UNIVERSITÉ DE RENNES 1

INSTITUT MATHÉMATIQUE DE RENNES

Licence de mathématiques

ALGÈBRE 2

et applications géométriques

Cours rédigé par Laurent Moret-Bailly
Dernières corrections : avril 2000

1. Groupes : définition, premières propriétés, exemples

Définition 1.1 *Un* groupe *est un couple $(G,*)$ où G est un ensemble et $*$ une loi de composition interne sur G, vérifiant les propriétés suivantes :*

(i) $*$ *est* associative *: pour tous $g,g',g''\in G$ on a $(g*g')*g''=g*(g'*g'')$.*

(ii) $*$ *admet un* élément neutre *: il existe $e\in G$ tel que pour tout $g\in G$ on ait $g*e=e*g=g$.*

(iii) *tout élément g de G admet un* symétrique *pour la loi $*$, c'est-à-dire qu'il existe $g'\in G$ tel que $g*g'=g'*g=e$ (l'élément neutre).*

Le groupe G est dit commutatif, *ou encore* abélien, *si de plus la loi $*$ est commutative, i.e. $g*g'=g'*g$ pour tous $g,g'\in G$.*

1.2. *Commentaires.*

1.2.1. Êtes-vous sûr de savoir ce que l'on entend par « couple », « ensemble », « loi de composition » ? Voilà une bonne occasion de vous rafraîchir la mémoire...

1.2.2. G est appelé *l'ensemble sous-jacent* au groupe. En pratique, on confond souvent (en particulier dans les notations) le groupe avec son ensemble sous-jacent, de sorte qu'on parle, par exemple, des « éléments d'un groupe G » plutôt que des éléments de l'ensemble G sous-jacent au groupe $(G,*)$. Il s'agit d'un abus de langage sans gravité s'il n'y a pas d'ambiguïté sur la loi de composition. (Cet abus a d'ailleurs été commis dans la définition : à quel endroit ? [S 1])

Par exemple, on dit qu'un groupe est *fini* si son ensemble sous-jacent est fini ; le nombre d'éléments (ou cardinal) de cet ensemble est alors appelé *l'ordre* du groupe. Noter au passage que cet ordre n'est pas nul car un groupe n'est *jamais vide* : il a au moins un élément, à savoir l'élément neutre.

1.2.3. L'élément neutre de G est unique : en effet si e et e' sont deux éléments neutres, on a $e*e'=e$ puisque e' est neutre, et $e*e'=e'$ puisque e est neutre, d'où $e=e'$. Ceci justifie la formulation adoptée dans (iii) : en toute rigueur, il aurait fallu écrire par exemple « ...tel que $g*g'$ et $g'*g$ soient neutres ».

1.2.4. De même le symétrique g' de $g\in G$ est unique : si g'' est un autre symétrique de g, on a $g'=g'*e=g'*(g*g'')=(g'*g)*g''=e*g''=g''$. À cause de cette propriété d'unicité (qui utilise l'associativité, contrairement à la précédente), il est légitime de parler *du* symétrique de g et de le désigner par une notation telle que g^{-1} (voir ci-dessous). Quel est le symétrique de l'élément neutre ? celui de g^{-1} ? celui de $g*g'$? [S 2] (Remarque sur ces questions et toutes les autres : il ne suffit pas de deviner la réponse, il faut la justifier).

1.2.5. La notation la plus courante pour une loi de groupe est la juxtaposition (ou notation multiplicative) : le composé de deux éléments g et g' est simplement noté gg'. Dans ce cas, on convient généralement de noter g^{-1} le symétrique de g, et de l'appeler son « inverse ». Éviter la notation $1/g$.

Sauf mention expresse, ou évidence, du contraire, tous les groupes considérés ici seront notés multiplicativement, et l'élément neutre d'un groupe G sera noté e_G, ou simplement e si aucune confusion n'en résulte.

1.2.6. Une autre notation souvent utilisée, mais *uniquement pour les groupes commutatifs*, est la notation additive : la loi de groupe est notée $+$, le symétrique de g est appelé son opposé et noté $-g$, et l'élément neutre est noté 0.

1.2.7. *Exercice.* [S 3] Il n'est nullement interdit, pour une loi de composition interne sur un ensemble E, de la noter comme n'importe quelle application, c'est-à-dire par exemple $(x, y) \mapsto m(x, y)$ (au lieu d'une notation telle que $(x, y) \mapsto x * y$). Formuler alors les axiomes de groupe en utilisant cette notation (par exemple, la commutativité s'écrit $m(x, y) = m(y, x)$). Expliquer ensuite le peu de succès d'une telle notation.

1.3. *Règles de calcul dans les groupes.* Soit G un groupe, noté multiplicativement ; on notera e l'élément neutre de G.

1.3.1. *Simplification.* Si $a, b, c \in G$ vérifient $ac = bc$ alors $a = b$ (la réciproque étant triviale). En effet $a = ae = a(cc^{-1}) = (ac)c^{-1} = (bc)c^{-1} = b(cc^{-1}) = be = b$. Bien entendu on se contente de résumer ces calculs d'une phrase telle que « multiplions à droite par c^{-1} les deux membres de l'égalité $ac = bc$ ». De même, $ca = cb$ implique $a = b$, « en multipliant à gauche par c^{-1} ». Par contre, une relation telle que $ab = ca$ n'implique pas en général que $b = c$, sauf si l'on sait que a et b *commutent*, c'est-à-dire que $ab = ba$.

1.3.2. Étant donnés a et $b \in G$, l'équation $ax = b$ a une unique solution x dans G, à savoir $x = a^{-1}b$, que l'on trouve en multipliant à gauche par a^{-1}. De même, l'équation $xa = b$ a pour unique solution $x = ba^{-1}$.

1.3.3. On peut reformuler 1.3.2 en disant que, pour tout $a \in G$, l'application $x \mapsto ax$ de G dans G (« translation à gauche par a ») est *bijective*, ainsi que la translation à droite définie par $x \mapsto xa$.

1.3.4. *Opérations « inverses » de la loi de groupe.* Il est important de noter que les deux équations $ax = b$ et $xa = b$ considérées en 1.3.2 sont (à moins que G ne soit commutatif) deux équations différentes, avec des solutions en général différentes. C'est pourquoi, même dans un groupe noté multiplicativement, on ne parle pas de « division » : il y a en effet *deux* « quotients » de b par a, qui sont $a^{-1}b$ et ba^{-1}. Bien entendu, ils coïncident si G est commutatif. En particulier, dans un groupe

noté *additivement* (1.2.6), l'usage permet de définir une soustraction par la formule $a - b = a + (-b) = (-b) + a$.

1.3.5. *Produits finis dans un groupe.* Si $n \in \mathbb{N}$ et si $a_1, \ldots, a_n$ sont n éléments de G, on définit par récurrence sur n leur produit $a_1 \cdots a_n$ comme étant l'élément neutre e si $n = 0$ (suite vide), et $(a_1 \cdots a_{n-1})a_n$ pour $n > 0$. Ainsi $abcd$ est défini comme étant $((ab)c)d$. On déduit alors de l'associativité la formule

$$(a_1 \cdots a_m)(b_1 \cdots b_n) = a_1 \cdots a_m b_1 \cdots b_n \qquad (1.3.5.1)$$

(exercice : récurrence sur n). Cette formule entraîne la règle de calcul suivante : le produit $a_1 \cdots a_n$ peut se calculer par regroupement arbitraire de termes *consécutifs*, par exemple $abcde = (a(bc))(de) = (ab)((cd)e)$. (Exercice : vérifier ces égalités d'abord directement à l'aide des définitions et de l'associativité, puis en utilisant (1.3.5.1)). En particulier, on peut supprimer tout terme égal à l'élément neutre, et toute suite du type aa^{-1}. Par contre, un changement dans l'ordre des termes change la valeur du produit, sauf si G est commutatif ou plus généralement si les termes commutent entre eux.

Un cas particulier important de la règle de regroupement est la formule

$$(ab)(b^{-1}a^{-1}) = e$$

qui donne la réponse à une question posée plus haut (1.2.4) en montrant que *l'inverse de ab est $b^{-1}a^{-1}$* (et non $a^{-1}b^{-1}$).

1.3.6. *Puissances.* Pour $n \in \mathbb{N}$ et $a \in G$, on définit a^n comme le produit $a_1 \cdots a_n$ où chacun des a_i est pris égal à a. On a donc notamment $a^0 = e$ et $a^1 = a$. Pour n entier *négatif*, on pose $a^n = (a^{-1})^{-n}$ (ce qui est compatible avec les notations antérieures pour $n = -1$). On vérifie alors que $a^{m+n} = a^m a^n$ pour m et n quelconques dans $\mathbb{Z}$ (par exemple en discutant suivant les signes, le cas où m et $n \in \mathbb{N}$ résultant de (1.3.5.1)). On a en particulier $a^{-n} = (a^n)^{-1}$, et $a^m a^n = a^n a^m$ (les puissances d'un même élément commutent entre elles). On a aussi $a^{mn} = (a^m)^n$. En revanche on n'a pas en général $(ab)^n = a^n b^n$, sauf si a et b commutent. (Exercice : pour $n = -1$ et pour $n = 2$, la formule $(ab)^n = a^n b^n$ est vraie *si et seulement si* a et b commutent).

Lorsque G est commutatif et noté additivement, on ne parle plus de puissances mais de *multiples* et on note évidemment na et non a^n.

1.4. *Exemples de groupes.*

1.4.1. *Le groupe trivial.* Soit $G = \{x\}$ un ensemble à un élément. Il existe sur G une unique loi de composition, définie (en notation multiplicative) par $xx = x$. Muni de cette loi, G est un groupe commutatif (vérifiez !).

1.4.2. *Les groupes additifs de nombres.* Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des groupes pour l'addition (c'est-à-dire que $(\mathbb{Z}, +)$, etc, sont des groupes). Ils ont 0 pour élément

neutre, et sont commutatifs. Le symétrique d'un nombre x est son opposé, au sens habituel : la notation $-x$ n'introduit donc pas de confusion.

Par contre, $(\mathbb{N},+)$, $(\mathbb{R}_+,+)$, $(\mathbb{R}_+^*,+)$ ne sont pas des groupes : quelle(s) propriété(s) leur manque-t-il ? [S 4]

1.4.3. Si n est un entier naturel, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo n est un groupe pour l'addition des classes. C'est un groupe fini d'ordre n si $n > 0$, et c'est un cas particulier très important de *groupe quotient* (voir plus loin, où la notation $\mathbb{Z}/n\mathbb{Z}$ sera expliquée).

1.4.4. *Les espaces vectoriels.* Si V est un espace vectoriel sur un corps K (par exemple sur $\mathbb{R}$ ou $\mathbb{C}$, revoir le cours d'algèbre linéaire), alors $(V,+)$ est un groupe commutatif : cela fait partie de la définition d'un espace vectoriel.

1.4.5. *Exercice.* [I 1] Dans l'exemple précédent, supposons que K contienne $\mathbb{Q}$ comme sous-corps. Pour $v \in V$ et $n \in \mathbb{Z}$, on a alors deux façons de définir nv : par la structure d'espace vectoriel (multiplication du « vecteur » v par le « scalaire » n), et par la structure de groupe additif de V (multiplication par un entier dans $(V,+)$, au sens de 1.3.6). Montrer que ces deux définitions donnent le même résultat. (Autrement dit, la notation nv n'est pas ambiguë).

1.4.6. *Les groupes multiplicatifs de nombres.* Les ensembles $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$ sont des groupes commutatifs pour la *multiplication* des nombres réels ou complexes.

Par contre, $(\mathbb{N}^*,\times)$, $(\mathbb{Z}^*,\times)$, ne sont pas des groupes : quelle(s) propriété(s) leur manque-t-il ? Est-ce que $(\mathbb{Q}^*,\times)$ est un groupe ? Et $(\mathbb{Z}/n\mathbb{Z},\times)$? (il va de soi qu'il faut éventuellement discuter suivant la valeur de n.) [S 5]

1.4.7. *Groupes de transformations.* Si E est un ensemble, l'ensemble des *bijections* de E sur lui-même est un groupe $\mathfrak{S}(E)$ pour la composition des applications. Il n'est pas commutatif, sauf lorsque E a au plus deux éléments (vérifiez !). Attention donc à la définition de la loi de composition : si f et $g \in \mathfrak{S}(E)$, la composée fg est définie par : $(fg)(x) = f(g(x))$ pour tout $x \in E$ (« d'abord g, puis f »). Quel est l'élément neutre de $\mathfrak{S}(E)$? [S 6]

Lorsque $E = \{1,\ldots,n\}$, où n est un entier naturel, on obtient le *groupe symétrique* $\mathfrak{S}_n$, qui est un groupe fini d'ordre $n!$ (et non d'ordre n, bien que certains auteurs l'appellent « groupe symétrique d'ordre n »).

Lorsque E est muni de structures supplémentaires, on obtient encore un groupe (en fait un sous-groupe de $\mathfrak{S}(E)$, voir 3.1) en considérant le sous-ensemble de $\mathfrak{S}(E)$ formé des bijections f qui « respectent les structures données », en un sens à préciser à chaque fois. Par exemple, si E est un espace vectoriel sur un corps K, l'ensemble des bijections K-linéaires de E sur E (c'est-à-dire des K-*automorphismes* de E) est un groupe pour la composition des automorphismes, noté $\mathrm{GL}(E)$ (groupe linéaire

de E). Si de plus $K = \mathbb{R}$ et si E est muni d'un produit scalaire noté $(v, w) \mapsto \langle v, w\rangle$, l'ensemble des $f \in \mathrm{GL}(E)$ vérifiant $\langle f(v), f(w)\rangle = \langle v, w\rangle$ pour tous $v, w \in E$ est encore un groupe, appelé *groupe orthogonal* de $(E, \langle\ ,\ \rangle)$.

1.4.8. *Groupes de matrices.* Si K est un corps et n un entier naturel, l'ensemble des matrices carrées d'ordre n *inversibles* à coefficients dans K est un groupe pour la multiplication des matrices, noté $\mathrm{GL}(n, K)$. Il est isomorphe (voir 2.4 plus loin) au groupe linéaire $\mathrm{GL}(K^n)$, et n'est pas commutatif sauf si $n \leq 1$.

1.4.9. *Exercice.* [I 2][S 7] Soit K un corps fini à q éléments, et soit $n \in \mathbb{N}$. Monter que $\mathrm{GL}(n, K)$ est un groupe fini et calculer son ordre.

1.4.10. *Exercice : groupes d'éléments inversibles.* [I 3] Soit E un ensemble muni d'une loi interne $*$ associative, admettant un élément neutre. Montrer que le sous-ensemble de E formé des éléments *inversibles*, c'est-à-dire admettant un symétrique pour $*$, est un groupe pour la loi $*$.

Un cas particulier important est celui d'un *anneau unitaire* A, muni de la multiplication. Le groupe des éléments inversibles de A est alors noté $A^\times$. Il est commutatif si A est un anneau commutatif (i.e. si la multiplication de A est commutative).

Exemples : $\mathbb{Z}^\times = \{-1, +1\}$; si K est un corps, $K^\times = K - \{0\}$ (c'est en fait la définition d'un corps), et $\mathrm{M}(n, K)^\times = \mathrm{GL}(n, K)$.

1.4.11. *Produits.* Si G et H sont deux groupes, le produit cartésien $G \times H$ est muni d'une structure de groupe naturelle, en définissant le composé de deux couples (g, h) et (g', h') comme le couple (gg', hh') (« on multiplie composante par composante »). Le groupe obtenu est le *groupe produit* $G \times H$. Cette notion se généralise en celle de produit d'une famille quelconque $(G_i)_{i\in I}$ de groupes : on obtient un groupe noté $\prod_{i\in I} G_i$, dont les éléments sont les familles $(g_i)_{i\in I}$ avec $g_i \in G_i$ pour tout $i \in I$.

1.5. *Exercice.* On appelle *groupe topologique* un groupe G muni d'une topologie (i.e. l'ensemble sous-jacent à G est muni d'une topologie) vérifiant les propriétés suivantes (on note G multiplicativement, comme toujours) :

(i) l'application $(x, y) \mapsto xy$ de $G \times G$ dans G est continue ;

(ii) l'application $x \mapsto x^{-1}$ de G dans G est continue.

Montrer que l'on peut remplacer les deux conditions ci-dessus par « l'application $(x, y) \mapsto xy^{-1}$ de $G \times G$ dans G est continue ».

1.5.1. [I 4] Montrer que les groupes suivants sont des groupes topologiques, pour la topologie donnée :

(i) tout groupe G muni de la topologie discrète (resp. de la topologie grossière) ;

(ii) $(\mathbb{R}^n, +)$, pour la topologie habituelle de $\mathbb{R}^n$;

(iii) $(\mathbb{R}^*, \times)$ (resp. $(\mathbb{C}^*, \times)$) muni de la topologie induite par celle de $\mathbb{R}$ (resp. de $\mathbb{C}$) ;

(iv) $\mathrm{GL}(n, \mathbb{R})$ (resp. $\mathrm{GL}(n, \mathbb{C})$) muni de la topologie induite par celle de $\mathrm{M}(n, \mathbb{R})$ (resp. $\mathrm{M}(n, \mathbb{C})$), identifié à $\mathbb{R}^{n^2}$ (resp. $\mathbb{C}^{n^2}$).

1.5.2. [I 5] Si G est un groupe topologique (noté multiplicativement, d'élément neutre e), montrer que :

(i) pour tout $a \in G$, les translations à droite $(x \mapsto ax)$ et à gauche $(x \mapsto xa)$ sont des homéomorphismes de G sur G ;

(ii) l'application $x \mapsto x^{-1}$ est un homéomorphisme de G sur G ;

(iii) pour que G soit discret il faut et il suffit que e soit un point isolé de G (i.e. que $\{e\}$ soit ouvert dans G) ;

(iv) pour que G soit localement compact il faut et il suffit que e admette un voisinage compact ;

(v) pour que G soit séparé il faut et il suffit que $\{e\}$ soit fermé dans G.

2. Morphismes de groupes

Définition 2.1 *Soient $(G,.)$ et $(H,*)$ deux groupes. Un* homomorphisme *(ou* morphisme*) de groupes de G dans H est une application $f : G \to H$ vérifiant*

$$\forall (x,y) \in G \times G, \quad f(x.y) = f(x) * f(y).$$

On notera $\mathrm{Hom}_{\text{groupes}}(G,H)$ *l'ensemble des morphismes de G dans H.*

2.2. *Commentaires.* (Les groupes sont notés multiplicativement.)

2.2.1. Si $f : G \to H$ est un morphisme, alors f envoie l'élément neutre e_G de G sur l'élément neutre e_H de H : en effet, posant $y = f(e_G)$, on a $yy = f(e_G e_G) = f(e_G) = y$ d'où $y = e_H$ par simplification. De même le lecteur vérifiera que, pour tout $x \in G$, on a $f(x^{-1}) = f(x)^{-1}$, et plus généralement $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$.

2.2.2. Exemples élémentaires de morphismes : si G et H sont deux groupes quelconques, le morphisme « trivial » envoie tout élément de G sur l'élément neutre de H. L'application $\mathrm{id}_G : G \to G$ est évidemment aussi un morphisme. Si $f : G \to H$ et $g : H \to K$ sont deux morphismes, le composé $g \circ f : G \to K$ est un morphisme.

2.2.3. Autres exemples (et contre-exemples) : si G est un groupe et n un entier, l'application $g \mapsto g^n$ de G dans G est un morphisme *si G est commutatif*, mais pas en général : en fait (exercice) pour que $g \mapsto g^2$ soit un morphisme, *il faut et il suffit* que G soit commutatif ; même chose pour $g \mapsto g^{-1}$.

2.2.4. *Exercice.* Plus généralement, si f et g sont deux morphismes de G dans H, alors l'application $fg : G \to H$ définie par $fg(x) = f(x)g(x)$ n'est pas en général un morphisme, mais elle l'est si H est commutatif. Dans ce dernier cas, l'application $(f,g) \mapsto fg$ ainsi définie est une loi de groupe commutatif sur $\mathrm{Hom}_{\text{groupes}}(G,H)$.

Quel est l'inverse d'un morphisme f pour cette loi ? Et en quoi cet exercice généralise-t-il 2.2.3 ? [S 8]

2.2.5. Si V et W sont deux espaces vectoriels sur un corps K et $f : V \to W$ une application K-linéaire, alors f est un morphisme de groupes de $(V,+)$ dans $(W,+)$. Il peut y en avoir d'autres : par exemple, si $K = \mathbb{C}$ et $V = W = \mathbb{C}$, l'application $z \mapsto \overline{z}$ (conjugaison complexe) est un morphisme de groupes (et même une application $\mathbb{R}$-linéaire) mais n'est pas $\mathbb{C}$-linéaire. Par contre :

Exercice : [I 6][S 9] si V et W désignent deux $\mathbb{Q}$-espaces vectoriels, tout morphisme de groupes de $(V,+)$ dans $(W,+)$ est $\mathbb{Q}$-linéaire.

2.2.6. Si G est un groupe et γ un élément de G, l'application $n \mapsto \gamma^n$ est un morphisme de $(\mathbb{Z},+)$ dans G. (Ce sont les seuls, comme nous allons le voir ci-dessous, cf (2.3)).

2.2.7. Un *endomorphisme* d'un groupe G est par définition un morphisme de G dans G. Exercice : montrer que les seuls endomorphismes de $\mathbb{Z}$ sont de la forme $n \mapsto an$, pour $a \in \mathbb{Z}$.

2.2.8. *Projections.* Si G et H sont deux groupes, considérons le produit cartésien $G \times H$ défini en 1.4.11 : on a un morphisme naturel $\mathrm{pr}_1 : G \times H \to G$ appelé « première projection » et envoyant tout couple (g, h) sur g. Bien entendu on a aussi une deuxième projection $\mathrm{pr}_2 : G \times H \to H$; ces morphismes sont surjectifs.

2.2.9. *Exercice* (« propriété universelle du produit »). Dans la situation de 2.2.8, considérons de plus un groupe quelconque Γ. Montrer qu'il revient au même de se donner un morphisme $f : \Gamma \to G \times H$ ou un couple (f_1, f_2) où f_1 (resp. f_2) est un morphisme de Γ dans G (resp. H) : on passe de (f_1, f_2) à f en posant $f(\gamma) = (f_1(\gamma), f_2(\gamma))$, et on passe de f à (f_1, f_2) en posant $f_1 = \mathrm{pr}_1 \circ f$ et $f_2 = \mathrm{pr}_2 \circ f$.

En d'autres termes, on a une bijection naturelle

$$\begin{array}{ccc} \mathrm{Hom}_{\text{groupes}}(\Gamma, G \times H) & \longrightarrow & \mathrm{Hom}_{\text{groupes}}(\Gamma, G) \times \mathrm{Hom}_{\text{groupes}}(\Gamma, H) \\ f & \longmapsto & (\mathrm{pr}_1 \circ f, \mathrm{pr}_2 \circ f). \end{array}$$

2.2.10. Dans la situation de 2.2.8, on a aussi un morphisme de G dans $G \times H$ donné par $g \mapsto (g, e_H)$ et un morphisme de H dans $G \times H$ donné par $h \mapsto (e_G, h)$. Ces morphismes sont injectifs.

2.2.11. *Exercice.* Généraliser 2.2.8, 2.2.9 et 2.2.10 au cas du produit d'une famille quelconque de groupes.

2.2.12. Avez-vous essayé de démontrer toutes les assertions ci-dessus ? Si oui, continuez :

Proposition 2.3 (propriété universelle du groupe $\mathbb{Z}$). *Soit G un groupe.*

(i) *Soit $\varphi : (\mathbb{Z}, +) \to G$ un morphisme. Il existe un unique $\gamma \in G$ tel que $\varphi(n) = \gamma^n$ pour tout $n \in \mathbb{Z}$. De plus γ se déduit de φ par la formule $\gamma = \varphi(1)$.*

(ii) *Réciproquement, soit γ un élément quelconque de G. Il existe un unique morphisme $\varphi_\gamma : \mathbb{Z} \to G$ tel que $\varphi_\gamma(1) = \gamma$; ce morphisme est donné par la formule : $\varphi_\gamma(n) = \gamma^n$ pour tout $n \in \mathbb{Z}$.*

En d'autres termes, on a une bijection naturelle de $\mathrm{Hom}_{\text{groupes}}(\mathbb{Z}, G)$ sur G donnée par $\varphi \mapsto \varphi(1)$, la bijection réciproque associant à un élément γ de G le morphisme $n \mapsto \gamma^n$ de $\mathbb{Z}$ dans G.

Démonstration. (i) Il est clair que

Stop ! Avez-vous fait la démonstration vous-même avant de la lire ci-dessous ? Le cours n'est jamais qu'une suite d'exercices corrigés et commentés. Ceci est valable pour TOUS les énoncés démontrés dans ces notes.

Reprenons. Il est clair que si φ est de la forme $n \mapsto \gamma^n$ pour un $\gamma \in G$, on a en particulier $\varphi(1) = \gamma^1 = \gamma$. Ceci montre l'unicité de γ et la manière de le déduire de φ.

Pour montrer l'existence, il reste à voir que si l'on *définit* $\gamma \in G$ par $\gamma = \varphi(1)$, alors on a bien $\varphi(n) = \gamma^n$ pour tout $n \in \mathbb{Z}$. Or ceci résulte de la propriété plus générale $\varphi(nx) = \varphi(x)^n$, valable pour tout $x \in \mathbb{Z}$ (le groupe de départ) et tout $n \in \mathbb{Z}$ (l'ensemble des entiers), propriété énoncée (et démontrée par le lecteur, n'est-ce pas ?) dans 2.2.1 (remarquez le passage à la notation additive).

(ii) Pour γ donné, l'unicité de φ_γ et la formule $\varphi_\gamma(n) = \gamma^n$ résultent de (i). Pour l'existence, il suffit de vérifier que φ_γ *défini* par cette formule est bien un morphisme de groupes envoyant 1 sur γ, ce qui est immédiat. ∎

2.3.1. *Remarque.* Il résulte immédiatement de 2.3(i) que si A est un *anneau unitaire* et $\varphi : \mathbb{Z} \to A$ un morphisme d'anneaux unitaires, alors φ est donné par $\varphi(n) = n.1_A$ (puisque φ est un morphisme entre les groupes additifs sous-jacents, envoyant 1 sur 1_A). Inversement, on constate immédiatement que l'application $n \mapsto n.1_A$ est bien un morphisme d'anneaux unitaires (compte tenu de 2.3(ii), il suffit de vérifier que φ respecte la multiplication).

On retrouve ainsi la *propriété universelle de l'anneau* $\mathbb{Z}$: pour tout anneau unitaire A, il existe un unique morphisme d'anneaux unitaires de $\mathbb{Z}$ dans A, qui est l'application φ ci-dessus.

Définition 2.4 *Soit $f : G \to H$ un morphisme de groupes. On dit que f est un* isomorphisme *s'il existe un morphisme $g : H \to G$ tel que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_H$.*

Deux groupes G et H sont dits isomorphes *s'il existe un isomorphisme de G sur H.*

Remarques :

2.4.1. Si f est un isomorphisme, il résulte de la définition que l'application f est bijective et que l'application g de l'énoncé est sa bijection réciproque. En particulier, g est unique et est un isomorphisme de H dans G. On aurait donc pu définir un isomorphisme comme un morphisme bijectif dont l'application réciproque est encore un morphisme. Nous allons voir ci-dessous (2.5) que cette dernière restriction est en fait superflue.

2.4.2. Le composé de deux isomorphismes composables est encore un isomorphisme. On voit en particulier que si G est un groupe, l'ensemble $\mathrm{Aut}(G)$ des *automorphismes* de G, c'est-à-dire des isomorphismes de G sur lui-même, est un *groupe* pour la composition des isomorphismes, le symétrique de $f \in \mathrm{Aut}(G)$ pour cette loi de groupe étant l'isomorphisme réciproque de f. Il y a ici un fâcheux conflit de notation : s'il est naturel de noter f^{-1} ce symétrique, il ne faut surtout pas le confondre avec l'application $g \mapsto f(g)^{-1}$ de G dans G, qui d'ailleurs n'est en général pas un mor-

phisme. De même le « carré » de f pour la loi de groupe de $\mathrm{Aut}(G)$ est l'application $g \mapsto f(f(g))$ et non l'application $g \mapsto f(g)^2$.

2.4.3. *Exercice : automorphismes intérieurs.* Si g est un élément d'un groupe G, on lui associe un automorphisme (dit « intérieur ») de G, noté int_g, par la formule

$$\mathrm{int}_g(x) := gxg^{-1}$$

pour tout $x \in G$. On laisse au lecteur le soin de vérifier que int_g est un endomorphisme de G et que $\mathrm{int}_{gh} = \mathrm{int}_g \circ \mathrm{int}_h$: cette formule entraîne que int_g est bien un automorphisme, d'inverse $\mathrm{int}_{g^{-1}}$. Elle montre aussi que l'application $g \mapsto \mathrm{int}_g$ est un morphisme de G dans $\mathrm{Aut}(G)$. Bien entendu ce morphisme est trivial si (et seulement si !) G est commutatif.

2.4.4. L'intérêt de la notion d'isomorphisme est que si G et H sont deux groupes isomorphes, toute propriété de G « exprimable en termes de la structure de groupe » est aussi satisfaite par H. Par exemple :

2.4.5. *Exercice.* [S 10] Parmi les propriétés suivantes, dire lesquelles sont invariantes par isomorphie (c'est-à-dire telles que si G possède la propriété considérée, tout groupe isomorphe à G la possède aussi) :

(i) G est commutatif ;

(ii) G est fini ;

(iii) il existe un élément g de G tel que $g \neq e_G$ et $g^2 = e_G$;

(iv) G est un sous-groupe de $\mathbb{Z}$ (voir plus bas pour la notion de sous-groupe) ;

(v) $G \cap \mathbb{Z} = \emptyset$.

2.4.6. Il est donc très utile, lorsque l'on a à étudier un groupe donné, de savoir qu'il est isomorphe à un groupe déjà connu, ou dont les éléments sont plus faciles à décrire.

Ainsi, si K est un corps et V un K-espace vectoriel de dimension finie n, alors V est isomorphe (comme K-espace vectoriel, donc a fortiori comme groupe additif) à K^n ; de même le groupe $\mathrm{GL}(V)$ (cf. 1.4.7) est isomorphe au groupe de matrices $\mathrm{GL}(n, K)$ de 1.4.8, ce qui facilite souvent l'étude du premier en la réduisant à des manipulations matricielles, et inversement éclaire ces mêmes manipulations en leur donnant un sens « géométrique ».

On observera que dans l'exemple ci-dessus, il n'existe pas en général d'isomorphisme « privilégié » de $(V, +)$ avec $(K^n, +)$ ou de $\mathrm{GL}(V)$ avec $\mathrm{GL}(n, K)$, le choix d'un tel isomorphisme dépendant de celui d'une *base* de V comme K-espace vectoriel.

Proposition 2.5 *Soit $f : G \to H$ un morphisme de groupes. Pour que f soit un isomorphisme, il faut et il suffit que f soit bijectif.*

Démonstration. La nécessité a déjà été vue en 2.4.1. Réciproquement, supposons f bijectif et soit $g : H \to G$ son application réciproque. Par définition de g, on a donc $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_H$ de sorte qu'il reste à voir que g est un morphisme. Soient donc x et $y \in H$: il faut voir que $g(xy) = g(x)g(y)$, or comme f est injective ceci équivaut à $f(g(xy)) = f(g(x)g(y))$. Le premier membre est égal à xy puisque $f \circ g = \mathrm{Id}_H$. Le second, puisque f est un morphisme, est égal à $f(g(x))f(g(y))$, donc à xy à nouveau parce que $f \circ g = \mathrm{Id}_H$. ∎

2.5.1. *Remarque.* En conséquence, nous aurions même pu, comme le font de nombreux auteurs, *définir* un isomorphisme comme un morphisme bijectif. Une telle définition, si elle a l'avantage de la concision, ne dispense pas pour autant de démontrer 2.5 (sous la forme modifiée : « l'application réciproque d'un isomorphisme de groupes est encore un isomorphisme »). Mais elle a surtout l'inconvénient de cacher un fait général : chaque fois que l'on définit une structure (groupe, anneau, espace vectoriel, espace topologique, espace de Banach, ensemble ordonné...) on a une notion correspondante de morphisme (morphisme de groupes, d'anneaux, application linéaire, application continue, application linéaire continue, application croissante...) et aussi une notion d'isomorphisme. *Dans tous les cas*, la « bonne » notion d'isomorphisme est celle de morphisme inversible (en un sens généralement évident), et elle n'est pas toujours équivalente à celle de morphisme bijectif. Exemples : une application continue bijective entre deux espaces topologiques n'est pas toujours un homéomorphisme ; l'inverse d'une application croissante bijective entre deux ensembles ordonnés n'est pas nécessairement croissante. Dans ces deux cas, c'est la notion de morphisme inversible qui est utile : ainsi (exercice), on peut trouver deux espaces topologiques X et Y, et une application continue bijective de X dans Y, tels que Y soit compact (resp. connexe) sans que X le soit ; on peut trouver deux ensembles ordonnés X et Y, et une application croissante bijective de X dans Y, tels que Y soit totalement ordonné sans que X le soit. Par contre les propriétés envisagées dans ces exemples sont bien conservées par isomorphisme.

2.6. *Exercices.*

2.6.1. Soit $G = \{e, x\}$ un groupe d'ordre 2. Il existe un unique isomorphisme de $(\mathbb{Z}/2\mathbb{Z}, +)$ sur G.

2.6.2. [S 11] Soit $G = \{e, x, y\}$ un groupe d'ordre 3 (multiplicatif, d'élément neutre e). Montrer que $y = x^2 = x^{-1}$, que $x = y^2 = y^{-1}$, et qu'il existe *deux* isomorphismes de $(\mathbb{Z}/3\mathbb{Z}, +)$ sur G.

3. Sous-groupes

Définition 3.1 *Soit G un groupe, noté multiplicativement. Un* sous-groupe *de G est un sous-ensemble H de G vérifiant les propriétés suivantes :*

(i) *H est* stable *pour la loi de groupe : pour tous $g, g' \in H$ on a $gg' \in H$.*

(ii) *Muni de la loi interne induite par celle de G d'après* (i)*, H est un groupe.*

3.2. *Remarques* (où H désigne une partie d'un groupe G, noté multiplicativement, d'élément neutre e).

3.2.1. Si H est un sous-groupe de G, alors l'application « d'inclusion » $i : H \to G$ donnée par $i(x) = x$ est un morphisme de groupes, évidemment injectif. En particulier (en vertu de 2.2.1) e est l'élément neutre de H, et l'inverse dans H d'un élément de H est son inverse dans G.

3.2.2. Pour que H soit un sous-groupe de G, il faut et il suffit qu'il vérifie les conditions suivantes :

(i) $e \in H$;

(ii) H est stable par la loi de groupe ;

(iii) pour tout $h \in H$ on a $h^{-1} \in H$.

En effet, ces conditions sont clairement nécessaires d'après 3.2.1. Réciproquement, si elles sont satisfaites, la seule propriété qui reste à vérifier pour H muni de la loi induite est l'associativité ; or celle-ci résulte trivialement de la même propriété dans G.

3.2.3. En fait, on peut encore « condenser » les conditions précédentes : pour que H soit un sous-groupe de G, il faut et il suffit que :

(i) $e \in H$;

(ii) si $g \in H$ et $h \in H$ alors $gh^{-1} \in H$.

En effet, si elles sont vérifiées, en prenant $g = e$ dans (ii) (ce qui est permis d'après (i)) on trouve que la condition (iii) de 3.2.2 est satisfaite. Donc, si g et h sont dans H, alors $h^{-1} \in H$ d'où $gh = g(h^{-1})^{-1} \in H$ d'après (ii), donc H est bien stable, cqfd.

On peut même remplacer la condition (i) par la condition « $H \neq \emptyset$ » : en effet, si H a un élément h_0 et vérifie (ii), alors $e = h_0 h_0^{-1} \in H$. En pratique, cependant, la manière la plus évidente de montrer que H est non vide est de voir qu'il contient l'élément neutre, de sorte que le critère le plus utile est celui que nous venons d'énoncer.

3.3. *Exemples de sous-groupes.*

3.3.1. Si G est un groupe d'élément neutre e, il est clair que $\{e\}$ et G sont des sous-groupes de G.

3.3.2. Si G est un groupe, le groupe $\mathrm{Aut}(G)$ des automorphismes de G (cf. 2.4.2) est un sous-groupe du groupe $\mathfrak{S}(G)$ des permutations de G. Si V est un espace vectoriel sur un corps K, $\mathrm{GL}(V)$ est un sous-groupe de $\mathrm{Aut}(V,+)$ et donc aussi de $\mathfrak{S}(V)$.

3.3.3. Soit $f : G \to H$ un morphisme de groupes.

Si G' est un sous-groupe de G, alors son image $f(G')$ est un sous-groupe de H. (Vérifiez, et profitez-en pour revoir les notions d'image et d'image réciproque d'un sous-ensemble...) Lorsque $G' = G$ on obtient un sous-groupe de H appelé simplement *image de* f et noté $\mathrm{Im}\,(f)$, ou $f(G)$.

Si H' est un sous-groupe de H, son image réciproque $f^{-1}(H')$ est un sous-groupe de G. En particulier, pour $H' = \{e_H\}$ on obtient un sous-groupe de G ne dépendant que de f, appelé *noyau de* f et noté $\mathrm{Ker}\, f$. Ainsi, par définition,

$$\mathrm{Ker}\, f = \{x \in G \mid f(x) = e_H\}.$$

Quels sont l'image et le noyau du morphisme trivial ? de l'identité de G ? du morphisme d'inclusion de 3.2.1 ?

3.3.4. Ce qui précède permet de construire facilement de nombreux exemples de sous-groupes, à partir des exemples de morphismes déjà connus. Ainsi, si G est un groupe *abélien* et n un entier, l'ensemble des $g \in G$ tels que $g^n = e$ est un sous-groupe de G, ainsi que l'ensemble des $g \in G$ de la forme γ^n, pour $\gamma \in G$: ce sont en effet le noyau et l'image de l'endomorphisme $g \mapsto g^n$ de G, cf. 2.2.3.

3.3.5. *Intersections.* Soit $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe G (où I désigne un « ensemble d'indices » quelconque). Alors il est immédiat que l'*intersection* $\bigcap_{i\in I} H_i$ de tous les H_i est un sous-groupe de G, et est le plus grand sous-groupe de G contenu dans chacun des H_i.

C'est l'occasion de « rappeler » que si $I = \emptyset$, l'intersection en question est G. Si l'on a un doute sur ce genre de cas limite, raisonner par contraposée : pour qu'un élément x de G *n'appartienne pas* à $\bigcap_{i\in I} H_i$, il faut et il suffit qu'*il existe* $i \in I$ tel que $x \notin H_i$, condition qui n'est jamais vérifiée si I est vide. (Un bon moyen mnémotechnique est de se dire que plus I est petit, plus l'intersection doit être grande.)

Noter aussi que le cas $I = \emptyset$ est le seul où l'intersection dépende de G : si tous les H_i sont contenus dans un sous-groupe G' de G, l'intersection des H_i vus comme sous-groupes de G' est la même que dans G, *sauf* si I est vide : il faudrait donc en toute rigueur préciser G dans la notation, ce que l'on ne fait pas en pratique : au lecteur de faire attention...

3.3.6. *Exercice.* La réunion d'une famille de sous-groupes n'est pas en général un

sous-groupe. Montrer par exemple que la réunion de *deux* sous-groupes de G n'est un sous-groupe que si l'un des deux est inclus dans l'autre.

(À propos, la réunion d'une famille vide de parties de G est vide : vérifiez sur la définition).

3.3.7. *Exercice.* Soit G un groupe commutatif. Pour tout $n \in \mathbb{Z}$ on pose $G_n = \{g \in G \mid g^n = e_G\}$. Montrer que $\bigcup_{n\in\mathbb{Z}\setminus\{0\}} G_n$ est un sous-groupe de G.

3.3.8. *Centralisateur.* Soit S une partie d'un groupe G. On appelle *centralisateur* de S dans G, et l'on note $Z_G(S)$, l'ensemble des éléments x de G qui commutent avec tous les éléments de S, c'est-à-dire tels que $xs = sx$ pour tout $s \in S$. On voit tout de suite que c'est un sous-groupe de G.

3.3.9. *Exercice.* [S 12] Quel est le centralisateur de l'ensemble vide ? de $\{e\}$? À quelle condition sur S a-t-on la propriété que $S \subset Z_G(S)$? Pouvez-vous trouver une formule donnant le centralisateur d'une réunion ? d'une intersection ? une relation entre $Z_G(S)$ et $Z_G(T)$ lorsque $S \subset T$? une relation entre $Z_G(S)$ et $Z_H(S)$ lorsque S est contenu dans un sous-groupe H de G ?

3.3.10. *Centre.* Le *centre* $C(G)$ d'un groupe G est par définition le centralisateur de G dans G. C'est donc l'ensemble des éléments de G qui commutent avec tout élément de G. C'est un sous-groupe commutatif de G : pourquoi ? À quelle condition sur G a-t-on $C(G) = G$? Si K est un corps et $n \in \mathbb{N}$, quel est le centre de $\mathrm{GL}(n, K)$? (C'est un exercice classique d'algèbre linéaire.)

3.3.11. *Exercice.* [S 13] Quel est le noyau du morphisme de G dans $\mathrm{Aut}(G)$ défini dans 2.4.3 ?

Proposition 3.4 *Soit $f : G \to H$ un morphisme de groupes. Pour que f soit injectif, il faut et il suffit que* $\mathrm{Ker}\, f = \{e_G\}$.

Démonstration. Supposons f injectif. Alors $\mathrm{Ker}\, f = f^{-1}(e_H)$ a au plus un élément (par définition de l'injectivité). Comme il contient de toute façon e_G il est égal à $\{e_G\}$.

Réciproquement, supposons que $\mathrm{Ker}\, f = \{e_G\}$; soient g et h dans G tels que $f(g) = f(h)$, et montrons que $g = h$: on a $f(gh^{-1}) = f(g)f(h)^{-1} = e_H$ d'où $gh^{-1} \in \mathrm{Ker}\, f$ donc $gh^{-1} = e_G$ d'après l'hypothèse, d'où enfin $g = h$. ∎

3.4.1. *Mise en garde.* La proposition 3.4 (déjà connue dans le cas des applications linéaires) est parfois victime de son succès : c'est un critère d'injectivité tellement commode que certains étudiants en viennent à oublier que la condition « $\mathrm{Ker}\, f = \{e_G\}$ » *n'est pas* la définition de l'injectivité, et n'a d'ailleurs de sens que pour un morphisme de groupes. Il n'est pas si rare de lire dans des copies de maîtrise des raisonnements du genre « l'application de $\mathbb{R}$ dans $\mathbb{R}$ définie par $x \mapsto x^2$ a un noyau

trivial (si $x^2 = 0$ alors $x = 0$) donc elle est injective ».

3.5. *Sous-groupe engendré par un élément.* Si γ est un élément fixé d'un groupe G, le morphisme $n \mapsto \gamma^n$ de $(\mathbb{Z}, +)$ dans G (cf. 2.2.6) a pour image un sous-groupe $\langle\gamma\rangle$ de G, qui est l'ensemble des puissances (avec exposants entiers relatifs) de γ. C'est le *sous-groupe engendré par* γ, sur lequel nous reviendrons ; en attendant le lecteur peut déjà vérifier, à titre d'exercice, que $\langle\gamma\rangle$ est un sous-groupe de G qui contient γ, et que c'est le *plus petit* sous-groupe de G ayant cette propriété, en ce sens que tout sous-groupe de G contenant γ contient $\langle\gamma\rangle$. Noter aussi que $\langle\gamma\rangle$ est automatiquement *commutatif*. On pourrait le noter $\gamma^{\mathbb{Z}}$ mais cette notation est peu utilisée ; par contre si G est noté additivement, on rencontre souvent la notation $\mathbb{Z}\gamma$ pour $\langle\gamma\rangle$.

3.5.1. *Exercice.* [S 14] Quel est le sous-groupe engendré par le nombre 1 (resp. 2, resp. -1) dans $(\mathbb{R}, +)$? Et dans $(\mathbb{R}^*, \times)$? Quel est le sous-groupe engendré par i dans $(\mathbb{C}, +)$? Et dans $(\mathbb{C}^*, \times)$?

Dans $\mathbb{Z}$, les sous-groupes de ce type sont en fait les seuls :

Proposition 3.6 *Soit H un sous-groupe de $(\mathbb{Z}, +)$. Il existe un unique entier $n \geq 0$ tel que $H = n\mathbb{Z}$.*

De plus n est caractérisé comme suit : si $H = \{0\}$ on a $n = 0$ et sinon n est le plus petit élément > 0 de H.

Démonstration. Elle a été vue en première année ; rappelons-la :

Unicité. Si m et n sont deux entiers tels que $n\mathbb{Z} = m\mathbb{Z}$, alors en particulier chacun est multiple de l'autre (puisque $n \in m\mathbb{Z}$ et $m \in n\mathbb{Z}$) de sorte que $n = \pm m$ d'où $n = m$ si de plus m et n sont ≥ 0.

Existence. Si $H = \{0\}$ il est clair que $H = 0\mathbb{Z}$. Supposons donc que H a au moins un élément non nul. Comme c'est un sous-groupe de $\mathbb{Z}$ il contient aussi l'opposé de cet élément, et il est donc clair qu'il contient au moins un élément positif. (Bien entendu vous avez fait la démonstration seul avant de lire ceci : avez-vous pensé à cette partie de l'argument ?)

Il existe donc dans H un plus petit élément positif (puisque toute partie non vide de $\mathbb{N}$ a un plus petit élément) ; notons-le n, et montrons que $H = n\mathbb{Z}$. Il est clair que $n\mathbb{Z} \subset H$ puisque $n \in H$ et que H est un sous-groupe. Réciproquement, soit $h \in H$: par division euclidienne, licite puisque $n > 0$ (et ça, vous y aviez pensé ?), il existe des entiers q et r tels que $h = nq + r$ et $0 \leq r < n$. La première relation montre que $r \in H$ puisque $r = h - nq$; la seconde implique alors que $r = 0$, sinon r serait un élément de H, positif et plus petit que n, en contradiction avec le choix de n. On a donc $h = nq \in n\mathbb{Z}$, cqfd. ∎

Proposition 3.7 *Soient m et n deux entiers. Alors :*

(i) $m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{ppcm}\,(m,n)\mathbb{Z}$;

(ii) $m\mathbb{Z} + n\mathbb{Z} = \mathrm{pgcd}\,(m,n)\mathbb{Z}$.

