Cours d'algèbre, compléments

Michel Demazure

23 mars 2009

Introduction

Comme je l'explique dans l'introduction à la nouvelle édition de mon *Cours d'Algèbre*, j'ai été amené à en supprimer « l'ancien chapitre 7 (Divisibilité) qui, à vrai dire, détonnait un peu dans l'ensemble par son caractère plus abstrait » et à ne conserver « de l'ancien chapitre 6 (Anneaux) [...] que les résultats utiles au reste du livre, qui ont été répartis dans le texte aux endroits convenables ».

Certains lecteurs m'ont fait remarquer que ces parties supprimées, et notamment le chapitre 7, prises isolément, fournissaient des références commodes et qu'il était dommage qu'elles disparaissent totalement. Aussi, avec l'accord de mon éditeur Cassini, j'ai décidé d'en faire un texte autonome disponible au téléchargement.

L'ancien chapitre 6 (Anneaux) est devenu le chapitre 1. Il a été complété des sections 1.3.5 à 1.4.2. L'ancien chapitre 7 est devenu le chapitre 2. La partie finale (2.4) a été notablement réécrite.

J'ai maintenu les quelques fragments incorporés à la nouvelle édition pour ne pas modifier les références : les références *x.y* ou *x.y.z* de l'ancienne édition se retrouvent ainsi en *(x-6).y* ou *(x-6).y.z* dans ces notes.

Chapitre 1
Anneaux

§ 1.1. Anneaux et idéaux

1.1.1. Congruences dans Z

La notion de congruence est ancienne. Les congruences modulo 2 ou 4 ont été utilisées par les Grecs (raisonnement par parité). La mise en forme de cette notion est due à Legendre et Gauss.

Notons $a \mid b$ (lire « a divise b ») la relation de divisibilité entre entiers. Précisons qu'ici comme ailleurs, le mot « entier » signifie « entier de signe quelconque » et que les entiers 0, 1, 2, ... sont dits « naturels » ou « positifs ». On note **Z** l'ensemble des entiers et **N** celui des entiers naturels.[1]

Si a, b et m sont trois entiers, on dit que a et b sont *congrus* modulo m, et on écrit $a \equiv b \ [\mathtt{mod}\ m]$ si m divise $a - b$. On peut additionner, soustraire, multiplier les congruences relatives au même module :

- ▷ $(x \equiv y \ [\mathtt{mod}\, m]$ et $x' \equiv y' \ [\mathtt{mod}\, m])$ implique $(x + x' \equiv y + y' \ [\mathtt{mod}\, m])$,
- ▷ $(x \equiv y \ [\mathtt{mod}\, m]$ et $x' \equiv y' \ [\mathtt{mod}\, m])$ implique $(x - x' \equiv y - y' \ [\mathtt{mod}\, m])$,
- ▷ $(x \equiv y \ [\mathtt{mod}\, m]$ et $x' \equiv y' \ [\mathtt{mod}\, m])$ implique $(xx' \equiv yy' \ [\mathtt{mod}\, m])$.

Notons aussi les propriétés suivantes :

- ▷ $(x \equiv y \ [\mathtt{mod}\, m])$ implique $(ax \equiv ay \ [\mathtt{mod}\, am])$,
- ▷ $(x \equiv y \ [\mathtt{mod}\, m]$ et $m' \mid m)$ implique $(x \equiv y \ [\mathtt{mod}\, m'])$,
- ▷ $(x \equiv y \ [\mathtt{mod}\, 0])$ équivaut à $(x = y)$.

En revanche, on ne peut pas toujours simplifier des congruences. De $ax \equiv ay \ [\mathtt{mod}\, m]$, on ne peut déduire $x \equiv y \ [\mathtt{mod}\, m]$ que si a est premier à m. Cela montre que la situation est meilleure lorsque le module est *premier* :

- ▷ Si p est premier, et si $a \not\equiv 0 \ [\mathtt{mod}\, p]$, alors $(ax \equiv ay \ [\mathtt{mod}\, p])$ implique $(x \equiv y \ [\mathtt{mod}\, p])$.

Exercice 1.1. [B] — Vérifier les assertions précédentes. [*hint*]

Critères de divisibilité

Une application simple des congruences est bien connue : les critères élémentaires de divisibilité. Choisissons une base b (par exemple $b = 10$) et écrivons un entier n dans le système de numération de base b :

1. La notation **Z** provient de l'allemand « Zahl » (nombre) ; quand à **N**, c'est sans doute l'initiale de « nombre » ou « naturel ».

$$n = \sum_{i=0}^{m} a_i b^i = a_m b^m + \cdots + a_0.$$

On a alors $n \equiv a_0 \ [\mathtt{mod}\ b]$, ce qui donne les critères de divisibilité par les diviseurs d de b (donc 2 et 5 lorsque $b = 10$) : n est divisible par d lorsque son dernier chiffre a_0 est divisible par d, et seulement en ce cas. De même, pour tout diviseur d de $b-1$ (donc 3 et 9 lorsque $b = 10$), on a $b \equiv 1 \ [\mathtt{mod}\ d]$, donc $n \equiv a_m + \cdots + a_0 \ [\mathtt{mod}\ d]$ et on trouve le critère usuel : n est divisible par d lorsque la somme de ses chiffres est divisible par d, et seulement en ce cas.

EXERCICE I.2. [A] — On considère maintenant les diviseurs de $b + 1$. Quel est le critère correspondant ? [*hint*]

I.1.2. Anneaux

La structure algébrique sans doute la plus importante est celle d'*anneau commutatif*, dont l'archétype est l'anneau $\mathbf{Z}$ des entiers. Pour bien fixer nos conventions, rappelons rapidement les définitions essentielles.

Un anneau est muni de deux lois de composition : une loi de groupe commutatif, notée additivement et une loi associative, notée multiplicativement, distributive par rapport à l'addition. Lorsque cette loi multiplicative ne possède pas d'élément unité, les propriétés d'une telle structure peuvent être assez inattendues. L'usage s'est ainsi généralisé de réserver le nom d'anneau au cas où la multiplication possède un élément unité.

Par ailleurs, la théorie des anneaux se sépare très rapidement en deux, selon que l'on suppose, ou non, que la multiplication est commutative.[2]

Comme nous n'aurons pas besoin dans la suite d'anneaux non commutatifs, *nous réservons désormais le nom d'anneau aux anneaux commutatifs*.

Formellement, la structure d'anneau est donc définie par la donnée de deux éléments privilégiés 0 (*élément nul*) et 1 (*élément unité*), d'une application $x \mapsto -x$ et de deux lois de composition binaires $(x, y) \mapsto x + y$ et $(x, y) \mapsto xy$, ces données étant liées par les axiomes suivants :

- $(x + y) + z = x + (y + z)$
- $x + y = y + x$
- $x + 0 = x$
- $x + (-x) = 0$
- $(xy)z = x(yz)$
- $xy = yx$

2. Bien évidemment, les énoncés généraux valables sans hypothèses de commutativité s'appliquent aux anneaux commutatifs, mais, dans la théorie générale des anneaux, on s'intéresse de façon approfondie à des questions qui perdent tout intérêt dans le cas commutatif.

▷ $1x = x$
▷ $x(y + z) = xy + xz$

On déduit de là toutes les règles de calcul habituelles. On a par exemple $0x = 0$, car $x = 1x = (0 + 1)x = 0x + 1x = 0x + x$, et par conséquent $0x = x + (-x) = 0$. On a de même $(-1)x = -x$.

Si $1 = 0$, alors l'anneau n'a qu'un élément car $x = 1x = 0x = 0$, et on dit que l'anneau est *nul*.

> EXERCICE I.3. [B] — Soit A un anneau à deux éléments. Prouver qu'on a $1 + 1 = 0$ et en déduire que les tables d'addition et de multiplication de A sont uniquement déterminées. [*hint*]

Comme pour toutes les lois de composition commutatives, on utilise les notations habituelles telles que $x - y$ pour $x + (-y)$, $2x$ pour $x + x$, $3x$ pour $x + x + x$, $-2x$ pour $(-x) + (-x)$, x^2 pour xx, ...Dans un anneau A, on utilisera donc librement des expressions du type nx pour $n \in \mathbf{Z}$ et $x \in \mathrm{A}$, x^n pour $n \in \mathbf{N}$ et $x \in \mathrm{A}$ (on a $x^0 = 1$). Un élément $x \in \mathrm{A}$ est dit *inversible* s'il existe y avec $xy = 1$; l'élément y, uniquement déterminé[3] se note x^{-1}. On étend la notation x^n au cas où x est inversible et $n \in \mathbf{Z}$. Il n'y a guère de danger à désigner par le même symbole 0 l'élément nul de tout anneau. En ce qui concerne l'élément unité, on écrira 1_{A} lorsqu'un risque de confusion apparaîtra.

C'est ainsi qu'on prendra garde à la chose suivante : pour $n \in \mathbf{Z}$ et $x \in \mathrm{A}$, on a $nx = n1_{\mathrm{A}}.x$, ce qui amène à confondre l'entier $n \in \mathbf{Z}$ et l'élément $n1_{\mathrm{A}}$ de A. Mais on peut avoir dans A l'égalité $n1_{\mathrm{A}} = 0$ sans que l'entier n soit nul ! On dit souvent que l'entier n est *nul dans* A si $n1_{\mathrm{A}} = 0$.

L'une des conséquences de la commutativité est la validité de la *formule du binôme*. Si n est un entier positif, les *coefficients du binôme* sont les entiers $\binom{n}{i}$ donnés par

$$\binom{n}{i} = \begin{cases} 0 & \text{pour } i < 0 \text{ et } i > n \\ \frac{n(n-1)\ldots(n-i+1)}{i!} & \text{pour } 0 \leqslant i \leqslant n. \end{cases}$$

Ils satisfont à la relation de récurrence

$$\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}, \qquad i \in \mathbf{Z}.$$

Si x et y sont deux éléments de A, on a

$$(x + y)^n = \sum_{i \in \mathbf{Z}} \binom{n}{i} x^i y^{n-i} = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

> EXERCICE I.4. [A] — Vérifier ce point. [*hint*]

3. Si $xy = xy' = 1$, alors $y = (xy')y = (xy)y' = y'$.

I.1.3. Sous-anneaux, homomorphismes, produits

Précisons maintenant le sens du mot « sous-anneau ». Si A est un anneau et B une partie de A, nous dirons que B est un sous-anneau de A si B est stable par les opérations de A, *et s'il contient l'élément unité de* A.

EXERCICE I.5. [A] — Chaque anneau possède un plus petit sous-anneau. Quels en sont les éléments ? [*hint*]

EXERCICE I.6. [A] — L'anneau $\mathbf{Z}$ ne contient pas de sous-anneau distinct de lui-même. [*hint*]

REMARQUE I.1. — Il peut arriver en effet qu'une partie B soit stable pour les deux lois et possède un élément unité (donc soit un anneau pour les lois induites) sans être un sous-anneau : les éléments unités de A et B différent. L'élément unité e_B de B est alors un « idempotent » de A : on a $e_B^2 = e_B$.

Donnons un exemple non commutatif bien connu : A est formé des matrices $n \times n$ et B est formé de celles de ces matrices dont la dernière ligne et la dernière colonne sont nulles.

De la même manière, si A et B sont deux anneaux et $f : A \to B$ une application, on dit que f est un *homomorphisme d'anneaux* si f commute aux opérations d'addition et de multiplication, *et applique élément unité sur élément unité*. L'image $f(A)$ de f est alors un sous-anneau de B. Si f est un homomorphisme bijectif, alors l'application réciproque f^{-1} est également un homomorphisme d'anneaux ; on dit que f est un *isomorphisme* d'anneaux.

A chaque anneau A sont associés deux groupes : le groupe additif de A, encore noté A, et le groupe multiplicatif A^* des éléments inversibles de A.

Bien évidemment, l'élément 0 de A n'est pas inversible, à moins que $A = \{0\}$ (anneau nul). On dit que A est un *corps* si A n'est pas nul et si tout élément non nul de A est inversible. Cela signifie aussi que A^* est le complémentaire de 0 dans A. Le corps le plus simple est le corps $\mathbf{F}_2$ à deux éléments ; les opérations de $\mathbf{F}_2$ sont données par les relations $-0 = 0$, $-1 = 1, 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0, 0.0 = 0, 0.1 = 1$ et $1.1 = 1$.

REMARQUE I.2. — Si on note les éléments de $\mathbf{F}_2$ plutôt `faux` $= 0$ et `vrai` $= 1$, la multiplication et l'addition coïncident respectivement avec la conjonction (`and`) et la disjonction exclusive (`xor`). La disjonction (`or`) se calcule par la formule x `or` $y = x + y + xy$.

On dit qu'un élément x de A est un *diviseur de zéro* s'il existe $y \neq 0$ avec $xy = 0$. Si A n'est pas nul et si le seul diviseur de zéro est 0 (autrement dit

si le produit de deux éléments non nuls n'est jamais nul), on dit que A est *intègre*[4] ; c'est le cas notamment si A est un corps.

> EXERCICE 1.7. [B] — Soit A un anneau. Pour tout $a \in A$, notons $h_a : x \mapsto ax$ l'homothétie de rapport a ; c'est un endomorphisme du groupe additif A (ce qui implique d'ailleurs $a0 = 0$). A quelle condition h_a est-elle injective (surjective, bijective) ? [*hint*]

Tout sous-anneau d'un anneau intègre est intègre. En particulier, tout sous-anneau d'un corps est intègre. Inversement, tout anneau intègre est un sous-anneau de son *corps des fractions* ; par exemple, l'anneau $\mathbf{Z}$ des entiers est un sous-anneau du corps $\mathbf{Q}$ des nombres rationnels.

> EXERCICE 1.8. [C] — Soit A un anneau. Notons S l'ensemble des éléments de A qui ne sont pas diviseurs de zéro. On a $1 \in S$ et $SS \subset S$. On définit un anneau K en considérant l'ensemble des fractions a/s avec $a \in A$ et $s \in S$ et en identifiant a/s et a'/s' lorsque $as' = a's$. Vérifier les détails de cette construction. L'application qui à $a \in A$ associe (la classe de) $a/1$ est un homomorphisme injectif d'anneaux. On a ainsi plongé A dans l'anneau K dans lequel les éléments de S sont inversibles. C'est *l'anneau total des fractions de* A. Pourquoi est-on obligé de se limiter à inverser les éléments de S ? Lorsque A est intègre, S est le complémentaire de $\{0\}$ et l'anneau K est un corps, appelé le *corps des fractions* de A. [*hint*]

Enfin, pour terminer ces généralités, notons que le *produit* $\prod_{i=1}^{n} A_i$ des anneaux $A_1, \ldots, A_n$, formé des suites $(a_1, \ldots, a_n)$ avec $a_i \in A_i$, est un anneau pour les lois évidentes (addition et multiplication composante par composante). Par exemple $\mathbf{F}_2^n$ est l'anneau des suites de n bits, les opérations se faisant composante par composante.

> EXERCICE 1.9. [B] — (suite du précédent) On prend $A = \mathbf{Z} \times \mathbf{Z}$. Identifier S et K. Généraliser au cas des produits d'anneaux. [*hint*]

1.1.4. Congruences et idéaux

La notion de divisibilité et le *calcul des congruences* s'étendent à tous les anneaux.

4. Dans presque tous les cas, la terminologie anglo-saxonne est parallèle à la terminologie française : « ring » pour « anneau » par exemple. Nous signalerons les variations imprévisibles. Ainsi « corps » (qui provient de l'usage du mot « Körper » dans les premiers articles allemands introduisant la théorie générale des corps) devient « field » ; on trouve d'ailleurs dans certains textes français « champ » au lieu de corps, surtout dans l'expression « champ de Galois », pour désigner les corps finis. Quant à l'adjectif « intègre », c'est plus compliqué. L'adjectif anglais « integral » signifie déjà « entier » et aussi « intégral ». Pour « anneau intègre », on ne dit pas « integral ring », mais « integral domain » ou simplement « domain ». Certains auteurs disent d'ailleurs en français « anneau d'intégrité » ou « domaine d'intégrité ».

Si a et b sont deux éléments d'un anneau A, on dit que a divise b ou que b est multiple de a (sous-entendu dans A) et on écrit souvent $a \mid b$, s'il existe $d \in \mathrm{A}$ avec $b = ad$. Si a n'est pas diviseur de zéro, un tel d est uniquement déterminé, on le note b/a.

> EXERCICE I.10. [A] — (suite de l'exercice I.8) Supposons que a ne soit pas diviseur de zéro. Dire que a divise b signifie que l'élément b/a de l'anneau total des fractions de A appartient à A lui-même. [*hint*]

REMARQUE I.3. — Avec les définitions précédentes, on a toujours $a \mid 0$. C'est pourquoi nous disons « diviseur de zéro » plutôt que « diviseur de 0 » !

Si a, b et m sont trois éléments d'un anneau A, on dit que a est congru à b modulo m, et on écrit $a \equiv b \ [\mathtt{mod}\ m]$ si m divise $a - b$. Les propriétés énoncées en I.1.1 restent valables (pour la dernière, voir la définition 2.2).

