujourd'hui justement le *groupe de Galois*) dont il s'est servi pour caractériser les polynômes P dont les racines *ne peuvent pas* être exprimées au moyen d'une formule en les coefficients [1].

1. Il faut savoir précisément ce qu'on entend par ≪formule≫, bien entendu. Ici, on s'intéresse aux polynômes P tels qu'aucune racine de P ne puisse s'exprimer à partir des coefficients de P *en utilisant les quatre opérations et les racines n-ièmes*, contrairement à ce que l'on sait toujours faire en degré 2, *via* l'expression bien connue $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

La notion de groupe abstrait

Ces différents exemples ont progressivement amené les mathématiciens à dégager une notion de groupe abstrait selon le principe suivant : on remplace l'ensemble concret de bijections, au sein duquel on sait composer des éléments, par un ensemble abstrait G *muni* d'une loi de composition interne (l'adjectif ≪muni≫ signifie que cette loi *fait partie des données*), qui satisfait un certain nombre d'*axiomes* vérifiés par la composition des applications dans le cas des groupes de transformations : associativité, existence d'un élément neutre, existence d'un symétrique.

Cette démarche – axiomatiser les propriétés de certains objets concrets que l'on manipule depuis longtemps – ne s'est bien évidemment pas limitée aux groupes, elle a peu ou prou concerné toutes les mathématiques au début du XXième siècle : citons par exemple l'arithmétique (avec les notions d'anneau, de corps, d'idéal), l'algèbre linéaire (avec la notion d'espace vectoriel) ou encore la topologie (avec la notion d'espace topologique) ; elle est devenue plus ou moins systématique aujourd'hui.

Elle permet de clarifier les idées en dégageant les propriétés qui ne découlent que des axiomes choisis, et pas d'aspects plus spécifiques aux objets concrets considérés jusqu'alors ; elle aide, en ce sens, à se concentrer sur l'essentiel et à ne pas s'encombrer l'esprit avec des hypothèses parasites.

Opérations et représentations linéaires : une revanche du point de vue concret

Cela dit, il est très vite apparu qu'une des meilleures manières de comprendre un groupe *abstrait* G est de le *voir* comme un groupe de transformations au sens donné plus haut. En termes techniques, cela veut dire qu'on cherche un ensemble X et un isomorphisme entre G et un sous-groupe du groupe S_X des bijections de X dans lui-même ; ou encore, ce qui revient au même, un homomorphisme *injectif* de G dans S_X.

En réalité, l'expérience montre qu'il n'est pas utile d'être si exigeant : certains homomorphismes non injectifs de G dans S_X peuvent être tout aussi intéressants. Se donner un tel homomorphisme permet encore de penser à un élément de G comme à une bijection de X dans lui-même, mais avec un bémol important : deux éléments différents de G peuvent induire la même bijection.

On est ainsi amené à s'intéresser, un ensemble X étant donné, à *tous* les homomorphismes de G dans S_X, que l'on appelle aussi les *opérations de G sur X*. Le paragraphe 2.1 du poly leur est consacré ; ses résultats seront appliqués plus tard à l'étude des sous-groupes de Sylow (§3.1).

Si k est un corps et X un k-espace vectoriel, il est fréquent qu'on se limite aux opérations *k-linéaires* de G sur X, c'est-à-dire aux homomorphismes de X dans S_X dont l'image est constituée d'applications k-linéaires, ou encore aux homomorphismes de G dans $\mathsf{GL}(X)$. Un tel homomorphisme est ce qu'on appelle une *représentation k-linéaire de G (d'espace sous-jacent X)* . Se donner une représentation k-linéaire de G d'espace sous-jacent X permet de voir un élément de G comme une bijection k-linéaire de X dans lui-même, avec le même bémol que ci-dessus : il peut arriver (dans le cas non injectif) que deux éléments différents de G induisent la même bijection linéaire.

Le chapitre 4 du poly est consacré à l'étude des représentations linéaires, avec une attention particulière portée aux représentations $\mathbb{C}$-linéaires des groupes finis, dont le $\mathbb{C}$-espace vectoriel sous-jacent est lui-même de dimension finie.

Groupes de transformation *versus* groupes abstraits : quelle conclusion ?

On pourrait avoir l'impression, au vu du paragraphe précédent, que la notion de groupe de transformations est finalement meilleure que celle de groupe abstrait puisque, chassée par la porte, elle revient aussitôt par la fenêtre *via* les opérations et représentations linéaires.

Mais attention : il est très fréquent, lorsqu'on s'intéresse à un groupe abstrait G, que l'on soit amené à considérer *différentes* opérations ou représentations de G. Autrement dit, s'il est souvent utile de voir G comme un groupe de transformations, il n'y a pas une unique façon de le faire, loin de là, et la pluralité des points de vue se révèle très féconde.

On pourra par exemple, selon les besoins, penser à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comme à un groupe de permutations de $\{1,2,3,4\}$ (en envoyant $(\overline{1},\overline{0})$ sur $(12)(34)$ et $(\overline{0},\overline{1})$ sur $(13)(24)$) ou un groupe d'isométries du plan (en envoyant $(\overline{1},\overline{0})$ sur la réflexion par rapport à (Ox), et $(\overline{0},\overline{1})$ sur la réflexion par rapport à (Oy)) [2].

Ainsi, les théories des opérations et représentations ne consistent pas à évincer les groupes abstraits pour revenir purement et simplement à la notion de groupe de transformations ; elles consistent à utiliser cette dernière pour attacher à chaque groupe abstrait une *multitude* de descriptions concrètes.

On observe ici un phénomène général en mathématiques : l'approche abstraite évite de sélectionner d'emblée, ou de privilégier artificiellement, un point de vue concret particulier sur un objet donné ; mais elle n'empêche nullement, à l'occasion, d'en adopter un qui soit pertinent vis-à-vis du problème étudié.

Vous aviez par exemple déjà rencontré ce genre de choses en algèbre linéaire abstraite : celle-ci fournit une approche conceptuelle, qui ne requiert pas de fixer arbitrairement une base ; mais vous pouvez fort bien le moment venu, en choisir une intelligemment – par exemple pour un calcul explicite.

1 Séance du 9 janvier 2012

Après une brève introduction, j'ai suivi le poly du début à la proposition 1.1.9 incluse, à quelques détails près que voici.

Définition 1.1.2 : je n'ai pas introduit – et n'utiliserai pas – la notation $\ll H < G \gg$ pour $\ll H$ est un sous-groupe de $G \gg$.

J'ai signalé que le sous-groupe $\langle S \rangle$ peut être décrit comme l'ensemble des produits de la forme $a_1 a_2 \dots a_n$, où les a_i appartiennent à $S \cup S^{-1}$ (en notant S^{-1} l'ensemble $\{g^{-1}\}_{g \in S}$. L'élément neutre est de cette forme : c'est le *produit*

2. Nous laissons le soin au lecteur de vérifier dans le premier (resp. le second) cas qu'il existe un unique homomorphisme de groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dans le groupe des permutations de $\{1,2,3,4\}$ (resp. dans le groupe des isométries du plan) prenant les valeurs requises sur $(\overline{1},\overline{0})$ et $(\overline{0},\overline{1})$; et que cet homomorphisme est injectif, ce qui permet ici de vraiment voir $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comme un groupe de transformations.

vide; dans le cas où S est non vide, on peut aussi l'écrire aa^{-1} pour n'importe quel élément a de S.

1.1.5 J'ai signalé que la classe à gauche xH s'interprète comme la classe d'équivalence de x pour la relation d'équivalence $\mathscr{R}$, dite de *congruence à gauche modulo* H, définie par la condition

$$x\mathscr{R}y \iff x^{-1}y \in H.$$

De façon analogue la classe à droite Hx s'interprète comme la classe d'équivalence de x pour la relation d'équivalence $\mathscr{S}$, dite de *congruence à droite modulo* H, définie par la condition

$$x\mathscr{S}y \iff yx^{-1} \in H.$$

On a $x\mathscr{R}y$ si et seulement si $x^{-1}\mathscr{S}y^{-1}$; par conséquent, la formule $xH \mapsto Hx^{-1}$, *a priori* ambigüe, a bien un sens et définit une bijection entre G/H et $H\backslash G$ (sans qu'il y ait besoin de supposer G fini).

1.1.7. J'ai remplacé la définition du poly par la proposition-définition suivante. *Soit G un groupe et soit H un sous-groupe de G. Les assertions suivantes sont équivalentes :*

i) il existe un groupe G' et un morphisme $f : G \to G'$ tel que $H = \mathrm{Ker}\, f$.
ii) pour tout $h \in H$ et tout $g \in G$ le produit ghg^{-1} appartient à H ;
iii) pour tout $g \in G$ on a $gH = Hg$;
iv) il existe une loi de groupe sur G/H telle que la flèche quotient $x \mapsto xH$ de G vers G/H soit un morphisme ; cette loi est alors la seule loi de groupe sur G/H qui ait cette propriété.

Lorsqu'elles sont satisfaites, on dit que H est distingué *dans G, et l'on écrit $H \lhd G$.*

Indiquons rapidement comment on démontre cette proposition. Il est immédiat que i)$\Rightarrow$ *ii*), et que ii) $\iff$ *iii*). Supposons que ii) est vraie, et nous allons montrer iv). Soient α et β deux éléments de G/H ; il existe $x \in G$ tel que $\alpha = xH$, et $y \in G$ tel que $\beta = yH$.

Unicité de la loi de groupe éventuelle. Si une telle loi de groupe existe, on a nécessairement

$$\alpha\beta = (xH)(yH) = (xy)H,$$

d'où l'unicité (remarquons que l'on n'a pas utilisé l'hypothèse ii) pour l'établir).

Existence de la loi de groupe cherchée. L'idée est d'utiliser la seule formule possible, exhibée ci-dessus, pour définir cette loi de groupe, et donc de *poser* $\alpha\beta = (xy)H$. Le problème est que $(xy)H$ dépend *a priori* du choix de x et y. Il faut montrer qu'il n'en est en réalité rien. Donnons-nous donc x' et y' tels que $x'H = xH$ et $y'H = yH$, c'est-à-dire tels que $x^{-1}x' \in H$ et $y^{-1}y' \in H$. Comme $x^{-1}x' \in H$, l'hypothèse ii) assure que $y^{-1}x^{-1}x'y \in H$. On a alors

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = \underbrace{y^{-1}x^{-1}x'y}_{\in H}\underbrace{y^{-1}y'}_{\in H} \in H.$$

Ainsi, $(x'y')H = (xy)H$, ce qu'on souhaitait établir.

Il reste à s'assurer que la loi ainsi définie fait bien de G/H un groupe, et que $G \to G/H$ est un morphisme. Ce dernier point découlera directement de la définition de notre loi, qui assure précisément que $(xH)(yH) = (xy)H$ pour tout couple (x, y) d'éléments de G.

La loi définie est associative. En effet, soient x, y et z des éléments de G. On a

$$(xH)((yH).(zH)) = (xH).((yz)H) = x(yz)H = (xy)zH$$
$$= ((xy)H).(zH) = ((xH).(yH)).(zH)$$

(toutes les égalités proviennent de la définition de la loi interne sur G/H, à l'exception de la troisième qui provient de l'associativité de la loi de G).

La loi admet $eH = H$ comme élément neutre. En effet, si $x \in G$ alors

$$(xH)(eH) = (xe)H = xH \text{ et } (eH)(xH) = (ex)H = xH.$$

Tout élément de G/H a un inverse. En effet, si $x \in G$ alors

$$(x^{-1}H)(xH) = (xx^{-1}H) = eH \text{ et } (xH)(x^{-1}H) = (xx^{-1}H) = eH.$$

Pour terminer la preuve il suffit maintenant de s'assurer que iv)⇒i). Supposons donc que iv) soit vraie. L'image de e dans G/H est alors le neutre de G/H, et n'est par ailleurs autre que la classe $eH = H$. Son image réciproque sur G par la flèche $G \to G/H$ est égale à H ; ainsi, ce dernier apparaît comme le noyau du morphisme $G \to G/H$, d'où i).

Remarque. On aurait pu tout aussi bien, dans ce qui précède, remplacer iv) par l'assertion identique concernant l'autre quotient $H\backslash G$. En fait, si $H \lhd G$, il résulte de iii) que $G/H = H\backslash G$.

Proposition 1.1.9. J'ai ajouté la remarque suivante : réciproquement, si f se factorise comme indiqué, alors $f(H) = \{e'\}$. On peut ainsi récrire la propriété universelle du quotient sous la forme suivante : $\overline{f} \mapsto \overline{f} \circ \pi$ *établit une bijection entre* $\mathrm{Hom}(G/H, G')$ *et l'ensemble des* $f \in \mathrm{Hom}(G, G')$ *tels que* $f(H) = \{e'\}$.

Autrement dit, *se donner un morphisme de G/H vers G', c'est se donner un morphisme de G vers G' qui est trivial sur H.* Cette dernière phrase doit être impérativement connue, et vous devez l'assimiler *comme un réflexe* : ce n'est pas dans le cerveau qu'il convient de la stocker, mais dans la moëlle épinière.

2 Séance du 16 janvier 2012

J'ai en gros suivi le poly de la proposition 1.1.10 jusqu'au théorème 1.2.3 (exclu), en rajoutant le lemme 1.3.2. Voici quelques précisions.

Quelle intuition se faire du quotient ? Il est fréquent en mathématiques qu'il y ait un certain écart entre la définition d'un objet et l'intuition qu'il convient de s'en faire ; cela ne signifie pas que la définition est mauvaise, mais que son rôle est avant tout *technique* (elle assure l'existence d'un objet ayant les propriétés requises, elle permet de raisonner rigoureusement avec celui-ci), et qu'elle ne permet pas de, ou disons ne suffit pas à, comprendre en profondeur ce qu'elle décrit.

C'est typiquement le cas en ce qui concerne les quotients : si l'on se contente de voir G/H comme un ensemble de classes d'équivalence (ce qu'il est *stricto sensu*), on risque très vite de ne plus rien comprendre à ce qui se passe, les classes d'équivalence étant elles-mêmes des sous-ensembles de G. Il vaut mieux y penser comme à un groupe construit à partir de G en *décrétant* que les éléments de H sont triviaux, et en n'imposant *aucune autre contrainte*, sinon bien sûr celles qui en découlent par la théorie générale des groupes.

J'ai rajouté en remarque que si G est un groupe abélien, tous ses sous-groupes sont distingués.

J'ai repoussé le paragraphe 1.1.13 au début de 1.2 (voir plus bas).

Paragraphe 1.1.4. J'ai donné l'essentiel des preuves des faits qui y sont énoncés. Les voici.

Soit $h \in G$ et soient g et g' deux éléments de G. On a

$$\mathrm{Int}(h)(gg') = hgg'h^{-1} = hgh^{-1}hg'h^{-1} = \mathrm{Int}(h)(g)\mathrm{Int}(h)(gg').$$

Par conséquent $\mathrm{Int}(h)$ est bien un morphisme de groupes de G dans lui-même.

Soient h et h' deux éléments de G et soit $g \in G$. On a

$$\mathrm{Int}(hh')(g) = hh'g(hh')^{-1} = hh'g(h')^{-1}h^{-1} = \mathrm{Int}(h)(\mathrm{Int}(h')(g)).$$

Par conséquent, $\mathrm{Int}(hh') = \mathrm{Int}(h) \circ \mathrm{Int}(h')$. Comme on a d'autre part

$$\mathrm{Int}(e) = g \mapsto ege^{-1} = g \mapsto g = \mathrm{Id},$$

il vient

$$\mathrm{Int}(h) \circ \mathrm{Int}(h^{-1}) = \mathrm{Int}(h^{-1}) \circ \mathrm{Int}(h) = \mathrm{Int}(e) = \mathrm{Id}.$$

Ainsi, le morphisme $\mathrm{Int}(h)$ est bijectif, de réciproque $\mathrm{Int}(h^{-1})$; c'est donc bien un élément de $\mathrm{Aut}(G)$, et la formule $\mathrm{Int}(hh') = \mathrm{Int}(h) \circ \mathrm{Int}(h')$ assure que $h \mapsto \mathrm{Int}(h)$ est un morphisme de groupes de G dans $\mathrm{Aut}(G)$.

En ce qui concerne la formule $f \circ \mathrm{Int}(h) \circ f^{-1} = \mathrm{Int}(f(h))$, voici comment elle se démontre. Soit $g \in G$. On a

$$f \circ \mathrm{Int}(h) \circ f^{-1}(g) = f(hf^{-1}(g)h^{-1}) = f(h)f(f^{-1}(g))f(h)^{-1}$$

$$= f(h)gf(h)^{-1} = \mathrm{Int}(f(h))(g),$$

d'où l'assertion.

J'ai rajouté la remarque suivante : si G est abélien alors $Z(G) = G$, par conséquent $\mathrm{Int}(G) = \{\mathrm{Id}\}$. J'ai mentionné qu'un sous-groupe caractéristique est toujours distingué. La réciproque est fausse : par exemple, prenons $G = (\mathbb{R}, +)$ et $H = \mathbb{Q}$. Comme G est abélien, H est distingué. Par contre, il n'est pas caractéristique : en effet, choisissons un réel irrationnel a (par exemple $a = \sqrt{2}$ ou $a = e$) ; l'application $x \mapsto ax$ est alors un automorphisme de $\mathbb{R}$ qui ne stabilise pas $\mathbb{Q}$, puisqu'il envoie 1 sur a qui est irrationnel.

Définition 1.1.15. Je l'ai énoncée un peu plus haut (avant les automorphismes intérieurs et extérieurs). Attention, il y a un oubli dans la définition du poly : un groupe G est simple *s'il n'est pas réduit à l'élément neutre* et s'il n'admet pas de sous-groupe distingué différent de G et de $\{e\}$.

Paragraphe 1.2. J'ai modifié l'ordre de présentation. Voici plus précisément ce que j'ai fait.

J'ai inséré le paragraphe 1.1.13 au début de cette section, en rajoutant quelques compléments :

- j'ai défini en général (sans supposer les G_i abéliens) $\coprod G_i$ comme le sous-ensemble de $\prod G_i$ formé des (g_i) tels que les $g_i = e_i$ pour presque tout i. J'ai signalé que $\coprod G_i$ est un sous-groupe distingué de $\prod G_i$, et que dans le cas où les G_i sont abéliens on le note plus volontiers $\bigoplus G_i$.

J'ai justifié comme suit cette notation : pour tout j, l'application de G_j dans $\bigoplus G_i$ qui envoie g sur (g_i) avec $g_i = g$ si $i = j$ et $g_i = e_i$ sinon est un morphisme injectif, qui permet d'identifier G_j à un sous-groupe de $\bigoplus G_i$. Modulo cette convention, tout élément g de G a une unique écriture sous la forme $\sum g_i$, où $g_i \in G_i$ pour tout i et où les g_i sont presque tous nuls (c'est indispensable pour que la somme est un sens, car *en algèbre, on ne sait faire que des sommes finies*) : il suffit de prendre pour g_i la i-ème composante de g, et l'on voit facilement que c'est le seul choix possible.

J'ai ensuite énoncé le premier lemme du paragraphe 1.2.1, mais sans exclure le cas nul, ce qui a donné l'énoncé suivant : si G est un sous-groupe de $\mathbb{Z}$ il est de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$. Je n'ai pas donné de preuve, en renvoyant à celle du poly. Elle ne couvre pas le cas $G = \{0\}$, qui se traite directement : il est égal à $0\mathbb{Z}$. Elle ne couvre pas non plus l'unicité, qui se démontre comme suit : si $G = \{0\}$ il ne peut être égal à $n\mathbb{Z}$ pour $n > 0$ (puisqu'il ne contient pas n) ; si $G \neq 0$ et s'il est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ alors $n \neq 0$ et n est nécessairement le plus petit entier strictement positif de G.

J'ai précisé que si $d \in \mathbb{N}$ alors $\mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}$ si $d = \{0\}$, et est de cardinal d sinon ; ses éléments sont $\overline{0}, \overline{1}, \ldots, \overline{d-1}$.

J'ai ensuite expliqué la chose suivante : si G est un groupe et si $g \in G$ alors l'application $\varphi : \mathbb{Z} \to G, n \mapsto g^n$ est un morphisme de groupes d'image $< g >$. Si d désigne l'unique élément de $\mathbb{N}$ tel que le noyau de ce morphisme soit égal à $d\mathbb{Z}$ alors φ induit un isomorphisme $\mathbb{Z}/d\mathbb{Z} \simeq < g >$. On distingue alors deux cas : ou bien $d = 0$, auquel cas $< g > \simeq \mathbb{Z}$ et g est d'ordre infini, ou bien $d > 0$, auquel cas $< g > \simeq \mathbb{Z}/d\mathbb{Z}$ et est de cardinal d ; ainsi, d est égal à l'ordre de g, et également au plus petit entier strictement positif n tel que $g^n = e$.

J'ai alors rappelé ce qu'était un anneau, et énoncé (sans preuve) le fait que si $(A, +\times)$ est un anneau (non nécessairement commutatif) l'ensemble A^* des éléments a de A pour lesquels il existe $b \in A$ tel que $ab = ba = 1$ est stable sous la loi $\times$ et que cette dernière en fait un groupe. J'ai rappelé, là encore sans preuve, la description de $(\mathbb{Z}/d\mathbb{Z})^*$, qui consiste en l'ensemble des classes $\overline{a}$ pour a premier à d. Lorsque $d = 0$ (auquel cas $a \wedge 0 = a$ pour tout a), on obtient ainsi la description de $\mathbb{Z}^*$: il est égal à $\{1, -1\}$. Lorsque $d > 0$ le cardinal de $(\mathbb{Z}/d\mathbb{Z})^*$ est le cardinal de l'ensemble des entiers compris entre 0 et $d-1$ et premiers à d ; on le note $\varphi(d)$, et certaines de ses propriétés sont rappelées dans le poly (page 6) et/ou seront étudiées en TD.