Démonstration. La première assertion équivaut à dire que l'ensemble des multiples communs à m et n coïncide avec l'ensemble des multiples du ppcm de m et n, ce qui n'est autre que la définition de celui-ci.

Montrons la seconde. On sait qu'il existe un entier d tel que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$; montrons que d est le pgcd de m et n. Il est d'abord clair que d divise m (et n, par symétrie) puisque $m \in m\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. Il reste donc à voir que tout diviseur commun à m et n divise d. Or comme $d \in d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$, il existe des entiers u et v tels que $d = mu + nv$ (« identité de Bézout »), et il est bien clair que tout diviseur commun à m et n divise $mu + nv$, cqfd. ∎

3.8. *Ordre d'un élément.* Nous allons maintenant, pour un élément donné γ d'un groupe G, étudier la structure du sous-groupe $\langle\gamma\rangle$ qu'il engendre. Nous allons voir qu'elle est déterminée par un entier (enfin presque) appelé *l'ordre* de γ.

Définition 3.9 *Soit γ un élément d'un groupe G. On dit que γ est* d'ordre infini *si $\langle\gamma\rangle$ est un groupe infini. Sinon, on dit que γ est* d'ordre fini *et son* ordre *est par définition l'ordre (c'est-à-dire le cardinal, cf.* (1.2.2)*) du groupe $\langle\gamma\rangle$.*

3.10. Essayons de cerner un peu mieux le groupe $\langle\gamma\rangle$ (G et γ étant fixés une fois pour toutes dans cette discussion). Par définition, $\langle\gamma\rangle$ est l'image du morphisme $\varphi : \mathbb{Z} \to G$ envoyant k sur γ^k. Distinguons deux cas :

3.10.1. *φ est injectif.* Alors φ est une bijection (donc un isomorphisme, puisque c'est déjà un morphisme) de $\mathbb{Z}$ sur $\langle\gamma\rangle$; ce dernier est donc un groupe infini, et γ est d'ordre infini.

3.10.2. *φ n'est pas injectif.* Alors le noyau H de φ n'est pas nul d'après (3.4), et est donc d'après (3.6) de la forme $n\mathbb{Z}$, pour un unique entier $n > 0$.

Nous allons voir que cet entier n n'est autre que l'ordre de γ. Pour cela, noter que par définition, H est l'ensemble des entiers k tels que $\gamma^k = e$; la proposition (3.6) nous fournit donc deux manières légèrement différentes de caractériser n :

(a) $n > 0$, et pour qu'un entier k vérifie $\gamma^k = e$, il faut et il suffit que n divise k ;

(b) n est le plus petit entier $k > 0$ tel que $\gamma^k = e$.

Nous allons en tirer deux démonstrations (essentiellement équivalentes) de l'assertion « n est l'ordre de γ ». Commençons par la plus terre-à-terre, utilisant (b). Tout élément de $\langle\gamma\rangle$ est de la forme γ^k, pour un entier k ; par division euclidienne, on peut écrire $k = nq + r$ avec q entier et $0 \leq r < n$. Or (b) entraîne que $\gamma^n = e$

d'où $\gamma^k = \gamma^r$. Autrement dit les éléments de $\langle\gamma\rangle$ sont $e, \gamma, \gamma^2, \dots \gamma^{n-1}$. De plus ces éléments sont distincts : si l'on avait $\gamma^a = \gamma^b$ avec $0 \leq a < b < n$, on en déduirait $\gamma^{b-a} = e$ qui contredirait (b). Donc le nombre d'éléments de $\langle\gamma\rangle$ est n, cqfd.

Montrons maintenant la même chose, mais en utilisant (a). La relation $\gamma^n = e$ implique que « γ^k ne change pas si l'on ajoute à k un multiple de n ». En d'autres termes, γ^k *ne dépend que de la classe de* k *modulo* n de sorte que l'on a une application $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \langle\gamma\rangle$ envoyant une classe κ modulo n sur γ^k où k est un élément quelconque de cette classe (le résultat ne dépendant pas du choix de k). Il est clair que cette application est surjective ; elle est aussi injective car si $\gamma^k = \gamma^{k'}$ alors $\gamma^{k-k'} = e$ donc n divise $k - k'$, c'est-à-dire $k \equiv k' \pmod{n}$.

Récapitulons en donnant ci-dessous les caractérisations de l'ordre que nous venons de voir (la première étant la définition adoptée ici) :

Proposition 3.11 *Soit γ un élément d'un groupe G, et soit n un entier > 0. .*

(i) *L'ordre de γ est égal à l'ordre du groupe $\langle\gamma\rangle$.*

(ii) *Pour que γ soit d'ordre infini il faut et il suffit que $\langle\gamma\rangle$ soit isomorphe à $\mathbb{Z}$.*

(iii) *Pour que γ soit d'ordre n il faut et il suffit que $\langle\gamma\rangle$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

(iv) *Si γ est d'ordre n alors $\langle\gamma\rangle = \{e, \gamma, \gamma^2, \dots \gamma^{n-1}\}$, et ces éléments sont deux à deux distincts. De plus $\gamma^n = e$.*

(v) *Si γ est d'ordre n et si k est un entier, alors pour que $\gamma^k = e$ il faut et il suffit que n divise k.* ∎

3.11.1. *Exercice.* [S 15] Si G est un groupe *commutatif*, montrer que l'ensemble des éléments d'ordre fini de G est un sous-groupe de G. Cet exercice a déjà été vu : où ?

Donner un contre-exemple dans le cas non commutatif (penser par exemple aux symétries orthogonales dans $\mathrm{GL}(2, \mathbb{R})$).

3.11.2. *Exercice.* [S 16] Pour tout $n \geq 1$, trouver un élément d'ordre n dans le groupe $\mathrm{GL}(2, \mathbb{R})$.

3.11.3. *Exercice.* [I 7][S 17] Trouver un élément d'ordre 5 dans $\mathrm{GL}(2, \mathbb{Q})$.

3.12. *Exercice.* Soit G un groupe topologique (cf. 1.5). Il pourra être commode de noter $m : G \times G \to G$ la loi de groupe, et $i : G \to G$ l'application $x \mapsto x^{-1}$.

3.12.1. [I 8][S 18] Si H est un sous-groupe de G, montrer que l'adhérence $\overline{H}$ de H dans G est un sous-groupe fermé de G, et que c'est le plus petit sous-groupe fermé de G contenant H.

3.12.2. [I 9][S 19] Montrer qu'il existe un plus grand sous-groupe connexe G^0 de G, qui est la composante connexe de e dans G, et qui est fermé dans G. On l'appelle

la *composante neutre* de G. Si de plus G est localement connexe (tout point de G admet une base de voisinages connexes), alors G^0 est ouvert dans G.

Déterminer G^0 pour : $G = \mathbb{R}^*$; $G = \mathrm{GL}(n, \mathbb{R})$; $G = \mathrm{GL}(n, \mathbb{C})$.

3.12.3. [I 10] Montrer que les sous-groupes fermés de $\mathbb{R}$ sont $\mathbb{R}$, $\{0\}$, et les sous-groupes de la forme $a\mathbb{Z}$ ($a \in \mathbb{R}$).

3.12.4. [S 20] Soit θ un nombre réel *irrationnel.*
(1) [I 11] Montrer que l'ensemble $H = \mathbb{Z} + \mathbb{Z}\theta$ des réels de la forme $a + b\theta$ avec a et $b \in \mathbb{Z}$ (qui est le sous-groupe de $\mathbb{R}$ engendré par $\{1, \theta\}$, cf. 4.4 plus bas) est dense dans $\mathbb{R}$.
(2) En déduire que, pour tout réel $\varepsilon > 0$, il existe des entiers p et q, avec $q \neq 0$, tels que $|\theta - \frac{p}{q}| < \frac{\varepsilon}{q}$.

3.12.5. [I 12] Soit ζ un nombre complexe de module 1. Montrer que, ou bien ζ est d'ordre fini dans $\mathbb{C}^*$ (i.e. est une racine de l'unité), ou bien il existe, pour tout réel $\varepsilon > 0$, un entier n tel que $\zeta^n \neq 1$ et $|\zeta^n - 1| < \varepsilon$.

3.12.6. Retrouver le résultat de 3.12.5 en remarquant que le groupe des nombres complexes de module 1 est compact.

4. Sous-groupe engendré par une partie d'un groupe

Définition 4.1 *Soit S une partie quelconque d'un groupe G. On appelle* sous-groupe de G engendré par S, *et l'on note $\langle S\rangle$, l'intersection de tous les sous-groupes de G contenant S.*

On dit que S engendre G *si $\langle S\rangle = G$.*

Il est clair que $\langle S\rangle$ est un sous-groupe de G, comme intersection d'une famille de sous-groupes (famille d'ailleurs non vide car G en fait partie). Il est clair aussi (j'espère ?) que $S \subset \langle S\rangle$. En fait :

Proposition 4.2 *Avec les notations de la définition* 4.1, *$\langle S\rangle$ est le* plus petit *sous-groupe de G contenant S.*

Rappelons (3.5) que « le plus petit » est à comprendre au sens de l'inclusion : l'énoncé signifie que, d'une part, $\langle S\rangle$ est un sous-groupe de G contenant S (ce que nous avons déjà dit), et d'autre part que tout sous-groupe H de G contenant S contient aussi $\langle S\rangle$. La *démonstration* de cette propriété est triviale : H fait alors partie de la famille des sous-groupes de G contenant S donc contient $\langle S\rangle$ qui est par définition l'intersection de cette famille ! ∎

4.2.1. *Exercice.*[S 21] Quel est le sous-groupe de G engendré par l'ensemble vide ? par $\{e\}$? par un sous-groupe donné de G ? Quel est le sous-groupe de $\mathbb{Z}$ engendré par $\mathbb{N}$?

4.3. *Remarque.* On a avec 4.2 un bon exemple de démonstration complètement « formelle » : elle n'utilise même pas la définition d'un groupe ou d'un sous-groupe, mais seulement le fait que l'intersection d'une famille de sous-groupes est encore un sous-groupe. À ce titre, la proposition ci-dessus a des analogues dans de nombreux contextes dont un exemple, au moins, devrait être connu : c'est celui du sous-espace vectoriel engendré par une partie d'un espace vectoriel, que l'on peut définir comme l'intersection de tous les sous-espaces contenant cette partie. L'analogue de 4.2 est encore vrai, avec la même démonstration.

Cependant, le lecteur, à l'esprit agile, se souvient sans doute d'une autre définition du sous-espace engendré : c'est aussi l'ensemble des *combinaisons linéaires* des éléments de la partie envisagée. Fort heureusement il existe un énoncé analogue ici :

Proposition 4.4 *Avec les notations de la définition* 4.1, *un élément x de G appartient à $\langle S\rangle$ si et seulement si x peut s'écrire comme le produit (au sens de la loi de groupe de G) d'un nombre fini d'éléments de S et d'inverses d'éléments de S ;*

autrement dit, si x peut s'écrire

$$x = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_m^{\varepsilon_m}$$

avec m dans $\mathbb{N}$, les s_i dans S et les ε_i dans $\{-1, +1\}$.

Démonstration. Appelons *mot sur S* tout élément de G de la forme spécifiée dans l'énoncé, et soit M l'ensemble des mots sur S.

Il est clair que M est une partie de G contenant S puisque tout élément de S est de façon évidente un mot sur S (avec $m = 1$).

Montrons que M est un sous-groupe de G : d'abord M contient l'élément neutre, qui correspond au « mot vide » (i.e. au cas $m = 0$, avec la notation de l'énoncé). (Il correspond aussi au mot ss^{-1}, où s est un élément quelconque de S ; cependant cet argument est en défaut si S est vide...) Ensuite il est clair que le produit de deux mots est un mot (il suffit de les « écrire bout à bout ») et que l'inverse d'un mot est un mot (appliquer la formule de l'inverse d'un produit). Donc M est bien un sous-groupe d'après 3.2.2.

Il résulte donc de 4.2 que $\langle S \rangle \subset M$.

Montrons l'inclusion réciproque : $\langle S \rangle$ contient tous les éléments de S, donc aussi leurs inverses puisque $\langle S \rangle$ est un sous-groupe de G, donc aussi, pour la même raison, tous les produits finis de ces gens-là. Autrement dit, $\langle S \rangle$ contient M. ∎

4.4.1. Remarque. On déduit immédiatement de 4.4 le cas particulier suivant : si γ est un élément de G, le sous-groupe engendré par $\{\gamma\}$ n'est autre que le « sous-groupe engendré par γ » déjà rencontré plus haut (3.5).

4.4.2. *Exercice.*[S 22] Montrer que la proposition 4.4 reste valable si à la fin de l'énoncé on remplace « les ε_i dans $\{-1, +1\}$ » par « les ε_i dans $\mathbb{Z}$ ». Reste-t-il valable si l'on remplace $\{-1, +1\}$ par $\mathbb{N}$? par $\{-1, +2\}$? par $\{-17, +10000\}$?

4.4.3. *Exercice.*[S 23] Quel est le sous-groupe de $(\mathbb{R}^*, \times)$ engendré par l'ensemble des nombres premiers ?

4.4.4. *Exercice.*[S 24] Soit $f : G \to H$ un morphisme de groupes, et soit S une partie de G telle que $f(s) = e_H$ pour tout $s \in S$. Montrer que $\langle S \rangle \subset \operatorname{Ker} f$, de deux manières différentes : en utilisant 4.2 et en utilisant 4.4. Que pensez-vous de la réciproque ?

4.4.5. *Exercice.* Généralisation de 4.4.4 : soit $f : G \to H$ un morphisme de groupes, et soit S une partie de G. Montrer que $f(\langle S \rangle) = \langle f(S) \rangle$. Comme dans 4.4.4, on fera la démonstration à l'aide de 4.4 (facile), puis directement à partir de 4.2 (moins évident [S 25]).

4.4.6. *Exercice.* Si S est une partie d'un groupe G, montrer que $Z_G(S) = Z_G(\langle S \rangle)$ (cf. 3.3.8). Si tous les éléments de S commutent entre eux, que peut-on dire du groupe $\langle S \rangle$? Réciproque ?

4.4.7. *Exercice.* Voici un exemple d'application de la notion de sous-groupe engendré. Soient $n \in \mathbb{N}$ et $a_1, \ldots, a_n$ des éléments d'un groupe *commutatif* G, et considérons le produit $p = a_1 \cdots a_n$. On a dit en 1.3.5 que « changer l'ordre des termes ne change pas le produit », ce qui signifie de façon précise que, pour toute permutation $\sigma \in \mathfrak{S}_n$ de $\{1, \ldots, n\}$ (cf. 1.4.7) on a $a_{\sigma(1)} \cdots a_{\sigma(n)} = p$. Notons p_σ le premier membre de cette relation.

Pour $1 \leq i \leq n-1$ notons τ_i la « transposition » échangeant i et $i+1$ et laissant fixes les autres éléments de $\{1, \cdots, n\}$. On verra plus loin (6.7) que le groupe symétrique $\mathfrak{S}_n$ est *engendré* par $\{\tau_1, \cdots, \tau_{n-1}\}$. Admettant ce résultat, il est facile de prouver pour tout $\sigma \in \mathfrak{S}_n$ la formule $p_\sigma = p$: considérer l'ensemble H des σ qui la vérifient, montrer que c'est un sous-groupe de $\mathfrak{S}_n$, et montrer qu'il contient les τ_i en utilisant la règle de regroupement de 1.3.5 et la commutativité de G.

Si l'on ne suppose plus que G est commutatif mais seulement que les a_i commutent entre eux, le résultat est encore valable : on peut reprendre l'argument précédent et constater qu'il marche encore, mais on peut aussi se ramener au cas où G est commutatif : comment ? [S 26]

4.4.8. *Exercice : sous-groupe engendré, cas commutatif.* Soient $n \in \mathbb{N}$ et $a_1, \ldots, a_n$ des éléments d'un groupe commutatif G. Montrer que le sous-groupe de G engendré par $\{a_1, \ldots, a_n\}$ est l'ensemble des éléments de G de la forme $a_1^{k_1} \ldots a_n^{k_n}$ avec $k_1, \ldots, k_n \in \mathbb{Z}$.

4.4.9. *Exercice.*[S 27] On appelle *commutateur* de deux éléments x et y d'un groupe G l'élément $[x, y] := xyx^{-1}y^{-1}$ (de sorte que $[x, y] = e$ si et seulement si x et y commutent). Le sous-groupe de G engendré par tous les commutateurs est appelé (improprement) le *sous-groupe des commutateurs* de G (on dit aussi *sous-groupe dérivé*) et est noté $[G, G]$ (tout aussi improprement, car ce n'est pas en général l'ensemble des commutateurs, ce que suggère pourtant la notation).

(1) Montrer que $[G, G]$ est l'ensemble des produits finis de commutateurs d'éléments de G.

(2) Montrer que pour tout morphisme $f : G \to H$ où H est *commutatif*, on a $[G, G] \subset \mathrm{Ker}\, f$.

(3) [I 13] Réciproquement, que peut-on dire de H si $[G, G] \subset \mathrm{Ker}\, f$?

4.4.10. *Exercice.*[S 28] Si S est une partie d'un groupe G, montrer que $\langle S \rangle = \bigcup_T \langle T \rangle$, où T parcourt l'ensemble des parties finies de S.

5. Groupe opérant sur un ensemble

Définition 5.1 *Soient G un groupe (noté multiplicativement, d'élément neutre e) et E un ensemble.*

Une opération *(ou* action*)* à gauche *de G sur E est une application*

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g * x \end{array}$$

vérifiant les propriétés suivantes :

(i) $\forall x \in E, e * x = x$;

(ii) $\forall (g, g', x) \in G \times G \times E, (gg') * x = g * (g' * x)$.

Une opération *(ou* action*)* à droite *de G sur E est une application*

$$\begin{array}{ccc} E \times G & \longrightarrow & E \\ (x, g) & \longmapsto & x * g \end{array}$$

vérifiant les propriétés suivantes :

(i) $\forall x \in E, x * e = x$;

(ii) $\forall (x, g, g') \in E \times G \times G, x * (gg') = (x * g) * g'$.

5.2. *Remarques.*

5.2.1. *Notations courantes.* Sauf mention du contraire, on notera gx (resp. xg) plutôt que $g * x$ (resp. $x * g$), et « action » signifiera « action à gauche ». Si une confusion est possible (avec la loi de groupe de G notamment) la notation $g.x$ pourra aussi être utilisée.

La propriété 5.1(ii) permet d'omettre les parenthèses dans les formules : on note en général $gg'x$ l'élément $(gg')x = g(g'x)$ de E.

Tout ceci suppose que G est noté multiplicativement, faute de quoi la notation gx est formellement déconseillée !

On dira « soit G un groupe opérant sur un ensemble E » plutôt que « soit $(g, x) \mapsto gx$ une action à gauche de G sur E ».

5.2.2. La distinction entre actions à droite et à gauche n'est pas une simple question de notation. Si G opère à gauche sur E (par $(g, x) \mapsto gx$) et si l'on pose $x * g = gx$ pour $g \in G$ et $x \in E$, alors on a bien défini une application de $E \times G$ dans E mais ce n'est pas pour autant une action à droite ! (exercice).

Par contre (exercice encore) on obtient une action à droite en posant $x * g = g^{-1}x$: cette remarque permet de déduire d'un énoncé sur les actions à gauche l'énoncé symétrique pour les actions à droite.

5.2.3. *G-ensembles et G-morphismes.* Si G est un groupe, on appelle G-ensemble (sous-entendu : à gauche) tout ensemble muni d'une action à gauche de G. Un *morphisme* d'un G-ensemble E vers un G-ensemble F (on dit aussi un G-morphisme de E dans F) est par définition une application $f : E \to F$ qui est *G-équivariante*, c'est-à-dire vérifie $f(gx) = gf(x)$ pour tout $g \in G$ et tout $x \in E$. Un *isomorphisme* de G-ensembles est un morphisme ayant un inverse qui est aussi un morphisme ; en fait il revient au même de dire que c'est un G-morphisme bijectif (exercice).

L'application identité d'un G-ensemble dans lui-même est un G-morphisme ; le composé de deux G-morphismes est un G-morphisme.

5.3. *Exemples.*

5.3.1. *L'action triviale.* Si E est un ensemble quelconque et G un groupe quelconque, on définit une action, dite *triviale*, de G sur E en posant $gx = x$ pour tout $g \in G$ et tout $x \in E$. *Exercice :* montrer que toute action d'un groupe trivial est triviale, ainsi que toute action d'un groupe quelconque sur un ensemble à moins de deux éléments.

5.3.2. Si E est un ensemble quelconque, le groupe $\mathfrak{S}(E)$ (cf. 1.4.7) opère à gauche sur E : pour $\sigma \in \mathfrak{S}(E)$ et $x \in E$ on pose $\sigma x = \sigma(x)$. En d'autres termes, E est de façon naturelle un $\mathfrak{S}(E)$-ensemble.

5.3.3. Si G opère sur E et si $f : G' \to G$ est un morphisme de groupes, alors G' opère aussi sur E par la formule $g'x = f(g')x$. L'action de G' ainsi définie est dite *induite* par l'action de G (sous-entendu : via le morphisme f). Un cas particulier très important est celui où G' est un sous-groupe de G et f le morphisme d'inclusion de G' dans G.

5.3.4. Soient G un groupe, E un ensemble et $f : G \to \mathfrak{S}(E)$ un morphisme. Combinant les deux exemples précédents on obtient une action de G sur E, donnée par $gx = f(g)(x)$.

Inversement, si G opère sur E, on peut associer à tout $g \in G$ une application $f(g)$ de E dans E, définie par $f(g)(x) = gx$ pour $x \in E$; la définition d'une action de groupe implique que $f(e) = \mathrm{Id}_E$ et que $f(gh) = f(g) \circ f(h)$ pour g et $h \in G$. En particulier, pour tout $g \in G$, $f(g) : E \to E$ est *bijective* (d'inverse $f(g^{-1})$) et finalement l'application $g \mapsto f(g)$ ainsi définie est un morphisme de G dans $\mathfrak{S}(E)$.

En résumé, *il revient au même de se donner une action à gauche de G sur E ou un morphisme de groupes de G dans $\mathfrak{S}(E)$.*

5.3.5. *Exercice.* Justifier le « il revient au même » ci-dessus en vérifiant soigneusement que les deux recettes décrites (pour passer d'une action de G sur E à un morphisme de G dans $\mathfrak{S}(E)$, et inversement) sont réciproques l'une de l'autre.

5.3.6. *Actions de $\mathbb{Z}$.* Soit $(n, x) \mapsto n * x$ une action à gauche de $(\mathbb{Z}, +)$ sur E. On

a en particulier une bijection σ de E sur lui-même donnée par $x \mapsto \sigma(x) := 1 * x$, et l'on vérifie sans peine (j'espère) que l'on a $n * x = \sigma^n(x)$ pour tout $n \in \mathbb{Z}$ et tout $x \in E$. Autrement dit, l'action est entièrement déterminée par σ.

Réciproquement, si $\sigma : E \to E$ est une bijection quelconque, on en déduit une action de $\mathbb{Z}$ sur E en posant $n * x = \sigma^n(x)$ pour tout $n \in \mathbb{Z}$ et tout $x \in E$, et la bijection associée à cette action n'est autre que σ. (Où utilise-t-on le fait que σ est une bijection ?)

En résumé (vous avez bien tout vérifié ?), il revient au même de se donner une action de $\mathbb{Z}$ sur E ou une bijection de E sur lui-même.

Tout ceci peut être vu comme un cas particulier de 5.3.4 : une action de $\mathbb{Z}$ est « la même chose » qu'un morphisme de $(\mathbb{Z}, +)$ dans $\mathfrak{S}(E)$, qui à son tour est « la même chose » qu'un élément de $\mathfrak{S}(E)$ d'après la propriété universelle de $\mathbb{Z}$ (2.3).

5.3.7. Si G opère sur E, alors G opère aussi sur $\mathcal{P}(E)$ (l'ensemble des parties de E) par la formule $\sigma A = \sigma(A)$.

Par exemple, prenons $E = \{1, \ldots, n\}$ et $G = \mathfrak{S}(E) = \mathfrak{S}_n$: on obtient ainsi, par le procédé de 5.3.4, un morphisme de $\mathfrak{S}_n$ dans $\mathfrak{S}(\mathcal{P}(E))$ et aussi, en numérotant les parties de E de 1 à 2^n, un morphisme de $\mathfrak{S}_n$ dans $\mathfrak{S}_{2^n}$. Ce genre d'argument est souvent utilisé pour construire des morphismes d'un groupe donné vers un groupe symétrique.

Autre exemple : de l'action naturelle de $\mathfrak{S}_4$ sur $E = \{1, 2, 3, 4\}$ on déduit une action sur l'ensemble X des partitions de E en deux parties à deux éléments. Comme X a 3 éléments (lesquels ?) on en tire un morphisme de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$. *Exercice :* montrer que ce morphisme est surjectif. Quel est son noyau ? [S 29]

5.3.8. Soit V un espace vectoriel sur un corps K. Alors $\mathrm{GL}(V)$ opère à gauche sur V (d'ailleurs c'est un sous-groupe de $\mathfrak{S}(V)$). D'autre part le groupe multiplicatif K^* opère à gauche sur V (et aussi à droite, parce que K^* est commutatif) « par homothéties », selon la formule $(\lambda, x) \mapsto \lambda x$ pour $\lambda \in K^*$ et $x \in V$. Ces deux actions sont *K-linéaires*, c'est-à-dire que pour tout $g \in \mathrm{GL}(V)$ (resp. $g \in K^*$) l'application $x \mapsto gx$ de V dans V est K-linéaire.

On a aussi une action du groupe additif V sur V par translations, donnée par $(v, x) \mapsto x + v$: celle-ci n'est pas K-linéaire et sera généralisée ci-dessous.

5.3.9. Gardons les notations de 5.3.8. De l'action de $\mathrm{GL}(V)$ sur V on déduit que ce groupe opère aussi sur « tout ensemble déduit naturellement de V ». Par exemple il opère à gauche sur l'ensemble des sous-espaces vectoriels de V (par $(g, W) \mapsto g(W)$), ou sur l'ensemble des bases de V. Si E est un K-espace vectoriel, $\mathrm{GL}(V)$ opère à gauche sur $\mathrm{Hom}_K(E, V)$ par $(g, f) \mapsto g \circ f$.

De même il opère *à droite* sur le dual V^* de V : pour $g \in \mathrm{GL}(V)$ et $\varphi \in V^*$ on pose $\varphi g = \varphi \circ g$. Il opère aussi à droite sur l'ensemble des formes bilinéaires sur V (comment ?). Si E est un K-espace vectoriel, $\mathrm{GL}(V)$ opère à droite sur $\mathrm{Hom}_K(V, E)$

par $(g, f) \mapsto f \circ g$; l'exemple de V^* est le cas particulier où $E = K$.

5.3.10. Soit H un sous-groupe d'un groupe G. On dispose de trois actions naturelles de H sur (l'ensemble sous-jacent à) G :

– l'action *à gauche par translation*, donnée par $(h, x) \mapsto hx$ pour $h \in H$ et $x \in G$;

– l'action *à droite par translation*, donnée par $(x, h) \mapsto xh$ pour $h \in H$ et $x \in G$;

– l'action *à gauche par conjugaison* (ou « par automorphismes intérieurs »), donnée par $(h, x) \mapsto hxh^{-1}$ pour $h \in H$ et $x \in G$.

Noter une différence importante entre ces actions : la troisième, contrairement aux deux premières, est une action *par automorphismes*, c'est-à-dire que pour tout $h \in H$ l'application $x \mapsto hxh^{-1}$ est un automorphisme de G. En d'autres termes, le morphisme de H dans $\mathfrak{S}(G)$ déduit de cette action est en fait un morphisme dans $\mathrm{Aut}(G)$.

Remarquer aussi que pour l'action par automorphismes intérieurs, il faut absolument éviter la notation $(h, x) \mapsto hx$ pour noter l'action de groupe !

5.3.11. *Exercice.* Prenant $H = G = \mathbb{Z}$ dans 5.3.10, on obtient trois actions de $\mathbb{Z}$ sur lui-même et donc, d'après 5.3.6, trois bijections de $\mathbb{Z}$ sur lui-même. Lesquelles ?

5.4. *Vocabulaire.* Soit G un groupe opérant à gauche sur un ensemble E.

5.4.1. *Stabilisateurs.* Le stabilisateur d'un élément x de E est le sous-groupe G_x de G défini par

$$G_x := \{g \in G \mid gx = x\}.$$

5.4.2. *Points fixes.* On dit que $x \in E$ est un point fixe de $g \in G$ si $g \in G_x$, c'est-à-dire si $gx = x$. On dit que x est un point fixe de G (ou de l'action de G) si $G_x = G$; on dit aussi dans ce cas que G *opère trivialement* sur x.

5.4.3. *Actions libres.* On dit que G opère *librement* sur E si $G_x = \{e\}$ pour tout $x \in E$ (autrement dit, si aucun élément non trivial de G n'a de point fixe).

5.4.4. *Exercice.* [S 30] Soit $f : G \to \mathfrak{S}(E)$ le morphisme déduit de l'action de G (cf. 5.3.4). Montrer que $\mathrm{Ker}\, f = \bigcap_{x \in E} G_x$.

On dit que l'action de G est *fidèle* si f est injectif. Peut-on déduire de ce qui précède que toute action libre est fidèle ? Que pensez-vous de la réciproque ?

5.4.5. *Exercice.* [S 31] Montrer que l'action à gauche de G sur lui-même par translation est fidèle. En déduire que G est isomorphe à un sous-groupe du groupe $\mathfrak{S}(G)$ des permutations de l'ensemble sous-jacent à G, puis que *tout groupe fini G est isomorphe à un sous-groupe de $\mathfrak{S}_n$, où n est l'ordre de G.*

5.4.6. *Orbites.* Pour $x \in E$, on appelle orbite de x (sous G) l'image de l'application

$g \mapsto gx$ de G dans E, autrement dit l'ensemble

$$Gx := \{gx\}_{g\in G} \subset E.$$

Ainsi, x est un point fixe si et seulement si $Gx = \{x\}$.

Attention : ne pas confondre le stabilisateur G_x et l'orbite Gx. Dans un document manuscrit (une copie d'examen par exemple) les deux notations peuvent devenir dangereusement proches, et le lecteur n'est pas forcément enclin à choisir la bonne...

5.4.7. *Exemple des actions de* $\mathbb{Z}$. Soit σ une bijection de E sur lui-même. On a alors (5.3.6) une action de $\mathbb{Z}$ sur E donnée par $(n, x) \mapsto \sigma^n(x)$. Pour $x \in E$ fixé, l'orbite de x pour cette action (appelée simplement l'orbite de x sous σ) est l'ensemble des transformés de x par les puissances (positives et négatives !) de σ.

5.4.8. *Exercice.* [S 32] Dans l'exemple 5.3.8, quelles sont les orbites pour l'action de $\mathrm{GL}(V)$ sur V ? Et pour l'action de K^* sur V ? Cette dernière action est-elle libre ? fidèle ? Et pour l'action de $\mathrm{GL}(V)$ sur l'ensemble des sous-espaces de V définie en 5.3.9 ? (On pourra supposer V de dimension finie).

5.4.9. *Exercice.* [S 33] Quelles sont les orbites pour l'action naturelle du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ sur $\mathbb{R}^n$? Et pour l'action du groupe spécial orthogonal $\mathrm{SO}(n, \mathbb{R}) = \{u \in \mathrm{O}(n, \mathbb{R}) | \det(u) = 1\}$?

5.4.10. *Parties stables.* Un sous-ensemble F de E est dit *G-stable* si $gF \subset F$ pour tout $g \in G$. On dit aussi que F est *G-invariant*, ou que c'est un sous-G-ensemble de E (il est clair que l'on a alors une action de G sur F, et que l'application d'inclusion de F dans E est un G-morphisme).

5.4.11. *Exercice.* Si F est une partie G-stable de E on a en fait $gF = F$ pour tout $g \in G$ (indication : utiliser l'inverse). Ceci justifie l'expression « G-invariant ».

5.4.12. *Exercice.* Toute orbite est G-stable ; plus généralement une partie F de E est G-stable si et seulement si elle est réunion d'orbites.

5.4.13. *Cas des actions à droite.* Les notions ci-dessus se transposent, mutatis mutandis, aux actions à droite ; bien entendu il est alors préférable de noter xG l'orbite de x.

Proposition 5.5 *Soit G un groupe opérant à gauche sur un ensemble E. Pour tout $x \in E$ et tout $g \in G$, le stabilisateur de gx est $G_{gx} = gG_xg^{-1}$.*

En particulier, les stabilisateurs des points d'une même orbite sont conjugués *les uns des autres.*

Démonstration. Pour $\gamma \in G$, on a les équivalences :

$$\gamma \in G_{gx} \iff \gamma gx = gx \iff g^{-1}\gamma gx = x \iff g^{-1}\gamma g \in G_x \iff \gamma \in gG_xg^{-1}. \quad \blacksquare$$

5.5.1. *Remarque.* Pour une action à droite, un raisonnement similaire montre que le stabilisateur de xg est, cette fois, $g^{-1}G_x g$. *Il est dangereux de vouloir retenir ces formules par cœur ;* il est bien plus sûr de refaire le raisonnement.

5.5.2. *Exercice.* Si G est *commutatif*, que devient l'énoncé ?

Proposition 5.6 (et définition) *Soit G un groupe opérant à gauche (resp. à droite) sur un ensemble E. Alors les orbites sous G forment une partition de E.*

En d'autres termes, la relation $y \in Gx$ (resp. $y \in xG$) sur E est une relation d'équivalence.

L'ensemble quotient de E par cette relation, c'est-à-dire l'ensemble des orbites, est appelé le quotient de E par l'action de G *et est noté $G\backslash E$ (resp. E/G) s'il n'y a pas de confusion sur l'action de G.*

La démonstration est laissée au lecteur. C'est d'ailleurs un bon exercice de démontrer indépendamment les deux versions (partition d'une part, relation d'équivalence de l'autre). ∎

5.6.1. Comme pour toute relation d'équivalence, on a une application naturelle, dite « canonique »

$$\pi : E \longrightarrow G\backslash E$$

qui à tout élément x de E associe son orbite (c'est-à-dire sa classe d'équivalence) Gx. Cette application a les vertus fondamentales suivantes :

(i) π est *surjective* ;

(ii) pour tous x, $y \in E$, on a $\pi(x) = \pi(y)$ si et seulement si x et y ont la même orbite, autrement dit s'il existe $g \in G$ tel que $y = gx$.

Corollaire 5.7 *Soit G un groupe opérant à gauche* librement (5.4.3) *sur un ensemble E. Alors, pour toute orbite X de E on a $|X| = |G|$, et de plus*

$$|E| = |G|\ |G\backslash E|.$$

Démonstration. Pour $x \in E$, l'application $g \mapsto gx$ est injective puisque l'action est libre ; elle induit donc une bijection de G sur son image qui n'est autre que l'orbite de x, d'où la première assertion.

D'autre part il résulte de 5.6 que $|E|$ est somme des cardinaux des orbites. Comme ceux-ci sont tous égaux à $|G|$ on a donc $|E| = |G| \times$ (nombre d'orbites), d'où la formule. ∎

5.7.1. *Remarque.* Le cas le plus intéressant est celui où E est fini et non vide : la formule montre que G est automatiquement fini dans ce cas (exercice : le prouver directement ; où sert l'hypothèse $E \neq \emptyset$?). On laisse au lecteur le soin de se convaincre que la formule de l'énoncé est encore valable si l'un des termes est infini, avec

les conventions usuelles. Noter le cas où E est vide : alors $G\backslash E$ l'est aussi, de sorte que la bonne convention est $\infty \times 0 = 0$.

5.7.2. *Remarque.* Bien entendu l'énoncé analogue pour une action à droite est valable ; il suffit de remplacer $|G\backslash E|$ par $|E/G|$ dans la formule.

5.8. *Actions transitives.* On dit que G opère *transitivement* sur E si $Gx = E$ pour tout $x \in E$; autrement dit, si pour x et y quelconques dans E il existe $g \in G$ tel que $y = gx$. D'après la proposition précédente, il revient au même de dire que $G\backslash E$ a au plus un élément (il y a au plus une orbite). Attention : avec la définition adoptée ici, l'unique action de G sur l'ensemble vide est transitive, mais n'a aucune orbite (c'est d'ailleurs la seule : toute action transitive sur un ensemble non vide a une orbite et une seule, qui est l'ensemble lui-même).

Inversement, si G opère sur un ensemble quelconque E, l'action induite sur chaque orbite de E sous G est transitive.

5.8.1. *Exercice.* Avec les notations de 5.3.9, supposons V de dimension finie sur K. Montrer que l'action naturelle de $\mathrm{GL}(V)$ sur l'ensemble des bases de V est libre et transitive.

5.9. *Exemple.* Soit H un sous-groupe de G ; voyons ce que donnent les notions ci-dessus dans le cas des actions définies en 5.3.10 :

5.9.1. L'action de H sur G par conjugaison n'est pas libre en général (par exemple e est un point fixe ; dans quels cas cette action est-elle tout de même libre ?). L'orbite d'un élément de G est appelée sa *classe de conjugaison* sous H.

Si $H = G$, l'orbite de x est donc l'ensemble des gxg^{-1} où g parcourt G, et on l'appelle simplement la classe de conjugaison de x dans G. Le stabilisateur de x est le *centralisateur* $Z_G(x)$ de x, déjà rencontré (3.3.8).

L'ensemble des classes de conjugaison sous H n'est *jamais* noté $H\backslash G$; cette notation sera réservée au quotient par l'action à gauche de H par translations.

5.9.2. Les actions de H sur G à droite et à gauche par translation sont libres ; nous allons les étudier en détail au paragraphe 7.

6. Le groupe symétrique

6.1. *Généralités.* Le groupe symétrique $\mathfrak{S}_n$, pour $n \in \mathbb{N}$, a déjà été défini, cf. 1.4.7 : c'est le groupe des bijections de l'ensemble $\{1, \ldots, n\}$ sur lui-même (appelées aussi *permutations* de $\{1, \ldots, n\}$).

6.1.1. Le fait de se restreindre à $\{1, \ldots, n\}$ est surtout une convention commode (analogue à celle, fréquente en algèbre linéaire sur un corps K, de démontrer les résultats pour K^n et de les utiliser sans commentaire pour un K-espace vectoriel de dimension n quelconque) : on pourrait la plupart du temps travailler avec le groupe $\mathfrak{S}(E)$ des permutations d'un ensemble E à n éléments.

En fait, si $f : \{1, \ldots, n\} \to E$ est une bijection quelconque, on vérifie tout de suite que l'application $\sigma \mapsto f \circ \sigma \circ f^{-1}$ est un *isomorphisme* de $\mathfrak{S}_n$ sur $\mathfrak{S}(E)$, qui de plus respecte la plupart des constructions que nous ferons plus bas (décomposition en cycles par exemple).

6.1.2. Rappelons que la loi de groupe de $\mathfrak{S}_n$ est la composition des applications, notée le plus souvent par juxtaposition et définie par $\sigma\tau(i) = \sigma(\tau(i))$ pour tout $i \in \{1, \ldots, n\}$. L'élément neutre de $\mathfrak{S}_n$ est l'application identité de $\{1, \ldots, n\}$, en général notée Id.

6.1.3. Le groupe $\mathfrak{S}_n$ *opère à gauche* sur $\{1, \ldots, n\}$ par $(\sigma, x) \mapsto \sigma(x)$. Cette action n'est pas libre si (et seulement si) $n \geq 3$; elle est transitive (exercice).

6.1.4. *Notation.* Une permutation σ se note en général comme un tableau :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

6.1.5. *Exercice.* Testez votre compréhension de 6.1.2 et 6.1.4 en vérifiant la relation

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

6.1.6. *Exercice.* [I 14] Montrer que, pour $n \geq 3$, le centre de $\mathfrak{S}_n$ est trivial.

6.2. *Vocabulaire.* C'est en général celui des actions de groupes, appliqué à une permutation σ donnée (ou à l'action du sous-groupe $\langle\sigma\rangle$ de $\mathfrak{S}_n$ qu'elle engendre). Rappelons l'essentiel :

6.2.1. *Points fixes.* Un élément i de $\{1, \ldots, n\}$ est un *point fixe* pour une permutation $\sigma \in \mathfrak{S}_n$ si $\sigma(i) = i$. C'est un cas particulier de la notion de point fixe pour une action de groupe, cf. 5.4.2.

6.2.2. *Orbites.* Les *orbites* sous $\sigma \in \mathfrak{S}_n$ sont les orbites sous l'action de $\langle\sigma\rangle$ sur $\{1,\dots,n\}$. C'est l'occasion de relire 5.3.6, 5.4.7 et 8.1.7 ; nous y reviendrons un peu plus loin.

6.2.3. *Parties stables.* Une partie A de $\{1,\dots,n\}$ est *stable*, ou *invariante*, par $\sigma \in \mathfrak{S}_n$ si $\sigma(A) = A$ (ou encore si $\sigma(A) \subset A$: c'est la même chose, cf. 5.4.11). Il revient au même de dire que A est invariante sous l'action de $\langle\sigma\rangle$, ou encore que A est une réunion d'orbites sous σ.

6.3. *Support.* Le *support* de $\sigma \in \mathfrak{S}_n$ est par définition le complémentaire de l'ensemble des points fixes de σ :

$$\mathrm{Supp}\,(\sigma) = \{i \in \{1,\dots,n\} \mid \sigma(i) \neq i\}.$$

C'est aussi la réunion des orbites sous σ ayant plus d'un élément. Quel est le support de Id ? Quelles sont les permutations dont le support a un seul élément ? deux éléments ? [S 34]

Le lecteur démontrera lui-même la proposition suivante (et la généralisera au cas d'un nombre fini quelconque de permutations) :

Proposition 6.3.1 *Soient σ et $\tau \in \mathfrak{S}_n$. Alors on a* $\mathrm{Supp}\,(\sigma\tau) \subset \mathrm{Supp}\,(\sigma) \cup \mathrm{Supp}\,(\tau)$.

De plus, si σ et τ sont à supports disjoints, i.e. si $\mathrm{Supp}\,(\sigma) \cap \mathrm{Supp}\,(\tau) = \emptyset$, *alors on a* $\mathrm{Supp}\,(\sigma\tau) = \mathrm{Supp}\,(\sigma) \cup \mathrm{Supp}\,(\tau)$, *et plus précisément :*

(i) *pour tout $i \in \{1,\dots,n\}$,*

$$(\sigma\tau)(i) = \begin{cases} \sigma(i) & \text{si } i \in \mathrm{Supp}\,(\sigma) \\ \tau(i) & \text{si } i \in \mathrm{Supp}\,(\tau) \\ i & \text{dans les autres cas.} \end{cases}$$

(ii) $\sigma\tau = \tau\sigma$;

(iii) *si* $\sigma\tau = \mathrm{Id}$ *alors* $\sigma = \tau = \mathrm{Id}$. ∎

6.4. *Cycles, décomposition d'une permutation.* Fixons une permutation $\sigma \in \mathfrak{S}_n$.

6.4.1. Pour $i \in \{1,\dots,n\}$ donné, rappelons (8.1.7) la structure de l'orbite de i sous σ : il existe un plus petit entier $l > 0$, appelé la période de i sous σ, tel que $\sigma^l(x) = x$; l'orbite de i est formée des l éléments distincts $\sigma^j(i)$ $(0 \leq j < l)$. L'action de σ sur cette orbite est donnée par

$$i \mapsto \sigma(i) \mapsto \sigma^2(i) \mapsto \cdots \mapsto \sigma^{l-1}(i) \mapsto i = \sigma^l(i).$$

Ceci suggère d'introduire la notion suivante :

Définition 6.4.2 *Soit l un entier ≥ 1, et soient $i_1, \ldots, i_l$ deux à deux distincts dans $\{1, \ldots, n\}$. On note*

$$(i_1, \ldots, i_l)$$

l'élément γ de $\mathfrak{S}_n$ défini comme suit :

$$\gamma(i) = \begin{cases} i & \text{si } i \notin \{i_1, \ldots, i_l\} \\ i_{k+1} & \text{si } i = i_k \ (1 \leq k < l) \\ i_1 & \text{si } i = i_l \end{cases}$$

Une permutation de la forme $(i_1, \ldots, i_l)$ est appelée cycle *(ou* permutation circulaire*)* de longueur l.

6.4.3. La notation $(i_1, \ldots, i_l)$ est standard mais pas très heureuse. D'une part elle est aussi utilisée pour désigner le l-uplet (la suite) des entiers $i_1, \ldots, i_l$, ce qui n'est pas la même chose, cf. 6.4.5 ci-dessous. D'autre part, elle ne contient pas n de sorte que par exemple la notation $(1, 2)$ désigne une infinité d'objets, un pour chaque $n \geq 2$; c'est parfois gênant.

6.4.4. Les orbites sous $(i_1, \ldots, i_l)$ sont $\{i_1, \ldots, i_l\}$ et les singletons $\{j\}$ pour $j \notin \{i_1, \ldots, i_l\}$; le support Supp $(i_1, \ldots, i_l)$ est vide si $l = 1$ et égal à $\{i_1, \ldots, i_l\}$ si $l > 1$. De plus (vérification immédiate), $(i_1, \ldots, i_l)$ est un élément *d'ordre* l de $\mathfrak{S}_n$.

6.4.5. On a $(i_1, \ldots, i_l) = (i_2, \ldots, i_l, i_1)$; en fait, pour que deux cycles $(i_1, \ldots, i_l)$ et $(j_1, \ldots, j_m)$ soient égaux, il faut et il suffit que, soit $l = m = 1$, soit $l = m > 1$ et il existe un entier a tel que $j_k = i_{\text{reste}(k+a)}$ pour tout k, où reste(x) désigne le reste de la division de l'entier x par l. Vérifiez !

6.4.6. *Transpositions.* On appelle *transposition* tout cycle d'ordre 2 ; c'est donc un élément de la forme (i, j) avec $i \neq j$, et il a pour effet d'échanger i et j en laissant fixes les autres éléments de $\{1, \ldots, n\}$.