La remarque essentielle à ce point est que, par construction, la notion de congruence modulo m ne dépend de m que par l'intermédiaire de l'ensemble (m) des multiples de m, puisqu'elle s'écrit aussi $a - b \in (m)$. D'ailleurs, (m) est l'ensemble des éléments congrus à 0. On a plus généralement le lemme suivant :

PROPOSITION I.4. — *Soit* A *un anneau et soit* $a \equiv b$ *une relation d'équivalence dans l'ensemble* A. *Les conditions suivantes sont équivalentes :*

(i) la relation $x \equiv y$ *est compatible avec l'addition et la multiplication : de* $(x \equiv x'$ *et* $y \equiv y')$ *on déduit* $(x + y \equiv x' + y'$ *et* $xy \equiv x'y')$ *;*

(ii) la relation $x \equiv y$ *s'écrit* $x - y \in \mathfrak{a}$, *où* $\mathfrak{a}$ *est une partie de* A *possédant les trois propriétés suivantes :*

- ▷ *on a* $0 \in \mathfrak{a}$,
- ▷ $(x \in \mathfrak{a}$ *et* $y \in \mathfrak{a})$ *implique* $(x + y \in \mathfrak{a})$,
- ▷ $(a \in \mathrm{A}$ *et* $x \in \mathfrak{a})$ *implique* $(ax \in \mathfrak{a})$.

> EXERCICE I.11. [B] — Démonstration de la proposition. [*hint*]

DÉFINITION I.5. *On appelle* idéal *de l'anneau* A *une partie de* A *satisfaisant aux trois propriétés du lemme précédent.*

Paraphrasons : un idéal de A est un sous-groupe additif qui est en outre stable par toutes les « homothéties » $x \mapsto ax$, pour a parcourant A. Un idéal est donc stable par addition et multiplication (mais, à moins d'être égal à l'anneau tout entier, ce n'est pas un sous-anneau, voir l'exercice suivant).

> EXERCICE I.12. [A] — Quel est le plus petit idéal de A ? Quel est le plus grand ? Montrer que, pour qu'un idéal soit égal à A, il faut et il suffit qu'il contienne 1. [*hint*]

Ainsi, pour qu'une relation d'équivalence sur un anneau A soit compatible avec l'addition et la multiplication, il faut et il suffit qu'elle s'écrive

$x - y \in \mathfrak{a}$ où $\mathfrak{a}$ est un idéal de A. Si $\mathfrak{a}$ est un idéal de l'anneau A, la relation $x - y \in \mathfrak{a}$ se note aussi $x \equiv y \ [\mathfrak{a}]$.

L'exemple le plus simple d'idéal, qui correspond à la congruence modulo un élément, est l'ensemble $Am = mA$, noté aussi (m), des multiples d'un élément fixé m de A. On a par exemple $(0) = \{0\}$ et $(1) = A$. Les relations $m' \mid m$, $m \in (m')$ et $(m) \subset (m')$ sont équivalentes. Passer des éléments aux idéaux correspondants transforme donc la relation de divisibilité en la relation d'inclusion.

EXERCICE I.13. [B] — Supposons m non diviseur de zéro. A quelle condition a-t-on $(m) = (m')$? [*hint*]

EXERCICE I.14. [B-C] — Soit $\mathfrak{a}$ un idéal de A. On appelle *racine* de $\mathfrak{a}$ l'ensemble des $x \in A$ tels qu'il existe un entier $n \in \mathbf{N}$ avec $x^n \in \mathfrak{a}$. Prouver que c'est un idéal de A. [*hint*]

EXERCICE I.15. [B] — (variante du précédent). Les éléments nilpotents de A, c'est-à-dire les $x \in A$ tels qu'il existe $n \in \mathbf{N}$ avec $x^n = 0$, forment un idéal. Dans l'anneau quotient de A par cet idéal, tout élément nilpotent est nul. [*hint*]

Idéaux de Z

Dans les anneaux les plus simples, les idéaux sont tous de la forme (m). C'est le cas notamment de l'anneau $\mathbf{Z}$:

PROPOSITION I.6. — *a*) *Les idéaux de* $\mathbf{Z}$ *sont exactement ses sous-groupes additifs.*

b) *Soit* $\mathfrak{a}$ *un idéal de* $\mathbf{Z}$. *Il existe un unique entier* $n \geqslant 0$ *tel que* $\mathfrak{a} = (n)$.

Démonstration. Un idéal est toujours un sous-groupe additif. Soit inversement $\mathfrak{a}$ un sous-groupe additif de $\mathbf{Z}$. Prouvons qu'il existe un entier $n \geqslant 0$ tel que $\mathfrak{a} = (n)$. C'est clair si $\mathfrak{a} = \{0\}$. Si $\mathfrak{a}$ n'est pas réduit à 0, il possède certainement des éléments > 0 (car il est stable par l'application $x \mapsto -x$). Soit n le plus petit élément > 0 de $\mathfrak{a}$. Alors tout multiple de n appartient à $\mathfrak{a}$, et il reste à prouver que tout élément x de $\mathfrak{a}$ est multiple de n. Or, on peut trouver un entier $i \in \mathbf{Z}$ avec $in \leqslant x < (i+1)n$. Alors $x - in$ appartient à $\mathfrak{a}$; mais on a $0 \leqslant x - in < n$, donc $x - in = 0$ par construction de n, et enfin $x = in \in (n)$. On a donc bien $\mathfrak{a} = (n)$. L'unicité de n est claire. □

Idempotents

Rappelons qu'un élément a de A est dit *idempotent* si $e^2 = e$.

Soient e un idempotent, et Ae l'idéal qu'il engendre. Pour tout $x \in Ae$, on a $x = ae = (ae)e = xe$; si inversement $x = xe$, alors $x \in Ae$. Par ailleurs e est uniquement déterminé par l'idéal Ae ; si en effet e' est un autre

idempotent tel que $Ae = Ae'$, on a $e' = ae = (ae)e = e'e$, et aussi $e = ee'$ pour la même raison, donc $e = e'$.

EXERCICE I.16. [A] — Pour les lois induites, l'idéal Ae est un anneau, d'élément unité e. [*hint*]

I.1.5. Produits d'idéaux

Dans le cas général, il y a d'autres idéaux que les (m). D'une certaine manière, il « manque » des nombres et c'est ce qui a conduit Kummer à introduire les idéaux (à l'origine « nombres idéaux » ou « diviseurs idéaux ») en théorie multiplicative des nombres algébriques. On définit en effet un *produit* pour les idéaux qui généralise le produit des nombres au sens suivant : le produit des idéaux (m) et (m') est (mm').

Par définition, le produit $\mathfrak{a}\mathfrak{b}$ de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ quelconques de A est formé des sommes finies $\sum x_i y_i$ avec $x_i \in \mathfrak{a}$ et $y_i \in \mathfrak{b}$. C'est bien un idéal (puisque $a \sum x_i y_i = \sum (a x_i) y_i$) ; c'est en fait le plus petit idéal contenant les produits xy avec $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$, car un tel idéal doit évidemment contenir les sommes finies de tels produits.

On a bien comme annoncé $(m)(m') = (mm')$. La multiplication des idéaux est une opération associative et commutative, d'élément neutre $A = (1)$: on a

$$(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}), \quad \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}, \quad (1)\mathfrak{a} = \mathfrak{a}, \quad (0)\mathfrak{a} = (0).$$

EXERCICE I.17. [B] — Vérifier les propriétés précédentes. [*hint*]

En termes savants, les idéaux de A forment un « monoïde » commutatif. On pose évidemment $\mathfrak{a}^2 = \mathfrak{a}\mathfrak{a}$, $\mathfrak{a}^3 = \mathfrak{a}\mathfrak{a}\mathfrak{a}$ et ainsi de suite. On notera que l'idéal $\mathfrak{a}^2$ est formé par définition des sommes finies de produits xy, avec x et y dans $\mathfrak{a}$. Il contient donc les carrés x^2 avec $x \in \mathfrak{a}$, donc aussi l'ensemble des sommes finies $\sum a_i x_i^2$ avec $a_i \in A$ et $x_i \in \mathfrak{a}$, mais en général ce dernier idéal est strictement inférieur à $\mathfrak{a}^2$.

EXERCICE I.18. [A] — Ces deux idéaux coïncident lorsque $2 \cdot 1_A$ est inversible. [*hint*]

EXERCICE I.19. [C] — Donner un cas où ces deux idéaux différent. [*hint*]

La multiplication des idéaux est compatible avec l'inclusion : de $\mathfrak{a} \subset \mathfrak{a}'$ et $\mathfrak{b} \subset \mathfrak{b}'$, on déduit $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}'\mathfrak{b}'$. On a toujours $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, avec en général inégalité, par exemple pour $\mathfrak{a} = \mathfrak{b}$.

On trouvera dans l'exercice qui suit un exemple montrant en quel sens il peut « manquer des nombres » et comment l'introduction des idéaux permet de mieux comprendre les propriétés multiplicatives des nombres.

EXERCICE I.20. [C] — On considère l'anneau $A = \mathbf{Z} + \mathbf{Z}\sqrt{-5} = \mathbf{Z} + \mathbf{Z}\alpha$ avec $\alpha^2 = -5$. On a dans cet anneau la relation $(1 + \alpha)(1 - \alpha) = 2.3$.

Montrer que les seuls éléments inversibles de A sont 1 et -1 et que les quatre éléments de la relation ci-dessus sont « premiers », au sens où $m \in \mathrm{A}$ est « premier »[5] s'il n'est divisible que par 1, -1, m et $-m$; on utilisera pour ce faire la *norme* : c'est l'application $\mathrm{N} : \mathrm{A} \to \mathbf{Z}$ définie par $\mathrm{N}(a+b\alpha) = (a+b\alpha)(a-b\alpha) = a^2+5b^2$; on a $\mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v)$. Ainsi, le nombre 6 se décompose en produit de facteurs « premiers » dans A de deux façons essentiellement distinctes ! Les quatre éléments précédents ne devraient pas être « premiers ». Et effectivement, ils ont des diviseurs, mais au sens des « diviseurs idéaux ».

Introduisons en effet les idéaux $\mathfrak{a}$, $\mathfrak{b}$ et $\mathfrak{b}'$ définis par

$$\mathfrak{a} = (1+\alpha)\mathrm{A} + (1-\alpha)\mathrm{A}, \quad \mathfrak{b} = 3\mathrm{A} + (2-\alpha)\mathrm{A}, \quad \mathfrak{b}' = 3\mathrm{A} + (2+\alpha)\mathrm{A}.$$

Prouver que

$$\mathfrak{a}\mathfrak{b} = (1+\alpha), \quad \mathfrak{a}\mathfrak{b}' = (1-\alpha), \quad \mathfrak{a}\mathfrak{a} = (2), \quad \mathfrak{b}\mathfrak{b}' = (3), \quad \mathfrak{a}\mathfrak{a}\mathfrak{b}\mathfrak{b}' = (6).$$

On retrouve ainsi des propriétés raisonnables, mais pour des décompositions en « facteurs premiers idéaux ». [*hint*]

I.1.6. Somme d'idéaux

On peut aussi additionner des idéaux : si U et V sont deux parties de l'anneau A, on note $\mathrm{U}+\mathrm{V}$ l'ensemble formé des éléments $u+v$ avec $u \in \mathrm{U}$ et $v \in \mathrm{V}$. Pour deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, la somme $\mathfrak{a}+\mathfrak{b}$ est un idéal ; c'est d'ailleurs le plus petit idéal contenant $\mathfrak{a}$ et $\mathfrak{b}$.

Exercice I.21. [B] — On a $\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b})+\mathfrak{c}$ et $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$. [*hint*]

L'addition des idéaux correspond à la notion de « plus grand commun diviseur ». Nous verrons cela en détail par la suite. Contentons-nous pour le moment de quelques brèves remarques. Soient a et b deux éléments d'un anneau A. Pour tout élément x de A, la condition « x est un diviseur commun de a et b », soit « $x \mid a$ et $x \mid b$ » s'écrit aussi « $(a) \subset (x)$ et $(b) \subset (x)$ », donc encore « $(a)+(b) \subset (x)$ ». Si on a la chance que l'idéal $(a)+(b)$ soit de la forme (d), alors cette condition est équivalente à « $x \mid d$ ». En ce cas, les diviseurs communs à a et b sont exactement les diviseurs de d, ce qu'on traduit en disant que d est un plus grand commun diviseur de a et b. Cela s'applique notamment à l'anneau $\mathbf{Z}$, vu I.6 :

Proposition I.7. — *Soient a et b deux entiers. L'idéal $(a)+(b)$, formé par définition des $ap+bq$ avec p et q dans $\mathbf{Z}$, est égal à (d), où d est le plus grand diviseur commun de a et b.*

5. Dans la terminologie que nous allons introduire ci-dessous (définition 2.1), il faudrait dire « extrémal » et non pas « premier ». Cet anneau est justement un exemple où ces deux notions diffèrent !

En particulier, le cas où $d = 1$ donne :

COROLLAIRE 1.8 (Bézout). — *Soient a et b deux entiers. Les conditions suivantes sont équivalentes :*

(i) a et b sont premiers entre eux (« étrangers ») : ils n'ont pas de diviseur commun autre que 1 et -1,

(ii) on a $(a) + (b) = \mathbf{Z}$,

(iii) il existe p et q dans $\mathbf{Z}$ avec $ap + bq = 1$.

REMARQUE 1.9. — Si l'on introduit l'anneau quotient $\mathbf{Z}/b\mathbf{Z}$ (voir plus loin), on peut aussi écrire la condition (iii) sous la forme :

(iv) l'élément a mod b de $\mathbf{Z}/b\mathbf{Z}$ est inversible.

Remarquons au passage que les seuls entiers premiers à 0 sont 1 et -1 : c'est ce qu'il résulte par exemple de la condition (iii), ou encore de la condition (iv) : pour que 0 soit inversible dans un anneau, il faut que l'anneau soit nul.

REMARQUE 1.10. — La démonstration précédente ne suggère pas comment calculer les entiers p et q. On utilise en général pour ce faire *l'algorithme d'Euclide étendu* (voir **??**).

> EXERCICE 1.22. [B] — On suppose donnés des entiers a, b, p et q avec $ap + bq = 1$. Alors a et b sont premiers entre eux, ainsi par conséquent que a et b^n. Trouver p' et q' avec $ap' + b^n q' = 1$. Application : a est impair et $b = 2$. [*hint*]

Il est évident que toute intersection d'idéaux est un idéal. En particulier, l'intersection de tous les idéaux de A contenant des éléments $x_1, \dots, x_n$ donnés est un idéal. Cet idéal, dit *engendré* par ces éléments, est formé des combinaisons linéaires $a_1x_1 + \cdots + a_nx_n$, où les a_i parcourent A. C'est donc la somme des idéaux (x_i). On note traditionnellement $(x_1, \dots, x_n)$ cet idéal, ce qui risque de créer une confusion avec la notation habituelle pour les suites. S'il y a un risque de confusion, on écrira plutôt $\mathrm{A}x_1 + \cdots + \mathrm{A}x_n$ ou $x_1\mathrm{A} + \cdots + x_n\mathrm{A}$.

> EXERCICE 1.23. [A] — On considère les idéaux $\mathfrak{a} = \mathrm{A}x_1 + \cdots + \mathrm{A}x_n$ et $\mathfrak{b} = \mathrm{A}y_1 + \cdots + \mathrm{A}y_m$. Décrire les idéaux $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ et $\mathfrak{a}^2$. Peut-on donner une description simple de $\mathfrak{a} \cap \mathfrak{b}$? [*hint*]

§ 1.2. Anneaux-quotient

1.2.1. Anneaux-quotient

Le pas suivant est un des acquis « modernes ». Le but est de ramener la notion de congruence à celle d'égalité. Dans les notations, il se traduit simplement par la substitution de l'écriture $a \bmod \mathfrak{a} = b \bmod \mathfrak{a}$ à l'écriture $a \equiv b \ [\bmod \mathfrak{a}]$. Formellement, cela consiste, étant donnés un anneau A et

un idéal $\mathfrak{a}$ (par exemple, $A = \mathbf{Z}$ et $\mathfrak{a} = n\mathbf{Z}$ avec $n > 0$), à introduire l'ensemble quotient $A/\mathfrak{a}$ de A par la relation d'équivalence $(a \equiv b \ [\mathrm{mod}\ \mathfrak{a}])$. Cet ensemble quotient est caractérisé par les propriétés suivantes :

- ▷ à chaque élément $a \in A$ correspond un élément $a \bmod \mathfrak{a}$ de $A/\mathfrak{a}$,
- ▷ il n'y a pas d'autres éléments de $A/\mathfrak{a}$ (en termes savants, l'application $a \mapsto a \bmod \mathfrak{a}$ de A dans $A/\mathfrak{a}$ est surjective),
- ▷ les relations $(a \equiv b \ [\mathrm{mod}\ \mathfrak{a}])$ et $(a \bmod \mathfrak{a} = b \bmod \mathfrak{a})$ sont équivalentes.

Mathématiquement, on définit en général $A/\mathfrak{a}$ comme l'ensemble des classes d'équivalence de la relation $a \equiv b \ [\mathrm{mod}\ \mathfrak{a}]$ et on prend pour $a \bmod \mathfrak{a}$ la classe d'équivalence de a. Dans la pratique, on prend souvent une autre solution, celle qui consiste à choisir un système de représentants des classes d'équivalence.

