Prépa CAPES UPMC 2008 Emmanuel Ferrand, Laurent Koelblen, Matthieu Romagny

Lundi 3 novembre 2008

Groupes monogènes, groupes symétriques

Groupes monogènes et cycliques

Exercice 1 On dit qu'un groupe est *monogène* s'il peut être engendré par un seul élément.
(1) Montrer qu'un groupe monogène est isomorphe, soit à $\mathbb{Z}$, soit à $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geq 1$.
(2) Montrez que le groupe $G = \mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Corrigé exercice 1
(1) On commence par décrire explicitement le sous-groupe $\langle x \rangle$ engendré par un élément x dans un groupe G. Il est clair que toutes les puissances x^k de x sont dans le sous-groupe engendré par x ; comme x^{-1} est dans le sous-groupe engendré par x, on a les puissances avec $k < 0$ aussi bien que les puissances avec $k \geq 0$. Comme $\{x^k\,, k \in \mathbb{Z}\}$ est un sous-groupe de G, finalement $\langle x \rangle = \{x^k\,, k \in \mathbb{Z}\}$.

Revenons à la question. Soit G un groupe monogène, il peut donc être engendré par un élément x. Ceci signifie que $\{x^k\,, k \in \mathbb{Z}\} = G$, ou encore, que le morphisme $f : \mathbb{Z} \to G$ défini par $f(k) = x^k$ est surjectif. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un $n \geq 0$. Si $n = 0$ le morphisme f est un isomorphisme et $G \simeq \mathbb{Z}$, et si $n \geq 1$ le morphisme f induit un isomorphisme $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G$.
(2) Nous allons aboutir à une contradiction en supposant que $G = \mathbb{Z} \times \mathbb{Z}$ est monogène. Soit x un générateur, on peut écrire $x = (a, b)$ avec a et b dans $\mathbb{Z}$. Comme G est un groupe abélien, on utilise naturellement une notation additive, en particulier on parle de multiples kx au lieu de puissances x^k. Comme x engendre G, les éléments $(0, 1)$ et $(1, 0)$ sont des multiples de x :

$$(0, 1) = (ka, kb) \quad \text{et} \quad (1, 0) = (\ell a, \ell b) \quad \text{avec} \quad (k, \ell) \in \mathbb{Z}^2\ .$$

Comme $\ell a = 1$ l'entier a est non nul, donc $ka = 0$ entraîne $k = 0$. Mais alors l'égalité $kb = 1$ est impossible. Par contraposée, G n'est pas monogène.

Exercice 2 (1) Montrez que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ est $n/\operatorname{pgcd}(k, n)$.
(2) Calculez l'ordre de (k, ℓ) dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Rappel sur le pgcd : avant de s'attaquer à la question (1), il est utile de commencer par un bref rappel sur le pgcd de deux entiers relatifs a et b. Le pgcd est bien défini lorsque a ou b n'est pas nul.

Une façon de le définir est de considérer l'ensemble des entiers naturels $e \in \mathbb{N}$ qui divisent a et b, c'est-à-dire tels qu'il existe des entiers relatifs u et v tels que $a = eu$ et $b = ev$. (On note alors $e|a$ et $e|b$.) Comme on a supposé que a ou b n'est pas nul, disons, par exemple $a \neq 0$, alors $e \leq |a|$ et donc cet ensemble d'entiers e est majoré. Donc il possède un plus grand élément que l'on note d et que l'on appelle le *plus grand commun diviseur*, ou *pgcd*, de a et b. On note $d = \text{pgcd}(a, b)$ ou parfois $d = a \wedge b$.

Une autre façon de définir le pgcd est de considérer l'ensemble des entiers relatifs $n \in \mathbb{Z}$ qui sont somme d'un multiple de a et d'un multiple de b, ou plus formellement, l'ensemble

$$\{n \in \mathbb{Z}\,, \exists (k, l) \in \mathbb{Z}^2\,, n = ka + lb\}\ .$$

Cet ensemble est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour un certain $d \geq 1$ (d ne peut pas être nul car on a supposé que a ou b n'est pas nul). On montre que cet entier naturel d est le même entier que dans la définition qui précède, c'est le pgcd de a et b.

Lorsque $\text{pgcd}(a, b) = 1$ on dit aussi que a et b sont *premiers entre eux*. Rappelons-nous un résultat important concernant les entier premiers entre eux : le *lemme de Gauss*, qui dit que si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Pour calculer le pgcd, la méthode la plus systématique (et bien souvent la meilleure) est d'utiliser l'algorithme d'Euclide, que je ne décris pas ici (je vous envoie à un livre de cours d'Arithmétique). Une autre méthode est d'écrire les nombres a et b comme produits de facteurs premiers. Supposons que a et b sont positifs pour simplifier (sinon, on met les signes -1 où il le faut). On peut écrire $a = (p_1)^{\alpha_1} \dots (p_1)^{\alpha_r}$ et $b = (p_1)^{\beta_1} \dots (p_1)^{\beta_r}$, où les p_i sont des nombres premiers distincts, avec des exposants éventuellement nuls. On fera bien attention au fait qu'*il ne s'agit pas des décompositions en facteurs premiers de a et b*, car dans la décomposition en facteurs premiers n'interviennent que des exposants > 0. On a alors

$$\text{pgcd}(a, b) = (p_1)^{\min(\alpha_1, \beta_1)} \dots (p_1)^{\min(\alpha_r, \beta_r)}\ .$$

Voici un dernier commentaire sur le pgcd. Soient a et b deux entiers non tous deux nuls, et $d = \text{pgcd}(a, b)$. Comme $d|a$ et $d|b$, il existe des entiers relatifs a', b' tels que $a = da'$ et $b = db'$, et de plus $\text{pgcd}(a', b') = 1$. L'existence des écritures

$$a = da' \quad , \quad b = db' \quad \text{avec} \quad \text{pgcd}(a', b') = 1$$

caractérise le pgcd de a et b, et est souvent extrêmement utile pour le manipuler.

