UNIVERSITÉ DE RENNES 1

INSTITUT MATHÉMATIQUE DE RENNES

Licence de mathématiques

ALGÈBRE

Cours rédigé par Laurent Moret-Bailly
Septembre 1997

Chapitre I

Groupes

1. Définitions, 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 ?)

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 $g * g'$? (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.

1.3. *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

$$(a_1 \cdots a_m)(b_1 \cdots b_n) = a_1 \cdots a_m b_1 \cdots b_n \tag{1.3.5.1}$$

(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 $a^{-1}b^{-1}$: aviez-vous trouvé ?).

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 ?

1.4.3. Si n est un entier naturel, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo n, étudié en première année, 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.* 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 (multplication 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.)

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 $\mathfrak{S}(E)$?

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 $n!$.

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. *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. 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. 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.

(Indications : pour (iii) et (iii) utiliser (i) ; pour (v) remarquer que la "diagonale" $\Delta = \{(x, y) \in G \times G \,|\, x = y\}$ 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 $G \times G$).

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 $\mathrm{Hom}_{\mathrm{groupes}}(G,H)$ *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. Plus généralement (exercice) : si f et g sont deux morphismes de G dans H, alors l'application $fg : G \to H$ défini 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 $\mathrm{Hom}_{\mathrm{groupes}}(G,H)$. Quel est l'inverse d'un morphisme f pour cette loi ? Et en quoi cet exercice généralise-t-il 2.2.3 ?

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 : si V et W désignent deux $\mathbb{Q}$-espaces vectoriels, tout morphisme de groupes de $(V,+)$ dans $(W,+)$ est $\mathbb{Q}$-linéaire. (Indication : utiliser 1.4.5).

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 1.4.9 : 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

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

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 $\mathrm{Hom}_{\mathrm{groupes}}(\mathbb{Z}, G)$ 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 fiormule est bien un morphisme de groupes envoyant 1 sur γ, ce qui est immédiat. ∎

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 morphisme. 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.* 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 $f \circ g = \mathrm{Id}_H$. ∎

2.6. *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. 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,

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

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 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. 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.

Par contre la réunion des H_i n'est pas en général un sous-groupe. Par exemple (exercice) la réunion de *deux* sous-groupes de G n'est un sous-groupe que si l'un des deux est inclus dans l'autre.

Autre exercice : si G est un groupe commutatif et si pour $n \in \mathbb{Z}$ on pose $G_n = \{g \in G \mid g^n = e_G\}$, alors $\bigcup_{n\in\mathbb{Z}\setminus\{0\}} G_n$ est un sous-groupe de G.

3.3.6. *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. Quel est le centralisateur de l'ensemble vide ? de $\{e\}$? À quelle condition sur S a-t-on la propritété 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 ?

3.3.7. *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.)

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 $g = h$. ∎

3.5. *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 $\langle\gamma\rangle$.

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'o ù $\gamma^k = \gamma^r$. Autrement dit les éléments de $\langle\gamma\rangle$ sont $e, \gamma, \gamma^2, \ldots \gamma^{n-1}$. 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'autre 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).

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 $\langle\gamma\rangle = \{e, \gamma, \gamma^2, \ldots \gamma^{n-1}\}$, 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.* ∎

3.12. *Exercice.* Soit G un groupe topologique (cf. 1.5).

3.12.1. 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. On suppose que G est localement connexe (tout point de G admet une base de voisinages connexes). 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 à la fois ouvert et fermé dans G.

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

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

(Indication : 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 $H = a\mathbb{Z}$).

3.12.4. Soit Θ un nombre réel *irrationnel*. Montrer que l'ensemble $\mathbb{Z} + \mathbb{Z}\Theta$ 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 $\mathbb{R}$. (Considérer son adhérence et utiliser 3.12.1 et 3.12.3).

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. 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 $|\zeta^n - 1| < \varepsilon$. (Indication : écrire $\zeta = e^{2i\pi\Theta}$ et appliquer 3.12.4).

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.*

"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 :* 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 H l'ensemble des mots sur S.

Il est clair que H 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 H est un sous-groupe de G : d'abord H 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 H est bien un sous-groupe d'après 3.2.2.

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

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 H. ∎

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.* 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.* 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 $\langle S \rangle \subset \mathrm{Ker}\, f$, de deux manières différentes : en utilisant 4.2 et en utilisant 4.4. Que pensez-vous de la réciproque ?

4.4.4. *Exercice.* Si S est une partie d'un groupe G, montrer que $Z_G(S) = Z_G(\langle S \rangle)$ (cf. 3.3.6). Si tous les éléments de S commutent entre eux, que peut-on dire du groupe $\langle S \rangle$? Réciproque ?

4.4.5. *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 (11.7) 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 ?

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 $x \in E$. 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. *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).

5.3.6. 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 ?

5.3.7. 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.

5.3.8. Gardons les notations de 5.3.7. 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 $E = K$.

5.3.9. 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 translations*, donnée par $(h, x) \mapsto hx$ pour $h \in H$ et $x \in G$;

– l'action à *droite par translations*, 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 !

5.3.10. *Exercice.* Prenant $H = G = \mathbb{Z}$ dans 5.3.9, on obtient trois actions de $\mathbb{Z}$ sur lui-même et donc, d'après 5.3.5, 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.* 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.* Montrer que l'action à gauche de G sur lui-même par translations 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 (5.3.5) 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 :* dans l'exemple 5.3.7, quelles sont les orbites pour l'action de $\mathrm{GL}(V)$ sur V ? (On doit trouver "en général" deux orbites). Et pour l'action de K^* sur V ? Cette dernière action est-elle libre ? Et pour l'action de $\mathrm{GL}(V)$ sur l'ensemble des sous-espaces de V définie en 5.3.8 ? (On pourra supposer V de dimension finie).

5.4.9. *Exercice.* 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, $g^{-1}G_xg$. *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 5.3.8, 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 5.3.9 :

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'apelle simplement la classe de conjugaison de x dans G. Le stabilisateur de x est le *centralisateur* $Z_G(x)$ de x, déjà rencontré (3.3.6).

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 translations sont libres ; nous allons les étudier en détail au paragraphe suivant.

6. Classes modulo un sous-groupe

6.1. *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 $A \subset CB^{-1}$?).

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 ?

6.2. *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 5.3.9 : elle est donnée, rappelons-le, par $(h, x) \mapsto hx$ pour $h \in H$ et $x \in G$, et elle est libre.

Définition 6.2.1 *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 $H\backslash G$.

6.2.2. *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".

6.2.3. 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 (6.7). Notons tout de suite que les classes à gauche et à droite coïncident lorsque G est commutatif.

6.2.4. *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 11.1.4 plus bas 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 6.3 *Avec les notations de* 6.2, *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. 6.1, et de même pour la dernière propriété. ∎

6.4. *Remarques.* On garde les notations de 6.2.

6.4.1. *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 6.3.

6.4.2. 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.

6.4.3. 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 6.5 *Soient G un groupe, H un sous-groupe de G. Alors*

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

■

Corollaire 6.6 (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). ∎

6.7. *Classes à gauche.* Les classes à gauche modulo un sous-groupe H d'un groupe G sont par définition (6.2.3) 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.

6.7.1. *Exercice.* Soit $f : G \to G'$ un morphisme de groupes, et soit $H = \operatorname{Ker} f$. 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 8.)

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).

6.7.2. *Exercice.* 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.

6.7.3. *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.

6.7.4. Les analogues de 6.5 et 6.6 pour les classes à droite 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.

6.8. *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 $(G : H) = \infty$.

6.8.1. *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.

6.8.2. *Exercice* (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 $G = \mathbb{Z}$).

6.8.3. *Exercice* ("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. (Si G est fini c'est une conséquence immédiate de 6.5 ; sinon on montrera que si $(x_i)_{i\in I}$ est un système de représentants de K modulo H (cf. 6.4.1) 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).

6.9. *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 $(Hx, g) \mapsto Hxg$.

6.10. *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.

6.10.1. Montrer que toute classe à droite Hx de G modulo H est homéomorphe à H. De plus si H est ouvert (resp. fermé) dans G, il en est de même de Hx. Même chose pour les classes à gauche.

6.10.2. Soit H un sous-groupe ouvert de G. Montrer que H est fermé. (Remarquer que le complémentaire de H est réunion de classes).

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

Montrer que $\pi : G \to H\backslash G$ est continue et ouverte. (Pour U ouvert dans G, remarquer que $\pi^{-1}(\pi(U))$ est la réunion des hU pour $h \in H$).

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.

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

7. Classes et actions de groupes

Théorème 7.1 *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. 6.7. ∎

7.1.1. *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.

7.1.2. *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 6.7.2.

7.1.3. *Remarque.* On a naturellement une variante de 7.1 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.

7.1.4. *Exercice.* G opère naturellement à gauche sur les deux ensembles G/G_x et Gx intervenant dans 7.1 : l'action sur Gx est induite par l'action sur E, et l'action sur G/G_x est celle de 6.9. Montrer que l'application φ est G-équivariante, et est donc un isomorphisme de G-ensembles (5.2.3).

7.1.5. *Remarque.* Les énoncés 5.5, 5.6 et 7.1 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) ; 7.1 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.

7.1.6. *Exercice.* Soit H un sous-groupe de G. Appliquant 7.1 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 ?

7.1.7. *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 (5.3.5) 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 7.1 n'est pas la même pour tous !

Corollaire 7.2 *Avec les hypothèses et notations de* 7.1*, 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 7.1, la première formule résulte de la définition de l'indice $(G : G_x)$ (6.8). La seconde en découle par 6.5, et la troisième par 6.6. ∎

7.2.1. *Exercice : applications à des questions de dénombrement.* 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...)

Corollaire 7.3 ("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 7.1 et 6.6. ∎

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

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

Proposition 7.5 *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. ∎

7.5.1. *Question.* Où a servi le fait que p est premier ?

7.5.2. *Exercice.* Pour p premier, $s \in \mathbb{N}$, et k entier vérifiant $0 < k < p^s$, appliquer 7.5 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 7.6 *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 7.5 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. ∎

8. Sous-groupes distingués, groupes quotients

Proposition 8.1 *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. ∎

8.1.1. *Question.* 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 8.2 *Un sous-groupe H d'un groupe G est dit* distingué *s'il vérifie les conditions équivalentes de* 8.1.

8.3. *Commentaires.*

8.3.1. 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".

8.3.2. *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.

8.3.3. *Noyaux, images réciproques.* L'exercice 6.7.1, ou une vérification immédiate, montre que *le noyau d'un morphisme est automatiquement distingué* ; la réciproque arrive, cf. 8.4. 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.

8.3.4. *Contre-exemples, images.* L'exercice 6.7.2 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 ?

8.3.5. *Sous-groupes d'indice 2.* Ils sont automatiquement distingués, comme le montre l'exercice 6.8.1.

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

Proposition 8.4 *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 (8.3.3). ∎

8.4.1. *Question.* La même qu'en 8.1.1 ; le lecteur observera ici l'intérêt "économique" d'une stratégie circulaire comme (i)⇒(ii)⇒(iii)⇒(i).

8.4.2. *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 6.1. Est-ce la même chose ?

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

8.4.4. 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.

8.4.5. *Exercice.* Soit G un groupe. Montrer que toute relation d'équivalence $\sim$ sur G compatible avec la loi de G est du type décrit en 8.4, pour un unique sous-groupe distingué H de G que l'on précisera.

8.4.6. *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 8.5 *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 $H = \mathrm{Ker}\,(f)$;*

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

Démonstration. Les implications (ii)⇒(iii) et (iii)⇒(i) sont immédiates, et l'implication (i)⇒(ii) résulte de la dernière assertion de 8.4. ∎

8.5.1. *Exercice.* Un groupe G est dit *simple* si les seuls sous-groupes distingués de G sont $\{e\}$ et G.

Montrer qu'un groupe *commutatif* est simple si et seulement si il est trivial ou 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.

Théorème 8.6 ("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) *$H \subset \mathrm{Ker}\, f$.*

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

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

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

8.7. *Commentaires.*

8.7.1. 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* 8.6, *le diagramme*

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

se prolonge de façon unique en un diagramme commutatif

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

8.7.2. 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.

8.7.3. À titre d'exercice, voici une autre manière de présenter 8.6 : étant donnés f, H et π comme dans l'énoncé, on considère l'application

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

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

Théorème 8.8 *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 8.6 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 8.6.

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. ∎

8.8.1. *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.

8.8.2. *Remarque.* Notons φ l'isomorphisme construit dans 8.8. 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'.

8.8.3. *Exercice.* L'isomorphisme de 8.8 est en particulier une bijection de $G/\mathrm{Ker}\, f$ sur $\mathrm{Im}\, f$. Montrer que c'est un cas particulier de 7.1. (Considérer l'action de G sur G' donnée par $(g, g') \mapsto f(g)g'$).

8.8.4. *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.

8.8.5. *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 ? Retrouver ainsi tous les résultats de 3.11.

8.8.6. *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.

8.8.7. *Exercice.* Soient G un groupe et C son centre (3.3.7). 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. 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

$$\pi : G \longrightarrow\!\!\!\!\!\rightarrow G'$$

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

$$H = \operatorname{Ker} \pi$$

qui est donc un sous-groupe distingué de G. Cette situation contient naturellement le cas particulier où $G' = G/H$, et 8.8 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 9.1 *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

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

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 $\pi^{-1}(\Delta) \cap \operatorname{Ker} \pi = \pi^{-1}(\Delta) \cap H = H$. L'isomorphisme annoncé se déduit donc de 8.8. ∎

Proposition 9.2 *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 un isomorphisme canonique

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

Démonstration. On sait déjà que $\pi(\Gamma)$ est un sous-groupe de G'. D'autre part, $\pi^{-1}(\pi(\Gamma))$ contient H d'après 9.1 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 "$\gamma^{-1}x \in \operatorname{Ker} \pi$").

Enfin, on a évidemment un morphisme surjectif $\Gamma \to \pi(\Gamma)$ induit par π, dont le noyau est $\Gamma \cap \operatorname{Ker} \pi = \Gamma \cap H$, d'où par 8.8 l'isomorphisme annoncé. ∎

9.2.1. *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.

9.2.2. *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.

Proposition 9.3 *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 9.1 ;

(2) si Γ est un sous-groupe de G contenant H, alors $\pi^{-1}(\pi(\Gamma)) = \Gamma$; mais ceci résulte de 9.2 puisqu'ici on a $H\Gamma = \Gamma$.

Que ces applications respectent les inclusions et les intersections est un petit exercice purement ensembliste ; d'autre part on sait déjà que $\pi^{-1}(\Delta) \lhd G$ si $\Delta \lhd G'$. 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 $\pi^{-1}(\Delta) \lhd G$ d'après ce qui précède. 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 par 8.8. ∎

9.4. *Exemple : sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.* Soit n un entier : on déduit de 9.3 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 9.5 *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 9.3 (prendre $G' = G/H$ et $\Delta = K/H$). ∎

9.5.1. *Exemple.* Revenant aux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (9.4) 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 6.6).

Théorème 9.6 *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 9.2 en prenant $G' = G/H$. ∎

9.6.1. *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.

10. Groupes cycliques

Définition 10.1 *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 $n > 0$).*

10.2. *Remarques.*

10.2.1. L'équivalence des conditions ci-dessus est immédiate et laissée en exercice.

10.2.2. 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.

10.2.3. 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.

10.2.4. 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.

10.2.5. *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 "$k \bmod n$". (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).

10.3. *Exercices.*

10.3.1. Soit G un groupe fini d'ordre n. Alors G est cyclique si et seulement si G admet un élément d'ordre n.

10.3.2. Soit G un groupe fini d'ordre n *premier*. Alors G est cyclique. (Utiliser 10.3.1 et le théorème de Lagrange).

10.3.3. 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.

10.3.4. 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 $\Gamma = \Gamma_n$. (Indication : considérer les racines du polynôme $X^n - 1$).

En particulier, *tout sous-groupe fini de* $\mathbb{C}^*$ *est cyclique* ; nous verrons plus loin que cette propriété est encore vraie si l'on remplace $\mathbb{C}^*$ par K^* où K est un corps commutatif quelconque.

10.3.5. Soient G un groupe et C son centre. On suppose que G/C est monogène. Montrer que G est commutatif (autrement dit, $G = C$). (Indication : considérer un élément γ de G dont la classe engendre G/C et montrer que G est engendré par $C \cup \{\gamma\}$.)

10.3.6. Soient p un nombre premier et G un groupe d'ordre p^2. Montrer que G est commutatif.

(Indications : soit C le centre de G ; on déduit de 7.6 que C est d'ordre p ou p^2. Comme on a gagné si C est d'ordre p^2 (pourquoi ?) il suffit de traiter — et, en fait, d'exclure — le cas $|C| = p$. Mais si $|C| = p$ on a aussi $|G/C| = p$ et l'on conclut en appliquant 10.3.2 et 10.3.5.)

10.3.7. *Exercice.* Déduire de 10.3.6 que, sous les mêmes hypothèses, G est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

(Indication : 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).

10.3.8. 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 $m = 1$?) Par contre :

Proposition 10.4 ("lemme chinois") *Soient a et b deux entiers* premiers entre eux. *Alors il existe un isomorphisme*

$$f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$$

vérifiant, 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. On peut supposer que a et b sont ≥ 0. De plus si par exemple $a = 0$ alors $b = \mathrm{PGCD}(a, b) = 1$ et l'énoncé se vérifie directement. On supposera donc dans la suite que a et b sont tous deux > 0, de sorte que les groupes apparaissant dans l'énoncé sont finis.

Considérons le morphisme $\varphi : \mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ défini par

$$\varphi(k) = (k \bmod a, k \bmod b)$$

pour tout $k \in \mathbb{Z}$. Son noyau est l'ensemble des entiers k tels que a et b divisent tous deux k ; c'est donc $m\mathbb{Z}$ où m désigne le PPCM de a et b. Comme ceux-ci sont premiers entre eux par hypothèse, on a $m = ab$. On déduit alors de 8.8 un isomorphisme $f : \mathbb{Z}/ab\mathbb{Z} \xrightarrow{\sim} \mathrm{Im}\,\varphi$ vérifiant de plus par construction la relation $f(k \bmod ab) = (k \bmod a, k \bmod b)$ de l'énoncé. Il ne reste plus, pour conclure, qu'à voir que φ est surjectif : or ce qui précède montre que $|\mathrm{Im}\,\varphi| = ab$ qui est aussi l'ordre du groupe $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$, d'où la conclusion. ∎

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 8.6.

Proposition 10.5 ("propriété universelle de $\mathbb{Z}/n\mathbb{Z}$") *Soient n un entier et Γ un groupe. L'application*

$$\begin{array}{ccc} \mathrm{Hom}_{\text{groupes}}(\mathbb{Z}/n\mathbb{Z}, \Gamma) & \longrightarrow & \{\gamma \in \Gamma \mid \gamma^n = e\} \\ f & \longmapsto & f(1 \bmod n) \end{array}$$

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 $\gamma^n = e$).* ∎

Le reste de ce paragraphe est consacré aux sous-groupes des groupes monogènes.

Proposition 10.6 *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 9.4 et 9.5.1. ∎

10.6.1. *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 (IV.6.4) une réciproque.

10.6.2. 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 mod 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 10.7 *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 9.2 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 $\Delta = d\mathbb{Z}/n\mathbb{Z}$. ∎

10.8. *Exercice.* Redémontrer 10.7 en utilisant l'assertion (i) de 3.7 et la dernière assertion de 9.2.

11. Le groupe symétrique

11.1. *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 $\{1, \ldots, n\}$).

11.1.1. 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).

11.1.2. 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.

11.1.3. 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 $n \geq 3$; elle est transitive (exercice).

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

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

11.1.5. *Exercice.* Testez votre compréhension de 11.1.2 et 11.1.4 en vérifiant la relation

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

11.1.6. *Exercice.* Montrer que, pour $n \geq 3$, le centre de $\mathfrak{S}_n$ est trivial.

11.2. *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 :

11.2.1. *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.

11.2.2. *Orbites.* Les *orbites* sous $\sigma \in \mathfrak{S}_n$ sont les orbites sous l'action de $\langle\sigma\rangle$ sur $\{1, \ldots, n\}$. C'est l'occasion de relire 5.3.5, 5.4.7 et 7.1.7 ; nous y reviendrons un peu plus loin.

11.2.3. *Parties stables.* Une partie A de $\{1, \ldots, n\}$ 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, pourquoi ?). 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.

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

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

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 ?

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

Proposition 11.3.1 *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 $i \in \{1, \ldots, n\}$,*

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

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

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

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

11.4.1. Pour $i \in \{1, \ldots, n\}$ donné, rappelons (7.1.7) 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 11.4.2 *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 :

$$\gamma(i) = \begin{cases} i & \text{si } i \notin \{i_1, \ldots, i_l\} \\ i_{k+1} & \text{si } i = i_k (0 \leq k < l) \\ i_1 & \text{si } i = i_l \end{cases}$$

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

11.4.3. 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. 11.4.5 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.

11.4.4. 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 $\mathrm{Supp}\,(i_1, \ldots, i_l)$ 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 $\mathfrak{S}_n$.

11.4.5. 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 $j_k = i_{\mathrm{reste}(k+a)}$ pour tout k, où $\mathrm{reste}(x)$ désigne le reste de la division de l'entier x par l. Vérifiez !

11.4.6. *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 $\{1, \ldots, n\}$.

11.4.7. *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 !

11.4.8. *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 11.4.1 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 $(6) = \mathrm{Id}$.

Proposition 11.5 *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 11.3.1 (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. ∎

11.6. *Propriétés de la décomposition en cycles.*

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

11.6.2. Une propriété très importante de la décomposition de 11.5 est que les γ_i *commutent* deux à deux, puisqu'ils sont à supports disjoints. En conséquence, on a (toujours avec les notations de 11.5) $\sigma^k = \sigma_1^k \cdots \sigma_m^k$ 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 11.3.1(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.

11.6.3. *Type et conjugaison des cycles.* Avec les notations de 11.5, 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 11.4.7 que *deux permutations conjuguées ont même type.* Inversement, il est facile de voir que le type détermine la classe de conjugaison :

Proposition 11.6.4 *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 11.4.7. 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 11.4.7 que $\alpha\sigma\alpha^{-1} = \sigma'$. ∎

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

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

Proposition 11.7 *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 11.5 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 ? ∎

11.7.1. Voici une autre preuve de 11.7 qui n'utilise pas 11.5 : 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 :

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

(Indication : remarquer que pour $1 \neq i \neq j \neq 1$, on a $(1, i)(1, j)(1, i)^{-1} = (i, j)$ d'après 11.4.7 ou par un calcul direct. Appliquer ensuite 11.7. Les arguments de conjugaison sont très fréquents dans ce genre de question.)

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

(Indications : si Γ est le sous-groupe engendré par ces transpositions, alors une relation similaire à celle vue dans la preuve de 11.7 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 11.7.2 ci-dessus.)

11.7.4. *Exercice.* Montrer que $\mathfrak{S}_n$ est engendré par $\{(1, 2), (1, 2, \ldots, n)\}$. (Utiliser 11.7.3 et un argument de conjugaison).

Définition 11.8 *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 11.9 *Soient σ et $\tau \in \mathfrak{S}_n$. Alors :*

(i) *si $x_1, \ldots, x_n$ 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

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

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 $\varphi(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n}(x_i - x_j)$. 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

$$(\sigma\tau)\varphi = \varepsilon(\sigma\tau)\, \varphi \tag{11.9.0.1}$$

et d'autre part

$$\sigma(\tau\varphi) = \sigma(\varepsilon(\tau)\, \varphi) = \varepsilon(\tau)\, (\sigma\varphi) = \varepsilon(\tau)\, \varepsilon(\sigma)\, \varphi \tag{11.9.0.2}$$

où l'on utilise le fait, évident, que l'action de de $\mathfrak{S}_n$ sur $\mathcal{F}$ est linéaire. Égalant (11.9.0.1) et (11.9.0.2) 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. ∎

11.10. *Remarques et exercices.*

11.10.1. Comme on le voit sur la démonstration, la relation (i) est encore valable lorsque $x_1, \ldots, x_n$ sont des éléments quelconques d'un *anneau commutatif unitaire* A (voir chapitre II), à condition d'interpréter $\varepsilon(\sigma)$ comme un élément de A (à savoir l'élément neutre 1_A de la multiplication de A ou son opposé).

L'argument utilisé pour déduire (ii) de (i) fonctionne-t-il encore si l'on remplace $\mathbb{R}$ par A ?

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

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

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

qui sert parfois de définition à la signature. *Exercice :* partir de cette formule pour redémontrer 11.9. Attention, il faut commencer par montrer que $\varepsilon(\sigma) \in \{-1, +1\}$!

11.10.4. *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.

11.10.5. *Exercice.* Que pensez-vous de l'idée de prendre 11.9(iii) comme définition de la signature ?

11.10.6. *Le groupe alterné.* L'assertion 11.9(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 $n \geq 2$ (puisque les transpositions sont impaires). Son noyau (l'ensemble des permutations paires) est donc un sous-groupe d'indice 2 de $\mathfrak{S}_n$, appelé *groupe alterné* et noté A_n. C'est un groupe d'ordre $n!/2$; il est trivial pour $n = 2$, cyclique d'ordre 3 pour $n = 3$ (il est formé de l'identité et des deux cycles d'ordre 3 de $\mathfrak{S}_3$), et non commutatif pour $n \geq 4$.

Un théorème célèbre (et pas très difficile) de Galois dit que pour $n \geq 5$ le groupe A_n est *simple* (cf. 8.5.1).

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.

11.10.7. *Exercice.* Déduire du théorème de Galois mentionné en 11.10.6 que, pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{S}_n$ et A_n.

11.11. *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).

11.11.1. 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* $1 \neq -1$ *dans* K. (C'est du DEUG deuxième année).

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

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \ldots, x_n) \qquad (11.11.2.1)$$

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 $x_i = x_j$. (Encore une fois on n'exclut pas que $1 = -1$ dans K !)

11.11.3. 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

$$f(x_1, \ldots, x_n) = (\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n \xi_{i,\sigma(i)}) f(e_1, \ldots, e_n). \tag{11.11.3.1}$$

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.

11.12. *Déterminants (suite de l'exercice précédent).* Avec les notations de 11.11.3, 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.

11.12.1. Déduire de 11.11.3 que $\dim \Omega^n(E) \leq 1$. Montrer ensuite que l'application φ de E^n dans K *définie* par

$$\varphi(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^n \xi_{i,\sigma(i)} \tag{11.12.1.1}$$

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.

(Indication : 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 $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.)

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

11.12.3. 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 $\det(v \circ u) = \det(u) \det(v)$.

11.13. *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.

11.14. *Remarques sur les exercices précédents.* Les exercices 11.11 et 11.12 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 11.11.3) de déduire de ces propriétés la formule (où les $a_{i,j}$ sont les coefficients de la matrice $A \in \mathrm{M}_n(K)$)

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}. \tag{11.14.1}$$

On peut d'ailleurs voir cette formule comme un cas particulier de (11.11.3.1). 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 (11.14.1), alors on a bien les propriétés exigées. C'est essentiellement le contenu de 11.12.1 : 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".

Chapitre II

Anneaux et corps

1. Anneaux et morphismes : définitions

Définition 1.1 *Un* anneau *est un ensemble A muni de deux lois de composition internes*

$$\begin{array}{ccll} A \times A & \longrightarrow & A & \\ (a,b) & \longmapsto & a+b & \text{(addition)} \\ (a,b) & \longmapsto & ab & \text{(multiplication)} \end{array}$$

vérifiant les propriétés suivantes :

(i) $(A,+)$ *est un* groupe commutatif *;*

(ii) *la multiplication est* associative *;*

(iii) *la multiplication est* distributive *à droite et à gauche par rapport à l'addition, c'est-à-dire que l'on a $a(b+c) = ab+ac$ et $(a+b)c = ac+bc$ pour tous $a,b,c \in A$.*

L'anneau A est dit commutatif *si de plus la multiplication est commutative ; il est dit* unitaire *si la multiplication admet un élément neutre.*

1.2. *Commentaires.*

1.2.1. *Abus de langage :* ce sont essentiellement les mêmes que pour les groupes. Il y en a un de plus ici : on aurait dû définir un anneau comme un triplet $(A,+,.)$ plutôt que comme "un ensemble muni de. . .".

1.2.2. *Notations.* Pour la multiplication on note parfois $a.b$ ou $a \times b$ au lieu de ab. Pour l'addition on applique les conventions en vigueur dans tout groupe commutatif noté additivement : 0 ou 0_A pour l'élément neutre, $-a$ pour l'opposé de a, etc.

Dans un anneau A unitaire, l'élément neutre de la multiplication (qui est unique) est noté 1 ou 1_A, et parfois appelé *l'élément unité* de A.

1.2.3. On peut reformuler la condition (iii) de la définition en disant que, pour tout $a \in A$, les deux applications

$$\begin{array}{rcl} A & \longrightarrow & A \\ x & \longmapsto & ax \\ \text{et} \quad x & \longmapsto & xa \end{array}$$

sont des *endomorphismes de groupe* de $(A, +)$. On voit en particulier que l'on a $x.0 = 0.x = 0$ et $x.(-y) = (-x).y = -(xy)$ pour tous $x, y \in A$. Si A est unitaire on en déduit que $(-1).x = -x = x.(-1)$.

1.3. *Exemples.*

1.3.1. *L'anneau nul.* Tout ensemble $A = \{x\}$ à un élément admet une unique structure d'anneau, d'ailleurs commutatif et unitaire. Noter que l'on a $1 = 0$ dans cet anneau ; inversement, si cette relation est vérifiée dans un anneau unitaire A, alors $A = \{0\}$ puisque l'on a $x = 1.x = 0.x = 0$ pour tout $x \in A$.

1.3.2. *Anneaux de nombres.* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition et de la multiplication habituelles sont des anneaux commutatifs unitaires.

Il en est de même de l'ensemble des *nombres décimaux*, i.e. de la forme $a/10^k$ avec $a \in \mathbb{Z}$ et $k \in \mathbb{N}$, et naturellement de tous les analogues obtenus en remplaçant 10 par un entier donné (2 par exemple).

1.3.3. *Polynômes.* L'ensemble $\mathbb{R}[X]$ des polynômes en une indéterminée X à coefficients réels est un anneau commutatif unitaire pour l'addition et la multiplication habituelles ; de même nous définirons plus loin l'anneau $A[X]$ lorsque A est un anneau commutatif unitaire quelconque.

1.3.4. *Produits.* Si $(A_i)_{i \in I}$ est une famille quelconque d'anneaux, le produit $\prod_{i \in I} A_i$ a une structure naturelle d'anneau, dont l'addition et la multiplication sont définies "composante par composante". Un cas particulier important est naturellement celui du produit $A \times B$ de deux anneaux A et B. Noter qu'un produit d'anneaux commutatifs (resp. unitaires) a la même propriété.

1.3.5. *Anneaux de fonctions.* Si, dans l'exemple précédent, les anneaux A_i sont égaux à un même anneau A, le produit $\prod_{i \in I} A_i$ est noté A^I et peut être vu comme l'ensemble des *applications* de I dans A, où l'addition et la multiplication sont définies "point par point".

On a souvent à considérer des sous-anneaux (voir plus loin pour la définition) de A^I : par exemple, si I est un espace topologique et $A = \mathbb{R}$, l'ensemble $\mathcal{C}(I, \mathbb{R})$ des applications *continues* de I dans $\mathbb{R}$ est un anneau commutatif unitaire.

1.3.6. Pour tout entier n, $\mathbb{Z}/n\mathbb{Z}$ a une structure naturelle d'anneau donnée par l'addition et la multiplication des classes modulo n ; c'est un cas particulier d'anneau quotient (voir plus loin).

1.3.7. L'ensemble $2\mathbb{Z}$ des entiers pairs fournit un exemple simple d'anneau non unitaire. (Pour le prouver, *il ne suffit pas* de dire que $1 \notin 2\mathbb{Z}$; par exemple, le sous-ensemble $\{0\}$ de $\mathbb{Z}$ ne contient pas 1 mais est bien un anneau unitaire...)

1.3.8. *Anneaux d'endomorphismes.* Si $(G, +)$ est un groupe commutatif, alors l'ensemble $\mathrm{End}(G)$ des endomorphismes de groupe de G a une structure naturelle d'anneau unitaire, obtenue en prenant pour addition l'addition des endomorphismes (déduite de la loi de groupe de G) et pour multiplication la *composition* des endomorphismes. L'anneau obtenu n'est pas commutatif en général ; son élément unité est l'identité Id_G (et non l'endomorphisme trivial, qui est l'élément neutre de l'addition).

De façon analogue, si V est un espace vectoriel sur un corps K, l'ensemble $\mathrm{End}_K(V)$ des K-endomorphismes de V est un anneau unitaire, non commutatif dès que V est de dimension ≥ 2.

Attention : si G est un groupe commutatif noté *multiplicativement*, l'anneau $\mathrm{End}(G)$ existe toujours, même si les notations deviennent problématiques...

Définition 1.4 *Soient A et B deux anneaux. Un (homo)morphisme (d'anneaux) de A dans B est une application $f : A \to B$ qui vérifie, pour tous x et $y \in A$,*

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y). \end{aligned}$$

Si A et B sont tous deux unitaires, un morphisme $f : A \to B$ est dit unitaire *s'il vérifie en outre $f(1_A) = 1_B$.*

1.5. *Remarques et exemples.*

1.5.1. Un morphisme d'anneaux est en particulier un morphisme entre les groupes additifs sous-jacents : il envoie donc 0 sur 0, par exemple.

1.5.2. L'inclusion de $\{0\}$ dans $\mathbb{Z}$ est un exemple de morphisme non unitaire.

Remarquer que pour les morphismes de groupes, par contre, l'élément neutre s'envoie automatiquement sur l'élément neutre : qu'est-ce qui ne marche pas pour la multiplication dans les anneaux ?

1.5.3. *Exercice.* Tout morphisme *surjectif* d'anneaux unitaires est unitaire. Plus précisément, si $f : A \to B$ est un morphisme surjectif d'anneaux et si A est unitaire, alors B est un anneau unitaire et f un morphisme unitaire.

1.5.4. *Exercice.* Pour tout élément a d'un anneau A, notons $\mu_a \in \mathrm{End}(A, +)$ la

multiplication à gauche par a (donnée par $\mu_a(x) = ax$). Montrer que l'application $a \mapsto \mu_a$ est un morphisme d'anneaux de A dans $\mathrm{End}(A, +)$.

Montrer que si A est unitaire, ce morphisme est injectif.

Que se passe-t-il si l'on considère les multiplications à droite ?

1.5.5. Si $\mathbf{0}$ désigne un anneau nul, tout anneau R admet un unique morphisme vers $\mathbf{0}$; ce morphisme est unitaire si R est unitaire.

Il existe aussi un unique morphisme de $\mathbf{0}$ dans R mais, sauf si R est lui-même nul, ce morphisme n'est jamais unitaire et sera donc "illégal" dès le prochain paragraphe.

1.5.6. Pour n entier fixé, l'application canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est un morphisme unitaire.

1.5.7. *Projections.* Si A et B sont deux anneaux, les deux projections $\mathrm{pr}_1 : A \times B \to A$ et $\mathrm{pr}_2 : A \times B \to B$ définies en (I.2.2.8) sont des morphismes surjectifs d'anneaux, unitaires si A et B sont unitaires.

Exercice : énoncer et démontrer l'analogue de la propriété universelle du produit de deux groupes de (I.2.2.9) (ou plutôt les analogues, unitaire et non unitaire).

Ces notions se généralisent immédiatement à un produit arbitraire d'anneaux (1.3.4).

1.5.8. Dans la situation de 1.5.7, on a aussi un morphisme injectif de A dans $A \times B$ donné par $a \mapsto (a, 0_B)$. Si A et B sont unitaires, ce morphisme n'est jamais unitaire sauf si B est nul.

1.5.9. *Morphismes d'évaluation.* Considérons l'anneau $R = A^I$ de 1.3.5. Pour $i \in I$ fixé, la projection de R sur le "i-ème facteur" définie en 1.5.7 est un morphisme d'anneaux qui, lorsque l'on interprète les éléments de R comme des applications de I dans A, n'est autre que "l'évaluation au point i" donnée par $f \mapsto f(i)$.

Cette notion s'étend naturellement aux anneaux tels que $\mathcal{C}(I, \mathbb{R})$ lorsque I est un espace topologique.

Insistons sur la formule $f \mapsto f(i)$: ici, c'est la fonction qui "varie", ce qui semble être une source de perplexité insondable chez beaucoup d'étudiants. Ne pas confondre non plus, dans cette formule, f et le morphisme d'évaluation lui-même ; si l'on note ev_i ce dernier, on a $\mathrm{ev}_i(f) = f(i)$ pour tout f appartenant à l'anneau de fonctions considéré.

1.5.10. *Polynômes et endomorphismes.* Soient K est un corps, V un K-espace vectoriel, et u un K-endomorphisme de V : alors on a une application de $K[X]$ dans $\mathrm{End}\,(V)$ donnée par $P \mapsto P(u)$. Cette application est un morphisme unitaire (voir le cours d'algèbre linéaire de deuxième année). Il s'agit en fait d'une variante de la notion de morphisme d'évaluation présentée ci-dessus.

Définition 1.6 *Soit $f : A \to B$ un morphisme d'anneaux. On dit que f est un* isomorphisme *s'il existe un morphisme d'anneaux $g : B \to A$ tel que $g \circ f = \mathrm{Id}_A$ et $f \circ g = \mathrm{Id}_B$.*

Deux anneaux A et B sont dits isomorphes *s'il existe un isomorphisme de A sur B.*

1.6.1. *Remarque.* On ne formule pas ici de variante "unitaire" : en effet (exercice), si f est un isomorphisme et si A (resp. B) est unitaire, alors B (resp. A) est unitaire et f est un morphisme unitaire.

Comme pour les groupes (cf. I.2.5) on a le critère suivant :

Proposition 1.7 *Soit $f : A \to B$ un morphisme d'anneaux. Pour que f soit un isomorphisme, il faut et il suffit que f soit bijectif.*

Démonstration. Entièrement analogue à celle de I.2.5. ∎

1.7.1. *Exercice.* Soient a et b deux entiers premiers entre eux. Montrer que l'isomorphisme de groupes du "lemme chiois" I.10.4 est un isomorphisme (unitaire) d'anneaux de $\mathbb{Z}/ab\mathbb{Z}$ sur l'anneau produit $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$.

Proposition 1.8 (propriété universelle de l'anneau $\mathbb{Z}$) *Soit A un anneau unitaire. Il existe alors un* unique morphisme unitaire *d'anneaux de $\mathbb{Z}$ dans A ; ce morphisme associe à tout entier k l'élément k_A de A défini par*

$$k_A := k1_A$$

(où le "produit" du membre de droite est celui de l'élément 1_A du groupe $(A, +)$ par l'entier k, au sens de (I.1.3.6)).

Démonstration. Si $\varphi : \mathbb{Z} \to A$ est un morphisme unitaire, alors φ est en particulier un morphisme de groupes (pour l'addition) qui de plus envoie 1 sur 1_A. Il résulte donc de (I.2.3) que φ est bien donné par la formule de l'énoncé. Ceci montre en particulier l'unicité.

Il résulte aussi de (I.2.3) que l'applicaiton φ *définie* par $\varphi(k) = k1_A$ est un morphisme de groupes envoyant 1 sur 1_A. Il reste à voir que, pour tous k et l dans $\mathbb{Z}$, on a $(k1_A)(l1_A) = (kl)1_A$: pour le voir on peut supposer que $k \geq 0$ (utiliser la formule $(-x)y = -(xy)$ de 1.2.3), et procéder ensuite par récurrence sur k. (Bien entendu, ces arguments utilisent de façon répétée la définition de $k1_A$; il faut donc la connaître...) ∎

1.8.1. *Exercice.* Montrer qu'il n'existe *aucun* morphisme unitaire de $\mathbb{Q}$ (resp. $\mathbb{R}$, resp. $\mathbb{C}$) dans $\mathbb{Z}$.