6.4.7. *Conjugaison des cycles.* Pour $\sigma \in \mathfrak{S}_n$ quelconque et $\gamma = (i_1, \ldots, i_l)$, le conjugué $\sigma\gamma\sigma^{-1}$ est le cycle $(\sigma(i_1), \ldots, \sigma(i_l))$. La vérification est un bon exercice !

6.4.8. *Cycles associés à une permutation.* Soit $\sigma \in \mathfrak{S}_n$ et soit X une orbite sous σ. Définissons un élément γ de $\mathfrak{S}_n$ par $\gamma(i) = \sigma(i)$ si $i \in X$ et $\gamma(i) = i$ sinon. (Pourquoi est-ce bien une permutation ?) La description de 6.4.1 montre que γ est en fait un cycle d'ordre $l = |X|$: en fait, si i est un élément quelconque de X, γ est le cycle $(i, \sigma(i), \sigma^2(i), \cdots, \sigma^{l-1}(i))$ (cette écriture dépend du choix de i mais γ ne dépend que de X). Les cycles ainsi obtenus sont dits *associés* à σ. Par exemple, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$ a trois cycles associés, à savoir $(1, 2, 4)$, $(3, 5)$ et $(6) = \text{Id}$.

Proposition 6.5 *Tout élément σ de $\mathfrak{S}_n$ peut s'écrire*

$$\sigma = \gamma_1 \cdots \gamma_m$$

où $m \in \mathbb{N}$ et où les γ_i sont des cycles à supports deux à deux disjoints.

Cette décomposition est unique à l'ordre près si l'on exclut les cycles de longueur 1 : plus précisément, les γ_i d'ordre > 1 sont les cycles associés à σ de longueur > 1.

Démonstration.

– *Unicité.* Si σ est décomposée comme dans l'énoncé, avec les γ_i tous de longueur > 1, alors il est immédiat que les cycles associés à σ sont bien les γ_i et ceux correspondant aux points fixes de σ.

– *Existence.* Si l'on désigne par $X_1, \ldots, X_m$ les orbites sous σ et par $\gamma_1, \ldots, \gamma_m$ les cycles associés correspondants, alors les supports des γ_i sont bien disjoints (ils sont contenus dans les orbites correspondantes, qui sont disjointes). Montrons que $\sigma = \gamma_1 \cdots \gamma_m$: pour tout $i \in \{1, \ldots, n\}$ il existe un unique j tel que $i \in X_j$ (les orbites forment une partition de $\{1, \ldots, n\}$) et il résulte alors de 6.3.1 (généralisé à m permutations) que $(\gamma_1 \cdots \gamma_m)(i) = \gamma_j(i)$ qui est égal à $\sigma(i)$ par définition de γ_j. ∎

6.6. *Propriétés de la décomposition en cycles.*

6.6.1. Le *calcul pratique* de la décomposition en cycles d'une permutation donnée est très simple puisqu'il suffit de trouver les cycles associés.

6.6.2. Une propriété très importante de la décomposition de 6.5 est que les γ_i *commutent* deux à deux, puisqu'ils sont à supports disjoints. En conséquence, on a (toujours avec les notations de 6.5) $\sigma^k = \sigma_1^k \cdots \sigma_m^k$ pour tout $k \in \mathbb{Z}$. (Noter cependant que les σ_i^k ne sont pas nécessairement des cycles).

On en déduit notamment que *l'ordre de σ dans $\mathfrak{S}_n$ est le ppcm des ordres des σ_i* : en effet les γ_i^k sont à support disjoints deux à deux, de sorte que d'après 6.3.1(iii) leur produit est l'identité si et seulement si chacun d'eux est l'identité, c'est-à-dire si et seulement si k est divisible par le ppcm de leurs ordres.

6.6.3. *Type et conjugaison des cycles.* Avec les notations de 6.5, la suite $(l_1, \cdots, l_m)$ des ordres des γ_i (d'où l'on exclut les cycles d'ordre 1) est bien déterminée à l'ordre près par σ, vu l'assertion d'unicité de la décomposition. Pour se débarrasser du problème de l'ordre on peut convenir, par exemple, de les ranger dans l'ordre décroissant (au sens large, évidemment). Appelons *type* de σ la suite $(l_1, \cdots, l_m)$ ainsi définie : c'est donc une suite décroissante d'entiers ≥ 2, dont la somme est $\leq n$ (pourquoi, lecteur ? Et comment s'interprète cette somme, en termes de σ ?) Par exemple, le type de l'identité est la suite vide (), et le type d'un cycle d'ordre $l > 1$ est la suite à un élément (l). Inversement (exercice) toute suite décroissante d'entiers > 1, de somme $\leq n$, est le type d'un élément de $\mathfrak{S}_n$.

Il résulte de 6.4.7 que *deux permutations conjuguées ont même type.* Inversement, il est facile de voir que le type détermine la classe de conjugaison :

Proposition 6.6.4 *Pour que deux permutations σ et $\sigma' \in \mathfrak{S}_n$ soient conjuguées dans $\mathfrak{S}_n$, il faut et il suffit qu'elles aient le même type.*

Démonstration. Comme on vient de le dire, la nécessité est une conséquence immédiate de 6.4.7. Inversement, supposons σ et σ' de même type $(l_1, \cdots, l_m)$ et écrivons $\sigma = \gamma_1 \cdots \gamma_m$, $\sigma' = \gamma'_1 \cdots \gamma'_m$ avec, pour chaque $k \in \{1, \ldots, m\}$,

$$\gamma_k = (i_{k,1}, \ldots, i_{k,l_k}) \quad \text{et} \quad \gamma'_k = (i'_{k,1}, \ldots, i'_{k,l_k}).$$

(Remarque : la notation est la seule difficulté de cette démonstration. Le lecteur a intérêt à méditer celle-ci, qui est typique. L'aurait-il trouvée tout seul ? Sinon, qu'il médite encore !)

Comme les $i_{k,j}$ (resp. les $i'_{k,j}$) sont deux à deux distincts, il existe une permutation α de $\{1, \ldots, n\}$ qui envoie $i_{k,j}$ sur $i'_{k,j}$ pour tout $k \in \{1, \ldots, m\}$ et tout $j \in \{1, \ldots, l_k\}$. Il résulte alors à nouveau de 6.4.7 que $\alpha\sigma\alpha^{-1} = \sigma'$. ∎

6.6.5. *Exercice.* [S 35] Montrer que tous les éléments d'ordre 12 de $\mathfrak{S}_8$ sont conjugués.

6.6.6. *Exercice.* [S 36] Montrer que tous les éléments d'ordre 12 de $\mathfrak{S}_6$ sont conjugués.

Proposition 6.7 *Pour tout $n \in \mathbb{N}$, le groupe $\mathfrak{S}_n$ est engendré par les transpositions.*
Plus précisément, tout élément de $\mathfrak{S}_n$ est un produit de transpositions.

Démonstration. Les deux assertions sont en fait équivalentes d'après 4.4 puisque l'on a $\tau = \tau^{-1}$ pour toute transposition τ.

Compte tenu de 6.5 il suffit de voir que tout cycle est un produit de transpositions. Par conjugaison, il suffit même de voir que, pour tout $l \geq 2$, le cycle $(1, 2, \ldots, l)$ est un produit de transpositions. (Ce dernier argument, très souvent utilisé, a pour principal avantage d'alléger les notations). Or on a l'une des deux formules suivantes :

$$\begin{aligned} (1, 2, \ldots, l) &= (1, 2)(2, 3) \cdots (l-1, l) \\ (1, 2, \ldots, l) &= (l, l-1) \cdots (3, 2)(2, 1). \end{aligned}$$

Laquelle ? [S 37] ∎

6.7.1. Voici une autre preuve de 6.7 qui n'utilise pas 6.5 : on procède par récurrence sur n, le cas où $n \leq 2$ étant clair. Soit $\sigma \in \mathfrak{S}_n$: si $\sigma(n) = n$ alors on peut considérer σ comme un élément de $\mathfrak{S}_{n-1}$ et appliquer l'hypothèse de récurrence. Sinon, soit τ la transposition $(\sigma(n), n)$: alors $\sigma' := \tau\sigma$ vérifie $\sigma'(n) = n$ donc est un produit de transpositions d'après le cas précédent, et il en est donc de même de $\sigma = \tau\sigma'$, cqfd.

Il existe de nombreux énoncés du type « $\mathfrak{S}_n$ est engendré par telle famille de permutations ». En voici quelques-uns :

6.7.2. *Exercice.* [I 15] Montrer que $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de la forme $(1,i)$ où i parcourt $\{2,\dots,n\}$.

6.7.3. *Exercice.* [I 16] Montrer que $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de la forme $(i,i+1)$ où i parcourt $\{1,\dots,n-1\}$.

6.7.4. *Exercice.* [I 17] Montrer que $\mathfrak{S}_n$ est engendré par $\{(1,2),(1,2,\dots,n)\}$.

Définition 6.8 *Soient $n \geq 1$ et $\sigma \in \mathfrak{S}_n$. La* signature *de σ est par définition*

$$\varepsilon(\sigma) := (-1)^{\mathrm{inv}\,(\sigma)}$$

où $\mathrm{inv}\,(\sigma)$ *désigne le* nombre d'inversions *de σ, c'est-à-dire le nombre de couples (i,j) tels que $1 \leq i < j \leq n$ et $\sigma(i) > \sigma(j)$.*

On dit que σ est paire *si $\varepsilon(\sigma) = +1$, et* impaire *sinon.*

Proposition 6.9 *Soient σ et $\tau \in \mathfrak{S}_n$. Alors :*

(i) *si $x_1,\dots,x_n$ sont des réels quelconques, on a*

$$\prod_{1\leq i<j\leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = \varepsilon(\sigma) \prod_{1\leq i<j\leq n} (x_i - x_j) \ ;$$

(ii) $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$;

(iii) *si σ est le produit de m transpositions, alors $\varepsilon(\sigma) = (-1)^m$;*

(iv) *si σ est un cycle d'ordre l, alors $\varepsilon(\sigma) = (-1)^{l+1}$.*

Démonstration. (i) Pour chaque couple (i,j) avec $i<j$, considérons le facteur correspondant $(x_{\sigma(i)} - x_{\sigma(j)})$ du premier membre. Si (i,j) n'est pas une inversion de σ, ce facteur se retrouve au second membre, indexé par le couple $(\sigma(i),\sigma(j))$; sinon, le second membre contient le facteur opposé $(x_{\sigma(j)} - x_{\sigma(i)})$ indexé par le couple $(\sigma(j),\sigma(i))$. La formule en résulte.

Pour en déduire (ii), désignons par $\mathcal{F}$ le $\mathbb{R}$-espace vectoriel des applications de $\mathbb{R}^n$ dans $\mathbb{R}$, et considérons l'action à gauche de $\mathfrak{S}_n$ sur $\mathcal{F}$ donnée par

$$(\gamma f)(x_1,\dots,x_n) = f(x_{\gamma(1)},\dots,x_{\gamma(n)})$$

pour $\gamma \in \mathfrak{S}_n$ et $f \in \mathcal{F}$. (Avez-vous vérifié que c'est bien une action à gauche ?) Considérons alors l'élément φ de $\mathcal{F}$ défini par $\varphi(x_1,\dots,x_n) = \prod_{1\leq i<j\leq n}(x_i - x_j)$. Alors l'assertion (i) montre que l'on a

$$\gamma\varphi = \varepsilon(\gamma)\,\varphi$$

pour tout $\gamma \in \mathfrak{S}_n$. On a donc notamment

$$(\sigma\tau)\varphi = \varepsilon(\sigma\tau)\,\varphi \tag{6.9.1}$$

et d'autre part

$$\sigma(\tau\varphi) = \sigma(\varepsilon(\tau)\,\varphi) = \varepsilon(\tau)\,(\sigma\varphi) = \varepsilon(\tau)\,\varepsilon(\sigma)\,\varphi \tag{6.9.2}$$

où l'on utilise le fait, évident, que l'action de de $\mathfrak{S}_n$ sur $\mathcal{F}$ est linéaire. Égalant (6.9.1) et (6.9.2) et remarquant que φ n'est pas identiquement nulle, on obtient (ii).

Pour (iii), il suffit d'après (ii) de voir que toute transposition est impaire. On peut le voir directement sur la définition ; on peut aussi se simplifier la vie en remarquant que, toujours d'après (ii), la signature est invariante par conjugaison (i.e. $\varepsilon(\tau\sigma\tau^{-1}) = \varepsilon(\sigma)$) de sorte qu'il suffit même de voir que la transposition $(1,2)$ est impaire, ce qui est évident puisque le couple $(1,2)$ est sa seule inversion.

Enfin (iv) est conséquence de (iii) puisqu'un cycle d'ordre l est produit de $l-1$ transpositions. ∎

6.10. *Remarques et exercices.*

6.10.1. *Exercice.* [S 38] La démonstration utilise le corps $\mathbb{R}$. Un corps quelconque ferait-il aussi bien l'affaire ?

6.10.2. Attention à (iv) : ce sont les cycles d'ordre pair qui sont des permutations impaires et inversement.

6.10.3. En prenant $x_i = i$ dans (i) on obtient la formule

$$\varepsilon(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}$$

qui sert parfois de définition à la signature. *Exercice :* partir de cette formule pour redémontrer 6.9. Attention, il faut commencer par montrer que $\varepsilon(\sigma) \in \{-1,+1\}$!

6.10.4. *Exercice.* Montrer que :

(i) $\varepsilon(\sigma) = (-1)^{n-m}$ où m est le nombre d'orbites sous σ ;

(ii) $\varepsilon(\sigma) = (-1)^{s}$ où s est le nombre d'orbites paires (i.e. de cardinal pair) sous σ.

6.10.5. *Exercice.* Que pensez-vous de l'idée de prendre 6.9(iii) comme définition de la signature ?

6.10.6. *Le groupe alterné.* L'assertion 6.9(ii) s'exprime aussi en disant que la signature définit un morphisme de groupes de $\mathfrak{S}_n$ dans le groupe multiplicatif $\{-1,+1\}$. Ce morphisme est surjectif si $n \ge 2$ (puisque les transpositions sont impaires). Son noyau (l'ensemble des permutations paires) est un sous-groupe de $\mathfrak{S}_n$, appelé *groupe alterné* et noté A_n. C'est un groupe d'ordre $n!/2$ (toujours si $n \ge 2$) : en effet, si τ est une transposition fixée, l'application $\sigma \mapsto \sigma\tau$ montre qu'il y a autant de permutations paires que d'impaires. Le groupe A_n est trivial pour $n = 2$, isomorphe à $\mathbb{Z}/3\mathbb{Z}$ pour $n = 3$ (il est formé de l'identité et des deux cycles d'ordre 3 de $\mathfrak{S}_3$), et non commutatif pour $n \ge 4$.

6.11. *Exercice : applications multilinéaires alternées.* Soient K un corps, n un entier naturel, E et F deux K-espaces vectoriels, $f : E^n \to F$ une application n-linéaire (c'est-à-dire que pour chaque $i \in \{1, \ldots, n\}$ et chaque choix des $x_j \in E$ pour $j \neq i$, l'application $x_i \mapsto f(x_1, \ldots, x_n)$ de E dans F est K-linéaire). On dit que f est *alternée* si $f(x_1, \ldots, x_n) = 0$ chaque fois qu'il existe $i \in \{1, \ldots, n-1\}$ tel que $x_i = x_{i+1}$. (Si $F = K$ on dit que f est une *forme n-linéaire alternée* sur E).

6.11.1. Si f est alternée, montrer que $f(x_1, \ldots, x_n)$ change de signe si l'on permute x_i et x_{i+1} ; inversement cette propriété implique que f est alternée *si K n'est pas de caractéristique* 2. (C'est du DEUG deuxième année).

6.11.2. En déduire que si f est alternée, on a

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \ldots, x_n) \tag{6.11.2.1}$$

pour tout $\sigma \in \mathfrak{S}_n$ et tout $(x_1, \ldots, x_n) \in E^n$, et que $f(x_1, \ldots, x_n) = 0$ chaque fois qu'il existe i et $j \in \{1, \ldots, n\}$ distincts tels que $x_i = x_j$. (On n'exclut pas que K soit de caractéristique 2 !)

6.11.3. Supposons f alternée, soient $e_1, \ldots, e_n \in E$ et $\xi_{i,j}$ $(i, j \in \{1, \ldots, n\})$ des éléments de K ; on pose $x_j = \sum_{i=1}^n \xi_{i,j} e_i$. Montrer que

$$f(x_1, \ldots, x_n) = \Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n \xi_{i,\sigma(i)} \Big) f(e_1, \ldots, e_n). \tag{6.11.3.1}$$

En particulier si $\{e_1, \ldots, e_n\}$ engendre E comme K-espace vectoriel, f est entièrement déterminée par l'élément $f(e_1, \ldots, e_n)$ de F.

6.12. *Déterminants (suite de l'exercice précédent).* Avec les notations de 6.11.3, on note $\Omega^n(E)$ le K-espace vectoriel des formes n-linéaires alternées sur E et l'on suppose que $(e_1, \ldots, e_n)$ est une *base* de E (de sorte que $n = \dim E$).

6.12.1. [I 18] Déduire de 6.11.3 que $\dim \Omega^n(E) \leq 1$. Montrer ensuite que l'application φ de E^n dans K *définie* (avec les mêmes notations) par

$$\varphi(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n \xi_{i,\sigma(i)} \tag{6.12.1.1}$$

est une forme n-linéaire alternée et que $\varphi(e_1, \ldots, e_n) = 1$. En déduire que $\Omega^n(E)$ est de dimension 1.

6.12.2. Avec les notations précédentes, montrer que $\varphi(x_1, \ldots, x_n)$ est le déterminant de $(x_1, \ldots, x_n)$ dans la base $(e_1, \ldots, e_n)$.

6.12.3. Soit u un endomorphisme de E. On définit un endomorphisme de $\Omega^n(E)$, noté $\Omega^n(u)$, en associant à toute forme $f \in \Omega^n(E)$ la forme $\Omega^n(u)(f)$ définie par

$$(x_1, \ldots, x_n) \mapsto f(u(x_1), \ldots, u(x_n))$$

(qui est bien un élément de $\Omega^n(E)$, n'est-ce pas ?). Montrer que $\Omega^n(\mathrm{Id}_E) = \mathrm{Id}_{\Omega^n(E)}$ et que $\Omega^n(u \circ v) = \Omega^n(v) \circ \Omega^n(u)$ pour u et $v \in \mathrm{End}(E)$.

Puisque $\dim \Omega^n(E) = 1$, $\Omega^n(u)$ est la multiplication par un unique scalaire $\delta(u) \in K$. Montrer que $\delta(u) = \det(u)$, et déduire de ce qui précède la formule $\det(v \circ u) = \det(u)\det(v)$.

6.13. *Exercice : matrices de permutation.* Soient K un corps et n un entier naturel. Alors $\mathfrak{S}_n$ opère à gauche linéairement sur K^n : si $(e_1, \ldots, e_n)$ désigne la base canonique de K^n, on associe à $\sigma \in \mathfrak{S}_n$ l'automorphisme de K^n envoyant e_i sur $e_{\sigma(i)}$, pour $i \in \{1, \ldots, n\}$.

Vérifier que c'est bien une action à gauche, et qu'elle est donnée par

$$(\sigma, (x_1, \ldots, x_n)) \mapsto (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

On obtient donc un morphisme de groupes $\varphi : \mathfrak{S}_n \longrightarrow \mathrm{GL}(n, K)$, qui est facile à décrire : pour $\sigma \in \mathfrak{S}_n$, $\varphi(\sigma)$ est la matrice dont la i-ème colonne est formée de zéros, à l'exception d'un 1 sur la $\sigma(i)$-ème ligne. (Une matrice de ce type est appelée *matrice de permutation*).

Montrer que l'on a alors pour tout $\sigma \in \mathfrak{S}_n$ la formule

$$\det \varphi(\sigma) = \varepsilon(\sigma)$$

(à condition naturellement d'interpréter $\varepsilon(\sigma)$ comme un élément de K ; en particulier, si K est de caractéristique 2, i.e. si $1 = -1$ dans K, on n'obtient rien d'intéressant !).

On peut naturellement prendre la formule ci-dessus comme définition de la signature (avec $K = \mathbb{Q}$ par exemple), à condition d'avoir adopté une définition du déterminant qui n'utilise pas la signature : voir ci-dessous.

6.13.1. *Exercice.* Montrer que le morphisme $\varphi : \mathfrak{S}_n \longrightarrow \mathrm{GL}(n, K)$ de l'exercice précédent est injectif. En déduire, en utilisant 5.4.5, que si K est un corps quelconque, tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathrm{GL}(n, K)$.

6.14. *Remarques sur les exercices précédents.* Les exercices 6.11 et 6.12 peuvent servir à définir les déterminants et à démontrer leurs principales propriétés. C'est en fait, parfois sous une forme déguisée, l'approche « classique » de la notion de déterminant dans les manuels de première année : on définit par exemple le déterminant des matrices carrées d'ordre n comme une application de $\mathrm{M}_n(K)$ dans K qui est n-linéaire alternée comme fonction des colonnes, et qui vaut 1 sur la matrice identité. Il

n'est pas très difficile (exactement comme dans 6.11.3) de déduire de ces propriétés la formule (où les $a_{i,j}$ sont les coefficients de la matrice $A \in \mathrm{M}_n(K)$)

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}. \tag{6.14.1}$$

On peut d'ailleurs voir cette formule comme un cas particulier de (6.11.3.1). On obtient ainsi l'unicité du déterminant, mais à ce stade on n'en a pas prouvé l'existence. Pour cela il faut montrer que si l'on *définit* le déterminant par la formule (6.14.1), alors on a bien les propriétés exigées. C'est essentiellement le contenu de 6.12.1 : le fait que $\det(\mathrm{Id}) = 1$ est facile, ainsi que la n-linéarité ; par contre, pour montrer que le déterminant s'annule lorsque deux colonnes consécutives sont égales, il faut en fait savoir, au minimum, que $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$ lorsque τ est une transposition de la forme $(i, i+1)$. Il est regrettable que certains ouvrages escamotent sans vergogne cette difficulté.

Une présentation du déterminant moins conceptuelle, mais qui évite ces écueils, consiste à le définir par récurrence sur n, en développant par rapport à la première colonne par exemple. On en déduit les propriétés voulues en utilisant systématiquement le fait que toute matrice de $\mathrm{M}_n(K)$ est produit de matrices « élémentaires ».

7. Classes modulo un sous-groupe

7.1. *Composition de sous-ensembles d'un groupe.* Si A et B sont deux parties d'un groupe G, on note simplement AB l'image de $A \times B$ par la loi de groupe, c'est-à-dire « l'ensemble des produits ab avec $a \in A$ et $b \in B$ ». Si A (resp. B) n'a qu'un élément a (resp. b) on note aB (resp. Ab) plutôt que $\{a\}B$ (resp. $A\{b\}$). On a $(AB)C = A(BC)$ avec ces notations, et la règle de regroupement (1.3.5.1) s'applique. (En fait, ce qui précède est valable pour tout ensemble G muni d'une loi associative et permet de définir une loi associative sur l'ensemble des parties de G).

On note aussi A^{-1} l'ensemble des inverses des éléments de A ; on a $(A^{-1})^{-1} = A$ mais pas $AA^{-1} = \{e\}$ en général. Par exemple, de l'égalité $AB = C$ entre parties de G on peut déduire $ABB^{-1} = CB^{-1}$ mais pas $A = CB^{-1}$ (exercice-piège : peut-on en déduire $A \subset CB^{-1}$?[S 39]).

Cependant on a bien $AA^{-1} = \{e\}$ si (et seulement si) A est réduit à un élément ; les implications du genre $aBc^{-1} = D \Rightarrow B = a^{-1}Dc$ (où a et c sont des *éléments* de G) sont donc valables.

Remarquer que si A est un sous-groupe de G on a $AA = A^{-1} = A$; la réciproque est-elle vraie ?[S 40]

7.2. *Classes à droite.* Soient G un groupe et H un sous-groupe de G. Considérons l'action *à gauche* de H sur G par translations, définie en 5.3.10 : elle est donnée, rappelons-le, par $(h, x) \mapsto hx$ pour $h \in H$ et $x \in G$, et elle est libre.

Définition 7.2.1 *Avec les notations ci-dessus, les orbites pour l'action à gauche de H sur G s'appellent les* classes à droite modulo H.

L'ensemble quotient pour cette action est noté $H\backslash G$.

7.2.2. *Remarque.* Bien entendu, ce dérapage du vocabulaire (les classes à droite sont les classes pour l'action à gauche) est regrettable mais il faut s'y faire ! Pour se rassurer, observer que, en notant h les éléments de H et g ceux de G :

- H opère à gauche sur G par $(h, g) \mapsto hg$;
- l'orbite de g pour cette action est Hg ;
- l'ensemble quotient (l'ensemble des orbites) pour cette action est $H\backslash G$.

Dans toutes ces notations, H figure « à gauche » ; le mauvais choix réside dans l'expression « classes à droite ».

7.2.3. De même les orbites sous H pour l'action *à droite* par translations s'appellent les *classes à gauche* de G modulo H ; la classe à gauche de $x \in G$ est xH. L'ensemble des classes à gauche est noté G/H. Nous reviendrons plus loin sur ces classes (7.7). Notons tout de suite que les classes à gauche et à droite coïncident lorsque G est commutatif.

7.2.4. *Exemple.* Prenons pour G le groupe symétrique $\mathfrak{S}_3$ (cf. 1.4.7). Dans G, notons σ la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et τ la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ (voir 6.1.4 pour les notations). On a alors $G = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, avec les relations $\sigma^3 = \tau^2 = e$ et $\tau\sigma = \sigma^2\tau$.

Le sous-ensemble $H = \{e, \tau\}$ de G est un sous-groupe ; les classes à droite modulo H sont :

$$He = H\tau = H = \{e, \tau\}; \quad H\sigma = H\sigma^2\tau = \{\sigma, \sigma^2\tau\}; \quad H\sigma^2 = H\sigma\tau = \{\sigma^2, \sigma\tau\}$$

et les classes à gauche modulo H sont :

$$eH = \tau H = H = \{e, \tau\}; \quad \sigma H = \sigma\tau H = \{\sigma, \sigma\tau\}; \quad \sigma^2 H = \sigma^2\tau H = \{\sigma^2, \sigma^2\tau\}.$$

On constate sur cet exemple que :

- les classes à droite et à gauche ont toutes le même cardinal, qui est celui de H ;
- H est une classe à droite et une classe à gauche ;
- les classes à droite ne coïncident pas avec les classes à gauche mais leur nombre est le même, et est égal à $|G|/|H|$.

Ce sont des faits généraux, comme on le verra dans la suite.

Considérons ensuite $K = \{e, \sigma, \sigma^2\}$: c'est encore un sous-groupe de G, et cette fois les classes à droite et les classes à gauche coïncident : ce sont K et $\tau K = K\tau = \{\tau, \sigma\tau, \sigma^2\tau\}$.

Proposition 7.3 *Avec les notations de* 7.2, *considérons l'application canonique*

$$\begin{array}{rccc} \pi : & G & \longrightarrow & H\backslash G \\ & x & \longmapsto & Hx \end{array}$$

définie en 5.6.1. *Pour x et y dans G, on a les équivalences :*

$$\pi(x) = \pi(y) \iff y \in Hx \iff x \in Hy \iff xy^{-1} \in H \iff yx^{-1} \in H.$$

Démonstration. L'équivalence des trois premières assertions est déjà connue, cf. 5.6.1(ii). D'autre part $x \in Hy$ équivaut à $xy^{-1} \in Hyy^{-1}$ donc à $xy^{-1} \in H$, cf. 7.1, et de même pour la dernière propriété. ∎

7.4. *Remarques.* On garde les notations de 7.2.

7.4.1. *Représentants.* Étant donné un élément α de $H\backslash G$, on appelle *représentant* de α un antécédent de α pour π, c'est-à-dire un $x \in G$ tel que $\pi(x) = \alpha$, ou ce

qui revient au même un élément de la classe α. (Noter que l'on a $\pi^{-1}(\alpha) = \alpha$: comprenez-vous cette formule ?) Cette terminologie est d'ailleurs utilisée pour toute relation d'équivalence.

On est parfois amené à choisir un représentant pour chaque classe, ce qui conduit à la notion de *système de représentants de G modulo H* : c'est par définition une famille $(x_i)_{i\in I}$ d'éléments de G telle que pour chaque classe $\alpha \in H\backslash G$, il existe un unique indice $i \in I$ tel que $x_i \in \alpha$.

Remarque sur l'ensemble d'indices I : comme les x_i sont obligatoirement deux à deux distincts (au fait, pourquoi ?) on peut très bien définir un système de représentants comme une *partie* de G, plutôt qu'une famille d'éléments. Par exemple, pour n entier > 0, $\{0, 1, \ldots, n-1\}$ est un système de représentants de $\mathbb{Z}$ modulo $n\mathbb{Z}$.

Un autre choix naturel est de prendre $H\backslash G$ lui-même comme ensemble d'indices, par exemple pour obtenir le résultat suivant (*exercice*) : il revient au même de choisir un système de représentants de G modulo H ou une application $\sigma : H\backslash G \to G$ telle que $\pi \circ \sigma = \mathrm{Id}_{H\backslash G}$, où π est l'application canonique de 7.3.

7.4.2. La classe de e_G est évidemment H. Pour $x \in G$, la classe de x est le « *translaté à droite* » de H par x, c'est-à-dire l'image de H par la translation à droite $y \mapsto yx$, cf. 1.3.3.

7.4.3. Comme l'action de H sur G est libre, on peut appliquer 5.7 et en déduire que *toutes les classes ont le même cardinal* qui est celui de H, et aussi :

Proposition 7.5 *Soient G un groupe, H un sous-groupe de G. Alors*

$$|G| = |H|\ |H\backslash G|.$$

∎

Corollaire 7.6 (théorème de Lagrange) *Soient G un groupe* fini, *H un sous-groupe de G. Alors $|H|$ divise $|G|$, et*

$$|H\backslash G| = \frac{|G|}{|H|}.$$

De plus l'ordre de tout élément de G divise $|G|$; autrement dit, on a (e désignant l'élément neutre de G)

$$\forall \gamma \in G, \quad \gamma^{|G|} = e.$$

Démonstration. Les assertions sur $|H|$ résultent trivialement de la proposition précédente ; il suffit ensuite de remarquer que l'ordre d'un élément est l'ordre du sous-groupe qu'il engendre, et enfin la dernière égalité s'obtient en appliquant 3.11(v).
∎

7.6.1. *Remarque.* Il est naturel de se demander si 7.6 admet une réciproque : si G est un groupe fini et si m est un entier naturel divisant $|G|$, existe-t-il un sous-groupe

de G d'ordre m ? La réponse est négative, l'exemple le plus simple étant le groupe alterné A_4 (voir 6.10.6), groupe d'ordre 12 qui n'admet aucun sous-groupe d'ordre 6. Par contre, nous verrons au paragraphe 16 que la réponse est affirmative lorsque m est une puissance d'un nombre premier.

Pour la question analogue de l'existence d'un *élément* d'ordre m dans G, nous verrons, toujours au paragraphe 16 que la réponse est affirmative lorsque m est premier ; voir aussi l'exercice 7.6.2 ci-dessous.

7.6.2. *Exercice.* [S 41] (i) Trouver un groupe fini d'ordre n qui n'a pas d'élément d'ordre n.

(ii) Soit G un groupe admettant un élément d'ordre fini n. Montrer que pour tout diviseur $d > 0$ de n, G admet un élément d'ordre d.

(iii) Soit p un nombre premier. Montrer que tout p-groupe non trivial admet un élément d'ordre p.

7.7. *Classes à gauche.* Les classes à gauche modulo un sous-groupe H d'un groupe G sont par définition (7.2.3) les parties de G de la forme xH pour $x \in G$, c'est-à-dire les translatés à gauche de H. Ce sont les classes d'équivalence pour la relation « $x^{-1}y \in H$ ». Nous laissons au lecteur le soin de formuler les analogues des considérations qui précèdent pour les classes à gauche. L'ensemble des classes à gauche modulo H est noté G/H.

7.7.1. *Exercice.* Soit $f : G \to G'$ un morphisme de groupes, et soit $H = \mathrm{Ker}\, f$. Montrer que, pour tout $x \in G$, $xH = Hx = f^{-1}(f(x))$.

(Autrement, dit, pour un sous-groupe qui est noyau d'un morphisme, les classes à gauche et à droite sont les mêmes. Nous verrons la réciproque au paragraphe 9.)

En déduire que pour x et $y \in G$, on a $f(x) = f(y)$ si et seulement si x et y ont la même classe à gauche (et à droite).

7.7.2. *Exercice.* [S 42] Soit G un groupe opérant à gauche sur un ensemble E. Pour x et $y \in E$, posons $\Gamma_{x,y} := \{g \in G \mid gx = y\}$. Montrer que $G_x = \Gamma_{x,x}$, que $\Gamma_{x,y}$ est soit vide, soit une classe à gauche modulo G_x, et que pour x fixé toutes les classes à gauche modulo G_x sont de cette forme. À quelles(s) condition(s) sur x et y a-t-on $\Gamma_{x,y} = \emptyset$? Dans ce cas, est-ce que $\Gamma_{x,y}$ est une classe à gauche ?

De manière symétrique montrer que $\Gamma_{x,y}$ est soit vide, soit une classe à droite modulo G_y, et que pour y fixé toutes les classes à droite modulo G_y sont de cette forme.

7.7.3. *Remarque sur l'exercice précédent.* L'auteur de ces lignes est parfaitement incapable de répondre à brûle-pourpoint à une question du genre : « est-ce que $\Gamma_{x,y}$, supposé non vide, est une classe à droite ou bien une classe à gauche modulo G_x ? », question qui se pose pourtant très souvent. La *seule* méthode sûre consiste à savoir refaire le raisonnement, rapidement et sans paniquer.

7.7.4. Les analogues de 7.5 et 7.6 pour les classes à gauche sont encore valables ; ceci suggère (et même prouve, si G est fini) qu'il doit y avoir une bijection entre G/H et $H\backslash G$. C'est bien le cas (*exercice*) : l'application $g \mapsto g^{-1}$ de G dans G envoie toute classe à gauche sur une classe à droite (et vice versa) , et induit la bijection cherchée.

7.7.5. [S 43] Montrer que toute classe à droite modulo un sous-groupe d'un groupe G est une classe à gauche modulo un autre sous-groupe que l'on précisera. Et réciproquement !

7.8. *Indice d'un sous-groupe.* On voit notamment que l'ensemble G/H est fini si et seulement si $H\backslash G$ est fini, et qu'alors $|G/H| = |H\backslash G|$. Dans ce cas, on dit que H est *d'indice fini* dans G, et l'entier $|G/H|$ est appelé l'indice de H dans G et noté $(G : H)$. Par exemple, pour n entier > 0, $n\mathbb{Z}$ est un sous-groupe d'indice n de $\mathbb{Z}$. Lorsque G/H est infini on convient de poser $(G : H) = \infty$.

7.8.1. *Exercice.* Soit H un sous-groupe d'indice 2 de G. Montrer que les classes à gauche (resp. à droite) modulo H sont H et le complémentaire de H dans G, et qu'en particulier les classes à droite et à gauche coïncident dans ce cas.

7.8.2. *Exercice* [S 44] (attention, source d'erreurs fréquentes !) : pourquoi n'a-t-on pas défini l'indice $(G : H)$ comme le quotient $|G|/|H|$? (Penser au cas où $G = \mathbb{Z}$).

7.8.3. *Exercice* [I 19] (« transitivité de l'indice »). Soient K un sous-groupe de G et H un sous-groupe de K. Montrer que l'on a $(G : H) = (G : K)(K : H)$, avec les conventions évidentes si l'un des termes est infini.

7.9. *Exercice : actions de G sur ses quotients.* Soit H un sous-groupe d'un groupe G : montrer que G opère à gauche sur l'ensemble quotient G/H par $(g, xH) \mapsto gxH$, et que l'application canonique de G dans G/H est G-équivariante (si l'on fait opérer G à gauche sur lui-même par translations).

L'action à gauche de G sur G/H ainsi définie est transitive ; le stabilisateur de la classe H (vue comme élément de G/H) est H, celui de la classe xH est xHx^{-1}.

De même G opère à droite transitivement sur $H\backslash G$ par $(Hx, g) \mapsto Hxg$.

Pourquoi ne pourrait-on pas faire opérer G à gauche sur $H\backslash G$ par $(Hx, g) \mapsto Hgx$? [S 45]

7.9.1. *Remarque.* On voit en particulier que tout sous-groupe d'un groupe G est un stabilisateur, pour une action convenable (à gauche ou à droite) de G.

7.10. *Exercice.* Soit G un groupe topologique (1.5), et soit H un sous-groupe de G. On note $\pi : G \to H\backslash G$ l'application canonique.

7.10.1. [S 46] Montrer que toute classe à droite Hx de G modulo H est homéomorphe à H (pour les topologies induites par celle de G). De plus si H est ouvert (resp. fermé) dans G, il en est de même de Hx. Même chose pour les classes à gauche.

7.10.2. [I 20] Soit H un sous-groupe ouvert de G. Montrer que H est fermé.

7.10.3. [I 21] On munit le quotient $H\backslash G$ de la « topologie quotient » suivante : par définition, une partie X de $H\backslash G$ est ouverte si et seulement si $\pi^{-1}(X)$ est un ouvert de G.

(i) Montrer que $\pi : G \to H\backslash G$ est continue et ouverte.

(ii) Si X est un espace topologique et f une application de $H\backslash G$ dans X, montrer que f est continue si et seulement si $f \circ \pi : G \to X$ est continue.

(iii) Montrer que $H\backslash G$ est séparé si et seulement si H est fermé dans G.

Pour terminer ce paragraphe, voici trois applications arithmétiques de 7.6 ; elles résultent toutes de l'application du théorème de Lagrange au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, où p est un nombre premier (c'est bien un groupe puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, et il est d'ordre $p-1$).

Corollaire 7.11 (« petit théorème de Fermat ») *Soit p un nombre premier. Alors :*

(i) *pour tout $k \in \mathbb{Z}$ non divisible par p, on a $k^{p-1} \equiv 1 \pmod{p}$;*

(ii) *pour tout $k \in \mathbb{Z}$, on a $k^p \equiv k \pmod{p}$.*

Démonstration. L'assertion (ii) est conséquence immédiate de (i) : si k n'est pas divisible par p, il suffit de multiplier par k la congruence de (i), et sinon k et k^p sont tous deux $\equiv 0 \pmod{p}$.

Pour montrer (i), il suffit de remarquer que puisque $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe d'ordre $p-1$ pour la multiplication, tout élément x de ce groupe vérifie $x^{p-1} = 1$, en vertu du théorème de Lagrange (7.6). ∎

Corollaire 7.12 (« théorème de Wilson ») *Soit p un nombre premier. Alors :*

$$(p-1)! \equiv -1 \pmod{p}.$$

Pour établir 7.12, montrons d'abord un lemme :

Lemme 7.12.1 *Soit G un groupe fini commutatif, noté multiplicativement. Alors le produit des éléments de G est égal au produit des éléments d'ordre 2 de G.*

Démonstration. Pour $x \in G$, dire que $x^2 \neq e$ équivaut à dire que $x \neq x^{-1}$. Chaque paire $\{x, x^{-1}\}$ de ce type peut être éliminée du produit de tous les éléments de G ; celui-ci est donc égal au produit de tous les $x \in G$ vérifiant $x^2 = e$, qui sont e et les éléments d'ordre 2. ∎

7.12.2. *Exercice.* [S 47] Où a servi l'hypothèse que G est commutatif ?

7.12.3. *Démonstration de* 7.12. Appliquons le lemme 7.12.1 au groupe $(\mathbb{Z}/p\mathbb{Z})^*$. Le produit de ses éléments est la classe modulo p de $(p-1)!$ puisque $(\mathbb{Z}/p\mathbb{Z})^*$ est l'ensemble des classes des entiers $1, 2, \ldots, p-1$. D'autre part, pour $x \in \mathbb{Z}/p\mathbb{Z}$, la relation $x^2 = 1$ équivaut à $(x-1)(x+1) = 0$ donc à $x = 1$ ou $x = -1$ puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. Le seul élément d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$ est donc -1, d'où la conclusion. (En fait, la dernière assertion n'est pas tout à fait exacte si $p = 2$, pourquoi ?) ∎

7.12.4. *Exercice.* [S 48] Que se passe-t-il dans 7.12 si p n'est plus supposé premier ?

7.12.5. *Exercice : autre démonstration du théorème de Wilson.* [I 22] Déduire du théorème de Fermat l'identité

$$X^{p-1} - \overline{1} = \prod_{i=1}^{p-1} (X - \overline{i})$$

entre polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$. En déduire le théorème de Wilson.

Corollaire 7.13 *Soit p un nombre premier impair. Pour tout entier a, notons $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ la classe de a modulo p. Les deux conditions suivantes sont équivalentes :*

(i) *$-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$;*

(ii) $p \equiv 1 \pmod 4$.

Démonstration. Comme p est impair, $-\overline{1}$ est un élément d'ordre 2 du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. L'assertion (i) entraîne donc que ce groupe admet un élément d'ordre 4 (puisque si $z^2 = -\overline{1}$ alors $z^2 \neq \overline{1}$ et $z^4 = \overline{1}$). Son ordre $p-1$ est donc divisible par 4, d'où (ii).

Pour voir que (ii) implique (i), considérons l'entier $N = (\frac{p-1}{2})!$. Sa classe modulo p est le produit des $\frac{p-1}{2}$ classes $\overline{1}, \overline{2}, \ldots, \overline{(\frac{p-1}{2})}$, dont les opposés sont les classes $\overline{p-1}, \overline{p-2}, \ldots, \overline{(\frac{p+1}{2})}$, c'est-à-dire précisément les autres éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. Donc le produit $N \times (-1)^{\frac{p-1}{2}} N$ a même classe modulo p que $(p-1)!$, d'où, d'après 7.12, $(-1)^{\frac{p-1}{2}} N^2 \equiv -1 \pmod p$. Mais si (ii) est vérifiée on a $(-1)^{\frac{p-1}{2}} = 1$, ce qui donne $N^2 \equiv -1 \pmod p$, et (i) est vraie. ∎

7.13.1. *Exercice.* [S 49] Soit p premier avec $p \equiv -1 \pmod 4$. En examinant la démonstration précédente, montrer que $(\frac{p-1}{2})! \equiv \pm 1 \pmod p$. Les deux valeurs 1 et -1 sont-elles possibles ?

7.13.2. *Exercice.* [S 50] Voici une autre démonstration de l'implication (ii) ⇒ (i) de 7.13 (on en trouvera d'autres plus loin, voir 14.5.4 et 14.5.5) : remarquer que si $p \equiv 1 \pmod 4$, le polynôme $X^{p-1} - 1$ est divisible par $X^2 + 1$ dans $\mathbb{Z}[X]$, et utiliser l'exercice 7.12.5.

8. Classes et actions de groupes

Théorème 8.1 *Soit G un groupe opérant à gauche sur un ensemble E, et soit $x \in E$. Alors il existe une bijection (dépendant du choix de x)*

$$\varphi : G/G_x \longrightarrow Gx$$

vérifiant, pour tout $g \in G$,

$$\varphi(gG_x) = gx.$$

Démonstration. Posons pour simplifier $H = G_x$ et considérons l'application $f : G \to Gx$ définie par $f(g) = gx$. Cette application est surjective par définition de l'orbite Gx. De plus, pour tous $h \in H$ et $g \in G$ on a $f(gh) = (gh)x = g(hx) = gx = f(g)$ de sorte que f est constante sur chaque classe gH — en d'autres termes, $f(g)$ ne dépend que de la classe de g et l'on a donc bien une application $\varphi : G/H \to Gx$ telle que $\varphi(gH) = f(g) = gx$ pour tout $g \in G$. Il est clair que l'image de φ est celle de f, c'est-à-dire que φ est surjective. Il reste à voir que φ est injective : soient donc g et $g' \in G$ vérifiant $\varphi(gH) = \varphi(g'H)$ et montrons que $gH = g'H$. Par définition de φ on a $gx = g'x$, d'où $g'^{-1}gx = x$, c'est-à-dire $g'^{-1}g \in H$ ce qui équivaut à $gH = g'H$, cf. 7.7. ∎

8.1.1. *Remarque.* Lorsque G opère *librement* sur E, on retrouve simplement le fait, déjà vu dans la preuve de 5.7 que $g \mapsto gx$ est une bijection de G sur Gx.

8.1.2. *Exercice.* Avec les notations de l'énoncé, montrer que l'application réciproque de φ associe à tout $y \in Gx$ la classe $\Gamma_{x,y} = \{g \in G \mid gx = y\}$ déjà rencontrée dans 7.7.2.

8.1.3. *Remarque.* On a naturellement une variante de 8.1 pour les actions à droite : pour G opérant à droite sur E et $x \in E$ on a une bijection $G_x\backslash G \to xG$ envoyant G_xg sur xg.

8.1.4. *Exercice.* G opère naturellement à gauche sur les deux ensembles G/G_x et Gx intervenant dans 8.1 : l'action sur Gx est induite par l'action sur E, et l'action sur G/G_x est celle de 7.9. Montrer que l'application φ est G-équivariante, et est donc un isomorphisme de G-ensembles (5.2.3).

8.1.5. *Remarque.* Les énoncés 5.5, 5.6 et 8.1 fournissent une *classification des G-ensembles à isomorphisme près* : 5.6 implique en effet que tout G-ensemble est (de façon essentiellement unique) réunion disjointe de G-ensembles non vides et *transitifs* (i.e. sur lesquels G opère transitivement) ; 8.1 affirme que tout G-ensemble non vide et transitif est isomorphe à un G-ensemble de la forme G/H, où H est un sous-groupe de G, lequel est de plus unique à conjugaison près d'après 5.5.

8.1.6. *Exercice.* [S 51] Soit H un sous-groupe de G. Appliquant 8.1 au cas où $E = G/H$ avec l'action transitive naturelle de G, et où x est la classe neutre $H = eH$, on obtient une bijection $G/H \to G/H$ puisque le stabilisateur de x est H. Quelle est cette bijection ? Plus généralement, qu'obtient-on en prenant $x = \gamma H$, pour γ donné dans G ?