Corrigé exercice 2, question (1)

Posons $d = \text{pgcd}(k, n)$ avec $k = dk'$, $n = dn'$ et $\text{pgcd}(k', n') = 1$. Il s'agit de montrer que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ est n'. Soit u un entier positif tel que $uk = 0$ dans $\mathbb{Z}/n\mathbb{Z}$. Ceci signifie qu'il existe v tel que $uk = vn$, ou encore $udk' = vdn'$. On en déduit $uk' = vn'$. En particulier n' divise uk', et comme n' et k' sont premiers entre eux, d'après le lemme de Gauss n' divise u, c'est-à-dire qu'il existe un entier w tel que $u = wn'$. En particulier $u \geq n'$, et comme $n'k = n'dk' = nk'$ est nul dans $\mathbb{Z}/n\mathbb{Z}$, on a bien montré que n' est le plus petit entier u tel que $uk = 0$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire, c'est l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$.

Rappel sur le ppcm : la question (2) est l'occasion de faire des rappels sur le ppcm, parallèles à ceux sur le pgcd. Ici on n'a pas besoin de supposer que a ou b est non nul. On considère l'ensemble des entiers naturels $e \in \mathbb{N}$ qui sont multiples à la fois de a et de b. C'est un sous-ensemble non vide de $\mathbb{N}$, donc il possède un plus petit élément noté m et appelé *plus petit commun multiple*, ou *ppcm*, de a et b. On note $m = \mathrm{ppcm}(a, b)$ ou parfois $m = a \vee b$.

On peut aussi considérer l'ensemble des entiers relatifs $n \in \mathbb{Z}$ qui sont multiples de a et de b, qui n'est autre que l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$. Cet ensemble est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$ pour un certain $m \geq 1$. Cet entier naturel m est le même entier que dans la définition qui précède, c'est le ppcm de a et b.

Pour calculer le ppcm, la méthode consistant à écrire les nombres a et b comme produits de facteurs premiers $a = (p_1)^{\alpha_1} \dots (p_1)^{\alpha_r}$ et $b = (p_1)^{\beta_1} \dots (p_1)^{\beta_r}$ fonctionne aussi. (On suppose ici aussi que a et b sont positifs pour simplifier.) Le résultat est :

$$\mathrm{ppcm}(a, b) = (p_1)^{\max(\alpha_1, \beta_1)} \dots (p_1)^{\max(\alpha_r, \beta_r)} \ .$$

Il n'y a pas véritablement de méthode analogue à celle de l'algorithme d'Euclide pour le pgcd, mais on peut s'y ramener toutefois, comme je l'explique dans quelques lignes.

Une propriété importante qui relie les nombres $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$ est la relation $dm = |ab|$. Notez que si a et b sont positifs on a plus simplement $dm = ab$, mais pour définir le pgcd et le ppcm nous n'avons pas supposé que a et b étaient positifs ; en revanche d et m ont été définis comme étant positifs. Pour démontrer que $dm = ab$ lorsque a et b sont positifs, on utilise les écritures

$$d = (p_1)^{\min(\alpha_1, \beta_1)} \dots (p_1)^{\min(\alpha_r, \beta_r)} \quad \text{et} \quad m = (p_1)^{\max(\alpha_1, \beta_1)} \dots (p_1)^{\max(\alpha_r, \beta_r)} \ .$$

Je vous laisse faire cette petite démonstration à titre d'exercice.

Je vous ai annoncé juste au-dessus qu'on peut se ramener à une méthode utilisant l'algorithme d'Euclide pour calculer le ppcm : en effet, commencez par calculer le pgcd en utilisant l'algorithme d'Euclide, puis utilisez la formule $dm = |ab|$. Sauf dans le cas où les nombres a et b ont des décompositions en facteurs premiers faciles à trouver (ce qui n'est pas le cas pour des entiers quelconques !!), cette méthode sera plus rapide.

Corrigé exercice 2, question (2)

Soit $n' = n/\,\mathrm{pgcd}(k, n)$ l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ = et $m' = m/pgcd(\ell, m)$ l'ordre de ℓ dans $\mathbb{Z}/m\mathbb{Z}$. On va montrer que l'ordre de (k, ℓ) dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est le ppcm de n' et de m'. En fait, ceci est très général : si G et H sont deux groupes, $x \in G$ est un élément d'ordre a et $y \in H$ est un élément d'ordre b, alors l'élément (x, y) du groupe produit direct $G \times H$ est d'ordre $\mathrm{ppcm}(a, b)$. Nous allons démontrer cela. Soit $u \geq 0$ un entier tel que $(x, y)^u = (x^u, y^u) = 1$ dans $G \times H$. Alors $x^u = 1$ dans G donc u est multiple de a (c'est une propriété de l'ordre a), et $y^u = 1$ dans H donc u est multiple de b. Ainsi u est un multiple commun de a et b. De plus, clairement pour tout multiple commun u de a et b on a $(x, y)^u = 1$. Donc l'ordre de (x, y) est le plus petit multiple commun, c'est-à-dire le ppcm, de a et b.