On définit ensuite des opérations dans l'ensemble $A/\mathfrak{a}$ par les relations

$$(x \bmod \mathfrak{a}) + (x \bmod \mathfrak{a}) = (x + y) \bmod \mathfrak{a}, \quad (x \bmod \mathfrak{a})(y \bmod \mathfrak{a}) = xy \bmod \mathfrak{a}.$$

> EXERCICE I.24. [B] — Vérifier que les définitions ci-dessus sont correctes et qu'on obtient ainsi un anneau, dont $0 \bmod \mathfrak{a}$ est l'élément nul et $1 \bmod \mathfrak{a}$ l'élément unité. [*hint*]

L'anneau $A/\mathfrak{a}$ ainsi obtenu est appelé l'anneau-quotient de l'anneau A par l'idéal $\mathfrak{a}$. L'application $a \mapsto a \bmod \mathfrak{a}$ de A dans $A/\mathfrak{a}$ est par définition un homomorphisme surjectif d'anneaux.

Anneau des entiers modulo *n*

Pour tout entier $n \geqslant 0$, on obtient ainsi l'anneau $\mathbf{Z}/n\mathbf{Z}$ des classes d'entiers modulo n, et on note $a \bmod n$ la classe dans $\mathbf{Z}/n\mathbf{Z}$ d'un entier a. Pour $n = 0$, on retrouve $\mathbf{Z}$, avec $a \bmod 0 = a$. Pour $n > 0$, l'anneau $\mathbf{Z}/n\mathbf{Z}$ possède n éléments. Pour $n = 2$, on retrouve le corps $\mathbf{F}_2$, dont les deux éléments $0 = 0 \bmod 2$ et $1 = 1 \bmod 2$ pourraient donc aussi s'appeler « pair » et « impair ».

On prend le plus souvent l'ensemble $\{0, 1, \ldots, n-1\}$ comme modèle de $\mathbf{Z}/n\mathbf{Z}$ et on définit $a \bmod n$ comme l'unique entier r congru à a modulo n et tel que $0 \leqslant r < n$, mais cela n'est pas une obligation. On pourrait tout aussi bien choisir par exemple $\{-1, 0, 1\}$ au lieu de $\{0, 1, 2\}$ pour $n = 3$.

On utilise souvent en informatique les anneaux $\mathbf{Z}/2^k\mathbf{Z}$, notamment pour $k = 16, 32, 64$; on représente leurs éléments en notation binaire par des suites de k bits, mais il ne faut pas confondre ces anneaux avec les anneaux produits $\mathbf{F}_2^k$. Contrairement à ces derniers, les opérations s'y font en effet « avec retenue », la retenue de plus haut poids étant perdue. Si l'on réintroduit cette retenue à l'autre extrémité, on obtient les anneaux $\mathbf{Z}/(2^k - 1)\mathbf{Z}$; si on gère astucieusement cette retenue, on peut travailler modulo $2^k + 1$.

Cela montre l'intérêt qu'il y a à trouver des nombres premiers de la forme $2^k - 1$ (dits *de Mersenne*) ou $2^k + 1$ (dits *de Fermat*).

EXERCICE I.25. [B] — Les anneaux $\mathbf{Z}/n\mathbf{Z}$, pour n parcourant $\mathbf{N}$, sont caractérisés par la propriété suivante : ils ne possèdent pas de sous-anneaux distincts d'eux-mêmes. [*hint*]

Noyaux et images

Un cas très fréquent d'introduction d'anneaux-quotient est le suivant. On considère un homomorphisme d'anneaux $f : A \to B$. Alors le *noyau* $\mathrm{Ker}(f)$ de f est par définition l'ensemble des éléments $a \in A$ tels que $f(a) = 0$. C'est un idéal de A et les conditions $f(a) = f(b)$ et $a \equiv b \ [\mathrm{mod}\ \mathrm{Ker}(f)]$ sont équivalentes.

EXERCICE I.26. [A] — Vérifier ces deux assertions. [*hint*]

Il en résulte que l'on peut prendre comme ensemble quotient $A/\mathrm{Ker}(f)$ l'image $f(A)$ de f. La définition des opérations dans l'anneau-quotient est alors telle que cet anneau est exactement le sous-anneau $f(A)$ de B. Nous rencontrerons souvent cette situation, et notamment dans le cas particulier où l'homomorphisme f est surjectif ; dans ce cas B s'identifie à l'anneau-quotient $A/\mathrm{Ker}(f)$.

Insistons sur ce point : en définitive, les seules propriétés que l'on utilise de l'anneau-quotient d'un anneau A par un idéal $\mathfrak{a}$ sont les suivantes : on a un homomorphisme surjectif d'anneaux $A \to A/\mathfrak{a}$, dont le noyau est $\mathfrak{a}$. La construction explicite choisie pour le quotient est en fin de compte indifférente.

Voici un exemple simple. On considère l'anneau de polynômes $\mathbf{Z}[X]$ et l'idéal engendré par le polynôme $2X - 1$. Dans l'anneau quotient cherché, la classe de X est un inverse de 2, que l'on a envie de noter $1/2$; de même, la classe de X^n est l'inverse de 2^n. Le candidat naturel pour le quotient est le sous-anneau de $\mathbf{Q}$ formé des fractions dont le dénominateur est une puissance de 2. Pourquoi est-ce effectivement le quotient cherché ? On considère l'application f de $\mathbf{Z}[X]$ dans $\mathbf{Q}$ qui applique un polynôme $P(X)$ sur $P(1/2) \in \mathbf{Q}$; c'est un homomorphisme d'anneaux, dont l'image est le sous-anneau considéré. Il reste à prouver que le noyau de f est bien l'idéal engendré par $2X - 1$.

EXERCICE I.27. [B] — Vérifier ce fait, en remarquant d'abord que si $f(P) = 0$, alors P peut s'écrire $(2X - 1)Q$ avec $Q \in \mathbf{Q}[X]$, puis en prouvant que Q est nécessairement à coefficients entiers. [*hint*]

Une autre situation que nous rencontrerons souvent est la suivante. On considère deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A tels que $\mathfrak{a} \subset \mathfrak{b}$. Alors la congruence

modulo $\mathfrak{a}$ implique la congruence modulo $\mathfrak{b}$ et on a un homomorphisme surjectif d'anneaux $A/\mathfrak{a} \to A/\mathfrak{b}$ qui applique $x \bmod \mathfrak{a}$ sur $x \bmod \mathfrak{b}$ pour tout $x \in A$.

EXERCICE 1.28. [A] — Vérifier ce point. [*hint*]

EXERCICE 1.29. [B] — Montrer que, par image réciproque par l'application naturelle de A dans $A/\mathfrak{a}$, les idéaux de $A/\mathfrak{a}$ correspondent bijectivement aux idéaux de A contenant $\mathfrak{a}$. [*hint*]

Ceci s'applique par exemple pour donner un homomorphisme naturel d'anneaux de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$ lorsque m divise n. C'est ainsi qu'on parlera de congruence modulo m de classes d'entiers modulo n. Par exemple, si n est pair, on peut distinguer dans $\mathbf{Z}/n\mathbf{Z}$ des éléments pairs et des éléments impairs.

1.2.2. Idéaux maximaux, idéaux premiers

A quelle condition l'anneau quotient $A/\mathfrak{a}$ est-il un corps ?

Regardons d'abord à quelle condition un élément $x \bmod \mathfrak{a}$ de $A/\mathfrak{a}$ est inversible. Cela signifie qu'il existe un élément $a \in A$ tel que $xa - 1$ appartienne à $\mathfrak{a}$, c'est-à-dire que 1 appartienne à l'idéal $\mathfrak{a} + xA$, ou encore que le plus petit idéal contenant $\mathfrak{a}$ et x soit égal à A.

Dire que cela est vrai pour tout élément x qui n'appartient pas à $\mathfrak{a}$ signifie que les seuls idéaux contenant $\mathfrak{a}$ sont A et $\mathfrak{a}$.

DÉFINITION 1.11. — *On dit que l'idéal* $\mathfrak{a}$ *de l'anneau* A *est* maximal *s'il est distinct de* A*, et si* A *est le seul idéal distinct de* $\mathfrak{a}$ *qui le contienne.*

PROPOSITION 1.12. — *Pour que l'anneau quotient* $A/\mathfrak{a}$ *soit un corps, il faut et il suffit que l'idéal* $\mathfrak{a}$ *soit maximal.*

EXERCICE 1.30. [A] — Pour que l'anneau A soit un corps, il faut et il suffit que l'idéal (0) soit maximal. [*hint*]

On a de même :

DÉFINITION 1.13. — *On dit que l'idéal* $\mathfrak{a}$ *de l'anneau* A *est* premier *s'il est distinct de* A *et si la condition* ($x \notin \mathfrak{a}$ *et* $y \notin \mathfrak{a}$) *implique* ($xy \notin \mathfrak{a}$).

Paraphrasons : l'idéal $\mathfrak{a}$ est premier si la condition $xy \in \mathfrak{a}$ implique ($x \in \mathfrak{a}$ ou $y \in \mathfrak{a}$).

PROPOSITION 1.14. — *Pour que l'anneau quotient* $A/\mathfrak{a}$ *soit intègre, il faut et il suffit que l'idéal* $\mathfrak{a}$ *soit premier.*

EXERCICE 1.31. [A] — Pour que l'anneau A soit intègre, il faut et il suffit que l'idéal (0) soit premier. [*hint*]

Nombres premiers

LEMME 1.15. — *Soit* A *un anneau fini. Tout élément de* A *non diviseur de zéro est inversible. En particulier, tout anneau intègre fini est un corps.*

Démonstration. Soit en effet x un élément non diviseur de zéro de l'anneau fini A. Par définition, la multiplication par x est une application injective de A dans A. Puisque l'ensemble A est fini, elle est bijective, ce qui signifie que x est inversible. □

PROPOSITION 1.16. — *Pour tout entier $n > 1$, les conditions suivantes sont équivalentes :*

(i) n est premier : le seul diviseur > 1 de n est n lui-même,

(ii) l'idéal $n\mathbf{Z}$ de $\mathbf{Z}$ est premier : l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre,

(iii) l'idéal $n\mathbf{Z}$ de $\mathbf{Z}$ est maximal : l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps.

Démonstration. L'équivalence de (ii) et (iii) résulte du lemme. L'équivalence de (i) et (ii) est la caractérisation usuelle des nombres premiers : dire que n est premier, c'est dire qu'il ne peut diviser un produit sans diviser l'un des deux facteurs. □

EXERCICE 1.32. [B] — Soient a et n deux entiers > 1. En utilisant des arguments simples de parité, et les facteurs connus des polynômes de la forme $X^m - 1$ et $X^m + 1$, prouver les deux assertions suivantes :

1) Si $a^n - 1$ est premier, alors on a $a = 2$ et n est premier (« nombres de Mersenne »).

2) Si $a^n + 1$ est premier, alors a est pair et n est une puissance de 2. [*hint*]

1.2.3. Le théorème chinois : version abstraite

On appelle généralement *théorèmes chinois*[6] les énoncés portant sur la résolution simultanée de congruences.

Commençons par le cas de deux modules : on considère un anneau A et deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$. On a un homomorphisme d'anneaux évident

$$\mathrm{A} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b}$$

qui applique x sur $(x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$. Son noyau est par définition l'idéal $\mathfrak{a} \cap \mathfrak{b}$, qui contient l'idéal produit $\mathfrak{a}\mathfrak{b}$. On en déduit un homomorphisme

$$h : \mathrm{A}/\mathfrak{a}\mathfrak{b} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b}$$

tel que, pour tout $x \in \mathrm{A}$, on ait $h(x \bmod \mathfrak{a}\mathfrak{b}) = (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$.

DÉFINITION 1.17. — *On dit que les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de l'anneau* A *sont* étrangers *s'il existe $\alpha \in \mathfrak{a}$ et $\beta \in \mathfrak{b}$ avec $\alpha + \beta = 1$.*

6. En anglais, on dit « Chinese remainder theorem ».

Cela signifie aussi que l'on a $\mathfrak{a} + \mathfrak{b} = \mathrm{A}$. Notons deux cas particuliers. D'abord, dire que les idéaux (a) et $\mathfrak{b}$ sont étrangers signifie que dans l'anneau $\mathrm{A}/\mathfrak{b}$, l'élément $a \bmod \mathfrak{b}$ est inversible. Ensuite, dire que les idéaux (a) et (b) sont étrangers signifie qu'il existe x et y dans A avec $ax + by = 1$. Par exemple, dire que les idéaux $a\mathbf{Z}$ et $b\mathbf{Z}$ de $\mathbf{Z}$ sont étrangers signifie que les entiers a et b sont étrangers (corollaire 1.8).

PROPOSITION 1.18. — *Les conditions suivantes sont équivalentes :*

(i) les idéaux $\mathfrak{a}$ *et* $\mathfrak{b}$ *sont étrangers,*

(ii) l'homomorphisme h *précédent est bijectif.*

De plus, ces conditions impliquent $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

Démonstration. Supposons (i) vérifiée et prouvons (ii). Soient $\alpha \in \mathfrak{a}$ et $\beta \in \mathfrak{b}$ avec $\alpha + \beta = 1$. Prouvons d'abord que l'on a $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ (ce qui signifie que h est injectif). Soit en effet $x \in \mathfrak{a} \cap \mathfrak{b}$. On a $x = x\alpha + x\beta$. Mais on a d'une part $x\alpha \in \mathfrak{a}\mathfrak{b}$, puisque $x \in \mathfrak{b}$ et $\alpha \in \mathfrak{a}$, et d'autre part $x\beta \in \mathfrak{a}\mathfrak{b}$. On en déduit $x \in \mathfrak{a}\mathfrak{b}$ et on a prouvé l'inclusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$. L'inclusion inverse est évidente.

Prouvons maintenant que h est surjectif. Soient y et z deux éléments de A. Il s'agit de trouver un élément $x \in \mathrm{A}$ avec $x \equiv y \ [\bmod \mathfrak{a}]$ et $x \equiv z \ [\bmod \mathfrak{b}]$. On a $y = y\alpha + y\beta$ et $z = z\alpha + z\beta$. Posant $x = y\beta + z\alpha$, on en déduit $x - y = z\alpha - y\alpha \in \mathfrak{a}$ et $x - z = y\beta - z\beta \in \mathfrak{b}$, et l'élément x convient.

Démontrons maintenant que (ii) implique (i), et même que (i) est vrai dès que h est surjectif. Si h est surjectif, on peut en effet trouver $\beta \in \mathrm{A}$ avec $\beta \equiv 1 \ [\bmod \mathfrak{a}]$ et $\beta \equiv 0 \ [\bmod \mathfrak{b}]$, et on a alors $1 = (1 - \beta) + \beta \in \mathfrak{a} + \mathfrak{b}$. □

Rappelons qu'un élément a de A est dit *idempotent* si $e^2 = e$.

COROLLAIRE 1.19. — *Supposons* $\mathfrak{a}$ *et* $\mathfrak{b}$ *étrangers et* $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. *Il existe alors un unique élément idempotent* $e \in \mathfrak{a}$ *tel que* $\mathfrak{a} = \mathrm{A}e$. *De plus* $\mathfrak{a}$ *est exactement l'ensemble des* $x \in \mathrm{A}$ *tels que* $x = ex$. *On a aussi* $\mathfrak{b} = \mathrm{A}f$ *où* f *est idempotent, avec de plus* $ef = 0$ *et* $e + f = 1$.

Démonstration. En effet, il existe par hypothèse $e \in \mathfrak{a}$ et $f \in \mathfrak{b}$ avec $e + f = 1$. Comme ef appartient à $\mathfrak{a} \cap \mathfrak{b}$, on a $ef = 0$. Cela implique $e = (e + f)e = e^2$. Pour $x \in \mathfrak{a}$, on a de même $fx = 0$, donc $x = (e + f)x = ex \in \mathrm{A}e$; inversement, si $x \in \mathrm{A}$ est tel que $x = ex$, on a $x \in \mathrm{A}e$; cela prouve à la fois l'égalité $\mathfrak{a} = \mathrm{A}e$ et la caractérisation annoncée. L'unicité de e est un fait général (voir plus haut). □

Le cas général

Soient maintenant $\mathfrak{a}$, $\mathfrak{b}$ et $\mathfrak{c}$ trois idéaux de A. Si $\mathfrak{a}$ et $\mathfrak{c}$ sont étrangers, ainsi que $\mathfrak{b}$ et $\mathfrak{c}$, alors $\mathfrak{a}\mathfrak{b}$ et $\mathfrak{c}$ sont étrangers ; en effet, si on prend a dans $\mathfrak{a}$, b dans $\mathfrak{b}$, et c et c' dans $\mathfrak{c}$ avec $a + c = 1$ et $b + c' = 1$, on a $ab + (ac' + bc + cc') = 1$. On a ainsi une bijection $\mathrm{A}/\mathfrak{a}\mathfrak{b}\mathfrak{c} \to \mathrm{A}/\mathfrak{a}\mathfrak{b} \times \mathrm{A}/\mathfrak{c}$. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont également étrangers, et si on utilise la première bijection h, on obtient une bijection $\mathrm{A}/\mathfrak{a}\mathfrak{b}\mathfrak{c} \to \mathrm{A}/\mathfrak{a} \times \mathrm{A}/\mathfrak{b} \times \mathrm{A}/\mathfrak{c}$.