8.1.7. *Exemple des actions de* $\mathbb{Z}$. Soit σ une bijection d'un ensemble E sur lui-même et considérons l'action associée de $\mathbb{Z}$ sur E, donnée (5.3.6) par $(n, x) \mapsto \sigma^n(x)$. Pour $x_0 \in E$ fixé, l'orbite de x_0 est l'ensemble $\{\sigma^n(x_0)\}_{n\in\mathbb{Z}}$. Soit $H \subset \mathbb{Z}$ le stabilisateur de x_0. Deux cas se présentent :

– ou bien l'on a $\sigma^n(x_0) \neq x_0$ pour tout $n \neq 0$, i.e. $H = \{0\}$. Alors l'orbite de x_0 est infinie, et les éléments $\sigma^n(x_0)$, pour n parcourant $\mathbb{Z}$, sont tous distincts ;

– ou bien il existe un unique entier $e > 0$ tel que $H = e\mathbb{Z}$.

Dans le second cas (automatique si E est fini, ou si σ est d'ordre fini dans $\mathfrak{S}(E)$) on dit parfois que x_0 est un *point périodique* de σ, et que e est sa *période.* L'orbite de x_0 est alors finie, et est en bijection avec $\mathbb{Z}/e\mathbb{Z}$, bijection donnée par $(n \bmod e) \mapsto \sigma^n(x_0)$. Autrement dit, l'orbite est formée des e éléments distincts $\sigma^i(x_0)$ $(0 \leq i < e)$. De plus on connaît l'action de σ sur cette orbite, donnée par

$$x_0 \mapsto \sigma(x_0) \mapsto \sigma^2(x_0) \mapsto \cdots \mapsto \sigma^{e-1}(x_0) \mapsto x_0 = \sigma^e(x_0).$$

Observer que tous les éléments de l'orbite sont aussi de période e : ils ont le même stabilisateur, mais la bijection de 8.1 n'est pas la même pour tous !

Corollaire 8.2 *Avec les hypothèses et notations de* 8.1, *on a les formules*

$$\begin{aligned} |Gx| &= (G : G_x) \\ |Gx|\,|G_x| &= |G| \end{aligned}$$

et, si G est fini, *la formule*

$$|Gx| = |G|/|G_x|.$$

Démonstration. Compte tenu de 8.1, la première formule résulte de la définition de l'indice $(G : G_x)$ (7.8). La seconde en découle par 7.5, et la troisième par 7.6. ∎

8.3. *Exercices : applications à des questions de dénombrement.*

8.3.1. *Factorielles et coefficients du binôme.* Soient k et n deux entiers avec $0 \leq k \leq n$, et soit E l'ensemble des parties à k éléments de l'ensemble $\{1, \ldots, n\}$. Le cardinal de E est noté $\binom{n}{k}$ (on rencontre aussi la notation C_n^k). Le groupe symétrique $G = \mathfrak{S}_n$ opère à gauche sur E ; montrer que cette action est *transitive.* Si X est un élément de E (par exemple $X = \{1, \ldots, k\}$), montrer que le stabilisateur de X est isomorphe à $\mathfrak{S}_k \times \mathfrak{S}_{n-k}$. En déduire que $\binom{n}{k} = |\mathfrak{S}_n|/(|\mathfrak{S}_k|.|\mathfrak{S}_{n-k}|)$.

Prenant en particulier $k = 1$, retrouver ainsi que $|\mathfrak{S}_n| = n!$; en déduire finalement la formule bien connue $\binom{n}{k} = n!/(k!(n-k)!)$. (On s'assurera, bien entendu, que ces formules n'ont pas été utilisées dans la démonstration...)

8.3.2. *Groupe linéaire sur un corps fini.* Soit K un corps fini, et posons $q = |K|$. Pour $n \in \mathbb{N}$, posons $G_n = \mathrm{GL}(n, K)$. On a évidemment $G_0 = \{\mathrm{Id}\}$, et G_1 est canoniquement isomorphe à $(K^*, \times)$; dans la suite on supposera que $n \geq 1$.

Considérons l'action à gauche naturelle de G_n sur K^n et le vecteur $v \in K^n$ de coordonnées $(1, 0, \ldots, 0)$: remarquer que l'orbite de v est $K^n - \{0\}$, et que le stabilisateur de v est le groupe des matrices $(a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ de $\mathrm{M}(n, K)$ telles que :

- $a_{1,1} = 1$;
- $a_{i,1} = 0$ pour tout $i \geq 2$;
- la matrice $(a_{i,j})_{i,j \geq 2}$ de $\mathrm{M}(n-1, K)$ est inversible.

On en déduit la formule de récurrence $|G_n| = (q^n - 1)\, q^{n-1}\, |G_{n-1}|$ et finalement la formule $|G_n| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$. Il faut espérer que ce résultat soit le même que celui de l'exercice 1.4.9 : vérifiez !

8.3.3. *Groupe linéaire sur un corps fini (bis).* Voici une variante de la méthode précédente. Si E est un espace vectoriel de dimension finie d sur un corps K, appelons *drapeau complet* dans E toute suite $\underline{D} = (D_0 \subset D_1 \subset \ldots \subset D_d)$ de sous-espaces de E avec $\dim D_i = i$ pour tout i (on a donc en particulier $D_0 = \{0\}$ et $D_d = E$). Il est clair que $\mathrm{GL}(E)$ opère à gauche sur l'ensemble $\Delta(E)$ des drapeaux complets de E. Montrer que cette action est transitive. (Remarquer par exemple que pour chaque drapeau $\underline{D}$ comme ci-dessus il existe une base de E dont les i premiers vecteurs, pour chaque i, engendrent D_i). Montrer que le stabilisateur d'un drapeau convenable de K^n est le sous-groupe T_n de $\mathrm{GL}(n, K)$ formé des matrices triangulaires supérieures.

Reprenant alors K et n comme dans 8.3.2, montrer que $|T_n| = (q-1)^n\, q^{n(n-1)/2}$, et d'autre part calculer le nombre δ_n de drapeaux complets de K^n par récurrence sur n (méthode : l'ensemble des $\underline{D}$ avec D_1 fixé s'identifie à l'ensemble $\Delta(E/D_1)$, donc a δ_{n-1} éléments ; d'autre part il y a $\frac{q^n-1}{q-1}$ droites dans K^n). Retrouver ainsi la formule de l'exercice précédent.

Corollaire 8.4 (« formule des orbites », ou « formule des classes ») *Soit G un groupe* fini *opérant sur un ensemble* fini *E. Soient $X_1, \ldots, X_r$ les orbites (distinctes) de E sous G et, pour chaque $i \in \{1, \ldots, r\}$, soit x_i un élément de X_i. Alors on a*

$$|E| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} (G : G_{x_i}) = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}.$$

Démonstration. La première égalité résulte de 5.6, les autres de 8.1 et 7.6. ∎

Cette formule a de nombreuses applications ; à titre d'exemple, et pour terminer ce paragraphe, nous allons l'appliquer à l'étude des « p-groupes ».

Définition 8.5 *Soit p un nombre* premier. *Un p-*groupe *est par définition un groupe fini dont l'ordre est une puissance de p.*

8.5.1. *Remarque.* Ne pas oublier que le groupe trivial est un p-groupe pour tout p (il est d'ordre p^0).

Proposition 8.6 *Soient p un nombre premier et G un p-groupe opérant à gauche sur un ensemble fini E. Notons E^G l'ensemble des points fixes de E sous G. Alors on a*

$$|E^G| \equiv |E| \pmod{p}.$$

Démonstration. Pour toute orbite X, on sait que $|X|$ divise $|G|$ donc est une puissance de p. En particulier $|X|$ est soit égal à 1, soit divisible par p. De plus la réunion des orbites à un élément est évidemment E^G. La formule des orbites donne donc le résultat. ∎

8.6.1. *Question.* [S 52] Où a servi le fait que p est premier ?

8.6.2. *Exercice.* [S 53] Pour p premier, $s \in \mathbb{N}$, et k entier vérifiant $0 < k < p^s$, appliquer 8.6 à l'action de $G = \mathbb{Z}/p^s\mathbb{Z}$ par translation sur l'ensemble des parties à k éléments de G ; en déduire la congruence bien connue $\binom{p^s}{k} \equiv 0 \pmod{p}$. Où a servi l'hypothèse sur k ? On n'a pas supposé que $s > 0$: n'est-ce pas bizarre ? Où a servi le choix de $\mathbb{Z}/p^s\mathbb{Z}$ (plutôt que n'importe quel groupe d'ordre p^s) ?

Corollaire 8.7 *Soient p un nombre premier et G un p-groupe non trivial. Alors le centre de G n'est pas réduit à l'élément neutre.*

Démonstration. Appliquons 8.6 à l'action de G sur lui-même par conjugaison : ici $|E| = |G|$ est divisible par p, donc il en est de même de $|E^G|$ qui n'est donc pas réduit à un élément. Or E^G n'est autre que le centre de G (immédiat sur la définition), d'où la conclusion. ∎

9. Sous-groupes distingués, groupes quotients

Proposition 9.1 *Soit H un sous-groupe d'un groupe G. Les conditions suivantes sont équivalentes :*

(i) *pour tout $x \in G$, $xHx^{-1} = H$;*

(ii) *pour tout $x \in G$, $xHx^{-1} \subset H$;*

(iii) *pour tout $x \in G$, $xH = Hx$;*

(iv) *toute classe à gauche modulo H est aussi une classe à droite ;*

(v) *toute classe à droite modulo H est aussi une classe à gauche.*

Démonstration. Il est trivial que (i) implique (ii) ; réciproquement, si (ii) est vérifiée et si $x \in G$ on a $xHx^{-1} \subset H$ mais aussi $x^{-1}Hx \subset H$ en « appliquant (ii) à x^{-1} », ce qui donne l'inclusion $H \subset xHx^{-1}$ et l'égalité, d'où (i).

Il est clair que (i) $\iff$ (iii), et que (iii) implique (iv) et (v). Montrons enfin que (iv) implique (iii) (la preuve de (v)$\Rightarrow$(iii) est tout analogue) : si (iv) est vrai et si $x \in G$, xH est une classe à gauche par définition, donc une classe à droite d'après (iv), et comme x en est un élément c'est la classe à droite de x, i.e. $xH = Hx$, cqfd. ∎

9.1.1. *Question.* [S 54] A-t-on véritablement prouvé l'équivalence de toutes les propriétés énoncées ? Par exemple, d'où sort l'implication (iv)$\Rightarrow$(ii) ? Comment s'assurer commmodément, dans ce genre de situation (très fréquente !) si aucune implication ne manque ?

Définition 9.2 *Un sous-groupe H d'un groupe G est dit* distingué *s'il vérifie les conditions équivalentes de* 9.1.

9.3. *Commentaires.*

9.3.1. On rencontre aussi dans la littérature les mots « invariant » ou « normal » au lieu de « distingué ». On note parfois

$$H \lhd G$$

pour « H est un sous-groupe distingué de G ».

9.3.2. En pratique, pour vérifier directement qu'un sous-groupe H est distingué, on utilise la propriété (ii) de 9.1 : autrement dit, on vérifie que, pour tout $h \in H$ et tout $x \in G$, xhx^{-1} appartient à H. Une erreur courante chez les débutants est d'essayer de montrer, avec ces notations, que $xhx^{-1} = h$, ce qui n'est évidemment (?) pas la même chose : comme on le vérifie immédiatement, cette dernière propriété signifie que H est contenu dans le centre de G.

9.3.3. *Exemples triviaux.* Il est clair que $\{e\}$ et G sont distingués, que tout sous-groupe de G est distingué si G est commutatif, que l'intersection d'une famille quelconque de sous-groupes distingués est distinguée.

Ne pas oublier de préciser « distingué *dans* G » s'il peut y avoir confusion.

9.3.4. *Noyaux, images réciproques.* L'exercice 7.7.1, ou une vérification immédiate, montre que *le noyau d'un morphisme est automatiquement distingué* ; la réciproque arrive, cf. 9.4. Plus généralement (encore immédiat) si $f : G \to G'$ est un morphisme et H' un sous-groupe distingué de G', alors $f^{-1}(H')$ est distingué dans G.

9.3.5. *Contre-exemples, images.* [S 55] L'exercice 7.7.2 fournit en revanche des exemples de sous-groupes non distingués, et donc de sous-groupes qui ne peuvent être des noyaux. Par la même occasion il montre *très simplement* que l'image, par un morphisme $G \to G'$, d'un sous-groupe distingué de G n'est pas nécessairement un sous-groupe distingué de G' : voyez-vous comment ?

9.3.6. *Sous-groupes d'indice 2.* Ils sont automatiquement distingués, comme le montre l'exercice 7.8.1.

L'intérêt de la notion de sous-groupe distingué réside principalement dans l'énoncé suivant :

Proposition 9.4 *Soit H un sous-groupe d'un groupe G. Notons $\sim$ la relation d'équivalence définie par les classes à gauche modulo H* (autrement dit : $x \sim x'$ si et seulement si $xH = x'H$)*, et $\pi : G \to G/H$ l'application canonique. Les conditions suivantes sont équivalentes :*

(i) *H est distingué dans G ;*

(ii) *la relation $\sim$ est compatible avec la loi de G, i.e. si $x \sim x'$ et $y \sim y'$ alors $xy \sim x'y'$;*

(iii) *il existe sur G/H une loi de composition interne (notée provisoirement $*$) qui fait de π un morphisme, i.e. $\pi(xy) = \pi(x) * \pi(y)$ pour tous x,$y \in G$.*

Si ces conditions sont vérifiées, la loi de (iii) *est unique et fait de G/H un groupe, appelé* groupe quotient *de G par H. Le noyau du morphisme $\pi : G \to G/H$ est H.*

Démonstration. Montrons que (i) implique (ii) : supposons que H soit distingué et que $x \sim x'$ et $y \sim y'$ avec $x, y, x', y' \in G$. On a donc $x' \in xH$ et $y' \in yH$, d'où $x'y' \in xHyH$. Or $Hy = yH$ d'où $x'y' \in xyHH = xyH$, cqfd.

Montrons que (ii) implique (iii) (l'équivalence de (ii) et (iii) s'étend d'ailleurs à tout ensemble muni d'une loi interne et d'une relation d'équivalence). La propriété (ii) signifie que, pour x et $y \in G$, la classe de xy ne dépend que des classes de x et de y. En d'autres termes, si α et $\beta \in G/H$, il existe $\gamma \in G/H$ tel que si $\pi(x) = \alpha$ et $\pi(y) = \beta$ alors $\pi(xy) = \gamma$. Posant $\alpha * \beta = \gamma$, on a bien la propriété (iii).

Il est clair d'ailleurs que la loi ainsi définie est la seule possible ; c'est l'assertion d'unicité de l'énoncé, qui provient essentiellement du fait que π est surjectif. Avant de montrer que (iii) implique (i), notons aussi qu'il est immédiat, supposant (iii), que G/H est un groupe (exercice, qui utilise encore la surjectivité de π). En outre, l'élément neutre de G/H est la classe de e_G, c'est-à-dire H, de sorte que $\mathrm{Ker}\,\pi = \pi^{-1}(\pi(e_G)) = H$.

L'implication (iii)⇒(i) est dès lors claire : nous venons de voir que si (iii) est vérifiée, H est le noyau d'un morphisme, donc est distingué (9.3.4). ∎

9.4.1. *Question.* La même qu'en 9.1.1 ; le lecteur observera ici l'intérêt « économique » d'une stratégie circulaire comme (i)⇒(ii)⇒(iii)⇒(i).

9.4.2. *Remarque.* La loi de groupe sur G/H est en général, s'il n'y a pas de confusion, notée comme celle de G. Voici d'ailleurs une jolie ambiguïté : si α et $\beta \in G/H$, alors $\alpha\beta$ désigne à la fois le produit dans G/H des classes α et β (qui est encore une classe, donc une partie de G) et une partie de G selon la notation de 7.1. Est-ce la même chose ? [S 56]

9.4.3. *Cas triviaux.* Si $H = G$ alors G/H est un groupe trivial ; si $H = \{e\}$ alors π est un isomorphisme.

9.4.4. Un exemple bien connu de groupe quotient est le groupe $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo n (entier fixé), dont la notation s'explique désormais. On rappelle aussi que tout sous-groupe d'un groupe *commutatif* est distingué, de sorte que dans le cas commutatif, on a toujours une structure naturelle de groupe sur le quotient.

9.4.5. *Exercice.* [S 57] Soit G un groupe. Montrer que toute relation d'équivalence $\sim$ sur G compatible avec la loi de G est du type décrit en 9.4, pour un unique sous-groupe distingué H de G que l'on précisera.

9.4.6. *Espaces vectoriels quotients.* Soient V un espace vectoriel sur un corps K, et W un sous-espace de V. Alors il existe sur le groupe quotient V/W une structure de K-espace vectoriel tel que le morphisme canonique $\pi : V \to V/W$ soit K-linéaire. En effet, la seule chose à définir est la multiplication, par un scalaire $\lambda \in K$, d'une classe $\alpha \in V/W$; il suffit pour cela de remarquer que, pour $v \in V$, la classe de λv modulo W ne dépend que de la classe de v. Le fait que V/W, muni de la loi de groupe quotient et de la multiplication externe ainsi définie, est un K-espace vectoriel, se réduit à des vérifications de routine, et la linéarité de π est claire par construction de la loi externe. L'espace V/W ainsi construit est naturellement appelé *l'espace vectoriel quotient* de V par W.

Corollaire 9.5 *Soit H un sous-groupe d'un groupe G. Les conditions suivantes sont équivalentes :*

(i) *H est distingué dans G ;*

(ii) *il existe un groupe G' et un morphisme surjectif $f : G \to G'$ tels que $H =$* Ker (f) *;*

(iii) *il existe un groupe G' et un morphisme $f : G \to G'$ tels que $H =$* Ker (f).

Démonstration. Les implications (ii)⇒(iii) et (iii)⇒(i) sont immédiates, et l'implication (i)⇒(ii) résulte de la dernière assertion de 9.4. ∎

9.5.1. *Exercice.* [S 58] Un groupe non trivial G est dit *simple* si les seuls sous-groupes distingués de G sont $\{e\}$ et G. (Voir aussi le §18).

Montrer qu'un groupe *commutatif* non trivial est simple si et seulement si il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ où p est premier.

Montrer qu'un groupe G est simple si et seulement si, pour tout groupe H, tout morphisme de G dans H est trivial ou injectif.

9.5.2. *Remarque.* Un théorème célèbre (et pas très difficile) de Galois dit que pour $n \geq 5$ le *groupe alterné* A_n est simple (cf. 9.5.1).

Par contre A_4 n'est pas simple : il admet un sous-groupe distingué d'ordre 4, formé de l'identité et des produits de deux transpositions disjointes.

9.5.3. *Exercice.* [S 59] Déduire du théorème de Galois mentionné en 9.5.2 ci-dessus que, pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{S}_n$ et A_n.

Théorème 9.6 (« propriété universelle du quotient »). *Soit H un sous-groupe distingué d'un groupe G, et soit $\pi : G \to G/H$ le morphisme canonique. D'autre part soit $f : G \to \Gamma$ un morphisme de groupes. Les conditions suivantes sont équivalentes :*

(i) *f se factorise par G/H ; i.e. il existe un morphisme de groupes $\overline{f} : G/H \to \Gamma$ tel que $f = \overline{f} \circ \pi$;*

(ii) *$f(H) = \{e_\Gamma\}$;*

(iii) *$H \subset$* Ker f.

Si ces conditions sont vérifiées, le morphisme $\overline{f}$ de (i) *est unique ; son image est celle de f, et son noyau est* (Ker $f)/H$.

Démonstration. L'équivalence de (ii) et (iii) résulte de la définition du noyau, et l'implication (i)⇒(ii) est immédiate puisque $\pi(H) = \{e_{G/H}\}$. D'autre part l'assertion d'unicité de $\overline{f}$ est conséquence de la surjectivité de π, ainsi que le fait que son image est celle de f.

Il reste à voir que (ii) implique (i), ainsi que l'assertion finale sur le noyau de $\overline{f}$ (mais bien sûr vous avez déjà vérifié qu'elle a un sens, c'est-à-dire que (Ker $f)/H$ est bien un sous-groupe de G/H).

Supposons donc (ii) vérifiée. Alors, si $x \in G$ et $h \in H$, on a $f(xh) = f(x)f(h) = f(x)$. En d'autres termes, f est constante sur chaque classe modulo H. Pour toute

classe $\alpha \in G/H$, définissons alors $\overline{f}(\alpha)$ comme la valeur commune des $f(x)$ pour $x \in \alpha$: alors, on a par construction $f = \overline{f} \circ \pi$. Le fait que $\overline{f}$ soit un morphisme résulte alors aisément de la définition, ou bien du fait que $\overline{f} \circ \pi$ est un morphisme et que π est surjectif.

Enfin, pour $\alpha \in G/H$, classe de $x \in G$, pour que $\alpha \in \operatorname{Ker} \overline{f}$ il faut et il suffit que $f(x) = e_\Gamma$, ou encore que $x \in \operatorname{Ker} f$, ce qui achève la démonstration. ∎

9.6.1. *Exercice.* Énoncer et démontrer une propriété universelle analogue pour les espaces vectoriels quotients, les applications linéaires remplaçant les morphismes de groupes.

9.7. *Commentaires.*

9.7.1. Le point essentiel de l'énoncé précédent est naturellement le fait que (ii) (ou (iii)) implique (i). Cette propriété est souvent présentée de la façon suivante : *étant donnés f, H et π comme dans* 9.6, *le diagramme*

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ & \searrow^{f} & \\ & & \Gamma \end{array}$$

se prolonge de façon unique en un diagramme commutatif

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ & \searrow^{f} \quad \swarrow_{\overline{f}} & \\ & \Gamma. & \end{array}$$

9.7.2. Le mot « commutatif » correspond naturellement à la condition $f = \overline{f} \circ \pi$ de l'énoncé. Cette présentation a sans doute l'avantage d'être plus « visuelle » que l'énoncé brut. Elle exige seulement quelques précautions d'utilisation. Il faut d'abord bien distinguer le premier diagramme (qui rassemble les données) du second (qui montre ce que l'on construit). Il faut aussi s'assurer que lesdites données ont bien été *définies*, ainsi que les conditions imposées au résultat. Il faut enfin être conscient des hypothèses tacites (ici, par exemple, le fait que toutes les flèches représentent des morphismes de groupes).

Pour résumer, un diagramme n'est pas une incantation ; essayer d'utiliser ce type de présentation (ou un autre !) sans en comprendre le **sens** ne peut conduire qu'à révéler cette incompréhension.

9.7.3. À titre d'exercice, voici une autre manière de présenter 9.6 : étant donnés f, H et π comme dans l'énoncé, on considère l'application

$$\begin{array}{rccc} \alpha : & \operatorname{Hom}_{\text{groupes}}(G/H, \Gamma) & \longrightarrow & \operatorname{Hom}_{\text{groupes}}(G, \Gamma) \\ & u & \longmapsto & u \circ \pi. \end{array}$$

Alors α induit une bijection entre $\mathrm{Hom}_{\text{groupes}}(G/H, \Gamma)$ et l'ensemble des morphismes $f \in \mathrm{Hom}_{\text{groupes}}(G, \Gamma)$ dont le noyau contient H.

Théorème 9.8 *Soit $f : G \to G'$ un morphisme de groupes. Alors on a un isomorphisme naturel*

$$\varphi : G/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f.$$

caractérisé par la propriété suivante : pour tout $g \in G$, on a, en posant $H = \mathrm{Ker}\, f$,

$$\varphi(gH) = f(g).$$

En particulier, si f est surjectif, alors G' est isomorphe à $G/\mathrm{Ker}\, f$.

Démonstration. Appliquons le théorème 9.6 avec $\Gamma = G'$ et $H = \mathrm{Ker}\, f$. Il est clair que la condition (iii) est vérifiée ; donc f se factorise par un morphisme $\overline{f} : G/H \to G'$.

On a bien la formule $\overline{f}(gH) = f(g)$: c'est la condition $f = \overline{f} \circ \pi$ de 9.6.

De plus $\mathrm{Ker}\, \overline{f}$ est un groupe *trivial* (c'est le quotient de $\mathrm{Ker}\, f$ par lui-même) de sorte que $\overline{f}$ est injectif. Il induit donc une bijection φ (donc un isomorphisme, puisque c'est un morphisme) de G/H sur son image, laquelle n'est autre que $\mathrm{Im}\, f$ comme on l'a vu. ∎

9.8.1. *Remarque.* L'énoncé ci-dessus révèle toute la puissance de la notion de quotient puisque, grâce à elle, on « connaît » (à isomorphisme près) l'image d'un morphisme dès qu'on en connaît la source et le noyau.

9.8.2. *Remarque.* Bien entendu, si G est fini, on obtient notamment l'égalité $|\mathrm{Im} f| = |G|/|\mathrm{Ker}\, f|$, très souvent utilisée pour calculer l'ordre d'un groupe. Par exemple, on retrouve le fait que, pour $n \geq 2$, le groupe alterné A_n est d'ordre $n!/2$ (cf. 6.10.6).

9.8.3. *Remarque.* Notons φ l'isomorphisme construit dans 9.8. Alors φ est *caractérisé* par la propriété suivante : le morphisme f de départ est égal au composé

$$G \xrightarrow{\pi} G/\mathrm{Ker}\, f \xrightarrow{\varphi} \mathrm{Im}\, f \xrightarrow{i} G'$$

où π est la surjection canonique de G sur $G/\mathrm{Ker}\, f$, et i le morphisme d'inclusion de $\mathrm{Im}\, f$ dans G'.

9.8.4. *Exercice.* L'isomorphisme de 9.8 est en particulier une bijection de $G/\mathrm{Ker}\, f$ sur $\mathrm{Im}\, f$. Montrer que c'est un cas particulier de 8.1. (Considérer l'action de G sur G' donnée par $(g, g') \mapsto f(g)g'$).

9.8.5. *Exemples triviaux.* Lorsque f est injectif, on trouve que $\mathrm{Im}\, f$ est isomorphe à G ce qui, j'espère, n'est pas une surprise.

On trouve aussi (ce qui n'est guère plus glorieux) que $\mathrm{Ker}\, f = G$ si et seulement si $\mathrm{Im}\, f = \{e_{G'}\}$, ou encore si et seulement si f est le morphisme trivial.

9.8.6. *Exemple.* Soit γ un élément d'un groupe G, et considérons le morphisme $\varphi : \mathbb{Z} \to G$ défini par $\varphi(k) = \gamma^k$. Son image est par définition le sous-groupe $\langle\gamma\rangle$ engendré par γ, et son noyau est un sous-groupe de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$ pour un unique entier $n \geq 0$ (3.6). On trouve donc un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $\langle\gamma\rangle$. *Exercice :* quel est le lien entre n et l'ordre de γ ? [S 60] Retrouver ainsi tous les résultats de 3.11.

9.8.7. *Exemple.* L'application $z \mapsto e^{2i\pi z}$ est un morphisme de groupes de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$, qui est de plus surjectif et dont le noyau est $\mathbb{Z}$. On en conclut que le groupe additif $\mathbb{C}/\mathbb{Z}$ est isomorphe au groupe multiplicatif $\mathbb{C}^*$. Le même morphisme induit d'ailleurs un isomorphisme entre $(\mathbb{R}/\mathbb{Z}, +)$ et le groupe multiplicatif des nombres complexes de module 1.

9.8.8. *Exercice.* [I 23] Soient G un groupe et C son centre (3.3.10). Montrer que C est distingué dans G ainsi que tous ses sous-groupes, et que G/C est isomorphe au groupe des automorphismes intérieurs de G (2.4.3).

9.8.9. *Exercice.* [I 24][S 61] Soient G un groupe et $G' = [G, G]$ son sous-groupe des commutateurs (cf. 4.4.9). Montrer que G' est distingué dans G et que G/G' est commutatif. Plus généralement, montrer qu'un sous-groupe distingué H de G contient G' si et seulement si G/H est commutatif. (Autrement dit, G/G' est le « plus grand quotient commutatif » de G ; on l'appelle parfois *l'abélianisé* de G).

Montrer enfin que le morphisme canonique $G \to G/G'$ est « universel pour les morphismes de G vers les groupes commutatifs », au sens suivant : pour tout morphisme $f : G \to \Gamma$ vers un groupe commutatif Γ, il existe un unique morphisme $\overline{f} : G/G' \to \Gamma$ tel que $f = \overline{f} \circ \pi$.

9.8.10. *Exercice : sous-groupe distingué engendré par une partie.* Soit S un sous-ensemble d'un groupe G. Notons $\langle\langle S\rangle\rangle$ l'intersection de tous les sous-groupes distingués de G contenant S ; on l'appelle le sous-groupe distingué de G engendré par S.

En s'inspirant (notamment) du paragraphe 4, montrer que :

(1) $\langle\langle S\rangle\rangle$ est le plus petit sous-groupe distingué de G contenant S ;

(2) $\langle\langle S\rangle\rangle$ est le sous-groupe de G engendré par $S' := \bigcup_{x\in G} xSx^{-1}$;

(3) soit $\pi : G \to G/\langle\langle S\rangle\rangle$ le morphisme canonique. Alors Ker (π) contient S, et tout morphisme de groupes $f : G \to G'$ dont le noyau contient S se factorise de façon unique par π ;

(4) on a les implications : S est invariant par conjugaison $\Rightarrow \langle S\rangle \lhd G \Leftrightarrow \langle\langle S\rangle\rangle = \langle S\rangle$. La réciproque de la première implication est-elle vraie ?

9.8.11. *Exercice : normalisateur d'un sous-groupe.* Soit H un sous-groupe d'un

groupe G. On définit le *normalisateur* $N_G(H)$ de H dans G par

$$N_G(H) = \{x \in G \mid xHx^{-1} = H\}.$$

Montrer que $N_G(H)$ est un sous-groupe de G contenant H et dans lequel H est distingué, et que c'est le plus grand sous-groupe de G ayant ces propriétés.

Montrer que le centralisateur $Z_G(H)$ de H dans G (cf. 3.3.8) est un sous-groupe distingué de $N_G(H)$, et que le quotient $N_G(H)/Z_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(H)$.

9.8.12. *Exercice.* Soient K un corps, n un entier ≥ 0, $G = \mathrm{GL}(n, K)$, D le sous-groupe de G formé des matrices diagonales. Décrire $N_G(D)$ et $Z_G(D)$, et montrer que $N_G(D)/Z_G(D)$ est « presque toujours » isomorphe à $\mathfrak{S}_n$.

10. Sous-groupes d'un groupe et de ses quotients

On se propose d'étudier le lien entre les sous-groupes d'un groupe G et ceux d'un groupe quotient G/H de G. Nous allons en fait travailler dans un cadre un peu plus général : dans tout ce paragraphe on se donne un morphisme *surjectif* de groupes

$$\pi : G \twoheadrightarrow G'$$

(la flèche $\twoheadrightarrow$ est utilisée pour noter une application surjective), et l'on pose

$$H = \mathrm{Ker}\, \pi$$

qui est donc un sous-groupe distingué de G. Cette situation contient naturellement le cas particulier où $G' = G/H$, et 9.8 montre qu'il suffirait d'étudier ce cas pour en déduire le cas général ; on suggère au lecteur d'expliciter, en termes de classes modulo H, les énoncés et les démonstrations ci-dessous lorsque $G' = G/H$. (Pour les plus importants, ce sera d'ailleurs fait en fin de paragraphe).

Proposition 10.1 *Soit Δ un sous-groupe de G'. Alors $\pi^{-1}(\Delta)$ est un sous-groupe de G contenant H, et l'on a $\pi(\pi^{-1}(\Delta)) = \Delta$.*

De plus on a un isomorphisme canonique

$$\pi^{-1}(\Delta)/H \xrightarrow{\sim} \Delta.$$

Enfin, pour que Δ soit distingué dans G', il faut et il suffit que $\pi^{-1}(\Delta)$ soit distingué dans G. De plus, si tel est le cas, on a un isomorphisme canonique de groupes

$$G/\pi^{-1}(\Delta) \xrightarrow{\sim} G'/\Delta.$$

Démonstration. La première assertion est évidente, et l'égalité $\pi(\pi^{-1}(\Delta)) = \Delta$ résulte de la surjectivité de π.

En particulier π induit un morphisme *surjectif* de $\pi^{-1}(\Delta)$ sur Δ, dont le noyau est évidemment $\pi^{-1}(\Delta) \cap \mathrm{Ker}\, \pi = \pi^{-1}(\Delta) \cap H = H$. D'après 9.8 on en déduit l'isomorphisme annoncé $\pi^{-1}(\Delta)/H \xrightarrow{\sim} \Delta$.

On sait déjà que si $\Delta \lhd G'$, alors $\pi^{-1}(\Delta) \lhd G$. Pour la réciproque le plus simple est d'appliquer les définitions (d'ailleurs ça ne fait pas de mal, de temps en temps) : supposons donc que $\pi^{-1}(\Delta) \lhd G$, soient $\delta' \in \Delta$ et $x' \in G'$, et montrons que $x'^{-1}\delta' x' \in \Delta$. Comme π est surjectif il existe x et δ dans G tels que $\pi(x) = x'$ et $\pi(\delta) = \delta'$. On a donc $\delta \in \pi^{-1}(\Delta)$ par définition de l'image réciproque (que vous devriez connaître, maintenant) d'où $x^{-1}\delta x \in \pi^{-1}(\Delta)$ qui est distingué, d'où $x'^{-1}\delta' x' = \pi(x^{-1}\delta x) \in \Delta$, cqfd.

Enfin supposons que $\Delta \lhd G'$, de sorte que $\pi^{-1}(\Delta) \lhd G$ comme on vient de le voir. Considérons le morphisme composé $G \overset{\pi}{\twoheadrightarrow} G' \overset{\rho}{\twoheadrightarrow} G'/\Delta$ où ρ désigne le morphisme canonique de passage au quotient. Ce morphisme est surjectif comme composé de deux

surjections, et de plus son noyau est l'ensemble des $g \in G$ tels que $\pi(g) \in \operatorname{Ker}\rho$, c'est-à-dire $\pi^{-1}(\Delta)$ puisque $\operatorname{Ker}\rho = \Delta$. On peut donc conclure à nouveau par 9.8. ∎

10.1.1. *Exercice.* Soit $[G,G]$ le sous-groupe des commutateurs de G (cf. 4.4.9 et 9.8.9). Utilisant le fait que $G/[G,G]$ est commutatif, déduire de 10.1 que tout sous-groupe de G contenant $[G,G]$ est distingué. Montrer ensuite ce résultat directement.

Proposition 10.2 *Soit Γ un sous-groupe de G. Alors $\pi(\Gamma)$ est un sous-groupe de G', et l'on a $\pi^{-1}(\pi(\Gamma)) = H\Gamma = \Gamma H$.*

De plus $\Gamma \cap H$ est distingué dans Γ, et on a des isomorphismes canoniques

$$\Gamma/\Gamma \cap H \xrightarrow{\sim} \Gamma H/H \xrightarrow{\sim} \pi(\Gamma).$$

Démonstration. On sait déjà que $\pi(\Gamma)$ est un sous-groupe de G'. D'autre part, $\pi^{-1}(\pi(\Gamma))$ contient H d'après 10.1 appliqué à $\Delta = \pi(\Gamma)$, et contient aussi Γ (c'est un fait général et facile). Comme c'est un sous-groupe il contient donc $H\Gamma$ et ΓH. Inversement montrons que $\pi^{-1}(\pi(\Gamma)) \subset H\Gamma$. Soit $x \in G$ tel que $\pi(x) \in \pi(\Gamma)$: il existe donc $\gamma \in \Gamma$ tel que $\pi(x) = \pi(\gamma)$, ce qui signifie que $x\gamma^{-1} \in \operatorname{Ker}\pi$, ou encore $x \in H\gamma \subset H\Gamma$, cqfd. L'inclusion $\pi^{-1}(\pi(\Gamma)) \subset \Gamma H$ se démontre de la même façon (en remplaçant « $x\gamma^{-1} \in \operatorname{Ker}\pi$ » par « $\gamma^{-1}x \in \operatorname{Ker}\pi$ »).

Appliquant la proposition 10.1 à $\Delta = \pi(\Gamma)$, on obtient (puisque $\pi^{-1}(\Delta) = \pi^{-1}(\pi(\Gamma)) = \Gamma H$) un isomorphisme canonique $\Gamma H/H \xrightarrow{\sim} \pi(\Gamma)$, induit par la restriction de π à ΓH.

Enfin, le morphisme $\rho : \Gamma \hookrightarrow \Gamma H \to \Gamma H/H$, composé de l'injection et de la surjection naturelles, a évidemment pour noyau $\Gamma \cap H$; pour trouver un isomorphisme $\Gamma/\Gamma \cap H \xrightarrow{\sim} \Gamma H/H$ il suffit de voir que ρ est surjectif. C'est clair soit directement (tout élément de ΓH appartient à la classe modulo H d'un élément de Γ), soit parce que le composé de ρ avec l'isomorphisme $\Gamma H/H \xrightarrow{\sim} \pi(\Gamma)$ est la surjection naturelle de Γ sur $\pi(\Gamma)$. ∎

10.2.1. *Remarque.* Les égalités $\pi^{-1}(\pi(\Gamma)) = H\Gamma = \Gamma H$ sont vraies pour toute partie Γ de G, pas seulement pour les sous-groupes.

10.2.2. *Remarque.* Si K et Γ sont deux sous-groupes quelconques de G, il est faux en général que $K\Gamma$ (ou ΓK) soit un sous-groupe. La proposition ci-dessus montre que c'est vrai si $K \lhd G$ (ou si $\Gamma \lhd G$, par symétrie) puisqu'il suffit de l'appliquer au morphisme canonique de G dans G/K. *Exercice :* le démontrer directement à partir de la définition d'un sous-groupe distingué.

Le théorème suivant rassemble l'essentiel des propositions 10.1 et 10.2 :

Théorème 10.3 *Les applications*

$$\begin{array}{ccc} \Gamma & \longmapsto & \pi(\Gamma) \\ \Delta & \longmapsto & \pi^{-1}(\Delta) \end{array}$$

sont des bijections réciproques l'une de l'autre entre l'ensemble des sous-groupes de G' et l'ensemble des sous-groupes de G contenant H.

Ces bijections respectent les inclusions et les intersections, et transforment sous-groupes distingués en sous-groupes distingués.

Enfin, si Δ est un sous-groupe distingué de G', on a un isomorphisme canonique de groupes

$$G/\pi^{-1}(\Delta) \xrightarrow{\sim} G'/\Delta.$$

Démonstration. Pour la première assertion il s'agit de voir que :

(1) si Δ est un sous-groupe de G', alors $\pi(\pi^{-1}(\Delta)) = \Delta$: or on l'a vu dans 10.1 ;

(2) si Γ est un sous-groupe de G contenant H, alors $\pi^{-1}(\pi(\Gamma)) = \Gamma$; mais ceci résulte de 10.2 puisqu'ici on a $H\Gamma = \Gamma$.

Que ces applications respectent les inclusions et les intersections est un petit exercice purement ensembliste. Les autres assertions ont déjà été vues. ∎

10.4. *Exemple : sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.* Soit n un entier : on déduit de 10.3 que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $H/n\mathbb{Z}$, où H est un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Un tel H est nécessairement de la forme $d\mathbb{Z}$, où d est un diviseur de n, uniquement déterminé par H si on lui impose de plus d'être ≥ 0. On trouve ainsi que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, où d parcourt les diviseurs de n. Remarquer d'ailleurs que comme sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, $d\mathbb{Z}/n\mathbb{Z}$ est simplement le sous-groupe engendré par la classe de d modulo n. Comme cette classe est d'ordre n/d (exercice !) on voit que $d\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/(n/d)\mathbb{Z}$.

Théorème 10.5 *Soient H et K deux sous-groupes distingués d'un groupe G. On suppose que $H \subset K$. Alors K/H est distingué dans G/H, et il existe un isomorphisme naturel*

$$(G/H)/(K/H) \xrightarrow{\sim} G/K.$$

Démonstration. C'est un cas particulier de 10.1 (prendre $G' = G/H$ et $\Delta = K/H$). ∎

10.5.1. *Exemple.* Revenant aux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (10.4) on voit par exemple que si d divise n, le quotient $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. (En particulier $d\mathbb{Z}/n\mathbb{Z}$ est d'indice d dans $\mathbb{Z}/n\mathbb{Z}$ mais ceci pouvait déjà se déduire de 7.6).

Théorème 10.6 *Soient H et Γ deux sous-groupes d'un groupe G. On suppose que H est distingué dans G. Alors :*

(i) $H\Gamma = \Gamma H$, *et* $H\Gamma$ *est un sous-groupe de* G ;

(ii) $\Gamma \cap H$ *est distingué dans* Γ, *et il existe un isomorphisme naturel*

$$\Gamma/(\Gamma \cap H) \xrightarrow{\sim} (\Gamma H)/H$$

.

Démonstration. Cela résulte de 10.2 en prenant $G' = G/H$. ∎

10.6.1. *Remarque.* Dans les deux théorèmes ci-dessus, on s'est contenté d'expliciter certains des résultats précédents dans le cas où $G' = G/H$. C'est sous cette forme que les résultats de ce paragraphe apparaissent le plus souvent dans la littérature ; les théorèmes ainsi formulés présentent l'avantage, *et le danger,* de pouvoir se condenser en des « formules » faciles (?) à mémoriser.

11. Compléments sur les groupes abéliens

11.1. *Conventions et rappels.* Dans ce paragraphe, tous les groupes abéliens seront notés *additivement*, sauf mention contraire. En particulier l'élément neutre d'un groupe abélien A est noté 0_A, ou 0 s'il n'y a pas de confusion, et le symétrique d'un élément x de A est noté $-x$.

Si A et B désignent deux groupes abéliens, l'ensemble des morphismes de groupes de A dans B sera simplement noté $\mathrm{Hom}(A,B)$. L'addition dans B munit cet ensemble d'une loi *interne* (contrairement à ce qui se passe pour les groupes généraux, cf. 2.2.4) encore notée additivement : la somme $f+g$ de deux morphismes f et g de A dans B est donc définie par $(f+g)(x) = f(x)+g(x)$ pour tout $x \in A$. Cette loi est une *loi de groupe*, évidemment commutative, sur $\mathrm{Hom}(A,B)$ (2.2.4).

11.1.1. *Exercice.* Pour $a \in A$ donné, montrer que l'application $\varepsilon_a : f \mapsto f(a)$ de $\mathrm{Hom}(A,B)$ dans B est un morphisme de groupes. Montrer que cette propriété (valable pour tout $a \in A$) caractérise la loi interne sur $\mathrm{Hom}(A,B)$ définie plus haut.

On a ainsi défini une application de A dans $\mathrm{Hom}(\mathrm{Hom}(A,B),B)$ par la formule $a \mapsto \varepsilon_a$. Est-ce un morphisme de groupes ?

11.2. *Multiplication externe.* Si A est un groupe abélien, on dispose d'une « loi externe », notée multiplicativement :

$$\begin{array}{ccc} \mathbb{Z} \times A & \longrightarrow & A \\ (n,a) & \longmapsto & na. \end{array}$$

On rappelle que na est la version additive de la « puissance n-ième », au sens de 1.3.6.

11.2.1. *Propriétés de la multiplication externe.* Pour $(a,b) \in A \times A$ et $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ on a

(i) $n(a+b) = na + nb$

(ii) $(m+n)a = ma + na$

(iii) $1a = a$

(iv) $m(na) = (mn)a$.

On invite le lecteur à démontrer ces formules, dont la plupart figurent déjà dans 1.3.6 (mais si !), et à s'attarder un peu sur leur sens : par exemple les deux signes + dans (i) désignent-ils la même opération ? Et dans (ii) ?

11.2.2. *Exercice.* [S 62] Dans un groupe noté multiplicativement, que « deviennent » les formules ci-dessus ?

11.2.3. *Remarque : notion de module sur un anneau.* Le lecteur perspicace n'aura pas manqué de relever la similitude entre les propriétés ci-dessus et celles qui figurent dans la définition d'un espace vectoriel sur un corps, les entiers jouant ici le rôle de « scalaires ». Les deux situations sont en fait des cas particuliers de la notion de *module*. Si R désigne un anneau (disons unitaire, mais non nécessairement commutatif), un *R-module* (à gauche) est par définition un groupe abélien M muni en outre d'une application de $R \times M$ dans M (« multiplication externe »), notée en général $(\lambda, x) \mapsto \lambda x$, vérifiant les propriétés analogues aux précédentes. (Ainsi, si R est un corps, un R-espace vectoriel n'est pas autre chose qu'un R-module.) Un « morphisme de R-modules », ou « application R-linéaire », se définit exactement comme en algèbre linéaire, et l'on a des notions évidentes de sous-module et de module quotient.

11.2.4. *Exercice.* [S 63] On a vu ci-dessus que tout groupe abélien A admet une structure « naturelle » de $\mathbb{Z}$-module. Montrer que c'est en fait la seule structure de $\mathbb{Z}$-module pour laquelle l'addition soit celle de A. Étant donnés deux groupes abéliens A et B, montrer que les morphismes de groupes et les morphismes de $\mathbb{Z}$-modules de A dans B sont les mêmes, et que les sous-$\mathbb{Z}$-modules de A sont les sous-groupes de A.

11.3. *Torsion.* Les éléments d'ordre fini d'un groupe (non nécessairement commutatif) sont également appelés ses *éléments de torsion*. On dit qu'un groupe est de torsion (resp. sans torsion) si tous ses éléments sont de torsion (resp. si son seul élément de torsion est l'élément neutre).

Si A est un groupe *abélien*, alors (3.11.1 ou 3.3.6) l'ensemble A_{tors} des éléments de torsion de A est un *sous-groupe* de A (on rappelle que c'est faux en général pour les groupes non commutatifs, cf. 3.3.7). A_{tors} (qui est évidemment le plus grand sous-groupe de torsion de A) est souvent appelé « le » sous-groupe de torsion, voire simplement « la torsion », de A. Noter que A est de torsion (resp. sans torsion) si et seulement si $A = A_{\text{tors}}$ (resp. $A_{\text{tors}} = \{0\}$).

11.3.1. *Exercice.* [S 64] Un groupe peut-il être à la fois de torsion et sans torsion ?

11.3.2. *Exercice.* [I 25] Montrer qu'un groupe G est de torsion si et seulement si G est la réunion de ses sous-groupes finis.