Exercice 3 Soit $n \geq 1$ un entier. On note $\varphi(n)$ le nombre d'entiers $1 \leq k \leq n$ premiers avec n (la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ est appelée *fonction indicatrice d'Euler*).

(1) Montrer que pour tout entier relatif non nul $a \in \mathbb{Z}$, premier avec n, on a $a^{\varphi(n)} \equiv 1\ (n)$.
(2) Soit p un nombre premier et $a \in \mathbb{Z}$. Montrer qu'on a $a^p \equiv a\ (p)$.

Corrigé exercice 3
(1) On sait que dans un groupe fini d'ordre d, tout élément x vérifie $x^d = 1$. On va interpréter la question demandée comme étant le reflet d'une relation dans un groupe d'ordre $\varphi(n)$, le groupe G des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Pour être complets, nous allons démontrer que, pour un entier relatif k dont on note $\overline{k}$ la classe modulo n, on a les conditions équivalentes suivantes :

(i) k est premier avec n,
(ii) $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$,
(iii) $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Pour répondre à la question de l'exercice, l'équivalence de (i) et (ii) suffit car elle montre que les éléments du groupe G des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les classes, modulo n, des entiers $1 \leq k \leq n$ premiers avec n. Donc le cardinal de G est égal à $\varphi(n)$. Il s'ensuit que pour tout $\overline{a} \in G$ on a $\overline{a}^{\varphi(n)} = 1$ dans G. Cela signifie exactement que pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1\ (n)$.

Montrons maintenant que (i) et (ii) sont équivalentes. D'après le théorème de Bézout, k et n sont premiers entre eux ssi il existe des entiers relatifs u, v tels que $uk + vn = 1$, ssi il existe un entier relatif u tel que $\overline{u}\overline{k} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$, ssi $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Pour finir on montre que (ii) et (iii) sont équivalentes. Si $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, alors il existe un entier relatif u tel que $\overline{u}\overline{k} = \overline{1}$, donc pour tout $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ on a $\overline{m} = \overline{mu}\overline{k}$. Ceci montre que tout élément de $\mathbb{Z}/n\mathbb{Z}$ est un multiple de $\overline{k}$, donc $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$. Réciproquement, si $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$, alors en particulier $\overline{1}$ est un multiple de $\overline{k}$, donc il existe $\overline{u}$ tel que $\overline{u}\overline{k} = \overline{1}$, ce qui montre que $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Notons que l'équivalence entre (i) et (iii) peut aussi se voir directement, puisque $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ ssi son ordre est égal à n. Or on a montré dans un exercice précédent que l'ordre de k est $n/\operatorname{pgcd}(k, n)$, d'où la conclusion.

(2) Si p est premier, tous les entiers $1 \leq k \leq p-1$ sont premiers avec p et donc $\varphi(p) = p-1$. D'après la question précédente, pour tout $a \in \mathbb{Z}$ premier avec p, on obtient $a^{p-1} \equiv 1\ (p)$. En multipliant par a ceci donne $a^p \equiv a\ (p)$. De plus, si a n'est pas premier avec p, c'est-à-dire si $p|a$, alors a^p et a sont tous les deux nuls modulo p donc la relation $a^p \equiv a\ (p)$ est encore vérifiée. Finalement, pour tout $a \in \mathbb{Z}$ on a $a^p \equiv a\ (p)$.

Exercice 4 (1) Montrer que le groupe additif $\mathbb{Q}$ n'est pas monogène.
(2) En déduire que le groupe additif $\mathbb{R}$ n'est pas monogène.
(3) Montrer que $\mathbb{Q}$ est engendré par l'ensemble $\{\frac{1}{n!}\}_{n\geq 1}$.
(4) Montrer que tout sous-groupe monogène non nul de $\mathbb{Q}$ est infini.
(5) Montrer que tout sous-groupe de type fini, non nul, de $\mathbb{Q}$ est isomorphe à $\mathbb{Z}$.

Corrigé exercice 4
(1) Supposons que $\mathbb{Q}$ soit monogène, engendré par un rationnel $x = m/n$ écrit sous forme de fraction irréductible, c'est-à-dire que m et n sont premiers entre eux. Alors $1/(2n)$ est un multiple de x, i.e. il existe $k \in \mathbb{Z}$ tel que $1/(2n) = km/n$. On en déduit l'égalité $2km = 1$ dans $\mathbb{Z}$, ce qui est impossible car $2km$ est pair. Donc $\mathbb{Q}$ n'est pas monogène.
(2) Supposons que $\mathbb{R}$ soit monogène. Comme il est infini, il est donc isomorphe à $\mathbb{Z}$. Alors le sous-groupe $\mathbb{Q}$ est isomorphe à un sous-groupe de $\mathbb{Z}$, donc un groupe de la forme $n\mathbb{Z}$. Or $n\mathbb{Z}$ est isomorphe à $\mathbb{Z}$, précisément on a un isomorphisme évident $f : \mathbb{Z} \to n\mathbb{Z}$ défini par $f(a) = na$. Finalement $\mathbb{Q}$ est isomorphe à $\mathbb{Z}$, donc monogène, ce qui est une contradiction avec la question précédente.
(3) Soit un rationnel $x = m/n$. Alors $x = m(n-1)!/n!$ ce qui montre que x est un multiple de $1/n!$. Donc tout élément de $\mathbb{Q}$ est multiple d'un des nombres $1/n!$, et a fortiori, les nombres $1/n!$ engendrent $\mathbb{Q}$.
(4) Soit $H \subset \mathbb{Q}$ un sous-groupe monogène non nul. Il est isomorphe soit à $\mathbb{Z}$, soit à $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geq 1$. Dans le deuxième cas, il existe dans H un élément $x \neq 0$ tel que $nx = 0$. Mais comme $\mathbb{Q}$ est un corps, ceci implique $x = 0$, en contradiction avec l'hypothèse sur x. Donc H est infini isomorphe à $\mathbb{Z}$.
(5) On va montrer par récurrence sur $k \geq 1$ qu'un sous-groupe de $\mathbb{Q}$ engendré par k éléments est isomorphe à $\mathbb{Z}$.