Définition 1.9 *Un* sous-anneau *d'un anneau A est une partie de A stable par addition et multiplication, et qui est un anneau pour l'addition et la multiplication induites.*

Si A est unitaire, un sous-anneau unitaire *de A est un sous-anneau de A contenant l'élément 1_A.*

1.10. *Remarques.*

1.10.1. De façon équivalente, on aurait pu définir un sous-anneau de A comme un sous-groupe de $(A, +)$ stable par multiplication.

1.10.2. Si B est un sous-anneau unitaire de A, alors B est évidemment un sous-anneau de A et un anneau unitaire ; la réciproque est fausse comme le montre l'exemple $A = \mathbb{Z}$, $B = \{0\}$.

1.10.3. L'intersection d'une famille quelconque de sous-anneaux (resp. de sous-anneaux unitaires) d'un anneau (resp. d'un anneau unitaire) A est un sous-anneau (resp. un sous-anneau unitaire) de A.

En particulier (nous nous limitons pour simplifier au cas unitaire), si S est une partie de A, l'intersection $\langle\langle S\rangle\rangle$ des sous-anneaux unitaires de A contenant S est le plus petit sous-anneau unitaire de A contenant S (même démonstration que pour I.4.2). On l'appelle le sous-anneau unitaire de A *engendré par* S.

1.10.4. *Exercice.* Avec les notations ci-dessus, montrer que $\langle\langle S\rangle\rangle$ est le sous-groupe de $(A, +)$ engendré par l'ensemble des produits finis d'éléments de S. (On n'exclut évidemment pas le produit vide).

1.10.5. *Exercice.* On suppose de plus que $S = \{s_1, \ldots, s_n\}$ est fini, et que les s_i commutent entre eux (par exemple, que A est commutatif, ou que $n = 1$). Alors $\langle\langle S\rangle\rangle$ est le sous-groupe de $(A, +)$ engendré par l'ensemble des "monômes" de la forme $s_1^{m_1} \cdots s_n^{m_n}$ avec $(m_1, \ldots, m_n) \in \mathbb{N}^n$.

Lorsque $S = \{s\}$ a un seul élément, on voit donc que $\langle\langle S\rangle\rangle$ est l'ensemble des éléments de A de la forme $P(s)$ où P est un polynôme à coefficients entiers (voir le chapitre IV).

1.10.6. *Exercice.* Quel est le sous-anneau unitaire de $\mathbb{R}$ engendré par $1/2$ (c'est-à-dire par $\{1/2\}$) ? par $1/10$? par l'ensemble des inverses des nombres premiers ? par $\sqrt{2}$?

1.10.7. *Exercice.* On voit notamment que si A est unitaire, il existe un *plus petit sous-anneau unitaire* de A (prendre $S = \emptyset$, ou $S = \{0\}$). Montrer que ce sous-anneau est l'image du morphisme de $\mathbb{Z}$ dans A de 1.8, et est le sous-groupe de $(A, +)$ engendré par 1_A.

1.10.8. On laisse au lecteur le soin de formuler et d'établir les propriétés telles que :

"l'image d'un sous-anneau par un morphisme est un sous-anneau" et toutes ses variantes (images réciproques, morphismes et sous-anneaux unitaires).

1.11. *Règles de calcul dans un anneau.* Dans ce qui suit, A désigne un anneau, que l'on supposera *unitaire* pour simplifier.

1.11.1. Les règles de calcul dans les groupes commutatifs s'appliquent évidemment au groupe additif $(A, +)$.

1.11.2. L'associativité de la multiplication permet de manipuler les produits finis comme en (I.1.3.5) (sauf pour ce qui concerne les inverses). On dispose notamment de la règle de regroupement de termes consécutifs ; les regroupements arbitraires sont licites si A est commutatif.

On peut également définir les puissances entières d'un élément, à condition que l'exposant soit ≥ 0. On convient *toujours* que $x^0 = 1_A$ (même si $x = 0_A$) et l'on a les mêmes règles de calcul qu'en (I.1.3.6), limitées aux exposants entiers naturels.

1.11.3. La distributivité permet de "développer les produits", ainsi $(a+b)(c+d) = ac+ad+bc+bd$. Attention à l'ordre des facteurs : ainsi, $(a+b)^2 = a^2+ab+ba+b^2$, qui n'est égal à $a^2 + 2ab + b^2$ que si $ab = ba$.

1.11.4. *Formule du binôme.* Soient a et b deux éléments de A *qui commutent*, i.e. tels que $ab = ba$, et soit $n \in \mathbb{N}$. Alors on a

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i \, b^{n-i}$$

où $\binom{n}{i} = C_n^i$ désigne le "coefficient du binôme" $n!/(i!(n-i)!)$. La démonstration se fait par récurrence sur n. L'exemple précédent (pour $n = 2$) montre la nécessité de l'hypothèse $ab = ba$.

1.11.5. Sous les mêmes hypothèses que ci-dessus, on a aussi l'identité

$$a^n - b^n = (a-b) \sum_{i=0}^{n-1} a^i \, b^{n-1-i}.$$

1.11.6. Les deux formules qui précèdent s'appliquent notamment si a ou b est égal à 1 (qui commute avec tout élément de A). On obtient donc les relations, valables pour tout $x \in A$ et tout $n \in \mathbb{N}$:

$$\begin{aligned} (1+x)^n &= \textstyle\sum_{i=0}^{n} \binom{n}{i} x^i \\ 1 - x^n &= (1-x) \textstyle\sum_{i=0}^{n-1} x^i. \end{aligned}$$

1.12. Convention. Dans toute la suite de ce cours, et sauf mention expresse du contraire, tous les anneaux seront supposés commutatifs et unitaires, et tous les morphismes et sous-anneaux seront unitaires.

2. Diviseurs de zéro, anneaux intègres

Définition 2.1 *Soit A un anneau, et soit a un élément de A. On dit que a est régulier dans A (ou encore* non diviseur de zéro *dans A) si la multiplication par a dans A est injective ; autrement dit (puisque c'est un morphisme de groupes additifs) si, pour tout $x \in A$, $ax = 0$ implique $x = 0$.*

On dit que a est diviseur de zéro *dans A s'il n'est pas régulier (autrement dit, s'il existe $x \in A$* non nul *tel que $ax = 0$.*

2.2. *Remarques.*

2.2.1. *Notation.* Dans ce cours on notera A^* l'ensemble des éléments réguliers de A. Cette notation sera surtout utilisée lorsque A est intègre (voir 2.3 ci-dessous), auquel cas A^* coïncide avec $A - \{0\}$.

2.2.2. 0 est diviseur de zéro dans A, sauf si $A = \{0\}$. Par contre 1 n'est jamais diviseur de zéro.

2.2.3. Dans $\mathbb{Z}$, le seul diviseur de zéro est 0. Même chose dans $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$.

2.2.4. Dans $\mathbb{Z}/4\mathbb{Z}$ l'élément $a = 2 \bmod 4$ est un diviseur de zéro non nul (on a même $a^2 = 0$).

2.2.5. *Exercice.* Dans $\mathcal{C}(\mathbb{R}, \mathbb{R})$ montrer que les diviseurs de zéro sont les fonctions $f : \mathbb{R} \to \mathbb{R}$ qui s'annulent sur un intervalle ouvert non vide (i.e. telles que $f^{-1}(0)$ soit d'intérieur non vide).

2.2.6. Pour $a \in A$ donné, il revient au même de dire que a est régulier ou que l'on peut simplifier par a dans A (si $ax = ay$ alors $x = y$).

2.2.7. *Exercice.* Pour qu'un produit ab soit régulier il faut et il suffit que a et b le soient. En particulier, A^* est stable par multiplication.

Définition 2.3 *Un anneau A est dit* intègre *s'il vérifie les deux conditions suivantes :*

(i) $A \neq \{0_A\}$ *;*

(ii) *tout élément non nul de A est régulier.*

2.4. *Remarques.*

2.4.1. Ne pas oublier la condition (i) de la définition.

2.4.2. La condition (ii) peut se reformuler comme une règle de calcul dans A : *on*

peut simplifier par tout élément non nul, autrement dit si $ac = bc$ et $c \neq 0$, alors $a = b$. Ou encore : si $ab = 0$ alors $a = 0$ ou $b = 0$.

2.4.3. *Exercice.* Soit A un anneau. Montrer les équivalences :
A est intègre $\iff$ l'ensemble des diviseurs de zéro de A est $\{0\}$ $\iff$ A contient un diviseur de zéro et un seul.

2.4.4. Même dans le monde non commutatif, c'est-à-dire dans les ouvrages qui n'adoptent pas la convention 1.12, un anneau intègre est commutatif et unitaire par définition.

2.4.5. Il est immédiat (avec la convention 1.12) que tout sous-anneau d'un anneau intègre est intègre.

2.4.6. *Exemples d'anneaux intègres :* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$. La plupart des autres anneaux donnés en exemple plus haut dans ce chapitre ne sont pas intègres. Pas tous, cependant (cherchez un peu).

2.4.7. *Exercice.* À quelle(s) condition(s) un produit $\prod_{i\in I} A_i$ d'anneaux est-il intègre ?

2.4.8. *Exercice.* Soit U un ouvert de $\mathbb{C}$, et soit A l'anneau des fonctions à valeurs complexes *holomorphes* sur U. Montrer que A est intègre si et seulement si U est connexe et non vide.

3. Éléments inversibles, corps

Définition 3.1 *Soit A un anneau, et soit a un élément de A. On dit que a est* inversible *dans A s'il vérifie les conditions équivalentes suivantes :*

(i) *a admet un symétrique pour la multiplication : il existe $b \in A$ tel que $ab = 1$;*

(ii) *la multiplication par a dans A est bijective ;*

(iii) *la multiplication par a dans A est surjective.*

3.2. *Remarques.*

3.2.1. L'équivalence des conditions de la définition est laissée comme exercice.

3.2.2. *Notations.* Si a est inversible, l'élément b de (i) est unique et appelé *l'inverse* de a ; on le note a^{-1}.

On note $A^\times$ l'ensemble des éléments inversibles de A ; noter que c'est un *groupe* pour la multiplication.

3.2.3. *Exemples.* $\mathbb{Z}^\times = \{-1, +1\}$; $\mathbb{R}^\times = \mathbb{R}^* = \mathbb{R} - \{0\}$; $\mathcal{C}(\mathbb{R}, \mathbb{R})^\times$ est l'ensemble des applications *partout non nulles* de $\mathbb{R}$ dans $\mathbb{R}$; $\mathbb{R}[X]^\times$ est l'ensemble des polynômes constants non nuls ; pour que $A^\times = A$ il faut et il suffit que $A = \{0\}$, ou encore que $0 \in A^\times$.

3.2.4. Tout élément inversible est régulier ; la réciproque est fausse comme le montrent plusieurs des exemples précédents : lesquels ?

3.2.5. *Exercice.* Soit A un anneau *fini* : alors tout élément régulier de A est inversible autrement dit, $A^* = A^\times$). (Considérer la multiplication par a).

3.2.6. *Exercice.* Pour qu'un produit ab soit inversible il faut et il suffit que a et b le soient.

3.2.7. *Exercice.* Un élément x d'un anneau A est dit *nilpotent* s'il existe un entier $k > 0$ tel que $x^k = 0$. Montrer que si x est nilpotent, alors $1 + x$ est inversible, et donner une formule pour $(1 + x)^{-1}$. (Indication : utiliser 1.11.6).

Plus généralement si u est inversible et x nilpotent, alors $u + x$ est inversible.

3.2.8. *Exercice.* Si $f : A \to B$ est un morphisme d'anneaux, et si $x \in A$ est inversible, alors $f(x)$ est inversible dans B. En d'autres termes, $f(A^\times) \subset B^\times$. (Noter que la propriété analogue pour les éléments réguliers est fausse).

3.2.9. *Exercice.* Peut-on trouver un anneau A non nul tel que $A^\times = \{1\}$?

Proposition 3.3 *Soient a et n deux entiers, avec $n \neq 0$. Posons $\alpha = a \bmod n \in \mathbb{Z}/n\mathbb{Z}$. Les conditions suivantes sont équivalentes :*

(i) *α est inversible dans $\mathbb{Z}/n\mathbb{Z}$;*

(ii) *α est régulier dans $\mathbb{Z}/n\mathbb{Z}$;*

(iii) *a et n sont premiers entre eux.*

Démonstration. On sait déjà que (i) implique (ii), et l'on a même la réciproque par 3.2.5. Il reste à voir que (i)⇔(iii). Pour que α soit inversible dans $\mathbb{Z}/n\mathbb{Z}$, il faut et il suffit qu'il existe un entier u tel que $au \equiv 1 \pmod{n}$, ou encore, qu'il existe des entiers u et v tels que $au + nv = 1$, ce qui équivaut bien à (iii). ∎

3.3.1. *Remarque.* Sans utiliser 3.2.5, on peut montrer que (ii) implique (iii) de façon plus terre-à-terre : si n et a ne sont pas premiers entre eux, il existe un entier $d > 1$ qui divise a et n. On a donc une relation $n = dn'$ où $0 < n' < |n|$, de sorte que $n' \not\equiv 0 \pmod{n}$, ce qui implique que $d \bmod n$ est diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$. Comme $\alpha = a \bmod n$ est un multiple de $d \bmod n$ dans $\mathbb{Z}/n\mathbb{Z}$, on conclut par 2.2.7 que α est aussi diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

3.3.2. *Exercice.* Pour chaque entier $n \leq 10$, faire la liste des inversibles de $\mathbb{Z}/n\mathbb{Z}$ et calculer leurs inverses.

3.3.3. *Remarque.* Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$, est appelé *l'indicateur d'Euler* de n et souvent noté $\varphi(n)$.

3.3.4. *Exercice.* Soient p un nombre premier, et n un entier > 0. Déduire de 3.3 que, avec la notation de 3.3.3, $\varphi(p^n) = p^n - p^{n-1}$.

3.3.5. *Exercice.* Soient a et b deux entiers naturels premiers entre eux. Déduire de 1.7.1 que le groupe $(\mathbb{Z}/ab\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. En déduire que $\varphi(ab) = \varphi(a)\varphi(b)$.

3.3.6. *Exercice.* Déduire de 3.3.4 et 3.3.5 la formule générale suivante : pour n entier > 0, si $p_1, \ldots, p_r$ sont les diviseurs premiers (distincts) de n, on a $\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$.

Définition 3.4 *Soit A un anneau commutatif unitaire. On dit que A est un* corps *s'il vérifie les deux conditions suivantes :*

(i) *$A \neq \{0_A\}$;*

(ii) *tout élément non nul de A est inversible.*

3.5. *Remarques.* (On comparera avec le cas des anneaux intègres.)

3.5.1. Ne pas oublier la condition (i) de la définition.

3.5.2. La condition (ii) peut se reformuler comme une règle de calcul dans A : *on peut diviser par tout élément non nul.* Autrement dit il existe une loi de composition "division" : $A \times (A - \{0\}) \to A$, notée souvent $(x, y) \mapsto x/y$, définie par $xy = xy^{-1}$ et ayant les propriétés habituelles.

3.5.3. *Exercice.* Soit A un anneau. Montrer les équivalences :

A est un corps $\iff A^\times = A - \{0\} \iff A - \{0\}$ est un groupe pour la multiplication.

3.5.4. Pour la commutativité, l'usage diffère de celui des anneaux intègres : un corps n'est pas nécessairement commutatif (sauf avec nos conventions, évidemment). Noter toutefois qu'en anglais le mot "field" désigne uniquement un corps commutatif.

3.5.5. Un sous-anneau d'un corps n'a aucune raison d'être un corps (cette remarque figure ici uniquement en raison du parallèle avec 2.4).

3.5.6. *Exemples de corps :* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, et aussi $\mathbb{Z}/p\mathbb{Z}$ pour p *premier* (voir ci-dessous).

3.5.7. *Exercice.* À quelle(s) condition(s) un produit $\prod_{i\in I} A_i$ d'anneaux est-il un corps ?

3.5.8. *Exercice.* Déduire de 3.2.5 que *tout anneau intègre fini est un corps.*

Proposition 3.6 *Soit n un entier > 0. Les conditions suivantes sont équivalentes :*

(i) *$\mathbb{Z}/n\mathbb{Z}$ est un corps ;*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ est intègre ;*

(iii) *n est premier.*

Démonstration. Si $n = 1$ alors les trois propriétés sont fausses : (i) et (ii) parce que $\mathbb{Z}/n\mathbb{Z}$ est nul, et (iii) parce qu'un nombre premier est *par définition* > 1. On supposera donc dans la suite que $n > 1$, et donc que $\mathbb{Z}/n\mathbb{Z} \neq \{0\}$.

L'implication (i) $\Rightarrow$ (ii) est triviale, et la réciproque résulte de 3.3 (ou de 3.5.8). Pour montrer que ces conditions sont équivalentes à (iii), on utilise encore 3.3 qui donne l'équivalence (puisque l'on suppose déjà que $\mathbb{Z}/n\mathbb{Z} \neq \{0\}$) :

$\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ tout entier non divisible par n est premier avec n.

Or la deuxième condition (jointe à l'hypothèse $n > 1$) caractérise bien les nombres premiers. ∎

3.6.1. *Remarque.* On prendra garde qu'il existe d'autres corps finis que ceux de la forme $\mathbb{Z}/p\mathbb{Z}$, pour p premier. Voir par exemple 5.9 et IV.8.9.4.

3.6.2. *Remarque.* L'énoncé serait en défaut pour $n = 0$: dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ donc est intègre, mais n'est pas un corps.

Une conséquence importante de 3.6 est la suivante :

Corollaire 3.6.3 *Soit p un nombre premier. Alors $\mathbb{Z}/p\mathbb{Z} - \{0\}$ est un groupe pour la multiplication.* ∎

3.6.4. *Remarque.* Bien entendu, ce groupe est commutatif d'ordre $p-1$. Autrement, dit, avec la notation de 3.3.3, on a $\varphi(p) = p - 1$ pour p premier.

Nous verrons plus loin (IV.6.3) que ce groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est *cyclique.*

3.6.5. *Exercice.* Pour chaque p premier ≤ 13, montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Voici trois applications arithmétiques de 3.6 :

Corollaire 3.7 ("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 $(\mathbb{Z}/p\mathbb{Z})^\times$ 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 (I.6.6). ∎

Corollaire 3.8 ("théorème de Wilson") *Soit p un nombre premier. Alors :*

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

Pour établir 3.8, montrons d'abord un lemme :

Lemme 3.8.1 *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. ∎

3.8.2. *Exercice.* Où a servi l'hypothèse que G est commutatif ?

3.8.3. *Démonstration de* 3.8. Appliquons le lemme 3.8.1 au groupe $(\mathbb{Z}/p\mathbb{Z})^\times$. Le produit de ses éléments est la classe modulo p de $(p-1)!$ puisque $(\mathbb{Z}/p\mathbb{Z})^\times$ 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 intègre. 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 ?) ∎

3.8.4. *Exercice.* Que se passe-t-il dans 3.8 si p n'est plus supposé premier ?

Corollaire 3.9 *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 $(\mathbb{Z}/p\mathbb{Z})^\times$. 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 $(\mathbb{Z}/p\mathbb{Z})^\times$. Donc le produit $N \times (-1)^{\frac{p-1}{2}} N$ a même classe modulo p que $(p-1)!$, d'où, d'après 3.8, $(-1)^{\frac{p-1}{2}} N^2 \equiv -1 \pmod p$. 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. ∎

Proposition 3.10 *Soit K un corps. Tout morphisme d'anneaux de K vers un anneau non nul est injectif.*

Démonstration. Soit $f : K \to A$ un morphisme d'anneaux. Si f n'est pas injectif, il existe $x \in K$ non nul (et donc inversible) tel que $f(x) = 0_A$. Donc, d'après 3.2.8, 0_A est inversible dans A, d'où $A = \{0_A\}$. ∎

3.11. *Sous-corps.* Un *sous-corps* d'un corps K est par définition un sous-anneau de K qui est un corps.

3.11.1. *Intersections, sous-corps premier.* Il est clair que l'intersection d'une famille quelconque de sous-corps de K est encore un sous-corps de K. En particulier, K admet un *plus petit sous-corps* qui est l'intersection de tous ses sous-corps. On l'appelle le *sous-corps premier* de K.

Un *corps premier* est par définition un corps égal à son sous-corps premier, c'est-à-dire un corps qui n'a pas d'autre sous-corps que lui-même.

3.11.2. *Exercice.* Soient K un corps, A un anneau, f et g deux morphismes de K dans A. Montrer que $\{x \in K \mid f(x) = g(x)\}$ est un sous-corps de K.

En déduire que si K est un corps premier et A un anneau, il existe *au plus un* morphisme de K dans A.

3.11.3. *Exercice.* Montrer que $\mathbb{Q}$ et $\mathbb{Z}/p\mathbb{Z}$ (où p est un nombre premier) sont des corps premiers. (Nous verrons plus loin que ce sont les seuls, à isomorphisme près).

3.11.4. *Exercice.* Montrer que le seul morphisme de $\mathbb{Q}$ dans $\mathbb{R}$ est l'inclusion, et que le seul morphisme de $\mathbb{Q}$ dans $\mathbb{Q}$ est l'identité. On donnera deux démonstrations : l'une "directe", et l'autre utilisant 3.11.3 et 3.11.2.

3.12. *Exercice.* Soit $f : \mathbb{R} \to \mathbb{R}$ un endomorphisme d'anneau. On se propose de montrer que f est l'identité.

3.12.1. Montrer que $f(x) = x$ pour tout $x \in \mathbb{Q}$.

3.12.2. Montrer que pour tout réel $x \geq 0$ on a $f(x) \geq 0$. (Indication : à quoi reconnaît-on un réel ≥ 0 ?)

3.12.3. Déduire de 3.12.2 que f est croissant, et conclure à l'aide de 3.12.1.

3.13. *Exercice.* Soit $f : \mathbb{C} \to \mathbb{C}$ un endomorphisme d'anneau. Montrer que les conditions suivantes sont équivalentes :

(i) f est égal à l'identité ou à la conjugaison complexe ;

(ii) f est continu (pour la topologie naturelle de $\mathbb{C}$) ;

(iii) $f(\mathbb{R}) \subset \mathbb{R}$;

(iv) $\forall x \in \mathbb{R}, f(x) = x$.

(Utiliser les exercices précédents).

3.13.1. *Remarque.* On peut montrer que $\mathbb{C}$ admet des endomorphismes non surjectifs, et des automorphismes non continus.

3.14. *Exercice : sous-corps engendré par une partie d'un corps.* Soit S une partie d'un corps K. Montrer que l'intersection de tous les sous-corps de K contenant S est aussi le plus petit sous-corps de K contenant S. On l'appelle le *sous-corps de K engendré par S*.

Montrer que le sous-corps de K engendré par S est égal à l'ensemble des quotients a/b où $b \neq 0$ et où a et b appartiennent au sous-anneau unitaire $\langle\langle S \rangle\rangle$ de K engendré par S (notation de 1.10.3).

Quel est le sous-corps de $\mathbb{R}$ engendré par $\sqrt{2}$? Comparer ce sous-corps (au sens de l'inclusion, ou de l'égalité) avec : le sous-groupe de $(\mathbb{R}, +)$ engendré par $\sqrt{2}$; le sous-groupe de $(\mathbb{R}^*, \times)$ engendré par $\sqrt{2}$; le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{2}$.

4. Idéaux

Définition 4.1 *Soit A un anneau* (commutatif et unitaire, comme toujours). *Un* idéal *de A est par définition un sous-groupe I de $(A,+)$ tel que $AI \subset I$ (autrement dit, tel que pour tout $a \in A$ et tout $\lambda \in I$, on ait $a\lambda \in I$).*

4.1.1. *Exemples triviaux.* $\{0\}$ et A sont des idéaux de A.

4.1.2. L'intersection d'une famille quelconque d'idéaux est encore un idéal.

4.1.3. Si $f : A \to B$ est un morphisme d'anneaux, et si J est un idéal de B, alors $f^{-1}(J)$ est un idéal de A. *En particulier,* Ker (f) *est un idéal de A.*

Par contre, si I est un idéal de A, il n'est pas vrai en général que $f(I)$ soit un idéal de B (exemple : $f =$ l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$ et $I = \mathbb{Z}$). Cette propriété est toutefois vraie si f est *surjectif* (exercice).

4.1.4. *Idéaux principaux.* Si a est un élément d'un anneau A, l'ensemble des multiples de a dans A, c'est-à-dire des éléments de la forme λa avec $\lambda \in A$, est un idéal de A noté tout naturellement aA mais aussi (a). C'est le plus petit idéal de A contenant a (exercice).

Un idéal de la forme (a) est dit *principal.*

Par exemple, *tout idéal de $\mathbb{Z}$ est principal* : ceci résulte de (I.3.6) et du fait qu'un idéal est en particulier un sous-groupe.

4.1.5. *Exercice.* Fixons $x_0 \in \mathbb{R}$. Soit $A = \mathcal{C}(\mathbb{R},\mathbb{R})$ et soit $I = \{f \in A \mid f(x_0) = 0\}$. Alors I est un idéal de A (c'est même le noyau d'un morphisme d'anneaux de A dans $\mathbb{R}$), et n'est pas principal (ce n'est pas tout à fait immédiat).

4.1.6. *Exercice.* Définissons cette fois I comme ci-dessus, mais dans l'anneau $A = \mathbb{R}[X]$ (resp. $A = C^\infty(\mathbb{R},\mathbb{R})$, resp. $A = \mathbb{R}^{\mathbb{R}}$). Dire dans chaque cas si I est principal.

4.1.7. *Exercice.* Montrer que l'ensemble des éléments *nilpotents* (3.2.7) d'un anneau A est un idéal de A (utiliser la formule du binôme).

4.2. *Idéaux et éléments inversibles.*

4.2.1. Un élément a d'un anneau A est inversible si et seulement si $(a) = A$: ceci n'est autre que la condition (iii) de 3.1. En conséquence, *tout idéal de A contenant un inversible est égal à A.*

4.2.2. *Idéaux d'un corps.* Il résulte de 4.2.1 ci-dessus que *si K est un corps, les seuls idéaux de K sont* $\{0\}$ *et* K puisque tout idéal non nul contient un inversible.

4.2.3. *Exercice.* Montrer la réciproque : si A est un anneau *non nul* ayant $\{0\}$ et A pour seuls idéaux, alors A est un corps.

On peut donc caractériser les corps comme les anneaux ayant *exactement deux idéaux* (remarque probablement sans aucun intérêt).

4.2.4. *Exercice.* Déduire de 4.2.2 une "autre" démonstration de 3.10. Ensuite, expliquer les guillemets.

Comme la notion de sous-groupe engendré par un élément, la notion d'idéal engendré par un élément se généralise :

Définition 4.3 *Soit S une partie d'un anneau A. L'idéal* engendré *par S (noté (S)) est par définition l'intersection de tous les idéaux de A contenant S.*

Les énoncés qui suivent sont entièrement analogues à (I.4.2) et (I.4.4) ; il en est de même de leurs démonstrations, que nous omettons, pour ne pas priver le lecteur du plaisir de tester sa compréhension des résultats du paragraphe I.4 en les faisant lui-même.

Proposition 4.4 *Avec les notations de la définition* 4.3, *(S) est le* plus petit *idéal de A contenant S.* ∎

Proposition 4.5 *Avec les notations de la définition* 4.3, *un élément x de A appartient à (S) si et seulement si x peut s'écrire comme combinaison linéaire à coefficients dans A d'un nombre fini d'éléments de S ; autrement dit, si x peut s'écrire*

$$x = \sum_{i=1}^{m} \lambda_i s_i$$

avec m dans $\mathbb{N}$, les s_i dans S et les λ_i dans A. ∎

5. Anneaux quotients

5.1. *Notation.* Si A est un anneau, I un sous-groupe de $(A,+)$, et a et b deux éléments de A, nous noterons

$$a \equiv b \pmod{I}$$

pour "$a-b \in I$". (À l'exception de l'énoncé qui suit, nous n'utiliserons cette notation que lorsque I est un idéal).

Proposition 5.2 (et définition) *Soient A un anneau, I un sous-groupe de $(A,+)$, $\pi : A \to A/I$ le morphisme de groupes canonique. Les conditions suivantes sont équivalentes :*

(i) *I est un idéal de A ;*

(ii) *la relation d'équivalence "$a \equiv b \pmod{I}$" sur A est compatible avec la multiplication : si $a \equiv a' \pmod{I}$ et $b \equiv b' \pmod{I}$, alors $ab \equiv a'b' \pmod{I}$.*

(iii) *il existe sur A/I une structure d'anneau (commutatif unitaire) faisant de π un morphisme d'anneaux.*

Si ces conditions sont vérifiées, la structure d'anneau de (iii) *est unique, et A/I muni de cette structure est appelé* l'anneau quotient *de A par I.*

Démonstration. Il est trivial que (iii) implique (i) puisque I est le noyau de π, et que le noyau d'un morphisme d'anneaux est un idéal.

Montrons que (i) implique (ii). Supposons donc que I est un idéal de A, et soient $a, a', b, b' \in A$ vérifiant $a \equiv a' \pmod{I}$ et $b \equiv b' \pmod{I}$. Il existe donc λ et μ dans I tels que $a' = a + \lambda$ et $b' = b + \mu$; multipliant membre à membre, on obtient $a'b' = ab + a\mu + b\lambda + \lambda\mu$. Du fait que I est un idéal contenant λ et μ on déduit que $a\mu + b\lambda + \lambda\mu \in I$, d'où $a'b' \equiv ab \pmod{I}$, cqfd.

Montrons que (ii) implique (iii). Si (ii) est vérifiée, on peut définir une "multiplication" dans A/I vérifiant $\pi(ab) = \pi(a)\pi(b)$ pour tous $a, b \in A$ (l'argument est le même que dans (I.8.4)). Le fait que A/I soit alors un anneau se déduit formellement du fait que π est surjectif et respecte addition et multiplication. ∎

Corollaire 5.3 *Soit I une partie d'un anneau A. Les conditions suivantes sont équivalentes :*

(i) *I est un idéal de A ;*

(ii) *il existe un anneau A' et un morphisme surjectif $f : A \to A'$ tels que $I =$* Ker (f) *;*

(iii) *il existe un anneau A' et un morphisme $f : A \to A'$ tels que $I = \mathrm{Ker}\,(f)$.*

■

Théorème 5.4 ("propriété universelle de l'anneau quotient"). *Soit I un idéal d'un anneau A, et soit $\pi : A \to A/I$ le morphisme canonique. D'autre part soit $f : A \to B$ un morphisme d'anneaux. Les conditions suivantes sont équivalentes :*

(i) *f se factorise par A/I; i.e. il existe un morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$;*

(ii) *$f(I) = \{0_B\}$;*

(iii) *$I \subset \mathrm{Ker}\, f$.*

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

Démonstration. Comme dans le cas des groupes quotients (I.8.6), l'équivalence de (ii) et (iii) résulte de la définition du noyau, et l'implication (i)⇒(ii) est triviale. 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.

On peut noter de toute façon que si $\overline{f}$ existe, c'est le morphisme de groupes construit en (I.8.6) de sorte que l'assertion finale sur le noyau de $\overline{f}$ résulte de loc. cit.

Supposons maintenant (ii) vérifiée, et montrons (i). Appliquant (I.8.6) on voit qu'il existe en tout cas un morphisme *de groupes additifs* $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$, et la seule chose à vérifier est que c'est un morphisme d'anneaux ; mais ceci se déduit formellement des propriétés suivantes : (a) $f = \overline{f} \circ \pi$; (b) f est un morphisme ; (c) π est un morphisme surjectif. ■

Théorème 5.5 *Soit $f : A \to B$ un morphisme d'anneaux. Alors on a un isomorphisme naturel d'anneaux*

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

caractérisé par la propriété suivante : pour tout $a \in A$, on a

$$\varphi(a + \mathrm{Ker}\, f) = f(a).$$

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

Démonstration. On peut répéter, mutatis mutandis, la preuve de (I.8.8) en utilisant 5.4 au lieu de (I.8.6).

On peut aussi utiliser (I.8.8) qui implique l'existence d'un morphisme φ *de groupes* ayant la propriété voulue. Le fait que φ respecte la multiplication (et les

unités) est une conséquence immédiate de la formule de l'énoncé et du fait que f est un morphisme d'anneaux. ∎

Les énoncés du §I.9 ont des analogues pour les anneaux quotients ; contentons-nous d'énoncer un analogue de (I.9.3) :

Proposition 5.6 *Soit $\pi : A \to B$ un morphisme* surjectif *d'anneaux, et soit $I =$ Ker π. Les applications*

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

sont des bijections réciproques l'une de l'autre entre l'ensemble des idéaux de B et l'ensemble des idéaux de A contenant J. Ces bijections respectent les inclusions et les intersections.

De plus, si $J \subset A$ et $K \subset B$ se correspondent par ces bijections, on a un isomorphisme canonique d'anneaux

$$A/J \xrightarrow{\sim} B/K.$$

Démonstration : exercice. ∎

5.7. *Application : construction de* $\mathbb{C}$. Montrons comment la notion d'anneau quotient permet de donner un définition très simple du corps des complexes, à partir du corps des réels.

5.7.1. Supposons d'abord qu'il existe bien un corps $\mathbb{C}$ ayant les propriétés habituelles. On a alors un morphisme naturel d'anneaux $\varepsilon : \mathbb{R}[X] \to \mathbb{C}$ ("évaluation au point i") qui associe à tout polynôme $P \in \mathbb{R}[X]$ le nombre complexe $\varepsilon(P) := P(i)$. Ce morphisme est surjectif (le nombre complexe $a + ib$, pour a et b réels, est égal à $\varepsilon(a+bX)$) et son noyau est l'idéal des polynômes ayant i pour racine, qui est engendré (exercice) par $X^2 + 1$. On déduit donc de 5.5 un isomorphisme $\mathbb{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{C}$, envoyant la classe de $P \in \mathbb{R}[X]$ sur $P(i)$.

5.7.2. Ce qui précède suggère de poser, *par définition*,

$$\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$$

et de vérifier ensuite les propriétés usuelles de $\mathbb{C}$, à savoir (on laisse les détails au lecteur) :

(i) $\mathbb{C}$ contient une copie de $\mathbb{R}$ (c'est-à-dire un sous-anneau isomorphe à $\mathbb{R}$) ; en d'autres termes il existe un morphisme injectif de $\mathbb{R}$ dans $\mathbb{C}$, grâce auquel on identifie $\mathbb{R}$ à un sous-anneau de $\mathbb{C}$. Ce morphisme est naturellement le composé de l'inclusion de $\mathbb{R}$ dans $\mathbb{R}[X]$ et de la surjection canonique de $\mathbb{R}[X]$ sur $\mathbb{C}$;

(ii) si l'on désigne par $i \in \mathbb{C}$ la classe du polynôme X, alors $i^2 = -1$ dans $\mathbb{C}$: en effet $i^2 + 1$ est la classe de $X^2 + 1$, c'est-à-dire 0 ;

(iii) $\{1, i\}$ est une base de $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel : en effet $\mathbb{C}$ est engendré comme $\mathbb{R}$-espace vectoriel par les puissances de i (ceci résulte de sa définition comme quotient de $\mathbb{R}[X]$, et du fait que les puissances de X engendrent $\mathbb{R}[X]$) ; la relation $i^2 = -1$ permet d'en déduire que $\mathbb{C}$ est engendré par $\{1, i\}$, et enfin 1 et i sont linéairement indépendants sur $\mathbb{R}$, car une relation $\lambda + i\mu = 0$ ($\lambda, \mu \in \mathbb{R}$) implique que $\lambda + X\mu$ est divisible par $X^2 + 1$, ce qui n'est possible que si $\lambda = \mu = 0$;

(iv) $\mathbb{C}$ est un corps : ceci résulte aisément de la formule $(a + ib)(a - ib) = a^2 + b^2$, conséquence formelle de $i^2 = -1$.

5.7.3. *Remarque.* La construction de $\mathbb{C}$ présentée ci-dessus relève de la "méthode d'adjonction de racines" qui sera généralisée plus loin (IV.7).

5.8. *Application : construction de* $\mathbb{R}$. Nous allons montrer maintenant (brièvement) comment le corps $\mathbb{R}$ lui-même peut être construit à partir de $\mathbb{Q}$ et de notions élémentaires d'analyse.

Considérons, dans l'anneau $\mathbb{Q}^{\mathbb{N}}$ des suites $(u_n)_{n\in\mathbb{N}}$ de rationnels, le sous-ensemble A des suites *de Cauchy* : on vérifie immédiatement que c'est un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$. (Noter que la notion de suite de Cauchy fait classiquement intervenir des "ε" réels : il est cependant aisé de vérifier que cette notion ne change pas si l'on se limite aux ε rationnels, ou même de la forme $1/n$ pour n entier).

L'ensemble des suites de rationnels *tendant vers* 0 est de plus un *idéal* de A : ceci résulte du fait que toute suite de Cauchy est bornée. Cet idéal sera noté J dans la suite.

5.8.1. Supposons construit le corps $\mathbb{R}$: on a alors une application $\ell : A \to \mathbb{R}$ qui à toute suite de Cauchy $(u_n)_{n\in\mathbb{N}}$ de rationnels associe sa limite dans $\mathbb{R}$. Les théorèmes classiques sur les limites montrent que ℓ est un morphisme d'anneaux. De plus ℓ est surjectif puisque tout réel est limite d'une suite de rationnels, et son noyau est J par définition de celui-ci. On a donc un isomorphisme d'anneaux de A/J avec $\mathbb{R}$.

5.8.2. Il est donc naturel de poser, *par définition*,

$$\mathbb{R} = A/J$$

et il s'agit alors de montrer que $\mathbb{R}$ ainsi défini possède toutes les propriétés voulues. C'est un peu plus complexe, si l'on peut dire, que pour la construction de $\mathbb{C}$ faite plus haut, et un exposé détaillé sortirait du cadre du présent cours. Le lecteur peut, à titre d'exemple, se poser la question suivante : $\mathbb{R}$ étant défini comme on vient de le faire, comment définir la notion de réel positif ?

5.9. *Exercice : un corps à 4 éléments.* Soit K le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, et soit $L = K[X]/(X^2 + X + 1)$. Montrer que L est un corps à 4 éléments, et écrire ses tables d'addition et de multiplication. (Indication : noter $\omega \in L$ la classe de X, remarquer que $1 + \omega + \omega^2 = 0$ et que $L = \{0, 1, \omega, \omega + 1\}$).

6. Caractéristique

6.1. Si A est un anneau, nous savons (1.8) qu'il existe un unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Notons-le $\varphi_A : \mathbb{Z} \to A$; rappelons que $\varphi_A(k) = k_A := k1_A$ pour tout $k \in \mathbb{Z}$.

Le *noyau* de φ_A est un idéal de $\mathbb{Z}$; il existe donc un unique entier $n \geq 0$ tel que $\operatorname{Ker} \varphi_A = n\mathbb{Z}$. Cet entier est un invariant fondamental de A :

Définition 6.2 *Soit A un anneau, et soit $\varphi_A : \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. On appelle* caractéristique *de A, et l'on note* $\operatorname{car}(A)$*, l'unique entier $n \geq 0$ tel que* $\operatorname{Ker} \varphi_A = n\mathbb{Z}$.

6.3. *Remarques.* Dans ce qui suit, A désigne un anneau et $\varphi_A : \mathbb{Z} \to A$ le morphisme d'anneaux de 6.1.

6.3.1. On prendra garde que si n désigne la caractéristique de A, alors n est bien un *entier naturel* et non un élément de A. Cet entier a la propriété remarquable que $nx = 0_A$ pour tout $x \in A$, puisqu'il est immédiat que $nx = n_A x$ (attention ici encore : multiplication externe à gauche de l'égalité, interne à droite).

6.3.2. *Image de φ_A.* Par construction, l'image de φ_A n'est autre que le *sous-groupe de $(A, +)$ engendré par 1_A*. C'est aussi le *plus petit sous-anneau de A*. Il est isomorphe, en vertu de 5.5, à $\mathbb{Z}/\operatorname{car}(A)\,\mathbb{Z}$: cette propriété caractérise l'entier $\operatorname{car}(A)$.

6.3.3. *Définition "naïve" de la caractéristique.* De façon plus terre-à-terre, $\operatorname{car}(A)$ peut être défini comme 0 si φ_A est injectif, et sinon comme le plus petit entier $n > 0$ tel que $n1_A = 0$, c'est-à-dire tel que $1_A + \cdots + 1_A = 0$ dans A. Ceci résulte de (I.3.6).

