3M270 : ALGÈBRE

par

Alberto Mínguez

1. Généralités

1.1. Groupes. —

Définition 1.1. — Un *groupe* est un couple $(G, *)$, où G est une ensemble non vide et $* : G \times G \to G$ est une loi de composition interne, satisfaisant aux propriétés suivantes :

(1) Il existe un élément neutre $e_G \in G$, c'est-à-dire, tel que $e_G * g = g * e_G = g$ pour tout $g \in G$.

(2) Pour tout $g \in G$ il existe un élément appartenant à G, noté g^{-1} et appelé élément symétrique ou inverse de g, tel que $g * g^{-1} = g^{-1} * g = e_G$.

(3) La loi de composition est associative, c'est-à-dire, $g * (h * i) = (g * h) * i$ pour tous $g, h, i \in G$.

On dit que $(G, *)$ est un groupe *commutatif* ou *abélien* si $g * h = h * g$ pour tous $g, h \in G$.

La définition de groupe est assez "simple", pourtant leur classification est assez compliquée... Pensez aux espaces vectoriels. Il y a beaucoup d'axiomes dans leur définition et leur classification ne dépend que de la dimension de l'espace : il y a une classe d'isomorphisme d'espace vectoriels à dimension fixée.

Exemple 1.2. — (1) $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q}^\times, \times)$ sont des groupes abéliens (vérifiez-le !)

(2) $(\mathbf{N}, +)$ et $(\mathbf{Z}, \times)$ ne sont pas de groupes (pourquoi ?)

(3) $M_2(\mathbf{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \right\}$ est un groupe abélien pour l'addition des matrices.

(4) On note $\mathrm{GL}(n, \mathbf{R})$ l'ensemble des matrices inversibles $n \times n$ à coefficients dans $\mathbf{R}$. Le couple $(\mathrm{GL}_n(\mathbf{R}), \times)$ est un groupe non abélien.

(5) $O_2(\mathbb{R}) = \{M \in M_2(\mathbf{R}) : {}^tMM = id\}$ est un groupe pour la multiplication des matrices.

(6) Soit X un ensemble. Notons $Sym(X)$ l'ensemble des bijections de X sur lui-même. Alors $Sym(X)$ est un groupe pour la composition. Il n'est pas abélien si $card(X) \geq 3$.

(7) Le groupe de quaternions de Hamilton $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$, avec la loi de composition caractérisée par $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$ et $ki = j$.

(8) L'ensemble des isométries du plan affine est un groupe (non abélien) pour la composition.

(9) L'ensemble des homographies du plan complexe est un groupe pour la composition.

(10) Soit $n \geq 1$ un entier naturel. $U_n(\mathbf{C}) = \{z \in \mathbf{C}/z^n = 1\}$ est un groupe abélien pour la multiplication.

Remarque 1.3. — On peut adopter différentes notations $(ab, a.b, a * b, \dots)$ pour décrire la loi de composition interne. Lorsque le groupe est commutatif, on note parfois $a + b$; dans ce cas l'élément neutre est 0, on écrit $-a$ pour a^{-1} et on dit opposé au lieu d'inverse. Dans ce poly si cela ne mène pas à confusion, on utilisera souvent la notation ab.

Des fois on dira aussi "soit G un groupe" et on sous-entendra que l'ensemble G est muni d'une loi de composition interne $*$ telle que le couple $(G, *)$ soit un groupe.

Proposition 1.4. — *L'élément neutre est unique. Pour tout $g \in G$, g^{-1} est unique.*

Démonstration. — Supposons qu'il existe deux éléments neutres e_G et e'_G. On considère le produit :

$$e_G * e'_G.$$

D'un côté, puisque e_G est un élément neutre, on a $e_G * e'_G = e'_G$. De l'autre, puisque e'_G est aussi un élément neutre, on a $e_G * e'_G = e_G$. On déduit que $e_G = e'_G$.

Pour montrer l'unicité de l'inverse g^{-1} de g, on suppose qu'il existe une autre inverse de g, notée h. On considère le produit :

$$(h * g) * g^{-1}.$$

D'un côté, puisque h est l'inverse de g, on a $(h * g) * g^{-1} = e_G * g^{-1} = g^{-1}$. Mais, par associativité de la loi de composition :

$$(h * g) * g^{-1} = h * (g * g^{-1}).$$

Puisque g^{-1} est l'inverse de g, on a aussi que $h * (g * g^{-1}) = h * e_G = h$. On déduit que $h = g^{-1}$. □

Définition 1.5. — Soient $(G, *)$ un groupe et $x \in G$. Soit $k \in \mathbf{Z}$. On définit l'élément $x^k \in G$ par récurrence. Si $k = 0$, alors $x^k = e_G$. Si $k \geq 1$, alors $x^k = x^{k-1} * x$. Et si $k < 0$, on pose $x^k = (x^{-1})^{-k}$.

On appelle l'*ordre* de x le plus petit $k > 0$ tel que x^k vaut e_G, si un tel entier existe. Sinon, on dit que l'ordre de x est infini et on note $\text{ord}(x) = \infty$.

Exemple 1.6. — Si G est le groupe $\mathbb{H}$ des quaternions, $\text{ord}(1) = 1$, $\text{ord}(-1) = 2$, $\text{ord}(j) = 4$. Si $G = \mathbf{Z}$ avec la somme comme loi de composition $\text{ord}(1) = \infty$.

La proposition suivante est claire et la preuve est laissée au lecteur :

Proposition 1.7. — *Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Alors le produit cartésien $G_1 \times G_2$ est un groupe muni de la loi :*

$$(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2).$$

L'élément neutre de $G_1 \times G_2$ est le couple (e_{G_1}, e_{G_2}) et l'inverse de (g_1, g_2) est (g_1^{-1}, g_2^{-1}).

1.2. Sous-groupes. —

Définition 1.8. — Soit H une partie d'un groupe G. On dit que H est un sous-groupe s'il est stable par la loi de composition et si H muni de cette loi de composition interne est un groupe.

Autrement dit, H est un sous-groupe de G si les trois conditions suivantes sont satisfaites.

(1) $e_G \in$ H.
(2) Si $h, h' \in$ H, alors $hh' \in$ H.
(3) Si $h \in H$, alors $h^{-1} \in H$.

Remarque 1.9. — (1) Un sous-groupe d'un groupe est un groupe.
(2) Tout sous-groupe d'un groupe abélien est abélien.
(3) $\mathbf{R}^*$ n'est pas un sous-groupe de $\mathbf{R}$ (pourquoi ?)

Exemple 1.10. — (1) $(\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{R}, +)$
(2) Soit $n \in \mathbf{N}$. Le sous-ensemble $\{nk : k \in \mathbf{Z}\}$ est un sous groupe de $(\mathbf{Z}, +)$. Tout sous-groupe de $\mathbf{Z}$ est de cette forme là.

L'exercice suivant (à faire) donne une autre caractérisation des sous-groupes.

Exercice 1.2.1. — *Soit G un groupe et H une partie de G. Montrer que H est un sous-groupe de G si, et seulement si, $e_G \in H$ et, pour tous $h_1, h_2 \in H$, on a $h_2^{-1} h_1 \in H$.*

Proposition 1.11. — *Soit G un groupe et $\{H_i : H_i \subset G, i \in I\}$ une famille (indexé par I éventuellement infini) de sous-groupes de G. Alors :*

$$\bigcap_{i \in I} H_i$$

est un sous-groupe de G.

Démonstration. — On va utiliser ici la caractérisation de sous-groupe de l'exercice 1.2.1.
Comme $e_G \in H_i$ pour tout $i \in I$, on a $e_G \in \bigcap_{i \in I} H_i$. De plus si $h, g \in \bigcap_{i \in I} H_i$, alors $h, g \in H_i$ pour tout $i \in I$. Comme les H_i sont des sous-groupes de G, on a $hg^{-1} \in H_i$ pour tout $i \in I$ et donc $hg^{-1} \in \bigcap_{i \in I} H_i$. On déduit que $\bigcap_{i \in I} H_i$ est un sous-groupe de G. □

Exemple 1.12. — On considère le groupe $(\mathbf{Z}, +)$. Alors $2\mathbf{Z} \cap 3\mathbf{Z} = 6\mathbf{Z}$. Soient $n, m \in \mathbf{N}$, quel sous-groupe de $\mathbf{Z}$ est $n\mathbf{Z} \cap m\mathbf{Z}$?

Exercice 1.2.2. — *Que peut-on dire de la réunion de deux sous-groupes de G?*

1.3. Générateurs d'un groupe. —

Définition 1.13. — Soient G un groupe et $E \subset G$ une partie de G. Il existe un plus petit sous-groupe H de G contenant E. On dit que E *engendre* H, ou que les éléments de E sont des *générateurs* de H. On note :

$$H = \langle E \rangle .$$

L'existence de H peut se voir de deux façons :

(1) "Par l'extérieur" : on considère tous les sous-groupes de G contenant E (il y a au moins G) et leur intersection convient.

(2) "Par l'intérieur" : on suppose E non vide (sinon $H = \{e_G\}$). On pose $E^{-1} = \{g \in G : g^{-1} \in E\}$, puis :

$$EE^{-1} = \{e_1 \dots e_n : n \in \mathbf{N}, e_i \in E \cup E^{-1}\}.$$

Alors EE^{-1} est un sous-groupe de G, contient E et évidemment est le plus petit possible.

Exemple 1.14. — On considère le groupe $(\mathbf{Z}, +)$.

(1) Soit $E = \{1\} \subset \mathbf{Z}$. Alors $\langle 1 \rangle = \mathbf{Z}$.
(2) $\langle 2, 3 \rangle = \mathbf{Z}$.
(3) $\langle 4, 6 \rangle = 2\mathbf{Z}$.
(4) $\langle n, m \rangle = \text{pgcd}(n, m)\mathbf{Z}$.

Remarque 1.15. — Soit G un groupe et $x \in G$. Le sous-groupe engendré par x est le sous-groupe de G :

$$\langle x \rangle = \{x^k : k \in \mathbf{Z}\}.$$

Définition 1.16. — Soit G un groupe. On dit que G est *cyclique* s'il existe $x \in G$ tel que $\langle x \rangle = G$. On dit alors que x est un *générateur* de G.

Exemple 1.17. — $\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}$ sont cycliques. Soit $X = \{1, 2, 3\}$, alors $G = Sym(X)$ n'est pas cyclique.

Exercice 1.3.1. — *Pouvez-vous classifier les groupes cycliques ?*

Exercice 1.3.2. — *Montrer que le cardinal du sous-groupe engendré par $g \in G$ est égal à l'ordre de g.*

1.4. Homomorphisme de groupes. —

Définition 1.18. — Soient $(G, *_G), (G', *_{G'})$ deux groupes. Une application $f : G \to G'$ est un *homomorphisme* de groupes si :

$$f(a *_G b) = f(a) *_{G'} f(b)$$

pour tous $a, b \in G$.

Remarque 1.19. — Des fois on dit "*morphisme*" à la place de "homomorphisme".

Exemple 1.20. — (1) $(\mathbf{R}, +) \to (\mathbf{R}_+^*, \times)$, $x \mapsto e^x$.

(2) $(\mathrm{GL}_n(\mathbf{R}), \times) \to (\mathbf{R}^\times, \times)$, $x \mapsto \det(x)$.

Proposition 1.21. — *Soient $(G, *_G), (G', *_{G'})$ deux groupes. Soit $f : G \to G'$ un morphisme de groupes. Alors,*

(1) $f(e_G) = e_{G'}$.
(2) *Pour tout $g \in G$, $f(g^{-1}) = f(g)^{-1}$.*

Démonstration. — (1) On a que $f(e_G) *_{G'} f(e_G) = f(e_G *_G e_G) = f(e_G)$. On multiplie cette égalité par $f(e_G)^{-1}$ et on trouve que $f(e_G) = e_{G'}$.

(2) Soit $g \in G$. Alors $f(g) *_{G'} f(g^{-1}) = f(g *_G g^{-1}) = f(e_G) = e_{G'}$ par (1). De la même façon on montre que $f(g^{-1}) *_{G'} f(g) = e_{G'}$. On déduit que $f(g^{-1})$ est l'inverse de $f(g)$ c'est-à-dire, $f(g^{-1}) = f(g)^{-1}$.

□

Définition 1.22. — (1) Soient G, G' deux groupes. Un *isomorphisme* f de G vers G' est un morphisme de groupes $f : G \to G'$ tel qu'il existe $g : G' \to G$ un homomorphisme avec $f \circ g = Id_{G'}$ et $g \circ f = Id_G$. On dit alors que G et G' sont isomorphes.

(2) Un homomorphisme $f : G \to G$ est dit un *endomorphisme* du groupe G. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G.

(3) Un endomorphisme $f : G \to G$ est dit un *automorphisme* s'il est aussi un isomorphisme. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Exemple 1.23. — Soit $(G, *_G)$ un groupe et soit $g \in G$. L'application

$$\begin{array}{rcl} i_g : G & \to & G \\ h & \mapsto & g *_G h *_G g^{-1} \end{array}$$

est un automorphisme (appelé intérieur). L'ensemble des automorphisme intérieurs sera noté $\mathrm{Int}(G)$.

Exercice 1.4.1. — *Montrer que i_g est un automorphisme. Montrer que* $\mathrm{Aut}(G)$ *avec la loi de composition est un groupe et que* $\mathrm{Int}(G)$ *en est un sous-groupe. Montrer que l'application*

$$\begin{array}{rcl} G & \to & \mathrm{Int}(G) \\ g & \mapsto & i_g \end{array}$$

est un homomorphisme de groupes.

Proposition 1.24. — *Soient $(G, *_G), (G', *_{G'})$ deux groupes. Soit $f : G \to G'$ un homomorphisme de groupes. Alors f est un isomorphisme si et seulement si f est bijectif.*

Démonstration. — Il est clair que, si f est un isomorphisme, alors f est bijectif. Supposons que f est bijectif; alors il existe une fonction inverse f^{-1}. Il faut montrer qu'elle est un homomorphisme. Or :

$$f^{-1}(f(a) *_{G'} f(b)) = f^{-1}(f(a *_G b)) = a *_G b = f^{-1}(f(a)) *_G f^{-1}(f(b)).$$

□

Remarque 1.25. — Soit $(G, *)$ un groupe. Soit $g \in G$. L'application :

$$\begin{aligned} T_g : G &\to G \\ h &\mapsto g * h \end{aligned} \tag{1.1}$$

est une bijection mais ce n'est pas un homomorphisme (quelle est son inverse ?)

Notation 1.4.2. — *Nous allons avoir un problème de notation auquel je vous demande de réfléchir un instant. Si $f : E \to E'$ est une application d'ensemble et si $P' \subset E'$, je noterais $f^{-1}(P')$ l'ensemble des éléments $x \in E$ vérifiant $f(x) \in P'$. J'appellerais souvent $f^{-1}(P')$ l'image inverse de la partie P'. Lorsque la partie P' est réduite à un seul élément, $P' = \{z\}$, j'écrirai $f^{-1}(z)$ au lieu de $f^{-1}(\{z\})$ et je parlerai alors de la "fibre" de z par f . Tout cela n'est pas très plaisant puisque nous utilisons le symbole f^{-1} alors qu'il n'y a peut être pas d'application inverse, mais vous verrez que c'est finalement assez pratique (et très pratiqué...).*

Définition 1.26. — Soient $(G, *_G), (G', *_{G'})$ deux groupes. Soit $f : G \to G'$ un morphisme de groupes.

(1) On appelle le *noyau* de f, que l'on note $\ker(f)$, l'ensemble :
$$f^{-1}(e_{G'}) = \{g \in G : f(g) = e_{G'}\}.$$
(2) On appelle l'*image* de f, que l'on note $\mathrm{im}(f)$, l'ensemble $f(G)$.

Proposition 1.27. — *Soient G et G' deux groupes. Soit $f : G \to G'$ un morphisme de groupes. Alors,*

(1) *Le noyau* $\ker f$ *est un sous-groupe de G et l'image* $\mathrm{im}\, f$ *est un sous-groupe de G'.*
(2) *Plus généralement si H est un sous-groupe de G et H' est un sous-groupe de G', $f(H)$ est un sous-groupe de G' et $f^{-1}(H')$ est un sous-groupe de G.*
(3) $\ker f = \{e_G\}$ *si, et seulement si, f est un morphisme injectif.*

Démonstration. — La preuve de (1) et (2) est simple et je vous la laisse comme exercice. On montre (3).

Supposons que $\ker f = \{e_G\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. Alors $f(x) *_{G'} f(y)^{-1} = e_{G'}$ et donc, puisque f est un homomorphisme, $f(x) *_{G'} f(y^{-1}) = e_{G'}$, ou encore, $f(x *_G y^{-1}) = e_{G'}$. On déduit de notre hypothèse que $x *_G y^{-1} = e_G$ c'est-à-dire, $x = y$. Ainsi, f est un morphisme injectif.