Initialisation de la récurrence : le cas $k = 1$ est simplement la question précédente.

Hérédité de la proposition : on suppose que tout sous-groupe engendré par k éléments est isomorphe à $\mathbb{Z}$. Soit H un sous-groupe engendré par $k+1$ éléments notés $x_1, \ldots, x_k, y$. D'après l'hypothèse de récurrence, le sous-groupe engendré par $x_1, \ldots, x_k$ est isomorphe à $\mathbb{Z}$, donc engendré par un élément $x = m/n$ (fraction irréductible). On est ainsi ramené au cas $k = 2$ avec deux générateurs x, y où $y = p/q$ (fraction irréductible). On a donc

$$H = \{ax + by\,, (a,b) \in \mathbb{Z}^2\} = \left\{ \frac{amq + bpn}{nq}\,, (a,b) \in \mathbb{Z}^2 \right\}\ .$$

L'ensemble des nombres $amq + bpn$, avec (a, b) variable, est un sous-groupe de $\mathbb{Z}$ qui est de la forme $d\mathbb{Z}$, avec pour d le pgcd de mq et de pn : c'est une des définitions du pgcd. Il s'ensuit que H est l'ensemble des multiples de $d/(nq)$, il est donc monogène, comme on le souhaitait.

Exercice 5 Montrez que si m et n sont deux entiers premiers entre eux, on a un isomorphisme $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Est-ce vrai lorsque m et n ne sont pas premiers entre eux ?

Corrigé exercice 5 De manière générale, si H, K sont deux sous-groupes distingués de G avec $H \subset K$, on a un morphisme surjectif $G/H \to G/K$. On le justifie ainsi : on part du morphisme $\pi : G \to G/K$. Le sous-groupe H est inclus dans K, qui est le noyau de π, donc par le théorème fondamental sur le quotient G/H (aussi appelé propriété universelle de G/H), le morphisme π induit un morphisme $G/H \to G/K$. Le fait que ce morphisme soit surjectif découle du fait analogue pour $G \to G/K$.

Dans le cas des quotients de $\mathbb{Z}$, comme $mn\mathbb{Z} \subset m\mathbb{Z}$ et $mn\mathbb{Z} \subset n\mathbb{Z}$ on a des morphismes $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, d'où un morphisme $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Si l'on note $\overline{a}$, $\widetilde{a}$, $\widehat{a}$ les classes modulo mn, m et n (respectivement), alors on peut écrire ce morphisme sous la forme :

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{a} & \mapsto & (\widetilde{a}, \widehat{a}) \end{array}$$

Comme $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont le même cardinal égal à mn, pour montrer que ce morphisme est un isomorphisme il suffit de montrer qu'il est injectif, ou surjectif, au choix. Montrons que ce morphisme est injectif, ce qui est assez facile. Si $\overline{a}$ est dans le noyau, alors a est multiple de m et de n. Donc il existe $a' \in \mathbb{Z}$ tel que $a = ma'$. Comme n divise a il divise ma', et comme n est premier avec m, par le lemme de Gauss on obtient que n divise a'. Ainsi mn divise a, donc $\overline{a} = 0$ dans $\mathbb{Z}/mn\mathbb{Z}$. On obtient l'injectivité recherchée.

Si m et n ne sont pas premiers entre eux, le résultat n'est plus vrai, et d'ailleurs on voit ce qui pêche dans l'argument précédent. Il est facile de donner un contre-exemple : on prend $m = n > 1$ et le morphisme est le morphisme $\mathbb{Z}/n^2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ce morphisme n'est certainement pas un isomorphisme, puisque le groupe de gauche possède un élément d'ordre n^2 alors que dans le groupe de droite, tous les éléments sont d'ordre $\leq n$.

Groupes symétriques

Avant de passer à l'exercice 6, on a besoin de quelques éléments de cours sur les actions de groupes et la structure du groupe symétrique.

Quelques notions sur les actions de groupes :

Dans l'étude du groupe symétrique, le vocabulaire des actions de groupes est extrêmement pratique. Faisons quelques rappels.

Soit G un groupe et X un ensemble. Une *action* de G sur X est un morphisme de groupes $\rho : G \to S_X$ du groupe G vers le groupe des bijections de X. C'est la même chose de se donner, pour tout élément $g \in G$, une bijection $\rho_g : X \to X$, de telle façon que

(i) $\rho_1 = \mathrm{id_X}$.

(ii) $\rho_{gg'} = \rho_g \circ \rho_{g'}$ pour tous g, g' dans G.

Par souci de concision, en général on note simplement g au lieu de ρ_g, et gx ou $g.x$ au lieu de $\rho_g(x)$.