6.3.4. Si A est un sous-anneau (unitaire) d'un anneau B, alors $\operatorname{car}(B) = \operatorname{car}(A)$. Ceci résulte par exemple de l'unicité de φ_B : si $j : A \to B$ désigne l'inclusion, alors φ_B et $j \circ \varphi_A$ sont deux morphismes d'anneaux de $\mathbb{Z}$ dans B, donc égaux. Donc $\operatorname{Ker} \varphi_B = \operatorname{Ker}(j \circ \varphi_A)$, mais puisque j est injectif on a $\operatorname{Ker}(j \circ \varphi_A) = ker\varphi_A$, cqfd.

Le même genre d'argument montre plus généralement que si $f : A \to B$ est un morphisme d'anneaux alors $\operatorname{car}(B)$ *divise* $\operatorname{car}(A)$.

Bien entendu, ces propriétés peuvent aussi (et doivent, ô lecteur curieux) se déduire de 6.3.3.

6.3.5. *Exercice.* Déduire des remarques précédentes les équivalences (pour A donné et n entier > 0 donné) :

$$\begin{aligned}
\operatorname{car}(A) = 0 &\iff 1_A \text{ est d'ordre infini dans } (A,+)\\
&\iff \varphi_A \text{ est injectif}\\
&\iff \operatorname{Im}\varphi_A \text{ est isomorphe à } \mathbb{Z}\\
&\iff A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
\operatorname{car}(A) = n &\iff 1_A \text{ est d'ordre } n \text{ dans } (A,+)\\
&\iff \operatorname{Im}\varphi_A \text{ est isomorphe à } \mathbb{Z}/n\mathbb{Z}\\
&\iff A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}/n\mathbb{Z}.
\end{aligned}$$

6.3.6. *Exercices.* Trouver la caractéristique de tous les anneaux usuels rencontrés jusqu'à présent, et notamment : de l'anneau nul ; de $\mathbb{Z}/n\mathbb{Z}$; de $\mathbb{Q}$; de $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$, et plus généralement du produit de deux anneaux, et plus généralement du produit d'une famille quelconque d'anneaux, comme par exemple $\prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$; de A^I où I est un ensemble quelconque (attention !) ; de $\mathcal{C}([0,1],\mathbb{R})$.

6.3.7. Dans toutes les assertions ci-dessus, notre convention voulant que tous les morphismes d'anneaux soient unitaires est *essentielle.* Sans cette convention, par exemple, $\mathbb{Z}/2\mathbb{Z}$ serait (isomorphe à) un sous-anneau de $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ et 6.3.4 serait donc en défaut.

7. Caractéristique d'un corps

Proposition 7.1 *Soit A un anneau intègre, et soit n sa caractéristique. Alors ou bien $n = 0$, ou bien n est un nombre premier.*

Démonstration. A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$ d'après 6.3.2. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre puisque A l'est (2.4.5), donc si n n'est pas nul il est premier d'après 3.6. ∎

7.1.1. *Exercice.* Refaire la démonstration ci-dessus en remplaçant les références par une preuve directe.

7.1.2. *Remarque.* Il existe des anneaux intègres de caractéristique 0, par exemple $\mathbb{Z}$ (et même des corps, par exemple $\mathbb{Q}$). De même, pour tout p premier, il existe au moins un anneau intègre de caractéristique p, à savoir $\mathbb{Z}/p\mathbb{Z}$, qui est même un corps, noté classiquement $\mathbb{F}_p$. (Il en existe évidemment beaucoup d'autres !)

7.1.3. *Exercice.* Soient K et L deux corps de caractéristiques différentes. Montrer qu'il n'existe aucun morphisme de K dans L.

Le même résultat vaut-il pour deux anneaux intègres ? (On pourra préciser la réponse en discutant selon les caractéristiques).

7.2. *Anneaux de caractéristique p.* Dans ce qui suit on fixe un nombre *premier* p.

7.2.1. Si A est un anneau de caractéristique p, alors le morphisme naturel j_A du corps $\mathbb{F}_p$ dans A permet de munir A d'une structure de $\mathbb{F}_p$-*espace vectoriel* : l'addition est celle de A, et pour $\lambda \in \mathbb{F}_p$ et $x \in A$ on pose $\lambda x = j_A(\lambda)x$. Autrement dit, si λ est la classe de l'entier l, alors $\lambda x = lx$. (C'est d'ailleurs la *seule* structure de $\mathbb{F}_p$-espace vectoriel sur A dont l'addition soit celle de A).

7.2.2. Si $n \in \mathbb{Z}$ est un entier *non divisible par* p, la classe de n dans $\mathbb{F}_p$ est inversible, et par suite la multiplication par n dans A est bijective. Autrement dit, pour tout $x \in A$ il existe un unique $y \in A$ tel que $ny = x$. Cet élément y est parfois noté x/n. Cette notation peut être dangereuse : il y a risque de confusion, par exemple, entre le nombre rationnel $1/n$ et l'élément $1_A/n$ de A (ce dernier est égal à $m1_A$ où m est n'importe quel entier tel que $mn \equiv 1 \pmod{p}$).

Exemple : si $p = 5$ alors on a $x/2 = 3x$ pour tout $x \in A$.

7.2.3. *Exercice.* Si A et B sont deux anneaux de caractéristique p, montrer que tout morphisme d'anneaux de A dans B est $\mathbb{F}_p$-linéaire (pour les structures d'espaces vectoriels définies ci-dessus).

7.2.4. *Exercice.* Si A est un anneau de caractéristique p, montrer que A est *fini* si et seulement si A est de dimension finie comme $\mathbb{F}_p$-espace vectoriel, et qu'alors le

cardinal de A est une *puissance de p.*

Proposition 7.3 (et définition) *Soient p un nombre premier et A un anneau de caractéristique p. Alors on a, pour tous $x, y \in A$:*

$$(x+y)^p = x^p + y^p.$$

En conséquence l'application $F_A : A \to A$ définie par $F_A(x) = x^p$ est un endomorphisme d'anneau, appelé l'endomorphisme de Frobenius *de A.*

Démonstration. La formule du binôme (1.11.4) donne immédiatement

$$(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i\, y^{p-i}$$

et il suffit de montrer que tous les termes de la somme apparaissant à droite sont nuls. Comme A est de caractéristique p, on a $nz = 0$ pour tout $z \in A$ et tout entier n divisible par p, de sorte que la proposition résulte du lemme 7.3.1 ci-dessous. ∎

Lemme 7.3.1 *Soit p un nombre premier. Alors $\binom{p}{i}$ est divisible par p pour tout entier i tel que $0 < i < p$.*

Démonstration. On considère l'égalité $i!(p-i)!\binom{p}{i} = p!$. Le nombre premier p divise évidemment $p!$ donc divise $i!(p-i)!\binom{p}{i}$, qui est produit de $\binom{p}{i}$ et d'entiers $< p$ donc non divisibles par p. On conclut par le "lemme d'Euclide" (si un nombre premier divise un produit, il divise l'un des facteurs). ∎

7.3.2. *Question.* Dans la preuve de 7.3.1, où a servi l'hypothèse que p est premier ? Et l'hypothèse que $0 < i < p$? L'énoncé est-il encore vrai sans ces hypothèses ?

7.3.3. *Remarque.* Pour une autre démonstration de 7.3.1, voir (I.7.5.2).

7.3.4. *Remarque.* Dans la situation de 7.3, on a évidemment $F_A(1_A) = 1_A$, d'où, puisque F_A respecte l'addition, $F_A(m1_A) = m1_A$ pour tout $m \in \mathbb{Z}$. Autrement dit F_A induit l'identité sur le sous-anneau (isomorphe à) $\mathbb{Z}/p\mathbb{Z}$ de A. Prenant en particulier pour A le corps $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, on retrouve le théorème de Fermat, déjà démontré en 3.7 : *pour tout entier m et tout p premier, on a $m^p \equiv m \pmod p$.*

7.3.5. *Frobenius itéré.* Bien entendu, si A est un anneau de caractéristique p et $i \in \mathbb{N}$, alors F_A^i est encore un endomorphisme de A ; il est donné par $F_A^i(x) = x^{p^i}$ pour tout $x \in A$.

7.4. *Corps de caractéristique p.* Soient p un nombre premier et K un corps de caractéristique p.

7.4.1. Rappelons que K admet un unique sous-anneau isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, qui est même un *sous-corps* (et en fait le plus petit sous-corps) de K.

7.4.2. *Frobenius.* Comme tout morphisme de corps, l'endomorphisme de Frobenius F_K de K est *injectif*. En d'autres termes, pour tout $a \in K$ il existe *au plus un* $y \in K$ tel que $y^p = x$. Si un tel y existe on peut sans inconvénient le noter $a^{1/p}$, voire $\sqrt[p]{a}$ et l'appeler "racine p-ième de a" (chose extrêmement dangereuse en temps normal !). Noter que si $a^{1/p}$ et $b^{1/p}$ existent on a $a^{1/p} + b^{1/p} = (a+b)^{1/p}$.

On voit donc, en d'autres termes, que pour tout $a \in K$ le polynôme $X^p - a$ admet *au plus une racine* dans K ; d'ailleurs il suffit de remarquer que si α est une telle racine on a $\alpha^p = a$ d'où $X^p - a = X^p - \alpha^p = (X-\alpha)^p$ puisque $K[X]$ est encore un anneau de caractéristique p.

7.4.3. *Exercice.* Si K est un corps *fini* (donc nécessairement de caractéristique positive), alors F_K est bijectif, donc est un *automorphisme* de K.

7.5. *Corps de caractéristique nulle.* Dans ce qui suit, K désigne un corps de caractéristique 0.

7.5.1. *Règles de calcul.* En plus des règles de calcul valables dans tous les corps, on dispose de la *division par un entier non nul :* si $a \in K$ et $n \in \mathbb{Z}^*$, il existe un unique $x \in K$ tel que $nx = a$, à savoir $x = a/n_K$ (en effet $n_K \neq 0$ puisque $n \neq 0$ et que car $K = 0$).

7.5.2. Il est facile de voir que tout corps admet un *plus petit sous-corps*, à savoir l'intersection de tous ses sous-corps. Pour un corps de caractéristique $p > 0$, nous avons vu que ce sous-corps est aussi le plus petit sous-anneau, isomorphe à $\mathbb{F}_p$. Mais ici, dire que K est de caractéristique 0 équivaut à dire que son plus petit sous-anneau est isomorphe à $\mathbb{Z}$, *qui n'est pas un corps* : la situation est donc un peu différente. La proposition suivante identifie le plus petit sous-corps de K :

Proposition 7.6 *Soit K un corps. Les conditions suivantes sont équivalentes :*

(i) *K est de caractéristique nulle ;*

(ii) *il existe un morphisme de corps de $\mathbb{Q}$ dans K.*

De plus, si ces conditions sont vérifiées, le morphisme de (ii) *est unique et son image est le plus petit sous-corps de K.*

Démonstration. Il est clair que (ii) implique (i) : si (ii) est vérifiée, K admet un sous-corps isomorphe à $\mathbb{Q}$ donc de caractéristique nulle, et est donc lui-même de caractéristique nulle.

Supposons désormais K de caractéristique nulle, et supposons trouvé un morphisme $j : \mathbb{Q} \to K$. La restricition de j à $\mathbb{Z}$ est un morphisme d'anneaux, donc ne

peut être que le morphisme $\varphi_K : n \mapsto n_K$. En conséquence, si $r = a/b \in \mathbb{Q}$ (avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$), l'égalité $br = a$ entraîne $j(b)j(r) = j(a)$ donc $b_K j(r) = a_K$ et finalement

$$j(a/b) = a_K/b_K$$

qui a bien un sens pusique $a_K \neq 0$ vu l'hypothèse sur car (K). Ceci montre l'unicité de j.

Il reste à voir, pour montrer l'existence de j :

- que la formule ci-dessus définit bien une application de $\mathbb{Q}$ dans K, c'est-à-dire que, pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, a_K/b_K ne dépend que du rationnel a/b ;
- que l'application en question est un morphisme.

Toutes ces vérifications sont triviales, et nous les omettons d'autant plus volontiers que nous redémontrerons cette propriété au paragraphe suivant (8.10) comme conséquence d'un résultat plus général.

Enfin soit K_0 l'image de j : c'est un sous-corps de K isomorphe à $\mathbb{Q}$. Il s'agit de voir que tout sous-corps de K contient K_0. Cela peut se faire de deux façons :

(1) Par construction, K_0 est l'ensemble des éléments de K de la forme a_K/b_K avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$; or tout sous-corps de K contient 1_K, donc tous les a_K $(a \in \mathbb{Z})$ puisque c'est un sous-groupe additif, donc aussi tous les quotients a_K/b_K puisque c'est un sous-corps.

(2) Soit K' un sous-corps de K : alors K' est de caractéristique nulle donc il existe un unique morphisme $j' : \mathbb{Q} \to K'$. Composant avec l'inclusion de K' dans K on obtient un morphisme de $\mathbb{Q}$ dans K qui ne peut être que j vu l'unicité de celui-ci. En particulier $\mathrm{Im}\, j = \mathrm{Im}\, j' \subset K'$, d'où la conclusion. ∎

7.6.1. *Remarque.* Si K est un corps de caractéristique 0, la proposition 7.6 permet d'identifier sans crainte $\mathbb{Q}$ à un sous-corps de K ; par exemple, on peut noter a/n l'élément a/n_K considéré en 7.5.1.

En particulier, K a une structure naturelle de $\mathbb{Q}$-espace vectoriel : l'argument est le même qu'en 7.2.1 mais cette fois il ne s'étend pas à tous les anneaux de caractéristique 0.

7.7. *Remarque.* Les résultats de ce paragraphe permettent notamment de trouver tous les *corps premiers* (cf. 3.11.1) :

- un corps de caractéristique 0 est premier si et seulement si il est isomorphe à $\mathbb{Q}$;

- si p est un nombre premier, un corps de caractéristique p est premier si et seulement si il est isomorphe à $\mathbb{F}_p$.

8. Corps des fractions d'un anneau intègre

On rappelle que si A est un anneau intègre, on désigne par A^* l'ensemble des éléments réguliers (c'est-à-dire non nuls) de A.

Définition 8.1 *Soit A un anneau intègre. On appelle* corps des fractions *de A tout couple (K, i) où K est un corps et $i : A \to K$ un morphisme d'anneaux, vérifiant les propriétés suivantes :*

(i) *i est injectif ;*

(ii) *tout élément de K est un quotient d'éléments de $i(A)$.*

8.1.1. *Remarque.* De façon explicite, la condition (ii) signifie que pour tout $x \in K$, il existe a et b dans A tels que $i(b) \neq 0$ et $x = i(a)/i(b)$. Noter cependant qu'à cause de la condition (i), la condition $i(b) \neq 0$ équivaut simplement à $b \neq 0$. On n'exige évidemment aucune condition d'unicité sur a et b. (Lecteur : pourquoi "évidemment" ?)

8.1.2. *Remarque.* En pratique, on identifie souvent un élément a de A et son image $i(a)$ dans K (autrement dit, on ne distingue pas A du sous-anneau de K image de i, qui est isomorphe à A par (i)). Cet abus de langage en entraîne un autre, consistant à appeler corps des fractions de A le corps K lui-même plutôt que le couple (K, i).

Dans ce paragraphe, consacré à l'existence et à l'unicité du corps des fractions, nous éviterons ces abus.

8.1.3. *Exemple.* Si A est un *corps*, alors (A, Id_A) est un corps des fractions de A, et c'est "essentiellement" le seul : en effet si (K, i) est un corps des fractions de A, la condition (ii) implique dans ce cas que i est surjectif, donc est un isomorphisme.

8.1.4. *Exemple.* Si i désigne le morphisme d'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$, le couple $(\mathbb{Q}, i)$ est un corps des fractions de $\mathbb{Z}$. C'est en fait la définition de $\mathbb{Q}$ (voir plus bas).

8.1.5. *Exercice.* Soit A un sous-anneau d'un corps L (A est donc automatiquement intègre), et soit K le sous-corps de L engendré par A (cf. 3.14). Montrer que K est l'ensemble des éléments de L qui sont quotients d'éléments de A ; en déduire que si i est le morphisme d'inclusion de A dans K, alors (K, i) est un corps des fractions de A.

8.1.6. *Exercice.* Déduire de 8.1.5 qu'un anneau intègre A admet un corps des fractions si et seulement si A est isomorphe à un sous-anneau d'un corps.

La définition suivante nous permettra de formuler commodément l'unicité du corps des fractions :

Définition 8.2 *Soient A, B, C trois anneaux et $i : A \to B$, $j : A \to C$ des morphismes d'anneaux. On appelle* A-morphisme *de (B, i) dans (C, j) tout morphisme d'anneaux $\varphi : B \to C$ tel que $j = \varphi \circ i$.*

8.2.1. *Remarque.* Il est clair que, pour A donné, le composé de deux A-morphismes est un A-morphisme, et que pour $i : A \to B$ donné, Id_B est un A-morphisme de (B, i) dans lui-même.

8.2.2. *Remarque.* On appellera *A-isomorphisme* de (B, i) dans (C, j) un A-morphisme qui est un isomorphisme de B dans C ; son inverse est alors automatiquement un A-isomorphisme de (C, j) dans (B, i).

Théorème 8.3 (existence du corps des fractions) *Tout anneau intègre admet un corps des fractions.*

Théorème 8.4 (propriété universelle du corps des fractions) *Soient A un anneau intègre et (K, i) un corps des fractions de A.*

D'autre part soient L un corps et $j : A \to L$ un morphisme injectif.

Alors il existe un unique A-morphisme de (K, i) dans (L, j).

Théorème 8.5 (unicité du corps des fractions) *Soient A un anneau intègre, et soient (K_1, i_1) et (K_2, i_2) deux corps des fractions de A. Alors il existe un unique A-morphisme $\theta : K_1 \to K_2$, et θ est un A-isomorphisme.*

Pour démontrer ces théorèmes nous établirons d'abord (c'est le plus simple et le plus "formel") que la propriété universelle (8.4) implique l'unicité (8.5). Ensuite (8.7) nous montrerons 8.4, et enfin (8.8) le théorème d'existence 8.3. Ces trois démonstrations sont d'ailleurs largement indépendantes, et le lecteur peut les aborder dans un autre ordre.

En pratique, la construction explicite 8.8 ne sert qu'à prouver l'existence du corps des fractions, et non à établir telle ou telle de ses propriétés. En fait, *toutes les propriétés utiles du corps des fractions peuvent se déduire de la définition ou de la propriété universelle.*

8.6. Montrons donc 8.5, en supposant 8.4 déjà établi. Avec les notations de 8.5, comme (K_1, i_1) est un corps des fractions de A et que i_2 est injectif, on peut appliquer 8.4 en prenant $(K, i) = (K_1, i_1)$ et $(L, j) = (K_2, i_2)$ ce qui montre déjà l'existence d'un unique A-morphisme θ de (K_1, i_1) dans (K_2, i_2). Mais on peut aussi appliquer 8.4 en prenant $(K, i) = (K_2, i_2)$ et $(L, j) = (K_1, i_1)$, d'où un A-morphisme $\psi : K_2 \to K_1$. Le composé $\psi \circ \theta$ est alors un A-morphisme de (K_1, i_1) dans (K_1, i_1). Mais Id_{K_1} en est un autre, et l'assertion d'unicité de 8.4 (en prenant $(K, i) = (L, j) = (K_1, i_1)$)

montre que $\psi \circ \theta = \mathrm{Id}_{K_1}$. Symétriquement, on voit que $\theta \circ \psi = \mathrm{Id}_{K_2}$, de sorte que θ est bien un isomorphisme. ∎

8.6.1. *Remarque.* Le raisonnement ci-dessus s'applique chaque fois que l'on a une "propriété universelle", et montre l'unicité, à isomorphisme unique près, de l'objet vérifiant cette propriété. Faute d'une *définition* de ce qu'est une propriété universelle, nous ne sommes pas en mesure dans le cadre de ce cours de donner un sens précis à cette remarque. Le lecteur peut néanmoins s'essayer à adapter l'argument de 8.5 à toutes les propriétés universelles rencontrées jusqu'ici (et plus tard). Voici deux exemples :

8.6.2. *Exercice.* Soit R un anneau. On suppose que pour tout anneau A il existe un unique morphisme d'anneaux de R dans A. Montrer qu'il existe un unique isomorphisme d'anneaux de R sur $\mathbb{Z}$.

8.6.3. *Exercice.* Soient G un groupe et g un élément de G. On suppose que pour tout groupe H et tout $h \in H$ il existe un unique morphisme de groupes $f : G \to H$ tel que $f(g) = h$. Montrer qu'il existe un unique isomorphisme de groupes de $\varphi : \mathbb{Z} \to G$ tel que $\varphi(1) = g$.

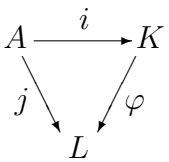
8.6.4. *Exercice.* Soient A un anneau intègre, K un corps et $i : A \to K$ un morphisme injectif vérifiant la propriété universelle 8.4. Montrer que (K, i) est un corps des fractions de A.

On pourra procéder de deux façons:

Première méthode. Soit (K', i') un corps des fractions de A : alors (K, i) vérifient la même propriété universelle donc sont A-isomorphies. (Cette méthode utilise l'existence du corps des fractions, et sa propriété universelle.)

Seconde méthode. Voici une preuve plus directe, n'utilisant pas 8.3 ni 8.4. Soit K_0 le sous-corps de K engendré par $i(A)$: alors la propriété universelle de (K, i) implique qu'il existe un A-morphisme $\varphi : K \to K_0$, et que $\varphi \circ f = \mathrm{Id}_K$ où f désigne l'inclusion de K_0 dans K. Donc φ est un isomorphisme (c'est un morphisme surjectif de corps), et d'autre part K_0 est un corps des fractions de A d'après 8.1.5, d'où la conclusion.

8.7. *Propriété universelle : démonstration de* 8.4. Avec les notations de 8.4, il s'agit de trouver un morphisme $\varphi : K \to L$ rendant commutatif le diagramme



et de montrer de plus l'unicité de φ.

8.7.1. *Unicité de φ.* Si $\varphi : K \to L$ est un A-morphisme, on remarque d'abord que si $a \in A$ et $b \in A^\times$, on a nécessairement $\varphi(i(a)/i(b)) = \varphi(i(a))/\varphi(i(b)) = j(a)/j(b)$ puisque φ est un morphisme de corps et que $\varphi \circ i = j$. Comme tout élément de K est de la forme $i(a)/i(b)$ pour a et b convenables, ceci montre bien l'unicité de φ, et suggère (pour la suite) de définir $\varphi(x)$, pour $x = i(a)/i(b) \in K$, comme égal à $j(a)/j(b)$.

8.7.2. *Remarque.* L'argument ci-dessus n'utilise pas le fait que L est un corps, ni l'injectivité de j. Il montre donc, plus généralement, que si (K, i) est un corps des fractions de A et $f : A \to B$ un morphisme d'anneaux quelconque, il existe *au plus un* A-morphisme de (K, i) dans (B, f). On suggère au lecteur de s'assurer qu'il a compris en refaisant la démonstration 8.7.1 dans ce cas plus général.

8.7.3. *Existence de φ.* Vérifions d'abord que la définition suggérée à la fin de 8.7.1 a bien un sens. Si $x \in K$, on peut écrire $x = i(a)/i(b)$ avec $a \in A$ et $b \in A^*$. Comme j est injectif et que L est un corps, $j(b) \in L^\times$ de sorte que $j(a)/j(b) \in L$ a un sens. Il faut encore vérifier que $j(a)/j(b)$ ne dépend en fait que de l'élément $x = i(a)/i(b)$ de K. Or, si $i(a)/i(b) = i(a')/i(b')$ alors $i(a)i(b') = i(a')i(b)$, donc $i(ab') = i(a'b)$, d'où $ab' = a'b$ puisque i est injectif. Par suite $j(a)j(b') = j(a')j(b)$ d'où $j(a)/j(b) = j(a')/j(b')$, cqfd.

On a donc montré qu'il existe une application $\varphi : K \to L$ telle que l'on ait $\varphi(i(a)/i(b)) = j(a)/j(b)$ pour tous $a \in A$ et $b \in A^*$. Prenant en particulier $b = 1$, on en déduit tout de suite que $\varphi \circ i = j$.

Il ne reste plus qu'à voir que φ est un morphisme : ce sont là calculs de routine laissés gracieusement au lecteur. La preuve de 8.4 est achevée. ∎

8.7.4. *Remarque.* Ici encore on peut généraliser. (K, i) désignant toujours un corps des fractions de A, soit $f : A \to B$ un morphisme d'anneaux ayant la propriété suivante : pour tout $a \in A$ non nul, $f(a)$ est inversible dans B (autrement dit, $f(A^*) \subset B^\times$). Alors il existe un A-morphisme de (K, i) dans (B, f) (nécessairement unique, d'après 8.7.2). On invite encore le lecteur à faire soigneusement la démonstration, et aussi à répondre à la question suivante : la condition $f(A^*) \subset B^\times$ implique-t-elle que f est injectif ?

8.8. *Construction du corps des fractions.* Nous allons maintenant prouver 8.3 en construisant explicitement, à partir d'un anneau intègre A, un corps des fractions de A.

8.8.1. *Heuristique.* Pour justifier la construction qui va suivre, supposons d'abord donné un corps des fractions (K, i) de A. Il existe une application $\varphi : A \times A^* \to K$ définie par $\varphi(a, b) = i(a)/i(b)$ (en effet, comme $b \neq 0$ et i est injectif, $i(b)$ n'est pas nul donc est inversible dans K). La condition (ii) de la définition 8.1 revient à dire que φ est *surjective*. De plus, pour (a, b) et $(a', b') \in A \times A^*$, l'égalité $\varphi(a, b) = \varphi(a', b')$ est

équivalente à $i(a)/i(b) = i(a')/i(b')$ donc à $i(a)i(b') = i(a')i(b)$, ou encore à $ab' = a'b$ puisque i est un morphisme injectif. (Ce calcul a déjà été fait dans 8.7.3).

Autrement dit, tout élément de K peut être "représenté" par un couple $(a, b) \in A \times A^*$, et deux couples (a, b) et (a', b') représentent le même élément de K si et seulement si $ab' = a'b$. De plus, pour $a \in A$, $i(a)$ est représenté (entre autres) par le couple $(a, 1)$.

8.8.2. *La construction.* Ne supposant plus l'existence d'un corps des fractions, considérons sur l'ensemble produit $A \times A^*$ la relation binaire $\sim$ définie par :

$$(a, b) \sim (a', b') \Longleftrightarrow ab' = a'b$$

(on suppose évidemment que $a, a' \in A$ et $b, b' \in A^*$; dans la suite ce genre d'hypothèse sera toujours implicite).

Il s'agit d'une *relation d'équivalence* sur $A \times A^*$: en effet la réflexivité et la symétrie sont évidentes, et si l'on a $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'')$, alors la relation $ab' = a'b$ implique $ab'b'' = a'bb''$ qui est égal à $a''bb'$ puisque $a'b'' = a''b'$. Comme $b' \neq 0$ et que A est intègre, on peut simplifier par b' la relation $ab'b'' = a''bb'$, d'où $ab'' = a''b$, c'est-à-dire $(a, b) \sim (a'', b'')$, cqfd.

8.8.3. *Définition de l'ensemble K.* On pose par définition

$$K := A \times A^*/\sim$$

c'est-à-dire que K est l'ensemble des classes d'équivalence pour la relation $\sim$.

Pour $a \in A$ et $b \in A^*$ nous noterons $[a, b] \in K$ la classe de (a, b).

(Lorsque nous aurons muni K d'une structure de corps et défini $i : A \to K$, $[a, b] \in K$ sera en fait le quotient $i(a)/i(b)$, comme il se doit d'après 8.8.1).

8.8.4. *Définition de i.* Pour tout $a \in A$ on définit $i(a) \in K$ par la formule $i(a) = [a, 1]$. Ceci définit une application $i : A \to K$.

Nous allons maintenant construire les lois de composition de K. Les vérifications de routine (i.e. ne nécessitant que l'application docile des définitions) seront laissées au lecteur : les faire constitue un bon exercice, les lire n'a strictement aucun intérêt.

8.8.5. *Multiplication dans K.* Définissons d'abord une loi "multiplication" sur l'ensemble $A \times A^*$ par la formule $(a, b)(c, d) = (ac, bd)$. Cette loi est commutative et associative, et elle admet comme élément neutre $(1, 1)$. D'autre part cette loi "passe au quotient" : pour $x = [a, b]$ et $y = [c, d]$ dans K, l'élément $[ac, bd]$ de K (la classe du produit $(a, b)(c, d)$) ne dépend que de x et y et non des représentants (a, b) et (c, d). On peut donc définir une loi de composition "multiplication" sur K vérifiant, pour tous (a, b) et $(c, d) \in A \times A^*$, la relation $[a, b][c, d] = [ac, bd]$.

Tout comme la multiplication dans $A \times A^*$, cette loi est commutative et associative, elle admet comme élément neutre $1_K := i(1) = [1,1]$, et de plus on a $i(aa') = i(a)i(a')$ pour tous $a, a' \in A$.

8.8.6. *Addition dans K.* On définit de même une addition sur $A \times A^*$ par la formule (inspirée évidemment de l'addition des fractions) $(a,b)+(c,d) = (ad+bc, bd)$. Elle est commutative et associative, admet $(0,1)$ pour élément neutre, et passe au quotient en une loi de composition "addition" sur K (vérifiant, donc, $[a,b]+[c,d] = [ad+bc, bd]$). Cette dernière hérite de la commutativité, de l'associativité et de l'élément neutre de son ancêtre (l'élément neutre de l'addition de K est donc la classe $0_K := i(0) = [0,1]$) et de plus c'est une loi de groupe : on a en effet $[a,b]+[-a,b] = [ab-ba, b^2] = [0,b^2] = [0,1]$. (Noter que la dernière égalité utilise la relation d'équivalence : l'addition dans $A \times A^*$ n'est pas uen loi de groupe).

Enfin la multiplication est distributive par rapport à l'addition (dans K, mais pas dans $A \times A^*$). On a donc montré que K est un anneau commutatif unitaire, et que i est un morphisme d'anneaux. Il est de plus injectif (vérification directe sur la définition, ou calcul du noyau).

8.8.7. *K est un corps.* Il est évidemment non nul puisque A est non nul et que i est injectif. Dire que $[a,b] \neq 0_K$ équivaut à dire que $a \neq 0$ (vérifier !). Dans ce cas, $[b,a]$ est bien un inverse de $[a,b]$.

8.8.8. *Finale.* Tout $x \in K$ s'écrit, pour $a \in A$ et $b \in A^*$ convenables, $x = [a,b] = [a,1][1,b] = i(a)\, i(b)^{-1}$. On a donc bien la propriété (ii) de l'énoncé. ∎

8.9. *Exemples.*

8.9.1. $\mathbb{Q}$ est *par définition* le corps des fractions de $\mathbb{Z}$ (le lecteur pourra se convaincre que la construction ci-dessus ne fait pas appel, même indirectement, à l'existence du corps $\mathbb{Q}$).

8.9.2. Si k est un corps, le corps des fractions de l'anneau intègre $k[X]$ (voir chapitre suivant) est par définition le *corps des fractions rationnelles en une indéterminée X à coefficients dans k* ; ce corps est noté $k(X)$.

Enfin on retrouve grâce à 8.4 un résultat déjà vu en 7.6 :

Corollaire 8.10 *Soit F un corps de caractéristique nulle. Alors il existe un unique morphisme de corps de $\mathbb{Q}$ dans F.*

Démonstration. Comme $\mathrm{car}\,(F) = 0$, l'unique morphisme d'anneaux $\varphi_F : \mathbb{Z} \to F$ est *injectif*. Il suffit alors d'appliquer 8.4 en prenant $A = \mathbb{Z}$, $K = \mathbb{Q}$, i=l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$, et $j = \varphi_F$. ∎

8.10.1. *Exercice.* Plus généralement, soit A un anneau. Montrer qu'il existe au plus un morphisme de $\mathbb{Q}$ dans A (utiliser soit 3.11.3 et 3.11.2, soit 8.7.2) et qu'il en existe un si et seulement si, pour tout entier $n \neq 0$, $n1_A$ est inversible dans A. (utiliser 8.7.4, et le cas échéant expliciter le morphisme de $\mathbb{Q}$ dans A). S'il en est ainsi, que peut-on dire de la caractéristique de A ?

Chapitre III

Divisibilité, anneaux principaux

1. Divisibilité dans les anneaux intègres

Définition 1.1 *Soit A un anneau intègre, et soient a et b deux éléments de A. On dit que a* divise *b (dans A) s'il existe $x \in A$ tel que $b = ax$ (autrement dit, si b appartient à l'idéal (a) engendré par a).*

On écrit "$a|b$" pour "a divise b".

1.1.1. Les expressions "a est un diviseur de b", "b est un multiple de a", "b est divisible par a" sont synonymes de "a divise b".

Ne pas oublier de préciser l'anneau lorsqu'il peut y avoir un doute. Par exemple 2 divise 1 dans $\mathbb{Q}$, mais pas dans $\mathbb{Z}$.

1.2. *Propriétés élémentaires :*

1.2.1. Il est clair que tout élément de A divise 0 (sans être pour autant un "diviseur de zéro" au sens de (II.2.1)), et que 1 (et plus généralement tout inversible de A) divise tout élément de A ; il est clair aussi que la divisibilité est une relation réflexive (a divise a) et transitive (si a divise b et b divise c alors a divise c).

1.2.2. Soient $a, b, c \in A$: si $a|b$ alors $ac|bc$, et la réciproque est vraie si $c \neq 0$.

1.2.3. Pour que $a|b$ il faut et il suffit que $(b) \subset (a)$: la relation de divisibilité ne dépend que des idéaux engendrés.

1.2.4. Si A est un corps, tout élément non nul de A divise tout élément de A.

1.2.5. *Exercice.* Soit U un ouvert de $\mathbb{C}$, connexe et non vide, et soit A l'anneau des fonctions holomorphes sur U (cf. (II.2.4.8)). Pour $f \in A$ et $z \in U$, notons $\mathrm{ord}_z(f)$ l'ordre de f en z (qui est $+\infty$ si $f = 0$, et est un entier naturel sinon).

Pour f et $g \in A$, montrer que $f|g$ dans A si et seulement si l'on a $\mathrm{ord}_z(f) \leq \mathrm{ord}_z(g)$ pour tout $z \in U$.

1.3. *Éléments associés :* on dit que a et $b \in A$ sont *associés* dans A si $a|b$ et $b|a$. Cette relation équivaut à "il existe $x \in A^\times$ tel que $ax = b$" (exercice ; on utilise là le fait que A est intègre). Ceci équivaut aussi à $(a) = (b)$.

L'association est une *relation d'équivalence* ; les deux caractérisations ci-dessus montrent que l'ensemble quotient de A par cette relation s'identifie d'une part à l'ensemble des idéaux principaux de A, et d'autre part à l'ensemble quotient de A par l'action de $(A^\times, \times)$ donnée par $(\lambda, x) \mapsto \lambda x$.

Pour les questions de divisibilité il n'y a pas lieu en général de distinguer entre deux éléments associés : par exemple, si a et a' sont associés dans et si $b \in A$, alors a divise b si et seulement si a' divise b, etc.

1.3.1. *Exemples.* Deux éléments de $\mathbb{Z}$ sont associés si et seulement si ils sont égaux ou opposés ; deux éléments P et Q de $k[X]$ (où k est un corps) sont associés si et seulement si il existe $\lambda \in k^*$ tel que $Q = \lambda P$; deux éléments d'un corps sont associés si et seulement si ils sont soit tous deux nuls, soit tous deux non nuls.

1.3.2. *Exercice.* Soit A l'anneau de 1.2.5.

Pour f et $g \in A$, montrer que f et g sont associés dans A si et seulement si l'on a $\mathrm{ord}_z(f) = \mathrm{ord}_z(g)$ pour tout $z \in U$ (autrement dit, si f et g ont les mêmes zéros, avec les mêmes multiplicités).

2. PGCD, PPCM, éléments irréductibles

2.1. *Notation.* Si a est un élément d'un anneau intègre A, nous noterons $\mathrm{Div}\,(a)$ l'ensemble des diviseurs de a. (Quant à l'ensemble des multiples de a, il n'a pas besoin d'une nouvelle notation : c'est l'idéal (a) engendré par a.)

Définition 2.2 *Soient A un anneau intègre, $(a_i)_{i\in I}$ une famille d'éléments de A, d et m deux éléments de A.*

(1) *On dit que d est un plus grand commun diviseur (en abrégé* PGCD*) de la famille (a_i) si l'on a*

$$\bigcap_{i\in I} \mathrm{Div}\,(a_i) = \mathrm{Div}\,(d).$$

(2) *On dit que m est un plus petit commun multiple (en abrégé* PPCM*) de la famille (a_i) si l'on a*

$$\bigcap_{i\in I} (a_i) = (m).$$

2.3. *Remarques.*

2.3.1. Pour montrer que d est un PGCD des a_i, il faut vérifier deux choses :

- d est un diviseur commun des a_i, c'est-à dire que $d|a_i$ pour tout $i \in I$;
- tout diviseur commun des a_i est un diviseur de d.

"Plus grand" signifie donc ici, par abus, "multiple de tous les autres" : il est inutile de préciser que, a priori, dire qu'un élément d'un anneau est plus grand qu'un autre n'a aucun sens.

(Est-ce vraiment inutile ?)

2.3.2. Pourquoi dit-on "plus grand commun diviseur" plutôt que "plus grand diviseur commun" ? Très bonne question.

2.3.3. Mêmes commentaires, mutatis mutandis, pour les PPCM.

2.3.4. Dans l'expression "un PGCD", l'article indéfini est essentiel. Il résulte immédiatement de la définition que si d est un PGCD des a_i, alors les PGCD des a_i sont tous les éléments de A *associés* à d. En d'autres termes, le PGCD n'est unique qu'à association près. Idem pour "le" PPCM.

2.3.5. *Mise en garde.* On écrit parfois des identités du genre "$d = \mathrm{PGCD}\,(a, b)$" où a, b, d sont les éléments d'un anneau A. Il s'agit d'un abus d'écriture qui peut

être dangereux. Par exemple, une autre identité $d' = \mathrm{PGCD}\,(a, b)$ ne permet pas de conclure que $d = d'$, mais seulement que d est associé à d'.

2.3.6. Il existe des exemples de familles (et même de couples) d'éléments d'un anneau intègre qui n'ont pas de PGCD (ni de PPCM) ; voir les exercices 2.5.1 et 2.5.2 plus bas.

2.3.7. *Exercice.* Pour $n \in \mathbb{N}$ et $a_1, \ldots, a_n \in A$, montrer que 0 est un PPCM des a_i si et seulement si l'un des a_i est nul.

Cette propriété ne s'étend pas aux familles infinies : ainsi, pour $A = \mathbb{Z}$, la famille de tous les entiers non nuls admet 0 comme PPCM.

2.3.8. *Exercice.* Soient $a, a', b \in A$. On suppose que $a \equiv a' \pmod{b}$. Montrer que tout PGCD de a et b est aussi un PGCD de a' et b.

Proposition 2.4 *Soit A un anneau intègre. On suppose que tout couple d'éléments de A admet un PPCM. Alors :*

(i) *toute famille finie d'éléments de A admet un PPCM, et l'on a la formule "d'associativité"*

$$\mathrm{PPCM}\,(a_1, \ldots, a_n) = \mathrm{PPCM}\,(a_1, \mathrm{PPCM}\,(a_2, \ldots, a_n))$$

valable pour tout entier $n \geq 3$ et toute suite $(a_1, \ldots, a_n)$ de n éléments de A. (Bien entendu, l'égalité s'entend à association près).

(ii) *pour $\lambda, a, b \in A$ on a (toujours à association près)*

$$\mathrm{PPCM}\,(\lambda a, \lambda b) = \lambda\,\mathrm{PPCM}\,(a, b).$$

Démonstration. L'assertion (i) résulte d'une récurrence immédiate et de l'associativité de l'intersection (plus précisément de la formule $\bigcap_{i=1}^{n}(a_i) = (a_1) \cap \bigcap_{i=2}^{n}(a_i)$).