J'ai ensuite prouvé la chose suivante : soit $d \in \mathbb{N}$ et soit φ un automorphisme de $\mathbb{Z}/d\mathbb{Z}$. Il existe un unique élément α de $(\mathbb{Z}/d\mathbb{Z})^*$ tel que φ soit égal à l'automorphisme $m_\alpha : \beta \mapsto \alpha\beta$ de $\mathbb{Z}/d\mathbb{Z}$.

Voici la preuve.

Unicité de α. Si $\varphi = m_\alpha$ on a nécessairement $\alpha = m_\alpha(\overline{1}) = \varphi(\overline{1})$, d'où l'unicité.

Existence de α. Posons $\alpha = \varphi(\overline{1})$, et soit $a \in \mathbb{Z}$ tel que $\alpha = \overline{a}$. Soit $n \in \mathbb{Z}$. On a $\varphi(\overline{n}) = \varphi(n.\overline{1}) = n.\varphi(\overline{1}) = \overline{n}.\overline{a} = \overline{an} = \alpha\overline{n}$, et $\varphi = m_\alpha$.

Par ailleurs, si α et β sont deux éléments de $(\mathbb{Z}/d\mathbb{Z})^*$ alors pour tout γ appartenant à $\mathbb{Z}/d\mathbb{Z}$ on a

$$m_{\alpha\beta}\gamma = (\alpha\beta)\gamma = \alpha(\beta\gamma) = m_\alpha(m_\beta(\gamma)).$$

Ainsi $m_{\alpha\beta} = m_\alpha \circ m_\beta$. Par conséquent, $\alpha \mapsto m_\alpha$ établit un isomorphisme entre $(\mathbb{Z}/d\mathbb{Z})^*$ et $\mathrm{Aut}(\mathbb{Z}/d\mathbb{Z})$. Comme $\mathrm{Int}(\mathbb{Z}/d\mathbb{Z}) = \{\mathrm{Id}\}$ puisque $\mathbb{Z}/d\mathbb{Z}$ est abélien, on a aussi $\mathrm{Out}(\mathbb{Z}/d\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}/d\mathbb{Z}) \simeq (\mathbb{Z}/d\mathbb{Z})^*$. Notez le cas particulier $d = 0$: comme $\mathbb{Z}^* = \{1, -1\}$, on a $\mathrm{Aut}(\mathbb{Z}) = \mathrm{Out}(\mathbb{Z})\{\mathrm{Id}, -\mathrm{Id}\}$.

J'ai ensuite énoncé sans preuve le lemme chinois (page 6).

Soit G un groupe abélien *fini*, noté additivement. Pour tout $g \in G$, soit e_g l'ordre de g. Comme G est fini, $< g >$ est fini et e_g est donc strictement positif ; il est caractérisé par le fait que $ng = 0 \iff e_g | n$.

L'ensemble E formé des entiers relatifs n tels que $ng = 0$ pour tout $g \in G$ est un sous-groupe de $\mathbb{Z}$; qui est donc de la forme $e\mathbb{Z}$ pour un certain $e \in \mathbb{N}$ uniquement déterminé. Si $n \in \mathbb{Z}$ alors $n \in E$ si et seulement si $ng = 0$ pour tout $g \in G$, donc si et seulement si $e_g | n$ pour tout $g \in G$, donc si et seulement si n est divisible par le $PPCM$ des e_g. Ainsi, e est égal au PPCM des e_g ; il est donc non nul (chacun d'eux étant non nul), et divise le cardinal de G (puisque chaque e_g divise le cardinal de G). On dit que e est *l'exposant* de G.

Lemme. Soient g et h deux éléments de G tels que e_g et e_h soient premiers entre eux. On a alors $e_{g+h} = e_g e_h$.

Démonstration. On a $e_g e_h (g + h) = 0$ puisque $e_g g = 0$ et $e_h h = 0$. Soit n un entier tel que $n(g + h) = 0$; nous allons montrer que $e_g e_h | n$, ce qui permettra de conclure.

On a $ng = -nh$. Par conséquent, $ng \in < g > \cap < h >$. Comme e_g et e_h sont strictement positifs, $< g >$ est de cardinal e_g et $< h >$ de cardinal e_h. De ce fait, le cardinal du groupe $< g > \cap < h >$ divise à la fois e_g et e_h. Ceux-ci étant premiers entre eux, ce cardinal est égal à 1, ce qui signifie que $< g > \cap < h >= \{0\}$. Par conséquent, $ng = -nh = 0$. Il s'ensuit que n est multiple de e_g et de e_h ; en utilisant une fois encore le fait qu'ils sont premiers entre eux, on voit qu'il est multiple de $e_g e_h$, ce qui achève la démonstration.

Proposition (lemme 1.3.2 du poly, avec une preuve un peu différente). Il existe un élément g de G tel que $e_g = e$.

Démonstration. L'entier e étant non nul, il admet une écriture $\prod p_i^{n_i}$ où les p_i sont des nombres premiers deux à deux distincts. Fixons i. Comme e est le PPCM des e_g pour $g \in G$, l'entier n_i est la plus grande valeur prise par l'exposant de p_i dans la décomposition de e_g, pour g parcourant G. Il existe donc $g_i \in G$ tel que $e_{g_i} = p_i^{n_i} q_i$, avec q_i premier à p_i. Posons $h_i = q_i g_i$. On a alors $e_{h_i} = p_i^{n_i}$. En effet, si $n \in \mathbb{Z}$ on a

$$nh_i = 0 \iff nq_i g_i = 0 \iff e_{g_i} | nq_i \iff p_i^{n_i} q_i | nq_i \iff p_i^{n_i} | n.$$

On a ainsi construit une famille (h_i) d'éléments de G tels que $e_{h_i} = p_i^{n_i}$ pour tout i. Posons $g = \sum h_i$. Comme les $p_i^{n_i}$ sont deux à deux premiers entre eux, le

lemme ci-dessus couplé à une récurrence immédiate assure que $e_g = \prod p_i^{n_i} = e$, CQFD.

Corollaire (proposition de la page 7 du poly, avec une preuve différente). Soit K un corps (commutatif) et soit G un sous-groupe fini de K^*. Le groupe G est cyclique.

Démonstration. Soit e l'exposant de G. On sait qu'il divise $|G|$, et la proposition ci-dessus assure l'existence de $g \in G$ tel que $g^e = 1$ (attention : comme $G \subset K^*$ on utilise la notation multiplicative). Par définition de e, on a $h^e = 1$ pour tout $h \in G$. Autrement dit, G est contenu dans l'ensemble des racines du polynôme $X^e - 1$. Celui-ci étant de degré e, il a au plus e racines dans K. Par conséquent, $|G| \leqslant e$. Puisque e divise $|G|$, on a $|G| = e$. L'ordre de g étant égal à e on a $< g >= G$, et G est donc cyclique, CQFD.

3 Séance du 23 janvier 2012

J'ai commencé par énoncer le théorème 1.3.1 sans le démontrer (et sans supposer $G \neq \{0\}$: le théorème reste en effet vrai si $G = \{0\}$, la famille d'entiers à considérer étant alors la *famille vide*).

J'ai continué avec le paragraphe 1.2.4, en en détaillant certains points.

J'ai défini les cycles, les transpositions et le support d'une permutation sur n'importe quel ensemble X. Les définitions sont les mêmes que celles en haut de la page 9, à ceci près que je ne suppose pas que $X = \{1, \ldots, n\}$; les i_k sont donc des éléments de X, et pas (forcément) des entiers. De même, j'ai introduit la notation d'une permutation qui figure au bas de la page 8, mais en remplaçant $1, \ldots, n$ par les éléments de X (lorsque X est fini). Dans ma définition d'un cycle, j'ai exclu le cas de l'identité (la longueur d'un cycle est toujours au moins 2).

J'ai précisé que si X et Y sont deux ensembles, toute bijection $\varphi : X \to Y$ induit un isomorphisme naturel de groupes $S_X \simeq S_Y$ qui est donné par la formule $g \mapsto \varphi \circ g \circ \varphi^{-1}$. Exemple : supposons que $X = \{a, b, c, d, e\}$ et que $Y = \{1, 2, 3, 4, 5\}$; soit φ la bijection $a \mapsto 2, b \mapsto 1, c \mapsto 4, d \mapsto 3, e \mapsto 5$, et soit g la permutation

$$\begin{pmatrix} a & b & c & d & e \\ b & a & e & d & c \end{pmatrix}.$$

La bijection $\varphi \circ g \circ \varphi^{-1}$ de Y est celle qui se déduit intuitivement, sans même connaître la formule, des données ci-dessus, par le procédé très simple suivant : on prend un élément de Y, on regarde à quel élément de X il correspond (application de φ^{-1}), on lui applique g, puis on regarde à quel élément de Y correspond ce nouvel élément de X (application de φ). On trouve

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}.$$

J'ai mentionné sans preuve la formule

$$\varphi(a_1, a_2, \ldots a_n)\varphi^{-1} = (\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)).$$

Lorsque X est fini, le cardinal de S_X ne dépend par ce qui précède que du cardinal de X. J'ai proposé la présentation suivante de la factorielle : on *définit*

$n!$ comme le cardinal de S_X pour X de cardinal n. On démontre alors que $0! = 1$ et que $(n+1)! = (n+1)n!$ pour tout n.

Voici la preuve. On a $S_\emptyset = \{\mathrm{Id}_\emptyset\}$ (en effet, quel que soit l'ensemble E, il existe un et une seule application de $\emptyset$ dans E, à savoir l'inclusion ; elle est bijective si et seulement si $E = \emptyset$, auquel cas elle coïncide avec l'identité) ; par conséquent, $0! = 1$.

Fixons maintenant n, et soit G le sous-groupe de S_{n+1} formé des permutations qui fixent $n+1$. Tout élément de G induit une permutation de $\{1, \ldots, n\}$ par restriction, et toute permutation de $\{1, \ldots, n\}$ se prolonge en un élément de G (en décrétant qu'il fixe $n+1$). On définit par ce procédé un isomorphisme $G \simeq S_n$.

On a $|S_{n+1}| = |G|.[S_{n+1} : G] = |S_n|.[S_{n+1} : G]$. Autrement dit,

$$(n+1)! = [S_{n+1} : G].n! \ .$$

Pour conclure, il reste à s'assurer que $[S_{n+1} : G] = n+1$.

Soient σ et τ deux éléments de S_{n+1}. On a les équivalences

$$\tau^{-1}\sigma \in G \iff \tau^{-1}(\sigma(n+1)) = n+1 \iff \sigma(n+1) = \tau(n+1).$$

L'application

$$S_{n+1} \to \{1, \ldots, n+1\}, \sigma \mapsto \sigma(n+1)$$

est surjective ($\mathrm{Id}(n+1) = n+1$, et si $i \neq n+1$ alors $(i, n+1)(n+1) = i$). Par ce qui précède, elle induit une bijection $S_{n+1}/G \simeq n+1$. Ainsi, $[S_{n+1} : G] = n+1$, ce qu'on voulait établir.

J'ai énoncé l'existence et l'unicité de la décomposition d'une permutation σ d'un ensemble fini X en produit de cycles à supports deux à deux disjoints. La preuve que j'en ai donnée est essentiellement celle du poly (assertion i) de la proposition de la page 9), avec un peu plus de détails. La voici.

L'uncité. Supposons que σ s'écrive $\prod c_i$ où les c_i sont des cycles à supports deux à deux disjoints ; nous allons montrer comment reconstituer la liste des c_i à partir de σ, ce qui établira leur unicité.

La réunion des supports des c_i coïncide nécessairement avec le support de σ. Soit a appartenant au support de σ. Le cycle dans lequel il figure est nécessairement égal à $(a, \sigma(a), \ldots, \sigma^{d-1}(a))$ où d est le plus petit élément de $\{n \in \mathbb{N}^*, \sigma^n(a) = a\}$. Ainsi, la liste des c_i se reconstitue bien à partir de σ.

L'existence. On note n le cardinal de X, et F l'ensemble des points fixes de σ. On raisonne par récurrence *descendante* sur le cardinal de F. Si F est de cardinal n alors tout point de X est fixe, et $\sigma = \mathrm{Id}_X$. On peut l'écrire comme le *produit vide* de cycles, et la propriété est vraie.

Supposons que le cardinal de F est strictement inférieur à n, et que la propriété est vraie en cardinal strictement plus grand. Comme le cardinal de F est strictement inférieur à n, la permutation σ admet au moins un point non fixe a. L'ensemble des entiers relatifs n tels que $\sigma^n(a) = a$ est un sous-groupe de $\mathbb{Z}$, qui est donc de la forme $d\mathbb{Z}$ pour un unique $d \in \mathbb{N}$. Comme X est fini σ est d'ordre fini, et d est donc strictement positif. Comme a n'est pas un point fixe, $d \geqslant 2$.

Si i et j sont deux entiers tels que $0 \leqslant i < j \leqslant d-1$ on a $\sigma^i(a) \neq \sigma_j(a)$ puisque $0 < j - i < d$. Par conséquent, les éléments $a, \sigma(a), \ldots, \sigma_{d-1}(a)$ de X

sont deux à deux distincts et $(a, \sigma(a), \ldots, \sigma_{d-1}(a))$ est un cycle c bien défini, de longueur d.

Posons $\tau = \sigma c^{-1}$. Soit $b \in F$. Il n'appartient pas à $\{a, \sigma(a), \ldots, \sigma_{d-1}(a)\}$ (aucun des éléments de cet ensemble n'est fixe par σ). Par conséquent $c^{-1}(b) = b$ et $\tau(b) = b$. Par ailleurs si $i \in \{0, \ldots, d-1\}$ alors $c^{-1}(\sigma^i(a)) = \sigma^{i-1}(a)$; il s'ensuit que $\tau(\sigma^i(a)) = \sigma(\sigma^{i-1}(a)) = \sigma^i(a)$. Ainsi, l'ensemble F' des points fixes de τ contient la réunion disjointe de F et de l'ensemble non vide $\{a, \sigma(a), \ldots, \sigma_{d-1}(a)\}$. Il est donc de cardinal strictement supérieur à celui de F. Par notre hypothèse de récurrence, τ s'écrit comme un produit $c_1 \ldots c_r$ où les c_i sont des cycles à supports deux à deux disjoints. Comme $\{a, \sigma(a), \ldots, \sigma^{d-1}(a)\}$ est contenu dans l'ensemble des points fixes de τ, il ne rencontre aucun des supports des c_i ; le support de c est donc disjoint de celui de chacun des c_i. Par définition $\tau = \sigma c^{-1}$. Il vient $\sigma = \tau c = c_1 \ldots c_r c$, ce qui achève la preuve.

J'ai ensuite mentionné l'écriture d'une permutation d'un ensemble fini comme produit de transpositions, grâce à la décomposition en cycles et à l'égalité

$$(a_1, \ldots, a_n) = (a_1, a_2)(a_2, a_3) \ldots (a_{n-1}, a_n)$$

(c'est l'assertion ii) de la proposition de la page 9 ; je n'ai pas énoncé iii) et iv) explicitement dans le cours).

En ce qui concerne la signature, j'ai démontré son existence, sous la forme suivante.

Théorème. Soit X un ensemble fini. Il existe un unique morphisme de groupes $\varepsilon : S_X \to \{-1, 1\}$, appelé *signature*, qui est tel que $\varepsilon(\tau) = -1$ pour toute transposition τ. Il est surjectif si et seulement si le cardinal de X est supérieur ou égal à 2.

Démonstration. L'unicité vient du fait que toute permutation est un produit de transpositions. Supposons avoir démontré l'existence de la signature. Si X est vide ou un singleton, $S_X = \{\mathrm{Id}_X\}$ et ε a nécessairement pour image $\{1\}$. Si le cardinal de X est supérieur ou égal à 2 il existe deux éléments a et b distincts dans X ; l'image de $\tau_{a,b}$ par ε vaut alors -1, et ε est surjective.

Il reste donc à prouver l'existence de ε. Pour cela, on peut supposer que $X = \{1, \ldots, n\}$ (en utilisant une bijection quelconque entre X et $\{1, \ldots, n\}$, et les remarques faites plus haut). On aura besoin de la convention suivante : si $\sigma \in S_n$, on note encore σ l'endomorphisme de $\mathbb{Z}[X_1, \ldots, X_n]$ qui envoie X_i sur $X_{\sigma(i)}$ pour tout i. On a $\sigma(\tau(Q)) = (\sigma\tau)(Q)$ pour tout $Q \in \mathbb{Z}[X_1, \ldots, X_n]$.

Soit P le polynôme $\prod_{i>j} X_i - X_j$. On a

$$P^2 = \prod_{i>j} (X_i - X_j)^2 = \prod_{i>j} (X_i - X_j)(X_j - X_i)(-1) = (-1)^{n(n-1)/2} \prod_{i \neq j} X_i - X_j.$$

Cette dernière égalité montre que $\sigma(P)^2 = \sigma(P^2) = P^2$ pour toute $\sigma \in S_n$, et donc que $\sigma(P) = \varepsilon(\sigma)P$ pour tout $\sigma \in S_n$, où $\varepsilon(\sigma) \in \{-1, 1\}$. On déduit aisément de l'égalité $\sigma(\tau(P)) = (\sigma\tau)(P)$ que ε est un morphisme de groupes de S_n vers $\{-1, 1\}$.

Il suffit maintenant de vérifier que ε prend la valeur -1 sur toute transposition. Si $n = 0$ ou 1 alors $S_n = \{\mathrm{Id}\}$, et ne possède pas de

transposition. L'assertion requise est donc trivialement vraie[3] ; nous allons maintenant supposer que $n \geqslant 2$.

Calcul de $\varepsilon(1,2)$. On a

$$P = \prod_{i>j} X_i - X_j = (X_2 - X_1) \prod_{i>2} (X_i - X_1) \prod_{i>2} (X_i - X_2) \prod_{i>j>2} X_i - X_j.$$

Lorsqu'on applique la transposition $(1,2)$ à P, on trouve

$$(X_1 - X_2) \prod_{i>2} (X_i - X_2) \prod_{i>2} (X_i - X_1) \prod_{i>j>2} X_i - X_j,$$

c'est-à-dire $(-P)$. En conséquence, $\varepsilon(1,2) = -1$.

Soient maintenant a et b deux entiers distincts compris entre 1 et n. Choisissons une permutation $\sigma \in S_n$ envoyant a sur 1 et b sur 2. On a l'égalité $\sigma(a,b)\sigma^{-1} = (1,2)$, et donc $\varepsilon(\sigma)\varepsilon(a,b)\varepsilon(\sigma)^{-1} = \varepsilon(1,2) = -1$. Mais comme $\{-1,1\}$ est commutatif, $\varepsilon(\sigma)\varepsilon(a,b)\varepsilon(\sigma)^{-1} = \varepsilon(a,b)$. Ainsi, $\varepsilon(a,b) = -1$, ce qui achève la démonstration.

Soit X un ensemble fini et soit $\sigma \in S_X$. Supposons que l'on ait deux égalités

$$\sigma = \tau_1 \dots \tau_r \text{ et } \sigma = \tau'_1 \dots \tau'_s$$

où les τ_i et les τ'_j sont des transpositions. On a alors $r = s$ modulo 2 ; en effet, par ce qui précède on peut écrire $\varepsilon(\sigma) = (-1)^r = (-1)^s$.

J'ai terminé ce paragraphe en donnant la définition de A_n (bas de la page 9).

Groupes opérant sur un ensemble

J'ai commencé ce paragraphe, en traitant essentiellement 2.1.1, 2.1.2, et une partie du 2.1.3 ; j'ai parfois rajouté un ou deux commentaires. Voici quelques détails.

Déf. 2.1.1. J'ai donné celle du poly, en rajoutant la remarque suivante : une opération à droite de G sur un ensemble X correspond à un morphisme de G^{op} vers S_X, où G^{op} est le groupe ayant même ensemble sous-jacent que G, et dont la loi $*$ est définie par la formule $g * h = hg$ (on renverse le sens du produit).

J'ai signalé que la phrase ≪Soit G un groupe opérant sur un ensemble X≫ signifie que *l'on s'est donné* une opération de G sur X.

J'ai indiqué deux faits triviaux : si G opère sur X et si Y est une partie de X stable sous G alors G opère sur Y par restriction ; si H est un sous-groupe de G alors H opère sur X par restriction.

Paragraphe 2.1.2 et une partie du paragraphe 2.1.3. J'ai simplement défini gY comme $\{g.y, y \in Y\}$ (mais pas AY en général) et indiqué que $(g,Y) \mapsto gY$ définit une opération de G sur $\mathscr{P}(X)$. J'ai défini les orbites, et signalé qu'elles étaient exactement les classes d'équivalence de la relation $\mathscr{R}$ définie par la condition

$$x \mathscr{R} y \iff \exists g \in G \; y = g.x.$$

3. Toute assertion de la forme $\forall x \in \emptyset \; \mathscr{P}(x)$ (où $\mathscr{P}$ est une proposition quelconque) est vraie, puisque sa négation est $\exists x \in \emptyset$, non$\mathscr{P}(x)$ qui est fausse : il n'existe aucun élément dans l'ensemble vide.

J'ai défini le stabilisateur d'un point et ai montré que si $x \in X$ et si $y = gx$ alors $G_y = gG_xg^{-1}$ (ce n'est signalé qu'un peu plus tard dans le poly, au 2.1.5) ; en particulier si G_x est distingué tous les éléments de l'orbite de x ont même stabilisateur (mais lorsque G_x n'est pas distingué, c'est faux). J'ai défini les notions d'opération fidèle, et d'opération transitive. J'ai signalé que lorsque G opère fidèlement sur X, l'injection $G \hookrightarrow S_X$ permet d'identifier G à un sous-groupe de S_X.

4 Séance du 30 janvier 2012

Groupes opérant sur un ensemble, suite

J'ai poursuivi et terminé le paragraphe 2.1.3. J'ai donné de surcroît la démonstration du fait suivant : l'ensemble $\{g \in G, gY \subset Y\}$ est un groupe si et seulement si il coïncide avec G_Y. En effet, il est clair que s'il coïncide avec G_Y c'est un groupe. Réciproquement, supposons que ce soit un groupe ; comme il contient G_Y, nous allons montrer qu'il est contenu dans celui-ci, et cela prouvera qu'ils sont égaux.