Le vocabulaire des actions de groupes permet d'utiliser l'intuition d'un problème géométrique dans lequel G est un groupe de transformations et X est un espace géométrique (en un sens volontairement un peu flou), par exemple un espace affine, ou euclidien, ou un espace topologique. À cause de cela, on appelle souvent les éléments de X des *points*.

L'*orbite d'un point $x \in X$ sous le groupe G*, ou *G-orbite de x*, est la partie de X définie par

$$O_G(x) = \{gx\,, g \in G\}\ .$$

La relation binaire sur X définie par $x \sim y$ ssi il existe $g \in G$ tel que $y = gx$ est une relation d'équivalence. On a évidemment :

$$x \sim y \iff y \in O_G(x) \iff O_G(x) = O_G(y) \ .$$

Les classes d'équivalence pour cette relation sont les orbites de l'action de G sur X, et elles forment la *partition en orbites* de X. Le *stabilisateur du point* $x \in X$ est le sous-groupe de G défini par $G_x = \{g \in G \, , gx = x\}$. La vérification du fait qu'il s'agit d'un sous-groupe est un exercice facile. Ce sous-groupe n'est pas distingué en général ; je vous invite fortement à chercher un contre-exemple pour illustrer cela avant de poursuivre la lecture.

L'action de G sur X est dite *transitive* s'il n'y a qu'une orbite. Ceci signifie que pour tous x, y dans X il existe $g \in G$ tel que $y = gx$, ou encore, que l'application $ev_x : G \to X$ définie par $g \mapsto gx$ est surjective. (Je note cette application ev_x car il s'agit de l'*évaluation en* x.) Par exemple, partant d'une action quelconque de G sur un ensemble X, et d'un point $x \in X$, il y a une action de G sur l'orbite $Y := O_G(x)$ et cette action est transitive par définition.

L'extrême opposé des « grosses » orbites (actions transitives) est le cas d'orbites réduites à un seul élément : $O_G(x) = \{x\}$. Dans ce cas, on parle d'*orbite ponctuelle*, ou d'*orbite réduite à un point*, ou parfois d'*orbite triviale*. On dit aussi que x est un point fixe sous G. Par définition, x est toujours un point fixe sous son stabilisateur G_x, c'est-à-dire $O_{G_x}(x) = \{x\}$.

Pour $x \in X$, nous introduisons maintenant l'application $ev_x : G \to X$ qui envoie $g \in G$ sur $g(x)$. Nous l'appellerons l'*application d'évaluation en* x.

Théorème : L'application d'évaluation en x induit une bijection $G/G_x \to O_G(x)$.

Démontrons ce résultat. Par définition de l'orbite, l'image de ev_x est l'orbite $O_G(x)$ donc ev_x induit une application surjective $G \to O_G(x)$. Pour cette application, deux éléments g, h ont la même image ssi $g^{-1}h \in G_x$. Il s'ensuit, d'après la définition de l'ensemble quotient G/G_x, ensemble des classes à gauche de G modulo G_x, que f induit une application bijective $G/G_x \to O_G(x)$. En particulier, si G est fini (mais *sans supposer que* X *est fini*), alors on voit que les orbites de X sous G sont finies et le cardinal de l'orbite de x est égal à l'ordre de son stabilisateur.

Quelques notions sur le groupe symétrique :

Le groupe symétrique agit naturellement (par sa définition même) sur l'ensemble des n premiers entiers $\{1, \ldots, n\}$. Lorsqu'on l'étudie, cette action est toujours en toile de fond et on utilise naturellement le vocabulaire des actions de groupes. Par exemple, chaque permutation σ a des orbites (les σ-orbites), qui sont les orbites de $\{1, \ldots, n\}$ sous $G = \langle \sigma \rangle$.

Cycles. Les permutations les plus simples (mise à part l'identité) du point de vue de cette action sont celles qui ont une et une seule orbite non ponctuelle. On les appelle les *cycles*. Une autre façon de les définir est de dire qu'un cycle est une permutation dont le support est non vide et est une orbite. Notez que, par cette définition, l'identité n'est pas un cycle. Si l'on note r le cardinal de l'orbite non ponctuelle, on dit aussi que σ est un *r-cycle*. Un petit exercice facile montre que l'ordre d'un r-cycle est r. Les cycles les plus simples sont

les 2-cycles, que l'on appelle aussi *transpositions*. Un fait classique, que nous ne ferons pas en exercice, mais que vous pouvez démontrer très facilement par récurrence sur n, est que le groupe S_n est engendré par les transpositions.

Support. Soit σ une permutation du groupe symétrique S_n. On appelle *support* de σ l'ensemble des points $x \in S_n$ tels que $\sigma(x) \neq x$. C'est donc le complémentaire de l'ensemble des points fixes de σ. On le note $\mathrm{Supp}(\sigma)$.