On suppose maintenant que f est un morphisme injectif. Soit $x \in \ker f$. Alors, par définition, $f(x) = e_{G'} = f(e_G)$. Puisque f est injectif, on déduit que $x = e_G$. □

On utilisera très souvent la propriété (3) ci-dessus.

Il est aussi clair que :

Proposition 1.28. — *Soient G et G' et G'' trois groupes. Soient $f : G \to G'$ $g : G' \to G''$ deux morphismes de groupes. Alors $g \circ f$ est un homomorphisme de groupes et*

(1) $\ker(g \circ f) = f^{-1}(\ker(g))$.
(2) $\mathrm{im}(g \circ f) = g(\mathrm{im}(f))$.

Définition 1.29. — Soit $(G, *_G)$ un groupe. Le noyau de l'application

$$\begin{array}{ccc} G & \to & \mathrm{Int}(G) \\ g & \mapsto & i_g \end{array}$$

est appelé le centre de G et noté $Z(G)$. Il est l'ensemble des $g \in G$ tels que $g * h = h * g$ pour tout $h \in G$.

1.5. Sous-groupes distingués. —

Définition 1.30. — Soient $(G, *_G)$ un groupe et H, H' deux sous-groupes de G. On dit que H et H' sont conjugués s'il existe $g \in G$ tel que :

$$H' = gHg^{-1}.$$

Remarque 1.31. — Dans ce cas, l'application $h \mapsto ghg^{-1}$ est une bijection entre H et H'. (Quelle est son inverse ?)

Exercice 1.5.1. — *La conjugaison est une relation d'équivalence.*

Définition 1.32. — Soient $(G, *_G)$ un groupe et K un sous-groupe de G. On dit que K est *distingué* dans G s'il est invariant par automorphisme intérieur, c'est-à-dire, si pour tout $g \in G$, $gKg^{-1} = K$. Autrement dit K est distingué dans G si pour tout $g \in G$ et tout $k \in K$, $gkg^{-1} \in K$. Ou encore si pour tout $g \in G$, $gK = Kg$.

Notation 1.5.2. — *Si H est un sous-groupe de G on notera $H < G$. Si de plus H est distingué dans G, on notera alors $H \lhd G$.*

Exemple 1.33. — (1) $\{e_G\}$ et G sont toujours distingués dans G. On dit que G est *simple* si ses seuls sous-groupes distingués sont $\{e_G\}$ et G. Par exemple : $\mathbf{Z}/p\mathbf{Z}$. (Quels sont tous les groupes simples ?)

(2) Si G est commutatif tout sous-groupe de G est distingué. (Et la réciproque ?)

(3) Soient G et G' deux groupes. Soit $f : G \to G'$ un morphisme de groupes. Le noyau $\ker f$ est un sous-groupe distingué dans G (et l'image ?)

(4) Soient G et G' deux groupes. Soit $f : G \to G'$ un morphisme de groupes et soient $H \lhd G$ et $H' \lhd G'$. Alors $f^{-1}(H') \lhd G$ et $f(H) \lhd f(G)$. Attention, en général, $f(H)$ n'est pas distingué dans G' (contre-exemple ?).

(5) Le centre $Z(G)$ est distingué dans G. Il est même un sous groupe caractéristique (c'est-à-dire, invariant par tout automorphisme).

(6) Le sous-groupe dérivé $D(G) = \langle g * h * g^{-1} * h^{-1} : g, h \in G \rangle$, engendré par les commutateurs, est distingué dans G. Il est aussi un sous groupe caractéristique

Exercice 1.5.3. — *Soit G un groupe contenant deux sous-groupes H et K tels que $H \lhd K$, $K \lhd G$. Est-ce que H est distingué dans G ?*

Remarque 1.34. — Soit $(G, *)$ un groupe.

(1) Soit H un sous-groupe de G. Le *normalisateur* de H dans G est :

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

C'est un sous-groupe de G (vérifiez-le !) et H en est un sous-groupe. En fait, H est un sous-groupe distingué de $N_G(H)$ qui est le plus grand sous-groupe de G contenant H et dans lequel H est distingué. Ainsi H est distingué dans G si, et seulement si, $G = N_G(H)$.

(2) Soit H un sous-groupe de G. On dit que H est un sous-groupe caractéristique s'il est stable par tout automorphisme de G. En particulier, il est distingué (puisque $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$). Par exemple $Z(G)$ est caractéristique : en effet, si $\phi \in \mathrm{Aut}(G)$, $g \in Z(G)$ et $h = \phi(h') \in G$ on a :

$$\phi(g)h = \phi(g)\phi(h') = \phi(gh') = \phi(h'g) = \phi(h')\phi(g) = h(\phi(g))$$

et donc $\phi(g) \in Z(G)$.

(Montrez que le sous-groupe dérivé est distingué. Pour ceci, vous pouvez utiliser la propriété suivante.)

(3) Supposons que $G = \langle E \rangle$ avec $E \subset G$ une partie non-vide de G. Soient G' un groupe et $\phi, \phi' : G \to G'$ deux homomorphismes de groupes. Si $\phi(e) = \phi'(e)$ pour tout $e \in E$, alors $\phi = \phi'$. Pour démontrer ceci on utilise que $G = EE^{-1}$.

(4) En particulier $\phi = \mathbf{Z} \to G$ est caractérisé par l'image de 1 ! (Combien y-a-t'il donc d'endomorphismes de $\mathbf{Z}$? et d'automorphismes ?)

1.6. Le groupe quotient. — Soient $(G, *)$ un groupe et H un sous-groupe de G. Soit $x \in G$. On pose :

$$\begin{aligned} xH &= \{xh : h \in H\} \\ Hx &= \{hx : h \in H\}. \end{aligned}$$

Proposition 1.35. — *Soit $\mathscr{R}$ la relation binaire sur G définie par :*

$$x\mathscr{R}y \Leftrightarrow xH = yH \Leftrightarrow y^{-1}x \in H$$

pour tous $x, y \in G$. Alors R *est une relation d'équivalence.*

Démonstration. — Il est clair que $\mathscr{R}$ est réflexive, symétrique et transitive (à vérifier !) □

Définition 1.36. — (1) On appelle ensemble des classes à droite de G pour H l'ensemble des classes pour la relation d'équivalence précédente. On le note G/H.

(2) On appelle ensemble des classes à gauche de G pour H l'ensemble des classes pour la relation d'équivalence définie par :

$$x\mathscr{R}y \Leftrightarrow Hx = Hy \Leftrightarrow yx^{-1} \in H$$

pour tous $x, y \in G$. On le note $H\backslash G$.

Théorème 1.37. — *Si G est un groupe fini et $H < G$, les ensembles G/H et $H\backslash G$ ont le même cardinal. Ce nombre noté $[G : H]$ est l'indice de H dans G. On a :*

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

Démonstration. — Je vous rappelle que la translation $h \mapsto xh$ est une bijection de G sur lui-même (voir (1.1)). Elle induit une bijection entre H et xH. De même la translation $h \mapsto hx$ est une bijection entre H et Hx. On déduit que toute classe (à gauche ou à droite) a le même cardinal que H. Comme G est la réunion disjointe des classes, le nombre de classes (à gauche ou à droite) est bien le cardinal $\frac{|G|}{|H|}$. □

Corollaire 1.38. — *En particulier, si G est un groupe fini et $H < G$ alors $|H|$ divise $|G|$.*

Cela fait l'un de liens entre la théorie de groupes et l'arithmétique. Par exemple, si $|G| = p$ premier, le seuls sous-groupes de G sont $\{e_G\}$ et G lui-même (pourquoi ?).

On voudrait maintenant répondre à la question suivante : est-ce qu'on peut munir G/H d'une loi "naturelle" telle que G/H devienne un groupe ? Par loi naturelle, on entend la loi suivante :

$$gH * g'H = (g * g')H. \tag{1.2}$$

Pour que cette loi soit bien définie il faut qu'elle ne dépende pas des représentants choisis de chacune de classes, c'est-à-dire, si $g_1, g_2, g_1', g_2' \in G$ sont tels que $g_1H = g_1'H$ et $g_2H = g_2'H$, il faut que $(g_1 * g_2)H = (g_1' * g_2')H$. Cette condition est satisfaite si, et seulement si, H est distingué dans G :

Théorème 1.39. — *Supposons H distingué dans G. Alors la loi définie par* (1.2) *fait de G/H un groupe tel que l'application classe $\boldsymbol{cl} : G \to G/H$ soit un homomorphisme de groupes dont le noyau est H.*

Démonstration. — Voyons d'abord que la loi est bien définie. Soient $g_1, g_2, g_1', g_2' \in G$ tels que $g_1H = g_1'H$ et $g_2H = g_2'H$. Alors

$$(g_1 * g_2)H = g_1 * (g_2H) = g_1 * (g_2'H) = g_1 * (Hg_2') = g_1'Hg_2' = (g_1' * g_2')H.$$

Il est clair que, avec cette loi, G/H est un groupe (quel est l'élément neutre ? et l'inverse de gH ? et pourquoi la loi est-elle associative ?). Par définition de la loi, l'application classe $\boldsymbol{cl} : G \to G/H$ est un homomorphisme de groupes. Le noyau de $\boldsymbol{cl}$ est le sous-groupe de G formé des éléments qui s'envoient vers e_GH, c'est-à-dire, H. □

Exemple 1.40. — On trouve ainsi le groupe que vous connaissiez déjà : $\mathbf{Z}/n\mathbf{Z}$.

Définition 1.41. — Une *suite exacte courte* est un couple de homomorphismes :

$$1 \to K \xrightarrow{i} G \xrightarrow{p} H \to 1$$

où K, G, H sont des groupes et :

(1) i est injectif.
(2) p est surjectif.
(3) $\mathrm{im}(i) = \ker(p)$.

Par exemple, si K est distingué dans G alors :

$$1 \to K \xrightarrow{i} G \xrightarrow{\boldsymbol{cl}} G/K \to 1$$

est une suite exacte courte.

Remarque 1.42. — L'intérêt des sous-groupes distingués est de permettre le *dévissage* des groupes. Si K est distingué dans G alors on essaie de ramener l'étude de G a celle de K et G/K (si G est fini ces groupes sont de cardinal plus petit). Les groupes simples sont indévissables d'où l'intérêt qu'on leur porte.

1.7. Les théorèmes d'isomorphisme. — On va prouver quelques théorèmes d'isomorphisme, introduits par la mathématicienne Emmy Noether, qui mettent en rapport les concepts de sous-groupe distingué, de groupe quotient et de homomorphisme. Souvent on les appelle premier, deuxième et troisième théorèmes mais ces noms ne sont pas reconnus partout (des fois le deuxième et le troisième sont échangés).

Proposition 1.43 **(Théorème de factorisation)**. — *Soient G, G' deux groupes et H un sous-groupe distingué de G. Soit $f : G \to G'$ un morphisme de groupes tel que $f(H) = e_{G'}$. Il existe alors un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \boldsymbol{cl}} & \nearrow_{\overline{f}} & \\ G/H & & \end{array}$$

c'est-à-dire, $f = i \circ \overline{f} \circ \boldsymbol{cl}$

Démonstration. — Soit $x \in G/H$. Il existe $a \in G$ tel que $x = \boldsymbol{cl}(a)$. Si $b \in G$ est un autre représentant de x, alors $ab^{-1} \in H$ et $f(a) = f(b)$. Si on pose $\overline{f}(x) = f(a)$, on obtient donc une application lui définie de G/H dans G'.

Soit $y = \boldsymbol{cl}(c)$. Alors $\overline{f}(xy) = \overline{f}(\boldsymbol{cl}(a)\boldsymbol{cl}(c)) = \overline{f}(\boldsymbol{cl}(ac)) = f(ac) = f(a)f(c) = \overline{f}(x)\overline{f}(y)$. G"application $\overline{f}$ est donc un homomorphisme.

Supposons qu'il existe $\psi \in Hom(G/H, G')$ tel que $\psi \circ \boldsymbol{cl} = \overline{f} \circ \boldsymbol{cl}$. Alors, pour tout $x = \boldsymbol{cl}(a)$, $\overline{f}(x) = \psi \circ \boldsymbol{cl}(a) = \psi(x)$. D'où l'unicité. □

Le premier théorème d'isomorphisme est un cas particulier de la proposition précédente :

Théorème 1.44 **(Premier théorème d'isomorphisme)**. — *Soit $f : G \to G'$ un morphisme de groupes. Il existe un unique morphisme de groupes $\overline{f} : G/\ker(f) \to \mathrm{im}(f)$ tel que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \boldsymbol{cl}} & & \uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow{\overline{f}} & \mathrm{im}(f) \end{array}$$

c'est-à-dire, $f = i \circ \overline{f} \circ \boldsymbol{cl}$

Démonstration. — On sait déjà que $\ker(f)$ est distingué dans G et donc $G/\ker(f)$ est un groupe ainsi que $\mathrm{im}(f)$. D'après la proposition 1.43, $\overline{f}$ est unique. Il est surjectif par construction. Il nous reste à vérifier qu'il est injectif. Supposons que $\overline{f}(x) = \overline{f}(y)$. Si $x = \boldsymbol{cl}(a)$ et $y = \boldsymbol{cl}(b)$ alors $ab^{-1} \in Ker(f)$ d'où $\boldsymbol{cl}(a) = \boldsymbol{cl}(b)$, c'est-à-dire $x = y$. □

Exercice 1.7.1. — *Prouver le théorème à l'aide du théorème 1.67.*

Remarque 1.45. — Il devient important de trouver des morphismes de groupes. A chaque morphisme on pourra lui associer un noyau, un groupe quotient et un isomorphisme de ce groupe vers son image ! On trouvera alors beaucoup d'information sur le groupe !

On peut maintenant répondre à l'exo 1.3.1.

Corollaire 1.46. — *Un groupe cyclique est isomorphe à* $\mathbf{Z}$ *s'il est infini ou à* $\mathbf{Z}/n\mathbf{Z}$ *s'il est fini de cardinal* n*.*

Démonstration. — Soit :

$$\begin{array}{rcl} f : \mathbf{Z} & \to & \langle g \rangle \\ k & \mapsto & g^k. \end{array}$$

Il est clair que c'est un morphisme de groupes surjectif. Si de plus f est injectif, alors $\mathbf{Z}$ est isomorphe à $\langle g \rangle$. Sinon, le noyau est un sous-groupe de $\mathbf{Z}$ et donc de la forme $n\mathbf{Z}$ pour un certain $n \in \mathbf{N}$. On trouve, d'après le théorème 1.44 que $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à $\langle g \rangle$. □

Soit K un sous-groupe distingué de G et H un sous-groupe de G. Alors :

(1) $HK := \{hk : k \in K, h \in H\}$ est le plus petit sous-groupe de G contenant K et H. (En général, si K n'est pas distingué, HK n'est un sous-groupe, contre-exemple ?). On pourrait le prouver à la main en utilisant 1.13(2) mais il est plus simple d'utiliser le morphisme :

$$\begin{array}{rcl} \boldsymbol{cl} : G & \to & G/K \\ g & \mapsto & \boldsymbol{cl}(g). \end{array}$$

et remarquer que $\boldsymbol{cl}^{-1} \circ \boldsymbol{cl}(H) = \{g \in G : gK \in \{hK : h \in H\}\} = HK$ et donc HK est un sous-groupe de G (pourquoi ?)

(2) $K \cap H$ est un sous-groupe distingué de H. Notons p la composée :

$$H \to HK \to HK/K$$

Alors $\ker(p) = \{h \in H : hK \in K\} = K \cap H$. On déduit que $K \cap H$ est un sous-groupe distingué de H (pourquoi ?)

En applicant le théorème 1.44 au morphisme surjectif p on trouve :

***Théorème 1.47* (Deuxième théorème d'isomorphisme)**
Soit K un sous-groupe distingué de G et H un sous-groupe de G. Alors p induit un isomorphisme de groupes :

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

Je vous rappelle les résultats suivants qu'on avait vu à la proposition 1.27(2) et à l'exemple 1.33(4) : Soit $f : G \to G'$ un morphisme de groupes. Alors :

(1) Si H est un sous-groupe de G et H' est un sous-groupe de G', $f(H)$ est un sous-groupe de G' et $f^{-1}(H')$ est un sous-groupe de G.
(2) Supposons $H \lhd G$ et $H' \lhd G'$. Alors $f^{-1}(H') \lhd G$ et $f(H) \lhd f(G)$. Attention, en général, $f(H)$ n'est pas distingué dans G'.

On va étudier plus en détail la correspondance entre les sous-groupes de G et G' dans le cas où f est un morphisme *surjectif* (ce qui évite le problème de (2) : dans le cas général on se limitera à considérer $G' = \mathrm{im}(f)$).