Montrons (ii). C'est trivial si $\lambda = 0$; nous supposerons donc désormais que $\lambda \neq 0$. Soit m un PPCM de a et b : on a d'abord $a|m$ et $b|m$ donc $\lambda a|\lambda m$ et $\lambda b|\lambda m$. Il reste à voir que si c est un multiple commun de λa et λb alors $\lambda m|c$. Or c est en particulier multiple de λ de sorte que l'on peut écrire $c = \lambda c'$ avec $c' \in A$. La relation $\lambda a|c$ et l'hypothèse $\lambda \neq 0$ entraînent que $a|c'$. De même $b|c'$, donc $m|c'$ par définition de m, et finalement λm divise $\lambda c' = c$, cqfd. ∎

Proposition 2.5 *Soit A un anneau intègre. On suppose que tout couple d'éléments de A admet un PGCD. Alors :*

(i) *toute famille finie d'éléments de A admet un PGCD, et l'on a la formule "d'associativité"*

$$\mathrm{PGCD}\,(a_1, \ldots, a_n) = \mathrm{PGCD}\,(a_1, \mathrm{PGCD}\,(a_2, \ldots, a_n))$$

valable pour tout entier $n \geq 3$ et toute suite $(a_1, \ldots, a_n)$ de n éléments de A. (Bien entendu, l'égalité s'entend à association près).

(ii) *pour $\lambda, a, b \in A$ on a (toujours à association près)*

$$\mathrm{PGCD}\,(\lambda a, \lambda b) = \lambda\,\mathrm{PGCD}\,(a, b).$$

Démonstration. Elle est tout analogue à celle de 2.4 et nous la laissons donc au lecteur, avec toutefois une indication pour la partie (ii) : plutôt que de partir d'un PGCD de a et b, ce qui serait le réflexe naturel, il faut d'abord considérer un PGCD de λa et λb, montrer qu'il est de la forme λd avec $d \in A$, et enfin vérifier que d est bien un PGCD de a et b. ■

2.5.1. *Exercice.* Soient a et $b \in A$ (intègre), non nuls et admettant un PPCM noté m. Montrer que ab/m est un PGCD de a et b.

(Remarque : le quotient ab/m a un sens dans le corps des fractions de A ; bien entendu il faut commencer par montrer qu'il est dans A, i.e. que m divise ab).

Autrement dit, l'existence d'un PPCM implique celle d'un PGCD (avec de plus le relation $\mathrm{PGCD}(a, b)\,\mathrm{PPCM}(a, b) = ab$, à association près). La réciproque est fausse comme le montre l'exercice suivant :

2.5.2. *Exercice.* Soit k un corps, et soit A le sous-ensemble de $k[X]$ formé des polynômes dans lesquels le coefficient de X est nul.

Montrer que A est un sous-anneau de $k[X]$, et que pour $n \in \mathbb{N}$ les diviseurs de X^n dans A sont les λX^i avec $\lambda \in k^*$ et soit $i = 0$, soit $i = n$, soit $2 \leq i \leq n - 2$.

En déduire que X^2 et X^3 ont 1 comme PGCD mais n'ont pas de PPCM, et que X^5 et X^6 n'ont ni PGCD, ni PPCM.

(Pour faire les calculs il est commode de remarquer que, pour P et $Q \in A$ non nuls, "P divise Q dans A" équivaut à "P divise Q dans $k[X]$ et le quotient Q/P appartient à A".)

2.6. Il est clair par définition que deux éléments a et b de A (intègre) ont un PPCM si et seulement si l'idéal $(a) \cap (b)$ est *principal*.

Pour le PGCD on n'a pas, a priori, de critère aussi simple en termes d'idéaux. On a toutefois une condition *suffisante* d'existence, fournie par la proposition suivante :

Proposition 2.7 *Soient a et b deux éléments d'un anneau intègre A. On suppose que l'idéal (a, b) engendré par $\{a, b\}$* (cf. II.4.3) *est* principal. *Alors, si d est un générateur de cet idéal :*

(i) *d est un PGCD de a et b ;*

(ii) *il existe u et v dans a tels que $au + bv = d$.*

Démonstration. La propriété (ii) résulte immédiatement du fait que d appartient à l'idéal (a, b), et de la description de cet idéal donnée en (II.4.5).

Montrons (i). D'abord d divise a : en effet a appartient à l'idéal $(a, b) = (d)$. De même d divise b.

Soit δ un diviseur commun de a et b : il faut montrer que $\delta | d$. Or on a $d = au + bv$ avec u et v dans A : comme δ divise a et b il divise aussi $au + bv$, d'où la conclusion. ∎

2.7.1. *Exercice.* Généraliser 2.7 à une famille quelconque d'éléments de A (dans le cas d'une famille infinie, on fera attention à la formulation de l'analogue de la condition (ii)).

Définition 2.8 *Soit $(a_i)_{i \in I}$ une famille d'éléments d'un anneau intègre A. On dit que les a_i sont* premiers entre eux *si 1 est un PGCD des a_i.*

2.8.1. En d'autres termes, les a_i sont premiers entre eux si et seulement si *tout diviseur commun des a_i est inversible* (vérifiez !).

2.8.2. Il résulte de 2.7 que pour que deux éléments a et b soient premiers entre eux, il *suffit* que l'idéal (a, b) soit égal à A, c'est-à-dire qu'il existe u et v dans A tels que $ua + vb = 1$.

Cette condition n'est cependant pas nécessaire, comme le montre l'exemple suivant :

2.8.3. *Exemple.* Dans l'anneau $A = \mathbb{Z}[X]$ des polynômes en une indéterminée X à coefficients entiers, les éléments 2 et X sont premiers entre eux : en fait les seuls diviseurs de 2 sont ± 1 et ± 2, et les seuls diviseurs de X sont ± 1 et $\pm X$, de sorte que les seuls diviseurs communs sont 1 et -1. Cependant il n'existe pas de polynômes $U, V \in \mathbb{Z}[X]$ tels que $2U + XV = 1$: il est immédiat, en effet, que tout polynôme de la forme $2U + XV$ a son terme constant *pair*.

Noter que ce raisonnement, joint à la proposition 2.7, montre que l'idéal $(2, X)$ de $\mathbb{Z}[X]$ n'est pas principal.

2.8.4. *Exercice.* Soit A l'anneau de 1.2.5 et 1.3.2. Pour f et $g \in A$, montrer que f et g sont premiers entre eux si et seulement si f et g n'ont aucun zéro commun dans U.

Définition 2.9 *Un élément a d'un anneau intègre A est dit* irréductible *s'il vérifie les propriétés suivantes :*

(i) *$a \neq 0$;*

(ii) *a n'est pas inversible ;*

(iii) *tout diviseur de a est soit inversible, soit associé à a.*

2.9.1. *Remarque.* Ne pas oublier les conditions (i) et (ii) de la définition.

2.9.2. *Remarque.* (démonstrations laissées en exercice) Si (i) et (ii) sont vérifiées, la condition (iii) peut se reformuler en disant que *pour tout $x \in A$, ou bien a divise x, ou bien a et x sont premiers entre eux.*

Si l'on suppose seulement que $a \neq 0$ alors a est irréductible si et seulement si la condition suivante est réalisée : pour tous $x, y \in A$ tels que $a = xy$, *un et un seul* des deux éléments x et y est inversible, l'autre étant associé à a.

2.9.3. *Remarque.* Il n'est peut-être pas inutile de préciser ce qu'est un élément *réductible* (c'est-à-dire non irréductible) : $a \in A$ est réductible si et seulement si :

- ou bien $a = 0$;
- ou bien a est inversible ;
- ou bien a est produit de deux éléments non inversibles de A.

(On peut remplacer la troisième condition par "a est produit de deux éléments de A non associés à a").

2.9.4. *Remarque.* Une démonstration "laissée en exercice" n'est pas pour autant facultative.

2.9.5. *Exemple.* Un entier n est irréductible dans $\mathbb{Z}$ si et seulement si $|n|$ est premier.

2.9.6. *Exemple.* Si A est un corps, il n'existe aucun élément irréductible dans A.

2.9.7. *Exercice.* Soit A l'anneau de 1.2.5, 1.3.2 et 2.8.4. Montrer qu'un élément f de A est irréductible si et seulement si f admet dans U un unique zéro et si de plus ce zéro est simple. De façon équivalente, les irréductibles de A sont, à association près, les fonctions de la forme $f(z) = z - a$, avec $a \in U$.

2.9.8. *Remarque.* Si A est un sous-anneau d'un anneau intègre B, un élément irréductible (resp. réductible) dans A ne le reste pas nécessairement dans B. On méditera les exemples suivants :

- 2 est irréductible dans $\mathbb{Z}$ mais pas dans $\mathbb{Q}$;
- $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$;
- $2X$ est réductible dans $\mathbb{Z}[X]$ mais pas dans $\mathbb{Q}[X]$.

3. Anneaux principaux et euclidiens

Définition 3.1 *Un anneau A est dit* principal *si A est* intègre *et si tout idéal de A est principal.*

3.1.1. *Exemples.* Tout corps est (trivialement) un anneau principal, les seuls idéaux étant engendrés respectivement par 0 et 1.

$\mathbb{Z}$ est un anneau principal, comme nous le savons depuis longtemps (I.3.6).

La définition ci-dessous, jointe à la proposition qui la suit, permet d'obtenir d'autres exemples :

Définition 3.2
(1) *Soit A un anneau intègre. On appelle* jauge euclidienne *sur A toute application*

$$\varphi : A \longrightarrow \mathbb{N}$$

avec la propriété suivante ("division euclidienne") *:*

Pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe q et r dans A tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$.
(2) *Un anneau A est dit* euclidien *si A est intègre et s'il existe une jauge euclidienne sur A.*

3.2.1. *Exercice.* Si φ est une jauge euclidienne sur A, montrer que le minimum de $\varphi(x)$ pour $x \in A$ est atteint pour $x = 0$, et seulement pour $x = 0$. (Appliquer la division euclidienne en prenant $b \in A - \{0\}$ tel que $\varphi(b)$ soit minimal).

3.2.2. *Remarque.* Aucune condition d'unicité n'est imposée sur q et r.

3.2.3. *Exemple.* $\mathbb{Z}$ est euclidien : en effet $\varphi(n) = |n|$ définit une jauge euclidienne sur $\mathbb{Z}$. On remarquera que même dans ce cas, il n'y a pas unicité de la division : par exemple pour $a = 1$ et $b = 2$, le couple (q, r) peut être pris égal à $(0, 1)$ (c'est la division euclidienne standard) mais aussi à $(1, -1)$.

3.2.4. *Exemple.* Si k est un corps, l'anneau $k[X]$ est euclidien (voir chapitre IV) : en effet, on a une jauge euclidienne $\varphi : k[X] \to \mathbb{N}$ définie par $\varphi(P) = 0$ si $P = 0$ et $\varphi(P) = 1 + \deg P$ si $P \neq 0$.

3.2.5. *Exercice.* Soit A l'anneau des *entiers de Gauss*, c'est-à-dire le sous-anneau de $\mathbb{C}$ formé des nombres complexes de la forme $x + iy$ avec x et y entiers. (C'est aussi le sous-anneau de $\mathbb{C}$ engendré par i, cf. II.1.10.3).

Montrer que $\varphi(z) = |z|^2$ définit une jauge euclidienne sur A.(Indication : pour $a \in A$ et $b \in A - \{0\}$, considérer le nombre complexe $w = a/b$, et montrer qu'il existe $q \in A$ tel que $|w - q| < 1$. On conseille de faire un dessin...)

3.2.6. *Exercice.* Soit φ une jauge euclidienne sur A. Définissons $\overline{\varphi} : A \to \mathbb{N}$ par

$$\overline{\varphi}(a) = \min_{x \in A^*} \varphi(ax).$$

(i) Montrer que $\overline{\varphi}(a) \leq \overline{\varphi}(ax)$ pour tous $a \in A$ et $x \in A^*$.

(ii) Montrer que $\overline{\varphi}$ est une jauge euclidienne sur A.

(iii) Soient a et $x \in A^*$. Montrer que $\overline{\varphi}(a) = \overline{\varphi}(ax)$ si et seulement si $x \in A^\times$.

Indication pour (ii) : pour faire la "$\overline{\varphi}$-division euclidienne" de a par b, choisir $x \in A^*$ tel que $\varphi(bx)$ soit minimum et faire la "φ-division euclidienne" de a par bx. Indication pour (iii) : la partie "si" résulte de (i) ; pour la réciproque, considérer la $\overline{\varphi}$-division euclidienne de a par ax.

L'intérêt de la notion d'anneau euclidien réside essentiellement dans la proposition suivante :

Proposition 3.3 *Soit A un anneau euclidien. Alors A est principal.*

De façon plus précise, soit $\varphi : A \longrightarrow \mathbb{N}$ une jauge euclidienne, et soit I un idéal non nul de A. Alors si $a \in I - \{0\}$ est tel que $\varphi(a) = \min_{x \in I - \{0\}} \varphi(x)$, on a $I = (a)$.

Démonstration. Il suffit de démontrer la dernière assertion : en effet, si J est un idéal quelconque de A, ou bien $J = \{0\}$ et J est engendré par 0, ou bien $J \neq \{0\}$ et l'ensemble des $\varphi(x)$ pour $x \in J - \{0\}$ admet un plus petit élément de sorte que la dernière assertion de l'énoncé s'applique.

Soient donc I et a comme dans l'énoncé. Il est clair que $(a) \subset I$ puisque $a \in I$. Montrons que $I \subset (a)$. Soit donc $x \in I$: d'après 3.2, il existe q et r dans A tels que $x = aq + r$ et $\varphi(r) < \varphi(a)$ (on utilise ici le fait que $a \neq 0$). Comme a et x sont dans I il en est de même de $r = x - aq$. Si r n'était pas nul, la propriété $\varphi(r) < \varphi(a)$ contredirait donc le choix de a. Par suite $r = 0$ et $x = aq \in (a)$, cqfd. ∎

4. Divisibilité dans les anneaux principaux

Dans tout ce paragraphe, A désigne un anneau *principal*.

4.1. *Existence des PPCM.* Si a et b sont deux éléments de A, alors a et b ont un PPCM (unique à association près, comme il se doit) : ceci résulte de 2.6.

4.2. *Existence des PGCD.* Si a et b sont deux éléments de A, alors a et b ont un PGCD d, unique à association près, et de plus il existe u et v dans A tels que $d = au + bv$ ("identité de Bézout"). Ceci résulte de 2.7.

4.3. En particulier les propositions 2.4 et 2.5 s'appliquent à tout anneau principal.

4.4. Plus généralement, *toute famille* d'éléments de A admet un PGCD et un PPCM.

4.5. Deux éléments a et b de A sont premiers entre eux si et seulement si il existe u et v dans A tels que $au + bv = 1$: ceci est un cas particulier de 4.2.

Proposition 4.6 ("lemme de Gauss") *Soient $a, b, c \in A$. On suppose que a divise bc et que a et b sont premiers entre eux. Alors a divise c.*

Démonstration. D'après 4.5 il existe u et v dans A tels que $au + bv = 1$. Multipliant par c on obtient $c = auc + bvc$. Comme a divise bc le second membre est divisible par a, d'où la conclusion. ∎

4.6.1. *Exercice.* Soient $a, b_1, \dots b_n \in A$. Montrer que pour que a soit premier avec $\prod_{i=1}^{n} b_i$, il faut et il suffit qu'il soit premier avec chacun des b_i.

En déduire que si a et $b \in A$ sont premiers entre eux, il en est de même de a^2 et b^2 (et plus généralement de a^m et b^n pour m et n entiers > 0). Pouvez-vous déduire cette propriété de la définition du PGCD ?

Corollaire 4.7 ("lemme d'Euclide") *Soient $p, b, c \in A$. On suppose que p est irréductible et divise bc. Alors p divise b ou p divise c.*

Démonstration. Si p ne divise pas b alors il est premier avec b (cf. 2.9.2), et l'on applique le lemme de Gauss. ∎

4.7.1. *Remarque.* On déduit immédiatement de 4.7 ou de 4.6.1 la propriété suivante : soient $a_1, \dots, a_n$ des éléments de A, et p un irréductible de A. Si p ne divise aucun des a_i, alors il est premier avec leur produit.

Corollaire 4.8 *Soient a et $b \in A$,* premiers entre eux. *Alors ab est un PPCM de a et b.*

Démonstration. Soit μ un multiple commun de a et b : alors $\mu = a\mu'$ avec $\mu' \in A$. Comme b divise $a\mu'$ et est premier avec a il divise μ' et donc ab divise $a\mu' = \mu$. ∎

La proposition suivante généralise II.3.3 :

Proposition 4.9 *Soient a un élément* non nul *de A. Pour tout $x \in A$ notons $\overline{x}$ la classe de x dans $A/(a)$. Alors, pour tout $x \in A$, les conditions suivantes sont équivalentes :*

(i) *$\overline{x}$ est inversible dans $A/(a)$;*

(ii) *$\overline{x}$ est régulier dans $A/(a)$;*

(iii) *a et x sont premiers entre eux dans A.*

Démonstration. (i)⇒(ii) est trivial.

Supposons (ii), et soit d un diviseur commun de a et x dans A. On a donc $a = da'$ et $x = dx'$ pour a' et $x' \in A$ convenables. Donc a divise $a'x$, c'est-à-dire $\overline{a'}\,\overline{x} = 0$ dans $A/(a)$. Vu l'hypothèse (ii), ceci entraîne que $\overline{a'} = 0$, donc $a = da'$ divise a' et d est inversible, d'où (iii).

Enfin si (iii) est vérifiée, il existe u et v dans A tels que $ua + vx = 1$, d'où $\overline{v}\,\overline{x} = 1$ dans $A/(a)$, d'où (i). ∎

On en tire la généralisation de II.3.6 aux anneaux principaux, avec une démonstration entièrement analogue :

Corollaire 4.9.1 *Soit a un élément non nul de A. Les conditions suivantes sont équivalentes :*

(i) *l'anneau $A/(a)$ est un corps ;*

(ii) *l'anneau $A/(a)$ est intègre ;*

(iii) *a est irréductible.* ∎

4.10. *Le lemme chinois.* Soient a et b deux éléments de A. On dispose alors d'un morphisme naturel d'anneaux :

$$\begin{array}{rccccc} \varphi_{a,b}: & A & \longrightarrow & A/(a) & \times & A/(b) \\ & x & \longmapsto & (x \bmod a & , & x \bmod b). \end{array}$$

Proposition 4.11 ("lemme chinois") *Gardons les notations de* 4.10 *et notons m un PPCM de a et b. On a les propriétés suivantes :*

(1) $\operatorname{Ker} \varphi_{a,b} = (m)$.

(2) *Supposons de plus que a et b soient* premiers entre eux *dans A. Alors :*

(i) $\operatorname{Ker} \varphi_{a,b} = (ab)$ *;*

(ii) $\varphi_{a,b}$ *est* surjectif *;*

(iii) $\varphi_{a,b}$ *induit par passage au quotient un isomorphisme d'anneaux*

$$\begin{array}{ccccc} A/(ab) & \xrightarrow{\sim} & A/(a) & \times & A/(b) \\ x \bmod ab & \longmapsto & (x \bmod a & , & x \bmod b). \end{array}$$

Démonstration. La définition de $\varphi_{a,b}$ donne immédiatement $\operatorname{Ker} \varphi_{a,b} = (a) \cap (b)$, de sorte que l'assertion (1) résulte trivialement de la définition du PPCM. La partie (i) de (2) s'en déduit compte tenu de 4.8. D'autre part (iii) est conséquence de (i) et (ii) d'après (II.5.5).

Il reste à prouver (ii) (sans utiliser (iii) !). Cela revient à montrer que, pour α et $\beta \in A$ quelconques, il existe $x \in A$ tel que l'on ait simultanément

$$\begin{cases} x \equiv \alpha \pmod{a} \\ x \equiv \beta \pmod{b}. \end{cases} \tag{4.11.1}$$

Or on sait qu'il existe u et v dans A tels que $ua + vb = 1$. On a donc

$$\begin{cases} ua \equiv 0 \pmod{a} \\ ua \equiv 1 \pmod{b} \end{cases} \qquad \begin{cases} vb \equiv 1 \pmod{a} \\ vb \equiv 0 \pmod{b}. \end{cases}$$

de sorte que $x_0 = ua\beta + vb\alpha$ est bien solution de (4.11.1). ∎

4.11.1. *Remarque.* Il résulte de (2)(i) (ou (iii)) que l'ensemble des solutions de (4.11.1) est $x_0 + abA$.

4.11.2. *Remarque.* La démonstration ci-dessus fournit une méthode effective de résolution d'un système de congruences tel que (4.11.1), une fois trouvés u et v vérifiant $ua + vb = 1$.

5. Décomposition en irréductibles

Nous allons dans ce paragraphe généraliser aux anneaux principaux la propriété bien connue de décomposition des nombres entiers en facteurs premiers. Pour formuler commodément l'unicité de cette décomposition, nous aurons besoin d'une définition :

Définition 5.1 *Soit A un anneau intègre. Un* système représentatif d'irréductibles *(en abrégé SRI) de A est une partie Σ de A vérifiant les propriétés suivantes :*

(i) *les éléments de Σ sont* irréductibles *et deux à deux non associés* (ou, ce qui revient au même, deux à deux premiers entre eux) *;*

(ii) *tout élément irréductible de A est associé à un élément de Σ* (qui est unique, d'après (i)).

5.1.1. *Exemple.* Dans $\mathbb{Z}$, l'ensemble des nombres premiers (c'est-à-dire des irréductibles positifs) est un SRI. L'ensemble de leurs opposés en est un autre.

5.1.2. *Exemple.* Soit k un corps et soit $A = k[X]$. L'ensemble des polynômes $P \in A$ qui sont irréductibles et *unitaires* (c'est-à-dire dont le coefficient dominant est égal à 1, cf. chapitre IV) est un SRI de A.

5.1.3. *Exemple.* Si A est un corps, l'ensemble vide est l'unique SRI de A.

5.1.4. *Remarque.* Il est clair que si Σ est un SRI, on en obtient un autre en multipliant chaque élément de Σ par un inversible arbitraire. En fait tous les SRI sont de cette forme : de façon précise (exercice) si Σ et Σ' sont deux SRI de A il existe une unique bijection $f : \Sigma \to \Sigma'$ telle que, pour tout $p \in \Sigma$, $f(p)$ soit associé à p.

5.1.5. *Remarque.* On peut montrer (à l'aide de l'axiome du choix) que tout anneau intègre admet un SRI.

5.1.6. *Exercice.* Peut-il arriver que A admette un SRI et un seul ? Peut-il arriver que l'ensemble des irréductibles de A soit un SRI ?

Théorème 5.2 *Soient A un anneau* principal*, et soit Σ un SRI de A. Alors tout élément x* non nul *de A peut s'écrire de façon unique sous la forme*

$$x = u \prod_{p \in \Sigma} p^{e_p} \tag{5.2.1}$$

où $u \in A^\times$ et où les e_p sont des entiers naturels presque tous nuls *(i.e. nuls sauf un nombre fini).*

5.3. *Avez-vous compris l'énoncé ?* Pour tout nombre premier p, posons $\hat{p} = 2$ si $p = 2$ et $\hat{p} = (-1)^{\frac{p-1}{2}} p$ sinon. Quels sont les nombres premiers p tels que $\hat{p} = p$? Montrer que l'ensemble Σ des entiers de la forme $\hat{p}$ est un SRI de $\mathbb{Z}$. Lorsque l'on écrit la décomposition (5.2.1) avec $A = \mathbb{Z}$, Σ comme on vient de le définir, et $x = -12870$, quelle est la valeur de u ?

5.4. *Démonstration de* 5.2 *: unicité.* Soit $x \in A^*$, supposé décomposé comme en (5.2.1). Pour montrer l'unicité de la décomposition, il suffit de voir que pour chaque $p \in \Sigma$, l'exposant e_p est déterminé par x et p (en effet u se déduit de x, des e_p et de la formule 5.2.1). Or on a plus précisément :

Lemme 5.4.1 *Soit $x \in A$ décomposé comme en* (5.2.1)*, et soit $p \in \Sigma$. Alors on a*

$$e_p = \max\{i \in \mathbb{N} \mid p^i \text{ divise } x\}.$$

Démonstration. On a la formule $x = p^{e_p} y$ avec $y = u \prod_{q \in \Sigma - \{p\}} q^{e_q}$. Il est donc clair que p^{e_p} divise x et il reste à voir que si $i > e_p$ alors p^i ne divise pas x. Or si $p^i | x$ on trouve en simplifiant $p^{i-e_p} | y$ et en particulier $p | y$. Mais ceci contredit le lemme d'Euclide, ou plutôt sa variante 4.7.1, puisque y est produit d'éléments non divisibles par p (on utilise ici le fait que Σ est un SRI). ∎

5.5. *Démonstration de* 5.2 *: existence.* Elle repose sur le lemme suivant :

Lemme 5.5.1 *Soit A un anneau principal, et soit T une partie non vide de A. Alors il existe un élément t de T qui est "minimal" au sens suivant : pour tout $y \in T$, si $y | t$ alors y est associé à t.* ∎

Nous admettrons ce lemme dans le cas général (sa démonstration utilise l'axiome du choix, bien que ce fait soit escamoté dans certains ouvrages). Dans les cas les plus utiles cependant, la démonstration est un exercice très facile :

- si $A = \mathbb{Z}$, considérer un élément de T de valeur absolue minimale ;
- si $A = k[X]$, où k est un corps, considérer un élément de T de degré minimal.

5.5.2. *Exercice.* Montrer plus généralement 5.5.1 lorsque A est euclidien. (Indication : choisir une "bonne" jauge euclidienne φ en utilisant 3.2.6, et prendre un élément t de T qui minimise φ.)

5.5.3. *Remarque.* Une formulation équivalente du lemme 5.5.1 est la suivante : dans un anneau principal, toute famille non vide d'idéaux admet un élément maximal (pour l'inclusion).

5.5.4. Revenant à 5.2, considérons l'ensemble D des éléments non nuls de A qui admettent une décomposition (5.2.1). Il s'agit de montrer que $D = A^*$. Commençons par remarquer que D a les propriétés suivantes :

- $A^\times \subset D$: en effet tout inversible admet une décomposition du type (5.2.1), où tous les e_p sont nuls ;
- $\Sigma \subset D$: en effet, tout élément p_0 de Σ admet une décomposition (5.2.1) avec $u = 1$, $e_{p_0} = 1$ et $e_p = 0$ pour tout $p \neq p_0$.
- D est stable par multiplication (immédiat) ;
- tout élément irréductible de A appartient à D : ceci résulte des propriétés précédentes puisque tout irréductible est produit d'un inversible par un élément de Σ.

Soit alors T le complémentaire de D dans A^* ; il s'agit de voir que T est vide. Raisonnons par l'absurde : si T n'est pas vide soit $t \in T$ comme dans le lemme 5.5.1. Alors $t \neq 0$ et, d'après les propriétés de D énoncées précédemment, t n'est ni inversible, ni irréductible, et il existe donc y et $z \in A$, *non associés à* t, tels que $t = yz$ (ceci résulte de la définition d'un irréductible). Vu le choix "minimal" de t, on a donc $y \notin T$ et $z \notin T$. Donc y et z appartiennent à D et il en est donc de même de leur produit t, contradiction. ■

6. Décomposition en irréductibles : propriétés et applications

Dans tout ce paragraphe, A désigne un anneau principal.

Définition 6.1 *Soit p un élément irréductible de A. Pour tout $x \in A$, on pose*

$$v_p(x) = \sup\{i \in \mathbb{N} \mid p^i \text{ divise } x\} \quad \in \mathbb{N} \cup \{+\infty\}.$$

L'application $v_p : A \to \mathbb{N} \cup \{+\infty\}$ est appelée la valuation *associée à p.*

Dans cette définition, il faut comprendre $+\infty$ comme un symbole arbitraire (n'importe quel objet mathématique fait l'affaire pourvu que ce ne soit pas un nombre), la relation d'ordre et l'addition sur $\mathbb{N}$ étant étendues à l'ensemble $\mathbb{N} \cup \{+\infty\}$ par les règles habituelles, à savoir : $+\infty > n$ pour $n \in \mathbb{N}$; $+\infty + x = +\infty$ pour $x \in \mathbb{N} \cup \{+\infty\}$.

6.2. *Propriétés de la valuation.*

6.2.1. Si p et p' sont deux irréductibles *associés*, alors $v_p = v_{p'}$: en effet, pour $i \in \mathbb{N}$, la condition "$p^i|x$" est équivalente à "$(p')^i|x$". En d'autres termes, la valuation v_p ne dépend que de l'idéal (p).

6.2.2. On a $v_p(0) = +\infty$; $v_p(p) = 1$; $v_p(x) = 0$ si et seulement si x n'est pas divisible par p.

6.2.3. *Lien avec la décomposition.* Il est fourni par le lemme 5.4.1 : si Σ est un SRI de A et si $x \in A^*$, alors, pour tout $p \in \Sigma$, $v_p(x)$ est *l'exposant de p* dans la décomposition de x associée à Σ.

En particulier (ce qui n'était pas évident a priori), $v_p(x)$ est *fini* pour tout $x \in A^*$. Cette propriété résulte donc du théorème de décomposition ; en fait c'est un bon exercice de la déduire directement du lemme 5.5.1 (indication : si $x \in A$ est divisible par p^i pour tout $i \in \mathbb{N}$, poser $x = p^i x_i$ et appliquer 5.5.1 à l'ensemble des x_i).

6.2.4. De même l'existence de la décomposition implique que, pour $x \neq 0$, l'ensemble des $p \in \Sigma$ tels que $p|x$ est *fini*, et aussi que tout élément non inversible de A est divisible par au moins un irréductible.

6.2.5. Une conséquence de ce qui précède est qu'un anneau principal qui n'est pas un corps admet au moins un irréductible ; curieusement, cette propriété n'était nullement évidente a priori, et je doute que l'on puisse la démontrer sans l'axiome du choix.

Les propriétés qui suivent se déduisent soit du théorème de décomposition, soit directement de la définition de v_p :

6.2.6. Pour tous x et $y \in A$, et pour tout $p \in A$ irréductible, on a (avec les conventions évidentes si l'un des termes est infini)

$$\begin{array}{lrcl} \text{(i)} & v_p(xy) & = & v_p(x) + v_p(y) \\ \text{(ii)} & v_p(x+y) & \geq & \min\{v_p(x), v_p(y)\} \\ \text{(iii)} & v_p(\text{PGCD}\,(x,y)) & = & \min\{v_p(x), v_p(y)\} \\ \text{(iv)} & v_p(\text{PPCM}\,(x,y)) & = & \max\{v_p(x), v_p(y)\} \\ \text{(v)} & x|y & \Leftrightarrow & \text{pour tout } q \in A \text{ irréductible, } v_q(x) \leq v_q(y). \end{array}$$

et de plus, dans la seconde formule, l'égalité a lieu si (mais pas seulement si) $v_p(x) \neq v_p(y)$.

6.2.7. On déduit des formules (i), (iii) et (iv) ci-dessus la relation

$$\text{PGCD}\,(x,y)\ \text{PPCM}\,(x,y) = xy$$

(ici encore, elle s'entend à association près), dont 4.8 est un cas particulier.

Cette relation peut s'obtenir autrement (cf. 2.5.1), mais les propriétés 6.2.6 la rendent particulièrement facile à démontrer.

6.3. *Exercice.* Un élément non nul a de A est dit *sans facteur carré* si $v_p(a) \leq 1$ pour tout p irréductible dans A. Montrer que les conditions suivantes sont équivalentes :

(i) a est sans facteur carré ;

(ii) l'anneau $A/(a)$ est isomorphe à un produit de corps ;

(iii) l'anneau $A/(a)$ est *réduit*, c'est-à-dire ne contient aucun élément nilpotent non nul.

(Indication : utiliser 5.2 et le lemme chinois).

6.4. *Exercice.* Essayer de redémontrer les résultats du paragraphe 4, jusqu'à 4.8 inclus, en utilisant uniquement la décomposition en irréductibles.

(Si certains de ces résultats résistent, voici une indication : le théorème de décomposition 5.2 est valable dans certains anneaux non principaux, comme par exemple $\mathbb{Z}[X]$.)

7. Le cas de $\mathbb{Z}$: nombres premiers

Ce paragraphe est consacré à quelques propriétés de l'ensemble des nombres premiers (c'est-à-dire des irréductibles positifs de $\mathbb{Z}$).

Théorème 7.1 (Euclide) *L'ensemble des nombres premiers est infini.*

Démonstration. (Vous la connaissez, bien sûr). Il suffit de trouver, pour tout ensemble *fini* S de nombres premiers, un nombre premier qui n'appartient pas à S. Or considérons l'entier $N = 1 + \prod_{p\in S} p$. Alors $N > 1$ (pourquoi ?) donc N a un diviseur premier q (pourquoi ?) lequel ne peut appartenir à S (pourquoi ?), cqfd (sûr ?). ∎

7.2. Voici quelques exercices sur le même thème :

7.2.1. Pour tout entier naturel m (avec une petite restriction *que l'on précisera*), montrer qu'il existe une infinité de nombres premiers p qui ne sont pas congrus à 1 modulo m (Indication : si S est un ensemble fini de nombres premiers, considérer les diviseurs premiers de $N = -1 + m\prod_{p\in S} p$).

7.2.2. Montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv -1 \pmod 6$.

7.2.3. Montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv -1 \pmod 4$.

7.2.4. Montrer qu'il existe une infinité de nombres premiers p congrus à 1 modulo 4. (Indication : si S est un ensemble fini de nombres premiers, considérer les diviseurs premiers de $N = 1 + \left(\prod_{p\in S} p\right)^2$ et utiliser II.3.9).

7.2.5. Soient n et d deux entiers. On suppose qu'il existe une infinité de nombres premiers p congrus à d modulo n. Montrer que d et n sont premiers entre eux.

7.2.6. *Remarque.* On peut montrer (théorème de Dirichlet, ou "théorème de la progression arithmétique") que la réciproque de 7.2.5 est vraie : si n et d sont deux entiers premiers entre eux, il existe une infinité de nombres premiers, de la forme $an + d$ avec $a \in \mathbb{Z}$. Les exercices 7.2.1 à 7.2.4 sont naturellement des cas particuliers de ce théorème. En voici un autre qui sera généralisé plus tard au cas d'un entier l non nécessairement premier, cf. IV.9.9.8) :

7.2.7. Soit l un nombre premier. Pour tout anneau A, on considère le polynôme $\Phi_A = \sum_{i=0}^{l-1} X^i \in A[X]$ (on anticipe sur la définition des polynômes à coefficients dans un anneau, pour laquelle on renvoie au début du chapitre IV). On remarquera que $(X-1)\Phi_A = X^l - 1$.

(i) Soit k un corps de caractéristique différente de l. Montrer que les racines de Φ_k dans k sont les éléments d'ordre l du groupe $k^\times$. Que se passe-t-il en caractéristique l ?

(ii) Soit N un entier, et soit p un diviseur premier de $\Phi_{\mathbb{Z}}(N)$. Montrer que p ne divise pas N, et que $\Phi_{\mathbb{F}_p}$ a une racine dans $\mathbb{F}_p$. En particulier, si N est divisible par l, déduire de (i) que $p \equiv 1 \pmod{l}$.

(iii) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo l.

7.3. *Exercice.* Si $(p_n)_{n\geq 1}$ désigne la suite des nombres premiers, montrer que la série de terme général $1/p_n$ est divergente.

Indications : si Log désigne le logarithme népérien, il suffit de voir, compte tenu de l'équivalence $1/p_n \sim -\mathrm{Log}\,(1-1/p_n)$, que le produit infini $\prod_{n-1}^{\infty}(1-1/p_n)^{-1}$ diverge. Si l'on écrit $(1-1/p_n)^{-1} = \sum_{k=0}^{\infty} p_n^{-k}$ et que l'on développe le produit, on trouve une série dont les termes sont les inverses de tous les produits finis de la forme $p_{i_1}^{k_1}\cdots p_{i_r}^{k_r}$, c'est-à-dire les inverses de tous les entiers naturels. Conclure par la divergence de la série harmonique.

Il va sans dire (?) que les arguments ci-dessus doivent être soigneusement justifiés pour prétendre au statut de démonstration. De plus, convenablement formulés (c'est-à-dire en considérant uniquement des sommes et des produits finis), ils sont valables sans supposer l'existence d'une infinité de nombres premiers, et donnent donc une autre démonstration de 7.1 (et bien plus : on voit par exemple qu'en un sens précis, les nombres premiers sont bien moins rares que les carrés).

7.3.1. *Remarque.* Démontrer 7.1 par la méthode de 7.3 peut paraître bizarrement artificiel. C'est pourtant par des méthodes analytiques de ce genre que Dirichlet a prouvé le théorème de la progression arithmétique (7.2.6), et non par des arguments du type de ceux de 7.2.1.

7.3.2. *Remarque.* C'est aussi par des méthodes analytiques que Hadamard et de la Vallée Poussin ont démontré (indépendamment) le célèbre "théorème des nombres premiers" : si, pour tout réel x, on désigne par $\pi(x)$ le nombre de nombres premiers $\leq x$, alors $\pi(x)$ est équivalent à $x/\mathrm{Log}\,x$ quand x tend vers $+\infty$. (On en déduit facilement que $p_n \sim n\mathrm{Log}\,n$ quand $n \to +\infty$, avec la notation de 7.3).

8. Application : structure du corps des fractions d'un anneau principal

Dans tout ce paragraphe on désigne par A un anneau principal, par K son corps des fractions, et par Σ un SRI (cf. 5.1) de A. Commençons par un énoncé qui n'utilise pas Σ :

Proposition 8.1 *Soit x un élément de K : alors il existe $a \in A$ et $b \in A^*$* premiers entre eux *et tels que $x = a/b$.*

De plus cette écriture est "presque unique" au sens suivant : si $a' \in A$ et $b' \in A^*$ sont premiers entre eux et vérifient encore $x = a'/b'$, alors il existe $u \in A^\times$ tel que $a' = ua$ et $b' = ub$.

Démonstration. Soient $\alpha \in A$ et $\beta \in A^*$ tels que $x = \alpha/\beta$, et soit d un PGCD de α et β : on peut alors écrire $\alpha = da$ et $\beta = db$ avec $a \in A$ et $b \in A^*$, et il résulte de 2.5(ii) que $d = d\,\mathrm{PGCD}(a, b)$ donc que a et b sont premiers entre eux, d'où l'assertion puisqu'il est clair que $a/b = \alpha/\beta = x$. (On a utilisé uniquement l'existence des PGCD dans A).

Montrons l'assertion d'unicité : de l'égalité $a/b = a'/b'$ on déduit $ab' = ba'$ donc b divise b' et b' divise b vu les hypothèses et le lemme de Gauss, donc b et b' sont associés. La fin de l'argument est laissée au lecteur. ∎

L'énoncé ci-dessus est déjà très utile (et bien connu pour $A = \mathbb{Z}$, j'espère). Si l'on utilise la décomposition en irréductibles on obtient un résultat bien plus précis :

Théorème 8.2 *Tout élément x* non nul *de K peut s'écrire de façon unique sous la forme*

$$x = u \prod_{p \in \Sigma} p^{e_p} \tag{8.2.1}$$

où $u \in A^\times$ et où les e_p sont des entiers relatifs presque tous nuls.

Démonstration. L'existence résulte de 5.2 et du fait que tout élément de K est quotient de deux éléments de A.