Si σ et τ sont deux permutations à supports disjoints, elles commutent. Voici la démonstration. Il s'agit de démontrer que pour tout $i \in \{1, \ldots, n\}$ on a $(\sigma\tau)(i) = (\tau\sigma)(i)$. Si i n'est ni dans le support de σ ni dans celui de τ, on a $\sigma(i) = \tau(i) = i$ donc $(\sigma\tau)(i) = (\tau\sigma)(i) = i$ et on a fini. Il reste à traiter le cas où i est dans le support de σ et le cas où i est dans le support de τ. Clairement le raisonnement sera le même dans les deux cas, en changeant σ en τ, donc il suffit de regarder le premier cas : $i \in \mathrm{Supp}(\sigma)$. Nous faisons l'observation que comme l'ensemble des points fixes est stable sous σ, son complémentaire, c'est-à-dire le support de σ, l'est aussi. Ainsi i et $\sigma(i)$ sont dans le support de σ. Comme σ et τ sont à supports disjoints, i et $\tau(i)$ ne sont pas dans le support de τ, en d'autres termes $\tau(i) = i$ et $\tau(\sigma(i)) = \sigma(i)$. Donc $\tau(\sigma(i)) = \sigma(i) = \sigma(\tau(i))$ et on a fini.

Décomposition en cycles à supports disjoints. Le résultat de base pour manipuler les permutations est le théorème suivant :

Théorème : toute permutation s'écrit de manière unique, à l'ordre près des facteurs, comme un produit de cycles à supports disjoints.

Pour démontrer ceci, on raisonne par condition nécessaire, ce qui démontrera l'unicité de la décomposition. On note que si $\sigma = \tau_1 \ldots \tau_s$ est un produit de cycles à supports disjoints notés $\mathcal{O}_1, \ldots, \mathcal{O}_s$, alors sur la partie $\mathcal{O}_i$ on a $\sigma = \tau_i$. Il s'ensuit que $\mathcal{O}_i$ est stable sous σ, et comme c'est une orbite de τ_i, c'est une orbite de σ. Ainsi $\mathcal{O}_1, \ldots, \mathcal{O}_s$ sont toutes les orbites non ponctuelles de σ, et de plus :

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

Ceci montre que τ_i est entièrement déterminé par σ, donc la décomposition recherchée est unique. Pour l'existence, on appelle $\mathcal{O}_1, \ldots, \mathcal{O}_s$ les orbites non ponctuelles de σ et on définit τ_i comme ci-dessus. Il est immédiat de vérifier que $\sigma = \tau_1 \ldots \tau_s$.

Exercice 6 (1) Soit σ un r-cycle dans le groupe symétrique S_n, $n \geq 2$. Pour quelles valeurs de k entier, $1 \leq k \leq r-1$, la permutation σ^k est-elle un cycle ?
(2) On note $\sigma = (i_1 i_2 \ldots i_r)$. Étant donné $\tau \in S_n$, montrez que $\tau\sigma\tau^{-1}$ est le cycle

$$(\tau(i_1)\tau(i_2)\ldots\tau(i_r)) \ .$$

(3) Soit $\sigma_1 = (12\ldots n)$ la *permutation circulaire* et $\tau_1 = (12)$. Pour k entier, calculez σ_1^k puis $\sigma_1^k \tau_1 \sigma_1^{-k}$. En déduire que les permutations σ_1 et τ_1 engendrent S_n.

Corrigé exercice 6
(1) Comme l'ordre d'un r-cycle est r, le groupe $G \subset S_n$ engendré par σ est isomorphe à $\mathbb{Z}/r\mathbb{Z}$. Notons O le support de σ, qui est son unique orbite non ponctuelle, de la forme $O = \{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$. Cette orbite est de cardinal r, de même que G, ce qui montre que l'application $ev_x : G \to O$ est une bijection (le stabilisateur G_x est réduit à $\{1\}$.

Nous devons dire pour quels entiers $1 \leq k \leq r-1$, la permutation σ^k est un cycle. Clairement, ce qui se passe en dehors du support O n'a aucune importance. Pour relier ce qu'il se passe dans $G = \langle\sigma\rangle$ et ce qu'il se passe dans O, nous allons utiliser la bijection $ev_x : G \to O$. La permutation σ^k engendre un sous-groupe H de G, donc un groupe cyclique d'ordre égal à l'ordre de k dans $\mathbb{Z}/r\mathbb{Z}$. Les orbites de H dans O correspondent, via la bijection ev_x, aux classes de H à droite modulo G ; elles sont toutes de même cardinal égal à l'ordre de H. En particulier, il n'y a qu'une orbite non ponctuelle ssi il n'y a qu'une orbite (dans O), ssi $H = G$. Donc σ^k est un cycle ssi c'est un r-cycle, ssi σ^k engendre G, ssi k est premier avec r.

(2) Soit $\sigma = (i_1 i_2 \dots i_r)$ et vérifions que $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_r))$. Notons $\gamma = \tau\sigma\tau^{-1}$ et soit $j \in \{1, \dots, n\}$. Si $j = \tau(i_k)$ pour un k tel que $1 \leq k \leq r$, alors il est clair que $\gamma(j) = \gamma(\tau(i_k)) = \tau\sigma(i_k) = \tau(i_{k+1})$. Si j n'est pas de la forme $\tau(i_k)$, c'est-à-dire si $\tau^{-1}(j)$ n'est pas dans le support de σ, alors $\sigma(\tau^{-1}(j)) = \tau^{-1}(j)$ donc $\gamma(j) = j$.

(3) Pour exprimer σ_1 il est commode d'identifier $\{1, \dots, n\}$ à $\mathbb{Z}/n\mathbb{Z}$, alors il est clair que $\sigma_1(j) = j+1$ modulo n. Donc $\sigma_1^k(j) = j+k$ modulo n. Ainsi, d'après la question précédente,

$$\sigma_1^k \tau_1 \sigma_1^{-k} = (\sigma_1^k(1)\ \sigma_1^k(2)) = (k+1\ \ k+2)\ .$$

Pour conclure que les permutations σ_1 et τ_1 engendrent S_n, il y a plusieurs façons de faire. Voici par exemple une solution par récurrence sur n.