11.3.3. *Exercice.* [I 26] Donner un exemple de groupe abélien de torsion et infini.

11.3.4. *Exercice.* [S 65] Quelle est la torsion de $\mathbb{Z}$? de $\mathbb{Z}/n\mathbb{Z}$? de $\mathbb{Q}$? de $\mathbb{R}/\mathbb{Z}$? du groupe multiplicatif $\mathbb{C}^*$? d'un groupe produit $A \times B$, en fonction de A_{tors} et de B_{tors} ?

11.3.5. *Exercice.* [S 66] Le produit d'une famille de groupes sans torsion (resp. de torsion) est-il encore sans torsion (resp. de torsion) ?

11.3.6. *Exercice.* Soit A un groupe abélien. Montrer que A/A_{tors} est sans torsion. Montrer que tout morphisme de A vers un groupe sans torsion se factorise par A/A_{tors}.

11.3.7. *Exercice.* [I 27][S 67] Donner un exemple de groupe abélien qui n'a pas de plus grand sous-groupe sans torsion.

Les résultats de la suite de ce paragraphe ne seront pas utilisés avant le paragraphe 15.

11.4. *Un peu d'algèbre $\mathbb{Z}$-linéaire.*

11.4.1. *Notations.* Fixons un entier $n \geq 0$, et posons

$$X_n = \{1, 2, \ldots, n\} = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}.$$

Si A est un ensemble, on rappelle que A^n peut être vu soit comme l'ensemble des suites $(a_1, a_2, \ldots, a_n)$ d'éléments de A, soit comme l'ensemble des applications de X_n dans A. (Si $n = 0$, alors X_n est vide et A^0 a un unique élément, même si A est vide).

Lorsque A est un groupe abélien, A^n admet une structure évidente de groupe abélien (qui est trivial si $n = 0$). Nous aurons en particulier à considérer le groupe $\mathbb{Z}^n$. Celui-ci contient n éléments « privilégiés » : pour chaque $i \in X_n$, on notera e_i (s'il n'y a pas d'ambiguïté sur n) l'élément de $\mathbb{Z}^n$ dont la i-ème composante vaut 1, les autres étant nulles.

La famille $(e_1, \ldots, e_n)$ d'éléments de $\mathbb{Z}^n$ (qui est donc un élément de $(\mathbb{Z}^n)^n \ldots$) s'appelle la *base canonique* de $\mathbb{Z}^n$. Nous verrons un peu plus loin ce qu'est une base mais on peut déjà remarquer que, pour tout $\underline{\lambda} = (\lambda_i)_{1 \leq i \leq n} \in \mathbb{Z}^n$ on a l'égalité $\underline{\lambda} = \sum_{i=1}^n \lambda_i e_i$, et que (pour $\underline{\lambda}$ donné) cette relation est « unique », i.e. détermine les entiers λ_i.

Proposition 11.4.2 *Avec les notations de* 11.4.1, *soit A un groupe abélien. Alors l'application*

$$\begin{array}{rcl} F : \mathrm{Hom}\,(\mathbb{Z}^n, A) & \longrightarrow & A^n \\ f & \longmapsto & (f(e_i))_{1 \leq i \leq n} \end{array}$$

est un isomorphisme de groupes, dont l'inverse est donné par

$$\begin{array}{rcl} G : A^n & \longrightarrow & \mathrm{Hom}\,(\mathbb{Z}^n, A) \\ \underline{a} = (a_i)_{1 \leq i \leq n} & \longmapsto & \varphi_{\underline{a}} \end{array}$$

où $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ est donné par la formule

$$\varphi_{\underline{a}}((\lambda_1, \ldots, \lambda_n)) = \sum_{i=1}^n \lambda_i a_i.$$

Démonstration. On laisse le lecteur vérifier que F est un morphisme de groupes.

Pour voir que $G \circ F = \mathrm{Id}_{\mathrm{Hom}(\mathbb{Z}^n, A)}$ il s'agit de montrer que pour tout morphisme $f : \mathbb{Z}^n \to A$ et tout $\underline{\lambda} = (\lambda_i)_{1 \leq i \leq n} \in \mathbb{Z}^n$ on a l'égalité $f(\underline{\lambda}) = \sum_{i=1}^n \lambda_i f(e_i)$. Or ceci résulte du fait que f est un morphisme et de l'identité $\underline{\lambda} = \sum_{i=1}^n \lambda_i e_i$ déjà mentionnée à la fin de 11.4.1.

Pour voir que $F \circ G = \mathrm{Id}_{A^n}$ il s'agit de montrer que pour toute famille $\underline{a} = (a_i)_{1 \leq i \leq n} \in A^n$, le morphisme $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ de l'énoncé envoie bien e_i sur a_i, pour tout $i \in X_n$, ce qui est immédiat sur la définition de $\varphi_{\underline{a}}$. ∎

11.4.3. *Exercice.* Expliquer pourquoi la propriété universelle de $\mathbb{Z}$ (2.3) est un cas particulier de 11.4.2.

11.4.4. *Exercice.* [S 68] On prend $A = \mathbb{Z}^n$ et $\underline{a} = (e_1, \ldots, e_n)$ (la base canonique). Quelle est l'application $\varphi_{\underline{a}}$ correspondante ?

11.4.5. *Exercice.* Soient m et $n \in \mathbb{N}$. En s'inspirant de 11.4.2 et de l'algèbre linéaire « classique », donner un isomorphisme de groupes entre $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}^m)$ et le groupe additif $\mathrm{M}_{m,n}(\mathbb{Z})$ des matrices à m lignes et n colonnes à coefficients dans $\mathbb{Z}$.

Lorsque $m = n$ montrer que c'est un isomorphisme d'anneaux (la multiplication de $\mathrm{End}(\mathbb{Z}^n)$ étant la composition, et celle de $\mathrm{M}_{n,n}(\mathbb{Z})$ la multiplication des matrices).

11.4.6. *Familles génératrices.* Avec les notations de la proposition 11.4.2, il est immédiat que l'image du morphisme $\varphi_{\underline{a}}$ est le sous-groupe de A^n *engendré* par l'ensemble $\{a_1, \ldots, a_n\}$ (voir l'exercice 4.4.8).

En particulier, pour qu'une suite $(a_1, \ldots, a_n)$ engendre A, il faut et il suffit que le morphisme $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ correspondant soit *surjectif*. On dit aussi, dans ce cas, que $(a_1, \ldots, a_n)$ est une *famille génératrice* d'éléments de A, ou que $\{a_1, \ldots, a_n\}$ est une *partie génératrice* de A.

Définition 11.4.7 *Avec les notations de* 11.4.1, *soit* $\underline{a} = (a_1, \ldots, a_n) \in A^n$. *On dit que* $\underline{a}$ *est une* famille libre, *ou que* $a_1, \ldots, a_n$ *sont* linéairement indépendants *dans* A, *si le morphisme* $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ *qui lui correspond par* 11.4.2 *est* injectif.

De façon équivalente d'après 11.4.2, $\underline{a}$ *est libre si et seulement si la seule suite* $(\lambda_i)_{1 \leq i \leq n} \in \mathbb{Z}^n$ *d'entiers vérifiant* $\sum_{i=1}^n \lambda_i a_i = 0$ *est la suite nulle.*

On dit que $\underline{a}$ *est une* base *de* A *si elle est libre et génératrice, ou de façon équivalente, si* $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ *est un isomorphisme.*

11.4.8. *Remarque.* Si une confusion est possible, on dira aussi « famille $\mathbb{Z}$-libre », « famille $\mathbb{Z}$-génératrice », « $\mathbb{Z}$-base ».

11.4.9. *Récapitulation.* Pour mémoire et utilisation future, rappelons donc que si $\underline{a} = (a_1, \ldots, a_n) \in A^n$ est une famille finie d'éléments de A et $f : \mathbb{Z}^n \to A$ le

morphisme correspondant, on a les équivalences :

$$\begin{aligned} \underline{a} \text{ est libre} &\Leftrightarrow f \text{ est injectif} \\ \underline{a} \text{ engendre } A &\Leftrightarrow f \text{ est surjectif} \\ \underline{a} \text{ est une base de } A &\Leftrightarrow f \text{ est bijectif.} \end{aligned}$$

D'autre part, pour que $\underline{a}$ soit une base de A, il faut et il suffit que tout élément x de A s'écrive de façon unique $x = \sum_{i=1}^{n} \lambda_i a_i$ où les λ_i sont des entiers.

11.4.10. *Remarque.* On vérifie sans peine que la propriété d'être libre, pour une suite $(a_1, \ldots, a_n) \in A^n$, est invariante par permutation des a_i. Par suite on dira, sans risque, qu'une *partie finie* Σ de A est ($\mathbb{Z}$-)libre (resp. est une base) si, pour une (et donc pour toute) bijection $f : X_n \to \Sigma$ (avec $n = |\Sigma|$), la suite $(f(1), \ldots, f(n))$ d'éléments de A est libre (resp. est une base). (Pour les parties génératrices il n'y a là rien de nouveau).

11.4.11. *Autres ensembles d'indices.* Il est parfois commode d'étendre les considérations qui précèdent (à partir de 11.4.1) en remplaçant l'« ensemble d'indices » $X_n = \{1, 2, \ldots, n\}$ par un ensemble fini I quelconque. On rappelle qu'une famille d'éléments de A, indexée par I, n'est pas autre chose qu'une application de I dans A ; seule la notation est traditionnellement différente, une telle famille étant notée par exemple $(x_i)_{i \in I}$ plutôt que « $x : I \to A$, $i \mapsto x(i)$ ».

Par exemple, la proposition 11.4.2 reste valable, en remplaçant $\mathbb{Z}^n$ et A^n par $\mathbb{Z}^I$ et A^I respectivement. La définition de $\varphi_{\underline{a}}$ à la fin de l'énoncé devient $\varphi_{\underline{a}}((\lambda_i)_{i \in I}) = \sum_{i \in I} \lambda_i a_i$: pour que cette somme ait un sens, il est naturellement essentiel que I soit fini (alors que le morphisme F de l'énoncé a un sens même pour I infini).

Bien entendu, si n désigne le nombre d'éléments de I, on peut aussi se ramener au cas traité plus haut en choisissant une bijection de X_n sur I, de sorte que la « généralisation » présentée ici peut paraître illusoire. Cependant elle évite, justement, d'avoir à choisir une telle numérotation, le plus souvent arbitraire. Par exemple, la définition d'une partie libre (11.4.10) devient bien plus naturelle si l'on dit simplement : « une partie finie Σ de A est dite libre si la famille $(a)_{a \in \Sigma} \in A^{\Sigma}$ est libre », c'est-à-dire si l'application de $\mathbb{Z}^{\Sigma}$ dans A donnée par $(\lambda_a)_{a \in \Sigma} \mapsto \sum_{a \in \Sigma} \lambda_a a$ est injective.

11.4.12. *Exercice.* Soit I un ensemble fini, et soit $(a_i)_{i \in I}$ un élément de A^I. Montrer que c'est une famille libre si et seulement si les deux conditions suivantes sont vérifiées :

(i) l'application $i \mapsto a_i$ est injective (la famille $(a_i)_{i \in I}$ est « sans répétition ») ;

(ii) l'ensemble $\{a_i\}_{i \in I}$ est une partie libre de A.

11.4.13. *Familles libres et bases infinies.* Nous n'utiliserons qu'épisodiquement ces notions. Une famille (finie ou non) $(a_i)_{i \in I}$ d'éléments de A est dite *libre* si toute

sous-famille finie est libre, c'est-à-dire si, pour tout partie fini J de I, la famille $(a_i)_{i\in J}$ est libre. (Noter que pour les familles finies cela ne change rien à la notion déjà introduite, pourquoi ?)

De même une partie Σ de A est libre si toute partie finie de Σ est libre. On peut reformuler cette définition ainsi : pour toute suite *finie* $(a_1, \ldots, a_n)$ d'éléments de Σ *deux à deux distincts*, et toute suite $(\lambda_1, \ldots, \lambda_n)$ d'entiers telle que $\sum_{i=1}^n \lambda_i a_i = 0$ dans A, on a $\lambda_i = 0$ pour tout $i \in X_n$.

Enfin, on dit que $\{a_i\}_{i\in I}$ est une *base* de A si c'est une famille libre et génératrice. Ceci équivaut à dire que tout élément de A s'écrit *de manière unique* sous la forme $\sum_{i\in I} \lambda_i a_i$ où les λ_i sont des entiers *presque tous nuls*, i.e. nuls sauf un nombre fini (de sorte que la somme a un sens).

La démonstration (sans regarder) de la proposition suivante est un bon test de compréhension des notions précédentes, ainsi que de la notion de groupe quotient. La proposition sera utilisée plus loin, cf. 15.6.

Proposition 11.5 *Soit $\pi : A \to A'$ un morphisme de groupes abéliens. Soit $\underline{a} = (a_1, \ldots, a_n)$ une famille finie d'éléments de A, et soit $p \leq n$ un entier naturel. On suppose que :*

- *$(a_1, \ldots, a_p)$ est une famille libre (resp. une famille génératrice, resp. une base) de* Ker π *;*
- *$(\pi(a_{p+1}), \ldots, \pi(a_n))$ est une famille libre (resp. une famille génératrice, resp. une base) de A'.*

Alors $(a_1, \ldots, a_n)$ est une famille libre (resp. une famille génératrice, resp. une base) de A.

Démonstration. Traitons simplement le cas « libre » (le cas « générateur » est similaire, et le dernier se déduit des précédents). Supposons donc $(a_1, \ldots, a_p)$ libre dans Ker π, $(\pi(a_{p+1}), \ldots, \pi(a_n))$ libre dans A' ; supposons une relation $\sum_{i=1}^n \lambda_i\, a_i = 0$, où les λ_i sont des entiers, et montrons que ceux-ci sont nuls. Appliquant π à la relation en question, on trouve $\sum_{i=p+1}^n \lambda_i\, \pi(a_i) = 0$ puisque les a_i avec $i \leq p$ sont dans Ker π. On a donc $\lambda_i = 0$ pour $i \geq p+1$, d'après l'hypothèse sur $(\pi(a_{p+1}), \ldots, \pi(a_n))$. Par suite la relation initiale se réduit à $\sum_{i=1}^p \lambda_i\, a_i = 0$, d'où aussi $\lambda_i = 0$ pour $i \leq p$, d'après l'hypothèse sur $(a_1, \ldots, a_p)$. ∎

11.6. *Exercices.*

11.6.1. Montrer que l'ensemble vide est l'unique base du groupe trivial.

11.6.2. Montrer que les seules bases de $\mathbb{Z}$ sont $\{1\}$ et $\{-1\}$.

11.6.3. [S 69] Montrer que $\{2\}$ est une partie libre maximale de $\mathbb{Z}$ mais n'est pas une base de $\mathbb{Z}$ (et n'est même pas contenue dans une base).

11.6.4. Montrer que $\{2,3\}$ est une partie génératrice minimale de $\mathbb{Z}$ mais n'est pas une base de $\mathbb{Z}$ (et ne contient aucune base).

11.6.5. [S 70] Montrer que, pour m entier > 1, $\mathbb{Z}/m\mathbb{Z}$ n'a aucune base. Que se passe-t-il pour $m = 0$? pour $m = 1$?

11.6.6. Montrer que les seules parties libres de $(\mathbb{Q}, +)$ sont $\emptyset$ et les parties à un élément non nul. En déduire que $\mathbb{Q}$ n'a pas de base.

11.6.7. [S 71] Soit θ un réel. Vrai ou faux :

(i) $\{1, \theta\}$ est une partie libre de $(\mathbb{R}, +)$ si et seulement si θ est irrationnel ;

(ii) $(1, \theta)$ est une famille libre de $(\mathbb{R}, +)$ si et seulement si θ est irrationnel.

11.6.8. *Un exemple de base infinie.* Notons $\mathbb{Z}[X]$ l'anneau des polynômes en une indéterminée X à coefficients dans $\mathbb{Z}$. Montrer que la famille $(X^n)_{n\in\mathbb{N}}$ des puissances de X est une base (au sens de 11.4.13) du groupe additif $\mathbb{Z}[X]$.

11.6.9. *Un autre.* Montrer que l'ensemble des nombres premiers est une base du groupe multiplicatif $\mathbb{Q}_+^*$ des rationnels positifs.

11.7. *Exercices.*

11.7.1. [S 72] Soient $n \in \mathbb{N}$, I un ensemble fini et soit $\underline{a} = (a_i)_{i\in I}$ une famille d'éléments de $\mathbb{Z}^n$ indexée par I. (Le lecteur frileux pourra prendre $I = \{1, \ldots, m\}$). On considère $\mathbb{Z}^n$ comme un sous-groupe additif du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$; on utilisera les exressions « $\mathbb{Q}$-libre », « $\mathbb{Q}$-base », etc. pour distinguer les notions d'algèbre linéaire sur $\mathbb{Q}$ des notions introduites en 11.4, désignées ici par « $\mathbb{Z}$-libre », « $\mathbb{Z}$-base », etc.

Montrer les implications suivantes :

(i) $\underline{a}$ est $\mathbb{Z}$-libre dans $\mathbb{Z}^n \Leftrightarrow \underline{a}$ est $\mathbb{Z}$-libre dans $\mathbb{Q}^n \Leftrightarrow \underline{a}$ est $\mathbb{Q}$-libre dans $\mathbb{Q}^n$;

(ii) $\underline{a}$ est $\mathbb{Z}$-génératrice dans $\mathbb{Z}^n \Rightarrow \underline{a}$ est $\mathbb{Q}$-génératrice dans $\mathbb{Q}^n$;

(iii) $\underline{a}$ est $\mathbb{Z}$-génératrice dans $\mathbb{Z}^n$ et $|I| = n \Leftrightarrow \underline{a}$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$.

11.7.2. Déduire de 11.7.1, sous les mêmes hypothèses, les implications suivantes :

(i) Si $\underline{a}$ est libre, alors $|I| \leq n$;

(ii) si $\underline{a}$ engendre $\mathbb{Z}^n$, alors $|I| \geq n$;

(iii) si $\underline{a}$ est une base de $\mathbb{Z}^n$, alors $|I| = n$;

(iv) si $\underline{a}$ engendre $\mathbb{Z}^n$ et si $|I| = n$, alors $\underline{a}$ est une base de $\mathbb{Z}^n$.

11.7.3. [S 73] Généraliser 11.7.2 au cas d'une famille $\underline{a}$ *infinie*.

11.7.4. Soient m et $n \in \mathbb{N}$, et soit $f : \mathbb{Z}^m \to \mathbb{Z}^n$ un morphisme de groupes. Déduire de 11.7.2 les implications suivantes :

(i) si f est injectif, alors $m \leq n$;

(ii) si f est surjectif, alors $m \geq n$;

(iii) si f est bijectif, alors $m = n$;

(iv) si f est surjectif et si $m = n$ alors f est bijectif.

(On voit notamment que si $\mathbb{Z}^m$ est isomorphe à $\mathbb{Z}^n$, alors $m = n$; pour une démonstration plus simple voir 15.5.)

11.7.5. [S 74] Montrer que la réciproque de l'implication (ii) de 11.7.1 est fausse, déjà pour $n = 1$.

Montrer de même que, dans 11.7.2, l'assertion « si $\underline{a}$ est libre et si $|I| = n$, alors $\underline{a}$ est une base de $\mathbb{Z}^n$ » est fausse, de même que, dans 11.7.4, l'assertion « si f est injectif et si $m = n$ alors f est bijectif ».

11.7.6. Sous les hypothèses de 11.7.4, montrer qu'il existe une unique application $\mathbb{Q}$-linéaire $f_{\mathbb{Q}} : \mathbb{Q}^m \to \mathbb{Q}^n$ dont la restriction à $\mathbb{Z}^m$ soit f.

Montrer alors les implications suivantes :

(i) f injectif $\Leftrightarrow$ $f_{\mathbb{Q}}$ injectif ;

(ii) f surjectif $\Rightarrow$ $f_{\mathbb{Q}}$ surjectif ;

(iii) f bijectif $\Rightarrow$ $f_{\mathbb{Q}}$ bijectif.

Pour chaque implication on pourra soit procéder directement, soit utiliser 11.7.1.

Bien entendu, on retrouve ainsi les résultats (i), (ii) et (iii) de 11.7.4

11.7.7. *Interprétations matricielles.* [I 28] Avec les notations de 11.7.4, on suppose de plus que $m = n$. Soit $M \in \mathrm{M}_n(\mathbb{Z})$ la matrice de f (cf. 11.4.5 ; c'est aussi la matrice de $f_{\mathbb{Q}}$ dans la base canonique de $\mathbb{Q}^n$). On peut considérer M comme un élément de $\mathrm{M}_n(\mathbb{Q})$: elle a donc un déterminant, et le développement des déterminants montre que $\det M$ est un *entier.*

(1) Montrer que f est injectif si et seulement si $\det M \neq 0$.

(2) Montrer que f est bijectif si et seulement si $\det M \in \{-1, +1\}$.

12. Groupes cycliques

Définition 12.1 *Un groupe G est dit* monogène *s'il vérifie les conditions équivalentes suivantes :*

(i) *G est engendré par un élément (autrement dit, il existe $\gamma \in G$ tel que $\langle\gamma\rangle = G$) ;*

(ii) *il existe un morphisme surjectif de $(\mathbb{Z}, +)$ sur G ;*

(iii) *G est isomorphe à un quotient de $(\mathbb{Z}, +)$;*

(iv) *il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$;*

(v) *il existe $n \in \mathbb{Z}$ tel que G soit isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Un groupe G est dit cyclique *s'il est monogène et* fini, *c'est-à-dire isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \neq 0$ (ou encore pour un entier $n > 0$).*

12.2. *Remarques.*

12.2.1. L'équivalence des conditions ci-dessus est immédiate et laissée en exercice.

12.2.2. Un groupe monogène est soit cyclique, soit isomorphe à $\mathbb{Z}$; on rencontre parfois dans la littérature le mot « cyclique » là où nous disons « monogène » ; autrement dit, certains auteurs considèrent $\mathbb{Z}$ comme un groupe cyclique.

12.2.3. Si G est un groupe monogène, il est automatiquement commutatif, et l'entier n de la condition (iv) (resp. (v)) est déterminé (resp. déterminé au signe près) par G puisque $|n|$ est nul si G est infini, et égal à l'ordre de G si G est fini.

Par contre, si G est, disons, cyclique d'ordre $n > 0$, il existe en général (dès que $n > 2$, en fait) *plusieurs isomorphismes* de $\mathbb{Z}/n\mathbb{Z}$ sur G ; de façon équivalente, $\mathbb{Z}/n\mathbb{Z}$ admet pour $n > 2$ des automorphismes différents de l'identité.

12.2.4. Il résulte immédiatement de la définition (sous la forme (ii) par exemple) que tout *quotient* d'un groupe monogène (resp. cyclique) a la même propriété.

12.2.5. *Notation.* Dans tout ce qui suit, la classe d'un entier k dans $\mathbb{Z}/n\mathbb{Z}$ sera notée

$$k \bmod n.$$

C'est donc un élément de $\mathbb{Z}/n\mathbb{Z}$ *qu'on ne confondra pas* avec le reste de la division euclidienne de k par n, qui est un entier et non une classe modulo n, et que certains logiciels désignent aussi par « k mod n ». (Ainsi, l'identité $(2 \bmod 3) + (2 \bmod 3) = (1 \bmod 3)$ est vraie avec nos notations, mais serait fausse si « mod » désignait le reste : faites l'essai avec MAPLE).

On rappelle (cf. cours Algèbre 1) qu'il existe sur $\mathbb{Z}/n\mathbb{Z}$ une unique structure *d'anneau commutatif unitaire*, caractérisée par le fait que la projection canonique

de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ soit un morphisme d'anneaux. Autrement, dit, l'addition est celle que nous connaissons déjà, et la multiplication est déterminée par la formule

$$(a \bmod n)(b \bmod n) = ab \bmod n$$

pour tous a, $b \in \mathbb{Z}$.

12.3. *Exercices.*

12.3.1. [S 75] Soit G un groupe fini d'ordre n. Alors G est cyclique si et seulement si G admet un élément d'ordre n.

12.3.2. [I 29] Soit G un groupe fini d'ordre n *premier*. Alors G est cyclique.

12.3.3. [S 76] Soit G un groupe. On suppose que les seuls sous-groupes de G sont G et $\{e\}$. Alors G est soit réduit à l'élément neutre, soit cyclique d'ordre premier.

12.3.4. Pour $n \geq 1$, posons $\Gamma_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Alors Γ_n est un sous-groupe de $\mathbb{C}^*$, cyclique d'ordre n.

Réciproquement, soit Γ un sous-groupe fini de $\mathbb{C}^*$, et soit n son ordre. Montrer que $\Gamma = \Gamma_n$. [I 30]

En particulier, *tout sous-groupe fini de* $\mathbb{C}^*$ *est cyclique* ; nous verrons au paragraphe 14 que cette propriété est encore vraie si l'on remplace $\mathbb{C}^*$ par K^* où K est un corps commutatif quelconque.

12.3.5. [I 31] Soient G un groupe et C son centre. On suppose que G/C est monogène. Montrer que G est commutatif (autrement dit, $G = C$).

12.3.6. [I 32] Soient p un nombre premier et G un groupe d'ordre p^2. Montrer que G est commutatif.

12.3.7. [I 33] Déduire de 12.3.6 que, sous les mêmes hypothèses, G est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

12.3.8. [S 77] Montrer que le groupe $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, pour $m > 1$, n'est jamais cyclique. (Et si $m = 0$? Et si $m = 1$?)

L'énoncé suivant généralise la propriété universelle de $\mathbb{Z}$ vue en 2.3. Sa démonstration est laissée en exercice ; on peut la faire entièrement « à la main », ou encore en combinant 2.3 et 9.6.

Proposition 12.4 (« propriété universelle de $\mathbb{Z}/n\mathbb{Z}$ ») *Soient n un entier et Γ un groupe. L'application*

$$\begin{array}{rcl} \mathrm{Hom}_{\text{groupes}}(\mathbb{Z}/n\mathbb{Z}, \Gamma) & \longrightarrow & \{\gamma \in \Gamma \mid \gamma^n = e\} \\ f & \longmapsto & f(1 \bmod n) \end{array}$$

est bijective ; *l'application réciproque associe à l'élément* γ *de* Γ *l'unique morphisme* $f : \mathbb{Z}/n\mathbb{Z} \to \Gamma$ *tel que* $f(k \bmod n) = \gamma^k$ *pour tout* $k \in \mathbb{Z}$ *(qui existe si* γ *vérifie* $\gamma^n = e$*).* ∎

12.4.1. Si l'on prend $\Gamma = \mathbb{Z}/n\mathbb{Z}$ dans l'énoncé ci-dessus, on trouve que tout endomorphisme (de groupe) de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $k \bmod n \mapsto ak \bmod n$ pour un entier a bien déterminé modulo n. Cet énoncé devient plus facile à formuler en termes de la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$: l'endomorphisme en question est simplement la multiplication par $a \bmod n$ dans cet anneau. De façon plus précise :

Proposition 12.4.2 *Soit* n *un entier. L'application*

$$\begin{array}{rcl} \mathrm{End}_{\text{groupe}}(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ f & \longmapsto & f(1 \bmod n) \end{array}$$

est un isomorphisme d'anneaux ; l'isomorphisme réciproque associe à l'élément γ *de* $\mathbb{Z}/n\mathbb{Z}$ *l'endomorphisme de multiplication par* γ *dans* $\mathbb{Z}/n\mathbb{Z}$*.*

Démonstration. Il ne reste qu'à vérifier que l'application en question est un morphisme d'anneaux ; il est en fait plus simple de le montrer pour l'inverse, ce qui est un exercice laissé au lecteur. ∎

12.4.3. *Exercice.* [S 78] Quels sont les endomorphismes *d'anneau unitaire* de $\mathbb{Z}/n\mathbb{Z}$?

L'énoncé suivant a été vu en Algèbre 1 :

Proposition 12.5 (« lemme chinois ») *Soient* a *et* b *deux entiers* premiers entre eux. *Alors il existe un unique isomorphisme d'anneaux*

$$f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}).$$

Cet isomorphisme vérifie, pour tout $k \in \mathbb{Z}$*,*

$$f(k \bmod ab) = (k \bmod a, k \bmod b)$$

En particulier le groupe $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ *est cyclique et engendré par l'élément* $(1 \bmod a, 1 \bmod b)$*.*

Démonstration. Voir cours d'Algèbre 1 (*après* avoir fait la démonstration soi-même). ∎

12.5.1. *Exercice.* [S 79] On n'a pas écrit « il existe un unique isomorphisme d'anneaux $f \ldots$ qui vérifie $f(k \bmod ab) = (k \bmod a, k \bmod b)$ ». Pourquoi ?

Corollaire 12.5.2 (« décomposition de $\mathbb{Z}/n\mathbb{Z}$ ») *Soit* n *un entier non nul, décomposé en facteurs premiers sous la forme*

$$n = \varepsilon\, p_1^{e_1} \ldots p_r^{e_r}$$

où $\varepsilon \in \{-1,+1\}$, les p_i $(1 \leq i \leq r)$ sont des nombres premiers deux à deux distincts, et les e_i sont des entiers naturels. Alors il existe un unique isomorphisme d'anneaux

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Cet isomorphisme envoie, pour tout entier k, la classe de k sur la famille $(k \bmod p_i^{e_i})_{1\leq i\leq r}$.

Démonstration. Comme $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/-n\mathbb{Z}$, on peut supposer $n > 0$. On procède alors par récurrence sur r (les détails étant laissés au lecteur) : le cas $r \leq 1$ est trivial (sûr ?), le cas $r = 2$ est le lemme chinois, et le cas général s'en déduit en remarquant que $p_r^{e_r}$ est premier avec $\prod_{i=1}^{r} -1 p_i^{e_i}$. ∎

12.5.3. *Exercice.* Soient a et n deux entiers. Pour abréger, on note $\overline{x}$ la classe d'un entier x modulo n. Montrer que les conditions suivantes sont équivalentes :

(i) $\overline{a}$ est un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$;

(ii) $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$;

(iii) a et n sont premiers entre eux.

12.5.4. *Exercice.* Soit n un entier > 0. Déduire de l'exercice 12.5.3 que l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (cf. 1.4.10) est égal au nombre d'entiers a premiers à n tels que $0 \leq a < n$. Ce nombre est appelé *l'indicateur d'Euler* de n et se note généralement $\varphi(n)$.

Calculer $\varphi(n)$ pour $n = 1, 2, \ldots, 12$. [S 80]

12.5.5. *Exercice.* Soient a et b deux entiers premiers entre eux. Déduire de 12.5 que le groupe $(\mathbb{Z}/ab\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. Conclure que $\varphi(ab) = \varphi(a)\,\varphi(b)$ où φ est l'indicateur d'Euler.

12.5.6. *Exercice.* [S 81] Soient p un nombre premier et r un entier > 0. Montrer que $\varphi(p^r) = p^r - p^{r-1}$.

12.5.7. *Exercice.* Déduire de 12.5.5 et de 12.5.6 la formule, valable pour tout entier $n > 0$:

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

12.5.8. *Exercice.* [S 82] Est-ce que $\varphi(n)$ tend vers $+\infty$ avec n ?

Le reste de ce paragraphe est consacré aux sous-groupes des groupes monogènes.

Proposition 12.6 *Soit n un entier. Tout sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ est monogène, de la forme $d\mathbb{Z}/n\mathbb{Z}$ où $d \geq 0$ est un entier divisant n, uniquement déterminé par*

H ; le quotient $(\mathbb{Z}/n\mathbb{Z})/H$ est alors isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Si $n \neq 0$, H est isomorphe à $\mathbb{Z}/(n/d)\mathbb{Z}$.

Démonstration. Déjà vu en 10.4 et 10.5.1. ∎

12.6.1. *Remarque.* On voit en particulier que, pour $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ a la propriété remarquable suivante : c'est un groupe fini d'ordre n qui admet, pour chaque diviseur $d > 0$ de n, un unique sous-groupe d'ordre d. Nous verrons plus loin (13.8) une réciproque.

12.6.2. Dans l'énoncé ci-dessus, le sous-groupe $d\mathbb{Z}/n\mathbb{Z}$ de $\mathbb{Z}/n\mathbb{Z}$ peut aussi être vu comme le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $d \bmod n$. Or ce dernier a un sens même si d ne divise pas n (contrairement à $d\mathbb{Z}/n\mathbb{Z}$: pourquoi ?).

En particulier, si l'on part d'un entier m quelconque, on peut appliquer la proposition précédente au sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m, et conclure qu'il est de la forme $d\mathbb{Z}/n\mathbb{Z}$ où d divise n. La proposition suivante identifie d :

Proposition 12.7 *Soient m et n deux entiers, et soit Δ le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de m. Alors $\Delta = d\mathbb{Z}/n\mathbb{Z}$ où d désigne le pgcd de m et n.*

En particulier Δ est d'ordre $|n/\mathrm{pgcd}\,(m,n)|$.

Démonstration. Par construction, Δ est l'image, par la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, du sous-groupe $\Gamma = m\mathbb{Z}$ de $\mathbb{Z}$. C'est donc aussi l'image de $\pi^{-1}(\pi(m\mathbb{Z}))$ qui est égal d'après 10.2 à $m\mathbb{Z} + n\mathbb{Z}$ (attention, ici la loi de groupe est l'addition). La proposition 3.7 montre donc que $\Delta = \pi(d\mathbb{Z})$ où d est le pgcd de m et n ; comme de plus $n\mathbb{Z} \subset d\mathbb{Z}$ (pourquoi ?), on a bien $\Delta = d\mathbb{Z}/n\mathbb{Z}$. ∎

12.8. *Exercices.*

12.8.1. Redémontrer 12.7 en utilisant l'assertion (i) de 3.7 et la dernière assertion de 10.2.

12.8.2. [S 83] Pour m et n entiers positifs donnés, quel est l'ordre du sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ formé des éléments x tels que $mx = 0$?

12.8.3. [S 84] Pour m et n entiers positifs donnés, quelle est la structure du groupe $\mathrm{Hom}_{\mathbf{groupes}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$?

13. Décomposition des groupes abéliens finis

13.1. *Conventions, rappels et notations.* Les conventions de 11.1 sont encore en vigueur dans ce paragraphe. Si A est un groupe commutatif et n un entier, on rappelle (cf. 11.2) que la multiplication par n est un endomorphisme de A, que l'on notera $[n]_A$, de sorte que l'on a, pour tout $x \in A$,

$$[n]_A(x) = nx.$$

On posera d'autre part

$${}_nA := \mathrm{Ker}\,[n]_A \subset A.$$

On dit parfois qu'un élément de A est *annulé par* n s'il appartient à ${}_nA$, et que A est annulé par n si $[n]_A = 0$. Par exemple, un groupe abélien fini d'ordre n est annulé par n. (On dit aussi « tué par n », surtout si le groupe n'est pas noté additivement).

On vérifie immédiatement les propriétés suivantes :

- si $m \mid n$, alors ${}_mA \subset {}_nA$;
- ${}_mA \cap {}_nA \subset {}_{m+n}A$;
- ${}_1A = \{0\}$;
- ${}_0A = A$.

La *réunion* de tous les ${}_nA$, pour n *non nul*, est le *sous-groupe de torsion* A_{tors} de A, vu en 11.3, qui n'est autre que l'ensemble des éléments d'ordre fini de A ; les éléments de ${}_nA$ sont les éléments de A dont l'ordre *divise* n.

13.1.1. *Exercice.* [S 85] Définir un isomorphisme naturel $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A) \xrightarrow{\sim} {}_nA$.

13.1.2. *Exercice.* [S 86] Notons nA l'image de $[n]_A$. Si A est fini, montrer que les groupes ${}_nA$ et A/nA ont même ordre.

Proposition 13.2 *Soient n un entier et A un groupe abélien annulé par n.*

(i) *Pour tout $a \in \mathbb{Z}$, l'endomorphisme $[a]_A$ de A ne dépend que de la classe de a modulo n. L'application*

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathrm{End}\,(A) \\ a \bmod n & \longmapsto & [a]_A \end{array}$$

ainsi définie est un morphisme d'anneaux unitaires.

(ii) *Si a est un entier* premier avec n, *alors $[a]_A$ est un isomorphisme.*

(iii) *Soient a et b deux entiers* premiers entre eux *tels que $n = ab$. Alors le morphisme naturel*

$$\begin{array}{ccc} {}_aA \times {}_bA & \longrightarrow & A \\ (x, y) & \longmapsto & x + y \end{array}$$

est un isomorphisme.

Démonstration. (i) est laissé au lecteur ; (ii) en résulte car, si a est premier avec n, a mod n est inversible dans $\mathbb{Z}/n\mathbb{Z}$ de sorte que son image par le morphisme de (i) est inversible dans $\mathrm{End}\,(A)$.

Pour montrer (iii), on remarque qu'il existe deux entiers u et v (que l'on fixe désormais) tels que $ua + vb = 1$. Soit φ le morphisme de l'énoncé. Alors :

– *φ est injectif :* son noyau est l'ensemble des $(x, -x)$ pour $x \in {}_aA \cap {}_bA$; l'injectivité revient donc à voir que ${}_aA \cap {}_bA = \{0\}$. Or ${}_aA \cap {}_bA \subset {}_{ua+vb}A = {}_1A = \{0\}$, cqfd.

– *φ est surjectif :* pour tout $x \in A$, on a $uax \in {}_bA$, $vbx \in {}_aA$, et $x = (ua + vb)\,x$ donc x est l'image par φ d'un élément de ${}_aA \times {}_bA$, à savoir (vbx, uax). ∎

13.2.1. *Remarque.* Dans 13.2(ii), l'inverse de $[a]_A$ est évidemment $[\alpha]_A$, où α mod n est l'inverse de a modulo n, que l'on calcule par la décomposition de Bézout $\alpha a + \beta n = 1$.

13.2.2. *Remarque.* De même, dans 13.2(iii), la démonstration fournit l'inverse de φ : avec les notations de la preuve, c'est le morphisme $x \mapsto (vbx, uax)$, vu comme application à valeurs dans ${}_aA \times {}_bA$.

13.2.3. *Remarque.* On notera l'analogie avec le résultat suivant d'algèbre linéaire : soient K un corps, V un K-espace vectoriel, u un endomorphisme de V, A et $B \in K[X]$ deux polynômes premiers entre eux. On suppose que le polynôme AB annule u. Alors V est somme directe de $\mathrm{Ker}\,A(u)$ et de $\mathrm{Ker}\,B(u)$. (On ne suppose pas V de dimension finie, de même que dans 13.2 le groupe n'est pas supposé fini).

Les analogies de ce genre ne sont jamais de simples coïncidences : les deux énoncés résultent d'une théorie générale. Le point essentiel est que $\mathbb{Z}$ (dans le cas de 13.2) et $K[X]$ (dans l'exemple considéré ici) sont des anneaux *principaux*.

Corollaire 13.3 *Soit n un entier positif, et soit*

$$n = \prod_{i=1}^{s} p_i^{e_i}$$

sa décomposition en facteurs premiers. Soit A un groupe abélien annulé par n ; pour tout $i \in \{1, \ldots, s\}$, posons $A_i = {}_{(p_i^{e_i})}A$. Alors le morphisme naturel

$$\begin{array}{ccc} A_1 \times \cdots \times A_s & \longrightarrow & A \\ (x_1, \ldots, x_s) & \longmapsto & x_1 + \cdots + x_s \end{array}$$

est un isomorphisme.

Démonstration. Comme les $p_i^{e_i}$ sont deux à deux premiers entre eux, ceci résulte de 13.2 par récurrence sur s. ∎

Le corollaire 13.3 s'applique notamment lorsque A est un groupe abélien *fini d'ordre n*. Dans ce cas, il entraîne que n est le produit des ordres des A_i, ce qui suggère fortement que, pour chaque i, A_i est d'ordre $p_i^{e_i}$. Pour le montrer, nous devons préciser le lien entre l'ordre d'un groupe abélien fini et les ordres de ses éléments :

Proposition 13.4 *Soit A un groupe abélien engendré par s éléments $x_1, \ldots, x_s$ d'ordres finis respectifs $m_1, \ldots, m_s$. Alors A est fini, et son ordre est divisible par le ppcm des m_i, et divise leur produit.*

Démonstration. Pour chaque i, notons A_i le sous-groupe de A engendré par x_i : il est d'ordre m_i, et l'on a un morphisme naturel de $B := \prod_{i=1}^{s} A_i$ vers A, envoyant $(y_1, \ldots, y_s)$ sur $y_1 + \cdots + y_s$. Comme les x_i engendrent A, ce morphisme est surjectif. Donc A est isomorphe à un quotient de B, de sorte qu'il est fini et que son ordre divise celui de B qui est le produit des m_i.

Enfin, d'après le théorème de Lagrange, $|A|$ est divisible par chacun des m_i, donc par leur ppcm. ∎

13.4.1. *Exercice : contre-exemples non commutatifs.* [S 87] Trouver :

(i) un groupe fini engendré par deux éléments d'ordre premier p, qui n'est pas un p-groupe ;

(ii) un groupe infini engendré par deux éléments d'ordre fini.

Corollaire 13.4.2 *Soient A un groupe abélien fini, n son ordre, et p un nombre premier.*

(i) *Pour que A admette un élément d'ordre p, il faut et il suffit que p divise n.*

(ii) *Pour que A soit un p-groupe, il faut et il suffit que tout élément de A ait pour ordre une puissance de p.*

Démonstration. Dans les deux cas, la partie « il faut » résulte du théorème de Lagrange. Le « il suffit » de (ii) est conséquence de 13.4.

Supposons maintenant que p divise n. La proposition 13.4 montre que A admet un élément x d'ordre multiple de p (si tous les ordres des éléments de A étaient premiers à p, n le serait aussi). Soit $q = mp$ cet ordre : alors mx est d'ordre p, de qui achève de prouver le corollaire. ∎

13.4.3. *Remarque.* Les deux assertions du corollaire sont encore valables pour les groupes finis non commutatifs ; la partie (i) ainsi généralisée est connue sons le nom de « théorème de Cauchy ».

Nous arrivons à présent au résultat principal de ce paragraphe :

Théorème 13.5 *Soit A un groupe abélien fini d'ordre $n = \prod_{i=1}^{s} p_i^{e_i}$ (où les p_i sont des nombres premiers distincts, et les e_i des entiers naturels). Alors A est isomorphe à un groupe de la forme $A_1 \times \cdots \times A_s$, où, pour chaque i, A_i est d'ordre $p_i^{e_i}$.*

De plus les A_i sont uniques à isomorphisme près : plus précisément, pour toute décomposition du type précédent, A_i est isomorphe à ${}_{(p_i^{e_i})}A$.

Démonstration. L'assertion d'unicité est évidente : si A est isomorphe à un groupe $B = A_1 \times \cdots \times A_s$ comme dans l'énoncé, alors, pour chaque i, ${}_{(p_i^{e_i})}A$ est isomorphe à ${}_{(p_i^{e_i})}B$, et ce dernier s'identifie à A_i.

Pour l'existence, on part de la décomposition de 13.3 : il s'agit de montrer que $|A_i| = p_i^{e_i}$. Mais il résulte de 13.4.2(ii) que A_i est un p_i-groupe puisqu'il est annulé par une puissance de p_i. Comme le produit des ordres des A_i est n, l'assertion en résulte. ∎

Nous allons donner une première application des résultats précédents à la structure des groupes abéliens finis.

Définition 13.6 *Soit G un groupe fini (non nécessairement commutatif, et noté multiplicativement). On appelle* exposant *de G le plus petit entier $m > 0$ tel que $x^m = e$ pour tout $x \in G$.*

13.6.1. *Remarques.*

(i) On étend parfois cette notion aux groupes non nécessairement finis ; l'exposant sera alors déclaré *infini* s'il n'existe aucun $m > 0$ tel que $x^m = e$ pour tout $g \in G$.

(ii) Il devrait être clair que l'on peut aussi définir l'exposant de G comme le ppcm (positif) des ordres des éléments de G,

(iii) et que si G est commutatif, l'exposant de G est le plus petit entier $m > 0$ tel que $G = {}_mG$.

13.6.2. *Exercice.* [S 88] Pour $n \in \mathbb{Z}$, quel est l'exposant de $\mathbb{Z}/n\mathbb{Z}$? Que peut-on dire de l'exposant d'un sous-groupe (resp. d'un quotient) d'un groupe G, par rapport à celui de G ? de celui d'un produit $\prod_{i \in I} G_i$, en fonction des exposants des G_i ?

13.6.3. *Exercice.* [S 89] Montrer que l'exposant d'un groupe abélien A ne dépend que de l'anneau $\mathrm{End}\,(A)$. Est-ce encore vrai pour un groupe non commutatif ?

Proposition 13.7 *Soit A un groupe abélien fini d'exposant m. Alors A admet un élément d'ordre m.*

Démonstration. Notons qu'il revient au même de dire que A admet un sous-groupe cyclique d'ordre m.

Traitons d'abord le cas où m est une puissance d'un nombre premier p. Alors tous les ordres des éléments de A sont des puissances de p (en fait A est même un p-groupe d'après 13.4.2(ii), mais nous n'en aurons pas besoin). Donc si $x \in A$ est un élément d'ordre maximum, son ordre est multiple des ordres de tous les autres, et est donc égal à l'exposant, cqfd.

Dans le cas général, on peut supposer d'après 13.3 que A est produit de groupes A_i $(1 \leq i \leq s)$ d'exposants respectifs $m_i = p_i^{e_i}$, où les p_i sont des nombres premiers distincts. Alors l'exposant de A est le ppcm des m_i (13.6.2), qui est aussi leur produit. Mais d'après le cas déjà traité, chaque A_i admet un sous-groupe cyclique C_i d'ordre m_i ; le produit des C_i est alors d'ordre m, et est cyclique d'après le lemme chinois. ■

13.8. *Exercice.* [I 34] Soit A un groupe abélien fini d'ordre n. Montrer que les conditions suivantes sont équivalentes :

(i) A est cyclique ;

(ii) pour tout entier $d \geq 1$ divisant n, A admet un unique sous-groupe d'ordre d ;

(iii) pour tout entier $d \geq 1$, A admet au plus un sous-groupe d'ordre d.

14. Groupes de racines de l'unité dans un corps

14.1. *Notations et rappels.* Dans ce paragraphe, k désigne un corps (commutatif). On notera simplement 0 (resp. 1) l'élément neutre de l'addition (resp. de la multiplication) dans k (on pourra les noter respectivement 0_k et 1_k s'il y a un risque de confusion).