Montrons l'unicité : pour $x \in K^*$ donné, écrivons $x = a/b$ comme dans la proposition 8.1, et considérons d'autre part une écriture du type (8.2.1). Alors on a aussi $x = ua'/b'$ où a' (resp. b') est le produit des p^{e_p} pour $e_p > 0$ (resp. des p^{-e_p} pour $e_p < 0$). Il est clair que ua' et b' n'ont aucun diviseur irréductible commun donc sont premiers entre eux. Il résulte donc de l'assertion d'unicité de 8.1 que a' (resp. b') est associé à a (resp. à b), d'où l'unicité des exposants e_p (on a nécessairement $e_p = v_p(a)$ si $p \mid a$, et $e_p = -v_p(b)$ sinon). L'unicité de u en résulte trivialement. ∎

Chapitre IV

Polynômes

1. Définition et premières propriétés

1.1. Intuitivement, un polynôme (en une indéterminée) est une "expression" de la forme

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

où les a_i sont des "constantes" appelées *coefficients* de P, et où X est l'"indéterminée". Celle-ci est appelée parfois "variable", terme qu'il vaut mieux éviter car il suggère qu'un polynôme n'est qu'une fonction particulière. Or le "mode d'emploi" des polynômes veut notamment que deux polynômes soient égaux si *et seulement si* ils ont les mêmes coefficients (à condition d'oublier les coefficients nuls, par exemple $a + bX = a + bX + 0X^2$), et non s'ils définissent la même fonction (voir plus loin).

La "bonne" définition d'un polynôme est donc la suivante (qui précise aussi ce que sont les coefficients) :

Définition 1.2 *Soit A un anneau commutatif unitaire. Un polynôme (en une indéterminée X, à coefficients dans A), est une suite infinie, indexée par* $\mathbb{N}$

$$P = (a_0, a_1, \ldots, a_n, \ldots)$$

d'éléments de A presque tous nuls *(i.e. nuls à partir d'un certain rang, dépendant de P). L'ensemble de tous ces polynômes est noté $A[X]$.*

Si P est comme ci-dessus et si $Q = (b_0, b_1, \ldots, b_n, \ldots) \in A[X]$, leur somme *est le polynôme $P + Q = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$, et leur* produit *est le polynôme $P \times Q = PQ = (c_0, c_1, \ldots, c_n, \ldots)$ où les coefficients c_n sont définis par $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.*

1.3. *Remarques.*

1.3.1. Dans la définition ci-dessus, il faut naturellement vérifier que $P + Q$ et PQ

sont bien des polynômes, c'est-à-dire que leurs coefficients sont presque tous nuls.

1.3.2. L'indéterminée X n'apparaît pas dans la définition : nous allons voir ci-dessous ce qu'elle est.

1.3.3. Si l'anneau A est nul — et seulement dans ce cas — il en est de même de $A[X]$.

1.3.4. Si l'on reprend la définition de $A[X]$ lorsque A n'est plus nécessairement commutatif, on obtient encore un anneau (non nécessairement commutatif) ; il a cependant de bien moins bonnes propriétés que dans le cas commutatif, comme nous le verrons plus loin à propos des fonctions polynômes.

Proposition 1.4

(i) *$(A[X], +, \times)$ est un anneau commutatif unitaire.*

(ii) *L'application $a \mapsto (a, 0, 0, \ldots, 0, \ldots)$ est un morphisme injectif de A dans $A[X]$* (grâce à quoi on identifiera toujours A à un sous-anneau de $A[X]$, le polynôme "constant" $(a, 0, 0, \ldots, 0, \ldots)$ étant simplement noté a).

(iii) *Si l'on pose*

$$X := (0, 1, 0, \ldots, 0, \ldots)$$

alors pour toute suite finie $(a_0, a_1, \ldots, a_n)$ d'éléments de A on a dans $A[X]$ l'identité

$$\sum_{i=0}^{n} a_i X^i = (a_0, a_1, \ldots, a_n, 0, \ldots, 0, \ldots).$$

La démonstration, laissée au lecteur, consiste en des vérifications de routine à partir des définitions, dont la moins immédiate est l'associativité de la multiplication. Pour la dernière formule, on pourra traiter d'abord le cas où un seul des a_i (au plus) est non nul. ∎

1.5. *Remarques.*

1.5.1. L'indéterminée X est donc définie comme un polynôme particulier. Il est parfois nécessaire de lui donner un autre nom ; on convient dans ce cas de changer aussi le nom de l'anneau des polynômes, par exemple de noter celui-ci $A[Y]$ si l'indéterminée est baptisée Y.

1.5.2. L'élément unité de $A[X]$ est le polynôme $(1, 0, 0, \ldots)$: cette assertion fait partie de 1.4(ii) puisque les morphismes doivent respecter l'élément unité.

1.5.3. Dorénavant nous ne désignerons plus un polynôme par une notation telle que $(a_0, a_1, \ldots, a_n, 0, \ldots, 0, \ldots)$ mais par les notations traditionnelles $\sum_{i=0}^{n} a_i X^i$ ou $a_0 + a_1 X + \cdots + a_n X^n$, légitimées par (iii).

Définition 1.6 *Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On définit le* degré *de P, noté* $\deg P$, *par:*

$$\deg P = \begin{cases} -\infty & \text{si } P = 0 \ ; \\ \max\{i \in \mathbb{N} \mid a_i \neq 0\} & \text{si } P \neq 0. \end{cases}$$

Si $P \neq 0$ et si $\deg P = d$, a_d est appelé le coefficient dominant *de P, et $a_d X^d$ son* terme dominant. *On dit que P est* unitaire *si son coefficient dominant est égal à 1.*

Ici $-\infty$ est un symbole arbitraire, et l'on étend à $\mathbb{N} \cup \{-\infty\}$ la relation d'ordre et les opérations usuelles de $\mathbb{N}$ par les règles suivantes : $-\infty < n$ pour $n \in \mathbb{N}$; $-\infty + x = -\infty$ pour $x \in \mathbb{N} \cup \{-\infty\}$; $-\infty \times n = -\infty$ pour $n \in \mathbb{N}$ non nul ; $-\infty \times 0 = 0$.

Avec ces conventions, il est immédiat par exemple que l'on a

$$\deg(P + Q) \leq \max(\deg P, \deg Q)$$

pour tous P, Q dans $A[X]$ (et que l'on a égalité sauf si les termes dominants de P et Q existent et sont opposés). Pour les produits, tout vient du lemme suivant, dont la preuve est laissée au lecteur :

Lemme 1.7 *Soient P et $Q \in A[X]$, et m, n deux entiers naturels. On suppose que $P = a_m X^m +$ (termes de degré $< m$) et que $Q = b_n X^n +$ (termes de degré $< n$). Alors $PQ = a_m b_n X^{m+n} +$ (termes de degré $< m + n$).* ∎

Corollaire 1.8 *Soient P et $Q \in A[X]$. Alors*

$$\deg(PQ) \leq \deg(P) + \deg(Q).$$

Si l'on suppose de plus que P n'est pas nul et que son coefficient dominant est régulier *dans A, alors on a $\deg(PQ) \leq \deg(P) + \deg(Q)$, et P est régulier dans $A[X]$.*

Démonstration. La première assertion (et même l'égalité !) est triviale si P ou Q est nul, et sinon elle résulte de 1.7 en prenant pour m et n les degrés respectifs de P et Q. Il en va de même de la seconde assertion : en effet a_m est régulier et $b_n \neq 0$ donc $a_m b_n \neq 0$. La dernière assertion en est une conséquence. ∎

Corollaire 1.9 *On suppose que A est* intègre. *Alors :*

(i) *Pour P, $Q \in A[X]$ on a $\deg(PQ) = \deg(P) + \deg(Q)$.*

(ii) *$A[X]$ est intègre.*

(iii) *$A[X]^\times = A^\times$.*

Démonstration. L'assertion (i) est triviale si P ou Q est nul ; sinon elle résulte du corollaire 1.8.

L'assertion (ii) résulte de la seconde assertion de 1.8.

Montrons (iii). Il est clair que $A^\times \subset A[X]^\times$. Réciproquement, soit $P \in A[X]^\times$ et soit Q son inverse. Alors d'après (i) on a $\deg P + \deg Q = \deg 1 = 0$ ce qui n'est possible que si $\deg P = \deg Q = 0$, c'est-à-dire si P et Q appartiennent à A. Comme $PQ = 1$, on a donc bien $P \in A^\times$, cqfd. ∎

1.9.1. *Remarque.* L'assertion (i) est en défaut si A n'est pas intègre. En effet, si a et b sont deux éléments non nuls de A vérifiant $ab = 0$, alors $\deg(a) + \deg(b) = 0$ alors que $\deg(ab) = -\infty$. (Le lecteur trouvant que cet exemple repose sur la convention $\deg 0 = -\infty$ et n'est donc pas convaincant pourra en trouver d'autres).

1.9.2. Donnons aussi un contre-exemple à (iii) pour A non intègre. Supposons qu'il existe $a \neq 0$ dans A tel que $a^2 = 0$ (exemple : $A = \mathbb{Z}/4\mathbb{Z}$, $a = 2$). Alors le polynôme $1 + aX$ n'est pas constant puisque $a \neq 0$, et il est inversible puisque $(1 + aX)(1 - aX) = 1$.

1.9.3. *Exercice.* Généraliser la remarque précédente en montrant que si P est un polynôme dont le terme constant est inversible et dont tous les autres coefficients sont *nilpotents* (cf. II.3.2.7), alors $P \in A[X]^\times$.

La proposition suivante sera surtout utilisée lorsque A est un corps, cas (en principe) déjà connu du lecteur :

Proposition 1.10 *Soient F et $G \in A[X]$. On suppose que $G \neq 0$ et que le coefficient dominant de G est* inversible *dans A. Alors il existe Q et $R \in A[X]$ uniques tels que $F = GQ + R$ et $\deg R < \deg G$.*

Démonstration. Notons $u_d X^d$ le terme dominant de G (de sorte que $u_d \in A^\times$).

Montrons d'abord l'unicité. Si l'on a $F = GQ + R = GQ' + R'$ avec $\deg R < d$ et $\deg R' < d$, alors $0 = G(Q - Q') + (R - R')$. Appliquant 1.8, on a donc $d > \deg(R' - R) = \deg G + \deg(Q - Q') = d + \deg(Q - Q')$ d'où $\deg(Q - Q') < 0$, ce qui n'est possible que si $Q = Q'$, condition qui entraîne immédiatement $R = R'$.

L'existence est immédiate si $\deg F < d$ (prendre $Q = 0$ et $R = F$). Sinon, notons $a_n X^n$ le terme dominant de F (avec $n \geq d$). Alors le polynôme $F - a_n b_d^{-1} X^{n-d} G$ est de degré $< n$, d'où le résultat par récurrence sur n (et une méthode de calcul de Q et R). ∎

1.11. *Fonctions polynômes.* Si $P = \sum_{i=0}^n a_i X^i \in A[X]$, et si $x \in A$, on définit $P(x) \in A$ par la formule $P(x) = \sum_{i=0}^n a_i x^i$. On vérifie sans peine que, pour P,

$Q \in A[X]$ et $x \in A$, on a dans A les égalités

$$\begin{aligned} (P+Q)(x) &= P(x)+Q(x) \\ (PQ)(x) &= P(x)Q(x). \end{aligned} \tag{1.11.1}$$

(noter que la seconde formule "explique" la définition du produit dans $A[X]$, et qu'elle utilise la commutativité de A).

L'application $x \mapsto P(x)$ de A dans A que nous venons de définir est la *fonction polynôme* associée à P ; notons-la $\widetilde{P} : A \to A$. Si l'on note A^A l'ensemble de toutes les applications de A dans A, on a ainsi défini une application $P \mapsto \widetilde{P} : A[X] \to A^A$. Les formules 1.11.1 montrent que cette application est un *morphisme d'anneaux*, lorsque l'on munit A^A de sa structure naturelle d'anneau (où les fonctions sont additionnées et multipliées "point par point").

Le morphisme $P \mapsto \widetilde{P} : A[X] \to A^A$ n'est pas en général surjectif (il existe des fonctions non polynomiales, par exemple si $A = \mathbb{R}$). Mais il n'est pas toujours injectif non plus (autrement dit, la fonction polynôme ne détermine pas le polynôme, ce qui explique qu'on ne puisse pas définir les polynômes comme des fonctions). Par exemple, prenons $A = \mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier : alors le polynôme (non nul) $P = X^p - X$ vérifie $P(x) = 0$ pour tout $x \in A$, en vertu du théorème de Fermat (II.3.7). Plus généralement, ce phénomène se produit chaque fois que A est un anneau *fini* : considérer le polynôme $\prod_{x \in A}(X - x)$ (qui est unitaire, donc non nul dès que A n'est pas nul).

1.11.1. *Exercice.* Pour $a \in A$ *fixé*, on a en particulier un morphisme $\varepsilon_a : A[X] \to A$ donné par $\varepsilon_a(P) = P(a)$ ("évaluation au point a"). Montrer que ε_a est surjectif et que $\operatorname{Ker} \varepsilon_a$ est l'idéal de $A[X]$ engendré par $X - a$. En déduire un isomorphisme d'anneaux $A[X]/(X - a) \cong A$.

1.11.2. *Exercice.* On suppose que A est un *corps fini*. Montrer que toute application de A dans A est une fonction polynôme (autrement dit, le morphisme $P \mapsto \widetilde{P} : A[X] \to A^A$ est surjectif dans ce cas). (Indication : pour chaque $A \in A$, trouver un polynôme $P_a \in A[X]$ tel que $P_a(a) = 1$ et $P_a(x) = 0$ pour tout $x \neq a$).

2. Cas où l'anneau de base est un corps

Dans tout ce paragraphe on désigne par k un corps, et l'on se propose d'étudier l'anneau $k[X]$.

2.1. Il résulte déjà de 1.9 que $k[X]$ est intègre et que $k[X]^\times = k^\times = k^*$: les polynômes inversibles sont simplement les constantes non nulles.

Une conséquence très utile en est que tout polynôme non nul P à coefficients dans k est associé dans $k[X]$ à un unique polynôme *unitaire* : explicitement, $P = aP_1$ où P_1 est unitaire et où a est le coefficient dominant de P. En particulier, les questions de divisibilité dans $k[X]$ peuvent souvent se ramener au cas où les polynômes concernés sont unitaires.

2.2. Il est clair que $k[X]$ a une structure naturelle de k-espace vectoriel. Les idéaux de $k[X]$ en sont des sous-espaces mais il y en a d'autres, par exemple, pour $d \in \mathbb{N}$ donné, l'espace des polynômes de degré $\leq d$ (qui admet pour base $(X^i)_{0\leq i\leq d}$ donc est de dimension $d+1$). Noter que $k[X]$ lui-même est de dimension infinie : nous venons en effet de voir qu'il contient des sous-espaces de dimension arbitrairement grande. (Une autre façon de le prouver est de remarquer que $P \mapsto XP$ est un k-endomorphisme de $k[X]$ qui est injectif mais non surjectif.)

Proposition 2.3 (division euclidienne des polynômes). *Soient A et $B \in k[X]$, avec $B \neq 0$. Il existe alors Q et $R \in k[X]$ uniques tels que $A = BQ + R$ et $\deg R < \deg B$.*

Démonstration. C'est un cas particulier de 1.10. ∎

Corollaire 2.4 *$k[X]$ est un anneau euclidien* (cf. (III.3.2)), *et en particulier* principal, cf. (III.3.3). ∎

2.5. On peut donc appliquer à $k[X]$ les résultats généraux démontrés pour les anneaux principaux : existence de PPCM et PGCD (ces derniers se calculant par l'algorithme d'Euclide), lemmes de Gauss et d'Euclide, identité de Bézout, décomposition en produit d'irréductibles.

La division euclidienne dans $k[X]$ a une autre vertu apparemment banale mais riche de conséquences : c'est *l'invariance par extension du corps de base*. Nous appellerons provisoirement *extension* de k tout corps contenant k comme sous-corps (la "vraie" définition, un peu plus générale, sera donnée en 3.4 ; le lecteur vérifiera alors que les énoncés démontrés dans l'intervalle n'en sont pas affectés). Si L est une extension de k, alors, avec les notations de 2.3, la division euclidienne de A par B dans $L[X]$ donne le même quotient Q et le même reste R que dans $k[X]$. Comme par ailleurs B divise A dans $k[X]$ si et seulement si $R = 0$, on en tire :

Corollaire 2.6 *Soient F et $G \in k[X]$, et soit L une extension de k. Alors :*

(i) *Pour que F divise G dans $k[X]$, il faut et il suffit que F divise G dans $L[X]$.*

(ii) *Si D est un PGCD (resp. un PPCM) de F et G dans $k[X]$, c'est aussi un PGCD (resp. un PPCM) de F et G dans $L[X]$.*

(iii) *Pour que F et G soient premiers entre eux dans $k[X]$, il faut et il suffit qu'ils le soient dans $L[X]$.*

(iv) *Si F est irréductible dans $L[X]$, il l'est aussi dans $k[X]$.*

Démonstration : exercice. ∎

2.6.1. *Remarque.* Noter que dans (ii) la réciproque est vraie *à condition que D appartienne* à $k[X]$. D'autre part la réciproque de (iv) est évidemment fausse (prendre $k = \mathbb{R}$, $L = \mathbb{C}$ et $F = X^2 + 1$).

À propos de la décomposition en irréductibles, il résulte de 2.1 que l'ensemble des irréductibles *unitaires* est un système représentatif d'irréductibles de $k[X]$. Le théorème de décomposition III.5.2 peut donc être précisé comme suit :

Théorème 2.7 *Soit $I \subset k[X]$ l'ensemble des polynômes irréductibles unitaires. Tout $F \in k[X]$* non nul *peut s'écrire de façon unique*

$$F = a \prod_{P \in I} P^{v_P(F)}$$

où les $v_P(F)$ sont des entiers presque tous nuls, et où $a \in k^*$. De plus a est le coefficient dominant de F. ∎

(La dernière assertion s'obtient en comparant les coefficients dominants des deux membres).

2.8. *Remarques sur les irréductibles de $k[X]$.*

2.8.1. Du fait que $k[X]$ est principal il résulte aussi (III.4.9.1) que, si F est un polynôme non nul, alors F est irréductible si et seulement si $k[X]/(F)$ est un corps : ceci permet de construire des corps contenant un corps k donné, nous y reviendrons.

2.8.2. Il est clair que pour tout $\alpha \in k$, le polynôme (unitaire) $X - \alpha$ est irréductible. Dans ce cas le corps $k[X]/(X - \alpha)$ s'identifie à k, cf. 1.11.1. Plus généralement tout polynôme de degré 1 est irréductible. Il peut arriver que ce soient les seuls (par exemple si $k = \mathbb{C}$, cf. § 7), ou non : ainsi, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, et l'on verra bien d'autres exemples au § 8.

2.8.3. *Exercice.* Montrer que l'ensemble des polynômes irréductibles unitaires de $k[X]$ est infini, en s'inspirant de la démonstration d'Euclide pour l'ensemble des nombres premiers.

2.8.4. *Exercice.* Il résulte de la remarque 2.8.2 que l'exercice 2.8.3 est trivial si k est infini : l'argument d'Euclide, bien que correct, est inutile dans ce cas. Si k est *fini*, déduire de 2.8.3 qu'il existe dans $k[X]$ des polynômes irréductibles de degré arbitrairement grand.

(On peut même montrer, toujours pour k fini, que, pour *tout* entier $d \geq 1$, il existe dans $k[X]$ des polynômes irréductibles de degré d : en quoi cette assertion — qui relève de la "théorie de Galois" des corps finis — diffère-t-elle de la précédente ?)

2.8.5. *Exercice.* Soit L une extension de k, et soit $F \in k[X]$. Si F est irréductible dans $k[X]$, est-il irréductible dans $L[X]$? Et réciproquement ?

Définition 2.9 *Soit $F \in k[X]$ non nul. On dit que F est* décomposé *dans $k[X]$ si tous les diviseurs irréductibles de F sont de degré 1.*

En d'autres termes, d'après 2.7, F est décomposé dans $k[X]$ si et seulement si F est constant ou produit d'une constante par des polynômes de la forme $X - \alpha$ ($\alpha \in k$).

3. Algèbres sur un corps

k désigne un corps commutatif.

Définition 3.1 *Une* k-algèbre *est un quadruplet* $(A, +, ., *)$ *où* A *est un ensemble,* $+$ *et* $*$ *sont deux lois internes sur* A*, et* $. : k \times A \to A$ *est une loi externe, vérifiant les propriétés suivantes :*

(i) $(A, +, *)$ *est un anneau unitaire (non nécessairement commutatif) ;*

(ii) $(A, +, .)$ *est un* k*-espace vectoriel ;*

(iii) *la multiplication* $*$ $: A \times A \to A$ *est* k-bilinéaire *pour la structure d'espace vectoriel de* (ii).

Une k *algèbre* $(A, +, ., *)$ *est* commutative *si* $(A, +, *)$ *est un anneau commutatif, c'est-à-dire si* $*$ *est commutative.*

3.2. *Remarques.*

3.2.1. La condition (iii) équivaut à dire, compte tenu de (ii), que pour tous $x, y \in A$ et $\lambda \in k$, on a $\lambda.(x * y) = (\lambda.x) * y) = x * (\lambda.y)$ (la compatibilité de $*$ avec l'addition de A est déjà contenue dans la condition (i)). Bien entendu, vous avez vérifié tout ceci, après avoir revu les définitions de base de l'algèbre bilinéaire...

3.2.2. Si $(A, +, ., *)$ est une k-algèbre, l'application $\lambda \mapsto \lambda.1_A$ de k dans A est un morphisme d'anneaux unitaires, appelé *morphisme structural* de la k-algèbre. En vertu de la remarque précédente, les éléments de l'image de ce morphisme *commutent* avec tous les éléments de A.

Réciproquement, soient $(R, +, \times)$ un anneau unitaire et φ $: k \to R$ un morphisme d'anneaux unitaires. Alors on obtient sur R une structure de k-espace vectoriel en posant $\lambda.x = \varphi(\lambda) \times x$ pour $\lambda \in k$ et $x \in R$. Le lecteur ne manquera pas de vérifier que $(R, +, ., \times)$ est une k-algèbre si et seulement si $\varphi(\lambda) \times x = x \times \varphi(\lambda)$ pour tous $\lambda \in k$ et $x \in R$.

Ceci fournit une autre définition possible de la notion de k-algèbre : c'est un anneau unitaire A muni d'un morphisme $\varphi : k \to A$ qui est *central*, c'est-à-dire que les éléments de l'image de φ commutent avec tous les éléments de A.

3.2.3. En pratique, on note souvent la multiplication interne $*$ et la loi externe $.$ par juxtaposition : la condition (iii) de la définition devient ainsi équivalente à $\lambda(xy) = (\lambda x)y = x(\lambda y)$ pour $\lambda \in k$, $x \in A$, $y \in A$. On va même souvent jusqu'à écrire λ plutôt que $\lambda 1_A$, pour $\lambda \in k$: ceci est en général sans danger, du moins si $A \neq \{0\}$, puisqu'alors le morphisme $\lambda \mapsto \lambda 1_A$ est injectif, k étant un corps.

3.3. *Exemples de* k*-algèbres.*

3.3.1. *Exemples triviaux :* la k-algèbre nulle, la k-algèbre k.

3.3.2. Tout anneau commutatif unitaire contenant k comme sous-anneau unitaire est de façon naturelle une k-algèbre commutative.

3.3.3. $k[X]$ est une k-algèbre commutative.

3.3.4. Tout quotient d'une k-algèbre est une k-algèbre.

3.3.5. Tout produit de k-algèbres est une k-algèbre. (Dans cet exemple et les précédents, "est une k-algèbre" est un abus de langage pour "admet une structure naturelle de k-algèbre". Il va donc de soi que le lecteur est censé, pour vérifier ces assertions, définir la structure en question).

3.3.6. Si p est un nombre premier, tout anneau A de caractéristique p est de façon naturelle une $\mathbb{F}_p$-algèbre : le morphisme structural est l'unique morphisme de $\mathbb{F}_p$ dans A, et la structure de $\mathbb{F}_p$-espace vectoriel est celle de II.7.2.1. Cette structure d'algèbre est unique (i.e. c'est la seule compatible avec la structure d'anneau de A), et de plus tout morphisme d'anneaux de caractéristique p est un morphisme de $\mathbb{F}_p$-algèbres.

Cette propriété s'étend à tout anneau nul. Réciproquement, toute $\mathbb{F}_p$-algèbre A est soit nulle, soit de caractéristique p (car si $A \neq \{0\}$ le morphisme structural de $\mathbb{F}_p$ dans A est nécessairement injectif).

En résumé, une $\mathbb{F}_p$-algèbre est "la même chose" qu'un anneau nul ou de caractéristique p (c'est-à-dire un anneau A tel que $p1_A = 0$).

3.3.7. Si V est un k-espace vectoriel, $\mathrm{End}_k(V)$ est une k-algèbre, non commutative dès que $\dim_k(V) \geq 2$. Le morphisme φ de 3.2.2 associe à $\lambda \in k$ l'endomorphisme $\lambda \,\mathrm{Id}_V$ de V : noter que celui-ci commute bien avec tous les endomorphismes de V.

Définition 3.4 *Une* extension *de k est par définition une k-algèbre qui est un corps.*

Une extension L de k est dite de degré fini, *ou simplement* finie, *si L est un k-espace vectoriel de dimension finie ; sa dimension est alors appelée le* degré *de l'extension et est notée $[L : k]$.*

3.4.1. *Exemple.* $\mathbb{C}$ est une extension de degré 2 de $\mathbb{R}$ mais n'est pas une extension finie de $\mathbb{Q}$. Que peut-on dire des extensions de degré 0 de k ? des extensions de degré 1 ?

3.4.2. *Remarque.* Si L est une extension de k, alors l'anneau L n'est jamais nul de sorte que l'on ne risque rien en général à identifier k à un sous-corps de L. Le plus souvent (et par abus) nous considérerons donc comme synonymes les expressions "L est une extension de k" et "k est un sous-corps de L".

3.4.3. *Remarque.* Tout corps de caractéristique nulle est de manière unique une

extension de $\mathbb{Q}$; pour p premier, tout corps de caractéristique p est de manière unique une extension de $\mathbb{F}_p$.

3.4.4. *Exercice.* Soit L une extension de k, et soit V un L-espace vectoriel. Alors V admet une structure naturelle de k-espace vectoriel. Montrer que si L est une extension finie de k et si V est de dimension finie sur L, alors V est de dimension finie sur k et l'on a $\dim_k V = [L : k] \dim_L V$. (Indication : si $(\lambda_1, \ldots, \lambda_d)$ est une base de L sur k et $(v_1, \ldots, v_n)$ une base de V sur L, montrer que la famille $(\lambda_i v_j)_{1 \leq i \leq d, 1 \leq j \leq n}$ est une base de V sur k).

En déduire la formule de "transitivité" suivante : si L est une extension finie de k et M une extension finie de L, alors M est une extension finie de k et $[M : k] = [M : L][L : k]$.

(Ces formules, avec des conventions convenables, restent valables si certains des termes sont infinis).

3.4.5. *Exercice.* Soit A une k-algèbre commutative de dimension finie (comme k-espace vectoriel), et soit $a \in A$. Montrer que $a \in A^\times$ si et seulement si a est non-diviseur de zéro dans A. (Considérer la multiplication par a). Comparer cette propriété (et sa démonstration) avec II.3.2.5.

En déduire que *toute k-algèbre intègre de dimension finie est un corps.*

Définition 3.5 *Soient A et B deux k-algèbres. Un* morphisme *(ou homomorphisme) de k-algèbres de A dans B est une application $f : A \to B$ qui est à la fois un morphisme d'anneaux unitaires et un morphisme de k-espaces vectoriels (i.e. une application k-linéaire).*

On notera $\mathrm{Hom}_{k-\mathrm{alg}}(A, B)$ l'ensemble des morphismes de k-algèbres de A dans B.

3.5.1. *Remarque.* On peut aussi définir cette notion en termes des morphismes structuraux $\varphi : k \to A$ et $\psi : k \to B$ de A et B (cf. 3.2.2) : une application $f : A \to B$ est un morphisme de k-algèbres si et seulement si c'est un morphisme d'anneaux vérifiant $f \circ \varphi = \psi$ (exercice). Autrement dit, dans le langage de II.8.2, un morphisme de k-algèbres de A dans B n'est rien d'autre qu'un k-morphisme de (A, φ) dans (B, ψ).

3.5.2. *Exemples triviaux.* Si A est une k-algèbre, alors l'unique application de A vers la k-algèbre nulle, l'identité de A, le morphisme structural de k dans A, sont des morphismes de k-algèbres. Le composé de deux morphismes de k-algèbres est un morphisme de k-algèbres.

3.5.3. *Exercice.* Si A est une k-algèbre et $a \in A$ notons $\mu_a : A \to A$ la multiplication à gauche $x \mapsto ax$ par a. Alors l'application $a \mapsto \mu_a$ est un morphisme injectif de A

dans la k-algèbre $\mathrm{End}_k(A)$ des k-endomorphismes du k-espace vectoriel sous-jacent à A.

En particulier, si A est de dimension finie n comme k-espace vectoriel, A est isomorphe à une sous-k-algèbre de l'algèbre de matrices $\mathrm{M}_n(k)$. (On comparera cet argument avec I.5.4.5).

Lorsque $k = \mathbb{R}$ et $A = \mathbb{C}$, expliciter le morphisme de $\mathbb{C}$ dans $\mathrm{M}_2(\mathbb{R})$ obtenu.

3.5.4. *Sous-algèbres.* Une *sous-(k-)algèbre* d'une k-algèbre A est une partie de A qui est à la fois un sous-anneau (unitaire) et un sous-k-espace vectoriel. Une telle sous-algèbre B est de façon évidente une k-algèbre et l'application d'inclusion est un morphisme. L'intersection d'une famille quelconque de sous-algèbres est une sous-algèbre.

3.6. *Exemple de morphisme : l'évaluation.* Soient B une k-algèbre, b un élément de B, et $P = \sum_{i=0}^{n} a_i X^i \in k[X]$. On *définit* $P(b) \in B$ par la formule

$$P(b) = \sum_{i=0}^{n} a_i \, b^i.$$

(avec la convention habituelle $b^0 = 1_B$). On vérifie alors (exercice) que l'application $\varepsilon_b \ : k[X] \to B$ définie par

$$\varepsilon_b(P) = P(b)$$

est un morphisme de k-algèbres. (La vérification ne pose aucune difficulté en ce qui concerne la k-linéarité de ε_b, et le fait que $\varepsilon_b(1_{k[X]}) = 1_B$. Pour la multiplicativité, i.e. le fait que $(PQ)(b) = P(b)Q(b)$, on se ramène par linéarité au cas où $P = \alpha X^m$ et $Q = \beta X^n$ sont des monômes, et l'on utilise 3.2.1).

3.6.1. Noter que $\varepsilon_b(X) = b$; noter aussi que lorsque $B = k$ on retrouve le morphisme de 1.11.1, lié à la notion de fonction polynôme.

3.6.2. Prenons en particulier $B = k[X]$ et $b = X$: alors on obtient $\varepsilon_X(P) = P(X) = P$. Ceci permet de justifier la notation $P(X)$ pour un polynôme P en une indéterminée X, notation que nous avons — du moins je l'espère — évitée jusqu'ici.

Ce calcul montre, en d'autres termes, que

$$\varepsilon_X = \mathrm{Id}_{k[X]} : k[X] \longrightarrow k[X].$$

3.6.3. *Exercice.* Soit $f : C \to B$ un morphisme de k-algèbres, et soit $c \in C$. Montrer que $f \circ \varepsilon_c = \varepsilon_{f(c)}$.

3.6.4. Qu'obtient-on lorsque $B = \mathrm{End}_k(V)$ (cf. 3.3.7) ? (Revoir le cours d'algèbre linéaire, si ça ne vous dit rien...)

Proposition 3.7 (propriété universelle de $k[X]$). *Soient B une k-algèbre et $b \in B$. Il existe alors un unique morphisme de k-algèbres de $k[X]$ dans B envoyant X sur b, à savoir le morphisme ε_b d'évaluation en b de* 3.5.1.

Démonstration. On a déjà vu que ε_b vérifie les conditions requises. (Sûr ?) Il reste donc à voir que si $f : k[X] \to B$ est un morphisme de k-algèbres et si $b = f(X)$, alors $f = \varepsilon_b$. Or si $P = \sum_{i=0}^{n} a_i X^i \in k[X]$, on a $f(P) = f(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} a_i f(X^i)$ puisque f est k-linéaire, d'où $f(P) = \sum_{i=0}^{n} a_i b^i$ puisque $b = f(X)$ et que, f étant un morphisme d'anneaux unitaires, $f(X^i) = f(X)^i$. D'où $f(P) = P(b) = \varepsilon_b(P)$. ∎

(Tiens, au fait : a-t-on utilisé le fait que f respecte les éléments unités ?)

3.7.1. *Exercice.* Dans la démonstration ci-dessus, redémontrer l'identité $f = \varepsilon_b$ en remplaçant le calcul par une application de 3.6.2 et 3.6.3 (avec $C = A[X], c = X$).

3.8. *Remarques.*

3.8.1. La propriété universelle de 3.7 peut encore se reformuler comme suit : si B désigne une k-algèbre, il revient au même de se donner un élément b de B ou un morphisme f de k-algèbres de $k[X]$ dans B. Plus précisément, l'application $f \mapsto f(X)$ est une bijection de $\mathrm{Hom}_{k-\mathrm{alg}}(k[X], B)$ sur B, la bijection réciproque étant l'application $b \mapsto \varepsilon_b$.

3.8.2. Le lecteur méditera l'analogie avec la propriété universelle du groupe $\mathbb{Z}$ (I.2.3).

3.9. *Propriété universelle de $k[X]/(F)$.* Gardons les notations de 3.7.

3.9.1. Pour $b \in B$ donné, le noyau de ε_b est l'idéal de $k[X]$ formé des polynômes F vérifiant $F(b) = 0$. On en déduit les équivalences (pour $b \in B$ et $F \in k[X]$ donnés) :

$$\begin{aligned} F(b) = 0 \quad &\Leftrightarrow \quad (F) \subset \mathrm{Ker}\, \varepsilon_b \\ &\Leftrightarrow \quad \varepsilon_b \text{ se factorise par un morphisme de } k\text{-algèbres} \\ &\qquad\ \ \overline{\varepsilon}_b : k[X]/(F) \to B. \end{aligned}$$

3.9.2. Ceci suggère de considérer, pour $F \in k[X]$ donné et pour toute k-algèbre B, le sous-ensemble de B formé des "zéros de F dans B", c'est-à-dire des solutions dans B de l'équation $F(x) = 0$:

$$\mathrm{sol}(F, B) = \{x \in B \mid F(x) = 0\}.$$

(on réserve le mot "racines" au cas où B est un corps). Si $\varphi : B \to B'$ est un morphisme de k-algèbres, il est immédiat que $\varphi(\mathrm{sol}(F, B)) \subset \mathrm{sol}(F, B')$ puisque, pour $x \in B$, $F(\varphi(x)) = \varphi(F(x))$.

3.9.3. En particulier, notons A la k-algèbre $k[X]/(F)$, et notons $\omega \in A$ la classe de X. Alors $F(\omega)$ est la classe de $F(X)$ donc la classe de F, c'est-à-dire 0_A. Autrement

dit, $\omega \in \mathrm{sol}(F, A)$, et on a donc une application

$$\begin{array}{rccc} \alpha : & \mathrm{Hom}_{k-\mathrm{alg}}(k[X]/(F), B) & \longrightarrow & \mathrm{sol}(F, B) \\ & \varphi & \longmapsto & \varphi(\omega) = \varphi(X \bmod F). \end{array} \tag{3.9.3.1}$$

Proposition 3.9.4 *Avec les notations ci-dessus, l'application α de* (3.9.3.1) *est* bijective *; la bijection réciproque associe à $b \in \mathrm{sol}(F, B)$ l'unique morphisme de k-algèbres $\varphi : k[X]/(F) \to B$ vérifiant $\varphi(P \bmod F) = P(b)$ pour tout $P \in k[X]$.*

Démonstration. Gardons les notations $A = k[X]/(F)$, et $\omega = X \bmod F$ introduites plus haut ; notons de plus $\pi : k[X] \to A$ le morphisme surjectif canonique (on a en particulier $\omega = \pi(X)$).

Remarquons d'abord que si $\varphi : A \to B$ est un morphisme de k-algèbres, φ est entièrement déterminé par $\varphi \circ \pi : k[X] \to B$ puisque π est surjectif (c'est l'une des assertions de la propriété universelle du quotient). Or, d'après (3.7) $\varphi \circ \pi$ est lui-même déterminé par $\varphi \circ \pi(X) = \varphi(\omega)$. Ceci montre déjà que α est injective.

Il reste à voir que, pour tout $b \in \mathrm{sol}(F, B)$, il existe un morphisme de k-algèbres de A dans B envoyant ω sur b. Or nous avons remarqué en 3.9.1 que $\varepsilon_b : k[X] \to B$ passe au quotient par A. Ceci montre l'existence de $\overline{\varepsilon}_b : A \to B$ qui a la propriété voulue puisque $\overline{\varepsilon}_b(\omega) = \varepsilon_b(X) = b$. ∎

3.9.5. *Remarque.* Comparer avec la propriété universelle du groupe $\mathbb{Z}/n\mathbb{Z}$ (I.10.5).

3.9.6. *Remarque.* Ce qui précède justifie une étude approfondie des algèbres quotients de $k[X]$ puisqu'elles sont étroitement liées à la résolution d'équations polynômes. Cette étude sera abordée au paragraphe 4.

3.10. *Exercice : les polynômes comme "fonctions universelles".*

Un polynôme $P \in k[X]$ définit pour toute k-algèbre A une application $\widetilde{P}_A : A \to A$ par la formule $\widetilde{P}_A(x) = P(x)$.

3.10.1. Montrer que pour tout morphisme $f : A \to B$ de k-algèbres, on a $f \circ \widetilde{P}_A = \widetilde{P}_B \circ f$.

3.10.2. Montrer que $\widetilde{P}_{k[X]}(X) = P$.

3.10.3. En déduire que pour que deux polynômes $P, Q \in k[X]$ soient égaux il faut et il suffit que, pour *toute* k-algèbre A, on ait $\widetilde{P}_A = \widetilde{Q}_A$.

3.10.4. Supposons donnée, pour *toute* k-algèbre A, une application $\varphi_A : A \to A$, de telle sorte que l'on ait $f \circ \varphi_A = \varphi_B \circ f$ pour tout morphisme $f : A \to B$ de k-algèbres. Montrer alors qu'il existe un unique $P \in k[X]$ tel que $\varphi_A = \widetilde{P}_A$ pour toute k-algèbre A.

(Indications : trouver le seul candidat P possible à l'aide de 3.10.2. Vérifier ensuite qu'il satisfait bien à la propriété voulue, de la façon suivante : si A est

une k-algèbre et $x \in A$, pour voir que $\varphi_A(x) = P(x)$, considérer le morphisme $f = \varepsilon_x : k[X] \to A$.)

3.11. *Exercice.* Donner un exemple d'un corps k et :

(i) d'un sous-k-espace vectoriel de $k[X]$ qui n'est pas une sous-algèbre ;

(ii) d'un sous-anneau de $k[X]$ qui n'est pas une sous-algèbre.

De tels exemples existent-ils pour tout k ?

3.12. *Exercices : Sous-algèbre engendrée par une partie d'une k-algèbre.*

3.12.1. Si A est une k-algèbre et S une partie de A, montrer qu'il existe une plus petite sous-algèbre de A contenant S.

Cette sous-algèbre est par définition la *sous-algèbre de A engendrée par S*. Elle est souvent notée $k[S]$, notation dangereuse en raison du risque de confusion avec les algèbres de polynômes.

Quelle est la sous-algèbre de $k[X]$ engendrée par X ? (Il va sans dire qu'il s'agit d'un abus d'écriture pour "engendrée par $\{X\}$".)

Quelle est la sous-algèbre de A engendrée par $\emptyset$ (c'est-à-dire la plus petite sous-algèbre de A) ?

3.12.2. Avec les notations ci-dessus, soit B la sous-k-algèbre de A engendrée par S. Montrer que :

(i) B est le sous-k-espace vectoriel de A engendré par les produits finis d'éléments de S ;

(ii) B est le sous-anneau (unitaire) de A engendré par $S \cup \operatorname{Im} \varphi$, où $\varphi : k \to A$ est le morphisme structural ;

(iii) si $S = \{s_1, \ldots, s_n\}$ est fini, et si les s_i commutent entre eux (par exemple si A est commutative, ou si $n = 1$), B est le sous-k-espace vectoriel de A engendré par l'ensemble des "monômes" de la forme $s_1^{m_1} \cdots s_n^{m_n}$ avec $(m_1, \ldots, m_n) \in \mathbb{N}^n$;

(iv) si $S = \{s\}$ a un seul élément, B est l'image de $\varepsilon_s : k[X] \to A$.