Soit donc 0 tel que $g_0Y \subset Y$. Comme $\{g \in G, gY \subset Y\}$ est un groupe, il contient g_0^{-1}, ce qui veut dire $g_0^{-1}Y \subset Y$. En appliquant g_0, il vient $Y \subset g_0Y$; par conséquent, $g_0Y = Y$ et $g_0 \in G_Y$, ce qu'il fallait démontrer.

J'ai indiqué deux cas dans lesquels $\{g \in G, gY \in Y\}$ coïncide avec G_Y : celui où Y est fini (qui figure dans le paragraphe 1.2.3 du poly), qui se traite en remarquant que sous cette hypothèse le cardinal de gY est égal à celui de Y (puisque $y \mapsto gy$ est bijective), et donc que l'inclusion $gY \subset Y$ entraîne l'égalité $g_Y = Y$; et celui où X est un espace vectoriel sur un corps k, où $x \mapsto gx$ est k-linéaire pour tout g, et où Y est un sous-espace vectoriel de dimension finie de X (l'argument est le même à ceci près qu'il faut remplacer le cardinal par la dimension).

Les exemples du 2.1.4. Je les ai traités (sans introduire l'expression ≪classe de conjugaison≫, ce qui sera fait prochainement en cours et/ou en TD) ; et en ne parlant de normalisateur et de centralisateur que pour un sous-groupe de G.

J'ai par contre donné un détail supplémentaire à propos de l'exemple i) : j'ai signalé que l'action de G sur lui-même par translation à gauche est transitive (si $g \in G$ alors $g = ge$ et g appartient donc à l'orbite de e), et fidèle (puisque les stabilisateurs sont tous triviaux), et qu'elle définit ainsi un plongement de G dans S_G. Corollaire : tout groupe fini est isomorphe à un sous-groupe de S_n pour un certain n.

Ce résultat est parfois appelé ≪théorème de Cayley≫, mais me semble trop trivial pour vraiment mériter le nom de théorème. Mentionnons par ailleurs que son intérêt pratique est plus faible que ce que l'on pourrait croire : il semble permettre de ramener l'étude des groupes à celle des sous-groupes de S_n, mais on se rend compte avec l'expérience que ce n'est pas un problème plus simple !

On dispose de résultats analogues pour l'action de G sur lui-même par translations à droite ; leurs énoncés précis sont laissés au lecteur.

J'ai également rajouté un exemple qui n'est pas traité au paragraphe 2.1.4, et généralise i). Soit G un groupe et soit H un sous-groupe de G. L'opération

à gauche de H sur G par translations s'étend en une opération à gauche de H sur $\mathscr{P}(G)$. Si $g' \in G$ alors

$$g.(g'H) = \{g\gamma\}_{\gamma \in g'H} = \{gg'h\}_{h \in H} = (gg')H.$$

Ainsi, G/H est stable sous l'action de G, et l'action de G à gauche sur G/H est donnée par la formule $g(g'H) = (gg')H$.

Cette action est transitive : si $g \in G$ alors $gH = g(eH)$, et gH appartient donc à l'orbite de la classe triviale $eH = H$.

Elle n'est par contre pas fidèle en général ; nous allons plus précisément décrire le noyau de la flèche $G \to S_{G/H}$ qu'elle induit.

Le stabilisateur de la classe triviale $eH = H$ est égal à $\{g \in G, gH = H\}$ c'est-à-dire à H. Soit maintenant $g \in G$. Comme $gH = g(eH)$, le stabilisateur de la classe gH est égal à gHg^{-1}, en vertu de la formule vue à la fin du cours précédent.

Le noyau de $G \to S_{G/H}$ est alors égal $\bigcap_{g \in G} gHg^{-1}$. On vérifie immédiatement que c'est le plus grand sous-groupe distingué de G contenu dans H.

On dispose de résultats analogues pour l'action de G sur lui-même par translations à droite ; leurs énoncés précis sont laissés au lecteur.

Cardinal d'une orbite et formule de Burnside

J'ai démontré la formule donnée au paragraphe 2.1.5 ($|Gx| = [G : G_x]$) mais n'ai pas traité la suite de ce paragraphe. J'ai par contre raffiné un peu le résultat sur le cardinal de l'orbite, comme suit.

Commençons par un peu de vocabulaire : soit G un groupe opérant sur deux ensembles X et Y. Une application $\varphi : Y \to X$ est dite *équivariante* si $\varphi(gx) = g\varphi(x)$ pour tout $(g, x) \in G \times X$; si φ est une bijection équivariante, sa réciproque est également équivariante.

Soit maintenant G opérant sur un ensemble X et soit $x \in X$. L'application $g \mapsto gx$ induit une surjection $G \to Gx$. De plus, si g et g' sont deux éléments de G, on a $gx = g'x$ si et seulement si $g^{-1}g' \in G_x$; par conséquent, $g \mapsto gx$ induit une bijection $G/G_x \to Gx$. On vérifie immédiatement que cette bijection est *équivariante*.

Lorsque G est fini, il s'ensuit que Gx est fini de cardinal $[G : G_x]$.

À la place du paragraphe 2.1.6 j'ai démontré la *formule de Burnside* : si X est un ensemble fini sur lequel opère un groupe fini G, et si l'on désigne par $\mathrm{Fix}(g)$, pour tout $g \in G$, l'ensemble des points fixes de g dans X alors

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = |G\backslash X|.$$

La preuve est la suivante : soit E l'ensemble des couples $(g, x) \in G \times X$ tels que $gx = x$. Son cardinal est égal de façon évidente à $\sum_{g \in G} |\mathrm{Fix}(g)|$. Mais il s'écrit aussi

$$\sum_{x \in X} |G_x| = \sum_{\mathscr{O} \in G\backslash X} \sum_{x \in \mathscr{O}} |G_x| = \sum_{\mathscr{O} \in G\backslash X} \sum_{x \in \mathscr{O}} \frac{|G|}{|\mathscr{O}|}$$

$$= |G| \sum_{\mathscr{O}\in G\backslash X} \sum_{x\in\mathscr{O}} \frac{1}{|\mathscr{O}|} = |G| \sum_{\mathscr{O}\in G\backslash X} \frac{1}{|\mathscr{O}|} \sum_{x\in\mathscr{O}} 1 = |G| \sum_{\mathscr{O}\in G\backslash X} \frac{1}{|\mathscr{O}|} \cdot |\mathscr{O}|$$

$$= |G| \sum_{\mathscr{O}\in G\backslash X} 1 = |G| \cdot |G\backslash X|,$$

d'où la formule souhaitée.

Produit semi-direct

J'ai suivi pour l'essentiel le document que j'ai mis en ligne sur le sujet (et non le paragraphe 2.2 du poly). J'ai plus précisément traité les chapitres 1.4, 2.1 et 2.2 de mon texte. En ce qui concerne les paragraphes introductifs 1.1–1.3, je les ai remplacés par la remarque suivante : si H est distingué alors $HK = KH$ (grâce aux formules $kh = khk^{-1}k$ et $hk = kk^{-1}hk$), et HK est donc un sous-groupe de G en vertu d'un résultat signalé en cours (poly, 1.1.4) et prouvé en TD. J'ai ensuite donné deux exemples.

Premier exemple. On se donne un corps k, un k-espace vectoriel E un espace affine $\mathscr{E}$ sur k d'espace directeur E. On fixe un point O dans $\mathscr{E}$; on note T le sous-groupe de $G := \mathrm{GA}(\mathscr{E})$ formé des translations – il est isomorphe à $(E, +)$ *via* la flèche $v \mapsto t_v$, et S le sous-groupe de G formé des applications affines f qui fixent O.

Le groupe T est distingué, en tant que noyau du morphisme de groupes $\mathrm{GA}(\mathscr{E}) \to \mathrm{GL}(E), \ell \mapsto \overrightarrow{\ell}$ par exemple.

On a $T \cap S = \{\mathrm{Id}\}$: si une translation fixe O, c'est l'identité.

On a $TS = G$. En effet, soit $g \in G$. Soit ℓ l'unique application affine de $\mathscr{E}$ dans $\mathscr{E}$ qui fixe O et admet $\overrightarrow{g}$ comme application linéaire associée. Comme $\overrightarrow{g}$ est bijective, ℓ est bijective. L'application $t_{\overrightarrow{Og(O)}} \circ \ell$ a pour application linéaire associée $\overrightarrow{g}$, et envoie O sur $g(O)$. Elle coïncide donc avec g ; ainsi, $g = t_{\overrightarrow{Og(O)}} \circ \ell$. Comme $t_{\overrightarrow{Og(O)}} \in T$ et $\ell \in S$, on a bien $TS = G$.

Il en résulte que G s'identifie à un produit semi-direct $T \rtimes_\varphi S$ pour un certain $\varphi : S \to \mathrm{Aut}\ T$ que nous allons déterminer.

Soit $\ell \in S$ et soit $v \in E$. On a $\varphi(\ell)(t_v) = \ell \circ t_v \circ \ell^{-1}$. Cette dernière application est une translation (son application linéaire associée est l'identité), et elle envoie O sur $\ell(t_v(\ell^{-1}(O))$. Comme $\ell \in S$ on a $\ell(O) = \ell^{-1}(O) = O$, et donc $\ell(t_v(\ell^{-1}(O)) = \ell(O + v) = O + \overrightarrow{\ell}(v)$. Par conséquent $\ell \circ t_v \circ \ell^{-1} = t_{\overrightarrow{\ell}(v)}$. Ainsi φ est l'application $\ell \mapsto (t_v \mapsto t_{\overrightarrow{\ell}(v)})$.

Second exemple. La multiplication par (-1) est un automorphisme d'ordre 2 de $\mathbb{Z}/5\mathbb{Z}$. On dispose donc d'un morphisme φ bien défini

$$\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}), \bar{n} \mapsto (\bar{a} \mapsto (-1)^n \bar{a}).$$

Le produit semi-direct $\mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est l'ensemble $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, muni de la loi $*$ définie par la formule :

$$(\overline{a}, \overline{n}) * (\overline{b}, \overline{m}) = (\overline{a} + (-1)^n \overline{b}, \overline{n} + \overline{m}).$$

5 Séance du 6 février

J'ai commencé par donner un exemple supplémentaire de produit semi-direct. Avant de l'énoncer, faisons une remarque, dont la vérification est laissée au lecteur. Soient G et H deux groupes, et soit φ un morphisme de H dans Aut G. Soient G' et H' deux groupes, et soient $i : G \simeq G'$ et $j : H \simeq H'$ deux isomorphismes. L'application

$$\varphi' : h \mapsto i \circ \varphi(j^{-1}(h)) \circ i^{-1}$$

définit un morphisme de H' dans Aut G', et l'application $(h, g) \mapsto (i(h), j(g))$ établit un isomorphisme entre $G \rtimes_\varphi H$ et $G' \rtimes_{\varphi'} H'$.

Venons-en maintenant à l'exemple annoncé. Fixons $n \geqslant 3$ et soit Γ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$, identifié à $\mathbb{R}^2$ (notons que Γ est plus précisément un sous-groupe de $\mathbb{C}^*$). L'ensemble Γ est alors l'ensemble des sommets d'un polygone régulier à n côtés. Soit G le groupe des isométries affines g de $\mathbb{R}^2$ qui stabilisent Γ, c'est-à-dire telles que $g(\Gamma) = \Gamma$, ou encore telles que $g(\Gamma) \subset \Gamma$ (puisque Γ est fini, *cf.* le cours précédent).

Comme l'origine O est l'isobarycentre de Γ, toutes les isométries de G fixent O ; autrement dit, elles sont linéaires. Une isométrie $\mathbb{R}$-linéaire de $\mathbb{C}$ est de la forme $z \mapsto uz$ ou $z \mapsto u\bar{z}$, avec $|u| = 1$; elle est directe dans le premier cas, et indirecte dans le second.

Il est immédiat qu'une isométrie de la forme $z \mapsto uz$ ou $z \mapsto u\bar{z}$ fixe Γ si et seulement si $u \in \Gamma$.

Soit G^+ le sous-groupe de G formé des isométries directes. C'est un sous-groupe distingué de G (en tant que noyau du déterminant). C'est par ce qui précède l'ensemble des isométries de la forme $z \mapsto uz$ avec $u \in \Gamma$. Il est donc isomorphe à $(\Gamma, \times)$, et partant à $(\mathbb{Z}/n\mathbb{Z}, +)$ (*via* l'isomorphisme entre ce dernier et Γ donné par la formule $\bar{k} \mapsto e^{2ik\pi/n}$).

Soit H le sous-groupe $\{\mathrm{Id}, z \mapsto \bar{z}\}$ de G (que ce soit un sous-groupe de G résulte du fait que la conjugaison complexe est d'ordre deux). Le groupe H est isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$ (l'identité correspond à $\bar{0}$, et la conjugaison complexe correspond à $\bar{1}$). On a $H \cap G^+ = \{\mathrm{Id}\}$, et la description explicite des éléments de G assure que $G = G^+.H$. Par conséquent, G s'identifie à un produit semi-direct de H et G^+ ; il reste à déterminer l'action de H sur G^+.

Soit $h \in H$. Si $h = \mathrm{Id}$ son action sur G^+ est triviale. Sinon, h est la conjugaison complexe. Soit $g \in G^+$; il existe $u \in \Gamma$ tel que $g(z) = uz$ pour tout $z \in \mathbb{C}$.

Soit $z \in \mathbb{C}$. On a $hgh^{-1}(z) = hg(\overline{z}) = h(u\overline{z}) = \overline{u\overline{z}} = \overline{u}z = u^{-1}z$ car u est de module 1. Ainsi, $hg^{-1}h = g^{-1}$.

En conséquence, G s'identifie à $G^+ \rtimes_\varphi H$, où H agit sur G^+ par la flèche

$$\mathrm{Id} \mapsto \mathrm{Id}, (z \mapsto \overline{z}) \mapsto (g \mapsto g^{-1}).$$

Compte-tenu des isomorphismes $G^+ \simeq \mathbb{Z}/n\mathbb{Z}$ et $H \simeq \mathbb{Z}/2\mathbb{Z}$, et de la remarque faite en début de section, on en déduit que G est isomorphe à

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z},$$

où ψ envoie $\overline{0}$ sur Id et $\overline{1}$ sur $\overline{a} \mapsto -\overline{a}$.

Le groupe $\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$ est également défini (de la même manière) pour $n = 0, 1$ et 2. Lorsque $n > 0$, il est noté D_n et est appelé le *n-ième groupe diédral*; il est alors d'ordre $2n$ (si $n = 0$ alors $\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z} = \mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$ est infini, et on le note plutôt D_∞).

Comme $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ sont commutatifs, $\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$ est trivial si et seulement si ses sous-groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ commutent, c'est-à-dire si et seulement si le produit semi-direct en jeu est direct. Cela revient à demander que ψ soit trivial, ou encore que la multiplication par (-1) soit l'identité de $\mathbb{Z}/n\mathbb{Z}$, ce qui équivaut à l'égalité $-1 = 1$ modulo n ; cette dernière condition est vérifiée uniquement si $n = 1$ ou 2. Par conséquent, D_1 et D_2 sont commutatifs, mais si $3 \leqslant n \leqslant \infty$ alors D_n n'est pas commutatif.

Produits semi-directs et suites exactes

J'ai traité essentiellement le paragraphe 3.1 de mon poly sur le produit semi-direct. J'ai ensuite défini la notion de morphisme entre deux diagrammes

$$1 \to G' \to G \to G'' \to 1 \text{ et } 1 \to H' \to H \to H'' \to 1$$

(G, G', G'', H, H' et H'' sont des groupes, et les flèches sont des morphismes de groupes) : c'est la donnée de trois morphismes $G' \to H', G \to H$ et $G'' \to H''$ tels que

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H' & \longrightarrow & H & \longrightarrow & H'' & \longrightarrow & 1 \end{array}$$

commute ; on dit que c'est un isomorphisme si les flèches verticales sont des isomorphismes.

Si deux tels diagrammes sont isomorphes, le premier est une suite exacte si et seulement si le second est une suite exacte (exercice).

Soit

$$1 \longrightarrow G' \xrightarrow{i} G \xrightarrow{p} G'' \longrightarrow 1$$

une suite exacte. Comme i est injective, elle identifie G' à son image $i(G')$, qui n'est autre que $\operatorname{Ker} p$; et comme p est surjective, elle identifie G'' à $G/\operatorname{Ker} p$. On dispose ainsi d'un isomorphisme de suites exactes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \\ 1 & \longrightarrow & \operatorname{Ker} p & \longrightarrow & G & \longrightarrow & G/\operatorname{Ker} p & \longrightarrow & 1 \end{array} .$$

L'exemple 1 du paragraphe 3.1 de mon poly est donc le prototype de la suite exacte.

J'ai ensuite montré que que si l'on dispose d'un isomorphisme entre deux suites exactes $\mathscr{S} : 1 \to G' \to G \to G'' \to 1$ et $\mathscr{T} : 1 \to H' \to H \to H'' \to 1$ alors $\mathscr{S}$ est scindée si et seulement si $\mathscr{T}$ est scindée.

En effet, supposons qu'il existe un isomorphisme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \longrightarrow & G & \xrightarrow{p} & G'' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle i} & & \\ 1 & \longrightarrow & H' & \longrightarrow & H & \xrightarrow{q} & H'' & \longrightarrow & 1 \end{array} .$$

Si p admet une section s, on vérifie aussitôt que $j \circ s \circ i^{-1}$ est une section de q ; si q admet une section t, on vérifie aussitôt que $j^{-1} \circ t \circ i$ est une section de p.

Deux remarques.

1) Si $1 \to G' \to G \to G'' \to 1$ est une suite exacte, la flèche $p : G \to G''$ est surjective. Elle admet donc toujours une section ensembliste, c'est-à-dire une application $s : G'' \to G$ telle que $p \circ s = \mathrm{Id}$: il suffit de choisir [4] pour chaque $g \in G$ un antécédent de g par p, que l'on note $s(g)$. C'est l'existence d'une telle section qui soit de surcroît un morphisme de groupes qui n'a rien de trivial (et n'est pas avérée en général).

2) Comme exemple de suite exacte non scindée, je n'ai pas repris l'exemple de mon poly (fin du paragraphe 3.2), mais j'ai donné le suivant : la suite

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \cdot$$

En effet, si la flèche quotient $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ admettait une section s, l'entier $s(\overline{1})$ serait un antécédent de $\overline{1}$, et donc impair ; par ailleurs, comme $2.\overline{1} = 0$, on aurait $2s(\overline{1}) = 0$ et donc $s(\overline{1}) = 0$, ce qui est absurde.

J'ai ensuite traité une partie des paragraphes 3.3, 3.4 et 3.5 de *loc. cit.* ; j'ai plus précisément simplement démontré la chose suivante, qui est un cas particulier des résultats du paragraphe 3.5 de *loc. cit.*.

Proposition. *Soit*

$$1 \longrightarrow G' \xrightarrow{i} G \xrightarrow{p} G'' \longrightarrow 1$$

une suite exacte. Les propositions suivantes sont équivalentes :

i) la suite exacte

$$1 \longrightarrow G' \xrightarrow{i} G \xrightarrow{p} G'' \longrightarrow 1$$

est scindée ;

ii) il existe un morphisme $\varphi : G'' \to \mathrm{Aut}\, G'$ et un isomorphisme de suites exactes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \longrightarrow & G' \rtimes_\varphi G'' & \longrightarrow & G'' & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & G' & \xrightarrow{i} & G & \xrightarrow{p} & G'' & \longrightarrow & 1 \end{array} .$$

4. Pour les puristes, la possibilité de *choisir* pour tout g un tel antécédent, même en sachant qu'il en existe, n'a rien d'évident du point de vue logique : elle repose sur un axiome de théorie des ensembles, précisément appelé *axiome du choix*.

Démonstration. Si ii) est vérifiée, la suite exacte étudiée est scindée, puisque la suite exacte du haut (dans le diagramme de ii)), est scindée (exemple de la fin du paragraphe 3.1 de *loc. cit.*). Supposons que i) soit vérifiée et soit s une section de p. Le morphisme s est injectif : si $s(g) = e$ alors $g = p(s(g)) = e$ (puisque $p \circ s = \mathrm{Id}$). Il induit donc un isomorphisme $G'' \simeq s(G'')$.

Comme i est injectif, il induit un isomorphisme $G' \simeq i(G')$, et $i(G')$ est un sous-groupe distingué de G. On a $i(G') \cap s(G'') = \{e\}$ et $G = i(G') \cap s(G'')$ (preuve : premier lemme du paragraphe 3.3 de *loc. cit.*).

Par conséquent, G s'identifie à un produit semi-direct de $i(G')$ et $s(G'')$. Par la remarque faite plus au (au tout début de la section), le groupe G s'identifie *via* i et s à un produit semi-direct de G' et G'', ce qui achève la preuve (il faut en toute rigueur vérifier que cette identification s'insère bien dans un isomorphisme de suites exactes tel que décrit au ii) ; cela découle immédiatement de sa construction – le lecteur pourra trouver les détails dans les preuves des paragraphes 3.3 et 3.4 de *loc. cit.*).

Groupe libre sur un ensemble

J'ai suivi le paragraphe 2.3.1 du poly de Jean-François Dat en ce qui concerne la construction du monoïde libre sur un ensemble X et sa propriété universelle (j'ai simplement utilisé la terminologie «monoïde» au lieu de «monoïde associatif»), puis j'ai introduit le monoïde libre M sur $X \coprod X^{-1}$ et ai défini les mots réduits. J'ai ensuite procédé autrement (avec davantage de détails) en ce qui concerne la construction du groupe libre sur X.

Définissons, pour tout groupe G, l'ensemble $h(M, G)$ comme l'ensemble des morphismes (de monoïdes) f de M dans G tels que $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in X$. Soit $\mathscr{R}$ la relation sur M définie par la condition $m\mathscr{R}n$ si et seulement si pour tout groupe G et tout $f \in h(M, G)$ l'on a $f(m) = f(n)$.