Pour $n = 1$, il n'y a rien à dire.

Supposons maintenant que pour un $n \geq 2$, les permutations $(12\dots n-1)$ et (12) engendrent S_{n-1} ; notons H le sous-groupe de S_n engendré par $(12\dots n)$ et (12) ; nous devons montrer que toute permutation γ est dans H.

Notons $j = \gamma(n)$. La permutation $\varphi = \sigma_1^{n-j}\gamma$ vérifie $\varphi(n) = n$, donc son support est dans $\{1, \dots, n-1\}$. D'après l'hypothèse de récurrence, φ est dans le sous-groupe engendré par $(12\dots n-1)$ et (12). Or

$$(12\dots n-1) = (1n)(12\dots n) = \sigma_1^{n-1}\tau_1\sigma_1^{-(n-1)}(12\dots n) = \sigma_1^{n-1}\tau_1\sigma_1^{-(n-1)}\sigma_1\ \in H\ .$$

Donc $\varphi \in H$, puis $\gamma = \sigma_1^{j-n}\varphi \in H$. Ceci conclut la démonstration par récurrence.

Exercice 7 Calculez la décomposition en cycles à supports disjoints et la signature des permutations suivantes :
(1) La multiplication par 3 dans $\mathbb{Z}/8\mathbb{Z}$;
(2) La multiplication par 2 dans $\mathbb{Z}/11\mathbb{Z}$;
(3) La multiplication par 5 dans $\mathbb{Z}/11\mathbb{Z}$;

On sait donner les décompositions en cycles, mais certains ne savent peut-être pas ce qu'est la signature. Je commence par dire ce qu'est la signature, et je donne le corrigé de

l'exercice. Je vous invite à ne lire *que* les notions sur la signature, et a poser ensuite le corrigé pour faire l'exercice (vous pouvez d'ailleurs d'ores et déjà calculer les décompositions en cycles).

Quelques notions sur la signature :

Soit $n \geq 2$ et S_n le groupe symétrique. Le groupe à 2 éléments, qui est unique à isomorphisme près, peut être représenté par le groupe additif $\mathbb{Z}/2\mathbb{Z}$ mais aussi par le groupe multiplicatif $\{\pm 1\}$.

Théorème : il existe un unique morphisme de groupes surjectif $\epsilon : S_n \to \{\pm 1\}$, que l'on appelle la *signature*.

Nous allons d'abord démontrer l'existence. Pour cela, étant donnée une permutation σ, nous définissons une *inversion* pour σ comme étant un couple d'entiers (i, j) dans $\{1, \ldots, n\}$ tels que $i < j$ et $\sigma(i) > \sigma(j)$. C'est donc un couple dont l'ordre est renversé par σ. On note n_σ le nombre d'inversions pour σ, et on pose $\epsilon(\sigma) = (-1)^{n_\sigma}$. Par exemple, si $\sigma = 1$, il n'y a pas d'inversion, donc $\epsilon(\sigma) = 1$, et si $\sigma = (12)$, la seule inversion est le couple $(1, 2)$ et donc $\epsilon(\sigma) = -1$. Ainsi $\epsilon : S_n \to \{\pm 1\}$ est surjectif.

Pour démontrer qu'on a bien défini un morphisme, on va utiliser l'ensemble $\mathbb{C}[X_1, \ldots, X_n]$ des polynômes en n indéterminées $X_1, \ldots, X_n$ (nous aurons besoin de très peu de choses sur lui) et l'action de S_n sur $\mathbb{C}[X_1, \ldots, X_n]$ par permutation des variables. Cette action est définie ainsi : étant donnés $P = P(X_1, \ldots, X_n)$ et $\sigma \in S_n$, on note σP le polynôme

$$(\sigma P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \ .$$

La variable X_i se trouve donc à la place d'indice $\sigma^{-1}(i)$. Vérifions qu'il s'agit bien d'une action : il est clair que $1P = P$, et il reste à vérifier que $(\tau\sigma)P = \tau(\sigma P)$. Or

$$\begin{aligned}(\tau(\sigma P))(X_1, \ldots, X_n) &= (\sigma P)(X_{\tau(1)}, \ldots, X_{\tau(n)}) \\ &= P(\ldots, X_{\tau(i)}, \ldots) \text{ (la variable } X_{\tau(i)} \text{ est à la place d'indice } \sigma^{-1}(i)) \\ &= P(X_{\tau\sigma(1)}, \ldots, X_{\tau\sigma(n)}) \\ &= ((\tau\sigma)P)(X_1, \ldots, X_n) \ .\end{aligned}$$

Nous pouvons passer à la démonstration proprement dite. Considérons le polynôme de Vandermonde défini par

$$V(X_1, \ldots, X_n) = \prod_{i<j} (X_j - X_i) \ .$$

Par exemple, pour $n = 3$, on a $V(X_1, X_2, X_3) = (X_3 - X_2)(X_3 - X_1)(X_2 - X_1)$. Nous voulons calculer σV, pour cela on va réordonner les facteurs dans l'expression

$$\sigma V(X_1, \ldots, X_n) = \prod_{i<j} (X_{\sigma(j)} - X_{\sigma(i)}) \ .$$

Si l'on prend un couple (i, j) avec $i < j$, il peut se passer deux choses :

- soit (i, j) est une inversion pour σ, auquel cas on pose $i' = \sigma(j)$, $j' = \sigma(i)$ et on a $i' < j'$.