Comment peut-on décrire les éléments de la sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$ engendrée par $\sqrt{2}$? Et par $\{\sqrt{2}, \sqrt{3}\}$? Montrer que ces sous-algèbres sont des corps, et des $\mathbb{Q}$-espaces vectoriels de dimension finie.

3.12.3. Soit B une k-algèbre, et soit $b \in B$. Montrer que l'image de $\varepsilon_b : k[X] \to B$ est la sous-algèbre de B engendrée par b.

3.13. *Exercices : sous-extension engendrée.* Soit maintenant L une *extension* d'un corps k. Une *sous-extension* de L est... devinez ! (Noter que k a malheureusement

disparu de l'expression : il faudrait dire "une sous-extension de k de L", formulation qui semble rebuter même les mathématiciens).

3.13.1. Et maintenant, devinez la question.

3.13.2. Bon, d'accord. Si S est une partie de L, montrer qu'il existe une plus petite sous-extension de L contenant S, que c'est l'ensemble des quotients a/b où $b \neq 0$ et où a et b appartiennent à la sous-algèbre engendrée par S, et que c'est un corps isomorphe (comme extension de k) au corps des fractions de ladite sous-algèbre. (Tiens, pourquoi existe-t-il, celui-là ?)

4. Structure des quotients de $k[X]$

Dans ce paragraphe, k désigne un corps. On se propose d'étudier les k-algèbres quotients de $k[X]$, c'est-à-dire, puisque $k[X]$ est principal, les k-algèbres de la forme $k[X]/(F)$ où $F \in k[X]$ est donné. Nous écarterons tout de suite le cas particulier trivial où $F = 0$: dans ce cas, $k[X]/(F)$ est isomorphe à $k[X]$. Nous adopterons donc les notations suivantes :

4.1. *Notations.* On fixe un polynôme

$$F = a_0 + a_1 X + \cdots + a_d X^d$$

avec $a_i \in k$ et $a_d \neq 0$ de sorte que $d = \deg F$. On note A la k-algèbre $k[X]/(F)$, et $\pi : k[X] \to A$ le morphisme canonique envoyant un polynôme sur sa classe.

On note $\omega := \pi(X) = X \bmod F$ la classe du polynôme X. Noter que comme π est un morphisme de k-algèbres envoyant X sur ω, on déduit de la propriété universelle 3.7 que l'on a $P(\omega) = \pi(P) = P \bmod F$ pour tout $P \in k[X]$. Un cas particulier important est $P = F$, qui donne dans A la relation fondamentale

$$F(\omega) = \sum_{i=0}^{d} a_i \, \omega^i = 0. \tag{4.1.1}$$

Enfin on note $V_d \subset k[X]$ le sous-espace vectoriel des polynômes de degré $< d$.

Proposition 4.2 *Le morphisme $\pi : k[X] \to A$ induit un isomorphisme de k-espaces vectoriels de V_d sur A.*

Démonstration. Comme π est évidemment k-linéaire, il suffit de voir que la restriction de π à V_d est bijective, ou encore que tout $P \in k[X]$ est congru modulo F à un unique polynôme de degré $< d$. Or c'est précisément ce qu'affirme le théorème de *division euclidienne* 2.3, le polynôme en question étant d'ailleurs le reste de la division de P par F. ∎

4.2.1. *Remarque.* On peut reformuler 4.2 en disant que V_d est un sous-k-espace vectoriel de $k[X]$ *supplémentaire* de (F) (qui est évidemment aussi un sous-k-espace vectoriel de $k[X]$).

4.2.2. *Remarque.* Une autre formulation de 4.2 consiste à dire que V_d est un *système de représentants* du groupe additif $k[X]$ modulo le sous-groupe (F), cf. (I.6.4.1). Il joue donc vis-à-vis de A le même rôle que le sous-ensemble $\{0, \ldots, n-1\}$ de $\mathbb{Z}$ vis-à-vis du quotient $\mathbb{Z}/n\mathbb{Z}$, pour $n > 0$: tout élément de A (resp. de $\mathbb{Z}/n\mathbb{Z}$) est la classe d'un unique élément de V_d (resp. de $\{0, \ldots, n-1\}$). En fait la situation est même meilleure ici, car V_d est un sous-espace vectoriel de $k[X]$ et la restriction de

π à V_d est k-linéaire, de sorte que pour calculer la somme de deux éléments de A il suffit d'additionner leurs représentants dans V_d ; par contre, $\{0, \dots, n-1\}$ n'est même pas un sous-groupe de $\mathbb{Z}$, et pour calculer la somme de deux éléments de $\mathbb{Z}/n\mathbb{Z}$ donnés par leurs représentants a et b dans $\{0, \dots, n-1\}$ il faut additionner a et b dans $\mathbb{Z}$, *puis* prendre le représentant de la classe modulo n du résultat.

Corollaire 4.2.3 *A est un k-espace vectoriel de dimension d ; plus précisément*

$$(1, \omega, \dots, \omega^{d-1})$$

est une k-base de A.

Démonstration. Résulte de 4.2 et du fait que $(1, X, \dots, X^{d-1})$ est une k-base de V_d. ∎

4.2.4. *Exercice.* Nous n'avons pas exclu que $d = 0$: que se passe-t-il dans ce cas ?

4.2.5. *Exercice.* Si $d = 1$, on a $V_d = k$ et l'isomorphisme de 4.2 est même un isomorphisme de k-algèbres. Montrer que l'isomorphisme réciproque est donné par $(P \bmod F) \mapsto P(-a_0/a_1)$.

4.3. *Calculs dans $k[X]/(F)$.* Il est facile de faire des additions dans A, grâce à 4.2.2. Pour effectuer des multiplications, il faut une méthode efficace pour calculer le représentant de degré $< d$ d'un polynôme quelconque P. La méthode générale est la division euclidienne : ce représentant n'est autre que le reste de la division euclidienne de P par F. Une autre approche, essentiellement équivalente mais parfois plus "parlante", consiste à remarquer qu'il s'agit d'exprimer $P(\omega)$ comme combinaison linéaire de $1, \omega, \dots, \omega^{d-1}$, et qu'il suffit pour cela de savoir le faire pour toute puissance ω^m avec $m \geq d$. Or la relation (4.1.1) implique que

$$\omega^d = -\frac{a_0}{a_d} - \frac{a_1}{a_d}\,\omega - \dots - \frac{a_{d-1}}{a_d}\,\omega^{d-1} \tag{4.3.1}$$

et donc que, pour $m \geq d$,

$$\omega^m = -\frac{a_0}{a_d}\,\omega^{m-d} - \frac{a_1}{a_d}\,\omega^{m-d+1} - \dots - \frac{a_{d-1}}{a_d}\,\omega^{m-1} \tag{4.3.2}$$

ce qui permet de faire le calcul de proche en proche. Ce point de vue (qui est, si l'on y réfléchit, l'idée de base de la division euclidienne !) est utile lorsque F est "simple", le cas le plus connu étant celui où $F = X^2 + 1$ (lorsque $k = \mathbb{R}$ on obtient un anneau bien connu, cf. (II.5.7)) : pour calculer modulo X^2+1 on remplace systématiquement X^2 par -1.

4.3.1. *Exemple : les "nombres duaux".* Prenons $F = X^2$: alors $\{1, \omega\}$ est une base de A sur k, de sorte que tout élément de A s'écrit de façon unique sous la forme $x + y\omega$

avec $x, y \in k$; la multiplication dans A est déterminée par la condition $\omega^2 = 0$ qui donne la formule $(x + y\omega)(x' + y'\omega) = xx' + (x'y + xy')\omega$. L'algèbre A ainsi obtenue est appelée la *k-algèbre des nombres duaux*.

4.3.2. *Exercice.* Dans l'exemple 4.3.1 ci-dessus, montrer que l'application $(a, b) \mapsto a\,(1 + b\omega)$induit un isomorphisme du groupe produit $(k^*, .) \times (k, +)$ sur le groupe $(A^\times, .)$. Quels sont les éléments de A de carré nul ? les éléments de A de carré 1 ? (Attention à la caractéristique !)

4.3.3. *Exercice.* Pour F quelconque, montrer que ω est inversible dans A si et seulement si $F(0) \neq 0$; dans ce cas, calculer son inverse.

4.3.4. *Exercice.* Pour tout $x \in A$, soit $\rho(x)$ la matrice dans la base $(1, \omega, \ldots, \omega^{d-1})$ de la multiplication par x dans A (qui est un endomorphisme du k-espace vectoriel A). Montrer que l'application ρ ainsi définie est un morphisme injectif d'anneaux unitaires de A dans $M_d(k)$; montrer aussi que pour tout $x \in A$, $\rho(x)$ est inversible dans $M_d(k)$ si et seulement si $x \in A^\times$.

Montrer que

$$\rho(\omega) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0/a_d \\ 1 & 0 & \ldots & 0 & -a_1/a_d \\ 0 & 1 & \ldots & 0 & -a_2/a_d \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{d-1}/a_d \end{pmatrix}$$

et calculer $\rho(x)$ pour x quelconque lorsque $F = X^2 + 1$ et lorsque $F = X^2$. En déduire une méthode de construction de $\mathbb{C}$ comme sous-anneau de $M_2(\mathbb{R})$. Déduire aussi du calcul ci-dessus que $\det \rho(\omega) = (-1)^d a_0/a_d$ et plus généralement que le polynôme caractéristique de $\rho(\omega)$ est donné par $\det \rho(\omega - \lambda) = \frac{(-1)^d}{a_d} F(\lambda)$.

Proposition 4.4

(1) *Soit α un élément de A, classe d'un polynôme $P \in k[X]$. On a les équivalences :*

$$\alpha \in A^\times \;\Leftrightarrow\; \alpha \text{ n'est pas diviseur de zéro dans } A \;\Leftrightarrow\; P \text{ et } F \text{ sont premiers entre eux dans } k[X].$$

(2) *On a les équivalences :*

A est un corps $\Leftrightarrow$ A est intègre $\Leftrightarrow$ F est irréductible dans $k[X]$.

Démonstration. (1) est un cas particulier de III.4.9 ; noter que l'équivalence des deux premières propriétés résulte aussi de 3.4.5, puisque A est de dimension finie sur k.

(2) est un cas particulier de III.4.9.1. ∎

4.4.1. *Remarque.* L'énoncé ci-desssus serait en défaut pour $F = 0$ (cas que nous avons exclu). Pourquoi ? Qu'est-ce qui ne marche pas dans la démonstration ?

4.4.2. *Exercice.* Voyons plus précisément ce qui se passe lorsque F n'est pas irréductible. (voir plus généralement l'exercice (III.6.3). Supposons pour simplifier F unitaire et non constant et écrivons $F = P_1^{e_1} \dots P_s^{e_s}$ avec $P_1, \dots, P_s$ irréductibles unitaires distincts et $e_1, \dots, e_s$ entiers > 0.

a) Déduire du lemme chinois que A est isomorphe au produit des k-algèbres $A_i = k[X]/(P_i)$ $(i = 1, \dots, s)$.

b) Si $e_1 > 0$, montrer que la classe α de $P_1^{e_1-1} P_2^{e_2} \dots P_s^{e_s}$ est un élément non nul de A vérifiant $\alpha^2 = 0$.

c) Montrer que A est un anneau *réduit* (i.e. sans élément nilpotent non nul) si et seulement si F est *sans facteur carré* (tous les e_i sont égaux à 1).

d) Montrer que $s = 1$ (i.e. F est une puissance d'un irréductible) si et seulement si tout diviseur de zéro de A est nilpotent.

4.5. *Exercice : éléments algébriques et transcendants.* Soit B une k-algèbre. Pour tout $b \in B$, on considère le morphisme $\varepsilon_b : k[X] \to B$ d'évaluation en b, et l'on adopte à regret la notation $k[b]$ pour l'image de ε_b (qui est aussi la sous-k-algèbre de B engendrée par b, cf. 3.12.3).

4.5.1. Montrer que les conditions suivantes sont équivalentes :

(i) ε_b n'est pas injectif ;

(ii) il existe $F \in k[X]$ non nul tel que $F(b) = 0$;

(iii) il existe $F \in k[X]$ non nul tel que $k[b]$ soit isomorphe (comme k-algèbre) à $k[X]/(F)$;

(iv) $\dim_k k[b] < \infty$;

(v) il existe une sous-k-algèbre de B contenant b, qui est de dimension finie sur k.

On dit que b est *algébrique* sur k si ces conditions sont vérifiées. Sinon, on dit que b est *transcendant* sur k.

4.5.2. Exemples : soient $k = \mathbb{Q}$ et $A = \mathbb{C}$. Montrer que $\sqrt{2}$ et $\sqrt{2}+\sqrt{3}$ sont algébriques sur $\mathbb{Q}$. Donner dans chaque cas un système générateur fini (et de préférence une base) sur $\mathbb{Q}$ de la sous-algèbre engendrée.

Pour k quelconque, soit $B = k[X]$. Montrer que X est transcendant sur k. Plus généralement, tout élément de $k[X]$ non constant est transcendant sur k.

4.5.3. Vrai ou faux : b est transcendant sur k si et seulement si $k[b]$ est isomorphe (comme k-algèbre) à $k[X]$.

4.5.4. On suppose que B est commutative. Soit c un autre élément de B. On suppose que b et c sont algébriques sur k. Montrer que la sous-k-algèbre $k[b, c]$ de B engendrée

par $\{b, c\}$ est de dimension finie sur k. (Indication : si $k[b]$ est engendrée comme k-espace vectoriel par $\{1, b, \ldots, b^n\}$ et $k[c]$ par $\{1, c, \ldots, c^m\}$ alors $k[b, c]$ est engendrée par les $b^i c^j$ avec $0 \leq i \leq n$ et $0 \leq j \leq m$. Conclure en utilisant 4.5.1).

En déduire que le sous-ensemble de B formé des éléments algébriques sur k est une sous-algèbre de B.

Montrer en outre que si b est algébrique sur k et inversible dans B, alors b^{-1} est algébrique sur k. En déduire que si B est un corps, le sous-ensemble de B formé des éléments algébriques sur k est un sous-corps de B.

4.5.5. On suppose que B est un corps (i.e. une extension de k). Outre l'algèbre $k[b]$, considérons la *sous-extension* (cf. 3.13.2). $k(b)$ de L engendrée par b. Montrer que les conditions suivantes sont équivalentes :

(i) b est algébrique sur k ;

(ii) $k[b]$ est un corps ;

(iii) $k[b] = k(b)$.

4.5.6. Une extension K de k est dite *algébrique* si tout élément de K est algébrique sur k. (Par exemple, $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$).

Si K est une extension algébrique de k, et L une extension algébrique de K, montrer que L est une extension algébrique de k.

(Indication : si $x \in L$, il existe un polynôme non nul $F \in K[X]$ tel que $F(x) = 0$. Montrer que comme les coefficients $a_0, \ldots, a_d$ de F sont algébriques sur k, la sous-k-algèbre $M = k[a_0, \ldots, a_d]$ de K qu'ils engendrent est de dimension finie sur k. En déduire que $M[x] = k[a_0, \ldots, a_d, x]$ est de dimension finie sur k et conclure.)

4.6. *Exercice : polynôme minimal.* Soient B une k-algèbre et b un élément de B *algébrique* sur k. On note $k[b]$ la sous-algèbre de B engendrée par b.

4.6.1. Le noyau de $\varepsilon_b : k[X] \to B$ est un idéal non nul de $k[X]$; il est donc engendré par un polynôme $F \in k[X]^*$, unique à multiplication près par une constante non nulle (on peut d'ailleurs lever cette ambiguïté en imposant à F d'être unitaire). Un tel polynôme est appelé *polynôme minimal* de b sur k.

Montrer que $\deg F = \dim_k k[b]$.

4.6.2. Quel est le polynôme minimal unitaire de $\sqrt{2}$ sur $\mathbb{Q}$? Et sur $\mathbb{R}$?

4.6.3. Si B est une extension de k, montrer que F est irréductible. Inversement, tout polynôme $F \in k[X]$ irréductible tel que $F(b) = 0$ est un polynôme minimal de b.

4.6.4. On suppose que $B = \mathrm{End}_k(V)$, où V est un k-espace vectoriel de dimension finie. Montrer que F divise le polynôme caractéristique de b.

5. Racines

Dans tout ce paragraphe, k désigne un corps commutatif.

Définition 5.1 *Soit $F \in k[X]$. On dit qu'un élément α de k est une* racine *(ou encore un* zéro*) de F si $F(\alpha) = 0$.*

Plus généralement, si L est une extension de k, un élément α de L est une racine de F (dans L) si $F(\alpha) = 0$, c'est-à-dire si α est racine de F vu comme élément de $L[X]$.

5.2. *Remarque fondamentale.* Soient $F \in k[X]$ et $\alpha \in k$. La division euclidienne de F par $X - \alpha$ donne

$$F = (X - \alpha)Q + F(\alpha)$$

(en effet le reste est nul ou de degré 0 donc constant, et il suffit donc de faire $X = 0$ pour obtenir le résultat, d'ailleurs valable dans tout anneau commutatif unitaire). En particulier *α est racine de F si et seulement si F est divisible par $X - \alpha$ dans $k[X]$.*

Définition 5.3 *Soient $F \in k[X]$ et $\alpha \in k$. On définit la* multiplicité *de F en α, notée* $\mathrm{mult}_\alpha(F)$*, par la formule*

$$\mathrm{mult}_\alpha(F) = v_{X-\alpha}(F) \in \mathbb{N} \cup \{+\infty\}$$

(notation de III.6.1*).*

5.4. *Remarques.*

5.4.1. En d'autres termes, $\mathrm{mult}_\alpha(F)$ est infinie si $F = 0$, et sinon est l'exposant de $X - \alpha$ dans la décomposition de F en facteurs irréductibles.

5.4.2. Il résulte de 5.2 que α est racine de F si et seulement si $\mathrm{mult}_\alpha(F) > 0$.

5.4.3. *Exercice.* Montrer que $\mathrm{mult}_\alpha(FG) = \mathrm{mult}_\alpha(F) + \mathrm{mult}_\alpha(G)$, et que $\mathrm{mult}_\alpha(F + G) \geq \inf(\mathrm{mult}_\alpha(F), \mathrm{mult}_\alpha(G))$ pour tous $\alpha \in k$ et $F, G \in k[X]$.

5.4.4. *Exercice.* Pour $m \in \mathbb{N}$ donné, $\alpha \in k$ et $F \in k[X]$, montrer que $\mathrm{mult}_\alpha(F) = m$ si et seulement si il existe $G \in k[X]$ tel que $F = (X - \alpha)^m G$ et $G(\alpha) \neq 0$.

5.4.5. On dit que α est racine simple (resp. double, triple, multiple,...) de F si $\mathrm{mult}_\alpha(F)$ est égale à 1 (resp. 2, 3, est $> 1 \ldots$).

Théorème 5.5 *Soit $F \in k[X]$ un polynôme non nul. Alors l'ensemble des racines de F dans k est fini, et l'on a l'inégalité*

$$\sum_{\alpha \in k} \mathrm{mult}_\alpha(F) \leq \deg F.$$

De plus l'égalité a lieu si et seulement si F est décomposé *dans $k[X]$* (2.9).

Démonstration. Désignons par $J \subset k[X]$ l'ensemble des polynômes irréductibles unitaires de degré ≥ 2. Alors la décomposition de P (2.7) peut encore s'écrire

$$F = a \prod_{\alpha \in k} (X - \alpha)^{\mathrm{mult}_\alpha(F)} \prod_{P \in J} P^{v_P(F)}.$$

Les exposants sont presque tous nuls, ce qui entraîne la finitude de l'ensemble des racines. D'autre part, prenant les degrés, on obtient :

$$\deg F = \sum_{\alpha \in k} \mathrm{mult}_\alpha(F) + \sum_{P \in J} v_P(F) \deg P.$$

d'où l'inégalité voulue puisque les degrés sont ≥ 0 ; enfin l'égalité a lieu si et seulement si $v_P(F) = 0$ pour tout $P \in J$, d'où la dernière assertion. ∎

Corollaire 5.6

(i) *Un polynôme non nul de degré d a au plus d racines dans k (et dans toute extension de k).*

(ii) *Soit $F \in k[X]$ un polynôme* unitaire *de degré d ayant d racines distinctes $a_1, \ldots, a_d$ dans k. Alors $F = \prod_{i=1}^{d} (X - a_i)$.*

(iii) *Soient P et $Q \in k[X]$ et $d \in \mathbb{N}$. On suppose que P et Q sont de degré $\leq d$ et qu'il existe $a_1, \ldots, a_{d+1} \in k$* deux à deux distincts *tels que $P(a_i) = Q(a_i)$ pour tout $i \in \{1, \ldots, d+1\}$. Alors $P = Q$.*

(iv) *Si k est* infini, *l'application $P \mapsto \widetilde{P}$ de* 1.11 *est injective ("la fonction polynôme détermine le polynôme").*

Démonstration. Toutes ces assertions résultent immédiatement de 5.5. ∎

5.6.1. *Remarque.* Les analogues de ces propriétés sont faux pour les polynômes à coefficients dans un anneau quelconque. Par exemple, le polynôme $F = X^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[X]$ vérifie $F(1 \bmod 8) = F(3 \bmod 8) = F(5 \bmod 8) = F(7 \bmod 8) = 0$ et a donc 4 "racines" dans $\mathbb{Z}/8\mathbb{Z}$.

Corollaire 5.7 (formules de Lagrange.) *Soient $d \in \mathbb{N}$, $a_1, \ldots, a_{d+1} \in k$ deux à deux distincts, et $b_1, \ldots, b_{d+1} \in k$. Il existe alors un* unique *$F \in k[X]$ tel que $\deg F \leq d$ et $F(a_i) = b_i$ pour tout $i \in \{1, \ldots, d+1\}$.*

De plus F est donné par la formule $F = \sum_{i=1}^{d+1} b_i L_i$, où L_i est le "polynôme d'interpolation de Lagrange"

$$L_i = \prod_{\substack{j \in \{1,\ldots,d+1\} \\ j \neq i}} \frac{X - a_j}{a_i - a_j}.$$

Démonstration. L'unicité résulte de 5.6(iii). Il reste donc à vérifier que le polynôme F de l'énoncé satisfait aux conditions requises. Il est immédiat que les L_i sont de degré d donc $\deg F \leq d$. Enfin les égalités $F(a_i) = b_i$ résultent de la propriété $L_i(a_j) = \delta_{ij}$ que le lecteur vérifiera sans peine. ∎

5.7.1. *Remarques.* L'existence de F — mais non la formule — peut se déduire de l'unicité : si V désigne le sous-k-espace vectoriel de $k[X]$ formé des polynômes de degré $\leq d$, on considère l'application k-linéaire $V \to k^{d+1}$ envoyant $P \in V$ sur $(P(b_1), \ldots, P(b_{d+1}))$. Cette application est injective d'après 5.6(iii) ; comme $\dim V = d + 1$, elle est bijective, d'où l'assertion.

Noter aussi que l'hypothèse que les a_i sont distincts sert pour pouvoir appliquer 5.6(iii), mais aussi pour pouvoir définir L_i !

5.7.2. *Exercice.* Refaire l'exercice 1.11.2.

5.8. *Racines communes.* Étant donnés deux polynômes F et G à coefficients dans k, on a souvent besoin de considérer leurs racines communes éventuelles, dans k ou dans une extension. La proposition suivante est alors utile :

Proposition 5.8.1 *Soient F et $G \in k[X]$, soit Δ un PGCD de F et G dans $k[X]$, et soit K une extension de k. Alors :*

(i) *pour tout $\alpha \in K$, on a $\mathrm{mult}_\alpha(\Delta) = \min\{\mathrm{mult}_\alpha(F), \mathrm{mult}_\alpha(G)\}$;*

(ii) *les racine communes de F et G dans K sont les racines de Δ dans K.*

Démonstration. (i) est un cas particulier de III.6.2.6 (avec $p = X - \alpha$), et entraîne évidemment (ii). ∎

Voici maintenant quelques applications arithmétiques de 5.5 :

Proposition 5.9 *Soit p un nombre premier. Alors on a dans $\mathbb{Z}[X]$ les congruences*

$$\begin{aligned} X^{p-1} - 1 &\equiv \textstyle\prod_{i=1}^{p-1}(X - i) \pmod p \\ X^p - X &\equiv \textstyle\prod_{i=0}^{p-1}(X - i) \pmod p. \end{aligned}$$

Démonstration. Bien entendu, dire que deux polynômes de $\mathbb{Z}[X]$ sont congrus modulo p signifie que leur différence est divisible par p dans $\mathbb{Z}[X]$, c'est-à-dire a ses coefficients divisibles par p. Les congruences considérées se ramènent donc à prouver *dans* $(\mathbb{Z}/p\mathbb{Z})[X]$ les égalités correspondantes :

$$\begin{aligned} X^{p-1} - 1 &= \textstyle\prod_{i=1}^{p-1}(X - \bar{i}) \\ X^p - X &= \textstyle\prod_{i=0}^{p-1}(X - \bar{i}) \end{aligned}$$

où $\bar{i} \in \mathbb{Z}/p\mathbb{Z}$ désigne la classe mod p de $i \in \mathbb{Z}$. Il suffit d'autre part de montrer la première égalité, la seconde s'en déduisant par multiplication par X.

Or il résulte du théorème de Fermat (II.3.7, II.7.3.4) que, pour $1 \leq i \leq p-1$, $\bar{i}$ est racine dans $\mathbb{Z}/p\mathbb{Z}$ du polynôme $X^{p-1} - 1$. Comme celui-ci est de degré $p-1$, et est unitaire, l'égalité cherchée résulte de 5.6(ii). ∎

On retrouve ainsi, en particulier, le résultat suivant, déjà démontré en II.3.8 :

Corollaire 5.10 (théorème de Wilson). *Pour tout nombre premier p, on a la congruence*

$$(p-1)! \equiv -1 \qquad (\mathrm{mod}\, p).$$

Démonstration. Il suffit de faire $X = p$ dans la première congruence de 5.9. (On peut aussi faire $X = 0$, en faisant un peu attention au signe, le cas $p = 2$ se traitant alors à part). ∎

5.10.1. *Remarque.* On vient d'utiliser la propriété évidente suivante : si un polynôme $F \in \mathbb{Z}[X]$ est congru à 0 modulo p, alors $F(n) \equiv 0 \pmod p$ pour tout entier n. On notera que la réciproque est fausse : ainsi, pour $p = 2$, le polynôme $F = X^2 - X = X(X-1)$ n'est pas divisible par 2 dans $\mathbb{Z}[X]$ bien que $F(n)$ soit pair pour tout $n \in \mathbb{Z}$.

5.10.2. *Exercice.* Trouver un contre-exemple analogue à 5.10.1 pour chaque p premier.

6. Application : sous-groupes finis de k^*

6.1. *Notations.* Dans ce paragraphe, k désigne un corps. Pour tout entier $n \geq 1$, posons

$$\mu_n(k) = \{z \in k \mid z^n = 1\}.$$

Il est clair que $\mu_n(k)$ est un sous-groupe (multiplicatif) de k^*. De plus :

Lemme 6.2 *Pour tout entier $n \geq 1$, $|\mu_n(k)| \leq n$.*

Démonstration. Ceci résulte de 5.6(i) puisque $\mu_n(k)$ est l'ensemble des racines dans k du polynôme $X^n - 1$. ∎

Théorème 6.3 *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 (I.6.6) 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 6.2, d'où l'assertion.

La propriété (1) a la conséquence suivante : pour tout entier $d \geq 1$, k^* admet *au plus un* sous-groupe d'ordre d (puisque s'il en a un, c'est $\mu_d(k)$). Par suite tout sous-groupe de k^* (et notamment G) a aussi la même propriété. L'assertion (2) résulte donc de la proposition ci-dessous, qui n'a plus rien à voir avec les polynômes. ∎

Proposition 6.4 *Soit G un groupe fini commutatif. Les conditions suivantes sont équivalentes :*

(i) *G est cyclique ;*

(ii) *pour tout entier $d \geq 1$ divisant $|G|$, G admet un unique sous-groupe d'ordre d ;*

(iii) *pour tout entier $d \geq 1$, G admet au plus un sous-groupe d'ordre d.*

Démonstration. L'implication (i)⇒(ii) est déjà connue, cf. (I.10.6.1).

L'implication (ii)⇒(iii) est triviale : si G vérifie (ii) et si $d \geq 1$ est un entier, alors ou bien d divise $|G|$ et l'on applique l'hypothèse, ou bien d ne divise pas $|G|$ et G n'admet aucun sous-groupe d'ordre d.

Pour montrer l'implication (iii)⇒(i), qui est la partie intéressante de l'énoncé, nous aurons besoin de deux lemmes (où tous les groupes seront notés multiplicativement) :

Lemme 6.4.1 *Soit G un groupe commutatif. Soient x et y deux éléments d'ordre fini de G, et soient a et b leurs ordres respectifs. Alors il existe dans G un élément z d'ordre $m = \mathrm{PPCM}\,(a,b)$.* (Ici le PPCM est par convention positif).

Démonstration. Supposons d'abord a et b premiers entre eux (de sorte que $m = ab$). Montrons qu'alors $z = xy$ convient. Il est clair que $z^m = x^{ab}y^{ab} = e$ (on rappelle que G est commutatif). Soit n un entier tel que $z^n = e$, et montrons que m divise n. On a $x^n y^n = e$; posons $t = x^n = y^{-n}$: comme t est une puissance de x (resp. de y) son ordre divise a (resp. b) donc est égal à 1 puisque a et b sont premiers entre eux. Donc $x^n = y^{-n} = e$, donc n est un multiple de a et de b, donc de m, cqfd.

Ne faisant plus d'hypothèse sur a et b, on peut toutefois écrire $m = a_1 b_1$ avec $a_1 | a$, $b_1 | b$ et a_1 et b_1 premiers entre eux : on peut prendre par exemple

$$a_1 = \prod_{\substack{p \text{ premier} \\ v_p(a) \geq v_p(b)}} p^{v_p(a)} \qquad \text{et} \qquad b_1 = \prod_{\substack{p \text{ premier} \\ v_p(a) < v_p(b)}} p^{v_p(b)}.$$

G contient alors les éléments $x' = x^{a/a_1}$ et $y' = y^{b/b_1}$ qui sont d'ordres respectifs a_1 et b_1. Comme a_1 et b_1 sont premiers entre eux, on peut appliquer le cas déjà étudié et conclure que $x'y'$ est d'ordre $a_1 b_1 = m$. ∎

Lemme 6.4.2 *Soit G un groupe commutatif, et soit x un élément de G d'ordre N* maximum. *Alors pour tout $y \in G$, l'ordre de y divise N.*

Démonstration. Si b est l'ordre de y, alors G contient d'après 6.4.1 un élément d'ordre $\mathrm{PPCM}\,(N,b)$, qui est $\geq N$. Vu le choix de N, on a donc $\mathrm{PPCM}\,(N,b) = N$ donc b divise N. ∎

6.4.3. Nous pouvons maintenant prouver l'implication (iii)⇒(i) de 6.4. Supposons donc que G vérifie la propriété (iii), et soit $x \in G$ d'ordre N maximum. Nous allons montrer que $G = \langle x \rangle$ (donc est cyclique d'ordre N).

Soit donc $y \in G$: il s'agit de voir que $y \in \langle x \rangle$. Si d est l'ordre de y, on sait d'après le lemme 6.4.2 que d divise N. Donc puisque $\langle x \rangle$ est cyclique d'ordre N il admet un sous-groupe H d'ordre d (c'est l'implication (i)⇒(ii) déjà vue). Comme H et $\langle y \rangle$ sont deux sous-groupes d'ordre d de G, l'hypothèse (iii) implique que $H = \langle y \rangle$. En particulier, $\langle y \rangle \subset \langle x \rangle$, cqfd. ∎

Corollaire 6.5 *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 6.6 *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 6.3. 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. ∎

6.7. *Exercices.* Nous montrerons au paragraphe 9 des résultats plus précis sur l'ordre (et donc la structure) de $\mu_n(k)$, en particulier lorsque k est algébriquement clos. Le lecteur peut déjà traiter les cas suivants :

6.7.1. Donner explicitement pour chaque n un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $\mu_n(\mathbb{C})$.

6.7.2. Quel est, en fonction de l'entier n, l'ordre de $\mu_n(\mathbb{Q})$? de $\mu_n(\mathbb{R})$?

6.7.3. Quel est l'ordre de $\mu_n(\mathbb{Z}/p\mathbb{Z})$, en fonction de l'entier n et du nombre premier p ?

6.7.4. Pour un corps k quelconque, montrer que $\mu_n(k(X)) = \mu_n(k)$, où $k(X)$ désigne le corps des fractions rationnelles en X à coefficients dans k. (Indication : utiliser III.8.2 avec $A = k[X]$).

6.8. *Exercice.* Existe-t-il un corps k tel que le groupe k^* soit isomorphe à $\mathbb{Z}$?

7. Corps algébriquement clos ; adjonction de racines

Proposition 7.1 *Soit k un corps. Les conditions suivantes sont équivalentes :*

(i) *tout polynôme de $k[X]$ non constant a au moins une racine dans k ;*

(ii) *tout polynôme irréductible de $k[X]$ est de degré 1 ;*

(iii) *tout polynôme de $k[X]$ non nul est décomposé.*

Démonstration. (i)⇒(ii) : supposons (i) vérifiée, et soit $P \in k[X]$ irréductible. Alors comme P n'est pas constant il a une racine $\alpha \in k$ donc est divisible par $X - \alpha$; comme il est irréductible il est donc de la forme $\lambda(X - \alpha)$ avec $\lambda \in k^*$, donc est de degré 1.

(ii)⇒(iii) : résulte du fait que tout $F \in k[X]$ est produit d'une constante par des polynômes irréductibles ;

(iii)⇒(i) : il est clair que tout polynôme décomposé non constant a une racine. ∎

Définition 7.2 *Un corps k est dit* algébriquement clos *s'il vérifie les conditions équivalentes de* 7.1.

Théorème 7.3 ("théorème de d'Alembert") $\mathbb{C}$ *est algébriquement clos.*

Démonstration. Soit $F \in \mathbb{C}[X]$ non constant. Supposons que F n'ait pas de racine dans $\mathbb{C}$: alors l'application $z \mapsto 1/F(z)$ de $\mathbb{C}$ dans $\mathbb{C}$ est bien définie et holomorphe. D'autre part si $a_d X^d$ est le terme dominant de F (avec $d \geq 1$) alors $|1/F(z)| \sim a_d^{-1} z^{-d}$ donc tend vers 0 lorsque $|z|$ tend vers l'infini, ce qui implique que cette fonction holomorphe est bornée. Elle est donc constante (théorème de Liouville), ce qui est absurde. ∎

Nous admettrons le théorème suivant :

Théorème 7.4 *Tout corps admet une extension qui est un corps algébriquement clos.* ∎

Ce théorème implique notamment que pour tout corps k et tout $F \in k[X]$ non nul, il existe une extension K de k telle que F soit décomposé dans $L[X]$. Nous allons démontrer ce résultat, qui suffit pour beaucoup d'applications (et qui est en fait à la base de la preuve de 7.4). De façon précise :

Proposition 7.5 (adjonction de racines) *Soient k un corps et $F \in k[X]$ non nul de degré d. Alors :*

(i) *si $d > 0$, il existe une extension finie K de k, de degré $\leq d$, (cf.* 3.4*) telle que F ait une racine dans K ;*

(ii) *il existe une extension L de k telle que F soit décomposé dans $L[X]$.*

Démonstration. (i) Si F est irréductible il suffit de prendre $K = k[X]/(F)$: c'est bien une extension de k d'après (III.4.9.1), de degré d d'après 4.2.3, et F a une racine dans K d'après 4.1.1.

Dans le cas général, si $d > 0$, alors il existe un polynôme irréductible P divisant F et donc, d'après ce qui précède, une extension de k de degré $\deg P \leq \deg F$ dans laquelle P, et donc F, a une racine, cqfd.

(ii) Récurrence sur d : c'est clair si $d = 0$ (prendre $L = k$, et réfléchir un peu...), et si $d > 0$ supposons l'assertion démontrée pour tout corps k et tout polynôme de degré $< d$. Comme $d > 0$ on peut appliquer (i) : F a une racine α dans une extension K de k. On a donc $F = (X - \alpha)G$ avec $G \in K[X]$ de degré $d - 1$; l'hypothèse de récurrence montre que G est décomposé dans $L[X]$ où L est une extension de K. Mais alors L est aussi une extension de k dans laquelle $F = (X-\alpha)G$ est décomposé. ∎

7.5.1. *Exercice.* Utilisant l'exercice 3.4.4, montrer que l'extension L de (ii) peut être choisie finie de degré $\leq d!$.

7.5.2. *Exercice.* Dans le cas où F est irréductible montrer que l'extension construite en (i) est "la plus petite possible" au sens suivant : toute extension de k dans laquelle F a une racine contient une extension de k isomorphe à $k[X]/(F)$. (Indication : utiliser la propriété universelle de $k[X]/(F)$, cf. 3.9.4).

Corollaire 7.6 *Soient F et $G \in k[X]$, et soit Ω une extension* algébriquement close *de k. Les conditions suivantes sont équivalentes :*

(i) *pour toute extension K de k, F et G n'ont aucune racine commune dans K ;*

(ii) *F et G n'ont aucune racine commune dans Ω ;*

(iii) *F et G sont premiers entre eux.*

Démonstration. Soit Δ un PGCD de F et G dans $k[X]$. Compte tenu de 5.8.1, l'énoncé revient à prouver l'équivalence suivante, qui est immédiate :

pour toute extension K de k, Δ n'a aucune racine dans K
$\iff$ Δ n'a aucune racine dans Ω
$\iff$ Δ est une constante non nulle.

∎

7.7. *Exercice.* Soit k un corps. Montrer l'équivalence :

k est algébriquement clos $\Longleftrightarrow$ toute extension algébrique de k est isomorphe à k.

(Pour la notion d'extension algébrique voir 4.5.6). Bien entendu "isomorphe" veut dire ici "isomorphe comme extension de k".

7.8. *Exercice.* Soient k un corps, Ω une extension algébriquement close de k. Posons

$$\overline{k} = \{x \in \Omega \,|\, x \text{ est algébrique sur } \Omega\}.$$

Montrer que $\overline{k}$ est une extension algébriquement close de k. (Utiliser 7.7 et 4.5.6).

7.9. *Exercice.* Pour tout corps k, montrer qu'il existe une extension *algébrique* de k qui est un corps algébriquement clos. Pour $k = \mathbb{Q}$ notamment, montrer que $\overline{\mathbb{Q}} = \{x \in \mathbb{C} \,|\, x \text{ est algébrique sur } \mathbb{Q}\}$ est une telle extension.

8. Quelques critères d'irréductibilité et d'existence de racines

Nous allons donner dans ce paragraphe quelques méthodes pour aborder le problème suivant : étant donnés un corps k et un polynôme non nul $P \in k[X]$, on demande si P a une racine dans k, et s'il est irréductible dans $k[X]$.

Les méthodes utilisées dépendent très fortement du corps k. Par exemple, si $k = \mathbb{C}$, la réponse est particulièrement simple et résulte du théorème de d'Alembert (7.3) : P a une racine si et seulement si $\deg P > 0$, et est irréductible si et seulement si $\deg P = 1$.