***Théorème 1.48* (Théorème de correspondance).** — *Soit $f : G \to G'$ un morphisme de groupes surjectif. Notons $K = \ker(f)$.*

(1) *Il existe une bijection :*

$$\begin{array}{rcl} \{\textit{sous-groupes de } G \textit{ contenant } K\} & \simeq & \{\textit{sous-groupes de } G'\} \\ H & \mapsto & f(H) \\ f^{-1}(H') & \leftarrow & H' \end{array}$$

pour tout H sous-groupe de G et tout H' sous-groupe de G'. On note souvent $H/K := f(H)$.

(2) *Il existe une bijection :*

$$\begin{array}{rcl} \{\textit{sous-groupes distingués de } G \textit{ contenant } K\} & \simeq & \{\textit{sous-groupes distingués de } G'\} \\ H & \mapsto & f(H) \\ f^{-1}(H') & \leftarrow & H' \end{array}$$

pour tout H sous-groupe distingué de G et tout H' sous-groupe distingué de G'.

(3) **Troisième théorème d'isomorphisme :** *Soient K, H deux sous-groupes distingués de G tels que $K < H$. On a un isomorphisme :*

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

Démonstration. — Les points (1) et (2) sont clairs (essayez de les prouver quand même !). Prouvons le troisième point. On considère la composée :

$$p : G \to G/K \to (G/K)/(H/K).$$

Etant la composée de deux fonctions surjectives p est un morphisme surjectif. Quel est le noyau de p ?

$$\ker(p) = \{g \in G : gK \in H/K\} = H.$$

Le théorème se déduit alors du théorème 1.44. □

Exemple 1.49. — Soit $n \geq 2$. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont en bijection avec les sous-groupes de $\mathbf{Z}$ contenant $n\mathbf{Z}$. Ils sont donc en bijection avec les entiers positifs d tels que $d|n$. Si $n = kd$, alors $\mathbf{Z}/n\mathbf{Z}$ a un unique sous-groupe d'ordre d, isomorphe à $\mathbf{Z}/d\mathbf{Z}$. Ce le sous-groupe engendré par $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$. On a donc que tout sous-groupe d'un groupe cyclique est cyclique. (Et la réciproque ?)

1.8. Suites de composition. — Développons un peu plus l'idée de la remarque 1.42. Etant donné un groupe G, on voudrait – si possible – trouver un sous-groupe distingué G_1 et étudier G_1 et le quotient G/G_1. Mais, pour comprendre G_1, on voudrait de même trouver une sous-groupe distingué G_2 dans G_1 et étudier G_2 et le quotient G_1/G_2... La définition suivante devient naturelle :

Définition 1.50. — Soit G un groupe. Une *suite de composition* de G est une suite finie croissante de sous-groupes $(G_i)_{0\leq i\leq l}$ de la forme :

$$\{e_G\} \subset G_l \subset G_{l-1} \subset \cdots \subset G_1 \subset G_0 = G.$$

telle que $G_{i+1} \lhd G_i$ pour tout $0 \leq i \leq l-1$.

On dit que les groupes G_i/G_{i+1} sont les facteurs ou les sous-quotients de la suite. Si la suite est strictement croissante, on dit que l est sa longueur.

Exemple 1.51. — (1) $\{e_G\} \subset G$ est une suite de composition de tout groupe G.
(2) $\{\overline{0}\} \subset \{\overline{0}, \overline{3}\} \subset \mathbf{Z}/6\mathbf{Z}$ et $\{\overline{0}\} \subset \mathbf{Z}/6\mathbf{Z}$ sont deux suites de composition de $\mathbf{Z}/6\mathbf{Z}$.

Dans l'exemple précédent, quelle suite de composition nous donne plus d'information sur $\mathbf{Z}/6\mathbf{Z}$? La première sans doute. A nouveau la définition suivante est naturelle :

Définition 1.52. — Soit G un groupe et soient $(G_i)_{0\leq i\leq l}$ et $(H_i)_{0\leq i\leq l'}$ deux suites de composition de G. On dit que $(H_i)_{0\leq i\leq l'}$ est un raffinement de $(G_i)_{0\leq i\leq l}$, ou encore que $(H_i)_{0\leq i\leq l'}$ est plus fine que $(G_i)_{0\leq i\leq l}$, si $(G_i)_{0\leq i\leq l}$ est extraite de $(H_i)_{0\leq i\leq l'}$, c'est-à-dire, s'il existe des indices $0 \leq j_0 < j_1 \ldots j_l \leq l$ tels que $H_{j_i} \simeq G_i$ pour tout $0 \leq i \leq l$.

Exemple 1.53. — $\{\overline{0}\} \subset \{\overline{0}, \overline{3}\} \subset \mathbf{Z}/6\mathbf{Z}$ est une suite de composition de $\mathbf{Z}/6\mathbf{Z}$ plus fine que $\{\overline{0}\} \subset \mathbf{Z}/6\mathbf{Z}$

Quelle est alors la plus fine des suites de composition ?

Définition 1.54. — Soit G un groupe. Une *suite de Jordan-Hölder* de G est une de composition telle que tous les sous-quotients de la suite sont des groupes simples. Ce qui revient à dire, d'après le théorème de correspondance, une suite de composition strictement croissante qui n'admet pas de raffinement autre qu'elle même.

Exemple 1.55. — (1) $\{\overline{0}\} \subset \{\overline{0}, \overline{3}\} \subset \mathbf{Z}/6\mathbf{Z}$ et $\{\overline{0}\} \subset \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbf{Z}/6\mathbf{Z}$ sont des suites de Jordan-Hölder de $\mathbf{Z}/6\mathbf{Z}$.
(2) On verra aussi que $\{Id\} \subset \{Id, (1\,2\,3), (1\,3\,2)\} \subset \mathcal{S}_3$ est une suite de Jordan-Hölder du groupe symétrique $\mathcal{S}_3$.

Remarque 1.56. — Regardons de plus près l'exemple précédent. $\mathbf{Z}/6\mathbf{Z}$ a deux suites de Jordan-Hölder différentes. Pourtant les deux facteurs de deux suites sont isomorphes à $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$. Et d'après le théorème chinois $\mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. On retrouve le groupe $\mathbf{Z}/6\mathbf{Z}$ à partir de ses facteurs dans les suites de Jordan-Hölder !

Mais ne soyons pas trop optimistes... Les facteurs dans la suite de $\mathcal{S}_3$ sont aussi isomorphes à $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$! Et $\mathcal{S}_3$ n'est pas isomorphe à $\mathbf{Z}/6\mathbf{Z}$... Comment faire alors pour les distinguer ?

Définition 1.57. — Soit G un groupe et soient $(G_i)_{0\leq i\leq l}$ et $(H_i)_{0\leq i\leq l'}$ deux suites de composition de G. On dit que $(H_i)_{0\leq i\leq l'}$ et$(G_i)_{0\leq i\leq l}$, sont *équivalentes* si $l = l'$ et il existe $\sigma \in \mathcal{S}_l$ telle que $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$ pour tout $0 \leq i \leq l-1$.

Exemple 1.58. — Les deux suites de composition dans l'exemple 1.55(1) sont équivalentes.

Est-ce que tout groupe possède une suite de Jordan-Hölder unique à équivalence près ?

Définition 1.59. — Soit G un groupe. On dit qu'il est *résoluble* s'il admet une suite de composition telle que tous les sous-quotients sont des groupes abéliens.

Exemple 1.60. — D'après l'exemple 1.55(2), $\mathcal{S}_3$ est résoluble. Tout groupe abélien est résoluble.

Exercice 1.8.1. — *Soit G un groupe. On note $D(G)$ le groupe dérivé de G. Montrer que $D(G)$ est le plus grand sous-groupe K de G tel que G/K soit abélien.*

Par récurrence on définit $D^n(G) = D(D^{n-1}(G))$. Montrer que G est résoluble si, et seulement s'il existe $n \geq 1$ tel que $D^n(G) = \{e_G\}$.

1.9. Annexe : Les relations d'équivalence. —

Définition 1.61. — Soit E un ensemble. Une *relation binaire* $\mathscr{R}$ sur E est une fonction :

$$\mathscr{R} : E \times E \to \{0, 1\}.$$

(1) Si $(x, y) \in E^2$ et $\mathscr{R}(x, y) = 1$ on écrit souvent simplement $x\mathscr{R}y$ et on dit que la relation $x\mathscr{R}y$ est vraie.
(2) Si $(x, y) \in E^2$ et $\mathscr{R}(x, y) = 0$, on dit que la relation $x\mathscr{R}y$ est fausse.

Exemple 1.62. — $E = \{$élèves dans une classe$\}$. Si $x, y \in E$, on définit $x\mathscr{R}y$ si x est assis à côté de y. La relation $\mathscr{R}$ ainsi définie est une relation binaire.

Définition 1.63. — Soient E un ensemble et $\mathscr{R}$ une relation binaire sur E. On dit que $\mathscr{R}$ est une *relation d'équivalence* sur E si, quels que soient x, y, z dans E, les conditions suivantes sont satisfaites :

(1) la relation $x\mathscr{R}x$ est vraie (réflexivité).
(2) la relation $x\mathscr{R}y$ implique $y\mathscr{R}x$ (symétrie).
(3) les relations $x\mathscr{R}y$ et $y\mathscr{R}z$ impliquent $x\mathscr{R}z$ (transitivité).

Exemple 1.64. — (1) Soit $E = \{\text{élèves d'un lycée}\}$. On définit sur E la relation binaire $\mathscr{R}$ par : $x\mathscr{R}y$ si l'élève x est dans la même classe que l'élève y.

(2) Soit $E = \{\text{voitures à Paris}\}$ et $x\mathcal{R}y$ si la voiture x est de la même couleur que y.

(3) Soit $n \geq 2$. Soit $E = \mathrm{Z}$ et $a\mathcal{R}b \Leftrightarrow n|(a-b)$.

(4) Soient E, F deux ensembles et $f : E \to F$ une fonction. Soient $x, y \in E$. On pose $x\mathscr{R}y$ si $f(x) = f(y)$. Elle est appelée la relation d'équivalence associée à f. En fait, cet exemple conduit à toutes les relations d'équivalence sur E comme on peut le constater ci-après.

Définition 1.65. — Soient E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. Soit $x \in E$. La *classe d'équivalence* de x est le sous-ensemble de E :

$$\boldsymbol{cl}(x) = \mathscr{R}(x) = \{y \in E : x\mathscr{R}y\}.$$

Dans le exemple 1.64(1), la classe de x est la classe du lycée de l'élève x. Et dans l'exemple 1.64(2), la classe de la voiture x c'est l'ensemble de voitures à Paris qui ont la même couleur que la voiture x. Quelle est la classe de a dans l'exemple 1.64(3) ?

Exercice 1.9.1. — *Soient E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. Soit $x, y \in E$. Montrer que les propriétés suivantes sont équivalentes :*

(1) $x\mathscr{R}y$
(2) $\mathscr{R}(x) = \mathscr{R}(y)$
(3) $\mathscr{R}(x) \cap \mathscr{R}(y) \neq \emptyset$

Montrer que l'ensemble des classes d'équivalence de E modulo $\mathscr{R}$ forme une partition de E. (Une partition de E est un ensemble de parties non vides de E, deux à deux disjointes, dont la réunion est E).

Définition 1.66. — Soient E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. L'*ensemble quotient* est l'ensemble de classes d'équivalence :

$$E/\mathscr{R} = \{\mathscr{R}(x) : x \in E\}.$$

Dans le exemple 1.64(1), l'ensemble quotient $E/\mathscr{R}$ est l'ensemble des classes du lycée. Et dans l'exemple 1.64(2), l'ensemble quotient $E/\mathscr{R}$ est l'ensemble des couleurs de voitures parisiennes.

On dispose de l'application classe :

$$\begin{array}{rccc} \boldsymbol{cl} : & E & \longrightarrow & E/\mathscr{R} \\ & x & \mapsto & \mathscr{R}(x). \end{array}$$

On l'appelle la surjection canonique. Par définition $\mathscr{R}$ est la relation d'équivalence associée à $\boldsymbol{cl}$.

Théorème 1.67 **(Théorème de factorisation)**. — *Soit $f : E \to E'$ une fonction et $\mathscr{R}$ la relation d'équivalence associée à f. Alors il existe une unique bijection :*

$$g : E/\mathscr{R} \to f(E)$$

telle que $f = i \circ g \circ \boldsymbol{cl}$ où i est l'inclusion évidente $f(E) \subset E'$.

Démonstration. — On définit $g : E/\mathscr{R} \to f(E)$ par $g(\mathscr{R}(x)) = f(x)$. Voyons d'abord qu'elle est bien définie. Soit $y \in \mathscr{R}(x)$, alors par définition de la relation on a $f(x) = f(y)$ et donc $g(\mathscr{R}(x)) = f(x) = f(y) = g(\mathscr{R}(y))$. Par définition elle satisfait $f = i \circ g \circ \boldsymbol{cl}$. Elle est surjective aussi par définition. Elle est de même injective : si $g(\mathscr{R}(x)) = g(\mathscr{R}(y))$, alors $f(x) = f(y)$ et donc $x\mathscr{R}y$. On déduit que $\mathscr{R}(x) = \mathscr{R}(y)$.

Montrons finalement l'unicité. Soit $g' : E/\mathscr{R} \to f(E)$ telle que $f = i \circ g' \circ \boldsymbol{cl}$. Soit $x \in E$ et montrons que $g(\mathscr{R}(x)) = g'(\mathscr{R}(x))$. Alors $i \circ g' \circ \boldsymbol{cl}(x) = i \circ g \circ \boldsymbol{cl}(x) = f(x)$. Puisque i est injective on déduit que $g(\mathscr{R}(x)) = g'(\mathscr{R}(x))$. □

2. Le groupe symétrique $\mathcal{S}_n$

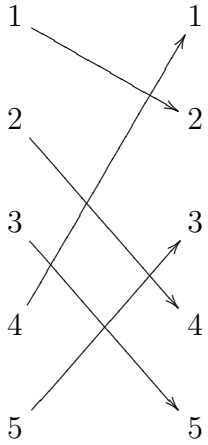
2.1. Définition et notation. —

Définition 2.1. — Si X est un ensemble non vide, une *permutation* de X est une bijection $\sigma : X \to X$. On note $\mathcal{S}_X$ l'ensemble de toutes les permutations de X.

Dans le cas important où $X = \{1, \ldots, n\}$, on écrit $\mathcal{S}_n$ à la place de $\mathcal{S}_X$.

Exercice 2.1.1. — *L'ensemble $\mathcal{S}_X$ muni avec la loi de composition de fonctions est un groupe.*

Exemple 2.2. — Soit $\sigma \in \mathcal{S}_5$ la permutation :



On la notera simplement par lignes sous la forme :

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

c'est-à-dire, si $\sigma \in \mathcal{S}_n$, on notera :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix} \tag{2.1}$$

Exercice 2.1.2. — *Quelle est la composée $\sigma \circ \tau$ avec :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

Et $\tau \circ \sigma$? Déduire que $\mathcal{S}_5$ n'est pas commutatif. Montrer que $\mathcal{S}_n$ n'est pas commutatif si $n \leq 3$. Et dans le cas $n = 2$?

Lagrange utilisa vers 1770 les permutations pour étudier les formules résolvant les équations de troisième et quatrième degré. Il ne put pas développer davantage la théorie car il ne considérait les permutations de $X = \{1, \ldots, n\}$ que comme des réarrangements c'est-à-dire, des suites $i_1, \ldots, i_n$ d'éléments de X sans répétitions ($i_1, \ldots, i_n$ correspondrait

à la seconde ligne de (2.1)). Il ne pouvait donc pas utiliser la composition des permutations ni utiliser les propriétés des groupes (concept défini plus tard et utilisé par Ruffini, Cauchy, Abel, Galois...)

Proposition 2.3. — *La cardinal de $\mathcal{S}_n$ est $n!$.*

Démonstration. — Montrons l'énoncé par récurrence sur n. C'est clair si $n \leq 2$. Pour $n > 2$, considérons dans $\mathcal{S}_n$ la relation d'équivalence $\sigma \mathscr{R} \sigma'$ si $\sigma(n) = \sigma'(n)$. Il est clair que les classes d'équivalence pour cette relation sont les sous-ensembles :

$$H_i = \{\sigma \in \mathcal{S}_n : \sigma(n) = i\}.$$

Rappelons que les classes d'équivalence sont disjointes et que leur réunion est $\mathcal{S}_n$. Il suffit de prouver que chacune des n classes a $(n-1)!$ éléments. Il y a une bijection évidente :

$$\begin{array}{rcl} \mathcal{S}_{n-1} & \to & H_n \\ \sigma & \mapsto & \tau \end{array}$$

où $\tau(i) = \sigma(i)$ pour tout $1 \leq i \leq n-1$ et $\tau(n) = n$.