- soit (i,j) n'est pas une inversion, alors on pose $i' = \sigma(i)$, $j' = \sigma(j)$ et on a $i' < j'$.

Avec ces notations, on a donc $X_{\sigma(j)} - X_{\sigma(i)} = (\pm 1)(X_{j'} - X_{i'})$ avec $i' < j'$, où le signe ± 1 vaut -1 lorsque i, j est une inversion et 1 sinon. En conclusion, lorsqu'on multiplie tous ces facteurs il apparaît un produit de signes -1 dont le nombre est égal au nombre d'inversions de σ, c'est-à-dire que :

$$\sigma V(X_1, \ldots, X_n) = \epsilon(\sigma) \prod_{i'<j'} (X_{j'} - X_{i'}) = \epsilon(\sigma) V(X_1, \ldots, X_n) \ .$$

Pour deux permutations σ, τ on a

$$\epsilon(\sigma\tau)V = \sigma\tau V = \sigma(\tau V) = \sigma(\epsilon(\tau)V) \overset{(*)}{=} \epsilon(\tau)\sigma V = \epsilon(\tau)\epsilon(\sigma)V \ .$$

On a utilisé, à l'endroit où il y a une étoile $(*)$, le fait que l'action de S_n sur $\mathbb{C}[X_1, \ldots, X_n]$ est une action par automorphismes de $\mathbb{C}$-espace vectoriel, donc en particulier $\sigma(\lambda P) = \lambda\sigma(P)$. Il résulte de ce calcul que $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$, donc ϵ est bien un morphisme de groupes.

Démontrons que ce morphisme est unique. Soit $\delta : S_n \to \{\pm 1\}$ un morphisme surjectif de groupes. Pour démontrer que δ est unique, il suffit de démontrer que sa valeur est -1 sur toutes les transpositions, car comme S_n est engendré par les transpositions, toute permutation σ est produit de transpositions : $\sigma = \tau_1 \ldots \tau_k$, et alors $\delta(\sigma) = \delta(\tau_1) \ldots \delta(\tau_k) = (-1)^k$.

Comme deux quelconques permutations τ, τ' sont conjuguées : $\tau' = \gamma\tau\gamma^{-1}$, on a $\delta(\tau') = \delta(\gamma\tau\gamma^{-1}) = \delta(\gamma)\delta(\tau)\delta(\gamma)^{-1} = \delta(\tau)$. La valeur de δ est donc la même sur toutes les transpositions. Si cette valeur est 1, alors $\delta(\tau) = 1$ pour toute transposition τ, donc $\delta(\sigma) = 1$ pour toute permutation σ (encore car S_n est engendré par les transpositions). Or on a supposé que δ est surjectif, donc ceci est impossible et finalement la valeur de δ sur les transpositions est -1.

Ceci termine la preuve du théorème sur la signature.

On dit qu'une permutation est *paire* si sa signature est $+1$ et *impaire* si sa signature est -1. Le noyau de la signature, ensemble des permutations paires, est un sous-groupe distingué de S_n appelé le *groupe alterné* et noté A_n.

Pour finir donnons diverses façons de calculer la signature :

1 $\epsilon(\sigma) = (-1)^{n_\sigma}$ où n_σ est le nombre d'inversions de σ. En général, ceci est peu pratique pour calculer $\epsilon(\sigma)$.

2 $\epsilon(\sigma) = (-1)^k$ lorsque σ est produit de k transpositions.

3 $\epsilon(\sigma) = (-1)^{r-1}$ lorsque σ est un r-cycle, car un r-cyle est produit de $r-1$ transpositions : $\sigma = (1 \ldots r) = (2\ 3)(3\ 4) \ldots (r-1\ r)(r\ 1)$ et tous les cycles sont conjugués à celui-ci (exercice 6, question 2).

4 $\epsilon(\sigma) = (-1)^{n-s}$ où s est le nombre d'orbites de σ (le nombre total, incluant les orbites ponctuelles). Je vous suggère de démontrer ceci en exercice, en utilisant la décomposition en cycles à support disjoint de σ.

Corrigé exercice 7

Commençons par les décompositions en cycles. Le calcul donne :

Multiplication par 3 dans $\mathbb{Z}/8\mathbb{Z} = (1\ 3)(2\ 6)(5\ 7)$.

Multiplication par 2 dans $\mathbb{Z}/11\mathbb{Z} = (1\ 2\ 4\ 8\ 5\ 10\ 9\ 7\ 3\ 6)$.

Multiplication par 5 dans $\mathbb{Z}/11\mathbb{Z} = (1\ 5\ 3\ 4\ 9)(2\ 10\ 6\ 8\ 7)$.

Pour calculer les signatures, on utilise la décomposition en cycles et la formule $\epsilon(\sigma) = (-1)^{r-1}$ lorsque σ est un r-cycle. On trouve :

Si σ est la multiplication par 3 dans $\mathbb{Z}/8\mathbb{Z}$, $\epsilon(\sigma) = (-1)^3 = -1$.

Si σ est la multiplication par 2 dans $\mathbb{Z}/11\mathbb{Z}$, $\epsilon(\sigma) = (-1)^{10-1} = -1$.

Si σ est la multiplication par 5 dans $\mathbb{Z}/11\mathbb{Z}$, $\epsilon(\sigma) = (-1)^{5-1}(-1)^{5-1} = 1$.