Continuant ainsi par récurrence, on obtient :

PROPOSITION I.20 (« théorème chinois »). — *Soient* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *des idéaux de* A *qui sont étrangers deux-à-deux, c'est-à-dire tels qu'on ait* $\mathfrak{a}_i + \mathfrak{a}_j = \mathrm{A}$ *pour* $i \neq j$. *L'application*

$$\mathrm{A}/\mathfrak{a}_1 \cdots \mathfrak{a}_r \to (\mathrm{A}/\mathfrak{a}_1) \times \cdots \times (\mathrm{A}/\mathfrak{a}_r)$$

qui applique $x \bmod \mathfrak{a}_1 \cdots \mathfrak{a}_r$ *sur* $(x \bmod \mathfrak{a}_1, \ldots, x \bmod \mathfrak{a}_r)$ *est un isomorphisme d'anneaux.*

Traduisons : pour toute suite $x_1, \ldots, x_r$ d'éléments de A, il existe un élément $x \in \mathrm{A}$, uniquement déterminé modulo l'idéal produit $\mathfrak{a}_1 \cdots \mathfrak{a}_n$, tel que $x \equiv x_i \ [\mathfrak{a}_i]$ pour $i = 1, \ldots, r$.

§ I.3. Polynômes

I.3.1. Polynômes à une variable

Soit A un anneau. On note A[X] l'anneau des polynômes à coefficients dans A en la variable X. Tout polynôme P s'écrit de façon unique $\sum_{i \in \mathbf{N}} \alpha_i \mathrm{X}^i$, où les α_i non nuls sont en nombre fini. Si P n'est pas nul, son coefficient non nul d'indice le plus élevé (cet indice est le *degré* de P) s'appelle son coefficient *dominant*, et le terme correspondant son terme dominant. On dit que P est *unitaire* si son coefficient dominant est égal à 1.

On note $\deg(\mathrm{P}) \in \mathbf{N}$ le degré du polynôme non nul P. On pose $\deg(0) = -\infty$; ainsi, dire que $\deg(\mathrm{P}) < m$ signifie que $\alpha_m = \alpha_{m+1} = \cdots = 0$.

> EXERCICE I.33. [A] — Si $\deg(\mathrm{P}) > \deg(\mathrm{Q})$, on a $\deg(\mathrm{P} + \mathrm{Q}) = \deg(\mathrm{P})$. Si $\deg(\mathrm{P}) = \deg(\mathrm{Q})$, on a $\deg(\mathrm{P} + \mathrm{Q}) \leqslant \deg(\mathrm{P})$. [*hint*]

> EXERCICE I.34. [B] — Soit $\mathfrak{m}$ l'ensemble des polynômes avec $\alpha_0 = 0$. Montrer que $\mathfrak{m} = (\mathrm{X})$ et que le quotient $\mathrm{A}[\mathrm{X}]/\mathfrak{m}$ s'identifie à A. Montrer que l'idéal $\mathfrak{m}^r$ est formé des polynômes avec $\alpha_0 = \cdots = \alpha_{r-1} = 0$. [*hint*]

LEMME I.21. — *Soient* P *et* Q *deux polynômes non nuls de* A[X]. *Si le coefficient dominant de* P *n'est pas diviseur de zéro, alors* PQ *n'est pas nul et l'on a* $\deg(\mathrm{PQ}) = \deg(\mathrm{P}) + \deg(\mathrm{Q})$.

> EXERCICE I.35. [B] — Faire la démonstration. [*hint*]

PROPOSITION I.22. — *Si* A *est intègre, alors* A[X] *est intègre et l'on a* $\mathrm{A}[\mathrm{X}]^* = \mathrm{A}^*$.

Démonstration. Le coefficient dominant de tout polynôme P non nul de A[X] n'est pas nul, donc n'est pas diviseur de zéro. Par conséquent, P n'est pas diviseur de zéro (lemme précédent). Par ailleurs, si PQ = 1, on a $\deg(\mathrm{P}) + \deg(\mathrm{Q}) = 0$, donc P et Q sont scalaires. □

EXERCICE 1.36. [B] — Soit $a \in A$. A quelle condition, le polynôme $1 - aT$ est-il inversible dans l'anneau $A[T]$? [*hint*]

EXERCICE 1.37. [C] — Soit $P \in A[X]$. Si P est diviseur de zéro, il existe $a \in A$ avec $a \neq 0$ et $aP = 0$ (« théorème de McKoy ») ; on considérera un polynôme Q non nul de degré minimal, tel que $QP = 0$. [*hint*]

1.3.2. Valeurs d'un polynôme

Soit $P = \sum \alpha_i X^i$ un polynôme en X à coefficients dans A. Pour tout élément $a \in A$, on peut considérer l'élément $P(a) = \sum \alpha_i a^i$ de A. L'application $P \mapsto P(a)$ est un homomorphisme d'anneaux. Nous verrons ci-dessous que son noyau est l'idéal $(X - a)$.

EXERCICE 1.38. [A] — L'application $f : P \mapsto P(a)$ est l'unique homomorphisme d'anneaux tel que $f(\alpha) = \alpha$ pour $\alpha \in A$ et $f(X) = a$. [*hint*]

PROPOSITION 1.23. — *Soient* $P \in A[X]$ *et* $a \in A$. *Alors* $P(X) - P(a)$ *est divisible dans* $A[X]$ *par* $X - a$.

Démonstration. En effet, on a pour tout n la relation

$$X^n - a^n = (X - a)(X^{n-1} + \cdots + a^{n-1}) = (X - a) \sum_{i+j=n-1} X^i a^j ,$$

donc $P(X) - P(a) = (X - a)Q(X)$ avec

$$Q(X) = \sum_{i,j} \alpha_{i+j+1} X^i a^j .$$

□

COROLLAIRE 1.24. — *Pour que* $P(a) = 0$*, il faut et il suffit que* $P(X)$ *soit divisible par* $X - a$ *dans* $A[X]$.

Démonstration. C'est nécessaire en vertu de ce qui précède. Inversement, si $P(X) = (X - a)Q(X)$, alors $P(a) = (a - a)Q(a) = 0$. □

COROLLAIRE 1.25. — *Soit* $a \in A$. *L'anneau-quotient* $A[X]/(X - a)$ *s'identifie à* A *: à la classe modulo* $(X - a)$ *d'un polynôme* $P \in A[X]$*, on associe* $P(a) \in A$.

Démonstration. En effet, l'application $P \mapsto P(a)$ est un homomorphisme d'anneaux, évidemment surjectif (prendre P constant), et on vient de voir que son noyau est justement l'idéal $(X - a)$. □

Soit maintenant B un anneau contenant A. La relation de définition $P(a) = \sum \alpha_i a^i$ s'applique tout aussi bien à un élément a de B, et on ob-

tient ainsi un homomorphisme d'anneaux $P \mapsto P(a)$ de $A[X]$ dans B. On peut ainsi parler de racines dans B de polynômes de $A[X]$.

> EXERCICE 1.39. [B] — Tout homomorphisme d'anneaux de $A[X]$ dans B qui prolonge l'identité sur A est de la forme précédente. [*hint*]

Le noyau de l'homomorphisme précédent est par définition l'idéal $\mathfrak{a} \subset A[X]$ formé des polynômes P de $A[X]$ tels que $P(a) = 0$, et l'homomorphisme se factorise *via* un homomorphisme $A[X]/\mathfrak{a} \to B$.

La situation précédente est très fréquente. On a par exemple dans l'anneau $A[X]$ la relation $P(X) = P$! On a rencontré ci-dessus un autre cas extrême : $B = A$ et $\mathfrak{a} = (X-a)$. Nous verrons d'autres exemples ci-dessous.

1.3.3. Division euclidienne des polynômes

PROPOSITION 1.26 (division euclidienne des polynômes). — *Soient* U *et* V *deux polynômes de* $A[X]$. *Supposons que le coefficient dominant de* V *soit inversible dans* A. *Il existe alors deux polynômes* Q *et* R, *uniquement déterminés, avec* $U = VQ + R$ *et* $\deg(R) < \deg(V)$.

Démonstration. Si $U = VQ+R = VQ'+R'$, alors $R'-R = V(Q-Q')$. Si $Q \neq Q'$, on a d'après le lemme 1.21, $\deg(R'-R) = \deg(V) + \deg(Q-Q') \geqslant \deg(V)$, ce qui est contradictoire. Cela prouve l'unicité.

Écrivons $V = bX^m + \cdots$, $m = \deg(V)$. Prouvons l'existence de Q et R par récurrence sur le degré n de U. Si $n < m$, on prend $Q = 0$ et $R = U$. Supposons $n \geqslant m$, et écrivons $U = aX^n + ...$, avec $a \neq 0$. Posons $U' = U - ab^{-1}X^{n-m}V$, de sorte que $\deg(U') < n$. Appliquant l'hypothèse de récurrence à U′, et écrivant $U' = VQ' + R'$, on obtient $U = V(ab^{-1}X^{n-m} + Q') + R'$. □

> EXERCICE 1.40. [B] — Qu'obtient-on pour R lorsque $V(X) = X - a$? que vaut $Q(a)$? [*hint*]

L'existence de la division euclidienne permet de décrire simplement le quotient de l'anneau de polynômes à une variable $A[X]$ par un idéal de la forme (V) où V est *unitaire* (nous verrons que tout idéal non nul est de cette forme lorsque A est un corps). Posons $m = \deg(V) > 0$. La proposition implique alors que les polynômes de degré $< m$ forment alors un système de représentants des classes modulo V. On peut donc identifier cet anneau-quotient $A[X]/(V)$ à l'ensemble des polynômes de degré $< m$; cette identification respecte l'addition et la multiplication par les constantes ; le produit des classes représentées par R et R′ est représenté par le reste de la division de RR′ par V.

Une autre manière de dire essentiellement la même chose est la suivante : notons $\xi = X \bmod V$ l'image de X dans l'anneau-quotient $A[X]/(V)$, de sorte que l'application de passage au quotient n'est autre que $P \mapsto P(\xi)$, ce qui signifie aussi que $P \bmod V = P(\xi)$. On a $V(\xi) = 0$ et chaque élément

de $A[X]/(V)$ s'écrit de manière unique $a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$, avec des $a_i \in A$. Pour $m = 1$, donc $V = X - a$, on retrouve la situation du corollaire 1.25. Pour $m = 2$, donc $V = X^2 - aX - b$, chaque élément de l'anneau quotient s'écrit $\alpha + \beta\xi$, et on a $\xi^2 = a\xi + b$; par exemple, pour $V = X^2 - b$, on obtient la construction algébrique de l'anneau $A[\sqrt{b}]$. Le cas de $\mathbf{C} = \mathbf{R}[X]/(X^2 + 1) = \mathbf{R}(\sqrt{-1})$, avec $i = X \bmod (X^2 + 1) \in \mathbf{C}$, est bien connu.

> EXERCICE 1.41. [B] — Dans l'anneau $A[X]/(X^2 - aX - b)$, on considère la classe de $X + c$; on obtient ainsi une nouvelle description de cet anneau sous la forme $A[Y]/(Y^2 - a'Y - b')$. Que valent a' et b' ? *[hint]*

Il résulte notamment de ce qui précède que si P est un polynôme de degré > 0 à coefficient dominant *inversible*, l'application naturelle de A dans $B = A[X]/(P)$ (qui applique $\alpha \in A$ sur $\alpha \bmod P$) est injective, et qu'on peut ainsi identifier A à un sous-anneau de B. Cela n'est pas vrai sans hypothèse sur P (voir l'exercice 1.42).

> EXERCICE 1.42. [C] — Soit $a \in A$. On pose $B = A[X]/(aX - 1)$. Quel est le noyau de l'application naturelle de A dans B ? *[hint]*

> EXERCICE 1.43. [C] — Soient U et V deux polynômes de $A[X]$. Notons c le coefficient dominant de V, et soit r l'entier $\sup(0, \deg(U) - \deg(V) + 1)$. En modifier comme il convient l'algorithme précédent, prouver qu'il existe deux polynômes Q et R avec $c^r U = VQ + R$ et $\deg(R) < \deg(V)$. *[hint]*

1.3.4. Racines des polynômes

On dit que $a \in A$ est une *racine* du polynôme $P \in A[X]$ si $P(a) = 0$, c'est-à-dire si P est divisible par $X - a$ dans $A[X]$.

Supposons P non nul et soit n son degré. Si $a \in A$ est une racine de P, alors $P(X)$ est divisible par $X - a$ dans $A[X]$ (corollaire 1.24), donc s'écrit $(X-a)Q(X)$. De plus, puisque $X-a$ n'est pas diviseur de zéro, le polynôme $Q(X)$ est uniquement déterminé. Si $Q(a) = 0$, on peut recommencer et écrire $P(X) = (X-a)^2R(X)$, etc. L'opération doit s'arrêter, puisque le degré du quotient diminue de 1 à chaque opération (le coefficient dominant ne change pas par division par le polynôme $X - a$).

Ainsi, pour tout $a \in A$, il existe un entier r, avec $0 \leqslant r \leqslant n$, tel que P soit divisible par $(X - a)^r$ et non par $(X - a)^{r+1}$. On dit que l'entier r est la *multiplicité* de a comme racine de P. Dire que a est racine de P signifie que r est > 0. On dit que a est une *racine simple* si $r = 1$, une *racine multiple* si $r > 1$.

A tout polynôme $P(X) = \sum \alpha_i X^i \in A[X]$, on peut associer son *polynôme dérivé* $P'(X) = \sum i\alpha_i X^{i-1} \in A[X]$. Si P n'est pas nul, le degré de P'

est strictement inférieur au degré de P. Les formules usuelles de dérivation sont valables : on a $(P+Q)' = P' + Q'$ et $(PQ)' = P'Q + PQ'$.

Si a est une racine de P et si l'on écrit $P(X) = (X-a)Q(X)$, on a $P'(X) = (X-a)Q'(X) + Q(X)$, donc $P'(a) = Q(a)$. Par conséquent :

PROPOSITION 1.27. — *Pour que a soit une racine simple de* P*, il faut et il suffit que l'on ait* $P(a) = 0$ *et* $P'(a) \neq 0$.

> EXERCICE 1.44. [C] — Comment peut-on généraliser ce critère aux multiplicités supérieures ? Attention aux facteurs entiers automatiques parasites dans les dérivées successives (introduire des dérivées successives « divisées »). [*hint*]

PROPOSITION 1.28. — *Supposons l'anneau* A *intègre, et soit* $P \in A[X]$. *Soient* $a_1, \ldots, a_m$ *des racines distinctes de* P *dans* A. *Alors* P(X) *est divisible par le produit* $(X-a_1)\cdots(X-a_m)$.

Démonstration. Puisque $P(a_m) = 0$, le polynôme P(X) est divisible par $X-a_m$ dans A[X], donc s'écrit $Q(X)(X-a_m)$. Pour $i < m$, on a $P(a_i) = 0$, donc $Q(a_i)(a_i-a_m) = 0$, ou encore $Q(a_i) = 0$ puisque A est supposé intègre. Ainsi Q a $a_1, \ldots, a_{m-1}$ comme racines et on conclut par récurrence. □

COROLLAIRE 1.29. — *Si l'anneau* A *est intègre, un polynôme de degré n a au plus n racines dans* A.

> EXERCICE 1.45. [B] — Généraliser la proposition et le corollaire précédents en tenant compte des multiplicités. [*hint*]

PROPOSITION 1.30 (« Interpolation de Lagrange »). — *Soient $a_1, \ldots, a_m$ des éléments de* A *tels que $a_i - a_j$ soit inversible pour $i \neq j$. Pour toute famille $\alpha_1, \ldots, \alpha_m$ d'éléments de* A*, il existe un unique polynôme* P *de* A[X] *de degré $< m$ tel que* $P(a_i) = \alpha_i$ *pour tout i.*

Démonstration. C'est une application directe du théorème chinois. Puisque $(X-a_i)-(X-a_j)$ est inversible pour $i \neq j$, les idéaux $(X-a_i)$ sont étrangers deux-à-deux. Tenant compte du corollaire 1.23, le théorème chinois 1.20 se traduit comme suit : l'application

$$(P \bmod (X-a_1)\cdots(X-a_m)) \mapsto (P(a_1), \ldots, P(a_m))$$

est un isomorphisme de l'anneau quotient $A[X]/\big((X-a_1)\cdots(X-a_m)\big)$ sur l'anneau produit A^m. Or cela est simplement une autre forme de l'énoncé. □

> EXERCICE 1.46. [C] — Démontrer directement cette proposition. Donner une formule explicite pour P. [*hint*]

> EXERCICE 1.47. [C] — Généraliser cette proposition avec des multiplicités (« interpolation d'Hermite »). [*hint*]

1.3.5. La méthode de Newton

Un cas de congruence est particulièrement intéressant algébriquement : c'est celui où l'idéal considéré est un carré, ce qui correspond exactement au calcul différentiel de l'Analyse. Expliquons-nous.