Soit $i \neq n$. Considérons la permutation (i, n) qui permute i et n et laisse fixe les autres entiers. La translation :

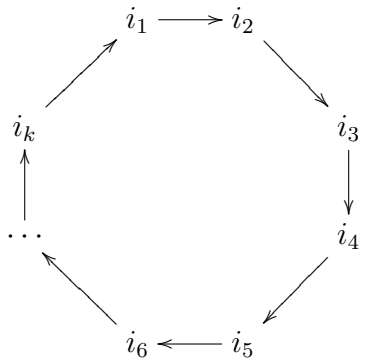
$$\begin{array}{rcl} T_{(i,n)} : \mathcal{S}_n & \to & \mathcal{S}_n \\ \sigma & \mapsto & (i,n)\sigma \end{array}$$

est une bijection d'après (1.1) et $T_{(i,n)}(H_i) = H_n$. On déduit que le cardinal de H_i vaut $(n-1)!$. □

Revenons à la notation. Il est clair que il est un peu trop long d'écrire une permutation sous la forme (2.1) : il faut écrire deux fois les entiers $1, \ldots, n$! De plus, comme on va voir, cette notation cache quelques aspects importants de certaines représentations particulières. En outre il est difficile de voir, par exemple, l'ordre d'un élément, cette notation étant encore très proche des idées de Lagrange. Revenons à l'exemple 2.2. On voit que $\sigma : 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 5, 4 \mapsto 1, 5 \mapsto 3$. On va faire la chose suivante : quand on a trouvé l'image d'un élément, on va voir où va celle-ci. Alors $\sigma : 1 \mapsto 2 \mapsto 4 \mapsto 1$ et $3 \mapsto 5 \mapsto 3$. On notera alors cette permutation $(1\,2\,4)(3\,5)$. Cela nous conduit à donner la définition suivante :

Définition 2.4. — Soient $i_1, \ldots, i_k$, $1 \leq k < n$ des éléments distincts de $\{1, \ldots, n\}$. Le k-cycle $(i_1 \ldots i_k)$ est la permutation $\sigma \in \mathcal{S}_n$ telle que $\sigma(i_l) = i_{l+1}$ pour $1 \leq l \leq k-1$, $\sigma(i_k) = i_1$ et $\sigma(j) = j$ pour $j \notin \{i_1, \ldots, i_k\}$. Si $k \geq 2$, l'ensemble $\{i_1, \ldots, i_k\}$ est le support du cycle. On dit que k est sa longueur.

On peut représenter un cycle sous la forme :



d'où son nom : *kuklos* en grek ancien veut dire *cercle*. On a clairement que $(i_1 \dots i_k) = (i_2 \dots i_k\, i_1) = \cdots = (i_k\, i_1 \dots i_{k-1})$. L'inverse du cycle $(i_1 \dots i_k)$ et le cycle $(i_k \dots i_1)$.

Exercice 2.1.3. — (1) *Montrez qu'on a* $(1\,2)(1\,3\,4\,2\,5) = (1\,3\,4)(2\,5)$.
(2) *Montrez que l'ordre d'un* k*-cycle est* k.

Un 2-cycle est aussi appelé une *transposition*. Un 1-cycle est l'identité.

Définition 2.5. — Le support d'une permutation $\sigma \in \mathcal{S}_n$ est l'ensemble des $1 \leq i \leq n$ tels que $\sigma(i) \neq i$. On le note $\mathrm{supp}(\sigma)$.

Proposition 2.6. — *Deux permutations à supports disjoints commutent.*

Démonstration. — La preuve est facile. Je vous la laisse en exercice. Si vous n'y parvenez pas, essayez avec un exemple d'abord. □

Proposition 2.7. — *Soit* $c = (i_1 \dots i_k)$ *un cycle et soit* $\sigma \in \mathcal{S}_n$. *Alors :*

$$\sigma c \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k)).$$

Démonstration. — Il suffit de montrer que pour tout $1 \leq j \leq k-1$, $\sigma c \sigma^{-1}(\sigma(i_j)) = \sigma(i_{j+1})$, que $\sigma c \sigma^{-1}(\sigma(i_k)) = \sigma(i_1)$ et que pour tout $j \notin \{i_1, \dots, i_k\}$, $\sigma c \sigma^{-1}(\sigma(j)) = \sigma(j)$ ce qui est clair.

□

2.2. Décomposition d'une permutation en cycles. — Ecrivons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$ à l'aide de cycles. Elle vaut $\sigma = (1\,6\,3)(2\,4)(7\,8\,9)$ (on n'a pas besoin d'écrire les 1-cycles). Est-ce que toute permutation peut s'écrire comme produit de cycles ?

Le théorème de ci-dessous, qui répond à cette question, est vraiment important. Vous devez le savoir et le comprendre.

Théorème 2.8. — *Toute permutation est le produit, unique à l'ordre près, de cycles disjoints de longueur supérieure ou égale à* 2.

Démonstration. — On va montrer par récurrence sur le cardinal du support de $\sigma \in \mathcal{S}_n$ la propriété suivante : "Il existe des cycles $c_1, \dots, c_t$ à supports disjoints tels que $\sigma = c_1 \dots c_t$ et le support de σ est égal à l'union disjointe des supports des c_i, $1 \leq i \leq t$."

Tout est clair si le support de σ est de cardinal 0, c'est-à-dire, si σ est l'identité. Supposons $k > 0$ et la propriété montrée pour toute permutation dont le support est de cardinal inférieur à k. Soit $i_1 \in \{1, \dots, n\}$ tel que $\sigma(i_1) \neq i_1$. Posons $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, ..., $i_{r+1} = \sigma(i_r)$, avec r le plus petit entier positif tel que $i_{r+1} \in \{i_1, \dots, i_r\}$ (la suite $\{i_j\}_{j \in \mathbf{N}}$ doit avoir des répétitions puisqu'il n'y a que n valeurs différents possibles). Alors $\sigma(i_r) = i_1$; en effet, si $\sigma(i_r) = i_j$ avec $j \geq 2$ on a $\sigma(i_{j-1}) = i_j = \sigma(i_r)$ ce qui contredit la injectivité de σ.

Soit $c = (i_1 \dots i_r)$ le cycle tel que $c|_{\{i_1,\dots,i_r\}} = \sigma|_{\{i_1,\dots,i_r\}}$. Si $r = n$, alors $\sigma = c$. Supposons $r < n$ et notons $Y = \{1, \dots, n\} \backslash \{i_1 \dots i_r\}$. Alors $\sigma(Y) = Y$ et $c(y) = y$ pour tout $y \in Y$. On définit $\sigma' \in \mathcal{S}_n$ par :

$$\sigma'(t) = \begin{cases} \sigma(t) & \text{si } t \in Y \\ t & \text{si } t \in \{i_1, \dots, i_t\}. \end{cases}$$

Alors σ' et c sont à support disjoints et $\sigma = \sigma' c$. De plus le cardinal du support de σ' est inférieur au cardinal du support de σ. Par hypothèse de récurrence, on a qu'il existe des cylces $c_1, \dots, c_t$ tels que $\sigma' = c_1 \dots c_t$ avec les supports de c_i disjoints deux a deux et aussi disjoints du support de c. On conclut que $\sigma = c c_1 \dots c_t$.

Montrons enfin l'unicité de la décomposition. Supposons que $\sigma = c_1 \dots c_t = c'_1 \dots c'_{t'}$, où les cycles c_1 d'une part et c'_i de l'autre sont deux à deux à support disjoint. On le montre par récurrence sur t le cas $t = 0$ étant trivial. Soit $i \in \{1, \dots, n\}$ tel que $i \in \mathrm{supp}(c_1)$. Il existe alors un unique $j \in \{1, \dots, t'\}$ tel que $i \in \mathrm{supp}(c'_j)$. Quitte à changer l'ordre des c'_i, on peut supposer $j = 1$. Alors il est clair qu'il existe $t > 0$ tel que $c_1 = (i\, \sigma(i) \dots \sigma^{t-1}(i)) = c'_1$. Il en résulte alors que $c_2 \dots c_t = c'_2 \dots c'_{t'}$ et par hypothèse de récurrence on a $t = t'$ et, quitte à changer l'ordre, $c_i = c'_i$ pour tout $i \leq t$. □

Exercice 2.2.1. — (1) *Décrire les éléments de $\mathcal{S}_4$ et $\mathcal{S}_5$.*

(2) *Montrer que, si c et c' sont deux k-cycles dans $\mathcal{S}_n$, il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $c' = \sigma c \sigma^{-1}$ (on dit que σ et σ' sont conjuguées).*

(3) *Montrer à l'aide de la proposition 2.7, que deux premutations σ et σ' de $\mathcal{S}_n$ sont conjuguées si et seulement si, on peut écrire $\sigma = c_1 \dots c_t$ et $\sigma' = c_1 \dots c_t$ où les cycles c_i d'une part et c'_i de l'autre sont deux à deux à support disjoint et $\mathrm{ord}(c_i) = \mathrm{ord}(c'_i)$ pour tout $1 \leq i \leq t$.*

(4) *Si $\sigma = c_1 \dots c_t$, donnez l'ordre de σ en fonction des ordres des c_i.*

(5) *Quel est le plus grand ordre possible pour un élément de $\mathcal{S}_4$, $\mathcal{S}_5$, $\mathcal{S}_n$?*

Corollaire 2.9. — *Toute permutation s'écrit comme produit de transpositions.*

Démonstration. — Compte tenu du théorème 2.8, il suffit de montrer la proposition pour un cycle. On vérifie que :

$$(i_1 \dots i_t) = (i_1\, i_t)(i_1\, i_{t-1}) \dots (i_1\, i_2).$$

□

2.3. La signature. — Attention! La décomposition d'une permutation en produit de transpositions n'est pas unique. Par exemple :

$$\begin{aligned}(1\,2\,3) &= (1\,3)(1\,2)\\ &= (2\,3)(1\,3)\\ &= (1\,3)(4\,2)(1\,2)(1\,4)\\ &= (1\,3)(4\,2)(1\,2)(1\,4)(2\,3)(2\,3).\end{aligned}$$

D'après cet exemple on pourrait conjecturer que la parité du nombre des transpositions dans la décomposition est fixe. Le théorème suivant confirme notre hypothèse.

Théorème 2.10. — *Soit $n \geq 2$. Il existe une unique fonction surjective $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$, appelée signature, telle que l'une des conditions équivalentes suivantes est satisfaite :*

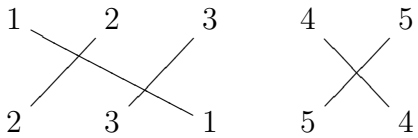
(1) *ε est un homomorphisme de groupes et $\varepsilon(\tau) = -1$ si τ est une transposition.*

(2) *$\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$ où $\mathrm{Inv}(\sigma)$ est le nombre d'inversions de σ, c'est-à-dire, le nombre de couples $(i,j) \in \{1,\ldots,n\}^2$ tels que $i < j$ mais $\sigma(i) > \sigma(j)$.*

On va présenter ici une preuve différente de celle qu'on a vu en cours. Vous devez connaître l'une des deux.

Exemple 2.11. — (1) La signature d'une permutation $\sigma \in \mathcal{S}_n$ quelconque vaut donc $\varepsilon(\sigma) = (-1)^a$ où a est le nombre de cycles de longueur paire dans une décomposition de σ en produit de cycles disjoints.

(2) Pour compter le nombre d'inversions d'une permutation il suffit de faire le diagramme suivant. Supposons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$. On trace un ligne entre chaque $1 \leq i \leq 5$ dans la première ligne et lui-même dans la séconde. Comme suit :



Le nombre de croisements des lignes du diagramme (3 dans notre exemple) est le nombre d'inversions (pourquoi ?)

Démonstration. — On définit $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$ par :

- $\varepsilon(Id) = 1$.
- Si c est un k-cycle, alors $\varepsilon(c) = (-1)^{k-1}$
- $\sigma = c_1 \ldots c_t$ est une décomposition de σ en produit de cycles disjoints, alors $\varepsilon(\sigma) = \varepsilon(c_1)\ldots\varepsilon(c_t)$.

Montrons que ε ainsi défini est un homomorphisme de groupes, c'est-à-dire, prouvons que $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$ si $\sigma, \tau \in \mathcal{S}_n$. On fait d'abord le cas où σ est une transposition.

Lemme 2.12. — *Soient* $1 \leq a \neq b \leq n$ *deux entiers différents positifs et soit* $\sigma \in \mathcal{S}_n$. *Alors* $\varepsilon((a\,b) \circ \tau) = -\varepsilon(\tau)$ *et* $\varepsilon(\tau \circ (a\,b)) = -\varepsilon(\tau)$.

Démonstration. — Prouvons que $\varepsilon((a\,b) \circ \tau) = -\varepsilon(\tau)$, l'autre égalité se montre de la même façon. Soit $\tau = c_1 \dots c_t$ une décomposition de τ en produit de cycles disjoints. Il faut traiter quatre cas distincts.

• Supposons d'abord que $a, b \notin \mathrm{supp}(c_i)$ pour tout $1 \leq i \leq t$. Alors $(a\,b)c_1 \dots c_t$ est la décomposition en produit de cycles disjoints de $(a\,b) \circ \tau$ donc, par définition, $\varepsilon((a\,b) \circ \tau) = \varepsilon((a\,b))\varepsilon(\tau) = -\varepsilon(\tau)$.

• Supposons maintenant que $a \notin \mathrm{supp}(c_i)$ pour tout $1 \leq i \leq t$ et qu'il existe $1 \leq l \leq t$ tel que $b \in \mathrm{supp}(c_l)$. On écrit $c_l = (b\,j_1 \dots j_k)$. Alors $c_1 \dots c_l' \dots c_t$, avec $c_l' = (b\,j_1 \dots j_k\,a)$, est la décomposition en produit de cycles disjoints de $(a\,b) \circ \tau$. Comme $\varepsilon(c_l') = -\varepsilon(c_l)$, on trouve que $\varepsilon((a\,b) \circ \tau) = -\varepsilon(\tau)$.

• Supposons qu'il existe $1 \leq l \leq t$ tel que $a, b \in \mathrm{supp}(c_l)$. On écrit $c_l = (b\,j_1 \dots j_r\,a\,j_{r+1} \dots j_k)$. Alors $c_1 \dots c_l' c_l'' \dots c_t$, avec $c_l' = (b\,j_1 \dots j_r)$ et $c_l'' = (a\,j_{r+1} \dots j_k)$, est la décomposition en produit de cycles disjoints de $(a\,b) \circ \tau$. Comme $\varepsilon(c_l')\varepsilon(c_l'') = -\varepsilon(c_l)$, on trouve que $\varepsilon((a\,b) \circ \tau) = -\varepsilon(\tau)$.

• Supposons finalement qu'il existe $1 \leq l < m \leq t$ tel que $a \in \mathrm{supp}(c_l)$ et $b \in \mathrm{supp}(c_m)$. On écrit $c_l = (a\,j_1 \dots j_r)$ et $c_m = (b\,f_1 \dots f_s)$. Alors $c_1 \dots c_{l-1}c_{l+1} \dots c_{m-1}c_{m+1} \dots c_t c$, avec $c = (a\,j_1 \dots j_r\,b\,f_1 \dots f_s)$, est la décomposition en produit de cycles disjoints de $(a\,b) \circ \tau$. Comme $\varepsilon(c_l')\varepsilon(c_m) = -\varepsilon(c)$, on trouve que $\varepsilon((a\,b) \circ \tau) = -\varepsilon(\tau)$.

□

Soient $\sigma, \tau \in \mathcal{S}_n$. Montrons par récurrence sur le cardinal de $\mathrm{supp}(\sigma)$ que $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Si $|\mathrm{supp}(\sigma)| = 0$, alors $\sigma = Id$ et le résultat est clair. Sinon soit $a \in \mathrm{supp}(\sigma)$ et notons $b = \sigma(a)$. On pose $\sigma' = \sigma \circ (a\,b)$. Alors $|\mathrm{supp}(\sigma')| < |\mathrm{supp}(\sigma)|$ car σ' laisse fixe les points fixes de σ et, en plus, b.

On a donc que $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma \circ (a\,b) \circ (a\,b) \circ \tau) = \varepsilon(\sigma' \circ (a\,b) \circ \tau) = \varepsilon(\sigma')\varepsilon((a\,b) \circ \tau)$ par hypothèse de récurrence. Mais, d'après le lemme 2.12, $\varepsilon(\sigma')\varepsilon((a\,b) \circ \tau) = \varepsilon(\sigma')\varepsilon((a\,b))\varepsilon(\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Cela prouve (1). Prouvons (2). On commence par calculer le nombre d'inversions d'une transposition $(a\,b)$.