On note k^* l'ensemble des éléments non nuls de k ; par définition d'un corps, c'est aussi l'ensemble des éléments inversibles de l'anneau k. C'est donc un groupe commutatif pour la multiplication. (Rappelons aussi qu'un corps est par définition non nul, de sorte que k^* n'est pas vide ou, ce qui revient au même, que $1_k \neq 0_k$).

14.1.1. On rappelle la propriété fondamentale suivante : si $P \in k[X]$ est un polynôme non nul à coefficients dans k, l'équation $P(x) = 0$ admet au plus d solutions en x dans k, où d désigne le degré de P. Ces solutions sont appelées racines (ou zéros) de P dans k.

14.1.2. Pour tout entier $n \geq 1$, posons

$$\mu_n(k) = {}_nk^* = \{z \in k \mid z^n = 1\}.$$

Les éléments de $\mu_n(k)$ sont appelés les *racines n-ièmes de l'unité* de k. (À titre d'information, les éléments d'ordre n de k^* s'appellent les racines n-ièmes *primitives* de l'unité).

On peut voir aussi $\mu_n(k)$ comme l'ensemble des racines dans k du polynôme $X^n - 1$. On peut donc lui appliquer la propriété 14.1.1, ce qui donne immédiatement :

Lemme 14.1.3 *Pour tout entier $n \geq 1$, $|\mu_n(k)| \leq n$.* ∎

14.1.4. *Exemple : $k = \mathbb{C}$.* Pour déterminer $\mu_n(\mathbb{C})$, on considère le morphisme surjectif

$$\begin{array}{rccc} \varphi : & (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ & z & \longmapsto & e^{2i\pi z} \end{array}$$

déjà mentionné en 9.8.7. L'image réciproque $\varphi^{-1}(\mu_n(\mathbb{C}))$ est l'ensemble des $z \in \mathbb{C}$ tels que $\varphi(z)^n = \varphi(nz) = 1$, c'est-à-dire l'ensemble des $z \in \mathbb{C}$ tels que $nz \in \operatorname{Ker}\varphi = \mathbb{Z}$. Donc $\varphi^{-1}(\mu_n(\mathbb{C})) = \frac{1}{n}\mathbb{Z}$. Comme ce groupe est engendré par $\frac{1}{n}$, on en conclut que $\mu_n(\mathbb{C}) = \varphi(\varphi^{-1}(\mu_n(\mathbb{C})))$ est engendré par $\varphi(\frac{1}{n}) = e^{2i\pi/n}$. Il est donc cyclique, et en fait cyclique d'ordre n : on a un isomorphisme explicite $(\mathbb{Z}/n\mathbb{Z}, +) \xrightarrow{\sim} \mu_n(\mathbb{C})$ par la formule : $a \bmod n \mapsto \varphi(\frac{a}{n}) = e^{2i\pi a/n}$.

14.1.5. *Exercice.* [S 90] Quel est, en fonction de l'entier n, la structure de $\mu_n(\mathbb{Q})$? de $\mu_n(\mathbb{R})$?

14.1.6. *Exercice.* [S 91] Montrer que le groupe des éléments inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique. Même question pour $\mathbb{Z}/15\mathbb{Z}$.

L'objet de ce paragraphe est la démonstration du théorème suivant :

Théorème 14.2 *Soit G un sous-groupe* fini *de $(k^*, \times)$, et soit n son ordre. Alors :*
(1) $G = \mu_n(k)$.
(2) G *est* cyclique *(donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$).*

Démonstration. Montrons (1). Il résulte du théorème de Lagrange (7.6) que tout élément z de G vérifie $z^n = 1$, donc $G \subset \mu_n(k)$. Mais alors on a forcément égalité puisque $|G| = n$ alors que $|\mu_n(k)| \leq n$ d'après 14.1.3, d'où l'assertion.

Compte tenu de la propriété 14.1.3, l'assertion (2) résulte du lemme ci-dessous (qui est une variante de l'exercice 13.8). ∎

Lemme 14.2.1 *Soit G un groupe abélien fini. Les conditions suivantes sont équivalentes :*

(i) *G est cyclique ;*

(ii) *pour tout entier $d \geq 1$, on a $|_dG| = \mathrm{pgcd}\,(d, |G|)$;*

(iii) *pour tout entier $d \geq 1$ divisant $|G|$, on a $|_dG| \leq d$.*

Démonstration. L'implication (i)⇒(ii) est laissée au lecteur (et ne sera pas utilisée ici). D'autre part il est trivial que (ii) implique (iii). Supposons (iii) et montrons que G est cyclique. Soit d l'exposant de G (13.6) : alors d divise $|G|$, donc d'après (iii) on a $|G| = |_dG| \leq d$, d'où $|G| = d$. Mais d'autre part on sait (13.7) que G a un sous-groupe cyclique d'ordre d, qui ne peut donc être que G lui-même. ∎

Corollaire 14.3 *Si k est un corps fini, le groupe k^* est cyclique.*

En particulier, pour tout nombre premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p - 1$. ∎

Corollaire 14.4 *Pour tout entier $n \geq 1$, le groupe $\mu_n(k)$ est cyclique d'ordre divisant n.*

Démonstration. On sait que $\mu_n(k)$ est cyclique d'après 14.2. Si d est son ordre, il admet donc un élément z d'ordre d. Par définition de $\mu_n(k)$ on a $z^n = 1$ donc d divise n. ∎

14.5. *Exercices.*

14.5.1. [S 92] Quel est l'ordre de $\mu_n(\mathbb{Z}/p\mathbb{Z})$, en fonction de l'entier n et du nombre premier p ?

14.5.2. [S 93] Soit n un entier positif. Un élément x d'un corps k est appelé *racine n-ième primitive de l'unité* dans k si c'est un élément d'ordre n de k^*. Notons $\mu_n^\circ(k)$ l'ensemble des racines n-ièmes primitives de l'unité dans k.

Vrai ou faux :

(i) $x \in \mu_n^\circ(k) \Leftrightarrow x$ engendre $\mu_n(k)$ dans k^* ;

(ii) si $x \in \mu_n^\circ(k)$ alors $\mu_n^\circ(k) = \{x^a\}$ où a parcourt les entiers premiers à n ;

(iii) $|\mu_n^\circ(k)|$ est soit nul, soit égal à $\varphi(n)$ (l'indicateur d'Euler, cf. 12.5.4).

14.5.3. [S 94] Avec les notations de l'exercice 14.5.2, décrire en fonction de n les ensembles $\mu_n^\circ(\mathbb{Q})$, $\mu_n^\circ(\mathbb{C})$, $\mu_n^\circ(\mathbb{Z}/7\mathbb{Z})$.

14.5.4. [S 95] Soit p un nombre premier impair, et soit $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

(1) Montrer que $y = x^{(p-1)/2}$ est égal à 1 ou à -1 (ici, 1 désigne évidemment la classe de l'entier 1 modulo p, c'est-à-dire l'élément neutre de la multiplication dans $\mathbb{Z}/p\mathbb{Z}$). (Remarquer que $y^2 = 1$).

(2) Déduire alors de 14.3 que, pour que $x^{(p-1)/2} = 1$, il faut et il suffit que x soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

(3) En prenant en particulier $x = -1$, retrouver l'une des implications de 7.13 (l'autre est, rappelons-le, une conséquence immédiate du théorème de Lagrange).

14.5.5. Retrouver le dernier résultat de 14.5.4 de façon plus rapide, en remarquant que si $p \equiv 1 \pmod 4$ le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre divisible par 4 et admet donc un élément y d'ordre 4, dont le carré ne peut être que -1.

14.5.6. Écrire un programme qui, étant donné un nombre premier p, calcule une « racine primitive modulo p », c'est-à-dire un entier a dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$.

14.5.7. [I 35] Existe-t-il un corps k tel que le groupe k^* soit isomorphe à $\mathbb{Z}$?

14.5.8. [I 36] Soient k un corps *algébriquement clos*, et n un entier positif.

(1) Si k est de caractéristique nulle, montrer que $X^n - 1 \in k[X]$ n'a que des racines simples. En déduire que $\mu_n(k) \cong \mathbb{Z}/n\mathbb{Z}$.

(2) Si k est de caractéristique $p > 0$, on écrit $n = mp^s$ avec $s \in \mathbb{N}$ et m premier à p. Montrer que $\mu_n(k) = \mu_m(k)$, et que $X^m - 1 \in k[X]$ n'a que des racines simples. En déduire que $\mu_n(k) \cong \mathbb{Z}/m\mathbb{Z}$.

15. Groupes abéliens de type fini

15.1. *Convention.* Dans ce paragraphe tous les groupes *abéliens* considérés seront, sauf mention contraire, notés additivement.

Définition 15.2 *Soit G un groupe. On dit que G est* de type fini *s'il existe une partie finie de G qui engendre G.*

Proposition 15.3 (i) *Tout groupe fini est de type fini.*

(ii) *Le groupe $\mathbb{Z}$ est de type fini.*

(iii) *Tout quotient d'un groupe de type fini est de type fini.*

(iv) *Soient G un groupe et H un sous-groupe distingué de G. Si H et G/H sont de type fini, alors G est de type fini.*

(v) *Le produit d'une famille finie de groupes de type fini est de type fini.*

(vi) *Un groupe* abélien *A est de type fini si et seulement si il existe $n \in \mathbb{N}$ tel que A soit isomorphe à un quotient de $\mathbb{Z}^n$.*

(vii) *Soit A un groupe* abélien *de type fini. Pour que A soit* fini, *il faut et il suffit qu'il soit* de torsion (11.3).

Démonstration. (i) est trivial (G engendre G), de même que (ii) ($\mathbb{Z}$ est engendré par $\{1\}$) et que (iii) (si Σ engendre G, l'image de Σ dans un quotient engendre ce quotient).

Montrons (iv). Notons $\pi : G \to G/H$ le morphisme canonique. Soient X une partie génératrice finie de H, et Y une partie génératrice finie de G/H. Choisissons une partie finie Y' de G telle que $\pi(Y') = Y$ (il suffit pour cela de choisir un représentant dans G de chaque élément de Y). Montrons que $X \cup Y'$ engendre G (ce qui suffit à démontrer l'assertion) : si G' désigne le sous-groupe de G engendré par $X \cup Y'$, alors G' contient X donc contient H qui est engendré par X. D'après 10.3, il est donc égal à $\pi^{-1}(\pi(G'))$. Or $\pi(G')$ est un sous-groupe de G/H contenant $\pi(Y') = Y$ donc égal à G/H d'où $G' = \pi^{-1}(G') = G$), cqfd.

Pour (v), on se ramène par récurrence au cas du produit de deux groupes, qui est laissé au lecteur (qui pourra procéder directement ou utiliser (iv)).

Montrons (vi) : il est clair que $\mathbb{Z}^n$ est de type fini (soit directement, soit par (ii) et (v)), donc aussi tout quotient de $\mathbb{Z}^n$ par (iii). La réciproque résulte de 11.4.2 et de 11.4.6 : si A est engendré par une suite finie $\underline{a} = (a_1, \ldots, a_n)$ d'éléments de A, le morphisme correspondant $\varphi_{\underline{a}} : \mathbb{Z}^n \to A$ (notation de 11.4.2) est surjectif donc A est isomorphe à $\mathbb{Z}^n/\mathrm{Ker}\ \varphi_{\underline{a}}$.

Pour (vii), l'assertion « il faut » est triviale, et la réciproque résulte de 13.4. ∎

15.3.1. *Remarque.* Il est *faux* que tout sous-groupe d'un groupe de type fini soit encore de type fini. C'est toutefois vrai pour les groupes commutatifs, comme nous le verrons.

15.3.2. *Exercice.* [I 37] Montrer que le groupe additif $\mathbb{Q}$ n'est pas de type fini. Plus précisément, montrer que tout sous-groupe de type fini de $\mathbb{Q}$ est engendré par un élément.

15.3.3. *Exercice.* [S 96] Soit G un groupe de type fini. Montrer que toute partie génératrice de G contient une partie génératrice *finie* de G.

15.3.4. *Exercice.* [I 38] Montrer que le groupe multiplicatif $\mathbb{Q}^*$ n'est pas de type fini.

Définition 15.4 *Soit A un groupe abélien de type fini.*

On dit que A est libre *s'il admet une base* (cf.11.4.7).

On dit que A est libre de rang *n (entier naturel donné) si A admet une base à n éléments, ou, de façon équivalente, s'il est isomorphe à $\mathbb{Z}^n$.*

15.4.1. *Remarque.* Plus généralement, un groupe abélien (non nécessairement de type fini) est dit libre s'il admet une base, au sens de 11.4.13.

15.4.2. *Mise en garde.* Il existe aussi une notion de *groupe libre* pour les groupes non commutatifs, que nous n'étudierons pas ici mais est distincte de la notion de groupe abélien libre : un groupe abélien libre n'est *pas* en général un « groupe libre », et un groupe libre n'est pas en général commutatif ! Une phrase telle que « A est libre » doit donc être maniée avec précaution.

15.4.3. *Exercice.* Soit A un groupe abélien libre, et soit a un élément d'une base de A. Pour tout entier $k > 2$, montrer que $a \notin kA$ (i.e. a n'est pas « divisible par k » dans A).

En déduire que $\mathbb{Q}$ n'est pas libre. Plus généralement, le groupe additif sous-jacent à un $\mathbb{Q}$-espace vectoriel non nul n'est jamais libre.

15.4.4. *Remarque.* Il est clair que tout groupe abélien libre est sans torsion (ainsi le groupe $\mathbb{Z}/2\mathbb{Z}$ n'est pas libre). La réciproque est fausse comme le montre l'exercice 15.4.3 : $\mathbb{Q}$ est sans torsion mais n'est pas libre. Rappelons cependant (15.3.2) qu'il n'est pas non plus de type fini ; de fait, nous verrons un peu plus loin que tout groupe abélien *de type fini* et sans torsion est libre.

15.4.5. *Remarque.* A priori, la notion de groupe abélien « libre de rang n » n'autorise pas à parler « du » rang d'un groupe donné : pour cela il faut montrer que toutes les bases d'un même groupe ont même cardinal (en d'autres termes : si $\mathbb{Z}^m$ et $\mathbb{Z}^n$ sont isomorphes alors $m = n$). Cette propriété résulte de l'exercice 11.7.2 (assertion (iii)) mais voici une démonstration plus simple :

Proposition 15.5 *Si L est un groupe abélien libre de rang r, alors $L/2L$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^r$* (et donc d'ordre 2^r, de sorte que r est déterminé par L).

Démonstration. Immédiat. ∎

15.5.1. *Remarque.* Au lieu de 2, on peut utiliser n'importe quel entier $k > 1$ dans l'argument ci-dessus. (Pourquoi > 1 ?)

15.5.2. *Exercice.* On a donc retrouvé, de façon particulièrement expéditive, l'assertion (iii) de 11.7.2 (ou, ce qui revient au même, de 11.7.4). Il est donc naturel de se demander si on ne pourrait pas prouver les autres assertions de ces exercices par une méthode similaire.

Il est plus commode ici de considérer, comme dans 11.7.4, un morphisme $f : \mathbb{Z}^m \to \mathbb{Z}^n$. Alors f induit par passage au quotient un morphisme $\overline{f} : \mathbb{Z}^m/2\mathbb{Z}^m \to \mathbb{Z}^n/2\mathbb{Z}^n$. Montrer alors que si f est surjectif (resp. bijectif) il en est de même de $\overline{f}$ (pour le cas bijectif, utiliser l'inverse de f).

Le cas « bijectif » est essentiellement l'argument de 15.5 ; du cas « surjectif » déduire 11.7.4(ii) : si f est surjectif alors $m \geq n$.

Remarquer enfin que cet argument ne permet pas de montrer 11.7.4(i) : il n'est pas vrai que si f est injectif alors $\overline{f}$ l'est (prendre pour f la multiplication par 2 dans $\mathbb{Z}$, avec $m = n = 1$).

Théorème 15.6 *Soit L un groupe abélien libre de rang r. Alors tout sous-groupe de L est libre de rang $\leq r$.*

Corollaire 15.6.1 *Tout sous-groupe d'un groupe abélien de type fini est encore de type fini.*

15.6.2. *Preuve du corollaire.* Soit A un groupe abélien de type fini. Il existe alors un entier r et un morphisme surjectif $\pi : \mathbb{Z}^r \to A$. Si B est un sous-groupe de A, alors B est (isomorphe à) un quotient de $\pi^{-1}(B)$. Comme $\pi^{-1}(B)$ est un sous-groupe de $\mathbb{Z}^r$, il est de type fini par 15.6, donc B aussi. ∎

15.6.3. *Exercice.* En raffinant la démonstration précédente, montrer que tout sous-groupe d'un groupe abélien engendré par r éléments peut être engendré par r éléments.

15.6.4. *Preuve du théorème* 15.6. Il suffit naturellement de montrer que tout sous-groupe de $\mathbb{Z}^r$ est libre de rang $\leq r$. (Noter que l'inégalité du rang se déduit, si l'on veut, de 11.7.4 ; cependant la démonstration qui suit la redonne facilement).

On procède par récurrence sur r. L'assertion est triviale pour $r = 0$, et pour $r = 1$ c'est la proposition 3.6 sur les sous-groupes de $\mathbb{Z}$. Supposons $r > 0$, et soit A un sous-groupe de $\mathbb{Z}^r$. Considérons la « projection » $\pi : \mathbb{Z}^r \to \mathbb{Z}$ donnée par la dernière coordonnée. C'est un morphisme dont le noyau H est isomorphe à $\mathbb{Z}^{r-1}$. Comme

$A \cap H$ (resp. $\pi(A)$) est un sous-groupe d'un groupe libre de rang $< r$ (resp. de rang 1) il admet, d'après l'hypothèse de récurrence, une base Σ_1 (resp. Σ_2') admettant au plus $(r-1)$ éléments (resp. un élément). Choisissons arbitrairement, pour chaque élément y' de Σ_2', un élément y de A tel que $\pi(y) = y'$, et notons $\Sigma_2 \subset A$ l'ensemble obtenu. Alors $\Sigma_1 \cup \Sigma_2$ a au plus r éléments, et il résulte de 11.5 que c'est une base de A. ∎

On a en fait un résultat bien plus précis, dont la preuve sera donnée en maîtrise :

Théorème 15.7 *Soit L un groupe abélien libre de rang r, et soit A un sous-groupe de L. Il existe alors une base $(v_1, \dots, v_r)$ de L et des entiers positifs $d_1, \dots, d_s$ (où $s \leq r$), avec les propriétés suivantes :*

(i) *$d_i \mid d_{i+1}$ pour tout $i \in \{1, \dots, s-1\}$;*

(ii) *$(d_1 v_1, \dots, d_s v_s)$ est une base de A.* ∎

On en déduit un théorème de structure pour tous les groupes abéliens de type fini :

Corollaire 15.8 *Soit A un groupe abélien de type fini. Alors il existe un entier $k \in \mathbb{N}$ et des entiers positifs $d_1, \dots, d_s$ avec les propriétés suivantes :*

(i) *$d_i \mid d_{i+1}$ pour tout $i \in \{1, \dots, s-1\}$;*

(ii) *A est isomorphe à $\mathbb{Z}^k \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.* ∎

Tout énoncé général de ce type doit être soigneusement médité. Une bonne méthode d'attaque consiste à examiner les cas particuliers : que se passe-t-il pour les groupes de type fini que l'on connaît déjà ? Voici deux cas particuliers en quelque sorte « opposés » :

Corollaire 15.8.1 *Tout groupe abélien de type fini sans torsion est libre.*

Démonstration. Avec les notations de 15.8, la torsion de A est isomorphe à celle de $\mathbb{Z}^k \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ qui évidemment est isomorphe à $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$. Elle ne peut donc être nulle que si $s = 0$, d'où la conclusion. ∎

Corollaire 15.8.2 *Soit A un groupe abélien* fini. *Alors A est (isomorphe à un) produit de groupes cycliques.*

Plus précisément, A est isomorphe à un groupe de la forme $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ où les d_i sont des entiers naturels > 1 avec $d_1 \mid d_2 \mid \cdots \mid d_s$. ∎

15.8.3. *Exercice.* [I 39] Montrer que la première assertion de 15.8.2 entraîne la seconde, en procédant comme suit :

(1) déduire de la première assertion que tout groupe abélien fini A est isomorphe à un groupe de la forme $\prod_{i=1}^{t} \mathbb{Z}/q_i\mathbb{Z}$ où chaque q_i est une puissance (d'exposant > 0) d'un nombre premier ;

(2) en déduire la seconde assertion.

15.8.4. *Exercice.* [S 97] Montrer que pour établir 15.8.2, il suffit de montrer que pour tout p premier, tout p-groupe abélien fini est produit de groupes cycliques.

15.9. *Exercices : questions d'unicité.* On se propose de montrer que les entiers $k, d_1, \ldots, d_s$ de 15.8 sont uniquement déterminés par A.

15.9.1. Avec A comme dans 15.8, montrer que A/A_{tors} est isomorphe à $\mathbb{Z}^k$. En déduire l'unicité de k.

15.9.2. [I 40] Avec les notations de l'exercice 15.8.3, montrer que les q_i trouvés sont uniques à l'ordre près.

En déduire l'unicité de la suite $(d_1, \ldots, d_s)$ de 15.8.2, puis celle de la suite $(d_1, \ldots, d_s)$ de 15.8.

16. Les théorèmes de Sylow

16.1. *Notations et conventions.* Dans tout ce paragraphe on désignera par p un nombre premier. On utilisera constamment la notion de p-groupe qui a été vue en 8.5. On conseille donc de relire la fin du paragraphe 8, d'autant plus que nous allons exploiter la formule des classes (8.4) de façon similaire aux raisonnements de 8.6 et 8.7.

Si G est un groupe fini, on appellera *p-sous-groupe* de G tout sous-groupe de G qui est un p-groupe.

16.1.1. *Devinette.* [S 98] À votre avis, pourquoi dire « p-sous-groupe » plutôt que « sous-p-groupe » ?

16.2. Soit G un groupe fini, et soit n son ordre. On peut écrire de façon unique

$$n = m\,p^r$$

où $r \in \mathbb{N}$ et où m est un entier positif premier à p. Si H est un p-sous-groupe de G, son ordre est une puissance de p qui divise n donc est de la forme p^s avec $0 \leq s \leq r$. De plus l'indice de H dans G est alors $m\,p^{r-s}$. Il revient donc au même, pour un sous-groupe de G, de dire que c'est un sous-groupe de G d'ordre p^r, ou que c'est un p-sous-groupe de G dont l'indice est premier à p.

Définition 16.3 *Soit G un groupe fini. Un* p-sous-groupe de Sylow *de G (ou, pour abréger, un* p-sylow *de G) est par définition un p-sous-groupe de G dont l'indice est premier à p.*

16.3.1. *Exemples idiots.* Si p ne divise pas $|G|$, le seul p-sylow de G est le sous-groupe trivial (et réciproquement !).

G est un p-groupe si et seulement si G est un p-sylow de G.

16.3.2. *Exemple un peu moins trivial.* Si G est un groupe cyclique d'ordre n, il admet pour chaque $d > 0$ divisant n un unique sous-groupe d'ordre d (cf. 12.6.1). En particulier, il admet un unique p-sylow, qui n'est autre (vérifier !) que l'ensemble des éléments de G dont l'ordre est une puissance de p.

16.3.3. *Exercice.* [I 41] Plus généralement, si G est un groupe fini *commutatif*, montrer que l'ensemble des éléments de G dont l'ordre est une puissance de p est l'unique p-sylow de G.

16.3.4. *Exercice.* [S 99] Soit k un corps fini de caractéristique p, soit $G = \mathrm{GL}_d(k)$ ($d \in \mathbb{N}$ donné) et soit U le « groupe triangulaire unipotent », i.e. le sous-groupe de

G formé des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. Montrer que U est un p-sylow de G.

16.3.5. *Exercice.* Soit G' un sous-groupe d'un groupe fini G, et soit S un p-sylow de G.

(1) [S 100] Montrer par un exemple que $G' \cap S$ n'est pas toujours un p-sylow de G'.

(2) [I 42] Montrer qu'il existe $g \in G$ tel que $G' \cap gSg^{-1}$ soit un p-sylow de G'.

16.3.6. *Exercice.* Déduire des exercices 16.3.4, 16.3.5 et 6.13.1 que tout groupe fini admet au moins un p-sylow. (Le résultat est aussi conséquence des théorèmes de Sylow ci-dessous, plus précis).

Théorème 16.4 (théorèmes de Sylow) *Soit G un groupe fini d'ordre $n = m\,p^r$ avec $r \in \mathbb{N}$ et m premier à p. Pour tout entier s tel que $0 \leq s \leq r$, notons X_s l'ensemble des sous-groupes de G d'ordre p^s. Alors :*

(i) *pour tout $s \in \{0, \ldots, r\}$ on a $|X_s| \equiv 1 \pmod{p}$, et en particulier X_s n'est pas vide ;*

(ii) *pour tout p-sous-groupe H et tout p-sylow S de G, il existe $g \in G$ tel que $H \subset gSg^{-1}$;*

(iii) *tout p-sous-groupe de G est contenu dans un p-sylow de G ;*

(iv) *le nombre des p-sylows de G est congru à 1 modulo p, et divise m ; deux p-sylows quelconques de G sont conjugués.*

Démonstration. La partie subtile est (i) ; nous commencerons par montrer les autres, en supposant (i) établie.

16.4.1. Montrons (ii). Pour cela, considérons l'action à gauche par translations de H sur G/S (associant à $h \in H$ et à la classe $\gamma S \in G/S$ la classe $h\gamma S$). Comme H est un p-groupe et que $|G/S| = m$ est premier à p, il résulte de 8.6 que le nombre de points fixes de cette action est premier à p donc n'est pas nul. Autrement dit, il existe $\gamma \in G$ tel que $H\gamma S = \gamma S$, ce qui équivaut à $\gamma^{-1}H\gamma S = S$, c'est-à-dire à $\gamma^{-1}H\gamma \subset S$, ou encore à $H \subset \gamma S\gamma^{-1}$, d'où l'assertion. (On n'a pas encore utilisé (i) ; ça vient !)

16.4.2. L'assertion (iii) résulte immédiatement de (ii), du fait qu'il existe au moins un p-sylow dans G (conséquence de (i)) et du fait que, bien sûr, avec les notations de (ii), gSg^{-1} est un p-sylow.

16.4.3. Montrons (iv) : l'assertion de conjugaison résulte de (iii) appliqué dans le cas particulier où le p-sous-groupe H considéré est lui-même un p-sylow (remarquer que H et gSg^{-1} ont alors même ordre). Le fait que $|X_r| \equiv 1 \pmod{p}$ est un cas particulier de (i). Enfin considérons l'action de G sur X_r par *conjugaison* : l'assertion

de conjugaison des p-sylows se reformule en disant que cette action est transitive, ce qui implique que $|X_r|$ divise $|G| = m\,p^r$ tout en étant premier à p, donc divise m (« lemme de Gauss »).

16.4.4. *Exercice.* [S 101] Avant de passer à la preuve de 16.4(i) : parmi les assertions précédentes, lesquelles peuvent se déduire de l'exercice 16.3.6 à la place de 16.4(i) ?

16.4.5. Pour montrer 16.4(i), fixons $s \in \{0, \ldots, r\}$ et notons E_s l'ensemble des *parties à p^s éléments* de G. De l'action à gauche de G sur lui-même par translations on déduit une action de G sur E_s (à $g \in G$ et à $A \in E_s$ on associe le translaté gA de A). En particulier, chaque $A \in E_s$ admet un stabilisateur $G_A = \{g \in G \mid gA = A\}$ et une orbite $\mathrm{O}(A)$, ensemble des parties de G de la forme gA pour un $g \in G$.

Parmi les éléments de E_s figurent notamment ceux de X_s, et aussi leurs translatés (c'est-à-dire les classes à gauche et à droite de G modulo ses sous-groupes d'ordre p^s). Le point essentiel de la preuve de 16.4(i) va consister à caractériser les translatés à droite d'éléments de X_s, parmi les éléments de E_s, en termes de l'action de G sur E_s.

16.4.6. *Exercice.* [S 102] Pourquoi la notation $\mathrm{O}(A)$ plutôt que GA ?

Lemme 16.4.7 *On garde les notations de* 16.4.5.

Soit A un élément de E_s. Alors A est une réunion disjointe de classes à droite modulo G_A. Il existe $i \in \{0, \ldots, s\}$ tel que $|G_A| = p^i$, et l'on a $|\mathrm{O}(A)| = m\,p^{r-i}$.

Démonstration. Par définition de G_A, A est une partie de G stable par translations à gauche sous G_A. C'est donc une réunion (forcément disjointe) d'orbites de G sous G_A, c'est-à-dire de classes à droite sous G_A. Comme toutes ces classes ont même cardinal que G_A il s'ensuit que le cardinal de G_A divise celui de A qui est p^s, donc a bien la forme annoncée. La dernière assertion en résulte par 8.2. ∎

Lemme 16.4.8 *Avec les notations de* 16.4.7, *les conditions suivantes sont équivalentes :*

(i) $|G_A| = p^s$ (« G_A est aussi gros que possible ») ;

(ii) $|\mathrm{O}(A)| = m\,p^{r-s}$ (« $\mathrm{O}(A)$ est aussi petite que possible ») ;

(iii) $|\mathrm{O}(A)| \not\equiv 0 \pmod{m\,p^{r-s+1}}$ (« $|\mathrm{O}(A)|$ est aussi peu divisible par p que possible ») ;

(iv) *A est une classe à droite modulo un sous-groupe de G ;*

(v) $\mathrm{O}(A) \cap X_s \neq \emptyset$;

(vi) *$\mathrm{O}(A)$ contient un unique élément de X_s.*

Démonstration. L'équivalence des conditions (i) à (iii) résulte du lemme 16.4.7 (si $|G_A| = p^i$ elles équivalent toutes à « $i = s$ »).

Si elles sont satisfaites alors (iv) l'est aussi : comme $|A| = |G_A|$ et que A est une réunion disjointe de classes à droite modulo G_A, il est lui-même une classe à droite.

(iv)⇒(v) : si A est de la forme $H\gamma$ où $\gamma \in G$ et où H est un sous-groupe de G, alors nécessairement H est d'ordre p^s et d'autre part $\mathrm{O}(A)$ contient l'élément $\gamma^{-1}A = \gamma^{-1}H\gamma$ qui est bien un élément de X_s.

(v)⇒(vi) : si $H \in \mathrm{O}(A)$ est un sous-groupe de G, les autres éléments de $\mathrm{O}(A)$ sont les classes à gauche modulo H et ne sont donc pas, sauf H lui-même, des sous-groupes.

(vi)⇒(i) : comme on vient de le dire, si $H \in \mathrm{O}(A)$ est un sous-groupe de G (d'ordre p^s), alors A est de la forme γH (pour un $\gamma \in G$ d'où $A = (\gamma H\gamma^{-1})\gamma$ de sorte que G_A contient $\gamma H\gamma^{-1}$ qui est d'ordre p^s. Comme $|G_A| \leq p^s$ de toute façon, (i) est démontré. ∎

Lemme 16.4.9 *On a la congruence :*

$$\binom{n}{p^s} \equiv |X_s|\, m\, p^{r-s} \pmod{m\, p^{r-s+1}}.$$

De plus la classe de l'entier $|X_s|$ modulo p ne dépend que des entiers n (l'ordre de G), p et s (et non du groupe G)

Démonstration. Le cardinal de E_s est $\binom{n}{p^s}$; il est réunion disjointe d'orbites de deux types : celles à $m\, p^{r-s}$ éléments, lesquelles correspondent bijectivement aux éléments de X_s (équivalences (ii) ⇔ (v) ⇔ (vi) de 16.4.8), et celles dont le cardinal est multiple de $m\, p^{r-s+1}$ (c'est l'équivalence (ii) ⇔ (iii)). La congruence cherchée en résulte.

La dernière assertion s'en déduit : si G' est un autre groupe d'ordre n, et X'_s l'ensemble de sous-groupes correspondant, on en tire en effet que $|X_s|\, m\, p^{r-s} - |X'_s|\, m\, p^{r-s}$ est divisible par $m\, p^{r-s+1}$ donc $|X_s| - |X'_s|$ est divisible par p. ∎

16.4.10. *Fin de la démonstration du théorème.* La manière « naturelle » de procéder consisterait à démontrer la congruence $\binom{m\,p^r}{p^s} \equiv m\, p^{r-s} \pmod{m\, p^{r-s+1}}$, valable pour des entiers naturels m, p, r, s avec p premier, $s \leq r$ et m non divisible par p. C'est possible mais par un calcul assez pénible, et il est bien plus élégant de s'en tirer (et d'obtenir ladite congruence comme sous-produit) en remarquant que, vu l'assertion d'invariance de 16.4.9, il suffit de prouver 16.4(i) pour *un* groupe G d'ordre n pour l'établir pour tous. Or l'assertion est claire pour $G = (\mathbb{Z}/n\mathbb{Z}, +)$ puisque dans ce cas $|X_s| = 1$, cf. 16.3.2. ∎

16.5. *Exercice : une autre démonstration de l'existence.* Nous avons vu dans 16.3.6 une démonstration de l'existence de p-sous-groupes de Sylow, qui toutefois ne donnait pas l'importante congruence de la partie (i) du théorème.

Voici maintenant une autre démonstration, qui est sans doute la plus naturelle et qui prouve, avec les notations du théorème, l'existence d'un sous-groupe d'ordre p^s de G, pour chaque entier s tel que $0 \leq s \leq r$. On procède par récurrence sur $n = |G|$, en supposant $s > 0$ (sinon tout est trivial). On suppose donc l'assertion

vérifiée (avec p fixé, disons) pour tout groupe G' d'ordre $< n$ et « tout s tel que p^s divise $|G'|$ ».

On remarque alors que :

(i) si G admet un sous-groupe H d'ordre $m'p^r$ avec $m' < m$ (c'est-à-dire un sous-groupe strict d'indice premier à p), alors l'assertion est vraie pour G (appliquer l'hypothèse de récurrence à H) ;

(ii) si G admet un sous-groupe H distingué d'ordre p, alors l'assertion est vraie pour G (appliquer l'hypothèse de récurrence à G/H, en « remplaçant s par $s-1$ », et en considérant l'image réciproque dans G du sous-groupe de G/H obtenu).

Pour appliquer ces remarques, on considère ensuite le centre C de G. Si son ordre est divisible par p, on applique la remarque (ii) ci-dessus, et 13.4.2(i) (remarquer que C est commutatif et que tout sous-groupe de C est distingué dans G). Sinon, on applique la formule des classes à l'action de G sur lui-même par conjugaison (dont C est l'ensemble des points fixes) pour trouver, parmi les stabilisateurs, un sous-groupe de G auquel la remarque (i) s'applique.

17. Produits semi-directs

17.1. *Suites exactes.*

17.1.1. On dit que deux morphismes de groupes composables

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \tag{17.1.1.1}$$

forment une *suite exacte* si l'on a $\operatorname{Im} f_1 = \operatorname{Ker} f_2$. Ceci implique notamment que $f_2 \circ f_1$ est trivial (condition qui équivaut à $\operatorname{Im} f_1 \subset \operatorname{Ker} f_2$), et aussi que $\operatorname{Im} f_1$ est un sous-groupe distingué de G_2.

Si G_1 (resp. G_3) est trivial, dire que $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$ est exacte équivaut simplement à dire que f_2 est injectif (resp. que f_1 est surjectif) : vérifiez !

Plus généralement, une suite $\cdots \to G_{i-1} \to G_i \to G_{i+1} \to \cdots$ de morphismes de groupes (où i parcourt un intervalle de $\mathbb{Z}$) est exacte si chaque couple de morphismes consécutifs forme une suite exacte.

17.1.2. *Suites exactes courtes.* En particulier, dire qu'une suite

$$1 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to 1 \tag{17.1.2.1}$$

(où « 1 » désigne le groupe trivial) est exacte signifie que f_1 est injectif, f_2 surjectif, et $\operatorname{Im} f_1 = \operatorname{Ker} f_2$. En d'autres termes, f_1 induit un isomorphisme de G_1 sur un sous-groupe distingué N de G_2, et f_2 un isomorphisme de G_2/N sur G_3. On appelle parfois *suite exacte courte* une suite de cette forme.

Ainsi, si G est un groupe et N un sous-groupe distingué de G, on a une suite exacte courte, dite « canonique » :

$$1 \to N \xrightarrow{j} G \xrightarrow{\pi} G/N \to 1 \tag{17.1.2.2}$$

où j (resp. π) est l'injection (resp. la surjection) canonique.

17.1.3. On a une notion de *morphisme* d'une suite exacte $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$ dans une suite exacte $G'_1 \xrightarrow{f'_1} G'_2 \xrightarrow{f'_2} G'_3$: c'est la donnée de morphismes de groupes φ_i : $G_i \to G'_i$ $(i = 1, 2, 3)$ rendant commutatif le diagramme suivant :

$$\begin{array}{ccccc} G_1 & \xrightarrow{f_1} & G_2 & \xrightarrow{f_2} & G_3 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ G'_1 & \xrightarrow{f'_1} & G'_2 & \xrightarrow{f'_2} & G'_3 \end{array}$$

(c'est-à-dire que $f'_1\varphi_1 = \varphi_2 f_1$ et $f'_2\varphi_2 = \varphi_3 f_2$).

Un tel morphisme est un *isomorphisme* si les φ_i sont des isomorphismes.

17.1.4. *Exercice.* [S 103] Montrer que toute suite exacte courte (17.1.2.1) est isomorphe à une suite exacte (17.1.2.2) avec $G = G_2$.

17.1.5. *Exemples de suites exactes* (les flèches non définies sont les flèches évidentes) :

(i) $0 \to \mathbb{Z} \xrightarrow{\times r} \mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \to 0$, où r est un entier non nul (ici il semble plus naturel de noter 0 le groupe trivial, les autres étant notés additivement) ;

(ii) $1 \to N \xrightarrow{i} N \times H \xrightarrow{p} H \to 1$, où N et H sont deux groupes quelconques, $i(n) = (n, e_H)$ et $p(n,h) = h$;

(iii) $0 \to \mathbb{Z} \xrightarrow{\times 2i\pi} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \to 1$, où exp est l'exponentielle ;

(iv) $1 \to \mathrm{A}_r \longrightarrow \mathfrak{S}_r \xrightarrow{\varepsilon} \{\pm 1\} \to 1$ où r est un entier ≥ 2 (pourquoi cette restriction ?) ;

(v) $1 \to \mathrm{SL}(r,k) \longrightarrow \mathrm{GL}(r,k) \xrightarrow{\det} k^* \to 1$ où k est un corps et r un entier ≥ 1 (pourquoi ?) ;

(vi) $0 \to \mathbb{Z} \xrightarrow{\times 2\pi} \mathbb{R} \xrightarrow{\rho} \mathrm{O}(2,\mathbb{R}) \xrightarrow{\det} \{\pm 1\} \to 1$ où $\rho(\theta)$ est la rotation d'angle θ, c'est-à-dire $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

17.1.6. *Extensions.* Lorsque l'on a une suite exacte courte telle que (17.1.2.1), on dit souvent que G_2 est *extension de G_3 par G_1* : cela signifie donc que G_2 admet un sous-groupe distingué isomorphe à G_1, à quotient isomorphe à G_3. (Attention à l'ordre : le « grand » groupe est extension du *quotient* par le *sous-groupe*).

Par exemple, $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$ sont tous deux extensions de $\mathbb{Z}/2\mathbb{Z}$ par lui-même.

La recherche de toutes les extensions d'un groupe donné par un autre, également donné, a une grande importance dans la classification des groupes. Si l'on veut étudier un groupe G donné, il est naturel de fractionner le problème en cherchant un sous-groupe distingué non trivial N de G : on est ainsi ramené, d'une part, à l'étude des deux groupes « plus petits » N et $\overline{G} = G/N$, et d'autre part à celle des extensions de $\overline{G}$ par N.

On donne aussi parfois le nom d'extension à toute suite exacte courte de groupes ; on dit qu'une telle extension est *triviale* si elle est isomorphe à une extension « produit », i.e. du type 17.1.5(ii). Ainsi, dire qu'un groupe G_2 est « extension triviale » de G_3 par G_1 revient simplement à dire qu'il est isomorphe au groupe produit $G_1 \times G_3$.

Définition 17.2 *Soit $f : G \to G'$ un morphisme de groupes. Une* section *de f est un morphisme $s : G' \to G$ tel que $f \circ s = \mathrm{Id}_{G'}$.*

17.2.1. *Remarque.* Toute section est évidemment injective, et l'existence d'une section implique que f est surjectif. La réciproque est fausse : par exemple le morphisme

canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ n'a pas de section.

17.2.2. *Remarque sur le vocabulaire.* Si X et Y sont deux ensembles et $f : X \to Y$ une application, on appelle parfois *section* de f toute *application* $s : Y \to X$ tel que $f \circ s = \mathrm{Id}_Y$. On a aussi des variantes évidentes dans le monde des morphismes d'anneaux, des applications linéaires... Ici, nous réserverons le mot « section », conformément à la définition qui précède, *au cas des morphismes de groupes* ; dans le cas d'une application $f : X \to Y$ comme ci-dessus, on parlera de « section ensembliste ».

Ainsi le morphisme canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ a des sections ensemblistes, comme par exemple l'application s définie par $s(0 \bmod 2) = 0$, $s(1 \bmod 2) = -53$.

Plus généralement, si G est un groupe et H un sous-groupe de G, le choix d'une section ensembliste de l'application canonique de G dans $H\backslash G$ équivaut au choix d'un système de représentants de G modulo H (7.4.1).

Enfin, *l'axiome du choix* peut se formuler en disant que toute application surjective admet une section ensembliste.

17.2.3. *Exercice* (qui n'a rien à voir avec les groupes). Montrer l'équivalence des trois versions suivantes de l'axiome du choix :

(i) toute surjection admet une section ensembliste ;

(ii) si $(E_i)_{i\in I}$ est une famille d'ensembles non vides (indexée par un ensemble I quelconque), alors le produit $\prod_{i\in I} E_i$ n'est pas vide ;

(iii) tout ensemble E admet une « fonction de choix », c'est-à-dire une application φ de l'ensemble P des parties non vides de E dans E telle que l'on ait $\varphi(A) \in A$ pour tout $A \in P$.

17.2.4. *Image d'une section ensembliste.* Si $s : Y \to X$ est une section ensembliste d'une application $f : X \to Y$, l'image de s est un sous-ensemble Y' de X tel que $f_{|Y'} : Y' \to Y$ soit bijective ; inversement, si Y' est un tel sous-ensemble de X, il est l'image d'une unique section ensembliste s de f, donnée par $s = (f_{|Y'})^{-1}$ (vérifications immédiates).

En d'autres termes, l'application $s \mapsto \mathrm{Im}\, s$ est une bijection de l'ensemble des sections ensemblistes de f sur l'ensemble des parties Y' de X tel que $f_{|Y'} : Y' \to Y$ soit bijective. Noter que si f n'est pas surjective, les deux ensembles sont vides ; la réciproque n'est autre que l'axiome du choix.

17.2.5. *Exercice.* [S 104] Il y a un abus d'écriture dans la formule $s = (f_{|Y'})^{-1}$: lequel ?

17.2.6. *Sections et sous-groupes.* Gardons les notations de 17.2.4, en supposant de plus que X et Y sont des groupes et f un morphisme. Alors une section ensembliste s est une section (i.e. un morphisme de groupes) si et seulement si son image Y' est un sous-groupe de X : le « seulement si » est clair, et le « si » résulte de la formule $s = (f_{|Y'})^{-1}$ ci-dessus, ou d'un raisonnement direct.

On a donc une bijection (encore donnée par $s \mapsto \operatorname{Im} s$) de l'ensemble des sections de f sur l'ensemble des sous-groupes Y' de X tel que $f_{|Y'} : Y' \to Y$ soit un isomorphisme. Si f n'est pas surjectif, les deux ensembles sont vides ; la réciproque est fausse.

17.2.7. *Sections et sous-groupes (suite).* Nous pouvons formuler autrement les conditions de 17.2.6. Prenons d'abord des notations plus conformes à la tradition : soit $\pi : G \to \overline{G}$ un morphisme de groupes, et soit $N = \operatorname{Ker} \pi$. La discussion qui va suivre n'a d'intérêt que si π est surjectif ; dans ce cas, si H est un sous-groupe de G, on a les équivalences suivantes :

- $\pi_{|H}$ est injectif $\Leftrightarrow N \cap H = \{e\}$;
- $\pi_{|H}$ est surjectif $\Leftrightarrow NH = G$.

En effet, le noyau de $\pi_{|H}$ est $N \cap H$, et d'autre part on rappelle (10.6) que $HN = NH = \pi^{-1}(\pi(H))$.

Définition 17.3 *Soit*

$$1 \to N \xrightarrow{j} G \xrightarrow{\pi} \overline{G} \to 1 \qquad (17.3.1)$$

une suite exacte de groupes. On dit que c'est une suite scindée, *ou que G est une extension scindée de $\overline{G}$ par N, si π admet au moins une section.*

17.3.1. *Remarque.* D'après 17.2.6, la suite (17.3.1) est scindée si et seulement si il existe un sous-groupe H de G tel que $\pi_{|H}$ soit bijectif, ou encore (17.2.7) tel que $j^{-1}(H) = \{e_N\}$ et $H\, j(N) = G$.

17.4. *Exemples.* Reprenons les exemples de 17.1.5.

17.4.1. *Exercice.* [S 105] Les suites 17.1.5(i) et (iii) ne sont pas scindées.

17.4.2. La suite « produit » 17.1.5(ii) est scindée, avec $s(h) = (e_N, h)$; le sous-groupe de $N \times H$ correspondant est $\{e_N\} \times H$.

Autrement dit, toute extension triviale (17.1.6) est scindée.

17.4.3. *Exercice.* Plus généralement, dans l'exemple 17.1.5(ii), montrer que les sections de p sont les applications de la forme $h \mapsto (\varphi(h), h)$ où φ est un morphisme de H dans N.

17.4.4. La suite 17.1.5(iv) (groupe symétrique) est scindée, en prenant pour H un sous-groupe de $G = \mathfrak{S}_r$ de la forme $H = \{e, \tau\}$ où τ est une transposition quelconque. La section s correspondante est définie par $s(1) = e$, $s(-1) = \tau$.