On considère un anneau A et un idéal I. Pour $x \in \mathrm{A}$ et $y \in \mathrm{I}$, on a $x^p y^q \in \mathrm{I}^2$ pour $q \geqslant 2$; modulo I^2, la formule du binôme se réduit donc à deux termes : $(x+y)^n = x^n + nx^{n-1}y$. On en déduit pour tout polynôme $f \in \mathrm{A}[\mathrm{X}]$ la relation

$$f(x+y) \equiv f(x) + f'(x)y \ [\mathtt{mod}\ \mathrm{I}^2], \quad x \in \mathrm{A}, \quad y \in \mathrm{I}.$$

D'ailleurs, on peut appliquer cela à l'idéal engendré par la variable Y dans l'anneau de polynômes à deux variables A[X, Y], et on retombe sur une définition possible du polynôme dérivé :

$$f(\mathrm{X}+\mathrm{Y}) \equiv f(\mathrm{X}) + f'(\mathrm{X})\mathrm{Y} \ [\mathtt{mod}\ \mathrm{Y}^2].$$

La méthode de Newton classique consiste à calculer une racine approchée d'un polynôme par itération de l'application $x \mapsto x - f(x)/f'(x)$. L'analogie algébrique consiste à remplacer la condition de petitesse $\|f(x)\| \leqslant \epsilon^n$ par $f(x) \in \mathrm{I}^n$.

PROPOSITION 1.31. — *Soient* A *un anneau,* I *un idéal de* A, *n un entier* > 0, *f un polynôme de* A[X] *et* ξ *une racine de f dans l'anneau-quotient* A/I. *Si* $f'(\xi)$ *est inversible dans* A/I, *il existe un élément x de* A *tel que* $x \ \mathtt{mod}\ \mathrm{I} = \xi$ *et* $f(x) \equiv 0 \ [\mathtt{mod}\ \mathrm{I}^n]$. *De plus, la classe de x modulo* I^n *est uniquement déterminée.*

Choisissons un représentant $a \in \mathrm{A}$ de ξ. On a $f(a) \in \mathrm{I}$ et $f'(a) \ \mathtt{mod}\ \mathrm{I}$ est inversible dans A/I. Choisissons un élément $u \in \mathrm{A}$ tel que $f'(a)u \equiv 1 \ [\mathtt{mod}\ \mathrm{I}]$. Définissons une application $\mathrm{N} : \mathrm{A} \to \mathrm{A}$ par

$$\mathrm{N}(z) = z - uf(z).$$

LEMME 1.32. — *Soit* $i > 0$ *un entier et soit* $z \in \mathrm{A}$ *avec* $z \equiv a \ [\mathtt{mod}\ \mathrm{I}]$ *et* $f(z) \in \mathrm{I}^i$. *On a alors* $\mathrm{N}(z) \equiv z \ [\mathtt{mod}\ \mathrm{I}^i]$ *et* $f\big(\mathrm{N}(z)\big) \in \mathrm{I}^{i+1}$.

Démonstration. Démontrons d'abord le lemme. On a $\mathrm{N}(z) - z = uf(z) \in \mathrm{I}^i$. Par ailleurs, on a, modulo I^{2i}, donc en tout cas modulo I^{i+1},

$$f\big(\mathrm{N}(z)\big) = f\big(z - uf(z)\big) \equiv f(z) - f'(z)uf(z) = f(z)\big(1 - uf'(z)\big).$$

Mais, modulo I, on a $1 - uf'(z) \equiv 1 - uf'(a) \equiv 0$, ce qui implique $f(z)\big(1-uf(z)\big) \in \mathrm{I}^i\,\mathrm{I} = \mathrm{I}^{i+1}$.

Démontrons maintenant la proposition. Définissons la suite (x_i) par $x_1 = a$ et $x_{i+1} = \mathrm{N}(x_i)$ pour $i > 1$. Alors $x = x_n$ convient. On a en effet d'après le lemme

$x_i \equiv a$ [mod I] et $f(x_i) \in \mathrm{I}^i$ pour tout i. Prouvons maintenant l'unicité. Soient x et y dans A avec $x \equiv a$ [mod I], $y \equiv a$ [mod I], $f(x) \in \mathrm{I}^n$ et $f(y) \in \mathrm{I}^n$. Prouvons, par récurrence sur l'entier $p \leqslant n$ que $x - y \in \mathrm{I}^p$, ce qui est vrai pour $p = 1$. Supposons $1 \leqslant p < n$ et $x - y \in \mathrm{I}^p$. On a alors $f(x) - f(y) \equiv f'(x)(x-y)$ [mod I^{2p}] et $1 - uf'(x) \in \mathrm{I}$, donc $x - y = \big(1 - uf'(x)\big)(x-y) + uf'(x)(x-y) \in \mathrm{I}^{p+1}$. □

Remarque 1.33. — La méthode de Newton classique converge « quadratiquement ». Or le lemme précédent montre une convergence « linéaire » : la condition $f(z) \in \mathrm{I}^i$ implique $f\big(\mathrm{N}(z)\big) \in \mathrm{I}^{i+1}$. Cela est dû à ce que u n'est qu'un inverse approché de $f'(z)$. Si l'on remplace cet inverse approché par un véritable inverse de $f'(z)$ dans A/I^i, on obtient comme pour la méthode classique une convergence « quadratique ». Expliquons-nous. Gardons les hypothèses du lemme. Puisque $f'(z)$ est inversible modulo I, il l'est modulo I^i (cela résulte de la méthode de Newton elle-même, par exemple). Notons $f'(z)^{-1}$ un inverse de $f'(z)$ modulo I^i ; on a alors $f\big(z - f'(z)^{-1} f(z)\big) \in \mathrm{I}^{2i}$, comme on le vérifie aisément.

1.3.6. La méthode de Hensel

On applique souvent le résultat précédent avec $\mathrm{A} = \mathbf{Z}$, et $\mathrm{I} = (p)$, où p est un entier (souvent premier dans les applications). On parle alors de *méthode de Hensel* plutôt que de méthode de Newton. L'hypothèse signifie que $\xi \in \mathbf{Z}/p\mathbf{Z}$ est une racine simple du polynôme déduit de $f(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ par réduction des coefficients modulo p. La conclusion implique que la congruence $f(x) \equiv 0$ [mod p^n] a des racines dans $\mathbf{Z}$ pour tout n.

Donnons un exemple. Prenons $\mathrm{A} = \mathbf{Z}$, $\mathrm{I} = (5)$, $f(\mathrm{X}) = \mathrm{X}^2 + 1$ et $\xi = 2$ mod 5. Il existe alors pour tout n un entier x congru à 2 modulo 5 et tel que $x^2 \equiv -1$ [mod 5^n]. On peut donner la construction explicite : on prend $a = 2$, on a $f'(2) = 4$ et on peut prendre $u = -1$, donc $\mathrm{N}(z) = z^2 + z + 1$. Cela donne la suite $x_1 = 2$, $x_2 = \mathrm{N}(2) = 7$, $x_3 = \mathrm{N}(3) = 57$…et on a bien

$$2^2 \equiv -1 \text{ [mod 5]}, \quad 7^2 \equiv -1 \text{ [mod 25]}, \quad 57^2 \equiv -1 \text{ [mod 125]}, \ldots$$

Exercice 1.48. [B] — Le but de cet exercice est de trouver les entiers x à n chiffres décimaux ayant la vertu suivante : si on élève x au carré, les n derniers chiffres de x^2 forment le nombre n. Par exemple, on a $76^2 = 5776$. Il s'agit donc de résoudre $x^2 - x \equiv 0$ [mod 10^n]. On élimine les deux solutions triviales $x = 0$ et $x = 1$. *[hint]*

On peut généraliser la méthode de Newton-Hensel au cas où la dérivée n'est pas inversible. Donnons simplement un exemple : pour tout entier m congru à 1 modulo 8 (par exemple 17), et tout entier n on peut trouver un entier x_n avec $x_n^2 \equiv m$ [mod 2^n]. Il s'agit ici du polynôme $\mathrm{X}^2 - m$, dont la dérivée 2X contient le facteur 2, donc ne peut être inversible modulo un entier pair. La méthode ne peut s'appliquer directement, mais on peut s'y ramener par l'astuce suivante. Écrivons $m = 1 + 8b$ et cherchons x sous la forme $1 + 4y$. L'équation $x^2 - m = 0$ devient $y + 2y^2 - b = 0$. Cette

fois-ci la dérivée $1+4y$ vaut 1 modulo 4. On peut prendre $\mathrm{I}=(4)$, $u=1$ et l'application N est donc $\mathrm{N}(y)=y-(y+2y^2-b)=b-2y^2$. On part de $y=0$, correspondant à $x=1$, qui convient modulo 4 et même modulo 8.

Traitons le cas particulier $m=17$, donc $b=2$ et $\mathrm{N}(y)=2(1-y^2)$. On obtient ainsi successivement :

- ▷ $y=0$, $x=1$ et $1^2\equiv 17$ [mod 16],
- ▷ $y=\mathrm{N}(0)=2$, $x=1+4.2=9$ et $9^2\equiv 17$ [mod 64],
- ▷ $y=\mathrm{N}(2)=-6$, $x=1-4.6=-23$ et $23^2\equiv 17$ [mod 256], ...

EXERCICE 1.49. [C] — Donner un cadre général contenant l'exemple ci-dessus : on part d'un élément a tel que $f(a)\in f'(a)^2\mathrm{I}$. Dans le cas où $f'(a)$ est inversible modulo I, on retrouve la méthode de Newton. [*hint*]

REMARQUE 1.34. — On voit apparaître dans les calculs précédents des séries de puissances par rapport au nombre (premier) p, dont les entiers trouvés sont les sommes partielles. On avait ainsi dans le premier calcul

$$\sqrt{-1}=2.5^0+1.5+2.5^2+\cdots$$

donnant les sommes partielles 2, 7, 57, ... et dans le second

$$\sqrt{17}=2^0+2^3-2^5+\cdots$$

donnant les sommes partielles 1, 9, −23, ... En fait, il s'agit de véritables séries convergentes. Il faut simplement se placer dans un autre corps que le corps **R** des nombres réels : le corps $\mathbf{Q}_p$ des nombres p-adiques, introduit par Hensel. Pour cette construction, voir [**?**], chapitre III.

1.3.7. Anneaux définis par générateurs et relations

Les anneaux s'introduisent souvent par une construction, qui est caractéristique de l'algèbre : on part d'un anneau « de base » déjà connu (par exemple **Z**, ou le corps **Q** des nombres rationnels, ou un anneau de classes de congruences $\mathbf{Z}/n\mathbf{Z}$) et on lui « adjoint » des éléments, assujettis à satisfaire à des relations fixées. Un exemple bien connu est la construction des nombres complexes : on adjoint au corps **R** des nombres réels un élément i tel que $i^2=-1$. Cela signifie en clair que l'on considère l'anneau de polynômes $\mathbf{R}[\mathrm{X}]$, l'idéal (X^2+1), et que l'on définit **C** comme l'anneau quotient $\mathbf{R}[\mathrm{X}]/(\mathrm{X}^2+1)$, dans lequel on désigne par i la classe de X. En fait, on confond souvent dans les notations la variable et sa classe, et on se permet d'écrire $\mathbf{C}=\mathbf{R}[i]/(i^2+1)$.

On construit de même l'anneau $\mathbf{Z}(i)$ des « entiers de Gauss » (nombres complexes dont les parties réelle et imaginaire sont entières) comme le quotient $\mathbf{Z}[\mathrm{X}]/(\mathrm{X}^2+1)$. Ou encore, lorsqu'on veut inverser un élément a de l'anneau A, on considère l'anneau $\mathrm{A}[\mathrm{X}]/(a\mathrm{X}-1)$ dans lequel la classe de a est « forcée d'être inversible », et qui est d'ailleurs égal à A (division euclidienne) lorsque a est inversible dans A. On voit bien sur cet exemple

comment la notion d'anneau-quotient permet de transformer une question d'existence (a possède-t-il un inverse dans A ?) en l'étude des propriétés d'un anneau auxiliaire ($A[X]/(aX-1)$ est-il égal à A ?).

De façon générale, on part d'un anneau A, on prend un anneau de polynômes $A[X_1, ..., X_n]$ en des variables X_1, ..., X_n, et on passe au quotient par l'idéal $\mathfrak{a}$ de cet anneau engendré par un certain nombre de polynômes $P_1(X_1, \dots, X_n), \dots, P_m(X_1, \dots, X_n)$. Notons B l'anneau quotient et notons b_1, ..., b_n les classes dans B des éléments X_1, ..., X_n. On a un homomorphisme naturel de A dans B qui associe à chaque élément de A sa classe modulo $\mathfrak{a}$ (et qui est injectif lorsque l'idéal $\mathfrak{a}$ ne contient pas de polynôme constant autre que 0, ce qui est souvent le cas). En appliquant aux coefficients des polynômes P_i cet homomorphisme, on obtient des polynômes à coefficients dans B que l'on désignera pour simplifier par le même nom. Cela étant, on a par construction dans B les relations voulues

$$P_1(b_1, \dots, b_n) = 0, \ \dots, \ P_m(b_1, \dots, b_n) = 0.$$

L'anneau B est (en un sens adéquat que l'on peut préciser) « le plus général possible » dans lequel on a ces relations. On dit souvent qu'il est obtenu à partir de A par « adjonction des générateurs b_i, soumis aux relations ci-dessus ».

> EXERCICE I.50. [B] — On considère le polynôme $P(X) = X^2 - sX + p \in A[X]$. On note B l'anneau $A[X]/(P(X))$, u la classe de X dans B, et on pose $v = s-u$. On a alors dans B la relation $uv = p$, donc $X^2 - sX + p = (X-u)(X-v)$. L'anneau B peut aussi se décrire comme le quotient de l'anneau A[U, V] par l'idéal engendré par les deux polynômes $U + V - s$ et $UV - p$. [*hint*]

REMARQUE I.35. — On ne confondra pas la notion de relation entre des éléments fixés avec celle d'*identité*, cette confusion étant facilitée par le fait que les mathématiciens appellent *variables* des quantités qui sont syntaxiquement des *constantes*. Ainsi, un anneau satisfaisant à l'identité $X^2 = X$ (« anneau de Boole ») est par définition tel que $a^2 = a$ pour tout $a \in A$, ce qu'il ne faut pas confondre avec un anneau du type $\mathbf{Z}[X]/(X^2 - X)$ où la constante a image de X est assujettie à la relation $a^2 = a$, mais où par exemple $2^2 \neq 2$.

> EXERCICE I.51. [B-C] — Le quotient de l'anneau $\mathbf{F}_2[X_1, \dots, X_n]$ par l'idéal engendré par les $X_i^2 - X_i$ s'identifie à l'ensemble des fonctions booléennes de n variables, c'est-à-dire à l'ensemble des applications de $\mathbf{F}_2^n$ dans $\mathbf{F}_2$, avec `xor` pour addition et `and` pour multiplication. [*hint*]

I.3.8. Un exemple : définition des suites de Lucas

Introduire un anneau auxiliaire peut se révéler bien commode dans certains calculs. Donnons l'exemple des *suites de Lucas*.

Supposons d'abord disposer dans un anneau A d'un élément inversible x. Posons $a = x+x^{-1} \in \mathrm{A}$. Si on pose $\mathrm{V}_n = x^n+x^{-n}$ pour tout $n \in \mathbf{N}$, il est clair que chaque V_n s'exprimera comme un polynôme en a. On a d'ailleurs la relation

$$a\mathrm{V}_n = (x+x^{-1})(x^n+x^{-n}) = x^{n+1}+x^{n-1}+x^{-n+1}+x^{-n-1} = \mathrm{V}_{n+1}+\mathrm{V}_{n-1},$$

d'où la formule de récurrence $\mathrm{V}_{n+1} = a\mathrm{V}_n - \mathrm{V}_{n-1}$ qui, jointe aux deux relations initiales $\mathrm{V}_0 = 2.1_\mathrm{A}$ et $\mathrm{V}_1 = a$, permet de calculer de proche en proche les V_n. On voit que ce calcul ne fait en aucune façon intervenir x. Posons donc la définition suivante

DÉFINITION I.36. — *Soient* A *un anneau et* a *un élément de* A. *On appelle* suite de Lucas *associée à* a, *la suite* (V_n) *d'éléments de* A *définie par récurrence par* $\mathrm{V}_0 = 2.1_\mathrm{A}$, $\mathrm{V}_1 = a$ *et* $\mathrm{V}_{n+1} = a\mathrm{V}_n - \mathrm{V}_{n-1}$.

S'il existe un élément $x \in \mathrm{A}$ tel que $a = x + x^{-1}$, on a alors $\mathrm{V}_n = x^n + x^{-n}$ par récurrence. Mais on peut considérer de toutes façons l'anneau quotient $\mathrm{B} = \mathrm{A}[\mathrm{X}]/(\mathrm{X}^2 - a\mathrm{X} + 1_\mathrm{A})$ et la classe x de X dans B ; on a par construction $x^2 - ax + 1_\mathrm{B} = 0$, soit $x(a1_\mathrm{B} - x) = 1_\mathrm{B}$, ce qui montre que x est inversible dans B avec $x + x^{-1} = a1_\mathrm{B}$. On a par conséquent $x^n + x^{-n} = \mathrm{V}_n 1_\mathrm{B}$. L'application $z \mapsto z1_\mathrm{B}$ de A dans B est injective. Pour démontrer une relation entre les $\mathrm{V}_n \in \mathrm{A}$, il suffit donc de prouver la relation analogue entre les $\mathrm{V}_n 1_\mathrm{B} \in \mathrm{B}$: en d'autres termes, pour prouver une relation entre les V_n, il suffit de le faire lorsqu'il existe un x avec $x + x^{-1} = a$, donc lorsque $x^n + x^{-n} = \mathrm{V}_n$.