Pour $k = \mathbb{R}$ un critère d'irréductibilité, un peu moins simple, s'en déduit aisément :

Proposition 8.1 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

(i) *les polynômes de degré 1 ;*

(ii) *les polynômes de degré 2 sans racine réelle.*

Démonstration. Il est immédiat que les polynômes de l'énoncé sont bien irréductibles (plus généralement voir 8.4 plus bas). Réciproquement, soit $P \in \mathbb{R}[X]$ irréductible et de degré > 1 : alors P a une racine complexe α, qui n'est pas réelle (si P avait une racine réelle il serait de degré 1). Comme P est réel on a aussi $P(\overline{\alpha}) = 0$. Comme $\alpha \neq \overline{\alpha}$, P est donc divisible dans $\mathbb{C}[X]$ par $Q := (X - \alpha)(X - \overline{\alpha})$. Or $Q \in \mathbb{R}[X]$, donc d'après 2.6, Q divise P dans $\mathbb{R}[X]$. Comme P est irréductible on a $P = \lambda Q$ avec $\lambda \in \mathbb{R}^*$, d'où la conclusion. ∎

8.1.1. *Exercice.* Décomposer dans $\mathbb{R}[X]$ le polynôme $X^4 + 1$; déduire du résultat que ce polynôme est irréductible dans $\mathbb{Q}[X]$ (considérant sa décomposition dans $\mathbb{Q}[X]$, remarquer que si F est un facteur irréductible de $X^4 + 1$ dans $\mathbb{Q}[X]$ c'est un produit de facteur irréductibles de $X^4 + 1$ dans $\mathbb{R}[X]$).

8.2. Toujours pour $k = \mathbb{R}$, il existe des méthodes permettant de trouver le nombre de racines d'un polynôme P donné dans un intervalle réel I donné. Elles reposent sur le théorème des valeurs intermédiaires qui montre que si P change de signe sur I il a au moins une racine dans I. Rappelons simplement la conséquence la plus élémentaire de ce théorème : tout polynôme réel de degré *impair* a une racine réelle. Nous conseillons au lecteur de refaire la démonstration, et aussi de retrouver ce résultat comme conséquence de 8.1.

8.3. Revenons à un corps k quelconque. Parmi les polynômes irréductibles de $k[X]$, les plus simples (au point que l'on risque de les oublier) sont les polynômes de degré 1 ; ce sont les seuls polynômes irréductibles de $k[X]$ ayant une racine dans k (voir

l'argument au début de la preuve de 7.1). Par contre, un polynôme sans racine n'est pas nécessairement irréductible (exemple : $(X^2+1)^2$ dans $\mathbb{R}[X]$). Toutefois :

Proposition 8.4 *Soit $P \in k[X]$ de degré 2 ou 3. Pour que P soit irréductible il faut et il suffit qu'il n'ait aucune racine dans k.*

Démonstration. Exercice. ∎

8.5. *Exercices : polynômes de degré 2.* Soit $P = aX^2 + bX + c$ avec $a, b, c \in k$ et $a \neq 0$. On note $\Delta = b^2 - 4ac \in k$ le "discriminant" de P, et l'on cherche des critères d'existence de racines de P dans k, généralisant la discussion faite classiquement pour $k = \mathbb{R}$.

8.5.1. Supposons car $(k) \neq 2$. Généraliser alors le résultat bien connu : P a une racine double (qui est nécessairement dans k) si et seulement si $\Delta = 0$; si $\Delta \neq 0$, alors P a une racine dans k si et seulement si Δ est un carré dans k^*. Dans ce cas, les racines de P sont données par les formules classiques, où cependant *la notation $\sqrt{\Delta}$ est à proscrire* si k n'est pas un sous-corps de $\mathbb{R}$: il faut écrire par exemple "soit δ un élément de k de carré Δ, alors les racines sont données par les formules..."

8.5.2. On suppose maintenant que car $(k) = 2$.

Montrer que P a une racine double (dans une extension de k, mais pas nécessairement dans k) si et seulement si $b = 0$ (condition qui équivaut, d'ailleurs, à $\Delta = 0$). Dans ce cas, P a une racine dans k si et seulement si c/a est un carré dans k.

Si $b \neq 0$, P a une racine dans k si et seulement si le polynôme $Y^2 + Y + (ac/b^2) \in k[Y]$ en a une ("poser $X = (b/a)Y$").

8.5.3. On voit donc qu'en caractéristique différente de 2, la résolution des équations du second degré se ramène à la recherche des carrés dans k. En caractéristique 2, elle se ramène soit à la recherche des carrés, soit à celle des éléments de k de la forme $y^2 + y$ ($y \in k$).

Noter que l'ensemble des carrés non nuls est un sous-groupe de k^* ; en caractéristique 2, l'ensemble des carrés est même un sous-corps de k, et l'ensemble des éléments de la forme y^2+y est un sous-groupe du groupe additif $(k, +)$ (c'est l'image de l'application $y \mapsto y^2 + y$ qui est un endomorphisme de ce groupe).

8.5.4. On suppose maintenant k *fini* de caractéristique $p \neq 2$, et l'on note q son cardinal (on rappelle que q est une puissance de p, pourquoi ?)

Montrer que les carrés de k^* forment un sous-groupe d'indice 2 de k^* (considérer le morphisme $x \mapsto x^2$).

En déduire en utilisant 6.5 qu'un élément x de k^* est un carré si et seulement si $x^{\frac{q-1}{2}} = 1$ (et dans le cas contraire, on a $x^{\frac{q-1}{2}} = -1$).

Montrer en particulier que -1 est un carré dans k si et seulement si $q \equiv 1 \pmod 4$ (le cas particulier où $k = \mathbb{F}_p$ a déjà été vu, cf. II.3.9).

Nous allons maintenant étudier le cas où $k = \mathbb{Q}$. Bien entendu, la question de l'irréductibilité ou de l'existence de racines n'est pas modifiée si l'on multiplie le polynôme donné par une constante non nulle ; ceci permet de se ramener au cas d'un polynôme à coefficients *entiers*, et même *entiers premiers entre eux*.

Proposition 8.6 *Soit $P = a_0 + a_1X + \ldots + a_dX^d$ avec $a_i \in \mathbb{Z}$, et soit α une racine de P dans $\mathbb{Q}$. Écrivons $\alpha = r/s$ avec r et s entiers premiers entre eux. Alors r divise a_0 et s divise a_d.*

Démonstration. Il suffit de remarquer que

$$0 = s^dP(r/s) = a_0s^d + a_1rs^{d-1} + \ldots + a_dr^d$$

et que par suite r divise a_0s^d donc (lemme de Gauss, III.4.6) r divise a_0 puisqu'il est premier avec s^d. Le fait que s divise a_d se démontre de façon similaire. ∎

Lorsque $a_d = 1$, on obtient :

Corollaire 8.6.1 *Soit x un nombre rationnel qui est racine d'un polynôme unitaire à coefficients entiers. Alors x est entier.* ∎

8.6.2. *Exercice.* Généraliser 8.6 aux polynômes à coefficients dans un anneau principal.

8.6.3. *Remarque.* Dans la situation de 8.6, pour trouver toutes les racines rationnelles de P il "suffit" donc de trouver tous les diviseurs $r_1, \ldots, r_m$ de a_0, (sans oublier les diviseurs négatifs !), tous les diviseurs $s_1, \ldots, s_n$ de a_d et, pour chaque quotient $x = r_i/s_j$, de tester si $P(x) = 0$. Cette méthode est efficace pour les polynômes à "petits" coefficients.

Le problème de l'*irréductibilité* d'un polynôme donné dans $\mathbb{Q}[X]$ est en général difficile. Commençons par un exemple élémentaire :

Proposition 8.7 *Soient a un rationnel* positif *et n un entier > 1. Pour que le polynôme $X^n - a$ soit* réductible *dans $\mathbb{Q}[X]$, il faut et il suffit qu'il existe un diviseur $d > 1$ de n tel que a soit une puissance d-ième dans $\mathbb{Q}$.*

Démonstration. Posons $F = X^n - a$.

La condition de l'énoncé est suffisante (même si $a \leq 0$, d'ailleurs) : si $n = dm$ et $a = b^d$ alors $X^n - a = X^{md} - b^d$ qui est divisible par $X^m - b$.

La condition est nécessaire : dans $\mathbb{C}[X]$, F est produit des polynômes $X - \zeta a^{1/n}$ où ζ parcourt l'ensemble Γ des racines n-ièmes de l'unité. Par suite, si F est réductible

et si G est un diviseur non constant de F dans $\mathbb{Q}[X]$, de degré $j < n$ (et que nous pouvons supposer unitaire) alors G est produit des $X - \zeta a^{1/n}$ où ζ parcourt un sous-ensemble Δ à j éléments de Γ. En particulier le terme constant de G, qui est rationnel, est le produit des $\zeta a^{1/n}$ pour $\zeta \in \Delta$ donc est de module $a^{j/n}$. Nous avons donc trouvé j entier vérifiant $0 < j < n$ et $a^{j/n} \in \mathbb{Q}$. Mais si δ désigne le PGCD (positif) de j et n, l'identité de Bézout implique immédiatement que $a^{\delta/n} \in \mathbb{Q}$ d'où le résultat avec $d = n/\delta$. ∎

8.7.1. *Remarque.* Si de plus a est un *entier* positif, on voit grâce à 8.6.1 que l'on peut remplacer dans 8.7 la condition "a est une puissance d-ième dans $\mathbb{Q}$" par la condition "a est une puissance d-ième dans $\mathbb{N}$", facile à tester en pratique.

8.7.2. *Remarque.* On voit en particulier qu'il existe dans $\mathbb{Q}[X]$ des polynômes irréductibles de degré arbitrairement grand, et même de tout degré > 0.

8.7.3. *Remarque.* Dans le cas du polynôme $X^n + a$ (avec $a > 0$), on voit facilement que le critère précédent est encore valable si n est impair. Pour n pair c'est plus compliqué : ainsi nous avons vu (8.1.1) que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, alors que (exercice) $X^4 + 4$ ne l'est pas.

Voici maintenant un autre critère utile, que nous admettrons :

Théorème 8.8 (critère d'Eisenstein) *Soit $P = a_0 + a_1X + \ldots + a_dX^d \in \mathbb{Z}[X]$, avec $d > 0$. On suppose qu'il existe un nombre premier p vérifiant les conditions suivantes :*

(i) *p ne divise pas a_d ;*

(ii) *p divise a_i pour $i = 0, \ldots, d-1$;*

(iii) *p^2 ne divise pas a_0.*

Alors P est irréductible dans $\mathbb{Q}[X]$. ∎

8.8.1. *Exemple.* Pour $a \in \mathbb{Z}$ et n entier > 0, le polynôme $X^n - a$ est irréductible dans $\mathbb{Q}[X]$ dès qu'il existe un nombre premier p tel que $v_p(a) = 1$ (par exemple si $\pm a$ est premier). Que peut-on dire si a n'est pas entier ?

8.8.2. *Exemple.* Montrons que, pour p premier, le polynôme $P = \sum_{i=0}^{p-1} X^i = \frac{X^p-1}{X-1}$ est irréductible dans $\mathbb{Q}[X]$. Bien entendu le critère d'Eisenstein ne s'applique pas directement puisqu'aucun nombre premier ne divise un coefficient de P. Mais pour que P soit irréductible il faut et il suffit que le polynôme $F(Y) = P(Y + 1)$ le soit dans $\mathbb{Q}[Y]$; or ce "changement de variable" donne $F(Y) = ((Y + 1)^p - 1)/Y$, polynôme dont tous les coefficients non dominants sont divisibles par p d'après (II.7.3.1) et dont le terme constant est $\binom{p}{1} = p$. On peut donc appliquer 8.8 à F. ∎

8.8.3. *Exercice.* Par un changement de variable convenable, retrouver à l'aide du critère d'Eisenstein l'irréductibilité de X^4+1 dans $\mathbb{Q}[X]$ dèjà vue en 8.1.1. Généraliser aux polynômes de la forme $X^{2^s}+1$ ($s \in \mathbb{N}$).

8.9. *Exercices : quelques exemples en caractéristique positive.* Dans ce qui suit on désigne par k un corps de caractéristique $p > 0$.

8.9.1. *Le polynôme $X^p - a$.* On fixe un élément a de k, et l'on désigne par F le polynôme $X^p - a \in k[X]$. Montrer alors que :

(i) si a admet une racine p-ième $\alpha \in k$, on a $F = (X-\alpha)^p$ dans $k[X]$;

(ii) sinon, F est irréductible dans $k[X]$.

Indications pour (ii) : soit α une racine de F dans une extension convenable K de k. Appliquant (i) dans K on voit d'abord que tout diviseur unitaire de F est de la forme $(X-\alpha)^i$, $0 \leq i \leq p$. Si un tel polynôme appartient à $k[X]$, montrer alors que l'on a soit $i = 0$, soit $i = p$, soit $\alpha \in k$ (considérer le coefficient de X^{i-1}).

8.9.2. *Exercice.* Dans l'exercice 8.9.1 ci-dessus, si k est un corps *fini*, on est automatiquement dans le cas (i) d'après (II.7.4.3). Pour trouver un exemple où le cas (ii) se produit, il faut donc utiliser un corps *infini* de caractéristique p. Montrer que $k = (\mathbb{Z}/p\mathbb{Z})(T)$, $a = T$ est un tel exemple.

8.9.3. *Le polynôme $X^p - X - a$.* On fixe un élément a de k, et l'on désigne par F le polynôme $X^p - X - a \in k[X]$. On note k_0 l'unique sous-corps de k isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (qui est l'image de l'unique morphisme d'anneaux de $\mathbb{Z}$ dans k). Montrer alors que :

(i) $F(X+n) = F(X)$ pour tout $n \in k_0$;

(ii) si F admet une racine $\alpha \in k$, alors $F = \prod_{n \in k_0}(X - \alpha - n)$;

(iii) sinon, F est irréductible dans $k[X]$.

(Indications : (ii) se déduit aisément de (i), et la preuve de (iii) est analogue à celle du cas (ii) de 8.9.1. Observer aussi l'analogie avec l'argument de 8.7.)

8.9.4. *Cas particulier.* Dans 8.9.3 on prend $k = \mathbb{Z}/p\mathbb{Z}$. Montrer que F est irréductible si et seulement si $a \neq 0$. Construire ainsi un corps à p^p éléments.

9. Dérivation et applications

Dans tout ce paragraphe, k désigne un corps.

Définition 9.1 *Soit*

$$F = \sum_{i=0}^{d} a_i X^i$$

un polynôme à coefficients dans k. On appelle polynôme dérivé *(ou simplement dérivée) de F le polynôme*

$$D(F) = \sum_{i=1}^{d} i\, a_i X^{i-1}$$

encore noté F', ou $\frac{dF}{dX}$.

Proposition 9.2 *L'application $D : k[X] \to k[X]$ de* 9.1 *a les propriétés suivantes :*

(i) *D est k-linéaire, et $D(a) = 0$ pour tout $a \in k$;*

(ii) *pour tous F et G dans $k[X]$, on a $D(FG) = F.D(G) + D(F).G$;*

(iii) *pour tout $F \in k[X]$ et tout entier $n > 0$, on a $D(F^n) = n\, F^{n-1} D(F)$;*

(iv) *pour tous F et G dans $k[X]$, on a $D(G \circ F) = (D(G) \circ F).D(F)$;*

(v) *pour tout $F \in k[X]$, on a $\deg D(F) \leq \deg F - 1$. De plus on a égalité si $\deg F$ n'est pas divisible par $\mathrm{car}\,(k)$, et en particulier si $\mathrm{car}\,(k) = 0$ et si F n'est pas constant ;*

(vi) *si k est de caractéristique nulle, $D : k[X] \to k[X]$ est surjective et son noyau est k ;*

(vii) *si $k = \mathbb{R}$ ou $\mathbb{C}$, la fonction polynôme $x \mapsto F'(x)$ de k dans lui-même est la dérivée, au sens de l'analyse, de la fonction $x \mapsto F(x)$.*

Démonstration. (Les détails sont laissés au lecteur). L'assertion (i) est immédiate sur la définition.

Il résulte de (i) que les deux membres de (ii) sont bilinéaires en (F, G), de sorte qu'il suffit de montrer (ii) lorsque F et G sont des monômes ; c'est alors trivial.

(iii) se déduit de (ii) et d'une récurrence sur n.

Dans (iv), $G \circ F$ désigne évidemment le polynôme $G(F)$ obtenu en substituant F à X dans G. Les deux membres de la formule étant linéaires en G, il suffit de la montrer lorsque $G = X^n$ ($n \in \mathbb{N}$), ce qui n'est autre que (iii). (Sûr ?)

(v) : si $a_d X^d$ est le terme dominant de F (de sorte que $a_d \neq 0$), alors $D(F) = d\, a_d\, X^{d-1} + G$ avec $\deg(G) < d - 1$, d'où les assertions.

Les propriétés (vi) et (vii) sont laissées au lecteur. ∎

9.2.1. *Exercice.* Pourquoi n'a-t-on pas défini la dérivation comme on le fait pour les fonctions d'une variable réelle ? On aurait pu de cette façon faire l'économie de (vii).

9.2.2. *Exercice.* Donner un exemple (non constant) où l'inégalité de 9.2(v) est stricte.

9.2.3. *Exercice.* Si k est de caractéristique $p > 0$, montrer que $\mathrm{Ker}\,(D)$ est formé des polynômes de la forme $G(X^p)$ pour $G \in k[X]$. Si k est *parfait*, c'est-à-dire si tout élément de k a une racine p-ième, montrer que $\mathrm{Ker}\,(D)$ est aussi l'ensemble des puissances p-ièmes de $k[X]$.

9.3. *Exercice : dérivations d'une k-algèbre.* Soit A une k-algèbre. On appelle *k-dérivation* de A une application $\Delta : A \to A$ qui est k-linéaire et vérfife $\Delta(ab) = a\Delta(b) + \Delta(a)b$ pour tous a, $b \in A$.

9.3.1. Montrer que l'on aurait obtenu une définition équivalente en remplaçant la condition "Δ est k-linéaire" par "pour tout $\lambda \in k$ on a $\Delta(\lambda 1_A) = 0$".

9.3.2. Montrer que si Δ est une k-dérivation de A et $a \in A$, alors $a\Delta : A \to A$ (définie par $(a\Delta)(x) = a(\Delta(x))$ pour tout $x \in A$) est encore une k-dérivation de A.

9.3.3. Montrer que si Δ est une k-dérivation de A et $a \in A$, on a $D(a^n) = na^{n-1}\Delta(a)$ pour tout entier $n > 0$. En déduire que pour tout $P \in k[X]$ on a $\Delta(P(a)) = P'(a)\Delta(a)$.

9.3.4. Montrer que pour toute k-dérivation Δ de $k[X]$ il existe un unique $R \in k[X]$ tel que $\Delta = RD$ où D est la dérivation de 9.1. De plus on a $R = \Delta(X)$.

9.4. *Dérivées successives.* Pour $i \in \mathbb{N}$ on note $D^i : k[X] \to k[X]$ la i-ème itérée de D, définie par récurrence par les formules $D^0 = \mathrm{Id}_{k[X]}$ et $D^{i+1} = D \circ D^i$. On note aussi $F^{(i)} = D^i(F)$ pour tout $F \in k[X]$: c'est la "dérivée i-ème" de F. Noter que $F^{(0)} = F$ et $F^{(1)} = F'$; on utilise aussi les notations traditionnelles F'' et F''' pour $F^{(2)}$ et $F^{(3)}$. Enfin, par une récurrence immédiate, on a la formule

$$D^i(X^n) = \begin{cases} n(n-1)\cdots(n-i+1)\,X^{n-i} & \text{si } i \leq n \\ 0 & \text{si } i > n. \end{cases} \tag{9.4.1}$$

En conséquence, pour $F \in k[X]$ quelconque, on a $F^{(i)} = 0$ pour tout entier $i > \deg(F)$, ce qui pouvait aussi se déduire de 9.2(v). (Lecteur : est-ce vraiment pour tout F, ou pour $F \neq 0$?)

Proposition 9.5 *Soit $F \in k[X]$, et soit $\alpha \in k$ une racine de F. Alors on a :*

$$\mathrm{mult}_\alpha(F') \geq \mathrm{mult}_\alpha(F) - 1.$$

De plus l'égalité a lieu dans chacun des cas suivants :

(i) $\mathrm{mult}_\alpha(F)$ *n'est pas divisible par* car (k) *;*

(ii) car $(k) = 0$ *;*

(iii) $\mathrm{mult}_\alpha(F) = 1$.

Démonstration. (Détails laissés au lecteur !) Posant $m = \mathrm{mult}_\alpha(F)$, on écrit $F = (X-\alpha)^m G$ avec $G(\alpha) \neq 0$ (cf. 5.4.4). On en tire immédiatement $F' = (X-\alpha)^{m-1}H$ où $H = mG + (X-\alpha)G'$ d'où l'inégalité.

De plus on a égalité si et seulement si $H(\alpha) \neq 0$. Or $H(\alpha) = mG(\alpha)$ et $G(\alpha) \neq 0$, de sorte que l'égalité *équivaut* en fait à $m1_k \neq 0$, ce qui est la condition (i). Les deux autres n'en sont que des cas particuliers, mentionnés ici car ce sont les plus utiles. ∎

9.5.1. *Exercice.* Donner un exemple où l'inégalité de 9.5 est stricte.

9.5.2. *Exercice.* (de l'importance des "détails laissés au lecteur"...) On a supposé dans 9.5 que α était une racine de F, c'est-à-dire que $F(\alpha) = 0$. Cette hypothèse est-elle nécessaire ? Si oui, à quel(s) endroit(s) est-elle utilisée ? Que peut-on dire si $F(\alpha) \neq 0$?

9.5.3. *Exercice.* Soient $F \in k[X]$ et $\alpha \in k$, où k est un corps de caractéristique nulle. Déduire de 9.5(ii) que, pour $i \in \mathbb{N}$, on a

$$\begin{array}{lll} F^{(i)}(\alpha) & = 0 & \text{si} \quad i < \mathrm{mult}_\alpha(F) \\ F^{(i)}(\alpha) & \neq 0 & \text{si} \quad i = \mathrm{mult}_\alpha(F). \end{array}$$

En d'autres termes, la multiplicité se lit sur les dérivées successives en α.

(Rappel : le lecteur est invité, poliment mais fermement, à vérifier que ces assertions sont valables *dans tous les cas, sans exception*. Un énoncé mathématique n'est acceptable qu'à cette condition.)

Au fait, pourquoi n'a-t-on pas écrit "$F^{(\mathrm{mult}_\alpha(F))}(\alpha) \neq 0$" ?

9.6. *Application : recherche des racines multiples.* La proposition 9.5, et notamment le cas (iii), fournit un moyen commode pour trouver les racines multiples éventuelles :

Proposition 9.6.1 *Soit $F \in k[X]$, et soit K une extension de k. Soit Δ un PGCD de F et F' dans $k[X]$. Alors, pour tout $\alpha \in K$, les conditions suivantes sont équivalentes :*

(i) *α est racine multiple de F ;*

(ii) $F(\alpha) = F'(\alpha) = 0$ *;*

(iii) $\Delta(\alpha) = 0$.

Démonstration. L'équivalence de (i) et (ii) n'est qu'une reformulation du cas (iii) de 9.5. Il est trivial que (iii) implique (ii), et la réciproque résulte de l'identité de Bézout (ou, si l'on veut, du fait que Δ est encore un PGCD de F et G dans $K[X]$). ∎

Corollaire 9.6.2 *Soit $F \in k[X]$, et soit Ω une extension* algébriquement close *de k. Les conditions suivantes sont équivalentes :*

(i) *pour toute extension K de k, F n'a aucune racine multiple dans K ;*

(ii) *F n'a aucune racine multiple dans Ω ;*

(iii) $\mathrm{PGCD}\,(F, F') = 1$.

Démonstration. (Bien entendu la formulation de (iii) est abusive). Il est trivial que (i) implique (ii).

Montrons que (ii) implique (iii) : si $\mathrm{PGCD}\,(F, F')$ n'est pas constant il a une racine dans Ω et celle-ci est racine multiple de F d'après 9.6.1, d'où la conclusion.

Enfin, l'implication (iii)⇒(i) résulte de l'implication (i)⇒(iii) de 9.6.1 (ou de la réciproque ? Réfléchissez...). ∎

Corollaire 9.6.3 *Soit $F \in k[X]$. On suppose que k est de* caractéristique nulle, *et que F est* irréductible. *Alors F vérifie les conditions de* 9.6.2.

Démonstration. Comme $\deg(F) > 0$, et que k est de caractéristique nulle, on a $\deg(F') = \deg(F) - 1$ d'après 9.2(v). En particulier F' n'est pas multiple de F et est donc premier avec F puisque celui-ci est irréductible. ∎

9.6.4. *Remarque.* Au lieu de supposer que k est de caractéristique nulle, on peut seulement supposer que le degré de F n'est pas divisible par la caractéristique. Mais sans cette hypothèse, l'exercice 8.9.1 fournit un contre-exemple.

9.7. *Application : racines de l'unité.* Pour tout corps k et tout entier $n > 0$, posons comme au paragraphe 6 (que nous conseillons de relire !) :

$$\mu_n(k) = \{z \in k^* \mid z^n = 1\}. \tag{9.7.1}$$

Comme on l'a vu en 6.6, c'est un sous-groupe cyclique de k^*, dont l'ordre divise n.

Proposition 9.7.1 *Soit k un corps* algébriquement clos, *et soit n un entier > 0. Alors :*

(i) *si* $\mathrm{car}\,(k) = 0$, *$\mu_n(k)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$;*

(ii) *si* $\mathrm{car}\,(k) = p > 0$, *écrivons $n = p^r\, m$ où $r \in \mathbb{N}$ et où m est un entier premier à p. Alors $\mu_n(k)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.*

Démonstration. Posons $F = X^n - 1$, de sorte que $\mu_n(k)$ est l'ensemble des racines de F dans k. On a $F' = nX^{n-1}$. En particulier, *si* car (k) *ne divise pas* n, F et F' sont premiers entre eux donc F a toutes ses racines distinctes de sorte que leur nombre est égal à n puisque k est algébriquement clos. Ceci implique déjà l'assertion (i) dans tous les cas, et aussi (ii) lorsque $p \not| n$. Pour montrer (ii) dans le cas général, il suffit de remarquer que $F = X^{p^r m} - 1 = (X^m - 1)^{p^r}$ de sorte que $\mu_n(k) = \mu_m(k)$ et la conclusion résulte encore du cas "premier à p". ∎

9.7.2. *Remarque.* La proposition 9.7.1, jointe aux résultats du paragraphe 6, fournit une "liste complète" des sous-groupes finis de k^* pour un corps k algébriquement clos. On sait en effet d'après 6.3 que pour chaque entier $n > 0$, k^* admet au plus un sous-groupe d'ordre n qui, s'il existe, est cyclique et égal à $\mu_n(k)$. Il suffit donc de connaître la liste des ordres des groupes $\mu_n(k)$, et celle-ci est fournie par 9.7.1 : c'est l'ensemble des entiers > 0 non divisibles par car (k), c'est-à-dire l'ensemble de tous les entiers si car $(k) = 0$, et l'ensemble des entiers premiers à p si car $(k) = p > 0$.

Proposition 9.8 (formule de Taylor) *Soit k un corps* de caractéristique nulle *et soit*

$$F = \sum_{i=0}^{d} a_i X^i$$

un polynôme à coefficients a_i dans k. Alors :

(i) *pour tout $i \in \{0, \ldots, d\}$ on a $a_i = \frac{F^{(i)}(0)}{i!}$;*

(ii) *pour tout $\alpha \in k$, on a la formule*

$$F(X + \alpha) = \sum_{i=0}^{d} \frac{F^{(i)}(\alpha)}{i!} X^i.$$

Démonstration. (i) : un calcul immédiat utilisant (9.4.1) donne, sans hypothèse sur la caractéristique, $F^{(i)}(0) = i!\, a_i$; l'assertion en résulte.

(ii) : pour $\alpha = 0$ c'est une conséquence immédiate de (i). Le cas général s'en déduit en posant $G = F(X + \alpha)$: on a en effet $F^{(i)}(\alpha) = G^{(i)}(0)$ par récurrence sur i (le cas $i = 1$ résultant de 9.2(iv)). ∎

9.8.1. *Remarque.* En caractéristique quelconque on a encore la formule $F^{(i)}(0) = i!\, a_i$.

9.8.2. *Exercice.* Retrouver le résultat de l'exercice 9.5.3 en utilisant 9.8.

9.9. *Exercices : polynômes cyclotomiques.*

9.9.1. Soient k un corps, $n \geq 1$ un entier, z un élément de k^*. Montrer que les conditions suivantes sont équivvalentes :

(i) z est d'ordre n dans le groupe k^* ;

(ii) $|\mu_n(k)| = n$, et z est un générateur du groupe $\mu_n(k)$;

(iii) (si $k = \mathbb{C}$) z est de la forme $e^{2ih\pi/n}$ où h est un entier premier à n.

Montrer aussi que si ces conditions sont vérifiées, n n'est pas divisible par car (k).

9.9.2. Avec les notations de 9.9.1, un élément z de k^* vérifiant les conditions de l'exercice est appelé *racine n-ième primitive de l'unité* dans k^*.

On notera $\mu_n^0(k)$ l'ensemble des racines n-ièmes primitives de l'unité dans k^*. Montrer que, pour tout $n \geq 1$, $\mu_n(k)$ est réunion disjointe des ensembles $\mu_d^0(k)$ où d parcourt les diviseurs (positifs) de n.

Si n n'est pas divisible par car (k) et si k est algébriquement clos, montrer que $|\mu_n^0(k)|$ est égal à l'indicateur d'Euler $\varphi(n)$ défini en II.3.3.3. (Utiliser la structure de $\mu_n(k)$).

9.9.3. On appelle *n-ième polynôme cyclotomique* le polynôme

$$\Phi_n = \prod_{\alpha \in \mu_n^0(\mathbb{C})} (X - \alpha) \quad \in \mathbb{C}[X].$$

Montrer que Φ_n est unitaire de degré $\varphi(n)$, et que

$$X^n - 1 = \prod_{d|n} \Phi_d. \tag{9.9.3.1}$$

(Le produit porte sur les diviseurs positifs d de n).

9.9.4. Utiliser la formule (9.9.3.1), ou la définition, pour calculer Φ_n pour tout $n \leq 10$, et plus généralement pour montrer les formules suivantes :

(i) pour p premier et $s \geq 1$, $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$, et $\Phi_{p^s}(X) = \Phi_p(X^{p^{s-1}})$;

(ii) pour m impair, $\Phi_{2m}(X) = \Phi_m(-X)$;

(iii) pour a et b entiers premiers entre eux, $\Phi_{ab}(X) = \mathrm{PGCD}\,(\Phi_a(X^b), \Phi_b(X^a))$, le PGCD étant évidemment choisi unitaire.

9.9.5. Déduire de (9.9.3.1) que $\Phi_n \in \mathbb{Z}[X]$ pour tout $n \geq 1$. (On procédera par récurrence sur n : la formule (9.9.3.1) donne $X^n - 1 = \Phi_n \Psi_n$ où, par hypotèse de récurrence, $\Psi_n \in \mathbb{Z}[X]$; comme de plus Ψ_n est unitaire, la division euclidienne de $X^n - 1$ par Ψ_n est possible dans $\mathbb{Z}[X]$ (cf. 1.10), et elle donne nécessairement le même résultat que la division dans $\mathbb{C}[X]$, vu l'unicité de cette dernière).

9.9.6. Pour tout anneau A, on notera $\Phi_{n,A} \in A[X]$ le polynôme Φ_n vu comme polynôme à coefficients dans A (ceci a un sens grâce à 9.9.5).

Si k est un corps algébriquement clos dont la caractéristique ne divise pas n, montrer que l'on a dans $k[X]$ la formule $\Phi_{n,k} = \prod_{\alpha \in \mu_n^0(k)} (X - \alpha)$. (Indication : utilisant la formule (9.9.3.1), remarquer que les éléments de $\mu_n^0(k)$ sont racines de $\Phi_{n,k}$ et conclure par un argument de degré.)

9.9.7. Soit k un corps fini à q éléments, où q est premier avec n. Montrer que les conditions suivantes sont équivalentes :

(i) $\Phi_{n,k}$ a une racine dans $k[X]$;

(ii) $|\mu_n(k)| = n$;

(iii) $q \equiv 1 \pmod{n}$.

(Pour l'équivalence de (i) et (ii) utiliser 9.9.6 ; (ii)⇒(iii) se déduit du théorème de Lagrange, et (iii)⇒(ii) du fait que k^* est cyclique).

9.9.8. *Application au théorème de la progression arithmétique.* Soient n un entier ≥ 1, N un entier quelconque. Montrer que $\Phi_n(N)$ est premier avec N. (Considérer le terme constant de Φ_n).

En déduire que si p est un diviseur premier de $\Phi_n(nM)$, où M est un entier arbitraire, on a $p \equiv 1 \pmod{n}$. (Remarquer que p ne divise pas n d'après ce qui précède, et d'autre part que $\Phi_{n,\mathbb{F}_p}$ a une racine dans $\mathbb{F}_p$, à savoir la classe de nM ; appliquer alors 9.9.7).

Conclure enfin qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

Bien entendu cet argument généralise III.7.2.7.

10. Notions sur les polynômes à plusieurs indéterminées

Les résultats de ce paragraphe sont, pour la plupart, énoncés sans démonstration. Les démonstrations sont analogues à celles du cas d'une indéterminée, ou bien s'en déduisent par récurrence.

La lettre n désigne un entier naturel.

10.1. *Définition(s).* Soient A un anneau. On peut définir de deux manières équivalentes (au moins) l'anneau $A_n = A[X_1, \ldots, X_n]$ des polynômes en n indéterminées $X_1, \ldots, X_n$ à coefficients dans A :

- par récurrence sur n, en posant $A_0 = A$ et $A_{n+1} = A_n[X_{n+1}]$;
- en définissant un élément

$$P = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n}\, X_1^{i_1} \cdots X_n^{i_n} \tag{10.1.1}$$

de A_n comme la famille $(a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ de ses coefficients, soumise aux seules conditions que les $a_{i_1,\ldots,i_n}$ soient dans A et presque tous nuls, et en définissant l'addition et la multiplication formellement, à la manière de 1.2.

La première méthode a l'avantage de la simplicité, et permet de démontrer facilement les propriétés de $A[X_1, \ldots, X_n]$ par récurrence sur n. Elle a l'inconvénient de détruire la symétrie : il n'est pas clair sur cette définition qu'il existe un automorphisme de $A[X_1, X_2]$ qui échange X_1 et X_2, et plus généralement que le groupe symétrique $\mathfrak{S}_n$ opère sur $A[X_1, \ldots, X_n]$ par permutation des X_i.

10.2. *Multi-indices.* Plutôt que la notation lourde (10.1.1), on écrit souvent

$$P = \sum_{I\in\mathbb{N}^n} a_I\, X^I \tag{10.2.1}$$

où, pour $I = (i_1, \ldots, i_n) \in \mathbb{N}^n$, la notation X^I désigne le monôme $X_1^{i_1} \cdots X_n^{i_n}$.

10.3. *Propriétés élémentaires.* Avec les notations de 10.1, $A[X_1, \ldots, X_n]$ est un anneau commutatif unitaire ; A s'identifie au sous-anneau de $A[X_1, \ldots, X_n]$ formé des polynômes "constants", i.e. (avec la notation (10.2.1)) tels que $a_I = 0$ pour tout $I \neq (0, \ldots, 0)$.

10.4. *Degré.* Le *degré total*, ou simplement degré, d'un monôme $X_1^{i_1} \cdots X_n^{i_n}$ est la somme $i_1 + \ldots + i_n$ de ses exposants ; son *degré par rapport à l'indéterminée* X_j est l'exposant i_j.

On définit le degré total $\deg P$ (resp. le degré en X_j, $\deg_{X_j} P$) d'un polynôme $P \in A[X_1, \ldots, X_n]$ comme étant $-\infty$ si $P = 0$, et, sinon, comme le maximum des degrés totaux (resp. des degrés en X_j) des monômes dont le coefficient dans P n'est pas nul.

10.5. *Cas intègre.* Si A est intègre (par exemple si A est un corps), on a $\deg(PQ) = \deg P + \deg Q$ pour tous P et $Q \in A[X_1, \ldots, X_n]$, et de même pour le degré en X_j. On en déduit que, dans ce cas, $A[X_1, \ldots, X_n]$ est intègre et $A[X_1, \ldots, X_n]^\times = A^\times$.

10.6. *Évaluation, fonctions polynômes.* Soit P le polynôme (10.1.1), et soit $x = (x_1, \ldots, x_n) \in A^n$. On définit $P(x) = P(x_1, \ldots, x_n) \in A$ par la formule

$$P(x) = \sum_{I \in \mathbb{N}^n} a_I \, x^I = \sum_{(i_1, \ldots, i_n) \in \mathbb{N}^n} a_{i_1, \ldots, i_n} \, x_1^{i_1} \cdots x_n^{i_n}.$$

L'application de A^n dans A ainsi définie est la *fonction polynôme* associée à P. Si on la note $\widetilde{P} : A^n \to A$, on a ainsi défini une application $P \mapsto \widetilde{P}$ de $A[X_1, \ldots, X_n]$ dans l'anneau A^{A^n} qui, comme dans le cas d'une indéterminée (1.11), est un morphisme d'anneaux. (En particulier, pour $x \in A^n$ fixé, l'application $P \mapsto P(x)$ de $A[X_1, \ldots, X_n]$ dans A est un morphisme d'anneaux.)

Le morphisme $P \mapsto \widetilde{P}$ ci-dessus n'est, en général, ni injectif ni surjectif. Cependant :

Proposition 10.6.1 *Soit k un corps* infini. *Alors le morphisme*

$$\begin{array}{ccc} k[X_1, \ldots, X_n] & \longrightarrow & k^{k^n} \\ P & \mapsto & \widetilde{P} \end{array}$$

est injectif. Autrement dit, pour qu'un polynôme $P \in k[X_1, \ldots, X_n]$ soit nul il faut et il suffit que $P(x) = 0$ pour tout $x \in k^n$.

Démonstration. Récurrence sur n. Le cas $n = 1$ est déjà connu par 5.6(iv) (et le cas $n = 0$, qu'en pensez-vous ?). Pour $n > 1$ donné, supposons la proposition démontrée pour les polynômes à $n - 1$ indéterminées, et soit $P \in k[X_1, \ldots, X_n]$ tel que $\widetilde{P} = 0$. On peut écrire P sous la forme (dite "ordonnée par rapport à X_n")

$$P(X_1, \ldots, X_n) = \sum_{i=0}^{d} F_i(X_1, \ldots, X_{n-1}) \, X_n^i$$

où les F_i sont dans $k[X_1, \ldots, X_{n-1}]$. Soit $(x_1, \ldots, x_{n-1}) \in k^{n-1}$ et considérons le polynôme $Q = P(x_1, \ldots, x_{n-1}, X_n) \in k[X_n]$. L'hypothèse $\widetilde{P} = 0$ implique que $Q(t) = P(x_1, \ldots, x_{n-1}, t)$ est nul pour tout $t \in k$. Donc $Q = 0$ d'après le cas $n = 1$.

Autrement dit, on a $F_i(x_1, \ldots, x_{n-1}) = 0$ pour tout i (ce sont les coefficients de Q). Ceci étant vrai pour tout $(x_1, \ldots, x_{n-1}) \in k^{n-1}$, l'hypothèse de récurrence implique que les F_i sont nuls, donc que $P = 0$. ∎

10.6.2. *Exercice.* Généralisation de 1.11.2 : si k est un corps fini, le morphisme de 10.6.1 est surjectif.

10.6.3. *Exercice.* Généraliser 10.6.1 comme suit. Soient k un corps et $S_1, \ldots, S_n$ n parties infinies de k, et soit $S = \prod_{j=1}^{n} S_j \subset k^n$. Soit $P \in k[X_1, \ldots, X_n]$ tel que $P(x) = 0$ pour tout $x \in S$. Montrer que $P = 0$.

10.6.4. *Exercice.* Soit $P \in k[X_1, \ldots, X_n]$ un polynôme non nul. Déduire de 10.6.3 les propriétés suivantes, et expliquer dans chaque cas l'hypothèse sur k :
1°) si car $(k) = 0$, il existe des *entiers* $a_1, \ldots, a_n$ tels que $P(a_1, \ldots, a_n) \neq 0$;
2°) si k est un sous-corps de $\mathbb{C}$, alors $\{x \in k^n \mid P(x) \neq 0\}$ est un *ouvert dense* de k^n (pour la topologie induite par la topologie naturelle de $\mathbb{C}^n$).

10.6.5. *Exercice.* Généraliser 10.6.1 au cas d'un anneau intègre infini. (On pourra utiliser 10.6.3 et le corps des fractions).