Lemme 2.13. — *Soient* $1 \leq a < b \leq n$ *deux entiers différents positifs. Alors* $\mathrm{Inv}((a\,b)) = 2(b-a) - 1$. *On a donc que* $(-1)^{\mathrm{Inv}((a\,b))} = -1$.

Démonstration. — Quand est-ce qu'un couple $\{i, j\}$ est une inversion ? Il faut que ou bien $i = a$ et $j \in \{a+1, \dots, b\}$ ou bien $j = b$ et $i \in \{a+1, \dots, b-1\}$ (si vous ne le voyez pas, faites d'abord l'exemple $(2\,6) \in \mathcal{S}_7$ et dessinez le diagramme de l'exemple 2.11). Le nombre total d'inversions est donc $2(b-a) - 1$. □

Le cas général se montre de la même façon une fois on a compris le cas d'une transposition :

Lemme 2.14. — *Soient $1 \leq a < b \leq n$ deux entiers différents positifs. Soit $\sigma \in \mathcal{S}_n$. Alors $(-1)^{\mathrm{Inv}((a\,b)\sigma)} = -(-1)^{\mathrm{Inv}(\sigma)}$.*

Démonstration. — Notons :

$$I_1 = \{\{i,j\} \in \{1,\dots,n\}^2 : i<j, \sigma(i) > \sigma(j);\ \text{et } \sigma(j) = a, \sigma(i) \in \{a+1,\dots,b\} \\ \text{ou } \sigma(i) = b, \sigma(j) \in \{a+1,\dots,b-1\}\}$$

$I_2 = \mathrm{Inv}(\sigma) \backslash I_1$

Le nombre d'inversions de $(a\,b)\sigma$ est, avec ces notations, $|I_2| + 2(b-a) - 1 - |I_1|$ qui a la parité opposée de $|I|$. □

Le lemme 2.14 implique l'équivalence de (1) et (2). □

Définition 2.15. — Soit $\sigma \in \mathcal{S}_n$. On dit que σ est une permutation *paire* si $\varepsilon(\sigma) = 1$. Sinon, on dit qu'elle est impaire.

Définition 2.16. — On définit le groupe alterné A_n comme le noyau du homomorphisme $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$, c'est-à-dire, le sous-groupe de $\mathcal{S}_n$ formé des permutations paires. C'est un sous-groupe distingué de $\mathcal{S}_n$ (pourquoi ?)

3. Groupes commutatifs finis

Avant de nous placer dans le cadre des groupes commutatifs, montrons un lemme général qu'on utilisera souvent dans la suite.

Lemme 3.1. — *Soient H, K deux sous-groupes distingués dans G, tels que :*

(1) $H \cap K = \{e_G\}$
(2) $HK = G$

Alors G est isomorphe à $H \times K$.

Démonstration. — Soient $(h,k) \in H \times K$. Prouvons d'abord que $hk = kh$. En effet $(hkh^{-1})k^{-1} \in K$ (car $K \lhd G$), mais aussi $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H$ (car $H \lhd G$). On déduit que $hkh^{-1}k^{-1} \in H \cap K$ et donc $hkh^{-1}k^{-1} = e_G$.

On déduit que HK est un sous-groupe de G et que l'application :

$$\begin{aligned} f : H \times K &\to G \\ (h,k) &\mapsto hk \end{aligned}$$

est un morphisme de groupes. Par l'hypothèse (2), f est surjectif. Et par l'hypothèse (1), $\ker(f) = \{e_G\}$. On déduit que f est un isomorphisme. □

Dans cette section on va prouver le théorème suivant que vous devez bien savoir :

Théorème 3.2 **(Classification des groupes commutatifs finis)**
Soit G un groupe fini commutatif. Alors il existe des uniques entiers positifs $n_1, n_2, \dots n_r$ tels que :

(1) *n_i divise n_{i+1} pour tout $1 \leq i \leq r-1$.*

(2) *G est isomorphe à* $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$

Définition 3.3. — Les $\mathrm{Z}/d_i\mathrm{Z}$ (ou la collection des entiers $d_1, ..., d_k$) intervenant dans la décomposition de G sont appelés *facteurs invariants* de G.

3.1. Rappels d'arithmétique. — Vous devriez connaître les résultats de ce paragraphe. On les rappelle.

Théorème 3.4 **(Théorème de Bézout)**. — *Soient $a, b \in \mathbf{Z}$. Alors :*

(1) *Il existe des entiers $u, v \in \mathbf{Z}$ tels que*

$$au + bv = \mathrm{pgcd}(a, b).$$

(2) $\mathrm{pgcd}(a, b) = 1$ *si, et seulement si, il existe des entiers $u, v \in \mathbf{Z}$ tels que $au + bv = 1$.*

Théorème 3.5 **(Théorème chinois)**. — *Le morphisme de groupes*

$$\begin{aligned} f : \mathbf{Z} &\to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \\ x &\mapsto (\boldsymbol{cl}(x), \boldsymbol{cl}(x)) \end{aligned}$$

est surjectif si, et seulement si $\mathrm{pgcd}(n, m) = 1$. *Dans ce cas,* $\ker(f) = nm\mathbf{Z}$.

On déduit du théorème 1.44 :

Corollaire 3.6. — *Soient $n, m \in ZZ$ deux entiers positifs premiers entre eux. Alors on a un isomorphisme de groupes :*

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/nm\mathbf{Z}$$

Qu'est-ce qu'il se passe lors que n et m ne sont pas premiers entre eux ? Le lemme suivant répond à cette question :

Lemme 3.7. — *Soient $n, m \in ZZ$ deux entiers positifs. Alors on a un isomorphisme de groupes :*

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/\mathrm{pgcd}(n, m)\mathbf{Z} \times \mathbf{Z}/\mathrm{ppcm}(n, m)\mathbf{Z}.$$

Démonstration. — On fait la décomposition de n et m en facteurs premiers :

$$n = \prod_{p \in P} p^{v_p(n)} \qquad m = \prod_{p \in P} p^{v_p(m)}.$$

où le produit porte su P l'ensemble de nombres premiers positifs et $v_p(x)$ denote la valuation p-adique de x. Par le théorème chinois on a un isomorphisme :

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} &\simeq \prod_{p \in P} \mathbf{Z}/p^{v_p(n)}\mathbf{Z} \times \prod_{p \in P} \mathbf{Z}/p^{v_p(m)}\mathbf{Z} \\ &\simeq \prod_{p \in P} \mathbf{Z}/p^{\max(v_p(n), v_p(m))}\mathbf{Z} \times \prod_{p \in P} \mathbf{Z}/p^{\min(v_p(n), v_p(m))}\mathbf{Z} \\ &\simeq \mathbf{Z}/\mathrm{pgcd}(n, m)\mathbf{Z} \times \mathbf{Z}/\mathrm{ppcm}(n, m)\mathbf{Z}, \end{aligned}$$

d'après, à nouveau, le théorème chinois. □

On va écrire le théorème de Bézout sous forme matricielle :

Proposition 3.8. — *Soient $a, b \in \mathbf{Z}$. Il existe un matrice 2×2 à coefficients dans $\mathbf{Z}$ et de déterminant 1 dont la première ligne et $(a\, b)$ si, et seulement si, a et b sont premiers entre eux.*

On déduit par récurrence la proposition suivante :

Proposition 3.9. — *Soient $n_1, n_2, \ldots, n_r \in \mathbf{Z}$. Il existe un matrice $r \times r$ à coefficients dans $\mathbf{Z}$ et de déterminant 1 dont la première ligne et $(n_1\, n_2 \ldots\, n_r)$ si, et seulement si,* $\mathrm{pgcd}(n_1, n_2, \ldots, n_r) = 1$.

Démonstration. — La preuve se fait par récurrence sur r, le cas $r = 2$ étant la proposition précédente. On suppose alors $r \geq 3$. Soient $d = \mathrm{pgcd}(n_1, n_2, \ldots, n_{r-1})$ et posons, pour $1 \leq i \leq r-1$, $b_i = n_i/d$. Les entiers b_i sont premiers entre eux donc par hypothèse de récurrence, il existe un matrice $(r-1) \times (r-1)$ à coefficients dans $\mathbf{Z}$ et de déterminant 1 dont la première ligne et $\mathbf{b} = (b_1\, b_2 \ldots\, b_{r-1})$.

D'un autre côté, $\mathrm{pgcd}(d, n_r) = 1$ donc il existe $u, v \in \mathbf{Z}$ tels que :

$$ud + vn_r = 1.$$

Soit C la matrice construite en supprimant la première ligne de B. Posons A la matrice $r \times r$ définie par :

$$\begin{pmatrix} db_1 & \ldots & db_{r-1} & n_r \\ & C & & 0 \\ -vb_1 & \ldots & -vb_{r-1} & u \end{pmatrix}$$

A partir de la dernière colonne on calcule le déterminant de A.

$$\begin{aligned} \det(A) &= (-1)^{r-1} n_r \det \begin{pmatrix} C \\ -v\mathbf{b} \end{pmatrix} + u \det \begin{pmatrix} d\mathbf{b} \\ C \end{pmatrix} \\ &= (-1)^r v n_r \det \begin{pmatrix} C \\ \mathbf{b} \end{pmatrix} + ud \det \begin{pmatrix} \mathbf{b} \\ C \end{pmatrix} \\ &= (-1)^{2r-2} v n_r \det \begin{pmatrix} \mathbf{b} \\ C \end{pmatrix} + ud \det \begin{pmatrix} \mathbf{b} \\ C \end{pmatrix} \\ &= vn_r + ud \\ &= 1. \end{aligned}$$

La réciproque est facile (je vous la laisse en exercice). □

Remarquons que si A est une matrice à coefficients dans $\mathbf{Z}$ et de déterminant 1 alors A^{-1} est une matrice à coefficients dans $\mathbf{Z}$ et de déterminant 1 (pourquoi ?)

3.2. Preuve du théorème 3.4. — Supposons dans le reste de cette section, que G est un groupe fini commutatif. On utilisera la notation additive, c'est-à-dire, on écrira $a+b$ au lieu de $a*b$, $-a$ au lieu de a^{-1}, na au lieu de a^n, etc. Ceci nous permet de faire des combinaisons linéaires des éléments de G avec des coefficients dans $\mathbf{Z}$ (on dit que G est un $\mathbf{Z}$-module...)

On déduit d'abord un corollaire de la proposition 3.9.

Corollaire 3.10. — *Supposons que G est engendré par des éléments $x_1, \dots, x_r$ et soient $n_1, n_2, \dots, n_r \in \mathbf{Z}$ tels que* $\mathrm{pgcd}(n_1, n_2, \dots, n_r) = 1$. *Alors il existe un ensemble générateur de G de cardinal r et dont l'un des éléments est $\sum_{i=1}^{r} n_i x_i$.*

Démonstration. — Soit A la matrice $r \times r$ à coefficients dans $\mathbf{Z}$ et de déterminant 1 dont la première ligne et $(n_1\, n_2 \dots\, n_r)$ donnée par la proposition 3.9. Soit X, Y les vecteurs colonnes défini par :

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix}, \qquad Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_r \end{pmatrix} := AX.$$

Les y_i étant des combinaisons linéaires des x_i sont des éléments de G. De plus $y_1 = \sum_{i=1}^{r} n_i x_i$. On a que $X = A^{-1}Y$. Comme A est une matrice à coefficients dans $\mathbf{Z}$ et de déterminant 1 on a que A^{-1} est une matrice à coefficients dans $\mathbf{Z}$. On déduit que les x_i sont des combinaisons linéaires des y_i, d'où le corollaire. □

Prouvons enfin le théorème 3.4 par récurrence sur le cardinal de G. Le cas où $|G| = 1$ étant trivial, on suppose que G a cardinal n et que le théorème est montré pour tout groupe commutatif de cardinal inférieur à n.

Soit r un entier minimal tel que G puisse être engendré avec r éléments. Parmi tous les ensembles de générateurs $\{x_1, \dots, x_n\}$ de taille r, on en choisit un qui contient un élément d'ordre minimal k (disons, pour fixer les notations, que cet élément est x_1). Soit $H = \langle x_2, \dots, x_r \rangle$. Alors H est un sous-groupe propre de G et donc par récurrence :

$$H \simeq \mathbf{Z}/n_2\mathbf{Z} \times \mathbf{Z}/n_3\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$$

avec $n_2 | n_3 | \dots | n_s$. Montrons que $G \simeq \langle x_1 \rangle \times H$. D'après le lemme 3.1, il suffit de montrer que $\langle x_1 \rangle \cap H = \{e_G\}$. Supposons qu'il existe $z \in \langle x_1 \rangle \cap H$ tel que $z \neq e_G$. Alors :

$$z = a_1 x_1 = \sum_{i=2}^{r} a_i x_i,$$

avec $0 < a_i < k$. Soit $d = \mathrm{pgcd}(a_1, a_2, \dots, a_r)$. Posons $g = \frac{a_1}{d} x_1 - \sum_{i=2}^{r} \frac{a_i}{d} x_i$. L'ordre de g est plus petit que k (car $dg = 0$ et $d \leq a_1 < k$). Comme les $\frac{a_i}{d}$, $1 \leq i \leq r$ sont premiers entre

eux, d'après le corollaire précédent, il existe un ensemble générateur de G de cardinal r et dont l'un des éléments est g. Contradiction.

Donc $G \simeq \langle x_1 \rangle \times H \simeq \mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$. Montrons que $k|n_2$. Sinon, d'après le lemme 3.7, on aurait que :

$$G \simeq \mathbf{Z}/\mathrm{pgcd}(k, n_2)\mathbf{Z} \times \mathbf{Z}/\mathrm{ppcm}(k, n_2)\mathbf{Z} \times \mathbf{Z}/n_3\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$$

avec $\mathrm{pgcd}(k, n_2) < k$ ce qui contredit la minimalité de k.

Prouvons enfin l'unicité. Soit :

$$G = \underbrace{\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_1\mathbf{Z}}_{t_1 \text{ fois}} \times \underbrace{\mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_2\mathbf{Z}}_{t_2 \text{ fois}} \times \cdots \times \underbrace{\mathbf{Z}/n_r\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}}_{t_r \text{ fois}}$$

avec $t_1, t_2, \ldots, t_r > 0$, $n_1|n_2| \ldots |n_r$ et $n_i \neq n_j$ si $i \neq j$. Montrons que les n_i et les t_i, $1 \leq i \leq r$, sont uniquement déterminés par G.

On le montre par récurrence sur r. Si $r = 1$, alors n_1 est le plus petit entier k tel que $kG = 0$ et $n_1^{t_1} = |G|$, ce qui détermine t_1.

Supposons $r > 1$ et l'unicité montré pour tout groupe commutatif :

$$G' = \underbrace{\mathbf{Z}/n'_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n'_1\mathbf{Z}}_{t'_1 \text{ fois}} \times \underbrace{\mathbf{Z}/n'_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n'_2\mathbf{Z}}_{t'_2 \text{ fois}} \times \cdots \times \underbrace{\mathbf{Z}/n'_{r'}\mathbf{Z} \times \cdots \times \mathbf{Z}/n'_{r'}\mathbf{Z}}_{t'_{r'} \text{ fois}}$$

avec $r' < r$. Alors :

$$n_1 G = \underbrace{\mathbf{Z}/\frac{n_2}{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/\frac{n_2}{n_1}\mathbf{Z}}_{t_2 \text{ fois}} \times \cdots \times \underbrace{\mathbf{Z}/\frac{n_r}{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/\frac{n_r}{n_1}\mathbf{Z}}_{t_r \text{ fois}}$$

Par hypothèse de récurrence on a que les n_i et les t_i, $2 \leq i \leq r$, sont uniquement déterminés par G. De même n_1 est le plus petit entier k tel que kG est engendré par moins d'éléments que G, par exactement t_1 générateurs en moins (ce qui détermine uniquement t_1).

3.3. On déduit la proposition suivante :

Proposition 3.11 **(Lemme de Cauchy pour les groupes commutatifs)**
Soit G un groupe commutatif fini de cardinal n. Soit p un nombre premier et supposons que p divise n. Alors il existe un élément $g \in G$ d'ordre p.

Démonstration. — D'après le théorème de classification G est isomorphe à un groupe de la forme $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$. Puisque p divise n il existe $1 \leq i \leq r$ tel que p divise n_i. Soit $t \in \mathbf{Z}$ tel que $n_i = tp$. Alors l'élément $g = (0, \ldots, 0, \overline{t}, 0, \ldots, 0) \in \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_{i-1}\mathbf{Z} \times \mathbf{Z}/n_i\mathbf{Z} \times \mathbf{Z}/n_{i+1}\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$, répond à la question.