On vérifie aussitôt que $\mathscr{R}$ est une relation d'équivalence. Soient m, n, m' et n' des éléments de M tels que $m\mathscr{R}n$ et $m'\mathscr{R}n'$. Soit G un groupe et soit $f \in h(M, G)$. Comme $m\mathscr{R}n$ et $m'\mathscr{R}n'$ on a $f(m) = f(m')$ et $f(n) = f(n')$. Il vient $f(mm') = f(m)f(m') = f(n)f(n') = f(nn')$. Ainsi, $mn\mathscr{R}m'n'$. Il s'ensuit que la loi interne de M passe au quotient, et induit une loi de monoïde sur $M/\mathscr{R}$ telle que $M \to M/\mathscr{R}$ soit un morphisme.

Le monoïde $M/\mathscr{R}$ est un groupe. Il s'agit de vérifier que chacun de ses éléments est inversible.

Tout élément de $M/\mathscr{R}$ est de la forme $\overline{x_1 \dots x_k} = \overline{x_1} \dots \overline{x_k}$ où les x_i appartiennent à $X \coprod X^{-1}$. Il suffit donc de vérifier que $\bar{x}$ est inversible pour tout $x \in X \coprod x^{-1}$. Nous allons montrer que si $x \in X$ alors $\bar{x}$ est inversible d'inverse $\overline{x^{-1}}$, ce qui permettra de conclure.

Soit $x \in X$, soit G un groupe et soit $f \in h(M, G)$. On a $f(x^{-1}) = f(x)^{-1}$, et donc $f(xx^{-1}) = f(x^{-1}x) = e = f(\emptyset)$. Par conséquent, $\overline{xx^{-1}} = \overline{x^{-1}x} = \overline{\emptyset}$, ce qui montre que $\bar{x}$ est inversible d'inverse $\overline{x^{-1}}$, comme annoncé.

La propriété universelle du groupe $M/\mathscr{R}$. Soit G un groupe et soit $\lambda : X \to G$ une application. Il existe alors un unique morphisme de groupes f de $M/\mathscr{R}$ vers G qui envoie $\overline{x}$ sur $\lambda(x)$ pour tout $x \in X$.

Commençons par l'unicité. Soit f un morphisme satisfaisant les propriétés de l'énoncé. Comme $\overline{x}^{-1} = \overline{x^{-1}}$ pour tout $x \in X$ par ce qui précède, et comme tout élément de $M/\mathscr{R}$ est de la forme $\overline{x_1 \dots x_k} = \overline{x_1} \dots \overline{x_k}$ où les x_i appartiennent à $X \coprod X^{-1}$, on voit que $M/\mathscr{R}$ est engendré en tant que groupe par l'ensemble des $\overline{x}$ pour $x \in X$. Par conséquent, f est entièrement déterminé par sa restriction à cet ensemble, laquelle est imposée par hypothèse (puisque $f(\overline{x}) = \lambda(x)$ pour tout $x \in X$) ; ainsi, f est unique.

Prouvons maintenant l'existence de f. Soit μ l'application de $X \coprod X^{-1}$ dans G qui envoie x sur $\lambda(x)$ et x^{-1} sur $\lambda(x)^{-1}$ pour tout $x \in X$. L'application μ se prolonge en un morphisme de monoïdes $g : M \to G$, qui appartient par construction à $h(M, G)$. Par conséquent, $g(m) = g(n)$ dès que $m\mathscr{R}n$, et g induit ainsi un morphisme $f = M/\mathscr{R} \to G$, qui envoie par construction $\overline{x}$ sur $\lambda(x)$ pour tout $x \in X$.

Proposition. *Toute classe de $\mathscr{R}$ contient un unique mot réduit.*

Démonstration (elle n'a été traitée qu'en partie le 6 février, je la terminerai le 13 ; je la rédige ici dans son intégralité). Soit $m \in M$. Nous allons tout d'abord montrer par récurrence sur la longueur de m l'existence d'un mot réduit équivalent à m. Si la longueur de m est nulle, m est le mot vide et est déjà réduit.

Supposons que la longueur de m est > 0, et que le résultat est vrai pour les mots de longueur strictement inférieure. Si m est réduit, il n'y a rien à faire. Sinon, m est de la forme $m'xx^{-1}m''$ ou $m'x^{-1}xm''$; par l'hypothèse de récurrence, $m'm''$ est équivalent à un mot réduit (sa longueur est strictement inférieure à celle de m). Il suffit maintenant de montrer que m est équivalent à $m'm''$. Supposons par exemple que $m = m'xx^{-1}m''$. On a

$$\overline{m} = \overline{m'}\overline{x}\overline{x^{-1}}\overline{'m''} = \overline{m}\overline{m''} = \overline{mm''},$$

puisque $\bar{x}$ et $\overline{x^{-1}}$ sont inverses l'un de l'autre. Par conséquent, $m\mathscr{R}m'm''$, ce qu'il fallait démontrer ; la preuve dans le cas où $m = m'x^{-1}xm''$ est analogue.

Nous allons maintenant nous assurer que deux mots réduits équivalents coïncident. Soit E l'ensemble des mots réduits. Pour tout $x \in X$, soit σ_x l'application de E dans E qui envoie un mot réduit m sur xm si m n'est pas de la forme $x^{-1}m'$, et sur m' si m est de la forme $x^{-1}m'$. C'est une bijection : sa réciproque envoie un mot réduit m sur $x^{-1}m$ si m n'est pas de la forme xm', et sur m' si m est de la forme xm'.

Cette application ensembliste $X \to S_E$ induit en vertu de la propriété universelle de $M/\mathscr{R}$ un morphisme de groupes φ de $M/\mathscr{R}$ vers S_E. Par construction, on a $\varphi(\bar{x}) = \sigma_x$ et $\varphi(\overline{x^{-1}}) = \sigma_x^{-1}$ si $x \in X$.

Soit m un mot réduit. On a $\varphi(\overline{m})(\emptyset) = m$. On le vérifie par récurrence sur la longueur de m. Si m est de longueur nulle, c'est le mot vide et $\varphi(\overline{m}) = \mathrm{Id}$, d'où l'assertion.

Supposons m de longueur strictement positive, et la propriété vraie pour les mots de longueur strictement inférieure à celle de m. On peut écrire $m = xm'$ avec $x \in X \coprod X^{-1}$. Comme m est réduit, m' est réduit.

On a $\varphi(\overline{m})(\emptyset) = \varphi(\overline{x})(\varphi(\overline{m'})(\emptyset))$. Par hypothèse de récurrence, $\varphi(\overline{m'})(\emptyset)$ est égal à m'. Si $x \in X$ alors comme m est réduit m' n'est pas de la forme $x^{-1}m''$, et l'on a donc $\varphi(\overline{x})(m') = \sigma_x(m') = xm' = m$; si $x = y^{-1}$ avec

$y \in X$ alors comme m est réduit m' n'est pas de la forme ym'', et l'on a donc $\varphi(\overline{x})(m') = \sigma_y^{-1}(m') = y^{-1}m' = m$.

Conclusion. Si m et n sont deux mots réduits tels que $m\mathscr{R}n$, on a $\overline{m} = \overline{n}$ et donc $m = \varphi(\overline{m})(\emptyset) = \varphi(\overline{n})(\emptyset) = n$, ce qu'il fallait démontrer.

6 Séance du 13 février

J'ai terminé la preuve de la proposition ci-dessus.

À propos des groupes libres

J'ai ensuite fait quelques commentaires sur les groupes libres, à commencer par ceux du paragraphe 2.3.2 du poly.

Je m'autoriserai désormais à commettre l'abus suivant : bien que le groupe libre sur X soit *stricto sensu* un quotient du monoïde libre sur $X \coprod X^{-1}$, j'omettrai es barres de réduction sur les mots ; je ne les ai utilisées que pour la construction et la démonstration de la proposition ci-dessus, qui nécessitaient d'être un peu soigneux.

La proposition ci-dessus (et l'abus que je viens d'évoquer) conduisent à la description suivante de $F(X)$: ce groupe est constitué de mots sur l'alphabet $X \coprod X^{-1}$, toute chaîne de la forme xx^{-1} ou $x^{-1}x$ étant égale au neutre. Par éliminations successives de telles chaînes, on voit que tout mot de $F(X)$ est égal à un mot réduit ; ce dernier est unique.

On peut donc aussi décrire $F(X)$ comme l'ensemble des mots réduits sur l'alphabet $X \coprod X^{-1}$. Pour faire le produit de deux éléments de $F(X)$, on les concatène, puis on simplifie le mot obtenu en éliminant tous les termes de la forme xx^{-1} ou $x^{-1}x$, et l'on recommence jusqu'à obtention d'un mot réduit [5]. Signalons par ailleurs que si $n > 1$ on écrira souvent x^n (resp. x^{-n}) à la place d'une chaîne de n termes x (resp. x^{-1}) consécutifs.

Par exemple, si $X = \{a, b, c, d\}$ les deux mots réduits

$$m = a^2b^{-1}c^3dada \text{ et } n = a^{-1}d^{-1}a^{-1}d^{-1}b^2ca^4$$

sont deux éléments de $F(X)$. La concaténation des deux mots est égale à

$$a^2b^{-1}c^3dadaa^{-1}d^{-1}a^{-1}d^{-1}b^2ca^4.$$

En quatre étapes (élimination de aa^{-1}, puis dd^{-1}, puis aa^{-1}, puis dd^{-1}), on obtient le mot réduit $a^2b^{-1}c^3b^2ca^4$, qui est donc le produit de m et n.

J'ai rajouté qu'il faut penser au groupe libre sur un ensemble X comme au groupe *le plus général* fabriqué à partir de l'ensemble X : il contient donc les éléments de X, leurs inverses, tous les produits finis que l'on peut former avec ceux-ci.... et ces éléments ne satisfont aucune relation entre eux (d'où l'adjectif «libre»), sinon celles imposées par la théorie des groupes, qui se limitent aux simplifications des mots non réduits.

5. Le lecteur se demandera peut-être pourquoi on n'a pas directement défini $F(X)$ comme l'ensemble des mots réduits, avec la concaténation-simplification comme loi interne. Pour le comprendre, nous lui suggérons de chercher à prouver l'associativité de cette loi.

À propos des groupes définis par générateurs et relations

J'ai donné la définition (celle du 2.3.3), puis expliqué qu'intuitivement, le groupe $\langle S|R\rangle$ est le groupe le plus général fabriqué à partir de l'ensemble S et dans lequel les mots de R sont triviaux ; ou si l'on préfère on décrète que les éléments de R sont nuls et on n'impose aucune autre relation.

Cette idée un peu vague se traduit de façon rigoureuse par la propriété universelle de $\langle S|R\rangle$: soit G un groupe et soit $f : S \to G$ une application (ensembliste) ; soit φ le morphisme induit de $F(S)$ vers G. Supposons que $\varphi(m) = e$ pour tout $m \in R$. Il existe alors un unique morphisme $\psi : \langle S|R\rangle \to G$ qui envoie s sur $f(s)$ pour tout $s \in S$.

Avant de la démontrer, faisons un commentaire. La condition que $\varphi(m) = e$ pour tout $m \in R$ signifie la chose suivante : soient $s_1, \dots s_n$ des éléments de S et pour tout i, soit $\varepsilon_i \in \{-1, 1\}$. Si $s_1^{\varepsilon_1} \cdot \ldots \cdot s_n^{\varepsilon_n} \in R$, alors $f(s_1)^{\varepsilon_1} \cdot \ldots \cdot f(s_n)^{\varepsilon_n} = e$.

Venons-en maintenant à la preuve. Le sous-ensemble S du groupe $F(S)$ engendre ce dernier, par sa construction même – il est constitué de (classes de) mots, donc de produits d'éléments de $S \cup S^{-1}$; par conséquent, $\{\overline{s}\}_{s\in S}$ engendre le quotient $\langle S|R\rangle$ de $F(S)$, et un morphisme de groupes de source $\langle S|R\rangle$ est ainsi entièrement déterminé par ses valeurs sur S, d'où l'unicité de ψ.

Pour l'existence, remarquons que le noyau de φ est un sous-groupe distingué qui contient R par hypothèse ; il contient donc le plus petit sous-groupe distingué de $F(S)$ contenant R ; dès lors, φ induit par passage au quotient un morphisme $\psi : \langle S|R\rangle \to G$. On a par construction pour tout élément s de S les égalités $\psi(\overline{s}) = \varphi(s) = f(s)$, ce qui achève la démonstration.

Faisons deux commentaires à propos du plus petit sous-groupe distingué H de $F(S)$ qui contient R.

1) Le groupe H est le noyau de $F(S) \to \langle S|R\rangle$; il décrit donc précisément l'ensemble des mots (réduits) qui sont tués dans $\langle S|R\rangle$. Or ce dernier a été construit en se contenant d'imposer la trivialité des éléments de R ; on voit donc que cette opération entraîne un certain nombre de ≪dommages collatéraux≫ : ses victimes ne se limitent pas aux éléments de R, puisque ses effets destructeurs s'étendent à tout le groupe H (qui le plus souvent contient *strictement* R).

2) La définition *théorique* de H est simple : c'est le plus petit sous-groupe distingué de $F(S)$ contenant R, c'est-à-dire encore l'intersection de tous les sous-groupes distingués de $F(S)$ contenant R ; on peut vérifier (exercice) que c'est aussi le sous-groupe engendré par les éléments de la forme grg^{-1} pour $g \in F(S)$ et $r \in R$.

Par contre, savoir *en pratique*, même lorsque S et R sont finis, si un mot (réduit) donné appartient à H est extrêmement difficile. C'est même impossible en toute généralité : on démontre qu'il *n'existe pas* d'algorithme permettant de décider si, un ensemble fini S, un sous-ensemble fini R de $F(S)$ et un mot $m \in F(S)$ étant donnés, le mot m appartient au plus petit sous-groupe distingué de $F(S)$ contenant R (ce qui revient à demander que m soit trivial dans $\langle S|R\rangle$).

Bien entendu, dans bon nombre de cas rencontrés, on sait tout de même résoudre ce problème : ce que j'affirme est seulement l'inexistence d'un algorithme marchant dans tous les cas.

Quelques exemples

1) Le seul mot sur un alphabet vide étant le mot vide, le groupe $F(\emptyset)$ est trivial.

2) Supposons que X est un singleton $\{a\}$. Un mot réduit sur $X \coprod X^{-1}$ est de la forme a^n pour $n \in \mathbb{Z}$; on voit ainsi que $n \mapsto a^n$ établit un isomorphisme entre $\mathbb{Z}$ et $F(\{a\})$: le groupe libre sur un singleton s'identifie à $\mathbb{Z}$.

Soit n un entier. Comme $F(\{a\})$ est abélien, son plus petit sous-groupe distingué contenant a^n est le groupe engendré par a^n. Il s'ensuit que $\langle a|a^n\rangle$ est une présentation de $\mathbb{Z}/n\mathbb{Z}$ par générateurs et relations.

3) Supposons que X est un ensemble à deux éléments $\{a, b\}$. Il n'y a rien de plus à dire sur $F(X)$ que les généralités mentionnées plus haut : ses éléments seront les mots réduits en les lettres a, b, a^{-1}, b^{-1}, et on les multiplie en concaténant et simplifiant.

Pour ceux qui connaissent un peu de topologie algébrique, ce groupe s'identifie au groupe fondamental du plan privé de deux points. Plus précisément, soit P l'espace topologique $\mathbb{R}^2 - \{-1, 1\}$; soit $f : [0; 1] \to P$ le lacet $t \mapsto -1 + \exp(2i\pi t)$ (basé en l'origine) et soit $g : [0; 1] \to P$ le lacet $t \mapsto 1 - \exp(2i\pi t)$ (basé en l'origine). L'application ensembliste $\{a, b\} \to \pi_1(P, O)$ qui envoie a sur f et b sur g induit un morphisme de groupes $F(\{a, b\}) \to \pi_1(P, O)$; on démontre que c'est un isomorphisme.

Une présentation de $\mathbb{Z}^2$ par générateurs et relations. Nous allons démontrer que le groupe $\langle a, b|aba^{-1}b^{-1}\rangle$ est isomorphe à $\mathbb{Z}^2$. Pour cela, considérons l'application ensembliste de $\{a, b\}$ dans $\mathbb{Z}^2$ qui envoie a sur $(1, 0)$ et b sur $(0, 1)$. Comme

$$(1, 0) + (0, 1) - (1, 0) - (0, 1) = (0, 0),$$

cette application induit un morphisme φ de $\langle a, b|aba^{-1}b^{-1}\rangle$ vers $\mathbb{Z}^2$.

Par ailleurs, $\langle a, b|aba^{-1}b^{-1}\rangle$ est engendré par $\overline{a}$ et $\overline{b}$ qui commutent, puisque $\overline{a}\overline{b} = \overline{b}\overline{a}$ en vertu de la relation imposée. L'application $\psi : \mathbb{Z}^2 \to \langle a, b|aba^{-1}b^{-1}\rangle$ vers $\mathbb{Z}^2, (n, m) \mapsto \overline{a}^n\overline{b}^m$ est par conséquent un morphisme de groupes. On vérifie immédiatement (sur les générateurs $\overline{a}$ et $\overline{b}$ d'une part, $(0, 1)$ et $(1, 0)$ de l'autre) que $\psi \circ \varphi = \mathrm{Id}$ et $\varphi \circ \psi = \mathrm{Id}$; ainsi, $\langle a, b|aba^{-1}b^{-1}\rangle$ est isomorphe à $\mathbb{Z}^2$.

Exercice. Soit $n \geqslant 1$. Montrez que $\langle a, b|a^2, b^n, bab^{-1}a\rangle$ s'identifie au groupe diédral D_n construit au cours précédent.

Je n'ai pas traité les paragraphes de 2.3.5 à 2.4.4 du poly. Il s'agit d'exemples, que le lecteur peut lire pour sa culture mathématique.

Les théorèmes de Sylow

J'ai donné la définition 3.1.1, puis ai ensuite modifié la présentation, et la preuve. J'ai plus précisément énoncé et démontré le théorème suivant.

Théorème. *Soit p un nombre premier et soit G un groupe fini de cardinal $p^n m$ avec $n \geqslant 0$ et m premier à p.*

1) Il existe un p-sous-groupe de Sylow dans G.

2) Soit H un p-sous-groupe de G, c'est-à-dire un sous-groupe de G dont le cardinal est une puissance de p, et soit P un p-sous-groupe de Sylow de G. Il existe alors $g \in G$ tel que $H \subset gPg^{-1}$. En particulier :

i) H est contenu dans un p-sous-groupe de Sylow de G (il est clair que gPg^{-1} est un p-sous-groupe de Sylow de G , puisqu'il est isomorphe à P) ;

ii) si H est lui-même un p-sous-groupe de Sylow de G, il est égal à gPg^{-1}, puisque ces deux groupes ont même cardinal ; autrement dit, deux p-sous-groupes de Sylow de G sont conjugués, et a fortiori *isomorphes ;*

iii) si P est distingué c'est le seul p-sous-groupe de Sylow de G (puisque deux tels sous-groupes sont conjugués d'après ii)).

3) Le nombre de p-sous-groupes de Sylow de G divise m, et est congru à 1 modulo p.

Démonstration. Nous allons tout d'abord montrer un lemme arithmétique.

Lemme. *L'entier $\binom{p^n m}{p^n}$ est premier à p.*

Preuve du lemme. Nous allons plus précisément montrer qu'il est congru à m modulo p. Pour cela, écrivons la formule du binôme

$$(X+Y)^{p^n m} = \sum_{k=0}^{p^n m} \binom{p^n m}{k} X^{p^n m - k} Y^k,$$

qui est valable dans $\mathbb{Z}[X,Y]$, où X et Y sont des indéterminées. L'entier $\binom{p^n m}{p^n}$ est le coefficient de $X^{p^n m - p^n} Y^{p^n} = X^{p^n (m-1)} Y^{p^n}$ dans le polynôme ci-dessus.

Le polynôme $(X+Y)^{p^n m}$ est égal à $((X+Y)^{p^n})^m$; son image dans $\mathbb{F}_p[X,Y]$ est donc égale à $(X^{p^n}+Y^{p^n})^m$ (l'élévation à la puissance p est un endomorphisme dans ton anneau de caractéristique p). Ce dernier terme se récrit

$$X^{p^n m} + mX^{p^n (m-1)} Y^{p^n} + \ldots + Y^{p^n m}.$$

Dans ce polynôme à coefficients dans $\mathbb{F}_p[X,Y]$, le coefficient de $X^{p^n (m-1)} Y^{p^n}$ est égal à m ; comme il coïncide avec la réduction de $\binom{p^n m}{p^n}$ modulo p, l'entier $\binom{p^n m}{p^n}$ est égal à m modulo p, comme annoncé.

Retour à la preuve du théorème. Démontrons tout d'abord 1). Le groupe G opère sur lui-même par translations à gauche. Cette opération en induit une sur $\mathscr{P}(G)$. Soit $\mathscr{E}$ le sous-ensemble de $\mathscr{P}(G)$ formé des parties de cardinal p^n. Si $E \in \mathscr{E}$ alors pour tout $g \in G$ la partie $gE = \{gh\}_{h \in E}$ est de cardinal p^n (la multiplication à gauche par g étant une bijection de G sur lui-même) ; par conséquent, $\mathscr{E}$ est stable sous l'action de G.

Le cardinal de $\mathscr{E}$ est, par le lemme ci-dessus, premier à p. Comme $\mathscr{E}$ est réunion disjointe d'orbites, l'une au moins d'entre elles a un cardinal premier à p. Soit donc $E \in \mathscr{E}$ tel que le cardinal de l'orbite de E soit premier à p, et soit P le stabilisateur de E. Nous allons montrer que P est un p-sous-groupe de Sylow de G.

Le cardinal de P divisant celui de G, il est de la forme $p^{n'} m'$ avec $n' \leqslant n$ et $m' | m$. Le cardinal de l'orbite de E est alors égal à $[G : P] = p^{n-n'}(m/m')$. Ce cardinal étant premier à p par hypothèse, il vient $n = n'$.