17.4.5. *Exercice.* [S 106] Dans l'exemple 17.1.5(iv) précédent, trouver *toutes* les sections de ε.

17.4.6. La suite 17.1.5(v) (groupe linéaire) est scindée, en définissant $s : k^* \to \mathrm{GL}(r,k)$ par $s(\lambda) =$ la matrice diagonale $\mathrm{diag}(\lambda, 1, \ldots, 1)$. Le sous-groupe correspondant est constitué par les matrices diagonales dont tous les éléments diagonaux, autres que le premier, sont égaux à 1.

17.5. *Autres exemples de suites exactes scindées.*

17.5.1. Soit k un corps. Alors toute suite exacte courte $0 \to U \xrightarrow{j} V \xrightarrow{\pi} W \to 0$ de k-espaces vectoriels, où j et π sont k-linéaires, est scindée (et même triviale). Plus précisément, une variante immédiate de la discussion de 17.2.7 fournit une bijection entre l'ensemble des *sections k-linéaires* de π et l'ensemble des sous-espaces de V *supplémentaires* de $j(V)$; or on sait que tout sous-espace de V admet un supplémentaire. (Ce dernier énoncé a été vu en DEUG lorsque V est de dimension finie ; il est vrai sans cette hypothèse, mais la démonstration utilise l'axiome du choix).

17.5.2. Pour r entier ≥ 1, la suite naturelle

$$1 \longrightarrow \mathrm{SO}(r,\mathbb{R}) \longrightarrow \mathrm{O}(r,\mathbb{R}) \xrightarrow{\det} \{-1,+1\} \longrightarrow 1$$

est scindée par le sous-groupe $H = \{\mathrm{Id}, \tau\}$ de $\mathrm{O}(r,\mathbb{R})$, où τ est la symétrie orthogonale par rapport à un hyperplan (ou plus généralement un sous-espace de codimension impaire). La section s correspondante est définie par $s(1) = \mathrm{Id}$, $s(-1) = \tau$.

17.5.3. *Exercice.* Dans l'exemple 17.5.2 précédent, trouver *toutes* les sections de det.

17.5.4. *Le groupe affine.* Fixons un corps k. Une application $f : V \to W$ d'un k-espace vectoriel dans un autre est dite *affine* si elle est composée d'une application linéaire et d'une translation, c'est-à- dire de la forme $x \mapsto f_0(x)+w$, avec $f_0 : V \to W$ linéaire et $w \in W$. (Ainsi, les applications affines de k dans k sont celles de la forme $x \mapsto ax + b$, avec $a, b \in k$). Noter que f_0 et w sont alors uniquement déterminés par f, puisque $w = f(0_V)$. On dit que f_0 est *l'application linéaire associée à f*. De plus, comme la translation $y \mapsto y + w$ est bijective, on voit tout de suite que f est injective (resp. surjective, bijective) si et seulement si f_0 a la même propriété.

Prenons en particulier $W = V$: alors l'ensemble des applications affines bijectives de V dans V est un sous-groupe de $\mathfrak{S}(V)$, appelé *groupe affine* et noté $\mathrm{GA}(V)$.

Le lecteur vérifiera alors qu'on a une suite exacte

$$1 \longrightarrow (V,+) \xrightarrow{t} \mathrm{GA}(V) \xrightarrow{\pi} \mathrm{GL}(V) \longrightarrow 1$$

où $t(v)$ est la translation par v et $\pi(f)$ est l'application linéaire associée à f. Cette suite est scindée par l'inclusion naturelle de $\mathrm{GL}(V)$ dans $\mathrm{GA}(V)$.

17.5.5. *Remarque.* Dans les exemples ci-dessus, le lecteur perspicace aura observé que le sous-groupe N de G est souvent « naturel » alors que H résulte d'un choix plus ou moins arbitraire (exemples : choix d'une transposition dans 17.4.4, d'un numéro de colonne dans 17.4.6, d'un hyperplan dans 17.5.2).

17.6. *Analyse d'une suite scindée.* On se propose, étant donnés deux groupes N et $\overline{G}$, de « classifier » toutes les extensions scindées de $\overline{G}$ par N.

17.6.1. On se donne donc une suite exacte

$$1 \longrightarrow N \xrightarrow{j} G \xrightarrow{\pi} \overline{G} \longrightarrow 1 \qquad (17.6.1.1)$$

et l'on suppose donnée une section s de π, d'image H dans G.

On supposera de plus, pour alléger les notations, que N est un sous-groupe de G et que j est le morphisme d'inclusion ; cela suffit pour nos besoins, car toute suite exacte (17.6.1.1) est isomorphe à une suite ayant cette propriété (celle que l'on obtient en remplaçant N par son image dans G).

17.6.2. *Remarque.* Plutôt qu'une suite exacte (17.6.1.1), il reviendrait au même de se donner un groupe G et deux sous-groupes N et H de G tels que $N \lhd G$, $NH = G$ et $N \cap H = \{e\}$.

17.6.3. On a alors une application

$$\begin{array}{rccc} m : & N \times H & \longrightarrow & G \\ & (n,h) & \longmapsto & nh. \end{array}$$

Montrons qu'elle est *bijective.* Son image dans G est $NH = \pi^{-1}(\pi(H))$ d'après 10.6, donc est bien G puisque $\pi_{|H}$ est surjectif.

Pour l'injectivité, soient (n,h) et (n',h') dans $N \times H$ tels que $nh = n'h'$. On en déduit que $\pi(h) = \pi(h')$ donc que $h = h'$ puisque $\pi_{|H}$ est injectif, et l'égalité $nh = n'h'$ entraîne donc que $n = n'$, cqfd.

En d'autres termes, nous venons de montrer que tout élément x de G sécrit de manière unique $x = nh$ avec $n \in N$ et $h \in H$.

17.6.4. *Remarque.* Ceux qui pensent avoir montré l'injectivité de m en cherchant son noyau ont perdu : en général, m n'est *pas un morphisme de groupes* du groupe produit $N \times H$ dans G, bien que son image soit un sous-groupe de G.

17.6.5. *Exercice.* Montrer que l'application m de 17.6.3 est un morphisme de groupes si et seulement si N et H commutent (c'est-à-dire si $nh = hn$ pour tout $n \in N$ et tout $h \in H$), et que dans ce cas l'extension est *triviale.*

17.6.6. *Remarque.* Il peut arriver, avec deux sous-groupes N et H *non distingués*, que l'application m de 17.6.3 soit bijective. Voici un exemple : on prend $G =$

$\mathrm{GL}(n,\mathbb{R})$ ($n \geq 2$), $H = \mathrm{O}(n,\mathbb{R})$, et on note N le sous-groupe de G formé des matrices triangulaires supérieures à éléments diagonaux positifs. Il est immédiat que H et N ne sont pas distingués, et le fait que m soit bijective dans ce cas est équivalent au théorème d'orthogonalisation de Gram-Schmidt.

17.6.7. *Exercice.* Montrer que l'application $m' : H \times N \to G$ définie par $m'(h,n) = hn$ est aussi bijective.

17.6.8. *Le calcul fondamental.* Bien que m ne soit pas un morphisme *du groupe produit* $N \times H$ dans G, c'est, comme nous l'avons vu, une bijection, de sorte qu'il existe (par « transport de structure ») une unique loi de groupe sur $N \times H$ faisant de m un morphisme (et en fait un isomorphisme). Nous allons calculer cette loi, que nous noterons $*$. On a par définition, pour (n,h) et (n',h') dans $N \times H$:

$$\begin{aligned}(n,h) * (n',h') &= m^{-1}(m(n,h)\,m(n',h')) \\ &= m^{-1}(nhn'h') \\ &= m^{-1}(n(hn'h^{-1})hh') \\ &= (n(hn'h^{-1}), hh').\end{aligned}$$

(Dans ce calcul, *qu'il faut savoir refaire rapidement,* on a utilisé le fait que, puisque N est distingué, $hn'h^{-1} \in N$, de sorte que le résultat est bien un élément de $N \times H$; en termes imagés, la conjugaison par h a permis de « faire passer n' devant h » dans le produit $nhn'h'$).

17.6.9. *Exercice.* Refaire le calcul de 17.6.8 dix fois sans regarder.

17.6.10. Le calcul qui précède a une conséquence importante : il montre que, non seulement on peut « décrire » l'ensemble G au moyen de N et H (via l'application m) mais la loi de groupe de G est elle-même *entièrement déterminée* par les données suivantes :

- les lois de N et H ;
- l'action de H sur N par automorphismes intérieurs dans G, c'est-à-dire l'application $(h,n) \mapsto hnh^{-1}$ de $H \times N$ dans N.

Noter que l'action en question est une action à gauche par automorphismes, c'est-à-dire qu'elle correspond à un morphisme de groupes $\varphi : H \to \mathrm{Aut}(N)$.

D'autre part, il est parfois commode de voir cette action comme une action de $\overline{G}$ (ou de G/N) sur N, puisque π induit un isomorphisme de H sur $\overline{G}$, d'inverse la section s. Explicitement, à $x \in \overline{G}$ on associe l'automorphisme de N « conjugaison par $s(x)$ dans G ». Noter que pour définir cette action de $\overline{G}$ il est nécessaire de connaître s.

17.7. Explicitons l'action de H (ou de $\overline{G}$) sur N dans les exemples déjà rencontrés :

17.7.1. Pour une extension triviale (17.1.5(ii) et 17.4.2), l'action est triviale. Il est facile de vérifier la réciproque ; cf. l'exercice 17.6.5.

17.7.2. De façon générale, comme l'action de H est donnée par les automorphismes intérieurs de G, elle est triviale chaque fois que G (donc aussi N et H) est *commutatif* : autrement dit, *une extension commmutative est triviale si et seulement si elle est scindée.*

17.7.3. Dans 17.1.5(iv) et 17.4.4 (groupe symétrique) l'élément $-1 \in \overline{G}$ opère sur $N = \mathrm{A}_r$ par la conjugaison par τ dans $G = \mathfrak{S}_r$; la situation est analogue dans 17.5.2 (groupe orthogonal).

17.7.4. Dans 17.1.5(v) et 17.4.6 (groupe linéaire), $\lambda \in K^*$ opère sur une matrice de $\mathrm{SL}(r, K)$ de la façon suivante : on multiplie la première ligne par λ, puis la première colonne par λ^{-1}.

17.7.5. Dans 17.5.4 (groupe affine), $\mathrm{GL}(V)$ opère sur $(V, +)$ par son action à gauche naturelle. Vérifiez !

17.8. *Où l'on renverse la vapeur : synthèse de suites exactes scindées.* Supposons maintenant donnés deux groupes N et H, et un morphisme de groupes $\varphi : H \to \mathrm{Aut}(N)$, correspondant à une action (à gauche) de H sur N par automorphismes, que nous noterons

$$\begin{array}{ccc} H \times N & \longrightarrow & N \\ (h, n) & \longmapsto & {}^h n \end{array}$$

(on a donc ${}^h n = (\varphi(h))(n)$). Ce qui précède montre qu'il existe (à isomorphisme près) *au plus un* groupe G qui soit extension scindée de H par N, de telle sorte que l'action de H sur N par conjugaison dans G soit donnée par φ. De plus, le calcul de 17.6.8 donne un candidat pour un tel groupe ; il reste à montrer qu'il vérifie les conditions voulues. Mais d'abord, il mérite un nom :

Définition 17.8.1 *Soient N et H deux groupes, et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme de groupes. On appelle* produit semi-direct *de N par H, relativement à φ, et l'on note*

$$N \rtimes_\varphi H,$$

l'ensemble produit $N \times H$ muni de la loi de composition

$$\begin{array}{ccc} (N \times H) \times (N \times H) & \longrightarrow & N \times H \\ ((n, h), (n', h')) & \longmapsto & (n\, {}^h n', hh') \end{array}$$

où l'on a posé ${}^h n' = (\varphi(h))(n')$.

17.8.2. On laisse le lecteur vérifier que $N \rtimes_\varphi H$ est un groupe, et que l'on a une suite exacte

$$1 \longrightarrow N \xrightarrow{j_{N,H}} N \rtimes_\varphi H \xrightarrow{\pi_{N,H}} H \longrightarrow 1 \qquad (17.8.2.1)$$

avec $j_{N,H}(n) = (n, e_H)$ et $\pi_{N,H}(n,h) = h$, scindée par la section $s_{N,H}$ donnée par $h \mapsto (e_N, h)$, et que l'action de H sur N associée est φ.

17.8.3. *Remarque.* Le rôle des groupes N et H n'est pas symétrique ; la notation $N \rtimes_\varphi H$ est faite pour rappeler que c'est N qui est distingué ($N \lhd G$).

17.9. *Exercices.* On garde les notations de 17.8.1. On pose $G = N \rtimes_\varphi H$ et on note multiplicativement la loi de groupe sur G ; les éléments neutres seront notés e s'il n'y a pas de confusion.

17.9.1. Montrer les formules $e_G = (e_N, e_H)$, $(n,h) = (n,e)(e,h)$ (dans cet ordre !), $(n,h)^{-1} = ({}^{h^{-1}}n^{-1}, h^{-1})$.

17.9.2. Montrer que les conditions suivantes sont équivalentes :

(i) les sous-groupes $N \times \{e\}$ et $\{e\} \times H$ de G commutent ;

(ii) G est le groupe produit de N par H ;

(iii) $\varphi : H \to \mathrm{Aut}\,(N)$ est le morphisme trivial ;

(iv) l'action donnée de H sur N est triviale ;

(v) $\{e\} \times H$ est distingué dans G.

17.9.3. Voici un exemple important : N est un groupe commutatif, $H = \{e, \tau\}$ est cyclique d'ordre 2, et φ envoie τ sur l'automorphisme $n \mapsto n^{-1}$ de N. Montrer que N est d'indice 2 dans G, que tout élément de $G - N$ est d'ordre 2, et que G est commutatif si et seulement si on a $x^2 = e$ pour tout $x \in G$.

17.9.4. [S 107] (1) Pourquoi, dans l'exemple 17.9.3, a-t-on pris N commutatif ?

(2) Plus généralement, soient G un groupe et N un sous-groupe d'indice 2 de G. On suppose que tout élément du complémentaire de N est d'ordre 2 dans G. Montrer que N est commutatif et que G est isomorphe au groupe de 17.9.3.

(3) Montrer que $G = \mathrm{O}\,(2, \mathbb{R})$ est un exemple d'une telle situation.

17.9.5. *Le groupe diédral.* Si, dans l'exemple 17.9.3, on prend N cyclique d'ordre r, on obtient un groupe d'ordre $2r$ appelé *groupe diédral d'ordre* $2r$ et noté D_r (parfois D_{2r} dans la littérature). Montrer que D_2 (resp. D_3) est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (resp. à $\mathfrak{S}_3$).

Pour r quelconque, désignons par ρ (resp. σ) un générateur de N (resp. H). Montrer que (avec les abus d'écriture habituels) tout élément de G s'écrit de manière unique sous la forme $\rho^a \sigma^b$ avec $0 \leq a < r$ et $b \in \{0,1\}$, la loi de groupe étant donnée par les règles $\rho^r = \sigma^2 = e$ et $\sigma\rho = \rho^{-1}\sigma$; on a plus généralement la formule

$$(\rho^a \sigma^b)(\rho^c \sigma^d) = \rho^{a+(-1)^b c} \sigma^{b+d}.$$

17.10. *Exercice : polygones réguliers.* [I 43] Fixons un entier $r \geq 3$. Dans le plan euclidien $\mathbb{R}^2$, soit X un ensemble de r points formant un polygone régulier centré à l'origine. Soit G le sous-groupe de $\mathrm{O}(2,\mathbb{R})$ formé des transformations orthogonales qui envoient X sur lui-même, et soit $N = G \cap \mathrm{SO}(2,\mathbb{R})$. Montrer que N est cyclique d'ordre r, et que G est isomorphe au groupe diédral D_r de 17.9.5

17.11. *Exercice.* [S 108] Soient N un groupe et u un automorphisme de N. Montrer qu'il existe un groupe G contenant (un groupe isomorphe à) N comme sous-groupe distingué, tel que u soit induit par un automorphisme *intérieur* de G.

17.12. *Exercice : groupes d'ordre $2p$ (p premier).* [S 109] Si p est un nombre premier, montrer que les seuls groupes d'ordre $2p$ (à isomorphisme près) sont $\mathbb{Z}/2p\mathbb{Z}$ et le groupe diédral D_p.

17.13. *Où l'on récapitule.* Partons d'une suite exacte courte (17.6.1.1), scindée par le choix d'une section s de π, d'image $H \subset G$. On en déduit un morphisme de groupes $\varphi : H \to \mathrm{Aut}(N)$, donc un groupe $N \rtimes H$, extension scindée de H par N comme en 17.8.2.1. On laisse le lecteur vérifier que l'on a alors un isomorphisme de suites exactes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{j_{N,H}} & N \rtimes_\varphi H & \xrightarrow{\pi_{N,H}} & H & \longrightarrow & 1 \\ & & \| & & \downarrow m & & \downarrow \pi_{|H} & & \\ 1 & \longrightarrow & N & \xrightarrow{j} & G & \xrightarrow{\pi} & \overline{G} & \longrightarrow & 1 \end{array}$$

où m est l'application de 17.6.3 (qui est bien un isomorphisme, par définition de la structure de groupe sur $N \rtimes_\varphi H$). Cet isomorphisme est de plus compatible aux sections données, c'est-à-dire que $m \circ s_{N,H} = s \circ \pi_{|H}$.

C'est pourquoi on dit souvent, par abus de langage, que G « est produit semi-direct » de N par H (ou par $\overline{G}$: le lecteur écrira lui-même une variante du diagramme ci-dessus utilisant $\overline{G}$ au lieu de H).

17.13.1. *Exercice.* Montrer que l'isomorphisme de suites exactes ci-dessus est le seul induisant l'identité sur N et le morphisme $\pi_{|H}$ sur H, et qui soit compatible aux sections.

18. Groupes simples

Définition 18.1 *Soit G un groupe, d'élément neutre e. On dit que G est* simple *si :*

(i) $G \neq \{e\}$;

(ii) *les seuls sous-groupes distingués de G sont G et $\{e\}$.*

Le lecteur a déjà fait l'exercice 9.5.1, il connaît donc la définition qui précède et les énoncés 18.2 et 18.3(i) qui suivent :

Proposition 18.2 *Soit G un groupe non réduit à l'élément neutre. Les conditions suivantes sont équivalentes :*

(i) *G est simple ;*

(ii) *pour tout groupe H, tout morphisme de G dans H est trivial ou injectif.*

Démonstration. (i)⇒(ii) : soit $f : G \to H$ un morphisme. Si G est simple, on a soit $\operatorname{Ker} f = \{e\}$ et f est injectif, soit $\operatorname{Ker} f = G$ et f est trivial.

(ii)⇒(i) : supposons (ii) et soit N un sous-groupe distingué de G. Le morphisme canonique $\pi : G \to G/N$ est alors soit trivial, soit injectif. Dans le premier cas, G/N est trivial (puisque π est surjectif) donc $N = G$; dans le second cas, $N = \operatorname{Ker} \pi = \{e\}$. Comme d'autre part G est non trivial par hypothèse, il est simple. ∎

Proposition 18.3 (i) *Soit G un groupe* commutatif. *Pour que G soit simple, il faut et il suffit qu'il soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier (autrement dit, que G soit fini d'ordre premier).*

(ii) *Soient p un nombre premier et G un p-groupe* (cf. 8.5). *Pour que G soit simple il faut et il suffit que G soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Dans les deux cas le « il suffit » est connu. Supposons donc G simple (et en particulier non trivial).

(i) Comme tout sous-groupe de G est distingué, G n'admet pas d'autre sous-groupe que G et $\{e\}$. En particulier, G est engendré par chacun de ses éléments distincts de e, et est donc monogène, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}$ convenable. L'étude des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (10.4) montre alors qu'un tel groupe est simple si et seulement si n est premier.

(ii) D'après 8.7, le centre de G n'est pas réduit à $\{e\}$. Comme c'est un sous-groupe distingué de G il est donc égal à G, ce qui signifie que G est commutatif. On conclut par (i). ∎

Théorème 18.4 *Soit G un groupe fini. Il existe un entier $s \in \mathbb{N}$ et une suite $(G_i)_{0 \leq i \leq s}$ de sous-groupes de G vérifiant :*

(i) $G_0 = \{e\}$ *et* $G_s = G$;

(ii) *pour tout* $i \in \{0, \ldots, s-1\}$, $G_i \lhd G_{i+1}$ *et* G_{i+1}/G_i *est simple.*

De plus (« théorème de Jordan-Hölder »*), l'entier* s *ne dépend que de* G*, de même que la suite des groupes* G_{i+1}/G_i*, à isomorphisme près et à l'ordre près (autrement dit, pour tout groupe simple* Γ*, le nombre d'indices* i *tels que* $G_{i+1}/G_i \sim \Gamma$ *ne dépend pas de la suite* $(G_i)_{0 \leq i \leq s}$ *vérifiant les propriétés ci-dessus).*

Démonstration. Nous admettrons ici l'assertion d'unicité. Pour l'existence on procède par récurrence sur $|G|$. Si G est trivial, prendre $s = 0$ et $G_0 = G$. Sinon, supposons (hypothèse de récurrence) l'énoncé vrai pour tout groupe d'ordre $< |G|$. Si G est simple, l'énoncé est immédiat avec $s = 1$, $G_0 = \{e\}$ et $G_1 = G$. Sinon, G admet un sous-groupe distingué H non trivial et distinct de G, de sorte que l'hypothèse de récurrence s'applique à H et à G/H, donnant des suites de groupes $H_0 \lhd H_1 \lhd \ldots \lhd H_r = H$ et $\Gamma_0 \lhd \Gamma_1 \lhd \ldots \lhd \Gamma_t = G/H$, à quotients successifs simples. Or le théorème 10.3 montre que chaque Γ_i est de la forme G_{r+i}/H où G_{r+i} est un sous-groupe de G (avec en particulier $G_{r+0} = H = G_r$, de sorte que la notation est cohérente), et que l'on a bien les propriétés voulues : $G_{r+i} \lhd G_{r+i+1}$, et G_{r+i}/G_{r+i+1} est simple car isomorphe à Γ_{i+1}/Γ_i. La suite $(G_i)_{0 \leq i \leq r+t}$ obtenue en mettant bout à bout les deux suites répond donc à la question. ∎

Définition 18.5 *Si* G *est un groupe fini, une suite* $(G_i)_{0 \leq i \leq s}$ *de sous-groupes de* G *vérifiant les propriétés du théorème* 18.4 *s'appelle une* suite de Jordan-Hölder *pour* G.

18.6. *Exemples.*

Nous avons déjà évoqué (9.5.2) le théorème suivant :

Théorème 18.6.1 (Galois) *Pour tout entier* $n \geq 5$*, le groupe alterné* A_n *est simple.*

Nous ne donnerons pas la démonstration, qui figure (souvent en exercice) dans de nombreux livres d'algèbre.

18.6.2. Le groupe $\mathbb{Z}/6\mathbb{Z}$ admet deux suites de Jordan-Hölder :

$$\begin{array}{ccccc} \{0\} & \subset & 2\mathbb{Z}/6\mathbb{Z} & \subset & \mathbb{Z}/6\mathbb{Z} \\ \{0\} & \subset & 3\mathbb{Z}/6\mathbb{Z} & \subset & \mathbb{Z}/6\mathbb{Z}; \end{array}$$

dans chaque cas, les deux quotients successifs sont isomorphes à $\mathbb{Z}/3\mathbb{Z}$ et à $\mathbb{Z}/2\mathbb{Z}$, mais pas dans le même ordre.

18.6.3. Dans le cas d'un groupe commutatif, (resp. d'un p-groupe), il résulte de 18.3 que les quotients successifs sont tous cycliques d'ordre premier (resp. tous isomorphes à $\mathbb{Z}/p\mathbb{Z}$). Des groupes non isomorphes peuvent donner les mêmes quotients de Jordan-Hölder (par exemple $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$).

18.6.4. [S 110] Pour chaque $n \in \mathbb{N}$, quels sont les quotients de Jordan-Hölder de $\mathfrak{S}_n$?

18.7. Nous allons maintenant étudier le groupe linéaire $G = \mathrm{GL}(n, K)$, où K est un corps commutatif et où $n \geq 2$ (si $n = 0$ le groupe est trivial, et si $n = 1$ il est isomorphe à K^*).

Ce groupe a deux sous-groupes distingués évidents :

- le groupe Δ des matrices scalaires, isomorphe à K^* et qui n'est autre que le centre de G ;
- le groupe $\mathrm{SL}(n, K)$ des matrices de déterminant 1 ; le quotient $G/\mathrm{SL}(n, K)$ s'identifie à K^* par le déterminant.

(Noter toutefois que lorsque $K = \mathbb{Z}/2\mathbb{Z}$, Δ est trivial et $\mathrm{SL}(n, K)$ est égal à G).

Le groupe $\Delta \cap \mathrm{SL}(n, K)$ est formé des matrices $\lambda \mathrm{I}_n$, où λ est une racine n-ième de l'unité dans K ; il est donc isomorphe au groupe $\mu_n(K)$ de 14.1.2.

On pose par définition

$$\mathrm{PGL}(n, K) = \mathrm{GL}(n, K)/\Delta \tag{18.7.1}$$

et d'autre part

$$\begin{aligned} \mathrm{PSL}(n, K) &= \mathrm{SL}(n, K)/\mathrm{SL}(n, K) \cap \Delta \\ &= \text{ image de } \mathrm{SL}(n, K) \text{ dans } \mathrm{PGL}(n, K). \end{aligned} \tag{18.7.2}$$

Ainsi, on a une suite de sous-groupes distingués de G :

$$\{\mathrm{I}_n\} \subset \mu_n(K)\mathrm{I}_n \subset \mathrm{SL}(n, K) \subset G$$

dont les quotients successifs sont isomorphes à $\mu_n(K)$, $\mathrm{PSL}(n, K)$ et K^*.

Théorème 18.8 (Jordan-Dickson) *Soient K un corps commutatif et n un entier ≥ 2. Alors le groupe $\mathrm{PSL}(n, K)$ est simple, sauf dans les deux cas suivants :*

- *$K \cong \mathbb{Z}/2\mathbb{Z}$ et $n = 2$;*
- *$K \cong \mathbb{Z}/3\mathbb{Z}$ et $n = 2$.*

18.8.1. *Exercice.* [I 44] Montrer que le groupe $\mathrm{PSL}(2, \mathbb{Z}/2\mathbb{Z})$ est isomorphe à $\mathfrak{S}_3$.

18.8.2. *Exercice.* [I 45] Montrer que le groupe $\mathrm{PSL}(2, \mathbb{Z}/3\mathbb{Z})$ est isomorphe à A_4.

18.9. Nous ne donnerons ici la preuve de 18.8 que dans le cas du groupe $\mathrm{PSL}(2, \mathbb{C})$, qui contient l'essentiel des idées.

Considérons donc un sous-groupe distingué de $\mathrm{PSL}(2, \mathbb{C})$, non réduit à l'élément neutre : il correspond à un sous-groupe distingué H de $G := \mathrm{SL}(2, \mathbb{C})$, contenant strictement le centre $C = \{\mathrm{I}_2, -\mathrm{I}_2\}$. Il s'agit de montrer que $H = G$.

Nous aurons pour cela à utiliser les éléments suivants de G :

$$t(z) := \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \quad (z \in \mathbb{C})$$
$$\delta(u) := \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \quad (u \in \mathbb{C}^*).$$

Observer que $z \mapsto t(z)$ et $u \mapsto \delta(u)$ sont des morphismes de $(\mathbb{C}, +)$ et de $(\mathbb{C}^*, \times)$, respectivement, dans G, et que l'on a la relation (qui servira plus loin)

$$[t(z), \delta(u)] = t(z)\,\delta(u)\,t(-z)\,\delta(u^{-1}) = t(z(1-u^2)) \tag{18.9.1}$$

pour tous $z \in \mathbb{C}$ et $u \in \mathbb{C}^*$ (on rappelle que $[a, b]$ est le commutateur $aba^{-1}b^{-1}$, cf. 4.4.9). Remarquons aussi que, si $h \in H$ et $g \in G$, on a $ghg^{-1} \in H$ donc aussi $[g, h] = (ghg^{-1})\,h^{-1} \in H$.

Soit maintenant h un élément de H qui n'est pas dans C (il en existe, par hypothèse). Ses valeurs propres sont deux nombres complexes λ, λ^{-1} inverses l'un de l'autre puisque $h \in G$. On a trois cas :

- $\lambda = 1$: alors h est semblable à une matrice $t(z)$, avec $z \neq 0$ (sinon on aurait $h = \mathrm{I}_2$) ;
- $\lambda = -1$: alors $-h \in H$ relève du cas précédent ;
- $\lambda \neq \pm 1$: alors $\lambda \neq \lambda^{-1}$, donc h est diagonalisable, et donc semblable à la matrice $\delta(\lambda)$.

Observer de plus que « h est semblable à h' » signifie qu'il existe $p \in \mathrm{GL}(2, \mathbb{C})$ tel que $php^{-1} = h'$; cependant la même relation est vraie si l'on remplace p par $d^{-1}p$, où $d \in \mathbb{C}$ vérifie $d^2 = \det(p)$; autrement dit h et h' sont alors *conjuguées dans* G. Mais comme H est supposé distingué, nous voyons donc que :

- dans les deux premiers cas ci-dessus, H contient un élément $t(z)$ avec $z \neq 0$;
- dans le troisième cas, H contient un élément $\delta(u)$ avec $u \neq \pm 1$; donc il contient aussi le commutateur $[t(-u), \delta(u)] = t(\lambda - \lambda^{-1})$.

Ainsi, dans tous les cas, H contient un $t(z_0)$ avec $z_0 \neq 0$. Par le même argument que ci-dessus, il contient donc aussi tous les $[t(z_0), \delta(u)]$ pour $u \in \mathbb{C}^*$, et la formule (18.9.1) montre donc qu'*il contient tous les* $t(z)$ pour $z \in \mathbb{C}$ (l'application $u \mapsto z_0\,(1-u^2)$ de $\mathbb{C}^*$ dans $\mathbb{C}$ est surjective).

En conjuguant par la matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, nous voyons de plus que H contient aussi toutes les matrices de la forme

$$t'(z) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \quad (z \in \mathbb{C}).$$

Nous aurons achevé la démonstration si nous voyons que G *est engendré par les matrice de la forme* $t(z)$ *et* $t'(z)$, ce qui est un cas particulier du lemme ci-dessous. ∎

Lemme 18.10 *Soient K un corps et n un entier ≥ 2. Pour $z \in K$ et i, j entiers vérifiant $1 \leq i, j \leq n$ et $i \neq j$, on note $t_{i,j}(z)$ la matrice définie par*

$$(t_{i,j}(z))_{k,l} = \begin{cases} 1 & \text{si } k = l \\ z & \text{si } (k,l) = (i,j) \\ 0 & \text{dans les autres cas.} \end{cases}$$

D'autre part, pour $u \in K^*$, notons $d(u)$ la matrice diagonale $\operatorname{diag}(1, \ldots, 1, u)$.

Alors tout élément g de $\mathrm{GL}(n, K)$ *peut s'écrire $g = t_1 t_2 \ldots t_r \, d(u) \, t_{r+1} \ldots t_s$ où les t_i sont de la forme $t_{i,j}(z)$ (et où nécessairement, $u = \det(g)$).*

Démonstration. Multiplier une matrice g à droite (resp. à gauche) par $t_{i,j}(z)$ revient à effectuer une « opération élémentaire » sur les colonnes (resp. sur les lignes) de g. Le lemme revient donc à montrer qu'une suite convenable d'opérations élémentaires transforme g en une matrice de la forme $d(u)$, ce qui est un exercice facile de calcul matriciel. ∎

Indications de solutions

[I 1] (1.4.5) Pour une démonstration de ce genre, il est *indispensable* de fixer deux notations différentes pour les objets que l'on veut comparer. Ici on pourra noter $n*v$ la loi déduite de la structure d'espace vectoriel, et $n.v$ l'autre. Pour $v \in V$ fixé, on montre alors par récurrence sur n que $n*v = n.v$ pour tout $n \in \mathbb{N}$, puis on traite le cas $n < 0$ en constatant que $n.v = -((-n).v)$ et $n*v = -((-n)*v)$. Toutes ces propriétés se déduisent des définitions ; encore faut-il les connaître, notamment celle d'un espace vectoriel...

[I 2] (1.4.9) L'ordre en question est le nombre de bases $(v_1, \ldots, v_n)$ de K^n. On le trouve en comptant les possibilités pour le premier vecteur, puis pour le deuxième, etc.

[I 3] (1.4.10) Ne pas oublier de vérifier que $*$ induit une loi interne sur l'ensemble en question.

[I 4] (1.5.1) Pour les exemples (ii), (iii) et (iv), tout se déduit (sans recours à des « ε et η ») de la continuité de l'addition et de la multiplication dans $\mathbb{R}$ et $\mathbb{C}$, et de l'inverse dans $\mathbb{R}^*$ et $\mathbb{C}^*$. Pour (iv), utiliser en outre la formule d'inversion d'une matrice et le fait que le déterminant est une fonction polynomiale des coefficients, donc une fonction continue de la matrice.

[I 5] (1.5.2) Pour (iii) et (iv) utiliser (i) ; pour (v) remarquer que la « diagonale » $\Delta = \{(x, y) \in G \times G \mid x = y\}$ est l'image réciproque de $\{e\}$ par l'application $(x, y) \mapsto xy^{-1}$, et que G est séparé si et seulement si Δ est un fermé de $G \times G$).

[I 6] (2.2.5) Utiliser 1.4.5.

[I 7] (3.11.3) On rappelle que le polynôme $P = X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ (critère d'Eisenstein, appliqué au polynôme $P(Y + 1)$).

[I 8] (3.12.1) On rappelle que si X et Y sont deux espaces topologiques et $f : X \to Y$ une application continue, alors pour toute partie A de X on a $f(\overline{A}) \subset \overline{f(A)}$. Si, en outre, B est une partie de Y, l'adhérence de $A \times B$ dans $X \times Y$ est $\overline{A} \times \overline{B}$.

Bien entendu, ces « rappels » sont supposés bien connus ; sinon, leur démonstration fait partie de l'exercice.

[I 9] (3.12.2) Si X est un espace topologique, et x un point de X, la composante connexe de x est la réunion des parties connexes de X contenant x. C'est aussi la plus grande partie connexe de X contenant x ; c'est un fermé de X, qui est de plus ouvert si X est localement connexe.

[I 10] (3.12.3) Si H est un sous-groupe fermé de $\mathbb{R}$, non nul et distinct de $\mathbb{R}$, montrer que $H \cap]0, +\infty[$ admet une borne inférieure $a > 0$; montrer alors que $a \in H$, puis que $H = a\mathbb{Z}$.

[I 11] (3.12.4) (1) Considérer l'adhérence de H et utiliser 3.12.1 et 3.12.3.

[I 12] (3.12.5) Écrire $\zeta = e^{2i\pi\Theta}$ et appliquer 3.12.4.

[I 13] (4.4.9) (3) Peut-être pas grand-chose, mais si f est surjectif ?

[I 14] (6.1.6) Remarquer que, pour tout $i \in \{1, \ldots, n\}$, il existe un élément de $\mathfrak{S}_n$ ayant i comme seul point fixe ; en déduire que, si α est dans le centre de $\mathfrak{S}_n$ on a $\alpha(i) = i$.

(Une autre façon de formuler cet argument est de dire que, pour $n \geq 3$, deux éléments distincts de $i \in \{1, \ldots, n\}$ ont des stabilisateurs dans $\mathfrak{S}_n$ distincts, et d'appliquer la proposition 5.5).

[I 15] (6.7.2) Remarquer que pour $1 \neq i \neq j \neq 1$, on a $(1,i)(1,j)(1,i)^{-1} = (i,j)$ d'après 6.4.7 ou par un calcul direct. Appliquer ensuite 6.7. (Les arguments de conjugaison sont très fréquents dans ce genre de question.)

[I 16] (6.7.3) Si Γ est le sous-groupe engendré par ces transpositions, alors une relation similaire à celle vue dans la preuve de 6.7 montre que Γ contient le cycle $(2, \ldots, n)$ (pour $n > 2$; sinon l'assertion est triviale). Pour chaque $i > 2$, Γ contient donc une permutation α envoyant 1 sur 1 et 2 sur i ; en conjuguant $(1,2)$ par α on obtient $(1,i)$ et l'on applique 6.7.2.

[I 17] (6.7.4) Utiliser 6.7.3 et un argument de conjugaison.

[I 18] (6.12.1) La seule difficulté est de montrer que φ est alternée. Si j est un indice tel que $x_j = x_{j+1}$ — i.e. $\xi_{i,j} = \xi_{i,j+1}$ quel que soit i — noter τ la transposition $(j, j+1)$ et remarquer que pour $\sigma \in \mathfrak{S}_n$ on a $\xi_{i,\sigma(i)} = \xi_{i,\tau\sigma(i)}$ alors que $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

[I 19] (7.8.3) Si G est fini c'est une conséquence immédiate de 7.5 ; sinon on montrera que si $(x_i)_{i\in I}$ est un système de représentants de K modulo H (cf. 7.4.1) et $(y_j)_{j\in J}$ un système de représentants de G modulo K, alors $(x_i y_j)_{(i,j)\in I\times J}$ est un système de représentants de G modulo H.

[I 20] (7.10.2) Remarquer que le complémentaire de H est réunion de classes modulo H.

[I 21] (7.10.3) Avez-vous vérifié que la topologie quotient est bien une topologie ?

(i) Pour U ouvert dans G, remarquer que $\pi^{-1}(\pi(U))$ est la réunion des hU pour $h \in H$.

(iii) Pour la partie « si » : montrer que $\Gamma = \{(x,y) \in G \times G \,|\, Hx = Hy\}$ est fermé dans $G \times G$; remarquer ensuite que si deux éléments $\pi(a)$ et $\pi(b)$ de $H\backslash G$ sont distincts on a $(a,b) \notin \Gamma$, de sorte qu'il existe des voisinages U et V, de a et b respectivement, dans G tels que $(U \times V) \cap \Gamma = \emptyset$. Conclure que $\pi(U)$ et $\pi(V)$ sont des voisinages disjoints, de $\pi(a)$ et $\pi(b)$ respectivement, dans $H\backslash G$.

[I 22] (7.12.5) Remarquer que le premier membre est unitaire de degré $p-1$ et admet comme racines distinctes les $p-1$ éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$. On conclut en donnant une valeur convenable à X.

[I 23] (9.8.8) Pour la dernière assertion, utiliser 3.3.11.

[I 24] (9.8.9) Remarquer que si $f : G \to \Gamma$ est un morphisme de groupes et si $x, y \in G$, alors pour que $f(x)$ et $f(y)$ commutent il faut et il suffit que $[x,y] \in \mathrm{Ker}\,(f)$.

[I 25] (11.3.2) Un élément est d'ordre fini si et seulement si le sous-groupe qu'il engendre est fini.

[I 26] (11.3.3) Voir l'exercice 11.3.4.

[I 27] (11.3.7) Il suffit de trouver un groupe abélien qui n'est pas sans torsion mais est engendré par ses éléments d'ordre infini.

[I 28] (11.7.7) (1) Utiliser 11.7.6(i) et le résultat bien connu d'algèbre linéaire.

(2) Il s'agit de voir que M est *inversible dans* $\mathrm{M}_n(\mathbb{Z})$ si et seulement si son déterminant est *inversible dans* $\mathbb{Z}$. La partie « seulement si » résulte de la multiplicativité des déterminants, et la partie « si » de la formule d'inversion, en remarquant que les mineurs d'une matrice à coefficients entiers sont encore des entiers.

[I 29] (12.3.2) Utiliser 12.3.1 et le théorème de Lagrange.

[I 30] (12.3.4) (réciproque) Considérer les racines du polynôme $X^n - 1$.

[I 31] (12.3.5) Considérer un élément γ de G dont la classe engendre G/C, remarquer que G est engendré par $C \cup \{\gamma\}$ et utiliser l'un des résultats de 4.4.6.

[I 32] (12.3.6) Soit C le centre de G ; d'après 8.7, C est d'ordre p ou p^2. Exclure le cas $|C| = p$ en appliquant 12.3.2 et 12.3.5.

[I 33] (12.3.7) Il est plus commode de noter G additivement. Si G a un élément d'ordre p^2 on a gagné. Sinon tout $x \in G$ vérifie $px = 0$, ce qui implique que G a une

structure naturelle d'espace vectoriel sur le corps $\mathbb{Z}/p\mathbb{Z}$. On conclut en considérant une base de G pour cette structure.

[I 34] (13.8) Pour (iii)⇒(i), soit m l'exposant de A : alors A admet un sous-groupe H cyclique d'ordre m d'après 13.7. Montrer alors que $A = H$ en remarquant que si $x \in A$, alors $\langle x \rangle$ est un sous-groupe cyclique de A d'ordre divisant m, et que H a aussi un sous-groupe du même ordre.

[I 35] (14.5.7) Si k est un tel corps, k^* n'a pas d'élément d'ordre 2 donc $-1_k = 1_k$, et par suite k est de caractéristique 2 ; noter qu'alors l'addition et la soustraction dans k coïncident. Soit a un générateur de k^*. Alors $a + a^2 \neq 0$ (sinon $a = a^2$) donc on a une relation de la forme $a + a^2 = a^d$. Multiplier par une puissance de a pour trouver une relation de la forme $a^m = 1 + a^r$ avec $0 < r < m$. En déduire par récurrence que pour tout $n > m$, a^n est une somme de puissances a^i avec $0 \leq i < m$, puis que l'ensemble des puissances de a est fini, et conclure.

[I 36] (14.5.8) Utiliser la dérivation pour détecter les racines multiples. Pour (2), utiliser Frobenius pour voir que $\mu_n(k) = \mu_m(k)$.

[I 37] (15.3.2) Remarquer que toute partie finie de $\mathbb{Q}$ est contenue dans un sous-groupe de la forme $\frac{1}{d}\mathbb{Z}$, pour d entier convenable. Observer alors que $\frac{1}{d}\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ et conclure.

[I 38] (15.3.4) Utiliser la décomposition en facteurs premiers et l'exercice 15.3.3.

[I 39] (15.8.3) Le lemme chinois est utilisé « dans un sens » pour (1), et « dans l'autre sens » pour (2).

[I 40] (15.9.2) Pour chaque entier q, puissance d'un nombre premier, calculer l'ordre du noyau de la multiplication par q dans A.

[I 41] (16.3.3) Utiliser 13.5.

[I 42] (16.3.5) (2) Considérer l'action de G' par translations à gauche sur G/S, et remarquer qu'il existe au moins une orbite dont le cardinal est premier à p.

[I 43] (17.10) Poser $H = \{\mathrm{Id}, \tau\}$ où τ est une symétrie convenable.

[I 44] (18.8.1) Posant $K = \mathbb{Z}/2\mathbb{Z}$, considérer l'action naturelle de $\mathrm{PSL}(2, K) = \mathrm{GL}(2, K)$ sur $K^2 - \{0\}$.

[I 45] (18.8.2) Posant $K = \mathbb{Z}/3\mathbb{Z}$, considérer l'action naturelle de $\mathrm{PSL}(2, K)$ sur l'ensemble des droites de K^2.

Solutions des exercices

[S 1] (1.2.2) Dans la dernière phrase : « le groupe G ».

[S 2] (1.2.4) Le symétrique de l'élément neutre e est e ; celui de g^{-1} est g ; celui de $g*g'$ est $g'^{-1}*g^{-1}$. À titre d'exemple, justification détaillée de la dernière assertion : on a $(g*g')*(g'^{-1}*g^{-1}) = g*(g'*(g'^{-1}*g^{-1})) = g*((g'*g'^{-1})*g^{-1}) = g*(e*g^{-1}) = g*g^{-1} = e$. La « règle de regroupement » de 1.3.5.1 permet heureusement de simplifier ce raisonnement.

[S 3] (1.2.7) Associativité : $m(m(g,g'),g'') = m(g,m(g',g''))$. Élément neutre : $m(e,g) = m(g,e) = g$. Symétrique : $m(g,g') = m(g',g) = e$.

[S 4] (1.4.2) Pas de symétriques dans $(\mathbb{N},+)$ et $(\mathbb{R}_+,+)$ (en fait aucun élément n'a de symétrique, sauf l'élément neutre).

Pas d'élément neutre dans $(\mathbb{R}_+^*,+)$: en effet, aucun élément x de $\mathbb{R}_+^*$ ne vérifie, disons $x+x=x$.

Remarque : pour justifier l'absence d'élément neutre dans $(\mathbb{R}_+^*,+)$, beaucoup se contentent de dire que « $1 \notin \mathbb{R}_+^*$ ». Cet argument *ne suffit pas*. Par exemple, la multiplication dans $\mathbb{N}$ a un élément neutre (à savoir 1) ; cet élément neutre n'appartient pas au sous-ensemble $\{0\}$ de $\mathbb{N}$, qui a pourtant un élément neutre pour la multiplication, à savoir $0\ldots$

[S 5] (1.4.6) 2 n'a pas d'inverse dans $(\mathbb{N}^*,\times)$, ni dans $(\mathbb{Z}^*,\times)$. $(\mathbb{Q}^*,\times)$ est un groupe. Montrons enfin que $(\mathbb{Z}/n\mathbb{Z},\times)$ en est un si et seulement si $n = \pm 1$. En effet, si $n = \pm 1$ alors $(\mathbb{Z}/n\mathbb{Z},\times)$ a un seul élément, et est donc bien un groupe ; sinon, l'élément neutre de la multiplication est la classe $\overline{1}$ de 1 ; la classe $\overline{0}$ de 0 modulo n est distincte de $\overline{1}$, et comme on a $\overline{0}x = \overline{0} \neq \overline{1}$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, on voit que $\overline{0}$ n'a pas d'inverse.

[S 6] (1.4.7) L'élément neutre de $\mathfrak{S}(E)$ est l'application identique Id_E.

[S 7] (1.4.9) Une fois fixés les i premiers vecteurs de base $v_1,\ldots,v_i$ $(0 \leq i < n)$, v_{i+1} peut être choisi arbitrairement dans le complémentaire du sous-espace de K^n engendré par $v_1,\ldots,v_i$. Ce sous-espace est de dimension i donc de cardinal q^i, il y a donc $q^n - q^i$ possibilités pour e_{i+1}. On trouve finalement

$$|\mathrm{GL}(n,K)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

(Plus généralement, le raisonnement montre que le nombre de familles libres à m éléments $(v_1,\ldots,v_m)$ de K^n est égal à $\prod_{i=0}^{m-1}(q^n - q^i)$; c'est sous cette forme que le résultat se montre le plus simplement par récurrence.)