□

Exercice 3.3.1 **(Lemme de Cauchy)**. — *Soit G un groupe fini non nécessairement commutatif de cardinal n. Soit p un nombre premier et supposons que p divise n. Montrer qu'il existe un élément $g \in G$ d'ordre p.*

3.4. Composantes primaires d'un groupe abélien fini.—

Définition 3.12. — Soit p un nombre premier et G un groupe abélien fini. On appelle composante p-primaire de G l'ensemble $G(p)$ des éléments de G dont l'ordre est une puissance de p.

Remarque 3.13. — (1) $G(p)$ est un sous-groupe de G .
(2) $G(p)$ est un p-groupe.
(3) $G(p) \neq \{e\} \Longleftrightarrow p$ divise $|G|$.

Théorème 3.14. — *Soit G un groupe abélien fini d'ordre $n = p_1^{n_1} \dots p_r^{n_r}$ où les p_i sont des nombres premiers distincts. Alors, pour chaque $i \in \{1, \dots, r\}$, $G(p_i)$ est d'ordre $p_i^{n_i}$ et*

$$G \simeq G(p_1) \times .... \times G(p_r).$$

Démonstration. — D'après le théorème G est isomorphe à $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z}$; on peut donc supposer que $G = \mathbf{Z}/n_1\mathbf{Z}$. Mais dans ce cas $G = \prod_{p \in P} \mathbf{Z}/p^{v_p(n_1)}\mathbf{Z}$ et $G(p) \simeq \mathbf{Z}/p^{v_p(n_1)}$ ce qui montre le théorème. □

4. Opération d'un groupe sur un ensemble

4.1. Généralités. — La notion d'opération d'un groupe sur un ensemble est très important. Cette section sera clé dans la suite du cours.

Définition 4.1. — On dit qu'un groupe G *opère* à gauche sur un ensemble X s'il existe une application

$$\begin{array}{rcl} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

telle que

(1) $e_G \cdot x = x$ pour tout $x \in X$.
(2) $(g * g') \cdot x = g \cdot (g' \cdot x)$ pour tous $g, g' \in G$ et tout $x \in X$.

On peut définir de façon naturelle les opérations à droite. Pour simplifier un peu on ne considérera ici que des opérations à gauche et le mot *opération* voudra dire *opération à gauche*. Des fois on dit aussi que G *agit* sur X.

Remarque 4.2. — Grâce à (2), on peut écrire simplement $g * g' \cdot x$ ou simplement $gg'x$ s'il n'y a pas de confusion entre le produit dans le groupe et l'opération du groupe sur l'ensemble (ce qui peut arriver quand $X = G$).

Exemple 4.3. — (1) D'abord un exemple d'importance historique. Lagrange faisait opérer $\mathcal{S}_n$ sur l'ensemble $K(x_1, \dots, x_n)$ des polynômes à n variables, par $\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. (Quels sont les polynômes invariants pas l'opération ?)
(2) Le groupe $\mathcal{S}_3$ opère sur le triangle équilatéral ABC par permutation des sommets.

(3) Le groupe symétrique $\mathcal{S}_n$ opère sur l'ensemble $\{1, \ldots, n\}$.
(4) Le groupe linéaire $\mathrm{GL}(3, \mathbf{R})$ opère sur $\mathbf{R}^3$.
(5) Le groupe d'isométries affines de $\mathbf{R}^2$ (ou $\mathbf{R}^3$) opère sur $\mathbf{R}^2$ (ou $\mathbf{R}^3$). C'est le groupe de transformations de $\mathbf{R}^2$ (ou $\mathbf{R}^3$) qui préservent la mesure.

Ces deux derniers groupes opèrent aussi sur l'ensemble de droites (du plan ou de l'espace). Est-ce qu'ils opèrent sur l'ensemble de cercles ?

(4) $\mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_n(\mathbf{R})$ opère sur l'ensemble de matrices $n \times n$ par $(A, B) \cdot M = AMB^{-1}$.

Les opérations de groupes font le lien entre la théorie de groupes et la géométrie. A chaque géométrie on peut lui associer un groupe qui préserve les notions de base de cette géométrie (par exemple les droites, les cercles...) : le groupe des isométries affines pour la géométrie euclidienne, le groupe de transformations affines pour la géométrie affine plane, le groupe des homographies pour la géométrie projective, le groupe de Lorentz pour la géométrie hyperbolique... Pour certains mathématiciens la définition même de géométrie est juste l'étude d'un ensemble muni de l'opération d'un groupe ![(1)]

Dans ce cours, plus modeste, on va se contenter simplement d'étudier les groupes eux-mêmes. Pour cela on va traduire cette notion naturelle d'opération en une autre, équivalente, qui s'adapte un peu mieux à nos besoins.

Soit $(g, x) \mapsto g \cdot x$ une opération d'un groupe G sur un ensemble X. Alors l'application :

$$\begin{aligned} \phi_g : X &\to X \\ x &\mapsto g \cdot x \end{aligned}$$

est une bijection (quelle est l'inverse ?) On trouve alors une fonction :

$$\begin{aligned} \phi : G &\to \mathcal{S}_X \\ g &\mapsto \phi_g \end{aligned} \tag{4.1}$$

Proposition 4.4. — *L'application ϕ est un morphisme de groupes.*

Démonstration. — Soit $x \in X$ et $g, g' \in G$. On a :

$$\phi_{g*g'}(x) = (g * g') \cdot x = g \cdot (g' \cdot x) = (\phi_g \circ \phi_{g'})(x).$$

□

Réciproquement, étant donné un morphisme de groupes $\phi : G \to \mathcal{S}_X$, on peut lui associer une opération $(g, x) \mapsto \phi(g)(x)$. Ces deux procédés sont inverses l'un de l'autre. On peut donc penser que chaque élément de G devient une *symétrie* de l'ensemble X... Selon la convenience, on utilisera une définition ou l'autre (il faut bien comprendre les deux et le passage entre elles !)

Définition 4.5. — Soit G un groupe qui opère sur un ensemble X. Soit $x \in X$.

(1) On dit que x est un *point fixe* si $g \cdot x = x$ pour tout $g \in G$. On notera X^G le sous-ensemble de X formé des points fixes.

(1) Si ça vous intéresse, vous pouvez faire de recherches sur internet sur le *programme d'Erlanguen* de Felix Klein. En particulier sur la page de Daniel Perrin, vous pouvez trouver certains textes sur ce programme.

(2) L'*orbite* de x, qu'on note $O(x)$, est le sous-ensemble de X défini par :

$$O(x) = \{g \cdot x : g \in G\}.$$

(3) Le *stabilisateur* de x est le *sous-groupe* (montrez-le !) de G défini par :

$$\mathrm{St}(x) = \{g \in G : g \cdot x = x\}.$$

Il est clair que x est un point fixe si et seulement si $O(x) = \{x\}$ ou encore si $\mathrm{St}(x) = G$. Encore des définitions !

Définition 4.6. — Soit G un groupe qui opère sur un ensemble X.

(1) On dit que G opère *fidèlement* si $g \cdot x = x$ pour tout $x \in X$ implique $g = e_G$, c'est à dire, l'élément neutre est le seul élément du groupe qui laisse invariant tous les éléments de X. Cette définition équivaut au fait que le morphisme ϕ défini en (4.1) soit injectif, c'est-à-dire, $\ker(\phi) = \{e_G\}$ (vous pouvez vérifier que $\ker(\phi) = \bigcap_{x \in X} \mathrm{St}(x)$).

(2) On dit que G opère *transitivement* si pour tous $x, x' \in X$ il existe $g \in G$ tel que $g \cdot x = x'$, c'est-à-dire, $O(x) = X$ pour tout $x \in X$. Remarquons que G opère transitivement sur chaque orbite.

(3) On dit que G opère *simplement transitivement* si pour tous $x, x' \in X$ il existe un unique $g \in G$ tel que $g \cdot x = x'$ (vous pouvez vérifier que une opération est transitive et fidèle si, et seulement si, elle est simplement transitive).

Exercice 4.1.1. — *Calculer les orbites, stabilisateurs et points fixes dans les exemples 4.3. Décidez si les opérations sont transitives, fidèles...*

De façon informelle, on dira qu'une propriété d'un groupe est *géométrique* si elle est relative à un opération (points fixes, orbites...) par opposition aux propriétés *algébriques* (ordre, commutativité...)

Soit G un groupe qui opère sur un ensemble X. On introduit la relation binaire suivante sur X :

$$x \mathscr{R} y \text{ si et seulement s'il existe } g \in G : g \cdot x = y.$$

qui mesure le défaut de transitivité.

Proposition 4.7. — *La relation binaire définie ci-dessus est une relation d'équivalence.*

Démonstration. — Exercice facile. □

Les classes d'équivalence pour cette relation sont les orbites de X. Si G opère transitivement il n'y a qu'une seule orbite.

Remarque 4.8. — On déduit que l'ensemble d'orbites forme une partition de X, c'est-à-dire :

$$X = \bigsqcup_{\overline{x} \in X/\mathscr{R}} O(x)$$

où x est un représentant de la classe $\overline{x}$. Si X est un ensemble fini, on déduit :

$$|X| = \sum_{\overline{x} \in X/\mathscr{R}} |O(x)|. \tag{4.2}$$

Proposition 4.9. — *Soit G un groupe qui opère sur un ensemble X. Soient $x \in X$ et $g, g' \in G$. On a : $g\mathrm{St}(x) = g'\mathrm{St}(x)$ si, et seulement si, $g \cdot x = g' \cdot x$. On déduit que l'application :*

$$\begin{array}{rcl} G/\mathrm{St}(x) & \to & O(x) \\ \overline{g} & \mapsto & g \cdot x \end{array}$$

est bien définie et est une bijection.

Démonstration. — On a : $g\mathrm{St}(x) = g'\mathrm{St}(x)$ si, et seulement si, $g^{-1}g' \in \mathrm{St}(x)$ si et seulement si, $g^{-1}g' \cdot x = x$, c'est-à-dire, $g \cdot x = g' \cdot x$.

On déduit que l'application :

$$\begin{array}{rcl} G/\mathrm{St}(x) & \to & O(x) \\ \overline{g} & \mapsto & g \cdot x \end{array}$$

est bien définie. Elle est surjective par définition d'orbite. Et si $g \cdot x = g' \cdot x$, alors $g\mathrm{St}(x) = g'\mathrm{St}(x)$, d'où l'injectivité. □

Remarque 4.10. — Si G est fini, on déduit :

$$|G| = |O(x)||\mathrm{St}(x)|. \tag{4.3}$$

En particulier, $|O(x)|$ divise $|G|$.

Les équations (4.2) et (4.3) sont très importantes pour les exercices et il faut bien les connaître !

4.2. Exemples importants d'opérations. — Les opérations suivantes sont très importantes, on va les utiliser très souvent.

(1) On peut faire opérer G sur lui même par translation à gauche : $g \cdot g' = g * g'$. On remarque que G opère simplement transitivement : si $g, g' \in G$ il existe un unique $h \in G$ tel que $gh = g'$ (on pose $h = g^{-1}g'$). En particulier G opère fidèlement. On déduit que le morphisme :

$$\phi : G \to \mathcal{S}_G$$

est injectif. En particulier, quand G est fini de cardinal n on a le théorème de Cayley :

Théorème 4.11 **(Théorème de Cayley)**. — *Si G est un groupe fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.*

On voit avec ce théorème l'importance du groupe symétrique : tout groupe fini est isomorphe à un sous-groupe du groupe symétrique. Il serait tentant de calculer les sous-groupes de $\mathcal{S}_n$ en général (faites-le pour $n = 2, 3, 4, 5$).

Etant donné un élément $g \in G$, quelle est la décomposition en cycles disjoints de $\phi(g)$?

Exercice 4.2.1. — *Soit G un groupe fini de cardinal n et soit $g \in G$ un élément d'ordre d.*

(a) *Prouvez que $\phi(g)$ est un produit de n/d cycles disjoints de longueur d.*

(b) *Supposons de plus que d est pair et n/d impaire. Montrez que G contient un sous-groupe distingué d'indice 2 (vous pouvez penser à la signature...) En particulier G n'est pas simple.*

(c) *En déduire qu'un groupe de cardinal $2m$ avec m impaire n'est pas simple.*

En fait on se rend compte qu'il n'est pas très pratique de considérer un groupe de cardinal n en tant que sous-groupe de $\mathcal{S}_n$: par exemple, le groupe alterné A_4 serait un sous-groupe de $\mathcal{S}_{12}$ qui a 12! éléments ! Il est bien plus simple d'étudier A_4 en tant que sous-groupe de $\mathcal{S}_4$...

(2) On peut aussi faire opérer G sur lui même par conjugaison : $g \cdot g' = g * g' * g^{-1}$. Les orbites s'appellent classes de conjugaison. Le stabilisateur de $g \in G$ s'appelle *centralisateur* :

$$Z(g) = \{h \in G = gh = hg\}.$$

L'ensemble des points fixes de G pour cette opération est le centre de G !

(3) Tout groupe opère sur l'ensemble de ses sous-groupes par conjugaison $g \cdot H = g * H * g^{-1}$ (et par translation ?). En fait il opère sur l'ensemble de ses sous-groupes de cardinal donné. (Quelle est l'orbite de H ? et le stabilisateur de H ?)

(4) Soit H un sous-groupe de G, pas nécessairement distingué. Le groupe G opère sur *l'ensemble* des classes G/H par $g \cdot g'H = (g * g')H$. Cette opération est transitive.

4.3. Première application aux p-groupes. —

Définition 4.12. — Soit p un nombre premier. Un p-groupe est un groupe de cardinal une puissance de p.

Exemple 4.13. — Si G est un groupe de cardinal p, alors G est un p-groupe. On a vu que, dans ce cas particulier, $G \simeq \mathbf{Z}/p\mathbf{Z}$ est cyclique.

Proposition 4.14. — *Soit G un p-groupe opérant sur un ensemble fini X. On rappelle qu'on note X^G l'ensemble des points fixes. Alors :*

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

Démonstration. — D'après l'équation (4.2), on a :

$$|X| = \sum_{\overline{x} \in X/\mathscr{R}} |O(x)|.$$

On décompose la somme de droite comme suit :

$$\sum_{\overline{x} \in X/\mathscr{R}} |O(x)| = |X^G| + \sum_{\overline{x} \in X/\mathscr{R}, x \notin X^G} |O(x)|.$$

Si $\overline{x} \in X/\mathscr{R}$ mais $x \notin X^G$, on a, d'après (4.3), que p divise le cardinal de $|O(x)|$. En regardant l'égalité :

$$|X| = |X^G| + \sum_{\overline{x} \in X/\mathscr{R}, x \notin X^G} |O(x)|$$

modulo p on trouve le résultat annoncé. □

On déduit le théorème :

Théorème 4.15. — *Le centre d'un p-groupe G n'est pas trivial.*

Démonstration. — On fait opérer G sur lui même par conjugaison. Dans ce cas, on a vu que $X^G = Z(G)$. La proposition précédente nous montre que

$$|Z(G)| \equiv 0 \mod p.$$

Comme $e_G \in Z(G)$ on a alors que $|Z(G) \geq p$, d'où le résultat.

□

Ce ci va nous permettre d'étudier les groupes de cardinal p^2. On montre d'abord un résultat facile qu'on utilisera ensuite.

Proposition 4.16. — *Soit G un groupe tel que $G/Z(G)$ soit cyclique. Alors G est abélien.*

Démonstration. — Notons $\pi = G \to G/Z(G)$ la projection canonique. Soit a_0 un générateur de $G/Z(G)$ et $g_0 \in G$ tel que $\pi(g_0) = a_0$.

Soient $g, g' \in G$. Puisque a_0 est un générateur de $G/Z(G)$, il existe $n, n' \in \mathbf{Z}$ tels que $a_0^n = \pi(g)$ et $a_0^{n'} = \pi(g')$. On a donc que $gZ(G) = g_0^n Z(G)$ et que $g'Z(G) = g_0^{n'} Z(G)$. Il existe donc $h, h' \in Z(G)$ tels que $g = hg_0^n$ et $g' = h'g_0^{n'}$. Alors :

$$gg' = hg_0^n h' g_0^{n'} = hh' g_0^n g_0^{n'} = hh' g_0^{n+n'} = hh' g_0^{n'} g_0^n = h' g_0^{n'} h g_0^n = g'g.$$

□

Corollaire 4.17. — *Un groupe G de cardinal p^2 est abélien.*

Démonstration. — La preuve se déduit directement de la proposition et du théorème précédents. On suppose que G n'est pas abélien. Alors, d'après le théorème 4.15, $Z(G)$ est de cardinal p. On déduit que $G/Z(G)$ est aussi de cardinal p : il est alors cyclique et donc abélien. Contradiction. □

5. Les théorèmes de Sylow

Définition 5.1. — Soit G un groupe fini de cardinal n. On écrit n sous la forme $n = p^\alpha m$ avec m non multiple de p. Un *p-sous-groupe de Sylow* de G est un sous-groupe de G de cardinal p^α, c'est-à-dire, un sous-groupe H de G tel que :

(1) H est un p-groupe (un p-sous-groupe de G).
(2) L'indice de H dans G est premier à p.