Soit $h \in E$. Si $g \in P$ on a $gE = E$ par définition du stabilisateur, et donc $gh \in E$. L'application $P \to E, g \mapsto gh$ est injective (la multiplication à droite par h étant une bijection de G sur lui-même). Le cardinal de P est donc inférieur ou égal à celui de E, qui vaut p^n ; il s'ensuit que $m' = 1$, et que P est un p-sous-groupe de Sylow de G, comme annoncé.

Prouvons maintenant 2). Le groupe G agit à gauche sur G/P de manière naturelle, et l'action est transitive, ce qui veut dire que G/P est une orbite. Le stabilisateur de $P = Pe$ est $\{g \in G, gP = P\}$, qui n'est autre que P lui-même. Par conséquent, le stabilisateur de tout élément de l'orbite G/P est un conjugué de P.

Restreignons l'action au sous-groupe H de G. Si $\mathscr{O}$ est une orbite sous H, son cardinal divise celui de H qui est une puissance de p. C'est donc ou bien 1, ou bien une puissance non triviale de p, et en particulier un multiple de p ; notons que c'est 1 si et seulement si $\mathscr{O}$ est de la forme $\{\theta\}$, avec θ fixe sous H.

Comme le cardinal de P est p^n, le cardinal de G/P est m, qui est premier à p. Il y a en conséquence au moins une orbite sous H dont le cardinal est premier à p, c'est-à-dire, par ce qui précède, au moins un élément $\theta \in G/P$ qui est fixe sous H. Mais cela signifie que H est contenu dans le stabilisateur de θ, lequel est comme on l'a vu un conjugué de P ; ainsi, 2) est établi.

Prouvons 3). On note $\mathscr{S}$ l'ensemble des p-sous-groupes de Sylow de G, et on fixe $P \in \mathscr{S}$. On fait agir G sur $\mathscr{S}$ par conjugaison ; en vertu de 2), cette action est transitive : $\mathscr{S}$ est l'orbite de P.

Le stabilisateur de P pour cette action est son normalisateur

$$N_G(P) = \{g \in G, gPg^{-1} = P\} ;$$

il contient P. Le cardinal de $N_G(P)$ est de la forme $p^{n'}m'$ avec $n' \leqslant n$ et $m'|m$; comme il contient P, on a $n' = n$. Le cardinal de $\mathscr{S}$ est égal à l'indice de $N_G(P)$ dans G, c'est-à-dire à m/m'. C'est un diviseur de m, ce qui prouve la première assertion de 3).

Pour ce qui concerne la seconde assertion, on restreint l'action de G sur $\mathscr{S}$ au sous-groupe P de G. Si $\mathscr{O}$ est une orbite sous P, son cardinal divise celui de P qui est une puissance de p. C'est donc ou bien 1, ou bien une puissance non triviale de p, et en particulier un multiple de p ; notons que c'est 1 si et seulement si $\mathscr{O}$ est de la forme $\{Q\}$, avec Q fixe sous P. Il s'ensuit que le cardinal de $\mathscr{S}$ est congru modulo p à celui de l'ensemble des points de $\mathscr{S}$ fixes sous l'action de P. Nous allons montrer qu'il y a un et un seul tel point fixe, ce qui achèvera la démonstration.

Existence. Si $g \in P$ on a $gPg^{-1} = P$; par conséquent, P est fixe.

Unicité. Soit $Q \in \mathscr{S}$ fixe sous l'action de P. Cela signifie que P est contenu dans le normalisateur $N_G(Q)$ de Q. Comme P et Q sont de cardinal p^n, et comme le cardinal de $N_G(Q)$ divise le cardinal de G, les sous-groupes P et Q de $N_G(Q)$ en sont deux p-sous-groupes de Sylow.

D'autre part, la définition même de $N_G(Q)$ assure que $Q \lhd N_G(Q)$. Ainsi, Q est un p-sous-groupe de Sylow de $N_G(Q)$ qui est distingué dans ce dernier ; il s'ensuit, en vertu de l'assertion 2) iii), que Q est le seul p-sous-groupe de Sylow de $N_G(Q)$; en conséquence, $Q = P$.

7 Séance du 27 février

Applications des théorèmes de Sylow

J'ai commencé par montrer comment utiliser les sous-groupes de Sylow pour classer les groupes de cardinal 51, en faisant remarquer qu'en général, espérer une classification des groupes de cardinal n pour tout entier n est illusoire ; les théories dans lesquelles on sait classer tous les objets à isomorphisme près, comme l'algèbre linéaire, sont très rares.

Soit donc G un groupe de cardinal $51 = 3 \times 17$. Le nombre de ses 17-sous-groupes de Sylow divise 3 et est congru à 1 modulo 17, il est donc égal à 1. Il possède donc un unique 17-sous-groupe de Sylow H, nécessairement distingué. Comme le cardinal de H est 17, il est isomorphe à $\mathbb{Z}/17\mathbb{Z}$.

Soit K un 3-sous-groupe de Sylow de G. Il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Les cardinaux de H et K sont premiers entre eux, leur produit est égal au cardinal de G, et H est distingué : on sait alors que G s'identifie à un produit semi-direct $H \rtimes_\varphi K$ pour un certain $\varphi : K \to \mathrm{Aut}\ H$. Par conséquent, G est isomorphe à un produit semi-direct $\mathbb{Z}/17\mathbb{Z} \rtimes_\psi \mathbb{Z}/3\mathbb{Z}$ pour un certain $\psi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\ \mathbb{Z}/17\mathbb{Z}$.

Le groupe $\mathrm{Aut}\ \mathbb{Z}/17\mathbb{Z}$ s'identifie à $(\mathbb{Z}/17\mathbb{Z})^*$ qui est de cardinal 16. Comme 16 est premier à 3, le morphisme ψ est trivial (le cardinal de son image doit diviser 16, car celle-ci est un sous-groupe de $\mathrm{Aut}\ \mathbb{Z}/17\mathbb{Z}$, et 3, car celle-ci est un quotient de $\mathbb{Z}/3\mathbb{Z}$). Par conséquent, G est isomorphe au produit *direct* $\mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, c'est-à-dire encore à $\mathbb{Z}/51\mathbb{Z}$.

Nous allons maintenant expliquer comment classer les groupes de cardinal 21. La démarche est similaire, mais le résultat final est un peu plus subtil, comme nous allons voir. Soit donc G un groupe de cardinal $21 = 3 \times 7$. Le nombre de ses 7-sous-groupes de Sylow divise 3 et est congru à 1 modulo 7, il est donc égal à 1. Il possède donc un unique 7-sous-groupe de Sylow H, nécessairement distingué. Comme le cardinal de H est 7, il est isomorphe à $\mathbb{Z}/7\mathbb{Z}$.

Soit K un 3-sous-groupe de Sylow de G. Il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Les cardinaux de H et K sont premiers entre eux, leur produit est égal au cardinal de G, et H est distingué : on sait alors que G s'identifie à un produit semi-direct $H \rtimes_\varphi K$ pour un certain $\varphi : K \to \mathrm{Aut}\ H$. Par conséquent, G est isomorphe à un produit semi-direct $\mathbb{Z}/7\mathbb{Z} \rtimes_\psi \mathbb{Z}/3\mathbb{Z}$ pour un certain $\psi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\ \mathbb{Z}/7\mathbb{Z}$.

Le groupe $\mathrm{Aut}\ \mathbb{Z}/7\mathbb{Z}$ s'identifie à $(\mathbb{Z}/7\mathbb{Z})^*$, qui est de cardinal 6 et est cyclique. Ce dernier point peut se prouver par des arguments généraux (on sait que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique), mais dans ce cas précis il n'est pas difficile d'exhiber un générateur : $(-2)^3 = -8 = -1$ et $(-2)^2 = 4$. Par conséquent, l'ordre de (-2) dans $(\mathbb{Z}/7\mathbb{Z})^*$ n'est ni 1, ni 2, ni 3 ; il s'ensuit que (-2) est d'ordre 6 ; c'est donc un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$.

Se donner un morphisme de $\mathbb{Z}/3\mathbb{Z}$ dans un groupe Γ revient à choisir un élément γ de G tel que $\gamma^3 = e$. Comme (-2) engendre $(\mathbb{Z}/7\mathbb{Z})^*$ et est d'ordre 6, les éléments de $(\mathbb{Z}/7\mathbb{Z})^*$ de cube trivial sont 1, $(-2)^2 = 4$, et $(-2)^4 = 16 = 2$. Il existe ainsi trois morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $(\mathbb{Z}/7\mathbb{Z})^*$:

- le morphisme trivial ψ_1 ; le morphisme ψ_4 qui envoie n (modulo 3) sur 4^n (modulo 7) ; et le morphisme ψ_2 qui envoie n (modulo 3) sur 2^n (modulo 7).

Ces morphismes donnent lieu à trois produits semi-directs :

- le produit direct $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_1} \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;
- le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_4} \mathbb{Z}/3\mathbb{Z}$, dont la loi est donnée par la formule

$$(a, b) * (a', b') = (a + 4^b a', b + b') \; ;$$

- le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_2} \mathbb{Z}/3\mathbb{Z}$, dont la loi est donnée par la formule

$$(a, b) * (a', b') = (a + 2^b a', b + b').$$

Les deux derniers ne sont pas isomorphes au premier : en effet, comme les actions ψ_2 et ψ_4 ne sont pas triviales, elles donnent naissance à des groupes dans lesquels les facteurs $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ ne commutent pas – et ils ne sont en particulier pas abéliens.

On vérifie par contre que l'application

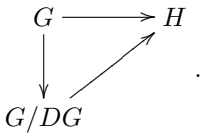
$$(a, b) \mapsto (a, -b)$$

établit un isomorphisme entre $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_2} \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_4} \mathbb{Z}/3\mathbb{Z}$: cela provient du fait que pour tout $b \in \mathbb{Z}/3\mathbb{Z}$ on a $2^b = 4^{-b}$ modulo 7, puisque $4 = 2^{-1}$ modulo 7 (en effet $2 \times 4 = 8 = 1$).

Il y a ainsi, à isomorphisme près, deux groupes de cardinal 21, à savoir $\mathbb{Z}/21\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z} \rtimes_{\psi_2} \mathbb{Z}/3\mathbb{Z}$; le second n'est pas abélien.

Groupes résolubles et nilpotents

J'ai essentiellement suivi le paragraphe 3.2 du poly, en détaillant un peu certains points. Le paragraphe 3.2.3 affirme que le groupe G/DG est abélien, et possède la propriété universelle suivante : pour tout groupe abélien H et tout morphisme de G dans H, il existe un unique morphisme de G/DG dans H faisant commuter le diagramme



.

Justifions brièvement ces affirmations. Si g et h appartiennent à G alors $ghg^{-1}h^{-1} \in DG$, donc $\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} = \bar{e}$ dans G/DG ; ainsi, ce dernier est abélien.

Soit φ un morphisme de G vers un groupe abélien H. Soient g et h deux éléments de G. On a $\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = e$ puisque H est abélien. Par conséquent, $DG \subset \mathrm{Ker}\, \varphi$, d'où la propriété d'unique factorisation évoquée.

Le groupe G/DG est appelé *l'abélianisé* de G, ou parfois aussi *le groupe G rendu abélien.* Ces expressions ont le mérite de bien traduire la façon intuitive dont il convient de penser à G/DG : c'est un groupe fabriqué en partant de G, en *décrétant* de surcroît que tous les éléments commutent, et en n'imposant aucune autre contrainte que celles qui découlent des précédentes par les propriétés générales des groupes.

Revenons aux groupes résolubles et nilpotents. Concernant le paragraphe 3.2.5, j'ai plus précisément énoncé et démontré la proposition suivante.
Proposition. *Soit G un groupe. Les propositions suivantes sont équivalentes :*

i) il existe une suite $G = G_0 \supset G_1 \ldots \supset \ldots \supset G_n = \{e\}$ où les G_i sont des sous-groupes de G, où $G_{i+1} \lhd G_i$ pour tout $i \leqslant n-1$, et où G_i/G_{i+1} est abélien pour tout i ;

ii) il existe n tel que $D^nG = \{e\}$;

iii) il existe une suite $G = G_0 \supset G_1 \ldots \supset \ldots \supset G_n = \{e\}$ où les G_i sont des sous-groupes de G, où $G_{i+1} \lhd G$ pour tout $i \leqslant n-1$, et où G_i/G_{i+1} est abélien pour tout i.

Remarque. Notez la différence entre ii) et iii) : dans iii) les sous-groupes G_i sont tous distingués *dans* G, alors que dans i), chacun est distingué dans son prédécesseur. Ainsi iii) semble *a priori* plus fort que i). Cette proposition révèle *a posteriori* qu'il n'en est rien.

Démonstration. i)⇒ii). Supposons donc qu'il existe une suite (G_i) comme dans i). Pour tout $i \leqslant n-1$, le groupe G_i/G_{i+1} est abélien. Par conséquent, si g et h sont deux éléments de G_i, on a $\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} = \bar{e} \in G_i/G_{i+1}$, et donc $ghg^{-1}h^{-1} \in G_{i+1}$. Ainsi, $DG_i \in G_{i+1}$. On en déduit par une récurrence immédiate que $D_iG \subset G_i$ pour tout $i \leqslant n$. En particulier, $D_nG \subset G_n = \{e\}$, et D_nG est donc trivial, ce qui montre ii).

ii)⇒iii). Si ii) est vraie posons $G_i = D_iG$ pour tout i compris entre 0 et n. La suite (G_i) satisfait alors par construction les conditions de iii).

iii)⇒i) est évident : qui peut le plus peut le moins.... (*cf.* la remarque préalable à la démonstration). □

L'égalité entre le plus petit entier n tel que $D_nG = 1$ et le plus petit entier n pour lequel il existe une suite $(G_i)_{0\leqslant i\leqslant n}$ comme en i) résulte de la preuve de la proposition ci-dessus.

Un groupe est résoluble de classe 0 (resp. de classe 1)) si et seulement si il est trivial (resp. abélien et non trivial).

Indiquons ici comment prouver la proposition 3.2.6.

Preuve de i). Soit G un groupe résoluble de classe b. On a $D^nG = \{e\}$.

Soit H un sous-groupe de G. On a $D^nH \subset D^nG$ et donc $D^nH = \{e\}$, et H est résoluble (de classe inférieure ou égale à n). Si H est un sous-groupe distingué de G, le groupe $D(G/H)$ est engendré par des éléments de la forme $\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1}$: il est donc égal à l'image de DG dans H. Par récurrence, $D_i(G/H)$ est pour tout i l'image de D_iG dans H ; comme $D_nG = \{e\}$ on a $D_n(G/H) = \{e\}$, et G/H est donc résoluble de classe inférieure ou égale à n.

Preuve de ii) (différente de celle que j'ai donnée en cours, elle est un peu plus simple). L'image de D_iG dans G/H est pour tout i égale à $D_i(G/H)$, comme on l'a vu. Comme $D_{n_2}(G/H)$ est trivial, $D_{n_2}G$ est contenu dans H. On a donc $D_{n_1+n_2}G = D_{n_1}(D_{n_2}G) \subset D_{n_1}H = \{e\}$. Ainsi, $D_{n_1+n_2}G$ est trivial, et G est résoluble de classe inférieure ou égale à $n_1 + n_2$.

Les exemples de S_3 et S_4.

Le groupe $\mathfrak{S}_3$ est résoluble. En effet, son sous-groupe distingué $\mathfrak{A}_3$ est abélien (étant de cardinal 3, il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$), et le quotient $\mathfrak{S}_3/\mathfrak{A}_3$ est isomorphe à $\{-1,1\}$ *via* la signature, et est donc abélien. Par conséquent, S_3 est résoluble de classe au plus deux, et comme il n'est pas abélien, il est résoluble de classe exactement 2.

Le groupe $\mathfrak{S}_4$ est résoluble. En effet, il admet $\mathfrak{A}_4$ comme sous-groupe distingué, et le quotient $\mathfrak{S}_4/\mathfrak{A}_4$ est isomorphe à $\{-1,1\}$ *via* la signature, et est donc abélien. Par ailleurs, $K := \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe de $\mathfrak{A}_4$ (vérifiez-le !), qui est distingué dans $\mathfrak{S}_4$ et abélien (il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$). Le quotient de $\mathfrak{A}_4/K$ est de cardinal 3, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et abélien. Ainsi, S_4 est résoluble de classe au plus 3. On peut montrer qu'il est résoluble de classe exactement 3.

Paragraphe 3.2.8. Attention, il y a un oubli dans le poly : les sous-groupes G_i de ce paragraphe doivent tout être *distingués dans G* (sinon G/G_{i+1} ne serait pas un groupe). L'équivalence entre les deux définitions de nilpotent se démontre de façon analogue à l'équivalence de ii) et iii) dans la proposition ci-dessus, en remplaçant D_iG par C^iG un peu partout. La preuve montre aussi que la classe de nilpotence du groupe est le plus petit entier n tel qu'il existe une suite $G_0, \ldots, G_n$ de sous-groupes distingués de G satisfaisant les conditions énoncées au 3.2.8.

En ce qui concerne la remarque sur les centres à la fin du paragraphe 3.2.8, je l'ai développée comme suit.

Soit G un groupe. On définit de manière récursive une suite croissante de sous-groupes distingués de G comme suit : $Z^0(G) = \{e\}$; si $Z^i(G)$ a été défini, le centre de $G/Z^i(G)$ est un sous-groupe distingué de ce dernier, il est donc de la forme $H/Z^i(G)$ pour un unique sous-groupe H de G contenant $Z^i(G)$, qui est lui-même distingué dans G. On pose alors $Z^{i+1}(G) = H$.

Proposition. *Le groupe G est nilpotent si et seulement si il existe n tel que $Z^n(G) = G$.*

Démonstration. Supposons que $Z^n(G) = G$. Posons $G_i = Z^{n-i}(G)$ pour $0 \leqslant i \leqslant n$. On vérifie immédiatement que (G_i) est une suite de sous-groupes distingués de G satisfaisant les conditions du paragraphe 3.2.8, et G est donc nilpotent.

Réciproquement, supposons qu'il existe une suite finie $(G_i)_{0\leqslant i\leqslant n}$ de sous-groupes distingués de G satisfaisant les conditions du paragraphe 3.2.8. La condition $G_i/G_{i+1} \subset Z(G/G_{i+1})$ permet de montrer très facilement par récurrence que $Z^i(G) \supset G_{n-i}$ pour tout i compris entre 0 et n. Par conséquent, on a $Z^n(G) \supset G_0 = G$, et $Z^n(G) = G$.

Remarque (non faite en cours). La preuve ci-dessus montre que le plus petit entier n tel que $Z^n(G) = G$ coïncide avec la classe de résolubilité de G.

Corollaire. *Si G est un groupe nilpotent non trivial, son centre est non trivial.*

Démonstration. Si l'on avait $Z(G) = \{e\}$ on aurait alors par une récurrence triviale $Z^i(G) = \{e\}$ pour tout i. Par conséquent, on aboutit à une contradiction avec l'existence d'un entier n tel que $Z^n(G) = G$. □

Remarque. Il découle des définitions qu'un groupe nilpotent est résoluble, et qu'un groupe est nilpotent de classe 0 (resp. 1) si et seulement si il est trivial (resp. abélien et non trivial).

Montrons qu'il existe un groupe résoluble de classe 2 et non nilpotent. Le centre du groupe $\mathfrak{S}_3$ est trivial (exercice). Par conséquent, $\mathfrak{S}_3$ n'est pas nilpotent, par le corollaire ci-dessus ; mais on a vu plus haut qu'il est résoluble de classe 2.

On a vu de plus à cette occasion qu'il possède un sous-groupe abélien distingué, à savoir $\mathfrak{A}_3$, tel que $\mathfrak{S}_3/\mathfrak{A}_3$ soit abélien. On voit donc que l'on a exhibé un contre-exemple à l'assertion ii) de la prop. 3.2.6. lorsqu'on remplace ≪résoluble≫ par ≪nilpotent≫. Notons par contre que si l'on remplace résoluble par nilpotent et que l'on exige par surcroît que H soit contenu dans le centre de G, l'assertion ii) de la prop. 3.2.6 redevient valable : c'est indiqué en remarque dans le poly au milieu du paragraphe 3.2.8, je ne l'ai pas signalé en cours.... et vous le laisse en exercice.

8 Séance du 5 mars

Fin du cours sur les groupes nilpotents

J'ai énoncé et démontré la proposition 3.2.10. J'ai donné quelques détails supplémentaires à propos de l'assertion i), que voici.

Pour prouver qu'un p-groupe est nilpotent, on commence par démontrer que tout p-groupe non trivial a un centre non trivial. Soit donc G un p-groupe non trivial ; son cardinal est p^n avec $n > 0$.

On fait opérer G sur lui-même par automorphismes intérieurs. On a la formule habituelle

$$|G| = \sum_{\omega \text{ orbite}} |\omega| = \sum_{\omega \text{ orbite singleton}} 1 + \sum_{\omega \text{ orbite non singleton}} |\omega|.$$

Si ω est une orbite son cardinal est l'indice du stabilisateur de n'importe lequel de ses éléments, et il est donc de la forme p^d ; si ω n'est pas un singleton, $d > 0$, et le cardinal de ω est nul modulo p.

Comme le cardinal de G est nul modulo p (c'est ici que sert l'hypothèse que G est non trivial), le nombre d'orbites singleton, c'est-à-dire de points fixes, est nul modulo p. Mais l'ensemble des points fixes de l'action de G sur lui-même par automorphismes intérieurs est précisément $Z(G)$. Son cardinal est donc nul modulo p ; en particulier, il n'est pas égal à 1 et $Z(G)$ est donc non trivial.