EXERCICE I.52. [C] — Il suffit en fait de considérer le cas de l'anneau $\mathrm{A} = \mathbf{Z}[a]$. Vérifier que l'on peut alors identifier B à $\mathbf{Z}[x, x^{-1}] = \mathbf{Z}[x, y]/(xy-1)$. Cela donne dans l'anneau $\mathbf{Z}[x, y]$ une relation :

$$x^n + y^n = \mathrm{V}_n(x + y) + (xy - 1)\mathrm{W}_n(x, y).$$

Comment calculer les W_n ? [*hint*]

PROPOSITION I.37. — *On a pour tout* n *les relations*

$$\begin{aligned} \mathrm{V}_{2n-1} &= \mathrm{V}_n\mathrm{V}_{n-1} - a \\ \mathrm{V}_{2n} &= \mathrm{V}_n^2 - 2 \\ \mathrm{V}_{2n+1} &= a\mathrm{V}_n^2 - \mathrm{V}_n\mathrm{V}_{n-1} - a \end{aligned}$$

Démonstration. On peut donc supposer l'existence d'un $x \in \mathrm{A}$ comme ci-dessus, ce qui donne par exemple

$$\mathrm{V}_n\mathrm{V}_{n-1} = (x^n+x^{-n})(x^{n-1}+x^{-n+1}) = (x^{2n-1}+x^{-2n+1})+(x+x^{-1}) = \mathrm{V}_{2n-1}+a.$$

La deuxième relation se prouve de manière analogue et la troisième se déduit des deux premières par la formule de récurrence. □

EXERCICE 1.53. [A] — Démontrer la relation $V_n V_m = V_{n+m} - V_{n-m}$. [*hint*]

On voit ainsi que si l'on note $f(n)$ le couple $(V_{n-1}, V_n) \in A^2$, on a $f(1) = (2, a)$ et on vient d'exprimer $f(2n)$ et $f(2n+1)$ en termes de $f(n)$: on a $f(2n) = Df(n)$ et $f(2n+1) = Ef(n)$ avec

$$D(x, y) = (xy - a, y^2 - 2), \quad E(x, y) = (y^2 - 2, ay^2 - xy - a).$$

Utilisant la construction donnée en **??**, on en déduit un *algorithme rapide de calcul* des suites de Lucas. Chaque pas D contient deux multiplications et deux soustractions, chaque pas E contient trois multiplications (dont l'une a un facteur a fixe) et trois soustractions. Le nombre total d'opérations pour le calcul de V_n est au plus $3\log(n)$ multiplications et autant d'additions.

EXERCICE 1.54. [N] — Calculer une table des polynômes $V_n \in \mathbf{Z}[a]$. [*hint*]

§ 1.4. Le passage au quotient dans la pratique

1.4.1. Calcul dans un anneau

Avant de parler de quotient, disons rapidement comment se présente la question du calcul sur machine dans un anneau. Bien évidemment, une machine concrète ne manipule pas directement d'objets aussi complexes que des éléments d'un anneau, mais simplement des structures combinatoires simples (suites de bits, chaînes de caractères, petits entiers, …).

On doit d'abord disposer d'une représentation en machine pour les éléments de A. Formellement, on suppose donc disposer d'un ensemble R (« représentations ») et d'une application « valeur » $v : R \to A$. Si on était vraiment réaliste, R devrait être supposé fini ; en tout cas, il est au plus dénombrable. Un élément $\alpha \in R$ tel que $v(\alpha) = a$ est appelé un *représentant* de a.

L'application v n'est pas nécessairement injective (un élément donné de A peut avoir plusieurs représentations), ni surjective (certains éléments de A peuvent ne pas être représentables dans le système choisi — c'est le cas par exemple pour les nombres réels qui, formant un ensemble non dénombrable, ne peuvent être tous représentés par un ensemble dénombrable).

Pour chaque élément privilégié de A (comme 0, 1, …), on se donne une représentation, disons $\hat{0}$, $\hat{1}$, …. Pour chaque opération de A, on se donne une opération correspondante dans R. On suppose ainsi disposer dans R d'opérations

$$\alpha \mapsto \ominus\alpha, \quad (\alpha, \beta) \mapsto \alpha \oplus \beta, \quad (\alpha, \beta) \mapsto \alpha \otimes \beta,$$

telles que

$$v(\ominus\alpha) = -v(\alpha), \quad v(\alpha \oplus \beta) = v(\alpha) + v(\beta), \quad v(\alpha \otimes \beta) = v(\alpha) \times v(\beta).$$

On ne suppose aucune propriété supplémentaire de ces opérations sur les représentations (commutativité, associativité, etc.), sinon d'être explicitement calculables (ce qui est une contrainte lorsque R est infini).

Ainsi, une expression algébrique dans A étant donnée, on peut en calculer effectivement une représentation à partir de représentations des éléments qui y interviennent.

> EXERCICE 1.55. [A] — Pour $A = \mathbf{Z}$, l'application « valeur » est nécessairement surjective. [*hint*]

Pour exécuter des programmes, il faut aussi être capable d'effectuer des *tests*, et spécifiquement de répondre à la question : a-t-on, ou non, $v(\alpha) = v(\beta)$? (*« test d'égalité »*), qui se ramène, en posant $\gamma = \alpha \ominus \beta$, à la question : a-t-on $v(\gamma) = 0$? (*« test de nullité »*). On suppose donc disposer d'un tel test effectif (encore une fois, c'est une contrainte si R est infini). Une manière commode de le faire est de s'arranger pour que l'élément 0 de A n'ait qu'une seule représentation, et il suffit alors de vérifier si γ est égal ou non à $\hat{0}$.

1.4.2. Algorithmes de division

Pour se donner maintenant un idéal de A, on se donnera des représentations $\alpha_1, \ldots, \alpha_n$ d'une famille génératrice, c'est-à-dire que l'on considérera un idéal de la forme $\mathfrak{a} = v(\alpha_1)A + \cdots + v(\alpha_n)A$. Passer effectivement au quotient signifie donner, pour l'anneau-quotient $A/\mathfrak{a}$ et ses opérations, un mécanisme de représentation analogue au précédent.

Une méthode brutale pour le faire est de « revenir avant même la définition du quotient » : on garde le même ensemble R et les mêmes opérations dans R, mais on prend comme valeur l'application $\alpha \mapsto v(\alpha) \bmod \mathfrak{a}$. La seule chose qu'il y aura à changer sera le test d'égalité (ou de nullité) : ce sera maintenant $v(\alpha) \equiv v(\beta)\ [\bmod \mathfrak{a}]$? (ou $v(\gamma) \in \mathfrak{a}$?). De ce point de vue, passer au quotient signifie simplement remplacer le test d'égalité par le *« test de congruence »* (ou le test de nullité par le *« test d'appartenance »*). Même dans le cas le plus simple, celui où l'on suppose que l'anneau donné est directement représenté par lui-même : on a $R = A$ et $v(\alpha) = \alpha$, il nous faut donc un algorithme capable au moins de répondre à la question suivante (*problème d'appartenance à un idéal*) : des éléments $a, a_1, \ldots, a_n$ de A étant donnés, décider s'il existe (et le cas échéant trouver) des éléments $q_1, \ldots, q_n$ de A avec $a = q_1a_1 + \cdots + q_na_n$.

Dans la pratique, on est un peu moins brutal, et on essaye de fabriquer un « vrai » mécanisme de représentation pour les classes de congruence. Pour simplifier la présentation, supposons comme ci-dessus que $R = A$ et fixons

les éléments $a_1, \dots, a_n$, donc l'idéal $\mathfrak{a}$. La situation idéale (sic !), c'est celle où l'on arrive à exhiber, *d'une part* une partie de A dont on baptise les éléments « réduits », de façon que

- ▷ tout élément de A est congru modulo $\mathfrak{a}$ à un élément réduit,
- ▷ deux éléments réduits congrus modulo $\mathfrak{a}$ sont égaux,

(ce qui signifie que chaque classe de congruence possède un unique élément réduit) et *d'autre part* un *algorithme de division*, c'est-à-dire une application effectivement calculable $a \mapsto (q_1, \dots, q_n, r)$ avec les deux propriétés suivantes :

- ▷ on a $a = q_1 a_1 + \cdots + q_n a_n + r$,
- ▷ r est réduit.

Ainsi, l'application de passage au quotient est simplement $a \mapsto r$ et l'algorithme de division résout les problèmes d'appartenance et de congruence.

L'exemple type est celui de la *division euclidienne* dans $\mathbf{Z}$: l'entier $b > 0$ étant fixé, on qualifie de « réduits » les entiers r tels que $0 \leqslant r < b$, et l'algorithme de division associe à tout entier a un entier q et un entier réduit r tels que $a = bq + r$. La situation est la même dans le cas des polynômes en une variable à coefficients dans un corps.

REMARQUE I.38. — Ce qui précède contient notamment le cas particulier de la *divisibilité* : il s'agit, deux éléments a et b de A étant donnés, de trouver s'il existe un $c \in \mathrm{A}$ avec $a = bc$. On voit bien ici la différence entre la théorie où l'on dit « ou bien a est divisible par b, ou bien il ne l'est pas », et la pratique où il faut bien décider dans quel cas on se trouve. Le problème est évidemment plus simple que le cas général décrit ci-dessus, mais il n'est pas totalement trivial pour autant.

Chapitre 2
Divisibilité

Dans ce qui suit, on désigne par A un anneau *intègre* (c'est-à-dire, rappelons-le, un anneau non nul sans diviseurs de zéro, ou ce qui revient au même, qui possède un corps des fractions).

§ 2.1. Plus grand commun diviseur

2.1.1. Idéaux principaux

A chaque élément x de A, on associe l'idéal $(x) = x\mathrm{A}$ formé des multiples de x. Les idéaux (x), pour $x \in \mathrm{A}$, sont dits *principaux*. Il en est ainsi de $\{0\} = (0)$ et de $\mathrm{A} = (1)$. Le cas où tous les idéaux de A sont principaux est particulièrement agréable ; on dit alors que l'anneau A est principal. Nous reviendrons sur ce cas un peu plus loin, après avoir mis en place le vocabulaire général de la divisibilité.

Les conditions « x divise y », « $y \in (x)$ » et « $(y) \subset (x)$ » sont équivalentes. On écrit en ce cas $x \mid y$. On a $1 \mid x \mid 0$. On notera que si $z \neq 0$, la relation $xz \mid yz$ équivaut à $x \mid y$.

De même, les conditions « x est inversible », « $(x) = \mathrm{A}$ » et « $x \mid 1$ » sont équivalentes. Les éléments inversibles de A forment un groupe multiplicatif, noté A^*. On les appelle parfois les *unités* de A.

Pour qu'on ait à la fois $x \mid y$ et $y \mid x$, c'est-à-dire $(x) = (y)$, il faut et il suffit qu'il existe $u \in \mathrm{A}^*$ avec $y = ux$. On dit alors que x et y sont *associés*. C'est une relation d'équivalence. Dans les situations les plus courantes, on dispose d'un système naturel de représentants pour cette relation d'équivalence. Ainsi par exemple, les unités de l'anneau $\mathbf{Z}$ des entiers sont 1 et -1 ; deux entiers sont associés s'ils sont égaux ou opposés ; tout entier est associé à un unique entier positif. De même, dans l'anneau K[X] des polynômes à une variable à coefficients dans un corps K, les éléments inversibles sont les constantes non nulles ; tout polynôme non nul est associé à un unique polynôme unitaire.

2.1.2. Elements extrémaux, éléments premiers

Notre but est d'établir dans un cadre suffisamment général l'analogue de la décomposition des entiers en facteurs premiers. Rappelons que l'existence de cette décomposition s'obtient comme suit : on écrit si on le peut

l'entier considéré comme produit de deux facteurs (distincts de ± 1), et on recommence tant que c'est possible. Tout entier apparaît ainsi comme produit de nombres qui ne peuvent se décomposer plus avant. Pour démontrer l'unicité d'une telle décomposition, on remarque que si l'on fait cette opération de deux façons différentes, alors chacun des facteurs obtenus dans la deuxième décomposition doit diviser le produit des facteurs obtenus dans la première. On utilise alors le fait capital que deux définitions possibles des nombres premiers sont équivalentes : l'entier $p > 1$ est premier lorsqu'il n'a comme diviseurs que $1, -1, p$ et $-p$; l'entier $p > 1$ est premier si chaque fois qu'il divise un produit xy, il divise x ou y. La première de ces propriétés assure l'existence de la décomposition, la seconde son unicité.

Ces deux définitions se transposent à un anneau quelconque. Dans les meilleurs cas, elles coïncident. Cela n'est hélas pas toujours vrai (voir l'exercice I.20), ce qui nous amène à introduire séparément les deux notions.

DÉFINITION 2.1. — *Un élément non nul p de* A *est dit* extrémal[1] *s'il n'est pas inversible, et si tout diviseur de p est soit inversible soit associé à p.*

En d'autres termes, dire que p est extrémal, c'est dire que si l'on écrit $p = xy$, alors x ou y est associé à p, l'autre élément étant alors inversible.

DÉFINITION 2.2. — *Un élément non nul p de* A *est dit* premier *s'il n'est pas inversible, et si chaque fois qu'il divise un produit, il divise l'un des facteurs.*

LEMME 2.3. — *Tout élément premier est extrémal.*

EXERCICE 2.1. [A] — Démontrer ce lemme. [*hint*]

Traduisons les deux définitions précédentes en termes d'idéaux.

Dire que p est premier, c'est dire par définition que l'idéal (p) est premier (définition I.13).

Dire que p est extrémal, c'est dire que $(p) \neq \mathrm{A}$ et que, pour tout x tel que $(p) \subset (x)$, on a $(x) = (p)$ ou $(x) = \mathrm{A}$. En d'autres termes, l'idéal (p) est maximal parmi les idéaux principaux distincts de A. Par conséquent, si tout idéal de A est principal, cela signifie que (p) est un idéal maximal.

Systèmes représentatifs d'éléments extrémaux

Tout élément associé à un élément extrémal (resp. premier) est extrémal (resp. premier). On appelle *système représentatif d'éléments extrémaux* un ensemble $\mathcal{P}$ d'éléments extrémaux de A tel que tout élément extrémal soit associé à un élément de $\mathcal{P}$ et un seul.

Prenons comme premier exemple $\mathrm{A} = \mathbf{Z}$. Les éléments extrémaux de $\mathbf{Z}$ sont les nombres premiers et leurs opposés ; les nombres premiers forment

1. On dit aussi *irréductible*.

un système représentatif d'éléments extrémaux. Les éléments extrémaux sont premiers ; en fait, pour tout nombre premier p, l'idéal (p) est même maximal (et non seulement premier) et l'anneau $\mathbf{Z}/(p)$ est un corps, d'après la proposition 1.16.

Comme autre exemple, prenons pour A l'anneau $K[X_1, \ldots, X_n]$ des polynômes à n variables à coefficients dans un corps K. Les éléments extrémaux de $K[X_1, \ldots, X_n]$ sont appelés *polynômes irréductibles*. Nous verrons ci-dessous que tout polynôme irréductible P est un élément premier de A, c'est-à-dire que l'idéal (P) est premier, et que, lorsque $n = 1$, l'idéal (P) est même maximal. Lorsque $n = 1$, on peut prendre comme système représentatif d'éléments extrémaux de K[X] l'ensemble des polynômes unitaires irréductibles.

2.1.3. Plus grand commun diviseur, plus petit commun multiple

Considérons une suite $x_1, \ldots, x_r$ d'éléments de A.

Définition 2.4. — *On dit qu'un élément m de* A *est un* plus petit commun multiple *(en abrégé* ppcm*) des x_i si m est un multiple de chacun des x_i et si tout multiple commun des x_i est un multiple de m.*

On dit qu'un élément d de A *est un* plus grand commun diviseur *(en abrégé* pgcd*) des x_i si d divise chacun des x_i et si tout diviseur commun des x_i divise d.*

> Exercice 2.2. [A] — Que donne cette définition lorsque $r = 1$? lorsque $r = 0$ (suite vide) ? lorsque l'un des x_i est nul ? lorsque l'un des x_i est égal à 1 ? [*hint*]

On notera que ces définitions ne font intervenir que les idéaux (x_i), (m) et (d).

Parlons d'abord du ppcm. Par définition, *pour qu'un élément m de* A *soit un ppcm des x_i, il faut et il suffit que l'idéal (m) soit l'intersection des (x_i).* Ainsi, si m est un ppcm des x_i, les ppcm des x_i sont exactement tous les éléments associés à m, et si l'on remplace les x_i par des éléments associés, on ne change pas leurs ppcm.

Lorsqu'on dispose d'une manière naturelle de choisir un représentant parmi des éléments associés (c'est le cas par exemple pour $\mathbf{Z}$ en choisissant le représentant $\geqslant 0$, ou pour K[X] en choisissant le représentant unitaire), on parle souvent *du* ppcm et on utilise l'écriture $m = \text{ppcm}(x_1, \ldots, x_r)$.

Lemme 2.5. — *Soit a dans* A *non nul. Si m est un* ppcm *des x_i, alors am est un* ppcm *des ax_i pour tout $a \in$* A.