10.7. *Structure d'algèbre.* Soit k un corps. L'anneau $k[X_1, \ldots, X_n]$ a une structure naturelle de k-algèbre : le produit d'un polynôme P par un élément λ de k s'obtient en multipliant les coefficients de P par λ, et le morphisme structural (3.2.2) associe à tout $\lambda \in k$ le polynôme "constant" dont le coefficient de multidegré $(0, \ldots, 0)$ est égal à λ, les autres étant nuls.

Si B désigne une k-algèbre et $b = (b_1, \ldots, b_n) \in B^n$, l'application $P \mapsto P(b)$ d'évaluation en b, définie comme en 10.6, est un morphisme de $k[X_1, \ldots, X_n]$ dans B, qui envoie X_j sur b_j. Réciproquement, tout morphisme de k-algèbres de $k[X_1, \ldots, X_n]$ dans B est de cette forme, pour un unique $b \in B^n$: c'est la *propriété universelle de* $k[X_1, \ldots, X_n]$, qui peut s'exprimer en disant que, pour toute k-algèbre B, l'application

$$\begin{array}{rcl} \mathrm{Hom}_{k-\mathrm{alg}}(k[X_1, \ldots, X_n], B) & \longrightarrow & B^n \\ f & \longmapsto & (f(X_1), \ldots, f(X_n)) \end{array}$$

est bijective.

10.8. *Fractions rationnelles.* Si k est un corps, le corps des fractions de l'anneau intègre $k[X_1, \ldots, X_n]$ s'appelle le *corps des fractions rationnelles en* $X_1, \ldots, X_n$; on le note $k(X_1, \ldots, X_n)$.

11. Relations entre coefficients et racines

11.1. *Polynômes symétriques élémentaires.* Soient n et d deux entiers naturels. On définit le *d-ième polynôme symétrique élémentaire ${}^n\Sigma_d$ en les n indéterminées* $X_1, \ldots, X_n$ par

$$ {}^n\Sigma_d = \sum_{\substack{I \subset \{1,\ldots,n\} \\ |I|=d}} \prod_{i \in I} X_i \quad \in \mathbb{Z}[X_1, \ldots, X_n] $$

(la sommation porte sur les parties I à d éléments de l'ensemble $\{1, \ldots, n\}$).

11.2. *Remarques, propriétés élémentaires.* L'entier n est souvent omis : s'il n'y pas de confusion possible, on note Σ_d au lieu de ${}^n\Sigma_d$.

11.2.1. *Valeurs spéciales de d.* On a :

$$\begin{array}{lcl} {}^n\Sigma_d & = & 0 \quad \text{si } d > n \\ {}^n\Sigma_0 & = & 1 \\ {}^n\Sigma_1 & = & \sum_{i=1}^n X_i \\ {}^n\Sigma_2 & = & \sum_{1 \le i < j \le n} X_i X_j \\ {}^n\Sigma_n & = & \prod_{i=1}^n X_i \end{array}$$

11.2.2. *Petites valeurs de n.* Pour $n \le 3$, les ${}^n\Sigma_d$ non nuls sont :

$$\begin{array}{llll} {}^0\Sigma_0 = 1 & & & \\ {}^1\Sigma_0 = 1 & {}^1\Sigma_1 = X_1 & & \\ {}^2\Sigma_0 = 1 & {}^2\Sigma_1 = X_1 + X_2 & {}^2\Sigma_2 = X_1X_2 & \\ {}^3\Sigma_0 = 1 & {}^3\Sigma_1 = X_1 + X_2 + X_3 & {}^3\Sigma_2 = X_1X_2 + X_2X_3 + X_3X_1 & {}^3\Sigma_3 = X_1X_2X_3. \end{array}$$

11.2.3. *Relations de récurrence.* Pour $i \ge 1$ et $n \ge 1$, on a :

$$ {}^n\Sigma_i = {}^{n-1}\Sigma_i + X_n \, {}^{n-1}\Sigma_{i-1} $$

et en particulier

$$ {}^n\Sigma_i(X_1, \ldots, X_{n-1}, 0) = {}^{n-1}\Sigma_i. $$

11.2.4. Pour tout $d \in \{1, \ldots, n\}$, ${}^n\Sigma_d$ est un polynôme *homogène de degré d* (tous ses termes non nuls sont de degré total d). D'autre part il est de degré 1 par rapport à chacune des indéterminées X_j.

11.2.5. ${}^n\Sigma_d$ est un polynôme *symétrique* en $X_1, \ldots, X_n$: pour tout $\sigma \in \mathfrak{S}_n$, on a $\Sigma_d(X_1, \ldots, X_n) = \Sigma_d(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

11.2.6. *Changement d'anneau de base.* Par définition, les ${}^n\Sigma_d$ sont des polynômes à coefficients dans $\mathbb{Z}$; cependant, si A est un anneau, on peut définir des polynômes

${}^n\Sigma_{d,A}$ à coefficients dans A par les mêmes formules ; s'il n'y a pas de confusion, on pourra désigner ces polynômes également par ${}^n\Sigma_d$. Les formules ci-dessus sont encore valables dans ce contexte. Noter que comme les coefficients non nuls des Σ_d sont égaux à 1, on a $\Sigma_{d,A} \neq 0$ chaque fois que $\Sigma_d \neq 0$, sauf évidemment si l'anneau A est nul.

Proposition 11.3 *Soient A un anneau, n un entier naturel et $\alpha_1, \ldots, \alpha_n$ n éléments de A. On a dans $A[X]$ la relation*

$$\prod_{j=1}^{n}(X - \alpha_j) = \sum_{i=0}^{n}(-1)^i\, {}^n\Sigma_i(\alpha_1, \ldots, \alpha_n)\, X^{n-i}.$$

Démonstration. Lorsque l'on développe le membre de gauche, on obtient la somme suivante (de 2^n termes) :

$$\sum_{I \subset \{1,\ldots,n\}} (\prod_{j \in I}(-\alpha_j))(\prod_{j \notin I} X)$$

indexée par les parties I de $\{1, \ldots, n\}$. Pour chaque $i \in \{0, \ldots, n\}$, le terme en X^{n-i} s'obtient en regroupant les termes avec $|I| = i$; la formule en résulte en appliquant la définition des Σ_i. ∎

11.3.1. *Remarque.* On peut notamment prendre $A = \mathbb{Z}[X_1, \ldots, X_n]$ et $\alpha_j = X_j$, ce qui donne l'identité polynomiale dans $\mathbb{Z}[X, X_1, \ldots, X_n]$

$$\prod_{j=1}^{n}(X - X_j) = \sum_{i=0}^{n}(-1)^i\, {}^n\Sigma_i\, X^{n-i}.$$

Réciproquement cette identité entraîne 11.3 : il suffit d'évaluer les deux membres en $(X, \alpha_1, \ldots, \alpha_n) \in A[X]^{n+1}$.

11.3.2. *Remarque.* En "faisant $X = X_j$" dans 11.3.1 (c'est-à-dire en évaluant les deux membres en $(X_j, X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]^{n+1}$) on obtient notamment les identités (pour $j \in \{1, \ldots, n\}$) :

$$X_j^n - \Sigma_1 X_j^{n-1} + \ldots + (-1)^n \Sigma_n = 0.$$

11.3.3. *Exercice.* Démontrer directement les identités de 11.3.2 à l'aide des relations de récurrence 11.2.3. Ensuite en déduire 11.3.1 — et donc 11.3 — en raisonnant dans $K[X]$ où K est le corps des fractions de $\mathbb{Z}[X_1, \ldots, X_n]$ (remarquer que le polynôme unitaire $\sum_{i=0}^{n}(-1)^i\, \Sigma_i\, X^{n-i} \in K[X]$ admet $X_1, \ldots, X_n \in K$ comme racines et appliquer 5.6(ii)).

Corollaire 11.4 ("relations entre coefficients et racines") *Soient k un corps, et*

$$P = \sum_{i=0}^{n} a_i \, X^{n-i}$$

un polynôme à coefficients a_i dans k, avec $a_0 \neq 0$ (attention à la numérotation des coefficients !). *On suppose que P est* décomposé (2.9) *dans $k[X]$, et l'on note $\alpha_1, \ldots, \alpha_n \in k$ les racines de P, comptées avec multiplicités. Alors on a pour tout $i \in \{0, \ldots, n\}$ la relation*

$$(-1)^i \, \frac{a_i}{a_0} = \Sigma_i(\alpha_1, \ldots, \alpha_n).$$

Démonstration. Il suffit d'appliquer 11.3 et la formule

$$\frac{1}{a_0} \, P = \prod_{j=1}^{n} (X - \alpha_j)$$

qui résulte de 5.6(ii). ∎

11.4.1. *Remarque.* Attention aux signes !

11.4.2. *Remarque.* Même si P n'est pas décomposé dans $k[X]$ il l'est dans $L[X]$ où L est une extension convenable de k ; les formules s'appliquent alors, en notant α_j les racines de P dans L. On en conclut notamment que $\Sigma_i(\alpha_1, \ldots, \alpha_n) \in k$ pour tout i, même si les α_j ne sont pas dans k.

11.4.3. *Exemple.* Pour $n = 2$ et $P = aX^2 + bX + c$ (avec $a \neq 0$) on retrouve les relations bien connues : $\alpha + \beta = -b/a, \alpha\beta = c/a$, où α et β sont les racines de P.

12. Polynômes et fonctions symétriques

12.1. *Actions de* $\mathfrak{S}_n$. Si E est un ensemble quelconque et n un entier naturel, de l'action à gauche du groupe symétrique $\mathfrak{S}_n$ sur $\{1,\dots,n\}$ on déduit une action à *droite* du même groupe sur E^n en posant

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

pour $\sigma \in \mathfrak{S}_n$ et $x_1,\dots,x_n \in E$. (On voit clairement qu'il s'agit d'une action à droite en remarquant que E^n n'est autre que l'ensemble des applications de $\{1,\dots,n\}$ dans E, et que l'action en question associe à $\sigma \in \mathfrak{S}_n$ et à $x : \{1,\dots,n\} \to E$ l'application $x \circ \sigma : \{1,\dots,n\} \to E$.)

Si F est un autre ensemble on en déduit derechef une action *à gauche* de $\mathfrak{S}_n$ sur l'ensemble F^{E^n} des applications de E^n dans F en posant, pour $f : E^n \to F$, $\sigma \in \mathfrak{S}_n$, et $x_1,\dots,x_n \in E$:

$$\begin{aligned}(\sigma f)(x_1,\dots,x_n) &= f((x_1,\dots,x_n)\sigma)\\ &= f(x_{\sigma(1)},\dots,x_{\sigma(n)})\end{aligned}$$

(“passer à un ensemble de fonctions renverse le sens de l'action”).

12.2. *Applications (ou fonctions) symétriques.* Une application $f : E^n \to F$ est dite *symétrique* si c'est un point fixe pour l'action de $\mathfrak{S}_n$ sur F^{E^n}, ce qui se traduit explicitement par la “formule”

$$\forall (x_1,\dots,x_n) \in E^n, \quad f(x_{\sigma(1)},\dots,x_{\sigma(n)}) = f(x_1,\dots,x_n).$$

Nous noterons $\mathrm{Sym}\,(E^n,F) \subset F^{E^n}$ l'ensemble de ces applications symétriques.

Si F est un groupe (resp. un anneau, resp. un corps k) alors F^{E^n} a une structure naturelle de groupe (resp. d'anneau, resp. de k-algèbre) et $\mathfrak{S}_n$ opère sur F^{E^n} par automorphismes de ladite structure, de sorte que $\mathrm{Sym}\,(E^n,F)$ est un sous-groupe (resp. un sous-anneau, resp. une sous-k-algèbre) de F^{E^n}.

Dire qu'une application $f : E^n \to F$ est symétrique équivaut à dire qu'elle est constante sur chaque orbite pour l'action de $\mathfrak{S}_n$ sur E^n ; autrement dit, on a une bijection naturelle entre $\mathrm{Sym}\,(E^n,F)$ et l'ensemble des applications de $E^n/\mathfrak{S}_n$ dans F (bijection qui est, le cas échéant, un isomorphisme de groupes, resp. d'anneaux, resp. de k-algèbres).

12.3. Si l'on prend pour E un corps k, on dispose en particulier des n applications symétriques de k^n dans k données par les polynômes symétriques élémentaires ${}^n\Sigma_i$ ($i = 1,\dots,n$) de 11.1 (on oublie ${}^n\Sigma_0$, sans intérêt). On peut les “regrouper” en une

seule application symétrique à valeurs dans k^n, à savoir

$$\begin{array}{rcl} {}^n\mathbf{\Sigma} : k^n & \longrightarrow & k^n \\ (x_1, \ldots, x_n) & \longmapsto & ({}^n\Sigma_1(x_1, \ldots, x_n), \ldots, {}^n\Sigma_n(x_1, \ldots, x_n)). \end{array} \tag{12.3.1}$$

Comme cette application est symétrique, elle passe au quotient en une application

$$\begin{array}{rcl} {}^n\overline{\mathbf{\Sigma}} : k^n/\mathfrak{S}_n & \longrightarrow & k^n \\ \text{orbite de } (x_1, \ldots, x_n) & \longmapsto & ({}^n\Sigma_1(x_1, \ldots, x_n), \ldots, {}^n\Sigma_n(x_1, \ldots, x_n)). \end{array} \tag{12.3.2}$$

S'il n'y a pas d'ambiguïté sur n — c'est-à-dire le plus souvent — on écrira $\mathbf{\Sigma}$ et $\overline{\mathbf{\Sigma}}$ au lieu de ${}^n\mathbf{\Sigma}$ et ${}^n\overline{\mathbf{\Sigma}}$.

12.3.1. *Exercice.* Expliciter ${}^n\mathbf{\Sigma}$ pour chaque $n \leq 3$.

12.4. *Exercice.* On garde les notations de 12.3.

12.4.1. $\mathbf{\Sigma}$ est-elle k-linéaire ? Et $\overline{\mathbf{\Sigma}}$, qu'en pensez-vous ?

12.4.2. Soit V un k-espace vectoriel. Montrer que les applications k-linéaires symétriques de k^n dans V sont les applications de la forme $(x_1, \ldots, x_n) \mapsto (x_1 + \cdots + x_n)v$ (pour $v \in V$). (Suggestion : commencer par le cas où $V = k$).

12.4.3. Soit H le sous-espace vectoriel de k^n engendré par les $\sigma(x) - x$ ($\sigma \in \mathfrak{S}_n$, $x \in k^n$). Montrer que $H = \{(x_1, \ldots, x_n) \in k^n \mid x_1 + \cdots + x_n = 0\}$, de deux manières :

- par le calcul ;
- en utilisant 12.4.2 (considérer l'espace vectoriel quotient k^n/H).

Proposition 12.5 *Soit k un corps, et soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n) \in k^n$. Les conditions suivantes sont équivalentes :*

(i) *α et β sont dans la même orbite pour l'action naturelle de $\mathfrak{S}_n$ sur k^n ; autrement dit, il existe $\sigma \in \mathfrak{S}_n$ tel que $\beta_j = \alpha_{\sigma(j)}$ pour tout $j \in \{1, \ldots, n\}$;*

(ii) *pour tout ensemble F et toute application symétrique $f : E^n \to F$, on a $f(\alpha) = f(\beta)$;*

(iii) *avec les notations de 12.3, on a $\mathbf{\Sigma}(\alpha) = \mathbf{\Sigma}(\beta)$; en d'autres termes, on a $\Sigma_i(\alpha_1, \ldots, \alpha_n) = \Sigma_i(\beta_1, \ldots, \beta_n)$ pour tout $i \in \{1, \ldots, n\}$.*

Démonstration. Il est clair que (i) implique (ii) (et ceci n'a rien à voir avec le fait que k soit un corps, non plus que la réciproque, qui est un exercice facile).

D'autre part (ii) implique (iii) puisque $\mathbf{\Sigma}$ est symétrique.

Montrons enfin que (iii) implique (i) (ce qui est la partie intéressante de l'énoncé). La condition (iii) implique d'après 11.3 que

$$\prod_{j=1}^{n}(X-\alpha_j)=\prod_{j=1}^{n}(X-\beta_j)$$

d'où la propriété (i) par unicité de la décomposition en facteurs irréductibles. ∎

12.6. *Remarques.*

12.6.1. Si l'on ne suppose pas que k soit un corps, l'implication (iii) ⇒ (i) est fausse : prendre $k=\mathbb{Z}/4\mathbb{Z}$, $n=2$, $\alpha=(0,0)$ et $\beta=(2 \bmod 4, 2 \bmod 4)$.

12.6.2. Par contre les implications (i) ⇔ (ii) ⇒ (iii), qui sont des trivialités, sont valables pour un anneau quelconque.

12.6.3. L'implication (i) ⇒ (iii), notamment, n'est qu'une reformulation de l'existence de l'application $\overline{\mathbf{\Sigma}}$ de (12.3.2).

12.6.4. L'implication (iii) ⇒ (i), elle, peut aussi s'exprimer en disant que $\overline{\mathbf{\Sigma}}$: $k^n/\mathfrak{S}_n \to k^n$ est *injective*. On évoque aussi cette propriété en disant que les Σ_i *séparent les orbites* pour l'action de $\mathfrak{S}_n$ sur k^n : étant données deux orbites distinctes, il existe $i\in\{1,\dots,n\}$ tel que Σ_i prenne des valeurs distinctes sur ces deux orbites.

12.6.5. Ce qui précède conduit naturellement à se demander si l'application $\overline{\mathbf{\Sigma}}$ est surjective, et plus généralement quelle est son image dans k^n, c'est-à-dire l'image de $\mathbf{\Sigma}$.

Or, dire qu'un point $(s_1,\dots,s_n)\in k^n$ appartient à l'image de $\mathbf{\Sigma}$ revient à dire qu'il existe $\alpha=(\alpha_1,\dots,\alpha_n)\in k^n$ tel que l'on ait dans $k[X]$

$$X^n+\sum_{i=1}^{n}(-1)^i\,s_i\,X^{n-i}=\prod_{j=1}^{n}(X-\alpha_j)$$

(appliquer la définition de $\mathbf{\Sigma}$ et 11.3). Autrement dit, *l'image de* $\overline{\mathbf{\Sigma}}$ *est formée des* $(s_1,\dots,s_n)\in k^n$ *tels que le polynôme* $X^n-s_1X^{n-1}+\cdots+(-1)^ns_0$ *soit décomposé dans* $k[X]$.

En particulier on obtient :

Corollaire 12.7 *Avec les hypothèses et notations de* 12.3*, supposons de plus que* k *soit* algébriquement clos*. Alors l'application*

$$^n\overline{\mathbf{\Sigma}} : k^n/\mathfrak{S}_n \longrightarrow k^n$$

de (12.3.2) *est bijective.* ∎

12.7.1. *Exercice.* Prouver, ou réfuter, la réciproque de 12.7.

Corollaire 12.8 *Soient k un corps algébriquement clos, n un entier, F un ensemble, et $f : k^n \to F$ une application symétrique. Alors il existe une unique application $\widehat{f} : k^n \to F$ telle que $f = \widehat{f} \circ {}^n\mathbf{\Sigma}$, c'est-à-dire telle que*

$$\forall (x_1, \ldots, x_n) \in k^n, \quad f(x_1, \ldots, x_n) = \widehat{f}\,({}^n\Sigma_1(x_1, \ldots, x_n), \ldots, {}^n\Sigma_n(x_1, \ldots, x_n)).$$

Démonstration. Ce n'est qu'une reformulation de 12.7, puisque f passe au quotient par $k^n/\mathfrak{S}_n$. ∎

12.8.1. *Exercice.* Si k n'est plus supposé algébriquement clos, montrer que 12.8 est encore valable à l'exception de l'assertion d'unicité.

12.8.2. *Remarque.* On formule souvent 12.8 en disant que "toute fonction symétrique sur k^n peut s'exprimer à l'aide des polynômes symétriques élémentaires". L'expression "peut s'exprimer" ne signifie pas que (avec les notations de l'énoncé) si f est donnée par une "formule" il en est de même de $\widehat{f}$. C'est pourtant ce que l'on constate souvent dans la pratique ; nous verrons plus bas, notamment, que si f est une fonction polynôme il en est de même de $\widehat{f}$. Plus généralement, on a souvent besoin d'énoncés du genre "si f possède telle propriété (continuité par exemple) il en est de même de $\widehat{f}$" : voir par exemple l'exercice 12.9 ci-dessous.

12.8.3. *Exercice.* On prend $k = \mathbb{C}$, $n = 2$, $F = \mathbb{R}$. Essayer de donner une formule pour $\widehat{f} : \mathbb{C}^2 \to \mathbb{R}$ dans les deux cas suivants :
(a) $f(x, y) = |x - y|$; (b) $f(x, y) = e^x + e^y$.

12.9. *Exercice.* Pour $k = \mathbb{C}$ et n quelconque on considère l'application $\mathbf{\Sigma} : \mathbb{C}^n \to \mathbb{C}^n$.

12.9.1. Montrer que $\mathbf{\Sigma}$ est continue.

12.9.2. Montrer que $\mathbf{\Sigma}$ est *propre* (si K est un compact de $\mathbb{C}^n$ alors $\mathbf{\Sigma}^{-1}(K)$ est un compact de $\mathbb{C}^n$).

12.9.3. En déduire que $\mathbf{\Sigma}$ est *fermée* (si Z est un fermé de $\mathbb{C}^n$ alors $\mathbf{\Sigma}(Z)$ est un fermé de $\mathbb{C}^n$).

12.9.4. En déduire que $\mathbf{\Sigma}$ est *ouverte* (si Z est un ouvert de $\mathbb{C}^n$ alors $\mathbf{\Sigma}(Z)$ est un ouvert de $\mathbb{C}^n$). (Indication : remarquer que $Z' = \bigcup_{\sigma \in \mathfrak{S}_n} Z\sigma$ est ouvert, que $\mathbf{\Sigma}(Z) = \mathbf{\Sigma}(Z')$, et que le complémentaire de $\mathbf{\Sigma}(Z')$ est l'image par $\mathbf{\Sigma}$ du complémentaire de Z' ; appliquer alors 12.9.3).

12.9.5. Dans 12.8 on prend $k = \mathbb{C}$ et on prend pour F un espace topologique quelconque. Déduire de 12.9.1 et 12.9.3 (ou 12.9.4) que f est continue si et seulement si $\widehat{f}$ est continue.

12.10. *Polynômes symétriques.* Si A est un anneau, le groupe $\mathfrak{S}_n$ opère à gauche sur l'anneau $A[X_1, \ldots, X_n]$: pour $\sigma \in \mathfrak{S}_n$ et $P \in A[X_1, \ldots, X_n]$ on pose $\sigma P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \in A[X_1, \ldots, X_n]$. Cette action est compatible avec l'action de $\mathfrak{S}_n$ sur l'ensemble A^{A^n} : on a $\widetilde{\sigma P} = \sigma \widetilde{P}$ où $\widetilde{P} : A^n \to A$ est la fonction polynôme définie par P. On qualifie de *symétriques* les éléments de $A[X_1, \ldots, X_n]$ fixes sous l'action de $\mathfrak{S}_n$. L'ensemble des polynômes symétriques est un sous-anneau de $A[X_1, \ldots, X_n]$, qui contient A et les polynômes symétriques élémentaires $\Sigma_1, \ldots, \Sigma_n$ définis en 11.1. Il contient notamment tout polynôme de la forme $F(\Sigma_1, \ldots, \Sigma_n)$ où F est un polynôme à coefficients dans A, à n indéterminées que nous noterons $S_1, \ldots, S_n$.

12.10.1. *Exercice.* Soit $P \in A[X_1, \ldots, X_n]$. Montrer que si P est symétrique alors la fonction polynôme $\widetilde{P}$ est symétrique, et que la réciproque est vraie si A est un corps infini.

12.10.2. *Remarque.* Il est facile en pratique de reconnaître un polynôme symétrique : cette propriété se lit sur les coefficients. Cependant, éviter la précipitation : par exemple, le polynôme $X^2Y + Y^2Z + Z^2X \in \mathbb{Z}[X, Y, Z]$ *n'est pas* symétrique.

Théorème 12.11 *Soient A un anneau, et n un entier naturel. L'application*

$$\begin{array}{rcl} \Phi_n : A[S_1, \ldots, S_n] & \longrightarrow & A[X_1, \ldots, X_n] \\ F & \longmapsto & F({}^n\Sigma_1, \ldots, {}^n\Sigma_n) \end{array}$$

induit un isomorphisme de $A[S_1, \ldots, S_n]$ sur le sous-anneau de $A[X_1, \ldots, X_n]$ formé des polynômes symétriques.

Démonstration.

12.11.1. Il est clair que Φ_n est un morphisme d'anneaux : par exemple on peut le voir comme le composé des deux morphismes suivants :
- l'inclusion de $A[S_1, \ldots, S_n]$ dans $A_n[S_1, \ldots, S_n]$ avec $A_n = A[X_1, \ldots, X_n]$;
- le morphisme d'évaluation de $A_n[S_1, \ldots, S_n]$ dans A_n envoyant S_i sur $\Sigma_i \in A_n$.

12.11.2. Montrons que Φ_n est injectif, par récurrence sur n. On a $\Phi_0 = \mathrm{Id}_A$. Supposons $n > 0$ et Φ_{n-1} injectif. Si Φ_n ne l'est pas, il existe un polynôme non nul $F \in \operatorname{Ker} \Phi_n$ dont le degré en l'indéterminée S_n est minimal. Ainsi on a dans $A[X_1, \ldots, X_n]$ la relation

$$F({}^n\Sigma_1, \ldots, {}^n\Sigma_n) = 0$$

dans laquelle on peut "faire $X_n = 0$" ce qui donne

$$F({}^n\Sigma_1(X_1, \ldots, X_{n-1}, 0), \ldots, {}^n\Sigma_n(X_1, \ldots, X_{n-1}, 0)) = 0.$$

Appliquant 11.2.3 on en tire dans $A[X_1, \ldots, X_{n-1}]$ la relation

$$F({}^{n-1}\Sigma_1, \ldots, {}^{n-1}\Sigma_{n-1}, 0) = 0$$

ce qui signifie que le polynôme (à $n-1$ indéterminées) $F(S_1, \ldots, S_{n-1}, 0)$ appartient au noyau de Φ_{n-1}, et est donc nul par hypothèse de récurrence. Or ceci veut dire que F est divisible par S_n : il existe $G \in A[S_1, \ldots, S_n]$ tel que $F = S_n G$, d'où $0 = \Phi_n(F) = \Phi_n(S_n)\Phi_n(G) = {}^n\Sigma_n \Phi_n(G)$. Mais il est immédiat que $\Sigma_n = \prod_{j=1}^n X_j$ est *non diviseur de zéro* dans $A[X_1, \ldots, X_n]$ (multiplier un polynôme par Σ_n revient simplement à "décaler ses coefficients"). Donc $\Phi_n(G) = 0$ d'où $G \in \operatorname{Ker} \Phi_n$. Mais ceci contredit le choix de F puisque $\deg_{S_n}(G) = \deg_{S_n}(F) - 1$.

12.11.3. Pour montrer que Φ_n est surjectif, on munit d'abord l'ensemble $\mathbb{N}^n$ de la relation d'ordre suivante (dite "ordre lexicograhique") :

$a = (a_1, \ldots, a_n) \leq b = (b_1, \ldots, b_n) \overset{\text{def}}{\Longleftrightarrow}$

pour tout $j \in \{1, \ldots, n\}$ tel que $(a_1, \ldots, a_{j-1}) = (b_1, \ldots, b_{j-1})$, on a $a_j \leq b_j$.

Ce n'est donc rien d'autre que l'ordre alphabétique, où l'alphabet $(\mathrm{a}, \mathrm{b}, \ldots, \mathrm{z})$ est remplacé par la suite des entiers naturels.

On vérifie alors les propriétés suivantes :

(i) la relation $\leq$ est un *bon ordre* sur $\mathbb{N}^n$, c'est-à-dire une relation d'ordre (vous connaissez la définition, bien sûr) pour laquelle toute partie non vide admet un plus petit élément. (En particulier c'est un ordre total, comme le sait bien quiconque a un jour cherché un mot dans un dictionnaire) ;

(ii) la relation $\leq$ est compatible avec l'addition des multi-indices : pour I, J, K et $L \in \mathbb{N}^n$, si $I \leq J$ et $K \leq L$ alors $I + K \leq J + L$.

Pour un polynôme non nul $P = \sum_{I \in \mathbb{N}^n} \lambda_I X^I \in A[X_1, \ldots, X_n]$ on définit le degré lexicograhique de P, noté $\operatorname{deglex}(P)$, comme le plus grand $I \in \mathbb{N}^n$ tel que $\lambda_I \neq 0$; le terme $\lambda_I X^I$ correspondant est noté $\operatorname{tdom}(P)$ (terme dominant lexicographique), et λ_I est noté $\operatorname{cdom}(P)$. On a alors :

(iii) si P est symétrique non nul, avec $\operatorname{deglex}(P) = (i_1, \ldots, i_n)$ alors la suite d'entiers $(i_1, \ldots, i_n)$ est *décroissante* ;

(iv) soient P, $Q \in A[X_1, \ldots, X_n]$ non nuls ; on suppose que $\operatorname{cdom}(P)$ n'est pas diviseur de zéro dans A. Alors $\operatorname{tdom}(PQ) = \operatorname{tdom}(P)\operatorname{tdom}(Q)$;

(v) pour tout $i \in \{1, \ldots, n\}$ on a $\operatorname{tdom}(\Sigma_i) = \prod_{j=1}^i X_j$;

(vi) pour tout $\lambda \in A$ non nul et tout $(l_1, \ldots, l_n) \in \mathbb{N}^n$ on a

$$\operatorname{tdom}(\lambda\, {\Sigma_1}^{l_1}\, {\Sigma_2}^{l_2} \cdots {\Sigma_n}^{l_n}) = \lambda\, X_1^{l_1+l_2+\cdots+l_n}\, X_2^{l_2+\cdots+l_n} \cdots X_n^{l_n}.$$

12.11.4. Montrons maintenant que l'image de Φ_n est l'ensemble des polynômes symétriques. Nous allons procéder par "récurrence" sur le degré lexicographique, au sens suivant : s'il existe dans $A[X_1, \ldots, X_n]$ des polynômes symétriques qui ne soient pas dans l'image de Φ_n, il en existe un, disons P, de degré minimum, ceci d'après la propriété (i) ci-dessus (noter qu'un tel polynôme n'est pas nul puisque 0 est dans l'image de Φ_n).

Or d'après (iii), le terme dominant de P est de la forme $\lambda X_1^{i_1} \ldots X_n^{i_n}$ avec $\lambda \in A$ et $i_1 \leq i_2 \leq \ldots \leq i_n$). On peut par suite trouver une (unique) suite d'entiers naturels $(l_1, \ldots, l_n)$ telle que $i_j = \sum_{\nu=j}^{n} l_\nu$ pour tout j (à savoir $l_j = i_j - i_{j+1}$ si $j < n$ et $l_n = i_n$). Il résulte alors de (vi) que le polynôme $Q = \lambda\, {\Sigma_1}^{l_1}\, {\Sigma_2}^{l_2} \cdots {\Sigma_n}^{l_n}$ a même terme dominant que P, de sorte que $\mathrm{deglex}\,(P-Q) < \mathrm{deglex}\,(P)$ ce qui, par le choix de P, entraîne que $P - Q \in \mathrm{Im}(\Phi_n)$ puisque $P - Q$ est évidemment symétrique. Mais Q est évidemment dans l'image de Φ_n (en fait $Q = \Phi_n(\lambda \prod_{j=1}^{n} S_j^{l_j})$ et il en est donc de même de P, ce qui est contraire à l'hypothèse. ∎

12.11.5. *Remarque.* La preuve ci-dessus fournit un algorithme effectif pour calculer, étant donné $P \in A[X_1, \ldots, X_n]$ symétrique, l'unique $F \in A[S_1, \ldots, S_n]$ tel que $P = \Phi_n(F)$: si $\mathrm{tdom}\,(P) = \lambda X_1^{i_1} \ldots X_n^{i_n}$, on pose $F_1 = \lambda S_1^{i_1 - i_2} S_2^{i_2 - i_3} \cdots S_n^{i_n}$ et l'on a alors $P = \Phi_n(F_1) + P_1$ où $\mathrm{deglex}\,(P_1) < \mathrm{deglex}\,(P)$. Il suffit de recommencer l'opération avec P_1.

12.11.6. *Remarque.* Comme toutes les méthodes générales, l'algorithme ci-dessus n'est à employer — du moins pour l'utilisateur humain — qu'en dernier recours. Les exemples suffisamment simples pour être traités à la main, comme ceux qui suivent, se résolvent généralement par des calculs "ad hoc".

12.11.7. *Exercice.* Vérifier que $\sum_{j=1}^{n} X_j^2 = \Sigma_1^2 - 2\Sigma_2$.

12.11.8. *Exercice.* Calculer $X^2Y^2 + Y^2Z^2 + Z^2X^2$ en fonction de $X + Y + Z$, $XY + YZ + ZX$, XYZ.

12.11.9. *Exercice.* Soit A un anneau intègre, K son corps des fractions, et soit $F \in A[X]$ non nul de degré n. Soient $\alpha_1, \ldots, \alpha_n$ les racines de F dans une extension convenable de K. Si $P \in A[X_1, \ldots, X_n$ est un polynôme symétrique, montrer que $P(\alpha_1, \ldots, \alpha_n)$ appartient à K, et même à A si F est unitaire.

12.12. *Exemple : le discriminant.* Considérons le polynôme suivant, en n indéterminées $X_1, \ldots, X_n$:

$$^n\delta = \prod_{1 \leq i < j \leq n} (X_i - X_j) \quad \in \mathbb{Z}[X_1, \ldots, X_n].$$

noté simplement δ s'il n'y a pas de confusion sur n. Il n'est pas symétrique mais il résulte de I.11.9(i) — ou plus exactement de sa généralisation I.11.10.1 — que pour

tout $\sigma \in \mathfrak{S}_n$ on a

$$\delta(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \varepsilon(\sigma)\, \delta(X_1, \ldots, X_n)$$

où $\varepsilon(\sigma)$ désigne, rappelons-le, la signature de σ. En particulier δ^2 est symétrique, et il existe donc un unique polynôme $D = {}^nD \in \mathbb{Z}[S_1, \ldots, S_n]$ tel que

$$\delta^2 = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2 = {}^nD(-\Sigma_1, \Sigma_2, \ldots, (-1)^n\, \Sigma_n).$$

Définition 12.12.1 *Soient A un anneau, n un entier naturel, et*

$$F = X^n + \sum_{i=1}^{n} a_i X^{n-i}$$

un polynôme unitaire *à coefficients $a_i \in A$. On appelle* discriminant *de F l'élément de A défini par*

$$\operatorname{disc}(F) = {}^nD(a_1, \ldots, a_n).$$

où ${}^nD$ est le polynôme défini ci-dessus.

12.12.2. *Remarque.* L'entier n n'a pas à être précisé dans la notation $\operatorname{disc}(F)$: c'est nécessairement le degré de F (sauf si A est l'anneau nul, où le problème ne se pose pas puisque tout, y compris le discriminant, est nul).

Proposition 12.12.3 *Soient A un anneau, n un entier naturel, et $\alpha_1, \ldots, \alpha_n$ des éléments de A. Alors :*

$$\operatorname{disc}\left(\prod_{i=1}^{n}(X - \alpha_i)\right) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Démonstration. Cela résulte des définitions et des relations 11.3 entre les α_i et les coefficients du polynôme $\prod_{i=1}^{n}(X - \alpha_i)$. ∎

12.12.4. *Remarque.* Cet énoncé explique le choix des signes dans la définition de D.

Proposition 12.12.5 *Soit k un corps, et soit F un polynôme unitaire à coefficients dans k, n son degré.*

(i) *Notons $\alpha_1, \ldots, \alpha_n$ les racines de F, comptées avec multiplicités, dans une extension L convenable de k. Alors*

$$\begin{aligned} \operatorname{disc}(F) &= \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} F'(\alpha_i). \end{aligned}$$

(ii) *Pour que F ait une racine multiple dans une extension de k il faut et il suffit que* $\operatorname{disc}(F)$ *soit nul.*

(iii) *Si F est décomposé dans $k[X]$, alors* $\operatorname{disc}(F)$ *est un carré dans k.*

Démonstration. La première égalité de (i) résulte de 12.12.3 (avec $A = L$) puisque $F = \prod_{i=1}^{n}(X - \alpha_i)$ dans $L[X]$. De plus cette égalité implique immédiatement (ii) et (iii).

Il reste à montrer la seconde égalité de (i). Dérivant l'identité $F = \prod_{i=1}^{n}(X-\alpha_i)$, on obtient

$$F' = \sum_{i=1}^{n} \prod_{\substack{1\le j\le n\\ j\neq i}} (X - \alpha_j)$$

d'où, pour chaque $i \in \{1, \dots, n\}$,

$$F'(\alpha_i) = \prod_{\substack{1\le j\le n\\ j\neq i}} (\alpha_i - \alpha_j)$$

et en faisant le produit

$$\prod_{i=1}^{n} F'(\alpha_i) = \prod_{\substack{1\le i\le n\\ 1\le j\le n\\ j\neq i}} (\alpha_i - \alpha_j).$$

Pour chacun des $n(n-1)/2$ couples (i, j) avec $1 \le i < j \le n$, le produit ci-dessus contient les facteurs $\alpha_i - \alpha_j$ et $\alpha_j - \alpha_i$, dont le produit est $-(\alpha_i - \alpha_j)^2$. On en tire la seconde égalité. ∎

12.12.6. *Exemple : $n = 2$.* Pour $F = X^2 + bX + c$, notons α et β les racines de F (dans une extension convenable, comme toujours). Alors $\operatorname{disc}(F) = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c$, comme prévu.

12.12.7. *Exemple : $n = 3$.* Contentons-nous d'un polynôme F sans terme en X^2, i.e. de la forme $X^3 + pX + q$. On a $F' = 3X^2 + p$. Si α, β, γ sont les racines de F, on a donc (en tenant compte des égalités $\alpha + \beta + \gamma = 0$, $\alpha\beta + \beta\gamma + \gamma\alpha = p$, $\alpha\beta\gamma = -q$ et des exercices 12.11.7 et 12.11.8) :

$$\begin{aligned}\operatorname{disc}(F) &= -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p)\\ &= -[27(\alpha\beta\gamma)^2 + 9p(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3]\\ &= -4p^3 - 27q^2.\end{aligned}$$

Le signe $-$ provient du $(-1)^{n(n-1)/2}$ de 12.12.5(i). Il est évidemment essentiel si l'on veut appliquer 12.12.5(iii), par exemple.

12.12.8. *Remarque.* Le cas traité ci-dessus d'un polynôme sans terme en X^2 n'est pas aussi restrictif qu'il peut le sembler. Plus généralement, pour un polynôme $F = X^n + \sum_{i=1}^{n} a_i X^{n-i} \in k[X]$, le "changement de variable $X = Y - (a_1/n)$" donne un polynôme unitaire en Y dont le terme de degré $n-1$ est nul. La seule restriction à cette opération (normalement, vous avez dû hurler en lisant la formule) est que l'on doit pouvoir diviser par n dans k ; autrement dit, elle n'est possible que si *la caractéristique de k ne divise pas n.*

Noter que le polynôme en Y obtenu a pour racines celles de P augmentées de a_1/n, et que 12.12.5(i) montre donc qu'il a même discriminant que F.

12.12.9. *Exercice.* Soit $F \in \mathbb{R}[X]$ de degré 3. Peut-on déduire du discriminant de F le nombre de racines réelles de F (comptées avec multiplicités) ? le nombre de racines réelles distinctes de F ?

12.12.10. *Remarque.* Il est possible de définir le discriminant d'un polynôme *non nécessairement unitaire* $F = \sum_{i=0}^{n} a_i X^{n-i}$, à coefficients dans un anneau A ; c'est un élément de A, qui s'exprime comme un polynôme en les a_i à coefficients entiers (ne dépendant que de n) ; il coïncide avec le discriminant défini plus haut si $a_0 = 1$, et si a_0 est inversible dans A il est égal à $a_0^{n-1}\mathrm{disc}\,(a_0^{-1}F)$.

Table des matières