***Théorème 5.2* (Sylow).** — *Soit G un groupe fini de cardinal $n = p^\alpha m$ avec m non multiple de p. Alors :*

(1) *G possède un p-sous-groupe de Sylow.*
(2) *Si H_p est un p-sous-groupe de Sylow de G, tout p-sous-groupe de G est contenu dans un conjugué de H_p.*
(3) *Les conjugués de H_p sont les p-sous-groupes de Sylow de G.*
(4) *Le nombre n_p des p-sous-groupes de Sylow de G satisfait aux propriétés suivantes :*
   (a) $n_p \equiv 1 \mod p$.
   (b) *n_p divise m.*

Le reste de cette section est consacré à la preuve du théorème.

5.1. Montrons la partie (1) par récurrence sur le cardinal de G. Supposons d'abord qu'il existe un sous-groupe propre K de G d'indice premier à p. Comme le cardinal de K est strictement inférieur au cardinal de G, il contient H_p un p-sous-groupe de Sylow. Par hypothèse sur l'indice, H_p est de cardinal n^α et il est donc aussi un p-sous-groupe de Sylow de G.

Sinon tout sous-groupe propre de G a un indice divisible par p. Donc les orbites de l'action de G sur un ensemble quelconque sont ou bien réduites à un point ou bien ont un cardinal divisible par p. On fait agir G sur G par conjugaison et on déduit que $Z(G)$ a un cardinal divisible par p (pourquoi ?)

Soit $g \in Z(G)$ d'ordre p (*cf* Proposition 3.11). Notons H le groupe $G/\langle g \rangle$ et considérons la projection :

$$\pi : G \to H.$$

Le groupe H a cardinal $p^{\alpha-1}m$ et par hypothése récurrence contient donc un p-sous-groupe de Sylow H' de cardinal $p^{\alpha-1}$. Soit $H_p = \pi^{-1}(H')$. Alors H_p est un sous-groupe de G de cardinal p^α (Pourquoi ? Quel théorème est-on en train d'utiliser ?). H_p est donc un p-sous-groupe de Sylow de G.

5.2. Soit P un p-sous-groupe de G. On a vu que G agit par translations sur G/H_p. Le stabilisateur de $aH_p \in G/H_p$ est aH_pa^{-1}. Par restriction on déduit que P agit par translations sur G/H_p. Le stabilisateur de $aH_p \in G/H_p$ est maintenant $P \cap aH_pa^{-1}$. Montrons qu'il existe $a \in G$ tel que $\mathrm{St}(aH_p) = P$, c'est-à-dire, aH_p est un point fixe.

D'après la proposition 4.14, on a :

$$|G/H_p| \equiv |(G/H_p)^P| \mod p,$$

où on a noté $(G/H_p)^P$ l'ensemble de points fixes. Comme H_p est un p-sous-groupe de Sylow on a que $|G/H_p| \not\equiv 0 \mod p$. On déduit que $|(G/H_p)^P| \not\equiv 0 \mod p$ et donc $|(G/H_p)^P| \neq 0$: il y a donc des points fixes.

5.3. (3) se déduit directement des résultats ci-dessus. Les conjugués de H_p sont des p-sous-groupes de Sylow. Réciproquement, si H est un p-sous groupe de Sylow on déduit de (2) que H est contenu dans un conjugué de H_p.

Corollaire 5.3. — *Un p-sous-groupe de Sylow de G est distingué dans G si et seulement si $n_p = 1$.*

Démonstration. — Soit H un p-sous-groupe de Sylow de G. Alors H est distingué dans G si et seulement si pour tout $g \in G$ on a $gHg^{-1} = H$ si et seulement si $n_p = 1$. □

5.4. Soit X l'ensemble des p-sous-groupes de Sylow de G. Alors G agit sur X par conjugaison. D'après (3), cette action n'a qu'une seule orbite (de cardinal $|X| = n_p$). On déduit de (4.3) que n_p divise n. Montrons enfin que $n_p \equiv 1 \mod p$ (ce qui implique que n_p est premier à p et donc, par le lemme de Gauss, n_p divise m.)

Encore par restriction H_p agit sur X par conjugaison. Par la proposition 4.14, on a :

$$n_p = |X| \equiv |X^{H_p}| \mod p.$$

Montrons que $|X^{H_p}| = 1$. Il est clair que $H_p \in X^{H_p}$. Réciproquement soit $T \in X^{H_p}$ et supposons que $T \neq H_p$. Comme $T \in X^{H_p}$ on a $hTh^{-1} = T$ pour tout $h \in H_p$. Considérons G' le sous-groupe de G engendré par H_p et T. Alors, T et H_p sont des p-sous-groupes de Sylow de G' et, par hypothèse $T \lhd G'$, donc, par le corollaire 5.3, $T = H_p$. Contradiction.

6. Applications des théorèmes de Sylow

6.1. Utilisation de Sylow pour montrer qu'un groupe G fini n'est pas simple. —

Exercice 6.1.1. — *La première méthode est de prouver que le nombre n_p de p-sous-groupes de Sylow vaut 1 et ceci en utilisant la partie (4) du théorème 5.2.*

Soient p et q deux nombres premiers.

(1) *Prouver qu'un groupe d'ordre $n = p^\alpha q$ avec $p > q$ n'est pas simple (exemples: $n = 18$, 54, 50...)*

(2) *Prouver qu'un groupe d'ordre $n = p^\alpha q^\beta$ avec $p^\alpha < q + 1$ n'est pas simple (exemples: $n = 20$, 28, 44...)*

(3) *Prouver qu'un groupe d'ordre $n = p^\alpha q^\beta$ lorsque aucun des p^i, $i \leq \alpha$ n'est congru à 1 modulo q, n'est pas simple (exemples: $n = 40$, 45...)*

Exercice 6.1.2. — *Lorsque cette méthode échoue, on peut parfois s'en tirer en dénombrant pour un p premier le nombre d'éléments qui sont dans le p-Sylow et en constatant qu'il reste peu de chose en dehors.*

Prouver qu'un groupe d'ordre $n = 12$, 30, 56 n'est pas simple.

Exercice 6.1.3. — *Si G a n_p sous-groupes de p-Sylow, comme ceux-ci forment une orbite, on a un homomorphisme dont le noyau peut fournir un sous-groupe distingué non trivial, par exemple, si $|G| > n_p!$ ou même si $|G|$ ne divise pas $n_p!$.*

Prouver qu'un groupe d'ordre $n = 12$, 24, 36 et 48 n'est pas simple.

Exercice 6.1.4. — *Montrer qu'un groupe non banal (c'est-à-dire, les groupes d'ordre p, premier) d'ordre $n < 60$ n'est pas simple*

Exercice 6.1.5. — *Soit G un groupe, S un 2-sous-groupe de Sylow. On suppose S cyclique et $|G| > 2$. Montrer que G n'est pas simple. En particulier, si G et simple et G est pair alors $4||G|$. (Idée: on peut faire opérer G sur G par translation et considérer la signature ϵ de la permutation induite sur G par le générateur s de S. On voit que $\epsilon(s) = -1$ d'où un homomorphisme non-trivial dans $\{-1, 1\}$.*

Montrer qu'un groupe d'ordre 90 n'est pas simple. Reprendre l'exercice précédent pour $n \leq 100$, $n \neq 60$.

6.2. Utilisation de Sylow pour montrer qu'un groupe G fini est cyclique. —

Théorème 6.1. — *Soit G un groupe fini et supposons que, pour chaque nombre premiers p divisant le cardinal de G, G ne possède qu'une seul p-sous-groupe de Sylow H_p. Alors G est le produit direct de ses sous-groupes de Sylow.*

Démonstration. — Notons $p_1, \dots, p_r$ les différents nombres premier qui divisent n, le cardinal de G, et pour chaque $1 \leq i \leq r$, H_{p_i} l'unique p_i-sous-groupe de Sylow de G. D'après le corollaire 5.3, $H_{p_i} \lhd G$. Ceci implique, comme dans le lemme 3.1, que l'application :

$$\begin{aligned} \phi : H_{p_1} \times \cdots \times H_{p_r} &\to G \\ (h_1, \dots, h_r) &\mapsto h_1 \dots h_r \end{aligned}$$

est un morphisme de groupes. Son image est égale au sous-gruope $H_{p_1} \dots H_{p_r}$ de G. Comme, pour chaque $1 \leq i \leq r$, H_{p_i} est un sous-groupe de $H_{p_1} \dots H_{p_r}$ on a que le cardinal de H_{p_i} divise le cardinal de $H_{p_1} \dots H_{p_r}$ et, puisque les p_i sont des nombres premiers distincts, on déduit que le cardinal de G divise le cardinal de $H_{p_1} \dots H_{p_r}$. On a donc que ϕ est surjective. Comme le cardinal de $H_{p_1} \times \cdots \times H_{p_r}$ est égal au cardinal de G, on a aussi l'injectivité. □

7. Groupes simples

L'idée ultime de la théorie de groupes finis serait de comprendre tous les groupes finis et, en particulier, pouvoir les classifier. Etant donné un entier n combien de groupes de cardinal n existent ? Quelles sont les tables de multiplications ? Quelles sont les propriétés principales des éléments ?

Etant donné un groupe fini G, on a vu qu'une façon d'attaquer le problème est de trouver un sous-groupe distingué non trivial $H \lhd G$, de considérer les groupes (plus petits) H et G/H et de reconstruire G à partir de H et G/H.

(1) Que se passe-t-il lorsque G est simple ? A-t-on une classification des groupes finis simples ?

(2) Etant données H et K des groupes finis. Combien de groupes G y a-t-il tels que $H \lhd G$ et $G/H \simeq K$?

Le deuxième point s'appelle le *problème d'extension* et aujourd'hui on ne sait pas le résoudre en général. Par contre on dispose d'une réponse à (1) qui, dans de cas particuliers, peux nous aider à résoudre aussi (2). La classification de groupes simples est la suivante :

(1) $\mathbf{Z}/p\mathbf{Z}$ avec p premier.
(2) A_n avec $n \geq 5$.
(3) Certaines familles des groupes *géométriques*.
(4) 26 groupes *sporadiques*.

Le groupe de la quatrième catégorie de plus grand ordre a cardinal 808017424794512875886 459904961710757005754368000000000. Il est appelé le *monstre*. C'est l'un des mystères de la théorie de groupes : on a une définition "*naturelle*" et simple de *groupe* mais on tombe sur un nombre si "*concret*" !

Le but de cette section est d'attaquer le point (2) de cette classification a savoir :

Théorème 7.1. — *Le groupe alterné A_n est simple si $n \neq 4$.*

Remarque 7.2. — Pourquoi veut-on résoudre ce problème ? D'un côté il a une importance historique et son lien avec la théorie de Galois (qu'on ne verra pas dans ce cours) et l'impossibilité de résoudre une équation de cinquième degré par radicaux.

D'un autre côté on va utiliser le cas de A_n comme excuse, et exemple préféré, pour un problème plus ambitieux, et en quelque sorte réciproque du problème de la section précédente. Comment fait-on pour montrer qu'un groupe G est simple ? Comme les stoïciens, on voudrait se munir d'une *paraskeuê*, c'est-à-dire, d'un ensemble des techniques acquises et à notre disposition qu'on pourra utiliser pour résoudre des problèmes concrets, par exemple lors de l'examen...

Comment faire en général pour prouver qu'un groupe G est simple ? L'idée est la suivante : on suppose qu'il existe $H \lhd G$ tel que $H \neq \{e_G\}$ et on va montrer que $H = G$, le but étant alors de montrer que H est très grand (si grand que G...). Pour cela on utilisera les quatre remarques suivantes :

(1) Si $h \in H$ alors $\langle h \rangle \subset H$.
(2) Si $h \in H$ alors, pour tout $g \in G$, $ghg^{-1} \in H$, c'est-à-dire, tous les conjugués de h sont dans H (il faut donc étudier les classes de conjugaison des éléments de G).
(3) Si $h \in H$, alors, pour tout $g \in G$, $h' = ghg^{-1}h^{-1} \in H$ et la classe de conjugaison de h' est, en général, différente de celle de h.
(4) Supposons qu'un p-sous-groupe de Sylow P de G soit inclus dans H. Alors, pour tout $g \in G$, $gPg^{-1} \subset H$. Tous les p-sous-groupes de Sylow de G sont donc inclus dans H.

7.1. Les groupes alternés A_2, A_3 et A_4.— Le groupe A_n, quand $n \leq 4$, a déjà été traité en TD. On sait que $A_2 = \{Id\}$, $A_3 \simeq \mathbf{Z}/3\mathbf{Z}$ et A_4 a 12 éléments et contient un

sous-groupe distingué, isomorphe au groupe de Klein, et dont ses éléments sont l'identité et les trois bi-transpositions.

7.2. Le groupe $A_n, n \geq 5$. — Pour montrer la simplicité de A_n, pour $n \geq 5$, nous devons étudier, dans un premier temps, les classes de conjugaison dans A_n. Je vous rappelle que les classes de conjugaison dans S_n ont été étudiées dans l'exercice 2.2.1 : deux premutations σ et σ' de $\mathcal{S}_n$ sont conjuguées (c'est-à-dire, il existe $\tau \in \mathcal{S}_n$ tel que $\sigma' = \tau\sigma\tau^{-1}$) si et seulement si, on peut écrire $\sigma = c_1 \dots c_t$ et $\sigma' = c_1 \dots c_t$ où les cycles c_i d'une part et c_i' de l'autre sont deux à deux à support disjoint et $\mathrm{ord}(c_i) = \mathrm{ord}(c_i')$ pour tout $1 \leq i \leq t$ (on dit que σ et σ' ont le même type).

La question est alors : supposons que σ et σ' sont dans A_n et qu'elles ont le même type, est-ce qu'on peut choisir $\tau \in \mathrm{A}_n$ (et non seulement dans $\mathcal{S}_n$) tel que $\sigma' = \tau\sigma\tau^{-1}$? Est-ce que l'orbite de σ sous l'action de A_n et la même que sous l'action de $\mathcal{S}_n$?

Notons $o_{A_n}(\sigma)$ (resp. $o_{\mathcal{S}_n}(\sigma)$) l'orbite de σ sous l'action de A_n (resp. S_n) et $\mathrm{St}_{A_n}(\sigma)$ (resp. $\mathrm{St}_{\mathcal{S}_n}(\sigma)$) le stabilisateur σ sous l'action de A_n (resp. $\mathcal{S}_n$). On a clairement $\mathrm{St}_{A_n}(\sigma) = \mathrm{St}_{\mathcal{S}_n}(\sigma) \cap A_n$ et $o_{A_n}(\sigma) \subset o_{\mathcal{S}_n}(\sigma)$. On voudrait savoir quand ces deux orbites sont égales :

Lemme 7.3. — (1) *On a $o_{A_n}(\sigma) = o_{\mathcal{S}_n}(\sigma)$ si, et seulement si, $\mathrm{St}_{\mathcal{S}_n}(\sigma) \not\subset A_n$.*

(2) *Si $\mathrm{St}_{\mathcal{S}_n}(\sigma) \subset A_n$, alors $o_{\mathcal{S}_n}(\sigma)$ est l'union disjointe de deux orbites sous l'action de A_n.*

Démonstration. — Puisque $\mathrm{St}_{A_n}(\sigma) = \mathrm{St}_{\mathcal{S}_n}(\sigma) \cap A_n$, on a que $\mathrm{St}_{A_n}(\sigma)$ est le noyau de la restriction de la signature au groupe $\mathrm{St}_{\mathcal{S}_n}(\sigma)$, c'est-à-dire, $\mathrm{St}_{A_n}(\sigma) = \ker(\varepsilon)$ avec :

$$\varepsilon : \mathrm{St}_{\mathcal{S}_n}(\sigma) \to \{\pm 1\}.$$

Si ε est surjectif alors, $\mathrm{St}_{A_n}(\sigma) = \ker(\varepsilon)$ est un sous-groupe d'indice 2 de $\mathrm{St}_{\mathcal{S}_n}(\sigma)$, et donc, d'un côté $\mathrm{St}_{\mathcal{S}_n}(\sigma) \not\subset A_n$, et de l'autre, par l'équation (4.3), on a :

$$|o_{A_n}(\sigma)| = \frac{|A_n|}{|\mathrm{St}_{A_n}(\sigma)|} = \frac{|\mathcal{S}_n|}{|\mathrm{St}_{\mathcal{S}_n}(\sigma)|} = |o_{\mathcal{S}_n}(\sigma)|,$$

et comme l'un est inclus dans l'autre, on a l'égalité.