> Exercice 2.3. [B] — Démontrer ce lemme. [*hint*]

Venons-en au pgcd. La situation n'est pas aussi simple. Dire que d est un pgcd des x_i signifie que (d) est le plus petit idéal *principal* contenant les (x_i), c'est-à-dire le plus petit idéal principal contenant l'idéal $\mathfrak{a} = x_1\mathrm{A} + \cdots x_r\mathrm{A}$. Cela ne signifie pas nécessairement que cet $\mathfrak{a}$ soit principal, mais seulement que parmi les idéaux principaux qui le contiennent, il y en a un plus petit que tous les autres. la condition $d\mathrm{A} = x_1\mathrm{A} + \cdots + x_r\mathrm{A}$ est donc a priori *plus forte* que la condition « d est un pgcd de $(x_1, \ldots, x_r)$ ».

Dans les mêmes conditions que pour le ppcm (choix de représentants parmi des éléments associés), on s'autorise à parler *du* pgcd et à écrire $d = \mathrm{pgcd}(x_1, \ldots, x_r)$. On trouvera souvent dans la littérature (x, y) au lieu de $\mathrm{pgcd}(x, y)$.

REMARQUE 2.6. — La définition que nous avons donnée pour le pgcd et qui nous suffira pour la suite, est trop faible dans le cas général. Par exemple, l'analogue du lemme précédent pour le pgcd n'est pas vrai. Il aurait fallu autoriser dans la définition 2.4 des diviseurs pris dans le corps des fractions de A, c'est-à-dire appeler pgcd des x_i un élément d tel que, pour chaque fraction b/a, dire que b/a divise d signifie que b/a divise tous les x_i. Chassant les dénominateurs, cela veut dire que les diviseurs communs des ax_i sont les diviseurs de ad. Autrement, d est un pgcd (au sens fort) des x_i si, pour tout $a \neq 0$, ad est un pgcd (au sens faible ci-dessus) des ax_i. On peut se demander pourquoi la situation est meilleure dans le cas du ppcm ; la raison en est simple : une fraction multiple d'un élément de A appartient à A par définition !

En fait, l'existence du ppcm implique l'existence du pgcd :

LEMME 2.7. *Soient x et y deux éléments non nuls de* A*, possédant un* ppcm *m. Alors m divise xy, et l'élément $d = xy/m$ de* A *est un* pgcd *de x et y. De plus, pour tout $a \neq 0$, ad est un* pgcd *de ax et ay.*

Démonstration. Puisque xy est un multiple de x et y, c'est un multiple de m. Posons $xy = dm$. On a $dy \mid dm = xy$, donc $d \mid x$; de même, $d \mid y$ et d est un diviseur commun à x et y. Inversement, soit z un diviseur commun de x et y ; on peut écrire $x = az$ et $y = bz$, de sorte que $azy = xy = bzx$ et que $ay = bx$. Posant $ay = bx = c$, on a $cz = xy = dm$. Puisque c est un multiple commun de x et y, on a $m \mid c$. Mais, de $cz = dm$ et $m \mid c$, on déduit $z \mid d$. Ainsi d est bien un pgcd de x et y. Pour tout $a \neq 0$, am est un ppcm de ax et ay, donc $ax.ay/am = ad$ est un pgcd de ax et ay. □

EXERCICE 2.4. [C] — Démontrer l'énoncé inverse : si x, y et d sont tels que ad soit un pgcd de ax et ay pour tout $a \neq 0$, alors xy/d est un ppcm de x et y. [*hint*]

2.1.4. Éléments étrangers

DÉFINITION 2.8. — *On dit que deux éléments non nuls x et y de* A *sont* étrangers *si xy en est un* ppcm*, c'est-à-dire s'ils satisfont à la propriété suivante :*

tout élément de A *divisible simultanément par* x *et par* y *est divisible par* xy.

Alors, d'après le lemme précédent, z est un pgcd de zx et zy pour tout $z \neq 0$. En particulier, tout diviseur commun de x et y est inversible. Dans le cas de $\mathbf{Z}$, on retrouve la notion d'entiers premiers entre eux.

On utilise souvent le classique *lemme d'Euclide* :

LEMME 2.9. — *Si* x *est étranger à* y *et divise* yz*, il divise* z.

Démonstration. En effet, l'élément x, divisant xz et yz, doit diviser leur pgcd z. □

REMARQUE 2.10. — Dire que les idéaux (x) et (y) sont étrangers signifie par définition qu'il existe a et b avec $ax + by = 1$. Cela implique que x et y sont étrangers : en effet, soit m un multiple commun de x et y ; écrivons $m = xz$; on a $z = axz + byz = am + byz$, de sorte que y divise z, ce qui implique que xy divise m. Mais la réciproque est en général fausse (voir l'exercice suivant).

> EXERCICE 2.5. [B] — Dans K[X, Y], où K est un corps, les éléments X et Y sont étrangers, mais $1 \notin (X) + (Y)$. [*hint*]

PROPOSITION 2.11. — *Supposons que, dans l'anneau* A*, l'intersection de deux idéaux principaux soit toujours un idéal principal. Alors :*

a) *tout couple d'éléments possède un pgcd et un ppcm ;*

b) *si* d *est un pgcd et* m *un ppcm de* x *et* y*,* dm *est associé à* xy *;*

c) *pour que deux éléments soient étrangers, il (faut et il) suffit que* 1 *en soit un pgcd, c'est-à-dire que tous leurs diviseurs communs soient inversibles ;*

d) *tout élément extrémal est premier.*

Démonstration. Les trois premières assertions résultent des définitions et du lemme 2.7. Démontrons la quatrième. Soit p un élément extrémal de A, et soient x et y dans A tels que p divise xy. Si p ne divise pas x, p et x n'ont pas de diviseurs communs non inversibles, donc sont étrangers d'après (c) ; alors p divise y (lemme 2.9). □

§ 2.2. Décomposition en produit

2.2.1. Anneaux factoriels

DÉFINITION 2.12. — *On appelle anneau* factoriel *un anneau intègre jouissant des deux propriétés suivantes :*

(a) tout élément non nul et non inversible est le produit d'un nombre fini d'éléments extrémaux ;

(b) tout élément extrémal est premier.

Nous donnerons un peu plus loin des exemples d'anneaux factoriels, autres que l'exemple évident des corps[2] et celui de $\mathbf{Z}$, par exemple les anneaux de polynômes à une ou plusieurs indéterminées à coefficients dans un corps. Dans les cas « concrets » (polynômes par exemple), la condition (a) est évidente : on décompose l'élément donné en produit de facteurs « tant qu'on peut », sans jamais utiliser de facteurs inversibles ; on constate que cela doit s'arrêter (pour des questions de degré par exemple) ; à ce moment là, les facteurs sont extrémaux par définition. La vraie difficulté est dans la condition (b) qui, comme on l'a vu plus haut, est liée à l'existence des ppcm.

Il est commode de disposer de la variante suivante de la définition précédente :

LEMME 2.13. — *Soient* A *un anneau intègre et* $\mathcal{P}$ *une partie de* A *formée d'éléments premiers. Supposons que tout élément non nul de* A *soit le produit d'un élément inversible et d'un nombre fini d'éléments de* $\mathcal{P}$. *Alors* A *est factoriel, et tout élément extrémal de* A *est associé à un élément de* $\mathcal{P}$.

Démonstration. Soit x un élément non nul de A. Écrivons $x = up_1 \cdots p_m$ avec $u \in \mathrm{A}^*$ et les p_i dans $\mathcal{P}$. Si x n'est pas inversible, alors $m \geqslant 1$ et on peut écrire $x = (up_1)p_2 \cdots p_m$, ce qui prouve (a). Si x est extrémal, p_1 divisant x doit lui être être associé, et x est premier. Cela prouve (b), et la dernière assertion du lemme. □

Le théorème de décomposition en facteurs

THÉORÉME 2.14. — *Soient* A *un anneau factoriel et* $\mathcal{P}$ *un système représentatif d'éléments extrémaux de* A. *Pour tout élément* $x \neq 0$ *de* A, *il existe un élément inversible* $u \in \mathrm{A}^*$ *et une famille d'entiers naturels* $(n_p)_{p\in\mathcal{P}}$, *uniquement déterminés, tels que seul un nombre fini des* n_p *soient* $\neq 0$ *et qu'on ait*

$$x = u \prod_{p\in\mathcal{P}} p^{n_p}.$$

On notera que ce produit n'est infini qu'en apparence, puisque tous ses termes, à l'exception d'un nombre fini, sont égaux à 1.

Démonstration. L'existence résulte directement de la condition (a) : si x est inversible, il s'écrit $x = x$; sinon, il s'écrit $q_1 \cdots q_m$ où chaque q_i est extrémal et il suffit d'écrire chaque q_i sous la forme vp avec $v \in \mathrm{A}^*$ et $p \in \mathcal{P}$.

L'unicité résulte de la condition (b) : supposons en effet que l'on ait

$$x = u \prod_{p\in\mathcal{P}} p^{n_p} = u' \prod_{p\in\mathcal{P}} p^{n'_p}.$$

Il s'agit de prouver que $n_p = n'_p$ pour tout p (car cela impliquera $u = u'$ par division). Si par exemple $n_{p_0} < n'_{p_0}$, alors l'élément $x/p^{n_{p_0}}$ est divisible par l'élément

2. car il n'y a alors ni élément non nul et non inversible, ni élément extrémal !

premier p_0 à cause de l'écriture de droite, mais apparaît à gauche comme produit d'un élément inversible et d'éléments extrémaux non associés à p_0, donc d'éléments non divisibles par p_0, ce qui est contradictoire. □

Pour chaque $p \in \mathcal{P}$, et chaque $x \neq 0$, nous noterons $v_p(x)$ le plus grand entier n tel que p^n divise x. Si x s'écrit comme ci-dessus, on a aussitôt $v_p(x) = n_p$, donc

$$x = u \prod_{p \in \mathcal{P}} p^{v_p(x)}, \quad u \in \mathrm{A}^*.$$

On a $v_p(u) = 0$ pour tout élément inversible u. On pose souvent $v_p(0) = +\infty$.

PROPOSITION 2.15. — *Soient x et y deux éléments non nuls de l'anneau factoriel* A.

a) On a $v_p(xy) = v_p(x) + v_p(y)$ pour tout p.

b) Pour que x divise y, il faut et il suffit que $v_p(x) \leqslant v_p(y)$ pour tout p.

c) L'élément $\prod_{p \in \mathcal{P}} p^{\inf\left(v_p(x), v_p(y)\right)}$ est un pgcd de x et y.

d) L'élément $\prod_{p \in \mathcal{P}} p^{\sup\left(v_p(x), v_p(y)\right)}$ est un ppcm de x et y.

e) Pour que x et y soient étrangers, il faut et il suffit que 1 *en soit un pgcd, c'est-à-dire que $\inf\left(v_p(x), v_p(y)\right) = 0$ pour tout p.*

Démonstration. Pour démontrer a), il suffit de multiplier des décompositions de x et y. Si x divise y, on a pour la même raison $v_p(x) \leqslant v_p(y)$ pour tout p ; inversement, si $v_p(x) \leqslant v_p(y)$ pour tout p, posons $z = \prod p^{v_p(y) - v_p(x)}$; alors xz et y sont associés, de sorte que x divise y. On a ainsi prouvé b), qui implique à son tour c), d) et e). □

Notons la conséquence suivante de c) : on a $v_p(x+y) \geqslant \inf\left(v_p(x), v_p(y)\right)$ pour tout p.

Notons explicitement que, puisque qu'un anneau factoriel possède des ppcm, une intersection d'idéaux principaux y est un idéal principal.

2.2.2. Fractions sur un anneau factoriel

Comme tout anneau intègre, un anneau factoriel A possède un corps des fractions K. Les éléments de K sont des fractions a/b, avec a et b dans A et $a \neq 0$, et on a $a/b = a'/b'$ si $ab' = ba'$. Une première nouveauté, c'est l'existence de plus grands communs diviseurs, qui permet de se ramener à des fractions a/b *irréductibles*, c'est-à-dire telles que a et b soient étrangers (il suffit en effet de diviser numérateur et dénominateur par un de leur pgcd). Une autre est l'existence de décompositions en facteurs extrémaux pour tous les éléments de $\mathrm{K}^* = \mathrm{K} - \{0\}$. Fixons un système représentatif

$\mathcal{P}$ d'éléments extrémaux de A. Alors tout élément x de K* s'écrit de façon unique

$$x = u \prod_{p \in \mathcal{P}} p^{n_p},$$

avec $u \in A^*$ et les $n_p \in \mathbf{Z}$. Il suffit en effet d'écrire $x = a/b$ avec a et b dans A et de prendre $n_p = v_p(a) - v_p(b)$. On pose $v_p(x) = n_p$. Dire que $v_p(x) = n$, avec $n \in \mathbf{Z}$, c'est dire que x peut s'écrire $p^n a/b$ avec a et b étrangers à p. Si l'on étend la notion de divisibilité à K* en posant $x \mid y$ lorsque $y/x \in A$, tout ce qu'on a fait dans la proposition 2.15 s'étend à K*.

2.2.3. Anneaux principaux

DÉFINITION 2.16. — *On appelle anneau* principal *un anneau intègre dont tous les idéaux sont principaux.*

PROPOSITION 2.17. — *a) L'anneau* $\mathbf{Z}$ *est principal.*

b) Pour tout corps K*, l'anneau de polynômes* K[X] *est principal.*

Démonstration. L'assertion a) est la proposition 1.6. La démonstration de b) se fait par la même méthode de division euclidienne : soit $\mathfrak{a}$ un idéal de K[X] non réduit à 0. Soit P un polynôme non nul et de degré minimum dans $\mathfrak{a}$. On a $(P) \subset \mathfrak{a}$. Inversement, soit $A \in \mathfrak{a}$. Écrivons $A = PQ + R$ avec $R = 0$ ou $\deg(R) < \deg(P)$. Alors $R = A - PQ \in \mathfrak{a}$, donc $R = 0$ à cause du choix de P. Ainsi $A = PQ \in (P)$. □

REMARQUE 2.18. — On peut croire que la démonstration auquel pensait Fermat pour l'inexistence de solutions entières de l'équation $x^n + y^n = z^n$ pour $n > 2$ se basait sur la forme équivalente $x^n = \prod(z - \zeta y)$, où ζ parcourt les racines n-ièmes de l'unité, et sur un argument de divisibilité. Hélas, l'anneau correspondant (celui qui est formé par les combinaisons linéaires à coefficients entiers des ζ) n'est en général pas principal (c'est par exemple faux pour $n = 23$). Notons au passage que pour ce type d'anneaux, être factoriel équivaut à être principal.

THÉORÉME 2.19. — *Soit* A *un anneau principal.*

a) L'anneau A *est factoriel.*

b) Pour qu'un élément d *de* A *soit un* pgcd *de deux éléments* x *et* y*, il faut et il suffit que* $(d) = (x) + (y)$.

c) Pour que x *et* y *soient étrangers, il faut et il suffit qu'il existe* a *et* b *tels que* $ax + by = 1$.

d) Pour tout élément extrémal p *de* A*, l'anneau* $A/(p)$ *est un corps : l'idéal* (p) *est maximal (définition 1.11).*

Démonstration. Prouvons d'abord d). Soit p un élément extrémal de A. Par définition, (p) est maximal parmi les idéaux principaux $\neq A$, donc parmi tous les idéaux $\neq A$.

Ainsi, A satisfait à la condition (b) de la définition 2.12. Pour prouver a), il s'agit de vérifier la condition (a) de cette définition. Soit F la partie de A formée des éléments qui ne sont ni nuls, ni inversibles, et qui ne peuvent s'écrire comme produit d'éléments extrémaux. Il s'agit de démontrer que F est vide. Soit $x \in F$. Alors x n'est ni nul, ni inversible, ni extrémal (sinon, on écrirait $x = x$!). Il existe donc y et z non inversibles avec $x = yz$. Si y et z avaient des décompositions en produit d'éléments extrémaux, il suffirait d'en faire le produit. Donc, l'un des deux au moins appartient à F. Ainsi, pour tout élément x de F, il existe $x' \in F$ tel que x' divise x et n'est pas associé à x. Si F n'est pas vide, on peut ainsi construire une suite infinie $x_0, x_1, \ldots$ d'éléments de A telle que pour tout $i > 0$, x_i divise x_{i-1} et ne lui soit pas associé. La suite des idéaux (x_i) est croissante, soit α sa réunion. C'est un idéal (le vérifier en exercice), nécessairement principal, donc de la forme (y). Il existe n tel que $y \in (x_n)$. Pour $m > n$, on a $(x_m) \subset (y) \subset (x_n)$, de sorte que $(x_m) = (x_n)$ et que les x_i sont tous associés à partir du rang m, ce qui est contradictoire. Par conséquent F est vide, et A est bien factoriel.

Prouvons b). L'idéal $(x) + (y)$ est principal, donc de la forme (d). Ainsi, pour tout $z \in A$, la condition ($z \mid x$ et $z \mid y$) équivaut-elle à $(d) \subset (z)$, c'est-à-dire à $z \mid d$.

La partie c) résulte de b) et de la proposition 2.11, c). □

Ce qui précède s'applique notamment lorsqu'on prend pour A l'anneau K[X] des polynômes à une variable à coefficients dans un corps K : tout polynôme unitaire non nul s'écrit de façon unique comme produit de polynômes unitaires irréductibles et, pour tout polynôme irréductible P, l'anneau K[X]/(P) est un corps.