[S 8] (2.2.4) L'inverse de f est le morphisme $x \mapsto f(x)^{-1}$. Plus généralement, pour $n \in \mathbb{Z}$, la n-ième puissance de f est le morphisme $x \mapsto f(x)^n$. En particulier, en prenant $H = G$ (commutatif) et $f = \mathrm{Id}_G$, on retrouve le morphisme $g \mapsto g^n$ de 2.2.3.

[S 9] (2.2.5) Soit $f : V \to W$ un morphisme de groupes additifs. Pour $x \in V$ et $r \in \mathbb{Q}$ il s'agit de voir que $f(rx) = rf(x)$. Si r est *entier*, ceci résulte (pour x quelconque) de 1.4.5, qui montre qu'alors $x \mapsto rx$ est aussi la multiplication par r au sens de l'addition de V (resp. de W) et est donc respectée par f d'après la dernière assertion de 2.2.1.

Pour $r \in \mathbb{Q}$ quelconque, on écrit $r = \frac{n}{d}$ avec $d \in \mathbb{Z}$ non nul et $n \in \mathbb{Z}$. D'après le cas précédent, on a $df(rx) = f(drx) = f(nx) = nf(x)$ d'où, puisque $d \neq 0$, $f(rx) = \frac{n}{d} f(x)$, cqfd.

[S 10] (2.4.5) Les propriétés (i), (ii) et (iii) sont invariantes ; les deux dernières ne le sont pas.

[S 11] (2.6.2) Comme $x \neq e$ on a $xy \neq y$, et comme $y \neq e$ on a $xy \neq x$ (règle de simplification). La seule possibilité est donc $xy = e$ (d'où aussi $yx = e$). Donc l'inverse de x n'est pas x donc $x^2 \neq e$ donc $x^2 = y$, et de même $y^2 = x$. On en déduit la table de G, et le fait que chacune des deux bijections de $\mathbb{Z}/3\mathbb{Z}$ (noté $\{0, 1, 2\}$) sur G envoyant respectivement 0, 1, 2 sur e, x, y (resp. sur e, y, x) est un isomorphisme.

[S 12] (3.3.9) $Z_G(\emptyset) = Z_G(\{e\}) = G$; $S \subset Z_G(S)$ si et seulement si tous les éléments de S commutent entre eux ; $Z_G(\bigcup_{i \in I} S_i) = \bigcap_{i \in I} Z_G(S_i)$ (remarquer que tout concorde lorsque $I = \emptyset$). Pas de formule analogue pour le centralisateur d'une intersection. Si $S \subset T$ alors $Z_G(T) \subset Z_G(S)$. Enfin $Z_H(S) = H \cap Z_G(S)$.

[S 13] (3.3.11) C'est le centre de G : un élément g de G est dans le noyau cherché si et seulement si $\mathrm{int}_g = \mathrm{Id}_G$, ce qui équivaut à $gxg^{-1} = x$ pour tout $x \in G$, ou encore à $gx = xg$ pour tout $x \in G$.

[S 14] (3.5.1) Dans $(\mathbb{R}, +)$: $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$; $\langle 2 \rangle = 2\mathbb{Z}$.

Dans $(\mathbb{R}^*, \times)$: $\langle 1 \rangle = \{1\}$; $\langle 2 \rangle = 2^{\mathbb{Z}} = \{\ldots, 1/4, 1/2, 1, 2, 4, 8, \ldots\}$;$\langle -1 \rangle = \{-1, 1\}$.

Dans $(\mathbb{C}, +)$: $\langle i \rangle = i\mathbb{Z}$.

Dans $(\mathbb{C}^*, \times)$: $\langle i \rangle = \{1, i, -1, -i\}$.

[S 15] (3.11.1) Le cas commutatif a été vu en 3.3.7.

Contre-exemple non commutatif : si D et D' sont deux droites du plan euclidien $\mathbb{R}^2$ faisant un angle $\pi\theta$, et si s et s' sont les symétries orthogonales correspondantes, alors s et s' sont des éléments d'ordre 2 de $\mathrm{GL}(2, \mathbb{R})$). La composée $s' \circ s$ est une rotation d'angle $2\pi\theta$, donc n'est pas d'ordre fini si θ n'est pas rationnel.

Autre exemple, peut-être plus simple : la composée de deux symétries centrales de centres O et O' est une translation envoyant O sur O' (ou O' sur O, suivant l'ordre de composition). Si $O \neq O'$ et si le corps de base est de caractéristique nulle, une telle translation est d'ordre infini. L'exemple « concret » le plus simple s'obtient en prenant un corps K de caractéristique nulle (par exemple $\mathbb{R}$), et en considérant les deux applications $s : x \mapsto -x$ et $t : x \mapsto 1 - x$ (symétries par rapport à 0 et 1/2). La composée $t \circ s$ est la translation $x \mapsto x + 1$, qui est d'ordre infini.

[S 16] (3.11.2) $\begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$.

[S 17] (3.11.3) Il n'y en a pas. Soit $u \in \mathrm{GL}(2,\mathbb{Q})$ vérifiant $u^5 = \mathrm{Id}$. Le polynôme minimal unitaire de u est un élément F non constant de $\mathbb{Q}[X]$, de degré ≤ 2 (Cayley-Hamilton) qui divise $X^5 - 1 = (X-1)P(X)$ où l'on a posé $P = X^4 + X^3 + X^2 + X + 1$. Comme P est irréductible, la seule possibilité est que $F = X - 1$, donc $u = \mathrm{Id}$.

[S 18] (3.12.1) Il est clair que $e \in \overline{H}$; compte tenu des propriétés rappelées dans l'indication, la continuité de i implique que $i(\overline{H}) \subset \overline{H}$; de plus l'adhérence de $H \times H$ dans $G \times G$ est $\overline{H} \times \overline{H}$ de sorte que la continuité de m implique que $m(\overline{H} \times \overline{H}) \subset \overline{H}$. Donc $\overline{H}$ est bien un sous-groupe. Comme d'autre part c'est le plus petit fermé de G contenant H, le reste en résulte.

[S 19] (3.12.2) Il suffit de définir G^0 comme la composante connexe de e, et de montrer que c'est un sous-groupe de G exactement comme pour l'adhérence d'un sous-groupe ; il suffit de remarquer qu'un produit d'espaces connexes est connexe, et que l'image d'un espace connexe par une application continue est connexe.

Il est immédiat que la composante neutre de $\mathbb{R}^*$ est $\mathbb{R}_+^*$.

Montrons que $\mathrm{GL}(n,\mathbb{C})$ est connexe pour tout $n \in \mathbb{N}$. C'est trivial pour $n = 0$. Pour $n > 0$, soit $A \in \mathrm{GL}(n,\mathbb{C})$: les matrices de la forme $I_n + tA$ sont inversibles pour $t \in \mathbb{C}$, sauf pour un nombre fini de valeurs (les racines du polynôme $P(t) = \det(I_n + tA)$). Comme $\mathbb{C}$ privé d'un ensemble fini est connexe, on en déduit que l'ensemble des $I_n + tA$ qui sont inversibles est connexe ; comme il contient A et I_n, on a bien $A \in \mathrm{GL}(n,\mathbb{C})^0$.

Enfin, la composante neutre de $\mathrm{GL}(n,\mathbb{R})$ est le sous-groupe $\mathrm{GL}^+(n,\mathbb{R})$ formé des matrices à déterminant positif. Comme il est clair que ce sous-groupe est un ouvert fermé de $\mathrm{GL}(n,\mathbb{R})$ (c'est aussi l'ensemble des matrices à déterminant ≥ 0), il ne reste qu'à montrer qu'il est connexe. Voici le principe : d'abord, par la « méthode d'orthogonalisation de Gram-Schmidt », on se ramène à prouver que le groupe $\mathrm{SO}(n,\mathbb{R})$ est connexe, ou, ce qui revient au même, que l'ensemble des *bases orthonormées directes* de l'espace euclidien orienté $\mathbb{R}^n$ est connexe. Pour cela, on procède par récurrence sur n. C'est clair pour $n = 1$, et pour $n = 2$ c'est bien connu : $\mathrm{SO}(2,\mathbb{R})$ est le groupe des rotations du plan, image continue de $\mathbb{R}$ par l'application qui à t associe

la rotation d'angle t. Si $n > 2$, soit $B = (v_1, \ldots, v_n)$ une base orthonormée directe et soit $B_0 = (e_1, \ldots, e_n)$ la base canonique. Si $v_1 \neq e_1$, il existe une rotation (autour de l'orthogonal Δ du plan engendré par v_1 et e_1) qui envoie v_1 sur e_1. Comme le groupe des rotations autour de Δ est évidemment homéomorphe à $\mathrm{SO}(2, \mathbb{R})$, il est connexe. On en déduit que B est dans la même composante qu'une base dont le premier vecteur est e_1. Mais l'ensemble des bases ayant cette propriété est homéomorphe à l'ensemble des bases orthonormées directes de l'orthogonal de e_1, qui est connexe par hypothèse de récurrence.

[S 20] (3.12.4) (1) Il s'agit de montrer que $\overline{H} = \mathbb{R}$. Si ce n'est pas le cas, comme $H \neq \{0\}$, il existe d'après 3.12.3 un réel $m > 0$ tel que $H = m\mathbb{Z}$. On a donc en particulier $1 = um$ et $\theta = vm$ pour u et v entiers convenables. Donc $\theta = v/u \in \mathbb{Q}$, contradiction.
(2) Comme H est dense dans $\mathbb{R}$, l'ouvert non vide $]0, \varepsilon[$ de $\mathbb{R}$ contient un élément de H, donc un réel de la forme $q\theta - p$ avec p et q entiers. On en déduit le résultat (en faisant attention aux signes).

[S 21] (4.2.1) $\langle\emptyset\rangle = \langle\{e\}\rangle = \{e\}$; S est un sous-groupe de G si et seulement si $\langle S\rangle = S$; dans $\mathbb{Z}$, on a $\langle\mathbb{N}\rangle = \mathbb{Z}$.

[S 22] (4.4.2) Non pour $\mathbb{N}$ (contre-exemple : $G = \mathbb{Z}$, $S = \{1\}$) ; oui pour les autres. Dans le cas de $\{-17, +10000\}$ il faut remarquer qu'il existe des entiers *positifs* u et v tels que $-17u + 10000v = 1$, et aussi des entiers positifs u' et v' tels que $-17u' + 10000v' = -1$.

[S 23] (4.4.3) $\mathbb{Q}_+^*$.

[S 24] (4.4.4) Première méthode : l'hypothèse équivaut à dire que $\mathrm{Ker}\, f$ contient S ; comme c'est un sous-groupe de G il contient donc $\langle S\rangle$, cqfd.

Deuxième méthode : soit $x \in \langle S\rangle$: alors x s'écrit $x = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_m^{\varepsilon_m}$ comme dans 4.4. Donc, puisque f est un morphisme, $f(x) = f(s_1)^{\varepsilon_1} f(s_2)^{\varepsilon_2} \cdots f(s_m)^{\varepsilon_m}$ d'où $f(x) = e$ puisque les s_i sont dans $\mathrm{Ker}\, f$.

La réciproque est triviale : si $\langle S\rangle \subset \mathrm{Ker}\, f$ alors $S \subset \mathrm{Ker}\, f$ puisque $S \subset \langle S\rangle$.

[S 25] (4.4.5) Démonstration « directe » (i.e. sans utiliser 4.4) :

$\langle f(S)\rangle \subset f(\langle S\rangle)$: le second membre est un sous-groupe de H qui contient $f(S)$ donc il contient aussi $\langle f(S)\rangle$;

$f(\langle S\rangle) \subset \langle f(S)\rangle$: $f(S)$ est contenu dans $\langle f(S)\rangle$, donc S est contenu dans $f^{-1}(\langle f(S)\rangle)$ qui est un sous-groupe de G. Donc $\langle S\rangle$ est aussi contenu dans ce sous-groupe, ce qui équivaut à l'inclusion voulue.

[S 26] (4.4.7) (question à la fin de l'exercice) : le cas commutatif s'applique au sous-groupe engendré par les a_i, qui est bien commutatif.

[S 27] (4.4.9) (1) Il suffit de remarquer que l'inverse d'un commutateur est un commutateur (explicitement, $[x,y]^{-1} = [y,x]$) et d'appliquer 4.4.

(2) Sans hypothèse sur H, il est clair que $f([x,y]) = [f(x), f(y)]$ pour tous $x, y \in G$. On en déduit que $f([G,G]) \subset [H,H]$ et, si H est commutatif, que $[G,G] \subset \mathrm{Ker}\, f$ (on peut aussi appliquer l'exercice 4.4.4).

(3) On ne peut évidemment rien dire sur H sans autre hypothèse (prendre H quelconque et f trivial). Par contre, montrons que l'image de f est un groupe *commutatif* (de façon équivalente, si f est surjectif et $[G,G] \subset \mathrm{Ker}\, f$, alors H est commutatif). Soient x et y dans $\mathrm{Im}\, f$: alors $x = f(x')$ et $y = f(y')$ pour x' et $y' \in G$ convenables. Donc $[x,y] = f([x',y']) = e_H$ vu l'hypothèse, donc x et y commutent, cqfd.

[S 28] (4.4.10) Soit X le second membre. L'inclusion $X \subset \langle S \rangle$ est triviale car chaque $\langle T \rangle$ est contenu dans $\langle S \rangle$. L'autre se déduit facilement de 4.4 (avec la notation de 4.4, x appartient à $\langle \{s_1, \ldots, s_m\} \rangle$), ou encore de 4.2, en remarquant que X (qui contient évidemment S) est un sous-groupe de G : en effet il est clairement non vide et stable par inverse, et si $x \in \langle T \rangle$ et $y \in \langle T' \rangle$ (avec T et T' finis) alors $xy \in \langle T \cup T' \rangle \subset X$.

[S 29] (5.3.7) (fin) $X = \{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$.

Le noyau du morphisme est le sous-groupe de $\mathfrak{S}_4$ formé de l'identité et des trois « doubles transpositions » $(1,2)(3,4)$, $(1,3)(2,4)$ et $(1,4)(2,3)$ (notations du §6).

[S 30] (5.4.4) Toute action libre *sur un ensemble non vide* est fidèle. Pour tout $n \in \mathbb{N}$ le groupe symétrique $\mathfrak{S}_n$ opère fidèlement sur $\{1, \ldots, n\}$ mais, si $n \geq 3$, il n'opère librement sur aucune partie non vide de $\{1, \ldots, n\}$.

[S 31] (5.4.5) L'action est fidèle puisqu'elle est libre et que G n'est pas vide. On en déduit un morphisme injectif de G dans $\mathfrak{S}(G)$, donc un isomorphisme de G sur l'image de ce morphisme. Si G est fini d'ordre n, alors $\mathfrak{S}(G)$ est isomorphe à $\mathfrak{S}_n$, d'où la dernière assertion.

[S 32] (5.4.8) Pour l'action de $\mathrm{GL}(V)$ sur V : si V est nul la seule orbite est $\{0\}$, sinon, les orbites sont $\{0\}$ et $V - \{0\}$.

Pour l'action de K^* sur V : si V est nul la seule orbite est $\{0\}$; sinon, les orbites sont $\{0\}$ et les droites de V privées de l'origine. L'action n'est pas libre (0 est un point fixe) ; elle est fidèle si et seulement si V n'est pas nul (l'action sur $V - \{0\}$ est libre).

Pour l'action de $\mathrm{GL}(V)$ sur l'ensemble des sous-espaces de V (en dimension finie) : l'orbite d'un sous-espace W est l'ensemble des sous-espaces de même dimension que W. (C'est vrai aussi en dimension infinie mais plus difficile).

(Toutes les démonstrations relèvent de l'algèbre linéaire élémentaire).

[S 33] (5.4.9) Pour l'action de $\mathrm{O}(n, \mathbb{R})$: les orbites sont les sphères

$$S_r = \{x \in \mathbb{R}^n | \parallel x \parallel = r\}$$

($r \geq 0$, ou seulement $r = 0$ si $n = 0$). Même réponse pour l'action de $\mathrm{SO}(n, \mathbb{R})$, sauf si $n = 1$: dans ce cas le groupe est trivial et les orbites ont un seul élément.

[S 34] (6.3) Supp (Id) $= \emptyset$; le support d'une permutation σ n'est jamais réduit à un élément ; il a deux éléments si et seulement si σ est une transposition (6.4.6).

[S 35] (6.6.5) Le seul type d'élément d'ordre 12 est $(4, 3)$.

[S 36] (6.6.6) $\mathfrak{S}_6$ n'a pas d'élément d'ordre 12 donc l'assertion est trivialement vraie.

[S 37] (6.7) (fin de la démonstration) La première.

[S 38] (6.10.1) Non. Supposons que l'on remplace $\mathbb{R}$ par un corps K. D'abord l'assertion « φ n'est pas identiquement nulle » n'est valable que si K a au moins n éléments (sinon on peut aussi aménager la preuve en remplaçant les fonctions par des polynômes). D'autre part, même si $\varphi \neq 0$, l'égalité $\varepsilon(\sigma\tau)\,\varphi = \varepsilon(\tau)\,\varepsilon(\sigma)\,\varphi$ n'implique $\varepsilon(\sigma\tau) = \varepsilon(\tau)\,\varepsilon(\sigma)$ que si $1_K \neq -1_K$, c'est-à-dire si K est de caractéristique différente de 2.

On peut aussi remplacer $\mathbb{R}$ par un anneau commutatif unitaire A (disons intègre infini de caractéristique $\neq 2$, tel que $\mathbb{Z}$), à condition de remplacer le vocabulaire des espaces vectoriels par celui des « A-modules ».

[S 38] (6.10.5) Cette définition n'en est une que si l'on prouve que le résultat de 6.9(iii) (c'est-à-dire la parité de m) ne dépend pas de la décomposition de σ en produit de transpositions.

[S 40] (7.1) $ABB^{-1} = CB^{-1}$ implique $A \subset CB^{-1}$, sauf si B est vide et A ne l'est pas.

Si $AA = A^{-1} = A$, A est vide ou est un sous-groupe de G.

[S 41] (7.6.2) (i) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ n'a pas d'élément d'ordre 4 ; $\mathfrak{S}_3$ n'a pas d'élément d'ordre 6. Voir l'exercice 12.3.1.

(ii) Si x est d'ordre $n = md$, alors x^m est d'ordre d : en effet $(x^m)^d = x^{md} = e$, et si $(x^m)^k = e$ alors n divise mk donc d divise k.

(iii) Le groupe admet un élément non trivial, qui est d'ordre p^e avec $e > 0$. Il suffit donc d'appliquer (ii).

[S 42] (7.7.2) $\Gamma_{x,y} = \emptyset$ si et seulement si x et y ne sont pas dans la même orbite. Dans ce cas $\Gamma_{x,y}$ n'est pas une classe à gauche (une classe d'équivalence est non vide par définition).

[S 43] (7.7.5) Soit $\Gamma = Hx$ une classe à droite modulo H : alors $\Gamma = x(x^{-1}Hx)$ donc Γ est une classe à gauche modulo $x^{-1}Hx$.

[S 44] (7.8.2) Si G et H sont infinis ce quotient n'a pas de sens.

[S 45] (7.9) (dernière question) Hxg ne dépend pas que de g et de la classe Hx, mais aussi, en général, du choix de x dans cette classe. Ce n'est pas le cas pour l'action à droite $(Hx, g) \mapsto Hxg$, bien définie puisque $Hxg = (Hx)g$. Une meilleure formulation de cette action aurait été « G opère à droite sur $H\backslash G$ par $(\Gamma, g) \mapsto \Gamma g$, l'égalité $(Hx)g = H(xg)$ montrant que Γg est bien une classe à droite ».

[S 46] (7.10.1) Hx est l'image de H par l'application $g \mapsto gx$ de G dans G, qui est un homéomorphisme.

[S 47] (7.12.2) Si G n'est pas commutatif, le « produit de tous les éléments de G » n'a pas de sens.

[S 48] (7.12.4) Si p n'est pas premier (et est > 1), $(p-1)!$ n'est pas premier à p donc ne peut être congru à -1 modulo p.

[S 49] (7.13.1) On trouve la valeur 1 (resp. -1) pour $p = 3$ ou 23 (resp. pour $p = 7, 11, 19$). Sauf erreur, évidemment, mais chacun peut vérifier.

[S 50] (7.13.2) Si $p - 1 = 4q$, alors $X^{p-1} - 1 = X^{4q} - 1$ est divisible par $X^4 - 1$, et a fortiori par $X^2 + 1$, dans $\mathbb{Z}[X]$. Par suite, avec les abus d'écriture habituels, $X^{p-1} - 1$ est divisible par $X^2 + 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Or, d'après 7.12.5, $X^{p-1} - 1$ est complètement décomposé dans $(\mathbb{Z}/p\mathbb{Z})[X]$; il en est donc de même de $X^2 + 1$, d'où le résultat.

[S 51] (8.1.6) Pour $x = eH$, on obtient l'identité de G/H. Pour $x = \gamma H$, le stabilisateur est $\gamma H \gamma^{-1}$, et on obtient une bijection de $G/\gamma H\gamma^{-1}$ sur G/H envoyant la classe $g\gamma H\gamma^{-1}$ sur $g\gamma H$, c'est-à-dire, en d'autres termes, une classe Γ modulo $\gamma H\gamma^{-1}$ sur la classe $\Gamma\gamma$ modulo H.

[S 52] (8.6.1) Tout diviseur d'une puissance de p est une puissance de p.

[S 53] (8.6.2) On remarque que l'action en question n'a pas de point fixe (ce qui est évidemment faux si $k = 0$ ou si $k = p^s$). Si $s = 0$ le résultat est vrai mais vide : il n'existe aucun k vérifiant l'hypothèse. Enfin le le choix de $\mathbb{Z}/p^s\mathbb{Z}$ est sans importance.

[S 54] (9.1.1) Le plus pratique est de faire un schéma des implications démontrées, ici :

$$\begin{array}{ccc} \text{(i)} & \longleftrightarrow & \text{(ii)} \\ \updownarrow & & \\ \text{(iii)} & \longleftrightarrow & \text{(iv)} \\ \updownarrow & & \\ \text{(v)} & & \end{array}$$

[S 55] (9.3.5) Si H est un sous-groupe non distingué d'un groupe G, alors H est un sous-groupe distingué de H dont l'image par le morphisme d'inclusion de H dans G n'est pas un sous-groupe distingué de G.

[S 56] (9.4.2) Oui. Si $\alpha = xH$ et $\beta = yH$, le produit $\alpha\beta$ dans G/H est $xyH = xHy = xHHy = xHyH$ (on a utilisé deux fois le fait que $yH = Hy$).

[S 57] (9.4.5) Par la compatibilité, il existe sur l'ensemble quotient $G/\sim$ une unique loi de composition telle que l'application canonique $\pi : G \to G/\sim$ soit un morphisme. Comme π est surjective et que G est un groupe, $G/\sim$ est aussi un groupe pour cette loi (vérifications immédiates). Les classes d'équivalence sont les parties de G de la forme $\pi^{-1}(\alpha)$, pour $\alpha \in G/\sim$; comme π est un morphisme de groupes ce sont les classes modulo le noyau de π, qui est la classe H de l'élément neutre de G. Donc $\sim$ est la relation associée à H.

(Bien entendu on peut aussi vérifier « à la main »que la classe de e est un sous-groupe distingué de G, et que $\sim$ est la relation associée).

[S 58] (9.5.1) Voir 18.3.

[S 59] (9.5.3) Soit H un sous-groupe distingué de $\mathfrak{S}_n$, pour $n \geq 5$. Alors $H \cap \mathrm{A}_n$ est distingué dans A_n. Puisque A_n est simple, on a donc deux cas :
(1) $H \cap \mathrm{A}_n = \mathrm{A}_n$. Autrement dit, H contient A_n. Mais comme A_n est d'indice 2 dans $\mathfrak{S}_n$, l'indice de H dans $\mathfrak{S}_n$ doit diviser 2, donc H est égal à $\mathfrak{S}_n$ ou à A_n.
(2) $H \cap \mathrm{A}_n = \{e\}$. Donc la signature induit un morphisme injectif de H dans $\{\pm 1\}$. Si H n'était pas trivial il serait donc d'ordre 2, formé de l'identité et d'un élément τ non trivial. Mais comme H est distingué dans $\mathfrak{S}_n$, τ serait nécessairement central : contradiction car le centre de $\mathfrak{S}_n$ est trivial (6.1.6).

[S 60] (9.8.6) Si $n = 0$, γ est d'ordre infini. Si $n > 0$, γ est d'ordre n.

[S 61] (9.8.9) L'ensemble des commutateurs est stable par conjugaison (et même par tout endomorphisme de G) : il en résulte immédiatement que le sous-groupe engendré G' est distingué. (Vous souvenez-vous que G' n'est pas l'ensemble des commutateurs ?)

La propriété donnée dans l'indication implique que si $f : G \to \Gamma$ est un morphisme de groupes, alors l'image de f est un groupe commutatif si et seulement si Ker (f) contient tous les commmutateurs de G, c'est-à-dire contient G'.

En appliquant ceci à un sous-groupe distingué H de G on obtient l'équivalence : « G/H commutatif $\Leftrightarrow$ $G' \subset H$ »(en particulier, G/G' est commutatif). On en tire aussi la propriété universelle : tout morphisme de G vers un groupe commutatif a un noyau qui contient G', donc se factorise par G/G'.

[S 62] (11.2.2) (i) $(ab)^n = a^n b^n$; (ii) $a^{m+n} = a^m a^n$; (iii) $a^1 = a$; (iv) $a^{mn} = (a^m)^n$.

[S 63] (11.2.4) Sur un $\mathbb{Z}$-module A, notons $(n,x) \mapsto n * x$ la loi externe donnée par la structure de $\mathbb{Z}$-module, et $(n,x) \mapsto nx$ celle décrite en 11.2. Pour $x \in A$, on a $1x = x = 1 * x$; pour un entier n quelconque, on en déduit $(n+1)x = nx + x$ et $(n+1) * x = n * x + x$, de sorte que l'égalité $nx = n * x$ est équivalente à $(n+1)x = (n+1) * x$. Comme elle est vraie pour $n = 1$, elle est vraie pour tout $n \in \mathbb{Z}$.

Si $f : A \to B$ est un morphisme de groupes abéliens, on sait que $f(nx) = nf(x)$ pour tout $x \in A$ et tout $n \in \mathbb{Z}$, donc f est un morphisme pour les uniques structures de $\mathbb{Z}$-module sur A et B. Argument similaire pour les sous-groupes.

[S 64] (11.3.1) Oui, si (et seulement si) le groupe est trivial.

[S 65] (11.3.4) $\{0\}$; $\mathbb{Z}/n\mathbb{Z}$ si $n \neq 0$, et $\{0\}$ si $n = 0$; $\{0\}$; $\mathbb{Q}/\mathbb{Z}$ (ce qui répond à l'exercice 11.3.3, de même que le groupe suivant) ; le groupe des racines de l'unité dans $\mathbb{C}$ (par définition...) ; $A_{\text{tors}} \times B_{\text{tors}}$.

[S 66] (11.3.5) Oui (resp. oui pour une famille *finie*). Dans le groupe $\prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$, l'élément $(e_n)_{n\geq 1}$ où e_n désigne la classe de 1 mod n, est d'ordre infini.

[S 67] (11.3.7) On peut prendre par exemple le groupe $A = \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$, qui est engendré par $\{(1,\overline{0}),(1,\overline{1})\}$.

[S 68] (11.4.4) L'identité de $\mathbb{Z}^n$.

[S 69] (11.6.3) Pour tout $n \neq 2$, $\{2,n\}$ n'est pas libre (on a la relation « non triviale » $n \times 2 - 2 \times n = 0$). $\{2\}$ est bien une partie libre mais engendre le sous-groupe strict $2\mathbb{Z}$ de $\mathbb{Z}$ donc n'est pas génératrice.

[S 70] (11.6.5) C'est un groupe non nul dont aucune partie non vide n'est libre : pour tout $x \in \mathbb{Z}/m\mathbb{Z}$, on a $mx = 0$, alors que l'entier m n'est pas nul.

Si $m = 0$ (resp. $m = 1$), on trouve un groupe isomorphe à $\mathbb{Z}$ (resp. trivial), qui a donc une base à un (resp. zéro) élément.

[S 71] (11.6.7) (i) L'assertion « seulement si » est fausse si $\theta = 1$: dans ce cas $\{1,\theta\} = \{1\}$ est une partie libre. L'assertion « si » est vraie, ainsi que « seulement si » pour $\theta \neq 1$: voir (ii).

(ii) Vrai : dire que $(1,\theta)$ n'est pas libre équivaut à dire qu'il existe des entiers m et n, non tous deux nuls, tels que $m + n\theta = 0$. Le cas $n = 0$ est exclu (il implique $m = 0$) donc une telle relation peut s'écrire $\theta = -m/n$.

[S 72] (11.7.1) (i) : la première équivalence résulte immédiatement des définitions, de même que l'implication « si $\underline{a}$ est $\mathbb{Q}$-libre alors $\underline{a}$ est $\mathbb{Z}$-libre » (dans $\mathbb{Q}^n$). Supposons que $\underline{a}$ soit $\mathbb{Q}$-liée, et montrons que $\underline{a}$ est $\mathbb{Z}$-liée. Par hypothèse, il existe une relation

$\sum_{i\in I} \lambda_i a_i = 0$ avec les $\lambda_i \in \mathbb{Q}$ non tous nuls. Comme il s'agit d'un nombre fini de rationnels, ils ont un dénominateur commun : il existe un entier $d > 0$ tel que $d\lambda_i \in \mathbb{Z}$ pour tout $i \in I$. Les $d\lambda_i$ sont donc des entiers non tous nuls, et l'on a évidemment $\sum_{i\in I}(d\lambda_i)\, a_i = 0$, donc $\underline{a}$ est $\mathbb{Z}$-liée, comme prévu.

(ii) : supposons que $\underline{a}$ soit $\mathbb{Z}$-génératrice dans $\mathbb{Z}^n$, et soit $x \in \mathbb{Q}^n$. Il existe un entier $d > 0$ tel que $dx \in \mathbb{Z}^n$ (un dénominateur commun des coordonnées de x). Par hypothèse, dx est combinaison linéaire (à coefficients entiers) des a_i. Divisant par d, on en déduit que x est combinaison linéaire à coefficients rationnels des a_i.

(iii) : si $\underline{a}$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$, il est trivial que $\underline{a}$ est $\mathbb{Z}$-génératrice dans $\mathbb{Z}^n$, et il résulte de (i) et (ii) que $\underline{a}$ est une $\mathbb{Q}$-base de $\mathbb{Q}^n$ et donc que $|I| = n$. Réciproquement, supposons que $\underline{a}$ soit $\mathbb{Z}$-génératrice dans $\mathbb{Z}^n$ et que $|I| = n$: alors d'après (ii), $\underline{a}$ est une famille $\mathbb{Q}$-génératrice à n éléments de $\mathbb{Q}^n$ donc est $\mathbb{Q}$-libre et donc $\mathbb{Z}$-libre d'après (i) : c'est donc bien une $\mathbb{Z}$-base de $\mathbb{Z}^n$.

[S 73] (11.7.3) Dans ce cas, on a $|I| > n$ donc (ii) et (iv) sont trivialement vrais ; d'autre part I contient une partie J à $n+1$ éléments, à laquelle on peut appliquer le cas fini : on déduit de 11.7.2(i) que $(a_i)_{i\in J}$ n'est pas libre, et donc $\underline{a}$ non plus d'après la définition d'une famille libre (11.4.13), de sorte que (i) et (iii) sont aussi trivialement vrais.

[S 74] (11.7.5) Voir 11.6.3.

[S 75] (12.3.1) Partie « seulement si » : la propriété d'avoir un élément d'ordre n est invariante par isomorphisme, et $\mathbb{Z}/n\mathbb{Z}$ en a bien un, par exemple la classe de 1.

Partie « si » : si $x \in G$ est un élément d'ordre n, il engendre un sous-groupe qui est d'ordre n donc égal à G.

[S 76] (12.3.3) Si G admet un élément $x \neq e$, alors le sous-groupe engendré par x est nécessairement égal à G. Donc G est cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ($n > 1$), lequel a donc la même propriété que G. Si n n'était pas premier, il aurait un diviseur d avec $1 < d < n$, et le sous-groupe $d\mathbb{Z}/n\mathbb{Z}$ contredirait la propriété en question.

[S 77] (12.3.8) Tous ses éléments sont annulés par m, il n'a donc aucun élément d'ordre m^2. Si $m = 1$ le groupe est cyclique d'ordre 1. Si $m = 0$ le groupe est infini, isomorphe à $\mathbb{Z}^2$; il n'est pas monogène (c'est un cas particulier de 11.7.4, très facile à démontrer directement).

[S 78] (12.4.3) L'identité.

[S 79] (12.5.1) Cette variante est vraie mais plus faible : l'unicité n'a évidemment pas le même sens dans les deux cas. L'énoncé tel qu'il est donné dans le texte implique que *tout* isomorphisme d'anneaux $f : \mathbb{Z}/ab\mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ *doit* vérifier la formule $f(k \bmod ab) = (k \bmod a, k \bmod b)$.

[S 80] (12.5.4)

n :	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4	10	4

[S 81] (12.5.6) Les entiers non premiers avec p^r sont les multiples de p. L'ensemble des éléments non inversibles de $\mathbb{Z}/p^r\mathbb{Z}$ est donc $p\mathbb{Z}/p^r\mathbb{Z}$ qui a p^{r-1} éléments.

[S 82] (12.5.8) Oui. Soit n entier > 0, décomposé en $\prod_{i=1}^{s} p_i^{e_i}$, où les p_i sont premiers distincts. Alors, par 12.5.5, on a

$$\varphi(n) = \prod_{i-1}^{s} \varphi(p_i^{e_i}); \tag{1}$$

d'autre part d'après 12.5.6 on a

$$\varphi(p_i^{e_i}) \geq p_i^{e_i}/2 \tag{2}$$

qui est ≥ 2 sauf peut-être si $p_i = 2$. Ceci montre déjà que $\varphi(n) \geq 2^{s-1}$, d'où

$$s \leq 1 + \log_2 \varphi(n). \tag{3}$$

Reportant (2) et (3) dans (1), on trouve $\varphi(n) \geq \frac{n}{2\varphi(n)}$, c'est-à-dire $\varphi(n) \geq \sqrt{n/2}$.

[S 83] (12.8.2) L'ordre est $d := \mathrm{pgcd}\,(m, n)$. En effet, la condition $mx = 0$ équivaut (pour $x \in \mathbb{Z}/n\mathbb{Z}$) à $dx = 0$. Le sous-groupe cherché est donc le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par n/d, qui est (cyclique) d'ordre d.

[S 84] (12.8.3) C'est un groupe cyclique d'ordre $d := \mathrm{pgcd}\,(m, n)$, d'après 12.4 et 12.8.2.

[S 85] (13.1.1) C'est la bijection de 12.4, qui dans le cas commutatif est un morphisme de groupes.

[S 86] (13.1.2) Comme nA est l'image de $[n]_A$ il est isomorphe à $A/{}_nA$ donc $|nA| = |A|/|{}_nA|$ d'où $|{}_nA| = |A|/|nA| = |A/nA|$. Bien entendu l'hypothèse que A soit fini est essentielle, même en supposant que ${}_nA$ et A/nA sont finis : considérer $A = \mathbb{Z}$ par exemple.

[S 87] (13.4.1) (i) Le groupe symétrique $\mathfrak{S}_3$ est engendré par deux transpositions.

(ii) Voir 3.11.1. (Bien entendu, la première assertion de 13.4 reste vraie dans le cas non commutatif : l'ordre du groupe est multiple du ppcm des ordres de ses éléments.)

[S 88] (13.6.2) L'exposant de $\mathbb{Z}/n\mathbb{Z}$ est $|n|$ si $n \neq 0$, et ∞ si $n = 0$ (ceux qui ont répondu « n » ont donc perdu). Celui d'un sous-groupe (ou d'un quotient) de G divise celui de G. Celui de $\prod_{i\in I} G_i$ est le ppcm (≥ 0) des exposants de G_i, ou ∞ si ce ppcm est nul.

[S 89] (13.6.3) L'exposant de A est la caractéristique de $\mathrm{End}\,(A)$ si celle-ci est non nulle, et est infini si cette caractéristique est nulle. Dans le cas d'un groupe G non commutatif, l'énoncé n'a pas de sens puisque $\mathrm{End}\,(G)$ n'a pas de structure naturelle d'anneau.

[S 90] (14.1.5) $\mu_n(\mathbb{Q}) = \mu_n(\mathbb{R}) = \begin{cases} \{-1,+1\} & (n \text{ pair}) \\ \{+1\} & (n \text{ impair}). \end{cases}$

[S 91] (14.1.6) $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$, groupe d'ordre 4 tué par 2 donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

D'après 12.5.5 (ou directement !), $(\mathbb{Z}/15\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$, donc à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ qui n'est pas cyclique.

[S 92] (14.5.1) C'est le nombre d'éléments annulés par n dans $\mathbb{Z}/(p-1)\mathbb{Z}$, égal d'après 12.8.2 au pgcd de n et $p-1$.

[S 93] (14.5.2) (i) L'implication $\Rightarrow$ est vraie, l'autre est fausse : $\mu_n^\circ(k)$ peut être vide. En fait $\mu_n^\circ(k)$ est non vide si et seulement si $|\mu_n(k)| = n$; si cette condition est réalisée, l'équivalence de (i) est vraie.

(ii) Vrai (cf. 12.5.3).

(iii) Vrai.

[S 94] (14.5.3) $\mu_n^\circ(\mathbb{Q}) = \begin{cases} \{1\} & \text{si } n = 1 \\ \{-1\} & \text{si } n = 2 \\ \emptyset & \text{si } n > 2. \end{cases}$

$\mu_n^\circ(\mathbb{C})$ est l'ensemble des $e^{2ik\pi/n}$ avec k entier premier à n (et $0 \leq k < n$, si l'on veut).

$$\mu_n^\circ(\mathbb{Z}/7\mathbb{Z}) = \begin{cases} \{1 \bmod 7\} & \text{si } n = 1 \\ \{6 \bmod 7\} & \text{si } n = 2 \\ \{2 \bmod 7, 4 \bmod 7\} & \text{si } n = 3 \\ \{3 \bmod 7, 5 \bmod 7\} & \text{si } n = 6 \\ \emptyset & \text{dans tous les autres cas.} \end{cases}$$

[S 95] (14.5.4) (1) D'après Fermat (7.11), on a $y^2 = 1$ donc $y = \pm 1$ puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps.

(2) Puisque $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$, l'énoncé se traduit par : « un élément de $\mathbb{Z}/(p-1)\mathbb{Z}$ est annulé par $(p-1)/2$ si et seulement si c'est la classe d'un entier pair », ce qui est élémentaire.

(3) Il suffit de remarquer que $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ si et seulement si $p \equiv 1 \pmod{4}$ (on rappelle que p est supposé impair, donc ≥ 3).

[S 96] (15.3.3) Soit Σ une partie génératrice de G. Par hypothèse, G est engendré par une partie finie $F = \{x_1, \ldots, x_n\}$. Pour chacun des x_i, on trouve en appliquant 4.4 une partie finie Σ_i de Σ telle que x_i soit produit d'éléments de $\Sigma_i \cup \Sigma_i^{-1}$. La réunion S des Σ_i est une partie finie de Σ telle que $\langle S \rangle$ contienne tous les x_i. Puisque ceux-ci engendrent G, $\langle S \rangle = G$.

[S 97] (15.8.4) D'après 13.5, la première assertion de 15.8.2 se ramène au cas des p-groupes, et la seconde en résulte d'après 15.8.3.

[S 98] (16.1.1) De préférence, on ne parle de « sous-truc » d'un objet que si celui-ci est lui-même un « truc » : seul un p-groupe peut avoir des « sous-p-groupes ».

[S 99] (16.3.4) Notons q le cardinal de k (qui est une puissance de p). Il est facile de montrer que U est un p-groupe. Pour voir que c'est un p-sylow on peut par exemple utiliser la formule de 8.3.2 donnant l'ordre de G ; si l'on veut éviter les calculs, on peut aussi remarquer que l'indice de U dans le groupe triangulaire supérieur T est premier à p (c'est $(q-1)^n$, correspondant aux coefficients diagonaux) et qu'il suffit donc de voir que $(G : T)$ est premier à p. Or d'après 8.3.3 cet indice est le nombre δ_d de drapeaux complets de K^d, lequel est déterminé par la formule de récurrence $\delta_d = \frac{q^d-1}{q-1}\,\delta_{d-1}$ $(d > 0)$, d'où le résultat par récurrence puisque $\delta_0 = 1$.

[S 100] (16.3.5) (1) Exemple avec $p = 2$: dans $G = \mathfrak{S}_3$, prendre pour G' et S deux sous-groupes d'ordre 2 distincts.

[S 101] (16.4.4) Toutes, sauf la congruence de (i), celle de (iv), et l'assertion de divisibilité de (iv).

[S 102] (16.4.6) Come G et A sont deux parties de G, la notation GA a déjà un sens différent (7.1).

[S 103] (17.1.4) Dans le diagramme ci-dessous, j et π sont les flèches canoniques, u est l'isomorphisme de G_1 sur $f_1(G_1)$ induit par f_1, et v est l'inverse de l'isomorphisme canonique de $G_2/f_1(G_1)$ sur G_3 déduit du fait que $f_1(G_1) = \mathrm{Ker}\,(f_2)$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_1 & \xrightarrow{f_1} & G_2 & \xrightarrow{f_2} & G_3 & \longrightarrow & 1 \\
 & & \downarrow u & & \| & & \downarrow v & & \\
1 & \longrightarrow & f_1(G_1) & \xrightarrow{j} & G_2 & \xrightarrow{\pi} & G_2/f_1(G_1) & \longrightarrow & 1
\end{array}$$

[S 104] (17.2.5) L'application composée $(f_{|Y'})^{-1}$ est une application de Y dans Y', et non de Y dans X. La bonne formule est $s = j \circ (f_{|Y'})^{-1}$, où $j : Y' \to X$ est l'application canonique d'inclusion.

[S 105] (17.4.1) L'énoncé est faux pour (i), si $r = \pm 1$. Dans les autres cas, il suffit de remarquer qu'il n'existe aucun morphisme injectif de $\mathbb{Z}/r\mathbb{Z}$ dans $\mathbb{Z}$ (resp. de $\mathbb{C}^*$ dans $\mathbb{C}$) car le premier groupe a de la torsion alors que le second n'en a pas.

[S 106] (17.4.5) Les sections sont les applications de la forme $1 \mapsto e$, $-1 \mapsto \alpha$ où α est un élément d'ordre 2 de $\mathfrak{S}_r$ qui est impair, c'est-à-dire le produit d'un nombre impair de transpositions disjointes.

[S 107] (17.9.4) (1) Pour que $n \mapsto n^{-1}$ soit bien un automorphisme de N.
(2) Comme N est d'indice 2 il est noyau d'un morphisme surjectif $\pi : G \to \{-1, +1\}$. Si l'on fixe arbitrairement $\tau \in G - N$, alors $H = \{e, \tau\}$ est un sous-groupe de G qui correspond à une section de π. Donc G est produit semi-direct $N \rtimes_\varphi \{-1, +1\}$. Mais la formule de définition du produit semi-direct montre que la condition de l'énoncé n'est réalisée que si $\varphi(-1)$ est l'application $n \mapsto n^{-1}$. Celle-ci est donc un automorphisme de N qui est donc nécessairement commutatif.
(3) Prendre $N = \mathrm{SO}(2, \mathbb{R})$ et remarquer que tout élément de G de déterminant -1 est une symétrie par rapport à une droite.

[S 108] (17.11) Prendre par exemple $G = N \rtimes_\varphi \mathbb{Z}$ où $\varphi : \mathbb{Z} \to \mathrm{Aut}(G)$ envoie n sur u^n. Variante : $G = N \rtimes_\varphi \Gamma$ où Γ est un sous-groupe de $\mathrm{Aut}(G)$ contenant u, et où φ est l'inclusion de Γ dans $\mathrm{Aut}(G)$.

[S 109] (17.12) On peut traiter à part le cas $p = 2$. Supposons p impair et soit G d'ordre $2p$. Soit N un p-sylow de G : alors N est d'indice 2 donc distingué, et G est extension de $\{-1, +1\}$ par N. Comme ce dernier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, $\mathrm{Aut}(N)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$ donc est cyclique d'ordre $p - 1$ et a donc un unique élément d'ordre 2, correspondant à l'automorphisme $\sigma : n \mapsto n^{-1}$ de N. Les deux seuls morphismes de $\{-1, +1\}$ dans $\mathrm{Aut}(N)$ sont donc le morphisme trivial (qui donne le groupe produit, cyclique d'ordre $2p$) et le morphisme envoyant -1 sur σ (qui donne le groupe diédral).

[S 110] (18.6.4) Pour $n = 0$ ou 1, il n'y en a pas (la seule suite de Jordan-Hölder d'un groupe trivial se réduit à ce seul groupe). Pour $n = 2$ le groupe est simple, isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Pour $n = 3$ et pour $n \geq 5$ il y a une unique suite de Jordan-Hölder qui est $\{e\} \lhd \mathrm{A}_n \lhd \mathfrak{S}_n$, à quotients successifs A_n et $\mathbb{Z}/2\mathbb{Z}$.

Enfin, pour $n = 4$, notons H le sous-groupe de A_4 (distingué dans $\mathfrak{S}_4$, et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$) formé de l'identité et des trois doubles transpositions : alors $\mathfrak{S}_4$ a trois suites de Jordan-Hölder, de la forme

$$\{e\} \lhd \Delta \lhd H \lhd \mathrm{A}_4 \lhd \mathfrak{S}_4$$

où Δ désigne l'un des trois sous-groupes d'ordre 2 de H. Les quotients sont donc $\mathbb{Z}/2\mathbb{Z}$ (3 fois) et $\mathbb{Z}/3\mathbb{Z}$.

Table des matières