Venons-en maintenant à la preuve de 1), par récurrence sur le cardinal de G. Si G est trivial il est nilpotent ; supposons maintenant que G est non trivial, et que l'assertion requise a été démontrée pour les p-groupes de cardinal strictement inférieur à celui de G. Par ce qui précède, $Z(G)$ est non trivial. Le quotient $G/Z(G)$ est un p-groupe de cardinal strictement inférieur à celui de G. En vertu de notre hypothèse de récurrence il est nilpotent : il existe donc i tel que $Z^i(G/Z(G)) = G/Z(G)$. Mais on a par construction $Z^i(G/Z(G)) = Z^{i+1}(G)/Z(G)$. Par conséquent $Z^{i+1}(G) = G$ et G est nilpotent.

J'ai enfin énoncé et démontré le théorème 3.2.11, mais en donnant davantage de détails sur l'équivalence iv) $\iff$ v), ce que je vais faire ici – en choisissant une présentation un peu plus simple que celle adaptée en cours.

Remarque. si $G_1, \ldots, G_n$ sont des groupes, alors $Z(G_1 \times G_2 \ldots \times G_n)$ s'identifie à $Z(G_1) \times Z(G_2) \ldots \times Z(G_n)$, d'où un isomorphisme naturel

$$(G_1 \times G_2 \ldots \times G_n)/Z(G_1 \times G_2 \ldots \times G_n) \simeq (G_1/Z(G_1)) \times (G_2/Z(G_2)) \ldots \times (G_n/Z(G_n)).$$

On en déduit par une récurrence immédiate sur i que

$$Z^i(G_1 \times G_2 \times \ldots G^n) \simeq Z^i(G_1) \times Z^i(G_2) \times \ldots Z^i(G_n)$$

pour tout i. Par conséquent, $G_1 \times G_2 \ldots \times G_n$ est nilpotent si et seulement si chacun de ses facteurs est nilpotent.

Lemme. *Soit G un groupe fini, et soient $G_1, \ldots, G_n$ des sous-groupes de G de cardinaux deux à deux premiers entre eux tels que $|G| = \prod |G_i|$. Supposons que pour tout (i, j) avec $i \neq j$ les éléments de G_i commutent avec ceux de G_j. Le groupe G est alors isomorphe au produit direct des G_i.*

Démonstration. Soit φ l'application de $G_1 \times G_2 \times \ldots G_n$ vers G qui envoie $(g_1, \ldots, g_n)$ sur $g_1 g_2 \ldots g_n$. Cette application est un morphisme : en effet si $(g_1, \ldots, g_n)$ et $(h_1, \ldots, h_n)$ sont deux éléments de $G_1 \times G_2 \times \ldots G_n$, on a

$$\varphi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) = \varphi((g_1 h_1, \ldots, g_n h_n)) = g_1 h_1 g_2 h_2 \ldots g_n h_n$$

$$= g_1 g_2 \ldots g_n h_1 h_2 \ldots h_n = \varphi((g_1, \ldots, g_n))\varphi((h_1, \ldots, h_n)),$$

l'avant-dernière égalité provenant du fait que g_i et h_j commutent par hypothèse dès que $i \neq j$.

L'image de ce morphisme contient chacun des G_i, car

$$\varphi(e, \ldots, e, \underbrace{g}_{\text{place } i}, e, \ldots, e) = g$$

pour tout $g \in G_i$. Comme les cardinaux des G_i sont premiers entre eux, le cardinal de l'image de φ est multiple de $\prod |G_i| = |G|$. Par conséquent, cette image est G et φ est surjective. Comme les groupes $G_1 \times G_2 \times \ldots G_n$ et G ont même cardinal, φ est bijective. □

On peut maintenant énoncer le lemme qui couvre l'équivalence de ii) et iii).

Lemme. *Soit G un groupe fini de cardinal $p_1^{n_1} \ldots p_r^{n_r}$ où les p_i sont des nombres premiers deux à deux distincts. Les assertions suivantes sont équivalentes :*

i) G est isomorphe à un produit de la forme $P_1 \times \ldots \times P_r$, où P_i est un groupe de cardinal p^i pour tout i.

ii) Pour tout couple (g, h) d'éléments de G d'ordres premiers entre eux, on a $gh = hg$.

De plus si elles sont satisfaites alors G n'a qu'un p_i-Sylow pour tout i.

Démonstration. Supposons que l'assertion i) soit satisfaite. L'ordre d'un élément $(g_1, \ldots, g_r)$ de G (identifié à $\prod P_i$) est le PPCM des ordres des g_i ; comme ceux-ci sont deux à deux premiers entre eux, c'est même le produit de ces ordres. Pour tout i, l'ordre de g_i est une puissance de p_i ; on voit donc que deux éléments $g = (g_1, \ldots, g_r)$ et $h = (h_1, \ldots, h_r)$ de G sont d'ordre premiers

entre eux si et seulement si on a $g_i = e$ ou $h_i = e$ pour tout i, ce qui entraîne immédiatement la commutation des éléments g et h.

On voit aussi que pour tout i, l'ensemble des éléments d'ordre une puissance de p_i de G est P_i, identifié à $\{e\} \times \ldots \times \{e\} \times P_i \times \{e\} \times \ldots \times \{e\}$. Tout p_i-sous-groupe de Sylow de G est donc contenu dans P_i, ce qui montre que celui-ci est l'unique p_i-sous-groupe de Sylow de G.

Il reste à s'assurer que ii)⇒i). On suppose donc que ii) est vraie. Pour tout i, on choisit un p_i-sous-groupe de Sylow P_i de G. L'hypothèse ii) assure que les éléments de P_i et de P_j commutent dès que $i \neq j$. On peut alors appliquer le lemme précédent, qui assure que $G \simeq P_1 \times \ldots \times P_r$. □

On peut maintenant prouver le théorème 3.2.11. L'équivalence iv) $\Longleftrightarrow$ v) est le lemme ci-dessus. On prouve i)⇒ii)⇒iii) comme dans le poly. Pour iii)⇒iv) on suit la preuve du poly, mais on remplace «d'où un morphisme injectif....» par le premier des deux lemmes ci-dessus, appliqués aux sous-groupes S_p de G. Enfin, iv)⇒i) se fait en combinant la remarque ci-dessus et l'assertion i) de la prop. 3.2.10.

Début du cours sur les représentations

J'ai suivi le paragraphe 4.1 du poly jusqu'au 4.1.2, exemple iv) ; j'ai remplacé l'exemple ii) par le suivant : on fixe $n \geqslant 3$ et l'on note D_n le groupe diédral $\mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$, où ψ envoie $\overline{0}$ sur Id et $\overline{1}$ sur $\overline{a} \mapsto -\overline{a}$. On a vu (séance du 6 février) qu'il s'identifie à un sous-groupe du groupe des isométries de $\mathbb{R}^2$, à savoir celui des isométries préservant le polygone régulier $\{e^{2ik\pi/n}\}_{0\leqslant k\leqslant n-1}$, *via* la flèche

$$(k,0) \mapsto (z \mapsto e^{2ik\pi/n}z), \quad (k,1) \mapsto (z \mapsto e^{2ik\pi/n}\bar{z}).$$

On obtient ainsi une représentation $\mathbb{R}$-linéaire de dimension 2 de D_n.

9 Séance du 12 mars

J'ai poursuivi la section 4.1. J'ai traité l'exemple v) de 4.1.2.

En ce qui concerne 4.1.3, 4.1.4 et 4.1.5, je les ai suivis à quelques détails près.

• J'ai oublié de mentionner ce qu'on appelle une représentation fidèle, je le ferai lors de la prochaine séance.

• en ce qui concerne l'exemple i), je l'ai remplacé par l'assertion suivante : soit G un groupe et soit X un G-ensemble, *i.e.* un ensemble muni d'une opération à gauche de G. Supposons que X est fini et que l'action de G est transitive. Alors $(KX)^G = K.(\sum e_x)$. C'est donc une droite, sauf si $\sum e_x = 0$, ce qui n'est possible que si $X = \emptyset$, auquel cas $KX = (KX)^G = \{0\}$.

Voici la preuve de cette assertion. Si $v \in K.(\sum e_x)$ alors $v = \lambda \sum e_x$ pour un certain $\lambda \in K$, et l'on a pour tout $g \in V$ l'égalité

$$g.v = \lambda \sum g.e_x = \lambda \sum e_{g.x} = \lambda \sum e_x,$$

car $x \mapsto g.x$ est une bijection de X sur X pour tout $g \in G$. Ainsi $g.v = v$ et $v \in (KX)^G$. Il vient $K.(\sum e_x) \subset (KX)^G$.

Montrons l'inclusion réciproque. Soit $v \in (KX)^G$. Écrivons $v = \sum \lambda_x e_x$. Soient x_0 et x_1 deux éléments de X. L'action de G sur X étant transitive, il existe $g \in G$ tel que $g.x_0 = x_1$. Comme $v \in (KX)^G$ on a $g.v = v$ et donc $\sum \lambda_x = \sum \lambda e_{gx}$. Le coefficient de e_{x_1} doit être le même dans les deux termes de l'égalité (la famille (e_x) étant une base). Or dans le terme de gauche, son coefficient est λ_{x_1} tandis que dans le terme de droite c'est λ_{x_0}. Par conséquent, $\lambda_{x_1} = \lambda_{x_0}$. Ceci valant pour tout couple (x_0, x_1) d'éléments de x, il existe $\lambda \in K$ tel que $\lambda_x = \lambda$ pour tout x. On a donc $v = \lambda \sum e_x$ et $v \in K.\sum e_x$. Par conséquent, $(KX)^G \subset K.(\sum e_x)$, et l'on a bien finalement $(KX)^G = K.\sum e_x$.

• en ce qui concerne l'exemple ii) :

- **attention : il y a un oubli dans l'énoncé, il faut en outre faire l'hypothèse que la représentation est non nulle** ;

- j'ai donné une preuve détaillée, que voici maintenant.

Comme $V \neq \{0\}$ il existe un vecteur v non nul dans V. Soit V_0 le sous $\mathbb{F}_p$-espace vectoriel de V engendré par l'orbite de v sous G. Comme G est fini, cette orbite est finie, et V_0 est donc un $\mathbb{F}_p$-espace vectoriel de dimension finie. Si d désigne sa dimension, il est de cardinal p^d ; notons que comme $v \in V_0$, l'espace V_0 n'est pas nul, et d est donc strictement positif.

Par construction, V_0 est stable par G. On a la formule habituelle

$$|V_0| = \sum_{\omega \text{ orbite}} |\omega| = \sum_{\omega \text{ orbite singleton}} 1 + \sum_{\omega \text{ orbite non singleton}} |\omega|.$$

Si ω est une orbite son cardinal est l'indice du stabilisateur de n'importe lequel de ses éléments, et il est donc de la forme p^m ; si ω n'est pas un singleton, $m > 0$, et le cardinal de ω est nul modulo p.

Le cardinal de V_0 est égal à p^d. Il est en particulier nul modulo p (puisque $d > 0$). Par conséquent, le nombre d'orbites singleton, c'est-à-dire de vecteurs fixes sous l'action de G, est nul modulo p. Autrement dit, le cardinal de V_0^G est nul modulo p ; en particulier, il n'est pas égal à 1 et V_0^G est donc non trivial ; l'espace V^G est *a fortiori* non trivial.

J'ai donné la définition d'une représentation irréductible (4.1.6). **Attention, il y a un oubli dans le poly : il faut inclure dans la définition d'une représentation irréductible (ρ, V) le fait que V est non nul**.

J'ai ensuite essentiellement traité les exemples de 4.1.7, mais avec quelques détails en plus.

Exemple i) : je l'ai traité en remplaçant $\mathbb{C}$ par un corps algébriquement clos K quelconque tel que $|G|$ soit non nul dans K. L'argument à rajouter est le suivant : il faut s'assurer, pour garantir la diagonalisabilité de $\rho(g)$, que $X^{o(g)} - 1$ est à racines simples dans K. Or sa dérivée est $o(g)X^{o(g)-1}$, qui ne s'annule sur aucune des racines de $X^{o(g)} - 1$ *car $o(g)$, divisant $|G|$, est non nul dans le corps K*.

Exemple ii). Je l'ai traité plus en détail. Appelons ρ la représentation $\mathbb{R}$-linéaire de D_n déjà évoquée ; on peut la restreindre à $\mathbb{Z}/n\mathbb{Z}$ et obtenir ainsi une représentation $\mathbb{R}$-linéaire $\rho_{|\mathbb{Z}/n\mathbb{Z}}$ de $\mathbb{Z}/n\mathbb{Z}$.

Par ailleurs, en travaillant dans la base canonique de $\mathbb{R}^2$, on peut voir ρ comme un morphisme de groupes de D_n dans $\mathrm{GL}_2(\mathbb{R})$. On vérifie

immédiatement qu'il est donné par les formules

$$(a,0) \mapsto \begin{pmatrix} \cos(2a\pi/n) & -\sin(2a\pi/n) \\ \sin(2a\pi/n) & \cos(2a\pi/n) \end{pmatrix},\ (a,1) \mapsto \begin{pmatrix} \cos(2a\pi/n) & +\sin(2a\pi/n) \\ \sin(2a\pi/n) & -\cos(2a\pi/n) \end{pmatrix}.$$

Comme $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$, cette représentation peut également être vue comme une représentation $\mathbb{C}$-linéaire $\rho_{\mathbb{C}}$; nous aurons aussi à considérer la restriction $(\rho_{\mathbb{C}})_{|\mathbb{Z}/n\mathbb{Z}}$ de cette dernière à $\mathbb{Z}/n\mathbb{Z}$.

La représentation $\rho_{|\mathbb{Z}/n\mathbb{Z}}$ est irréductible. En effet, comme $\mathbb{R}^2$ est de dimension 2, il suffit de s'assurer que $\mathbb{R}^2$ ne contient aucune droite stable sous l'action de $\mathbb{Z}/n\mathbb{Z}$. Or si D était une telle droite, elle serait en particulier stable sous $\rho(1,0)$, qui n'est autre que la rotation de matrice

$$\begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

Son polynôme caractéristique est $X^2 - 2\cos(2\pi/n)X + 1$, qui a deux racines complexes $e^{2i/pi/n}$ et $e^{-2i\pi/n}$ qui ne sont pas réelles puisque $n \geqslant 3$. Cette rotation n'ayant pas de valeur propre réelle, elle n'a pas de droite stable dans $\mathbb{R}^2$, ce qui achève la preuve.

La représentation ρ est irréductible. C'est une conséquence triviale de ce qui précède : une droite de $\mathbb{R}^2$ stable sous l'action de D_n le serait *a fortiori* sous celle de $\mathbb{Z}/n\mathbb{Z}$, et l'on vient de voir que c'était impossible.

La représentation $(\rho_{\mathbb{C}})_{|\mathbb{Z}/n\mathbb{Z}}$ n'est pas irréductible. En effet, $\rho(1,0)$ a, comme on vient de le voir, deux valeurs propres complexes distinctes, et est donc diagonalisable en tant qu'endomorphisme de $\mathbb{C}^2$. Il existe donc deux droites complexes D et D' stables sous $\rho(1,0)$ telles que $\mathbb{C}^2 = D \oplus D'$. Comme $\rho(k,1) = \rho(1,0)^k$ pour tout k, chacune de ces droites est stable sous l'action de $\mathbb{Z}/n\mathbb{Z}$, et $(\rho_{\mathbb{C}})_{|\mathbb{Z}/n\mathbb{Z}}$ n'est pas irréductible.

La représentation $\rho_{\mathbb{C}}$ est irréductible. En effet, supposons qu'il existe une droite Δ de $\mathbb{C}^2$ stable sous l'action de D_n. Elle est en particulier stable sous l'action de $\rho(0,1)$, qui est la symétrie de matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Celle-ci étant diagonale avec deux valeurs propres distinctes, ses seules droites stables sont $\mathbb{C}\cdot(0,1)$ et $\mathbb{C}\cdot(1,0)$, et Δ est donc l'une de ces deux droites. Mais comme

$$\underbrace{(1,0)}_{\in D_n} \cdot \underbrace{(0,1)}_{\in \mathbb{C}^2} = (-\sin(2\pi/n), \cos(2\pi/n)) \text{ et } \underbrace{(1,0)}_{\in D_n} \cdot \underbrace{(1,0)}_{\in \mathbb{C}^2} = (\cos(2\pi/n), \sin(2\pi/n)),$$

et comme $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont tous deux non nuls, on voit qu'aucune de ces deux droites n'est stable sous l'action de D_n, et l'on aboutit ainsi à une contradiction.

Je n'ai pas mentionné l'exemple iii), il sera évoqué lors de la prochaine séance.

J'ai traité l'exemple iv).

J'ai traité un peu plus en détail l'exemple v), comme suit. Soit K un corps algébriquement clos et soit n un entier non nul dans K. D'après l'exemple i) (dans la variante générale que j'en ai donnée), les représentations irréductibles de K sont ses représentations de dimension 1. Soit V une telle représentation. Comme V est de dimension 1, l'application $\lambda \mapsto (v \mapsto \lambda v)$ établit un isomorphisme entre K^* et $\mathrm{GL}(V)$. La représentation étudiée est donc donnée par un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans K^*, c'est-à-dire encore par un élément x de K^* tel que $x^n = 1$. Comme les racines de $X^n - 1$ sont simples (l'argument a été donné lors de l'exemple i)), il y en a n exactement.

Pour toute racine n-ième de l'unité λ de K, notons ρ_λ la représentation d'espace sous-jacent K donnée par le morphisme $1 \mapsto \lambda$ de $\mathbb{Z}/n\mathbb{Z}$ dans K^*. D'après ce qu'on vient de voir, toute représentation K-linéaire irréductible de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à ρ_λ pour une certaine racine n-ième de l'unité λ.

On obtient ainsi au plus n classes d'isomorphie de représentations. Pour vérifier qu'il y en a exactement n il faut s'assurer que si λ et μ sont deux racines n-ièmes distinctes de l'unité dans K, les représentations ρ_λ et ρ_μ ne sont pas isomorphes. Mais c'est immédiat : s'il existait un isomorphisme f entre les deux, on aurait

$$f(\underbrace{1}_{\in \mathbb{Z}/n\mathbb{Z}} \cdot \underbrace{1}_{\in (\rho_\lambda, K)}) = f(\underbrace{1}_{\in \mathbb{Z}/n\mathbb{Z}} \cdot \underbrace{1}_{\in (\rho_\mu, K)}),$$

c'est-à-dire $\lambda f(1) = \mu f(1)$ et donc $\lambda = \mu$ puisque $f(1) \neq 0$ (l'application f est un isomorphisme) ; on aboutit ainsi à une contradiction.

Il y a en conséquence exactement n classes d'isomorphie de représentations K-linéaires irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

10 Séance du 19 mars

J'ai poursuivi le cours sur les représentations, de la proposition 4.1.8 au lemme 4.1.13. J'ai traité certains points plus en détail.

Après la prop. 4.1.8, j'ai donné un exemple de représentation irréductible dont l'algèbre des endomorphismes équivariants est une algèbre à division qui n'est pas triviale. Pour cela, introduisons brièvement l'anneau $\mathbb{H}$ des *quaternions*, qui se décrit comme suit : c'est un $\mathbb{R}$-espace vectoriel de la forme

$$\mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k,$$

muni d'une multiplication définie par les formules suivantes :

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

On vérifie que c'est une algèbre à division ; elle contient le groupe

$$\mathrm{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Remarque. Soit $\mathbb{H}_\mathbb{C}$ la $\mathbb{C}$-algèbre $\mathbb{C} \cdot 1 \oplus \mathbb{C} \cdot i \oplus \mathbb{C} \cdot j \oplus \mathbb{C} \cdot k$, dont la multiplication est définie par les formules $(*)$. On vérifie que $\mathbb{H}_\mathbb{C}$ n'est pas une algèbre à division ; on peu montrer plus précisément qu'elle est isomorphe à $M_2(\mathbb{C})$.

On fait opérer H_8 sur $\mathbb{H}$ par multiplication à gauche.

La représentation $\mathbb{H}$ *de* H_8 *est irréductible.* En effet, soit V un sous-$\mathbb{R}$-espace vectoriel de $\mathbb{H}$ stable sous l'action de H_8. Il est alors stable par multiplication à gauche par i, j et k, et donc, par linéarité, par multiplication à gauche par n'importe quel élément h de $\mathbb{H}$. Supposons $V \neq 0$ et soit v un élément non nul de V. Pour tout $h \in \mathbb{H}$, on a $h = (hv^{-1})v$, lequel appartient à V par ce qui précède. Ainsi $V = \mathbb{H}$ et $\mathbb{H}$ est irréductible.

L'anneau des endomorphismes de $\mathbb{H}$ *s'identifie à l'algèbre à division* $\mathbb{H}^{\mathrm{op}}$, où $\mathbb{H}^{\mathrm{op}}$ désigne l'algèbre qui admet $\mathbb{H}$ comme espace vectoriel sous-jacent et dont la loi $*$ est définie par la formule $a * b = ba$.

En effet, soit $a \in \mathbb{H}$ et soit d_a la multiplication à droite par a. Cet endomorphisme $\mathbb{R}$-linéaire de $\mathbb{H}$ commute à la multiplication à gauche par les éléments de $\mathbb{H}$, et en particulier à l'action de H_8. Comme $d_{ab} = d_b \circ d_a$, l'application $a \mapsto d_a$ est un morphisme d'algèbres de $\mathbb{H}^{\mathrm{op}}$ dans $\mathrm{End}_{\mathrm{H}_8}\mathbb{H}$.

Ce morphisme est injectif. En effet si $d_a = 0$ alors $d_a(1) = a = 0$.

Ce morphisme est surjectif. Soit $f \in \mathrm{End}_{\mathrm{H}_8}\mathbb{H}$. Posons $a = f(1)$. Comme f commute à l'action de H_8, on a $f(i) = f(i.1) = if(1) = ia$, et de même $f(j) = ja$ et $f(k) = ka$. Par linéarité, $f(h) = ha$ quel que soit $h \in \mathbb{H}$, et l'on a donc $f = d_a$.