Si ε est trivial, alors $\mathrm{St}_{A_n}(\sigma) = \ker(\varepsilon)$ est égal à $\mathrm{St}_{\mathcal{S}_n}(\sigma)$, et donc, d'un côté $\mathrm{St}_{\mathcal{S}_n}(\sigma) \subset A_n$, et de l'autre, par l'équation (4.3), on a :

$$|o_{A_n}(\sigma)| = \frac{|A_n|}{|\mathrm{St}_{A_n}(\sigma)|} = \frac{|\mathcal{S}_n|}{2|\mathrm{St}_{\mathcal{S}_n}(\sigma)|} = \frac{1}{2}|o_{\mathcal{S}_n}(\sigma)|.$$

Comme A_n agit sur $o_{\mathcal{S}_n}(\sigma)$ on trouve que $o_{\mathcal{S}_n}(\sigma)$ est l'union disjointe de deux orbites sous l'action de A_n.

□

Exemple 7.4. — Traitons le cas de A_5. Dans A_5 on dispose de l'identité, de 15 bi-transpositions, de 20 3-cycles et de 24 5-cycles.

(1) Comme $(4\,5) \in \mathrm{St}((1\,2\,3))$, et $(4\,5) \notin A_5$ on a que tous les 3-cycles sont conjugués (en fait ceci preuve que tous les 3-cycles sont conjugués dans A_n si $n \geq 5$.)

(2) Comme $(1\,2) \in \mathrm{St}((1\,2)(3\,4))$, et $(1\,2) \notin A_5$ on a que toutes les bi-transpositions sont conjuguées.

(3) Les 5-cycles ne peuvent pas être tous conjuguées car leur nombre 24 ne divise pas 60, l'ordre de A_5.

Montrons que A_5 est simple. Soit $H \subset A_5$ un sous-groupe non réduit à l'identité. Si H contient un 3-cycle alors, il contient les 20 3-cycles. Si H contient une bi-transposition alors, il contient les 15 bi-transpositions. Si H contient un 5-cycles, alors il contient le sous-groupe engendré par celui-ci, c'est-à-dire, il contient un 5-sous-groupe de Sylow; il contient donc tous les 5-sous-groupes de Sylow et, a fortiori, il contient les 24 5-cylces.

Or H ne peut pas contenir l'identité et un seul des types d'éléments précédents. En effet, 60 n'est pas divisible par $15+1$, par $20+1$ ni par $24+1$. Il doit donc contenir au moins deux de trois types, c'est-à-dire, au moins, $1+15+20 = 36$ éléments. Par le théorème de Lagrange, on déduit que $H = A_5$ et donc A_5 est simple.

Traitons le cas général.

Lemme 7.5. — *Si $n \geq 5$, les 3-cylces engendrent A_n.*

Démonstration. — Tout élément de A_n s'écrit comme produit d'un nombre pair de transpositions. Il suffit de prouver alors que le produit de deux transpositions est un produit de 3-cycles. En effet :

$$\begin{aligned}(a\,b)(b\,c) =& (a\,b\,c)\\ (a\,b)(c\,d) =& (a\,c\,b)(a\,c\,d).\end{aligned}$$

□

Pour démontrer le théorème, il suffira donc de prendre $H \subset A_5$ un sous-groupe non réduit à l'identité et de montrer ensuite que tous les 3-cycles sont dans H. Or, comme tous les 3-cycles sont conjugués, il suffira de montrer que H contient *un* 3-cycle. Et pour cela, on va se ramener au cas où $n = 5$.

Soit σ un élément non trivial de H. On a vu que, pour tout $\tau \in A_n$, le commutateur $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$ est un élément de H. On peut regarder ρ comme le produit $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$, c'est-à-dire, comme le produit de deux éléments du type de τ. Si on prend τ de support petit, on aura que le support de ρ est aussi petit. On choisira donc pour τ un 3-cycle : si on fait le bon choix le support de ρ aura au plus 5 éléments.

Soit $a \in \mathrm{supp}(\sigma)$ et notons $b = \sigma(a)$. On choisit $c \in \{1, \ldots, n\}$ tel que $c \notin \{a, b, \sigma(b)\}$ et on note $\tau = (a\,c\,b)$ de sorte que $\tau^{-1} = (a\,b\,c)$. Alors $\rho = \tau(\sigma\tau^{-1}\sigma^{-1}) = (a\,c\,b)(\sigma(a)\,\sigma(b)\,\sigma(c))$ et l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ contient au plus 5 éléments car $\sigma(a) = b$. On a $\rho(F) = F$ et $\mathrm{supp}(\rho) \subset F$ et, quitte à rajouter des éléments à F on peut supposer que F a cinq éléments. De plus $\rho \neq Id$ car $\rho(b) = \tau(\sigma(b)) \neq b$ puisque $\tau^{-1}(b) = c \neq \sigma(b)$.

Soit maintenant $A(F)$ l'ensemble des permutations paires de F. On a que $A(F)$ est isomorphe à A_5. On voit $A(F)$ inclus dans A_n par le morphisme de groupes injectif :

$$\begin{aligned} A(F) &\hookrightarrow A_n \\ u &\mapsto \overline{u}, \end{aligned}$$

où $\overline{u}$ coïncide avec u sur F et avec l'identité ailleurs. Notons enfin $H_0 = \{u \in A(F) : \overline{u} \in H\}$. Il est clair que H_0 est un sous-groupe non trivial distingué dans $A(F)$ donc d'après le cas $n = 5$, H_0 contient un 3-cycle c. Alors $\overline{c} \in H$ ce qui achève la preuve du théorème.

8. Produit semi-direct

Soient G un groupe et H et K deux sous-groupes de G tels que :

(1) $H \cap K = \{e_G\}$.
(2) $HK = G$.

On a vu que, sous ces hypothèses, l'application l'application :

$$\begin{aligned} f : H \times K &\to G \\ (h, k) &\mapsto hk \end{aligned}$$

est bijective, c'est-à-dire, tout élément de G s'écrit de façon unique sous la forme $g = hk$. Quel est le produit de $g_1 = h_1k_1$ et $g_2 = h_2k_2$? Ce produit vaut

$$h_1k_1h_2k_2, \tag{8.1}$$

mais quelle est sa décomposition en produit d'un élément de H fois un élément de K ?

On a vu que, si H et K sont distingués dans G, alors les éléments de H commutent aux éléments de G, et donc le produit (8.1) vaut $(h_1h_2)(k_1k_2)$.

Dans cette section, on va traiter le cas où seulement l'un des sous-groupes, disons H, est distingué dans G. En, effet, dans ce cas, on a $h_1k_1h_2k_2 = [h_1(k_1h_2k_1^{-1})](k_1k_2)$ et, par hypothèse $h_1(k_1h_2k_1^{-1}) \in H$ et $k_1k_2 \in K$.

Théorème 8.1. — *Soient G un groupe et H et K deux sous-groupes de G tels que :*

- $H \cap K = \{e_G\}$.
- $HK = G$.
- $H \lhd G$.

Alors :

(1) *Pour tous $h_1, h_2 \in H$ et $k_1, k_2 \in K$, on a :*

$$h_1k_1h_2k_2 = [h_1(k_1h_2k_1^{-1})](k_1k_2) \in HK.$$

(2) *L'application*

$$\begin{aligned} i : K &\to \mathrm{Aut}(H) \\ k &\mapsto i_k, \end{aligned} \tag{8.2}$$

où $i_k(h) = khk^{-1}$ est un homomorphisme de groupes.

(3) *La loi de composition* $(h_1, k_1) \rtimes (h_2, k_2) = (h_1 i_{k_1}(h_2), k_1 k_2)$ *donne à l'ensemble produit* $H \times K$ *une structure de groupe, noté* $H \rtimes K$.

(4) *L'application :*

$$\begin{aligned} f : H \rtimes K &\to G \\ (h, k) &\mapsto hk \end{aligned}$$

est un isomorphisme de groupes.

Démonstration. — On a déjà montré (1). On vérifie (2) de façon élémentaire (exercice). Montrons (3). Il est clair que (e_G, e_G) est l'élément neutre de $H \rtimes K$. Montrons l'associativité :

$$\begin{aligned} [(h_1, k_1) \rtimes (h_2, k_2)] \rtimes (h_3, k_3) &= (h_1 i_{k_1}(h_2), k_1 k_2) \rtimes (h_3, k_3) \\ &= (h_1 i_{k_1}(h_2) i_{k_1 k_2}(h_3), (k_1 k_2) k_3) \\ &= (h_1 i_{k_1}(h_2 i_{k_2}(h_3)), k_1 (k_2 k_3)) \\ &= (h_1, k_1) \rtimes (h_2 i_{k_2}(h_3), k_2 k_3) \\ &= (h_1, k_1) \rtimes [(h_2, k_2) \rtimes (h_3, k_3)]. \end{aligned}$$

L'inverse de (h, k) est $(k^{-1}h^{-1}k, k^{-1})$ comme on peut le vérifier.

Pour montrer (4), on vient de voir que la application f est un morphisme et il est clair qu'elle est bijective.

□

Réciproquement, soient H et K deux groupes et supposons qu'on dispose d'un morphisme de groupes $\phi : K \to \mathrm{Aut}(H)$. Notons $H \underset{\phi}{\rtimes} K$ le groupe défini par :

- $H \times K$ en tant qu'ensemble.
- $(h_1, k_1) \underset{\phi}{\rtimes} (h_2, k_2) = (h_1 \phi(k_1)(h_2), k_1 k_2)$.

Alors $H \underset{\phi}{\rtimes} K$ est un groupe tel que :

(1) $H \times \{e_K\} \lhd H \underset{\phi}{\rtimes} K$.

(2) $\{e_H\} \times K < H \underset{\phi}{\rtimes} K$.

Démonstration. — La preuve du fait que $H \underset{\phi}{\rtimes} K$ est un groupe se fait de la même façon que dans le théorème précédent. Il est clair que $H \times \{e_K\}$ et $\{e_H\} \times K$ sont des sous-groupes de $H \underset{\phi}{\rtimes} K$. Pour montrer que $H \times \{e_K\}$ est distingué on remarque qu'il est le noyau du morphisme :

$$\begin{aligned} i : H \underset{\phi}{\rtimes} K &\to K \\ (h, k) &\mapsto k. \end{aligned}$$

□

Remarque 8.2. — Si le morphisme ϕ n'est pas trivial alors, $H \underset{\phi}{\rtimes} K$ n'est pas commutatif. En effet, soit $(h,k) \in H \times K$ tels que $\phi(k)(h) \neq h$. Alors :

$$(e_H, k) \rtimes (h, e_K) = (\phi(k)(h), k) \neq (h,k) = (h, e_K)(e_H, k)$$

Le produit semi-direct est direct si, et seulement si, ϕ est le morphisme trivial.

Corollaire 8.3. — *Soient G un groupe et H et K deux sous-groupes de G tels que :*

- $H \cap K = \{e_G\}$.
- $HK = G$.
- $H \lhd G$.

Alors G est isomorphe à $H \underset{i}{\rtimes} K$ où i est le morphisme défini en (8.2).

8.1. Exemples. —

(1) Le groupe symétrique $\mathcal{S}_3$ est isomorphe à $A_3 \rtimes \{Id, (1\,2)\}$.

(2) Plus généralement, le groupe symétrique $\mathcal{S}_n$ est isomorphe à $A_n \rtimes \{Id, (1\,2)\}$.

(3) Soit D_n le groupe diédral, c'est-à-dire, le groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. Il est formé des n rotations d'angle $2\pi k/n$, avec $0 \leq k \leq n-1$ (de centre le centre du polygone) et n symétries passant par le centre et les sommets ou les centres des côtes du polygone. Le sous-groupe des rotations est un sous-groupe cyclique distingué (pourquoi ?) d'ordre n de D_n et donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Soit T une symétrie et K le sous-groupe d'ordre 2 engendré par elle. On a donc :

$$D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}.$$

(4) H_8 le groupe de quaternions n'est pas un produit semi-direct. En effet, les seuls sous-groupes de H_8 sont ceux engendrés pas i, j, k, 1 ou -1 et ces sous-groupes ne satisfont pas aux conditions de notre corollaire.

(5) De même $\mathbf{Z}/8\mathbf{Z}$ n'est pas un produit semi-direct. En effet, s'il était un produit semi-direct non trivial alors, d'après la remarque il ne serait pas commutatif. Il est donc un produit direct de deux groupes (commutatifs) : ceci contredit notre classification de groupes commutatifs !

Exercice 8.1.1. — *Montrer que les groupes de cardinal 8 sont isomorphes à $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, H_8 ou D_4.*

8.2. Groupes d'ordre pq.— Soient p, q deux nombres premiers et G un groupe d'ordre pq. On connaît les groupes d'ordre pq si $p = q$ (*cf.* corollaire 4.17). On suppose ici que $p < q$. Notons respectivement n_p et n_q le nombre des p-sous-groupes de Sylow et de q-sous-groupes de Sylow. Alors, comme $p < q$, on a $n_q = 1$, $n_p \equiv 1 \mod p$ et $n_p = 1, q$. On a deux cas :

(1) Si $q \not\equiv 1 \mod p$ alors $n_p = 1$ et donc, d'après le théorème 6.1, $G \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \simeq \mathbf{Z}/pq\mathbf{Z}$.

(2) Si $q \equiv 1 \mod p$ alors $n_p = 1$ ou $n_p = q$.

(a) Si $n_p = 1$, d'après le théorème 6.1, $G \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \simeq \mathbf{Z}/pq\mathbf{Z}$.

(b) Si $n_p = q$, notons $H_p \simeq \mathbf{Z}/p\mathbf{Z}$ l'un de ses p-sous-groupes de Sylow. Alors, d'après le corollaire :

$$G \simeq \mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}.$$

Le produit semi-direct est déterminé par un morphisme :

$$\phi = \mathbf{Z}/p\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$$

et ce morphisme est déterminé à son tour par l'image de $\overline{1}$ (pourquoi ?). L'ordre de $\phi(\overline{1})$ divise p : il vaut donc 1 ou p. Si $\phi(\overline{1}) = \overline{1}$, alors ϕ est le morphisme trivial et donc le produit est direct. Supposons donc que $\phi(\overline{1}) = g$ où g est un élément d'ordre p de $\mathbf{Z}/(q-1)\mathbf{Z}$. Si :

$$\phi' = \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/(q-1)\mathbf{Z}$$

est un autre morphisme de groupes non trivial, alors $\phi(\overline{1}) = g'$ où g' est un autre élément d'ordre p de $\mathbf{Z}/(q-1)\mathbf{Z}$ et donc de la forme rg avec r un entier premier à p (pourquoi ?). On a un diagramme commutatif :

$$\begin{array}{ccc} \mathbf{Z}/p\mathbf{Z} & \xrightarrow{\phi'} & \mathbf{Z}/(q-1)\mathbf{Z} \\ \downarrow{\scriptstyle \alpha} & \nearrow{\scriptstyle \phi} & \\ \mathbf{Z}/p\mathbf{Z} & & \end{array}$$

où $\alpha(x) = rx$ pour tout $x \in \mathbf{Z}/p\mathbf{Z}$. Alors l'application :

$$\begin{array}{rcl} \Psi : \mathbf{Z}/q\mathbf{Z} \underset{\phi'}{\rtimes} \mathbf{Z}/p\mathbf{Z} & \to & \mathbf{Z}/q\mathbf{Z} \underset{\phi}{\rtimes} \mathbf{Z}/p\mathbf{Z} \\ (x, y) & \mapsto & (x, \alpha(y)) \end{array}$$

est un isomorphisme. En effet, il est clair que c'est une bijection (pourquoi ?); montrons que c'est un morphisme de groupes :

$$\begin{array}{rcl} \Phi[(x,y) \underset{\phi'}{\rtimes} (x',y')] & = & \Phi[(x\phi'(y)(x'), yy')] \\ & = & (x\phi'(y)(x'), \alpha(yy')) \\ & = & (x\phi(\alpha(y))(x'), \alpha(y)\alpha(y')) \\ & = & (x, \alpha(y)) \underset{\phi}{\rtimes} (x', \alpha(y')) \\ & = & \Phi[(x,y)] \underset{\phi}{\rtimes} \Phi[(x',y')]. \end{array}$$

On a donc que dans le cas où $q \equiv 1 \mod p$, il y a exactement deux groupes d'ordre pq, l'un cyclique et l'autre non commutatif. Par exemple, il y a deux groupes de cardinal 6 : $\mathbf{Z}/6\mathbf{Z}$ et $\mathcal{S}_3$.

Alberto Mínguez, Institut de Mathématiques de Jussieu, Université Paris 6. 4, place Jussieu. 75005, Paris, France. URL: http://www.math.jussieu.fr/∼minguez/
E-mail : minguez@math.jussieu.fr