Remarque. L'anneau $\mathbb{H}^{\mathrm{op}}$ est en fait isomorphe à $\mathbb{H}$, *via* une sorte de conjugaison : l'application qui envoie $z = a+bi+cj+dk$ sur $\overline{z} := a-bi-cj-dk$ est en effet une application $\mathbb{R}$-linéaire telle que $\overline{z_1 z_2} = \overline{z_2}\,\overline{z_1}$ pour tout $(z_1, z_2) \in \mathbb{H}^2$. Elle induit donc un isomorphisme de $\mathbb{H}$ sur $\mathbb{H}^{\mathrm{op}}$.

En ce qui concerne la proposition 4.1.10, je l'ai remplacée par la suivante, de preuve presque analogue : soit G un p-groupe et soit X un ensemble fini de cardinal $\geqslant 2$ sur lequel G opère transitivement. Si K est de car. p alors la représentation KX n'est pas irréductible, mais est indécomposable.

La preuve est la suivante : comme le cardinal de X est supérieur ou égal à 2, $\dim KX \geqslant 2$ et la représentation KX n'est donc pas irréductible (assertion iv), haut de la page 29 du poly).

Soient V et W deux sous-espaces stables non triviaux de KX. Comme K est de car. p et comme G est un p-groupe, V^G et W^G sont tous deux non nuls (§4.1.3, exemple ii). Mais $(KX)^G = K \cdot (\sum e_x)$ (voir le cours précédent), qui est une droite. Celle-ci ayant une intersection non nulle avec V et W, elle est contenue dans chacun des deux et donc dans leur intersection. Celle-ci est dès lors non nulle, ce qui montre que KX ne peut pas être une somme directe de sous-espaces stables non triviaux.

Preuve de la proposition 4.1.11 : rajoutons quelques détails.

L'application p *est* G*-équivariante.* On a en effet pour tout $h \in G$ les égalités

$$p \circ \rho(h) = |G|^{-1} \sum_{g \in G} \rho(g) \circ \tilde{p} \circ \rho(g^{-1}h) = |G|^{-1} \rho(h) \circ \sum_{g \in G} \rho(h^{-1}g) \circ \tilde{p} \circ \rho(g^{-1}h).$$

Comme $g \mapsto h^{-1}g$ est une bijection de G sur G, ceci peut se récrire

$$|G|^{-1} \rho(h) \circ \sum_{g \in G} \rho(g) \circ \tilde{p} \circ \rho(g^{-1}) = \rho(h) \circ p,$$

et p est bien G-équivariant.

L'application p est un projecteur sur W. Notons pour commencer que $p(v)$ appartient par construction à W pour tout $v \in V$. Soit maintenant $w \in W$. On a alors $\rho(g)^{-1}(w) \in W$ pour tout $g \in G$, et donc $\tilde{p}(\rho(g)^{-1}(w)) = \rho(g)^{-1}(w)$ pour tout $g \in G$. Ainsi,

$$p(w) = |G|^{-1} \sum_{g \in G} \rho(g) \circ \tilde{p} \circ \rho(g^{-1})(w) = |G|^{-1} \sum_{g \in G} \rho(g)(\rho(g)^{-1}(w))$$

$$= |G|^{-1} \sum_{g \in G} w = |G|^{-1} \cdot |G| \cdot w = w.$$

On a ainsi $p(w) = w$ pour tout $w \in W$; il s'ensuit que W est égal à l'image de p (puisqu'on a déjà vu que W contient l'image de p). Par ailleurs, soit $v \in V$. Comme $p(v) \in W$, on a $p(p(v)) = p(v)$ par ce qui précède, et donc $p^2(v) = p(v)$. Ainsi $p^2 = p$ et p est un projecteur.

Comme p est G-équivariant, son noyau est stable et constitue donc bien un supplémentaire stable de W.

Remarque. L'hypothèse que $|G|$ n'est pas nulle dans K a été utilisée lorsqu'on a divisé par $|G|$.

Corollaire 4.1.12. Son assertion i) est une conséquence immédiate de ii). Donnons une preuve de ii). On raisonne par récurrence sur la dimension de V. Si $V = \{0\}$ le résultat est vrai : on écrit V comme la *somme directe vide* de représentations irréductibles.

On suppose maintenant que dim $V > 0$ et que le résultat est vrai en dimension strictement inférieure à celle de V. Si V est irréductible alors ii) est vraie (avec un seul terme dans la décomposition, à savoir V lui-même). Sinon, V possède un sous-espace stable W qui n'est ni $\{0\}$, ni V. Par la proposition 4.11, le sous-espace W admet un supplémentaire stable W'. Comme $W \neq \{0\}$ et $W \neq V$, les espaces W et W' sont tous deux de dimension strictement inférieure à celle de V. D'après l'hypothèse de récurrence, ils sont tous deux somme directe de sous-représentations irréductibles, et V est donc somme directe de sous-représentations irréductibles.

Lemme 4.1.13. Je vais en préciser l'énoncé et la preuve ; la présentation que je donne ici est un peu simplifiée par rapport à celle que j'ai faite en cours.

Voici l'énoncé que je propose : supposons que la représentation V s'écrive comme une somme directe $\bigoplus_{i \in I} V_i$ de sous-représentations irréductibles, et soit W une représentation irréductible fixée de V. Le cardinal de

$$J := \{i \in I, V_i \simeq W\}$$

ne dépend pas de la décomposition $V = \bigoplus V_i$ qui a été choisie.

Donnons une démonstration de ce fait. Posons $V' = \bigoplus_{i \in J} V_i$. Comme chaque V_i pour $i \in J$ est isomorphe à W, le cardinal de J est égal à dim V'/dim V. Pour montrer que le cardinal de J est indépendant de la décomposition choisie, il suffit de s'assurer que V' est indépendant de la décomposition choisie, et donc de s'assurer qu'il peut être défini en termes des propriétés intrinsèques de la représentation V.

Soit $\mathscr{E}$ l'ensemble des sous-représentations de V qui sont isomorphes à W^r pour un certain r. Nous allons montrer que V' est le plus grand élément de $\mathscr{E}$,

ce qui permettra de conclure. On a $V' = \bigoplus_{j\in J} V_i \simeq W^{|J|}$; par conséquent, $V' \in \mathscr{E}$.

Soit $U \in \mathscr{E}$; nous allons prouver que $U \subset V'$. Pour tout i, notons π_i la projection de V sur V_i parallèlement à $\bigoplus_{j\neq i} V_j$; c'est une application équivariante. Pour montrer que $U \subset V'$, il suffit de vérifier que $\pi_{i|U} = 0$ pour tout $i \in I \setminus J$.

Soit donc $i \in I \setminus J$. Comme W et V_i sont irréductibles, tout morphisme de W vers V_i est ou bien nul, ou bien un isomorphisme. L'indice i n'appartenant pas à J, les représentations W et V_i ne sont pas isomorphes, et tout morphisme de W dans V_i est donc nul.

Fixons un isomorphisme $\iota : W^r \simeq U$ (il en existe puisque $U \in \mathscr{E}$). La composée $\pi_{i|U} \circ \iota$ est un morphisme de représentations de W^r vers V_i. Sa restriction à chacun des facteurs W de W^r est un morphisme de représentations $W \to V_i$, et est donc nul par ce qui précède. Il s'ensuit que $\pi_{i|U} \circ \iota = 0$; le morphisme ι étant un isomorphisme, il vient $\pi_{i|U} = 0$, ce qui achève la démonstration.

Un exemple. Fixons un corps k de caractéristique différente de 2 et 3 ; soit V la représentation de permutation sur le corps k associée à l'action de $\mathfrak{S}_3$ sur $\{1, 2, 3\}$. L'espace vectoriel V possède par définition une base (e_1, e_2, e_3) telle que $\sigma.e_i = e_{\sigma(i)}$ pour tout i et toute permutation σ.

Le vecteur $e_1 + e_2 + e_3$ appartient à V^G. La droite D qu'il engendre est donc une sous-représentation de V, irréductible puisque de dimension 1. La théorie assure que D possède un supplémentaire stable dans V. Nous allons en exhiber un. Soit W le sous-espace vectoriel de V formé des vecteurs dont les coordonnées (x, y, z) dans (e_1, e_2, e_3) satisfont l'équation $x+y+z = 0$. Il est immédiat que W est stable sous l'action de $\mathfrak{S}_3$; comme il est défini par une équation non nulle, c'est un plan.

Soit $\lambda \in k$. Supposons que $\lambda(e_1 + e_2 + e_3) \in W$. On a alors $3\lambda = 0$, et donc $\lambda = 0$ puisque $3 \neq 0$ dans k. Par conséquent, $D \cap W = \{0\}$ et $V = D \oplus W$.

Nous allons montrer que la représentation W de $\mathfrak{S}_3$ est irréductible. Pour cela, on remarque que le vecteur de W de coordonnées $(1, -1, 0)$ est un vecteur propre pour $\tau_{1,2}$, associé à la valeur propre (-1) ; et que $(1, 1, -2)$ est un vecteur propre pour $\tau_{1,2}$, associé à la valeur propre 1. Comme $1 \neq -1$ dans le corps k (il est de caractéristique différente de 2), l'endomorphisme $(\tau_{1,2})_{|W}$ a deux valeurs propres distinctes, 1 et -1 ; son sous-espace propre associé à 1 est $k \cdot (1, 1, -2)$; celui associé à (-1) est $k \cdot (1, -1, 0)$.

Si la représentation W n'était pas irréductible, elle possèderait une sous-représentation de dimension 1, c'est-à-dire une droite Δ stable. Étant en particulier stable sous $(\tau_{1,2})_{|W}$, la droite Δ serait engendrée par un vecteur propre de $(\tau_{1,2})_{|W}$, et serait donc égale ou bien à $k \cdot (1, 1, -2)$, ou bien à $k \cdot (1, -1, 0)$. Mais aucune de ces deux droites n'est stable sous $(\tau_{2,3})_{|W}$, car $(1, -2, 1)$ n'est pas colinéaire à $(1, 1, -2)$ et car $(1, -1, 0)$ n'est pas colinéaire à $(1, 0, -1)$. On aboutit donc à une contradiction.

Ainsi, $V = D \oplus W$ est une écriture de V en somme directe de représentations irréductibles.

11 Séance du 26 mars

J'ai traité le 4.1.16, en rajoutant une remarque : supposons que V est de dimension finie et soit $(e_1, \dots, e_n)$ une base de V. Soit $g \in G$; si M désigne la matrice de $\rho(g)$ dans $(e_1, \dots, e_n)$, la matrice de $\rho^*(g)$ dans la base duale $(e_1^*, \dots, e_n^*)$ est égale à ${}^tM^{-1}$: cela découle des propriétés connues de la transposition en dualité.

J'ai traité 4.1.17.

Produit tensoriel

J'ai donné plus de détails au sujet du produit tensoriel qu'il n'en figure dans le poly.

Motivation. Soient V et W deux K-espaces vectoriels. On cherche à définir une application bilinéaire $(vw) \mapsto v \otimes w$ sur $V \times W$, à valeur dans un K-espace vectoriel, et qui soit ≪la plus générale possible≫ : on souhaite, en quelque sorte, qu'elle ne vérifie rien d'autre que ce qui est imposé par la bilinéarité et la théorie générale des espaces vectoriels.

Comme souvent en mathématiques, le fait d'être ≪le plus général possible≫ s'exprime rigoureusement en termes de satisfaction d'une propriété universelle.

Proposition (variante de la proposition 4.1.19 du poly). *Soient V et W deux K-espaces vectoriels. Il existe un espace vectoriel $V \otimes_K W$ et une application bilinéaire $(v, w) \mapsto v \otimes w$ de $V \times W$ dans $V \otimes_K W$ telle que la propriété universelle suivante soit satisfaite : pour toute application bilinéaire b de $V \times_K W$ dans un K-espace vectoriel U, il existe une unique application* linéaire *f de $V \otimes_k W$ vers B telle que le diagramme*

$$\begin{array}{ccc} V \times W & \xrightarrow{b} & U \\ {\scriptstyle\otimes}\downarrow & \nearrow_{f} & \\ V \otimes_K W & & \end{array}$$

commute.

De plus, si (M, β) est un couple formé d'un K-espace vectoriel et d'une application bilinéaire $\beta : V \times W \to M$ qui satisfait la même propriété universelle, il existe une unique application linéaire i de $V \otimes_K W$ dans M telle que $i \circ \otimes = \beta$, et i est un isomorphisme.

Démonstration. Commençons par montrer l'existence de $(V \otimes_K W, \otimes)$. La preuve consiste essentiellement à *imposer par décret* les relations souhaitées.

Soit E un K-espace vectoriel possédant une base $e_{v,w}$ indexée par tous les couples (v, w) d'éléments de $V \times W$, et soit F le sous-espace vectoriel de E engendré par

$$\mathscr{S} = \{e_{v,w+\lambda w'} - e_{v,w} - \lambda e_{v,w'}, e_{v+\lambda v',w} - e_{v,w} - \lambda e_{v',w}\}_{v \in V, w \in W, \lambda \in K}.$$

On pose $V \otimes_K W = E/F$; pour tout $(v, w) \in V \times W$, on note $v \otimes w$ la classe de $e_{v,w}$ dans $V \otimes_K W$.

L'application $\otimes$ est bilinéaire. Il résulte en effet de la définition de F que l'on a, pour tout $(v, w) \in V \times W$ et tout $\lambda \in K$, les égalités

$$v \otimes (w + \lambda w') - v \otimes w + \lambda v \otimes w' = 0 \text{ et } (v + \lambda v') \otimes w - v \otimes w + \lambda v' \otimes w = 0$$

dans $V \otimes_K W = E/F$, d'où l'assertion.

Le couple $(V \otimes_K W, \otimes)$ satisfait la propriété universelle requise. En effet, commençons par remarquer que comme $(e_{v,w})_{v,w}$ est une base de E, et en particulier une partie génératrice de ce dernier, les $v \otimes w$ engendrent $V \otimes_K W$.

Soit U un K-espace vectoriel et soit b une application bilinéaire de $V \times W$ dans U. Nous allons montrer qu'il existe une unique application f comme dans l'énoncé. Commençons par l'unicité ; si f existe, la commutativité du diagramme assure que $f(v \otimes w) = b(v, w)$ pour tout $(v, w) \in V \times W$. La valeur de f est ainsi uniquement déterminée sur chacun des éléments de la forme $v \otimes w$ avec $v \in V$ et $w \in W$. Comme ceux-ci engendrent $V \otimes_K W$, on en déduit que f est uniquement déterminée.

Montrons maintenant l'existence de f. Soit ℓ l'unique application linéaire de E dans U qui envoie $e_{v,w}$ sur $b(v, w)$ pour tout $(v, w) \in V \times W$. La bilinéarité de b implique immédiatement que ℓ s'annule sur les éléments du système générateur $\mathscr{S}$ de F ; par conséquent, ℓ s'annule sur F et induit donc par passage au quotient une application linéaire $f : V \otimes_k W \to B$. Soit $(v, w) \in V \times W$. Comme $v \otimes w$ est la classe de $e_{v,w}$ modulo F, on a $f(v \otimes w) = \ell(e_{v,w}) = b(v, w)$. Ainsi, $f \circ \otimes = b$, ce qu'il fallait démontrer.

Unicité de $V \times_K W$. Soit (M, β) comme dans l'énoncé. La propriété universelle de $(V \otimes_K W, \otimes)$ assure l'existence d'une unique application linéaire $i : V \otimes_K W \to M$ telle que $i \circ \otimes = \beta$. Il reste à s'assurer que i est un isomorphisme.

La propriété universelle de (M, β) assure l'existence d'une unique application linéaire $j : M \to V \otimes_K W$ telle que $j \circ \beta = \otimes$. La composée $j \circ i$ est une application linéaire de $V \otimes_K W$ dans lui même, et l'on a $(j \circ i) \circ \otimes = \otimes$. Comme on a par ailleurs $\mathrm{Id}_{V \otimes_K W} \circ \otimes = \otimes$, la partie ≪unicité≫ de la propriété universelle de $(V \otimes_K W, \otimes)$ garantit que $j \circ i = \mathrm{Id}_{V \otimes_K W}$. On montre de même que $i \circ j = \mathrm{Id}_M$. □

Quelques commentaires.

1) Il résulte de la construction que $V \otimes_K W$ est engendré par les $v \otimes w$. Notons une conséquence : $V \otimes_K W$ est nul dès que l'un des deux facteurs est nul.

2) L'application $b : V \times K \to V$ qui envoie (v, λ) sur λv est bilinéaire ; il existe donc une unique application linéaire $f : V \otimes_K K \to V$ telle que $f \circ \otimes = b$; on vérifie (exercice !) que f est un isomorphisme, de bijection réciproque $v \mapsto v \otimes 1$.

3) Nous avons dit plus haut qu'il fallait penser à $\otimes$ comme à la loi bilinéaire la plus générale possible définie sur $V \times_K W$. Indiquons une propriété tangible qui apparaît comme une manifestation de ce principe un peu vague : si (v_i, w_i) est une famille d'éléments de $V \times_K W$ alors $\sum v_i \otimes w_i = 0$ si et seulement si $\sum b(v_i, w_i) = 0$ pour toute application bilinéaire b définie sur $V \times_W$ et à valeurs dans un K-espace vectoriel U.

En effet, l'implication $\Leftarrow$ est claire, puisque $\otimes$ est une application bilinéaire de $V \times W$ vers $V \otimes_K W$. Réciproquement, supposons que $\sum v_i \otimes w_i = 0$, et soit b une application bilinéaire définie sur $V \times W$ et à valeurs dans un K-espace vectoriel U. La propriété universelle du produit tensoriel garantit l'existence (et l'unicité) d'une application linéaire $f : V \otimes_K W \to U$ telle que $f \circ \otimes = b$. On a alors

$$\sum b(v_i, w_i) = \underbrace{\sum f(v_i \otimes w_i) = f\left(\sum v_i \otimes w_i\right)}_{\text{car } f \text{ est linéaire}} = 0.$$

4) Soit (e_i) une base de V et (f_j) une base de W. La famille $(e_i \otimes f_j)_{i,j}$ est alors une base de $V \otimes_K W$. En effet, les éléments de la forme $v \otimes w$ engendrent $V \otimes_K W$. Chacun de ces éléments est, par bilinéarité de $\otimes$, combinaison linéaire d'éléments de la forme $e_i \otimes f_j$; par conséquent, $(e_i \otimes f_j)_{i,j}$ est génératrice.

Il reste à s'assurer qu'elle est libre. Supposons donc donnée une famille $(\lambda_{i,j})$ de scalaires telle que $\sum \lambda_{ij} e_i \otimes f_j = 0$. Fixons (i_0, j_0), et soit b l'application de $V \times W$ dans K qui envoie $(\sum \alpha_i e_i, \sum \beta_j f_j)$ sur $\alpha_{i_0}\beta_{j_0}$. L'application b est visiblement bilinéaire ; il existe donc une application linéaire (par ailleurs unique) $f : V \otimes_K W \to K$ telle que $f \circ \otimes = b$. On a en particulier pour tout (i, j) l'égalité $f(e_i \otimes f_j) = b(e_i, f_j)$, qui vaut 0 si $(i, j) \neq (i_0, j_0)$ et 1 sinon.

En appliquant f à $\sum \lambda_{ij} e_i \otimes f_j$, on obtient $\lambda_{i_0,j_0} = 0$, et la famille $(e_i \otimes f_j)_{i,j}$ est bien libre, ce qui achève la preuve.

5) Voici quelques conséquences de 4) : si V et W sont non nuls, alors $V \otimes_K W$ est non nul ; si V et W sont de dimension finie, alors $V \otimes_k W$ est de dimension finie, et $\dim (V \otimes_K W) = \dim V \times \dim W$.

6) Si $W = W_1 \oplus W_2$, on montre (exercice) l'existence d'un isomorphisme naturel

$$V \otimes_K W \simeq (V \otimes_K W_1) \oplus (V \otimes_K W_2).$$

J'ai ensuite défini le produit tensoriel de deux représentations, comme dans le poly en bas de la page 32. J'ai rajouté une description matricielle de ce produit, dans le cas de la dimension finie. La voici. On se donne donc (V, ρ) et (W, σ) deux représentations de G de dimension finie, et l'on fixe une base (e_i) de V et une base (f_j) de W. Soit $g \in G$. Notons (a_{ri}) la matrice de $\rho(g)$ dans (e_i), et (b_{sj}) la matrice de $\sigma(g)$ dans (f_j).

Fixons i et j. On a

$$\rho \otimes \sigma(g)(e_i \otimes f_j) = \rho(g)(e_i) \otimes \sigma(g)(f_j))$$

$$= \left(\sum_r a_{ri} e_r\right) \otimes \left(\sum_s b_{sj} f_s\right) = \sum_{r,s} a_{ri} b_{sj} e_r \otimes f_s.$$

Ainsi, la matrice de $\rho \otimes \sigma$ dans $(e_i \otimes e_j)$ est égale à $(a_{ri} b_{sj})_{(r,s),(i,j)}$.

Je n'ai pas traité l'exemple 4.1.20. J'ai traité le 4.1.21. En ce qui concerne le lemme 4.1.22, je n'ai pas mentionné l'injectivité de ι en général, j'ai admis ii), mais j'ai donné une preuve de i). La voici : on se fixe une base (e_i) de V et une base (f_j) de W. Par le point 4) ci-dessus, la famille $(f_j \otimes e_i^*)$ est une base de $W \otimes_K V^*$.

Fixons (i,j). L'image de $f_j \otimes e_i^*$ par ι est l'application K-linéaire de V dans W qui envoie un vecteur v sur $e_i^*(v)f_j$. On voit en particulier : que si $i' \neq i$ alors $\iota(f_j \otimes e_i^*)(e_i') = 0$; et que $\iota(f_j \otimes e_i^*)(e_i) = f_j$. Ainsi, $\iota(f_j \otimes e_i^*)(e_i')$ est l'application linéaire de matrice E_{ij} dans les bases $(e_i), (f_j)$. On voit donc que ι transforme une base de $W \otimes_K V^*$ en une base de $\mathrm{Hom}_K(V,W)$; elle est par conséquent bijective.

J'ai démontré le lemme 4.1.23. Voici plus précisément ce que j'ai expliqué. L'application de $V \times V^*$ vers K qui envoie un coupe (v,φ) sur $\varphi(v)$ est bilinéaire ; elle induit donc une forme linéaire $\psi : V \otimes_K V^*$ vers K. Lorsque V est de dimension finie, la composée de ψ avec l'isomorphisme $\mathrm{End}_k V \simeq V \otimes_K V^*$ est égale à la trace.

Il suffit en effet de le vérifier sur une base de $\mathrm{End}_k V$. Fixons une base (e_i) de V. Pour tout (i,j), on note ℓ_{ij} l'endomorphisme de V de matrice (E_{ij}) dans la base (e_i). Les (ℓ_{ij}) forment une base de $\mathrm{End}_K V$.

Fixons (i,j). Par ce qu'on a vu plus haut, l'isomorphisme entre $\mathrm{End}_k V$ et $V \otimes_K V^*$ envoie ℓ_{ij} sur $e_j \otimes e_i^*$. Quand on applique ψ à ce dernier on trouve $e_i^*(e_j)$, soit δ_{ij}, qui n'est autre que $\mathrm{Tr}(\ell_{ij})$. Ceci achève la démonstration.

Caractères d'une représentation

J'ai suivi pour l'essentiel le paragraphe 4.2, en me limitant dès le début au cas où le corps de base est $\mathbb{C}$.

J'ai donc énoncé et prouvé le théorème 4.2.3 uniquement dans le cas complexe ; j'ai en conséquence commencé par établir 4.2.6 (le caractère de la contragrédiente de ρ est le conjugué du caractère de ρ), puis énoncé le th. 4.2.3 assertions ii), iii) et iv), en remplaçant dans iv) $\chi_V(g^{-1})$ par $\overline{\chi_V(g)}$.

J'ai donné une preuve de l'assertion iii) qui diffère de celle du poly, et qui était la suivante. On fixe $g \in G$, on choisit une base (e_i) de V, et l'on note (a_{ri}) la matrice de $\rho_V(g)$ dans la base (e_i). On choisit une base (f_j) de W, et l'on note (b_{sj}) la matrice de $\rho_W(g)$ dans la base (e_i). D'après ce qu'on a vu plus haut, ma matrice de $\rho_{V\otimes W}(g)$ dans la base $(e_i \otimes f_j)$ de $V \otimes W$ est égale à $(a_{ri}b_{sj})_{(r,s)(i,j)}$. La trace de $\rho_{V\otimes W}(g)$ est donc égale à

$$\sum_{(i,j)} a_{ii}b_{jj} = (\sum_i a_{ii})(\sum_j b_{jj}) = \mathrm{Tr}(\rho_V(g)) \cdot \mathrm{Tr}(\rho_W(g)).$$

Ainsi, $\chi_{V\otimes W}(g) = \chi_V(g) \cdot \chi_W(g)$.

12 Séance du 2 avril 2012

Résultats généraux sur les caractères

J'ai démontré le théorème 4.2.7, le corollaire 4.2.8 et le théorème 4.2.9, en rajoutant quelques détails dans les preuves, que je vais maintenant donner.

Début de la preuve du corollaire 4.2.8. J'ai justifié l'affirmation sur la trace d'un élément r de la représentation régulière. Plus généralement, soit X un ensemble fini sur lequel G opère, et soit KX la représentation de permutation associée. L'espace KX possède une base $(e_x)_{x\in X}$, telle que $g.e_x = e_{g.x}$ pour tout g et tout x. La matrice de $v \mapsto gv$ dans la base (e_x) est une matrice de

permutation ; sa trace est donc égale au nombre de 1 qui se trouvent sur la diagonale, soit encore eu nombre de vecteurs e_x tels que $e_x = g.e_x = e_{g.x}$, c'est-à-dire finalement au nombre de points fixes de g dans l'ensemble X. Dans le cas de la représentation régulière, si $g \neq e$ l'application $h \mapsto gh$ n'a aucun point fixe, et si $g = e$ c'est l'identité, et elle a donc $|G|$ point fixe, d'où l'affirmation en début de preuve du cor. 4.2.8.

Preuve du théorème 4.2.9. Il y a deux points à préciser.

- Justification du fait que φ_V est un G-morphisme. Soit $h \in G$. On a

$$\rho_V(h) \circ \varphi_V \circ \rho_V(h^{-1}) = \underbrace{\sum_{g\in G} f(g)h \circ \rho_V(hgh^{-1}) = \sum_{g\in G} f(hgh^{-1})h \circ \rho_V(hgh^{-1})}_{\text{car } f \text{ est centrale}}$$

$$= \sum_{g\in G} f(g)\rho_V(g) = \varphi_V,$$

l'avant-dernière égalité étant due au fait que $g \mapsto hgh^{-1}$ est une bijection de G sur lui-même. Ainsi, $\rho_V(h)\varphi_V\rho_V(h)^{-1} = \varphi_V$ pour tout $h \in G$, ce qui signifie exactement que φ_V est un G-morphisme.

- La preuve utilise implicitement le fait que si V est irréductible, alors V^* l'est aussi (puisqu'on dit que le produit scalaire de f et χ_{V^*} est nul). Voici comment le justifier. On remarque tout d'abord que l'isomorphisme naturel $V \simeq V^{**}$ est un isomorphisme équivariant (exercice). Supposons maintenant que V est irréductible, et soit W une sous-représentation de V^*. Son orthogonal $W^\perp$ dans V^{**} est alors une sous-représentation de ce dernier. Comme $V^{**} \simeq V$ il est irréductible ; par conséquent $W^\perp = V^{**}$ ou $W^\perp = \{0\}$, ce qui signifie que $W = 0$ ou $W = V^*$; ainsi, V^* est irréductible.

Deux exemples : les représentations irréductibles de $\mathfrak{S}_3$ et $\mathfrak{S}_4$

J'ai appliqué ce qui précède à la détermination des tables de caractère de $\mathfrak{S}_3$ et $\mathfrak{S}_4$; je n'ai pas traité les exemples $\mathbb{Z}/n\mathbb{Z}$, D_4 et H_8 du poly ; je vous invite à les lire avec attention.

Avant d'expliciter ces exemples, faisons quelques remarques.

1) Soit G un groupe et soit V une représentation de G, donnée par un morphisme $\rho : G \to \mathrm{GL}(V)$. Soit H un groupe et soit $f : H \to G$ un morphisme. La composée $\rho \circ f$ définit un morphisme de H vers $\mathrm{GL}(V)$, et fait donc de V une représentation de H. Si χ désigne le caractère de V comme représentation de G, et ψ son caractère comme représentation de H, on a par construction $\psi = \chi \circ f$.Tout sous-espace vectoriel de V stable sous l'action de G est encore stable sous l'action de G, et la réciproque est vraie si f est surjective (exercice). En particulier, si f est surjective et si V est irréductible comme représentation de G, alors V est encore irréductible comme représentation de H.

2) Comme tout caractère est une fonction centrale on préfère, pour simplifier l'écriture, présenter les caractères comme des fonctions non pas d'un groupe G vers $\mathbb{C}$, mais de l'ensemble $\mathscr{C}$ des classes de conjugaison de G vers $\mathbb{C}$. Il faut alors

faire attention à la définition du produit scalaire : si χ et ψ sont deux fonctions centrales de G vers $\mathbb{C}$, leur produit scalaire $\langle \chi, \psi \rangle$ s'écrit $(1/|G|) \sum_{g \in G} \chi(g) \cdot \overline{\psi(g)}$. Si on les voit maintenant comme des fonctions de $\mathscr{C}$ vers G, et si pour toute classe $c \in \mathscr{C}$ on note par abus $\chi(c)$ et $\psi(c)$ les valeurs constantes respectives de χ et ψ sur c, on alors

$$(*)\ (*)\ \langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{c \in \mathscr{C}} |c| \cdot \chi(c) \cdot \overline{\psi(c)}\ ;$$

il ne faut pas oublier le cardinal de la classe de conjugaison dans la formule.

3) La remarque qui suit est très utile pour calculer des tables de caractères, et j'ai donc choisi de la faire figurer ici, même si je ne l'ai pas faite en cours. Soit G un groupe fini, et soient $\chi_1, \ldots, \chi_r$ ses caractères irréductibles, vus comme des fonctions sur l'ensemble $\mathscr{C}$ des classes de conjugaison de G ; l'ensemble $\mathscr{C}$ est lui-même de cardinal r, écrivons $\mathscr{C} = (c_1, \ldots, c_r)$. La famille $(\chi_i(c_j))$ est une matrice carrée M de taille r. Les caractères forment une famille orthonormée pour le produit scalaire défini plus haut ; cela se traduit, en vertu de $(*)$, par l'égalité

$$\frac{1}{|G|}\ {}^t\overline{M} D M = I_r,$$

où $D = \mathrm{diag}(|c_1|, \ldots, |c_r|)$. Par conséquent, ${}^t\overline{M}$ est inversible d"inverse $(1/|G|)DM$. On a donc également

$$\frac{1}{|G|} D M\ {}^t\overline{M} = I_r.$$

Soient i et j deux entiers compris entre 1 et et r avec $i \neq j$. Le terme (i, j) de la matrice $\frac{1}{|G|} D M\ {}^t\overline{M}$ est égal à $(c_i/|G|) \sum_\ell \chi_i(c_\ell) \overline{\chi_j(c_\ell)}$; mais comme cette matrice est égale à l'identité, ledit terme est nul. On voit ainsi que les vecteurs colonnes $(\chi_i(c_j))_j$ sont, lorsque i varie, deux à deux orthogonaux pour le produit hermitien usuel, sans intervention du cardinal des classes de conjugaison.

4) Soit n un entier. Le groupe $\mathfrak{S}_n$ agit sur $\{1, \ldots, n\}$; notons W_n la représentation de permutation associée sur $\mathbb{C}$. Le vecteur $\sum e_i$ est non nul, et est fixe sous l'action de $\mathfrak{S}_n$. Il engendre donc une droite D_n stable sous $\mathfrak{S}_n$, l'action induite étant triviale : D_n est donc isomorphe à la représentation triviale de dimension 1 de $\mathfrak{S}_n$, notée $\mathbf{1}_{\mathfrak{S}_n}$. La théorie assure que D_n possède un supplémentaire stable ; mais ici, il est facile d'en exhiber un : on peut prendre $V_n := \{\sum \lambda_i e_i, \sum \lambda_i = 0\}$. La représentation V_n est de dimension $n - 1$.

Calculons son caractère. Comme W_n est une représentation de permutation, $\chi_{W_n}(\sigma)$ est égal au nombre $|\mathrm{Fix}\ \sigma|$ de points fixes de σ pour toute $\sigma \in \mathfrak{S}_n$; par ailleurs, $\chi_{D_n}(\sigma) = 1$ puisque σ agit trivialement sur la droite D_n.

L'égalité $\chi_{W_n} = \chi_{D_n} + \chi_{V_n}$ assure alors que $\chi_{V_n}(\sigma)$ est égal, pour toute $\sigma \in \mathfrak{S}_n$, à $|\mathrm{Fix}\ \sigma| - 1$.

5) La signature définit un morphisme $\mathfrak{S}_n \to \{-1, 1\} \subset \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ qui induit une représentation Σ_n de $\mathfrak{S}_n$, de dimension 1 et donc irréductible, que l'on appelle la *signature.*

Table des caractères de $\mathfrak{S}_3$. Le groupe $\mathfrak{S}_3$ a 3 classes de conjugaison : la classe $c_\emptyset$ de l'identité, qui est un singleton ; la classe $c_{(**)}$ des transpositions, qui est

de cardinal 3 ; et la classe $c_{(***)}$ des trois cycles, qui est de cardinal 2. Il s'ensuit que $\mathfrak{S}_3$ admet trois (classes d'isomorphie de) représentations irréductibles. On en connaît déjà deux : la représentation triviale $\mathbf{1}_{\mathfrak{S}_3}$, et la signature Σ_3. Le caractère $\chi_{\mathbf{1}_{\mathfrak{S}_3}}$ est trivial, et χ_{Σ_3} envoie $c_\emptyset$ et $c_{(***)}$ sur 1, et $c_{(**)}$ sur (-1). Il reste une troisième représentation irréductible U . Si d désigne sa dimension on a $1^2+1^2+d^2=6$, et donc $d=2$. Pour calculer son caractère χ, on remarque que comme elle est de dimension 2, on a $\chi(c_\emptyset)=2$. Il reste à calculer $a=\chi(c_{(**)})$ et $b=\chi(c_{(***)})$. Dans la table de caractère suivantes

	$c_\emptyset$	$c_{(**)}$	$c_{(***)}$
$\mathbf{1}_{\mathfrak{S}_3}$	1	1	1
Σ_3	1	-1	1
U	2	a	b

les colonnes sont orthogonales en vertu de 3) ci-dessus. Il vient alors $a=0$ et $b=-1$. Comme l'identité a trois points fixes, comme une transposition en a un, et comme un 3-cycle n'en a pas, on voit que $\chi_V=\chi_{V_3}$; par conséquent, $U\simeq V_3$. La table des caractères de $\mathfrak{S}_3$ est ainsi

	$c_\emptyset$	$c_{(**)}$	$c_{(***)}$
$\mathbf{1}_{\mathfrak{S}_3}$	1	1	1
Σ_3	1	-1	1
V_3	2	0	-1

.

Montrons comment calculer la décomposition de $V_3\otimes_{\mathbb{C}} V_3$ en somme directe de représentations irréductibles. Le caractère ψ de $V_3\otimes_{\mathbb{C}} V_3$ est égal à $\chi_{V_3}^2$; il envoie donc $c_\emptyset$ sur 4, $c_{(**)}$ sur 0, et $c_{(***)}$ sur 1. Pour déterminer la décomposition de $V_3\otimes_{\mathbb{C}} V_3$, il suffit de calculer le produit scalaire de ψ avec chacun des trois caractères irréductibles – et là, attention, il ne faut pas oublier le cardinal classes de conjugaison.

$$\langle\psi,\chi_{\mathbf{1}_{\mathfrak{S}_3}}\rangle=\frac{1}{6}(4+2)=1.$$

$$\langle\psi,\chi_{\Sigma_3}\rangle=\frac{1}{6}(4+2)=1.$$

$$\langle\psi,\chi_{V_3}\rangle=\frac{1}{6}(8-2)=1.$$

Ainsi, $V_3\otimes_{\mathbb{C}} V_3\simeq \mathbf{1}_{\mathfrak{S}_3}\oplus\Sigma_3\oplus V_3$.

Table des caractères de $\mathfrak{S}_4$. Le groupe $\mathfrak{S}_4$ a 5 classes de conjugaison : la classe $c_\emptyset$ de l'identité, qui est un singleton ; la classe $c_{(**)}$ des transpositions, qui est de cardinal 6 ; la classe $c_{(**)(**)}$ des produits de deux transpositions, qui est de cardinal 3 ; la classe $c_{(***)}$ des trois cycles, qui est de cardinal 8 ; et la classe $c_{(****)}$ des 4-cycles, qui est de cardinal 6.

Par conséquent, $\mathfrak{S}_4$ possède cinq (classes d'isomorphie de) représentations irréductibles. On en connaît déjà deux : la représentation triviale $\mathbf{1}_{\mathfrak{S}_4}$, et la signature Σ_4. Le caractère $\chi_{\mathbf{1}_{\mathfrak{S}_4}}$ est trivial, et χ_{Σ_4} envoie $c_\emptyset, c_{(**)(**)}$ et $c_{(***)}$ sur 1, et $c_{(**)}$ et $c_{(****)}$ sur (-1).

Nous allons maintenant vérifier que la représentation V_4 est irréductible. Son caractère a été calculé en 4) : il envoie σ sur $|\mathrm{Fix}\,\sigma| - 1$. Il s'ensuit que χ_{V_4} vaut 3 sur $c_\emptyset$, 1 sur $c_{(**)}$, (-1) sur $c_{(**)(**)}$, 0 sur $c_{(***)}$, et (-1) sur $c_{(****)}$.

Calculons son carré scalaire – sans oublier le cardinal des classes de conjugaison. Il vaut

$$\frac{1}{24}(9 + 1 \cdot 6 + 1 \cdot 3 + 1 \cdot 6) = 1.$$

Par conséquent, V_4 est irréductible.

Considérons maintenant la représentation $V_4 \otimes_{\mathbb{C}} \Sigma_4$. Elle est de dimension 3, et son caractère est égal à $\chi_{V_4} \cdot \chi_{\Sigma_4}$. Il vaut dès lors 3 sur $c_\emptyset$, -1 sur $c_{(**)}$, (-1) sur $c_{(**)(**)}$, 0 sur $c_{(***)}$, et (1) sur $c_{(****)}$. On observe deux choses à son sujet : il diffère de χ_{V_4}, ce qui montre que $V_4 \otimes_{\mathbb{C}} \Sigma_4$ n'est pas isomorphe à V_4 ; et il a même carré scalaire que χ_{V_4}, puisque ses valeurs sont au signe près les mêmes que celles de χ_{V_4}. Il est dès lors de carré scalaire égal à 1, ce qui montre que $V_4 \otimes_{\mathbb{C}} \Sigma_4$ est irréductible.

On a ainsi exhibé quatre représentations irréductibles de $\mathfrak{S}_4$; il en manque une, disons W. Si d désigne sa dimension on a $1^2 + 1^2 + 3^2 + 3^2 + d^2 = 24$; il vient $d = 2$. On a $\chi_W(c_\emptyset) = \dim W = 2$; appelons a, b, c et d les valeurs de χ_W sur $c_{(**)}$, $c_{(**)(**)}$, $c_{(***)}$, et $c_{(****)}$. La table de caractères de $\mathfrak{S}_4$ se présente ainsi :

	$c_\emptyset$	$c_{(**)}$	$c_{(**)(**)}$	$c_{(***)}$	$c_{(****)}$
$\mathbf{1}_{\mathfrak{S}_4}$	1	1	1	1	1
Σ_4	1	-1	1	1	-1
V_4	3	1	-1	0	-1
$V_4 \otimes_{\mathbb{C}} \Sigma_4$	3	-1	-1	0	1
W	2	a	b	c	d

.

Comme les colonnes sont orthogonales pour le produit scalaire usuel, il vient : $a = 0$, $b = 2$, $c = -1$, $d = 0$. Ainsi, la table des caractères de $\mathfrak{S}_4$ est finalement

	$c_\emptyset$	$c_{(**)}$	$c_{(**)(**)}$	$c_{(***)}$	$c_{(****)}$
$\mathbf{1}_{\mathfrak{S}_4}$	1	1	1	1	1
Σ_4	1	-1	1	1	-1
V_4	3	1	-1	0	-1
$V_4 \otimes_{\mathbb{C}} \Sigma_4$	3	-1	-1	0	1
W	2	0	2	-1	0

.

La théorie assure ainsi l'existence d'une représentation W de $\mathfrak{S}_4$ irréductible, de degré 2, ayant le caractère indiqué ci-dessus. On peut en donner une description un peu plus tangible, comme suit.

Soit $\mathscr{E}$ l'ensemble des partitions de $\{1, 2, 3, 4\}$ en deux ensembles de cardinal 2. L'ensemble $\mathscr{E}$ comprend trois éléments :

$$\{1,2\} \coprod \{3,4\}, \quad \{1,3\} \coprod \{2,4\} \text{ et } \{1,4\} \coprod \{2,3\}.$$

Le groupe $\mathfrak{S}_4$ opère de façon naturelle sur $\mathscr{E}$, d'où un morphisme de $\mathfrak{S}_4$ vers $\mathfrak{S}_{\mathscr{E}}$ puis, par composition avec un isomorphisme $\mathfrak{S}_{\mathscr{E}} \simeq \mathfrak{S}_3$ (obtenu en numérotant arbitrairement $\mathscr{E}$) , un morphisme $\varphi : \mathfrak{S}_4 \to \mathfrak{S}_3$. On vérifie (exercice) que le noyau de φ est le groupe de Klein $\{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$. Comme $\mathfrak{S}_4$

est de cardinal 24, comme $\mathfrak{S}_3$ est de cardinal 6, et comme le groupe de Klein est de cardinal 4, l'égalité $24/4 = 6$ assure que φ est surjectif.

Dès lors, la représentation V_3 de $\mathfrak{S}_3$, qui est irréductible et de dimension 2, induit *via* φ une représentation de $\mathfrak{S}_4$, qui est également irréductible et de dimension 2 (voir 1) ci-dessus). Elle coïncide nécessairement avec W – mais j'invite le lecteur à vérifier par le calcul que $\chi_{V_3} \circ \varphi$ est bien égal à χ_W.

Commentaire culturel. Le lecteur attentif aura remarqué que la construction des différentes représentations irréductibles de $\mathfrak{S}_3$ et $\mathfrak{S}_4$ évoquées ci-dessus ne fait pas intervenir le corps des complexes : toutes peuvent être définie sur le corps $\mathbb{Q}$ des nombres rationnels, et *a fortiori* sur tout corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{C}$, et notamment $\mathbb{R}$.

Notons Σ_4', V_3' et V_4', les représentations $\mathbb{R}$-linéaires définies exactement comme Σ_4, V_3 et V_4 (simplement, le corps de base est $\mathbb{R}$ au lieu de $\mathbb{C}$) ; elles sont irréductibles, de même que $V_4' \otimes_{\mathbb{R}} \Sigma_4'$ (on peut le déduire formellement de l'irréductibilité des représentations complexes correspondantes – pour Σ_4', c'est par ailleurs automatique puisqu'elle est de dimension 1).

Nous avions déjà signalé plus haut que V_3' s'identifie à la représentation de $\mathfrak{S}_3$ consistant à voir celui-ci comme le groupe des isométries d'un triangle équilatéral (centré en l'origine).

On vérifie que V_4' s'identifie à la représentation de $\mathfrak{S}_4$ consistant à voir celui-ci comme le groupe des isométries d'un tétraèdre régulier (centré en l'origine), et que $V_4' \otimes_{\mathbb{R}} \Sigma_4'$ s'identifie à la représentation de $\mathfrak{S}_4$ consistant à voir celui-ci comme le groupe des isométries *directes* d'un cube centré en l'origine.