> EXERCICE 2.6. [A] — L'anneau introduit dans l'exercice 1.20 n'est pas factoriel, donc n'est pas principal. Exhiber un élément extrémal non premier et un idéal non principal. [*hint*]

REMARQUE 2.20. — Comme on l'aura remarqué, la seule chose un peu délicate dans l'énoncé précédent est la vérification de la condition (a). Mais comme on l'a déjà dit, cette condition est souvent évidente dans les exemples.

> EXERCICE 2.7. [C] — Pour qu'un anneau intègre A soit factoriel, il faut et il suffit qu'il satisfasse à la condition (b) de la définition 2.12 et à la condition suivante :
>
> (a') il n'existe pas de suite infinie $x_0, x_1, \ldots$ d'éléments de A telle que pour tout $i > 0$, x_i divise x_{i-1} et ne lui soit pas associé.
>
> [*hint*]

> EXERCICE 2.8. [B] — Pour qu'un anneau intègre A soit factoriel, il faut et il suffit qu'il satisfasse aux deux conditions suivantes :
>
> (a") tout suite croissante d'idéaux principaux est stationnaire ;
>
> (b') un idéal intersection de deux idéaux principaux est principal.
>
> [*hint*]

2.2.4. Polynômes sur un anneau factoriel

Notons A un anneau factoriel.

DÉFINITION 2.21. — *On appelle* contenu *d'un polynôme non nul de* $A[X]$ *un pgcd de ses coefficients. On dit qu'un polynôme* P *est* primitif *si* 1 *est un contenu de* P.

Si c est un contenu de P, alors ac est un contenu de aP pour tout $a \neq 0$. Tout polynôme non nul peut s'écrire aP où $a \in A$ et où $P \in A[X]$ est primitif (diviser le polynôme donné par l'un de ses contenus). Une telle décomposition est essentiellement unique : les autres sont $(au)(u^{-1}P)$ avec $u \in A^*$. Dire que P est primitif signifie qu'aucun élément extrémal de A ne divise simultanément tous les coefficients de P.

PROPOSITION 2.22 (« lemme de Gauss »). — *Soient* P *et* P' *deux polynômes non nuls de* $A[X]$, c *un contenu de* P, c' *un contenu de* P'. *Alors* cc' *est un contenu de* PP'.

Démonstration. Divisant P par c et P' par c', on se ramène à prouver que si P et P' sont primitifs, alors PP' est primitif. Supposons donc P et P' primitifs, et soit p un élément extrémal de A. Il s'agit de prouver que p ne divise pas tous les coefficients de PP'. Si on remplace chaque coefficient d'un polynôme Q de $A[X]$ par sa classe dans l'anneau-quotient $A/(p)$, on obtient un polynôme $\overline{Q}$ de l'anneau $\big(A/(p)\big)[X]$; bien évidemment, cette construction est compatible avec la multiplication des polynômes. Mais $\overline{P}$ et $\overline{P}'$ sont non nuls, et $\big(A/(p)\big)[X]$ est intègre puisque l'anneau $A/(p)$ est lui-même intègre. Par conséquent $\overline{PP'}$ n'est pas nul, et p ne divise pas tous les coefficients de PP'. □

> EXERCICE 2.9. [B] — Changer la fin de la démonstration précédente pour éviter d'utiliser la réduction modulo p : considérer le premier coefficient de P non divisible par p, et de même pour P'. Est-ce vraiment une autre démonstration ? [*hint*]

REMARQUE 2.23. — Ce qui précède s'étend immédiatement au cas de plusieurs variables.

THÉORÉME 2.24 (Gauss). — *Soient* A *un anneau factoriel et* K *son corps des fractions.*

a) *L'anneau* $A[X]$ *est factoriel.*

b) *Les éléments extrémaux de* $A[X]$ *sont, d'une part les éléments extrémaux de* A, *et d'autre part les polynômes primitifs de* $A[X]$ *qui sont irréductibles dans* $K[X]$.

Démonstration. Notons $\mathcal{P}_1$ et $\mathcal{P}_2$ les ensembles formés respectivement des éléments de chacun des deux types précédents et posons $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$. Puisque $A[X]^* = A^*$, tout élément de $A[X]$ associé à un élément de $\mathcal{P}$ appartient à $\mathcal{P}$.

Vu le lemme 2.13, il nous suffit de prouver les deux assertions suivantes : tout élément non nul de $A[X]$ est produit d'un élément de A^* et d'un nombre fini d'éléments de $\mathcal{P}$; tout élément de $\mathcal{P}$ est premier.

Commençons par la seconde. Soit p un élément de $\mathcal{P}_1$, c'est-à-dire un élément extrémal (donc premier) de A. S'il divise un produit de deux polynômes, il divise l'un d'eux d'après le lemme de Gauss. Ainsi, p est premier dans A[X].

Soit maintenant P un élément de $\mathcal{P}_2$, et Q et R deux polynômes de A[X] tels que P divise QR dans A[X]. Puisque P est irréductible dans K[X], il divise Q ou R dans cet anneau, par exemple Q. Choisissant un dénominateur commun pour les coefficients de Q/P, on voit qu'il existe $S \in A[X]$ et $a \in A$ avec $aQ = PS$. Passant aux contenus, et appliquant le lemme de Gauss, on voit que, puisque P est primitif, a divise le contenu de S, donc divise S dans A[X]. Cela donne $Q = P.(S/a)$ et P divise Q. On a ainsi prouvé que P est premier.

Il reste à prouver que tout polynôme non nul et non inversible Q de A[X] est produit d'un nombre fini d'éléments de $\mathcal{P}$. Chaque polynôme irréductible de K[X] est multiple d'un élément de $\mathcal{P}_2$ (rendre le polynôme à coefficients dans A en le multipliant par un dénominateur commun des coefficients, puis diviser le polynôme obtenu par son contenu). Ainsi, Q est, dans K[X], associé à un produit d'éléments de $\mathcal{P}_2$, disons R. Il existe donc a et b non nuls dans A avec $aQ = bR$. Puisque R est un produit de polynômes primitifs, le lemme de Gauss implique que a divise b. Mais, dans l'anneau factoriel A, l'élément b/a est le produit d'un élément de A^* et d'un nombre fini d'éléments de $\mathcal{P}_1$. Par conséquent, $Q = (b/a).R$ est le produit d'un élément de A^* et d'un nombre fini d'éléments de $\mathcal{P}$, ce qu'on voulait démontrer. □

COROLLAIRE 2.25. — *Tout anneau de polynômes en un nombre fini d'indéterminées à coefficients dans un anneau factoriel est un anneau factoriel.*

Démonstration. Il suffit d'adjoindre successivement les indéterminées. □

En particulier, les anneaux $K[X_1, \ldots, X_n]$ où K est un corps sont factoriels. Tout polynôme s'y décompose de façon essentiellement unique (aux facteurs scalaires près) en produit de polynômes irréductibles.

§ 2.3. Anneaux euclidiens

2.3.1. Définitions

Pour calculer dans un anneau principal, et d'ailleurs déjà pour savoir qu'un anneau donné est principal, on doit être capable, un idéal étant donné, d'en trouver un générateur. Ce n'est pas toujours facile. Il existe une classe d'anneaux principaux plus maniables : ceux où l'on dispose d'un mécanisme de division euclidienne. Expliquons cela en restant d'abord sur le plan théorique.

Supposons donnés un anneau A et une application $\phi : A - \{0\} \to \mathbf{N}$ satisfaisant à la condition suivante :

(E) Pour tout couple d'éléments a et b non nuls de A, il existe deux éléments q et r avec $a = bq + r$ et, soit $r = 0$, soit $\phi(r) < \phi(b)$.

Alors tout idéal $\mathfrak{a}$ de A est principal. Il suffit en effet de copier la démonstration de la proposition 1.6. C'est évident si $\mathfrak{a} = \{0\}$. Si $\mathfrak{a} \neq \{0\}$, soit $b \in \mathfrak{a}$ avec $\phi(b)$ minimal. On a $(b) \subset \mathfrak{a}$. Inversement, soit $a \in \mathfrak{a}$; appliquons (E) ; on a $r = a - bq \in \mathfrak{a}$, ce qui implique $r = 0$ à cause du choix de b, et donc $a = bq \in (b)$. Indiquons tout de suite que non seulement A est principal, mais qu'on va donner ci-dessous un algorithme de calcul des pgcd, donc un moyen de *construire effectivement* un générateur d'un idéal donné.

Remarque 2.26. — On s'est en fait à peine servi des hypothèses. L'application ϕ n'intervient que par l'intermédiaire de la relation $\phi(x) > \phi(y)$ sur $A - \{0\}$, et la seule propriété de cette relation qui serve, c'est que si on la note $x \succ y$ par exemple, on ne puisse pas avoir de chaînes infinies $x_0 \succ x_1 \succ \cdots$.

Donnons des exemples. D'abord $A = \mathbf{Z}$ et $\phi(n) = |n|$ ou $\phi(n) = n^2$ (division euclidienne des entiers). Ensuite $A = K[X]$ et $\phi(P) = \deg(P)$ (division euclidienne des polynômes). Généralisant le cas de $\mathbf{Z}$, on a celui des entiers de Gauss : $A = \mathbf{Z}(i)$ et $\phi(\alpha + \beta i) = \alpha^2 + \beta^2$ (voir exercice 2.10).

Remarque 2.27. — En fait, le cas le plus agréable, c'est celui où ϕ est compatible avec la multiplication, comme dans les exemples de $\mathbf{Z}$ et $\mathbf{Z}(i)$. Dans le cas des polynômes, on peut l'obtenir en prenant $\phi(P) = 2^{\deg(P)}$.

Supposons donc que $\phi(ab) = \phi(a)\phi(b)$ pour a et b dans $A - \{0\}$. Si ϕ est identiquement nul, alors A est un corps (d'après (E)) ; éliminons ce cas. Alors $\phi(1) = 1$ (prendre dans l'identité ci-dessus $a = 1$). Pour tout $u \in A^*$, on a $\phi(u)\phi(u^{-1}) = \phi(1) = 1$, donc nécessairement $\phi(u) = 1$. On ne peut jamais avoir $\phi(b) = 0$, car (E) appliqué avec $a = 1$ impliquerait que b est inversible. Réappliquant (E) avec $a = 1$, on voit que $\phi(b) = 1$ implique $b \in A^*$. Ainsi, la condition $\phi(u) = 1$ caractérise les éléments inversibles.

> Exercice 2.10. [C] — Fixons un entier d qui n'est pas un carré parfait et considérons les anneaux $A = \mathbf{Z}(\sqrt{d})$ et $K = \mathbf{Q}(\sqrt{d})$ formés des expressions $(\alpha + \beta\sqrt{d})$ avec α et β parcourant $\mathbf{Z}$ et $\mathbf{Q}$ respectivement. Pour $u = \alpha + \beta\sqrt{d} \in K$, posons $\overline{u} = \alpha - \beta\sqrt{d} \in K$ et définissons $\phi : \mathbf{Q}(\sqrt{d}) \to \mathbf{Q}$ et $\phi : \mathbf{Z}(\sqrt{d}) \to \mathbf{N}$ par $\phi(\alpha + \beta\sqrt{d}) = |\alpha^2 - d\beta^2|$.
>
> a) Prouver que $u\overline{u} = \pm\phi(u)$, et en déduire que K est le corps des fractions de A. Démontrer les relations $\overline{uv} = \overline{u}\,\overline{v}$ et $\phi(uv) = \phi(u)\phi(v)$.
>
> b) Montrer que la propriété (E) équivaut à la suivante : pour tout $x \in K$, il existe $a \in A$ avec $\phi(x - a) < 1$.
>
> c) Montrer que cette propriété est vraie pour $d = -1$, $d = -2$, $d = 2$, $d = 3$. Dans ces quatre cas, A est donc principal. Pour $d = -5$, A n'est pas principal (exercice 1.20). [*hint*]

La définition formelle des anneaux euclidiens est assez variable selon les auteurs. La propriété (E) ci-dessus fait intervenir explicitement une fonction ϕ et implicitement l'existence d'un procédé de division. Pour nous, qui nous intéressons ici à des algorithmes concrets, les priorités sont inverses :

l'existence de la fonction ϕ va assurer la terminaison de l'algorithme d'Euclide, mais nous avons besoin d'un procédé de division explicite pour définir cet algorithme.

DÉFINITION 2.28. — *Nous appellerons* anneau euclidien *un anneau intègre* A *dans lequel on a fixé une application de* $\mathrm{A} \times (\mathrm{A} - \{0\})$ *dans* A, *notée*

$$(v, u) \mapsto (v \div u)$$

possédant la propriété suivante :

il existe une application $\phi : \mathrm{A} - \{0\} \to \mathbf{N}$ *telle que, pour tout couple* (v, u) *d'éléments de* A *avec* $u \neq 0$ *on ait, soit* $v - (v \div u)u = 0$, *soit* $\phi(v - (v \div u)u) < \phi(u)$.

Dans l'anneau K[X] par exemple, on prendra pour $(v \div u)$ le quotient de la division euclidienne : c'est l'unique polynôme tel que ait

$$\deg(v - (v \div u)u) < \deg(u).$$

L'algorithme d'Euclide

Un anneau euclidien est principal, comme on l'a vu plus haut. Dans un anneau euclidien, l'algorithme d'Euclide est donné par les règles usuelles :

ALGORITHME 2.29. — *Algorithme d'Euclide*

Entrées : éléments x et y d'un anneau euclidien. *Sorties :* $\mathrm{pgcd}(x, y)$.
Règles :

$$\begin{array}{lccl} [x \neq 0] : & (x, y) & \mapsto & (y - (y \div x)x, x) \\ [x = 0] : & (x, y) & \mapsto & x \end{array}$$

Cet algorithme transforme tout couple (x, y) en un pgcd de x et y, c'est-à-dire un élément d tel que $\mathrm{A}x + \mathrm{A}y = \mathrm{A}d$.

EXERCICE 2.11. [A] — Vérifier la terminaison et la correction de cet algorithme. [*hint*]

EXERCICE 2.12. [B] — Soient $a_1, \ldots, a_n$ des éléments de A. Comment calcule-t-on un pgcd des a_i, donc un générateur de l'idéal engendré par les a_i ? [*hint*]

Le cas des entiers

Dans le cas de $\mathbf{Z}$, plusieurs divisions sont possibles. Fixons une application $\mathrm{E} : \mathbf{R} \mapsto \mathbf{Z}$ telle que

$$|x - \mathrm{E}(x)| < 1 \text{ pour tout } x \in \mathbf{R}.$$

On peut par exemple prendre

$$\begin{array}{rcll} \mathrm{E}(x) \leqslant & x & < \mathrm{E}(x) + 1 & \text{(partie entière par défaut),} \\ \mathrm{E}(x) - 1 < & x & \leqslant \mathrm{E}(x) & \text{(partie entière par excès),} \\ \mathrm{E}(x) - \frac{1}{2} \leqslant & x & < \mathrm{E}(x) + \frac{1}{2} & \text{(entier le plus proche par défaut),} \\ \mathrm{E}(x) - \frac{1}{2} < & x & \leqslant \mathrm{E}(x) + \frac{1}{2} & \text{(entier le plus proche par excès).} \end{array}$$

Alors $(y \div x) = \mathrm{E}(y/x)$ convient, car $|y - \mathrm{E}(y/x)x| = |x|.|y/x - \mathrm{E}(y/x)| < |x|$. La division euclidienne usuelle correspond à la partie entière par défaut.

On note traditionnellement $\lfloor x \rfloor$ la partie entière par défaut et $\lceil x \rceil$ la partie entière par excès. On a donc

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1, \qquad \lceil x \rceil - 1 < x \leqslant \lceil x \rceil$$

EXERCICE 2.13. [A] — Exprimer les deux fonctions « entier le plus proche » ci-dessus à l'aide des fonctions « partie entière ». [*hint*]

EXERCICE 2.14. [C] — Considérons une fonction $\mathrm{E} : \mathbf{R} \to \mathbf{Z}$ telle que $|x - \mathrm{E}(x)| < 1$.

Supposons d'abord que $\mathrm{E}(x+1) = \mathrm{E}(x) + 1$ pour tout x. Alors $\mathrm{E}(x + n) = \mathrm{E}(x) + n$ pour $n \in \mathbf{Z}$ et $\mathrm{E}\big(x - \mathrm{E}(x)\big) = 0$. De plus, $\mathrm{E}(x)$ est l'unique entier n tel que $\mathrm{E}(x - n) = 0$. Ainsi, la donnée de E équivaut à celle de la partie I de $\mathbf{R}$ formée des x tels que $\mathrm{E}(x) = 0$. Cette partie doit satisfaire aux deux conditions suivantes : I est contenue dans l'intervalle ouvert $]-1, 1[$, $\mathbf{R}$ est réunion disjointe des translatées $\mathrm{I} + n$.

On suppose de plus que E est croissante. Alors I est un intervalle semi-ouvert de longueur 1. Ainsi, E est de l'une des deux formes suivantes $\mathrm{E}(x) = \lfloor x + \alpha \rfloor$ avec $0 \leqslant \alpha < 1$, ou $\mathrm{E}(x) = \lceil x - \alpha \rceil$ avec $0 \leqslant \alpha < 1$. [*hint*]

2.3.2. Expression matricielle de l'algorithme d'Euclide

Nous allons étudier de plus près le fonctionnement des algorithmes du type d'Euclide. Fixons un cadre : on travaille dans un anneau, disons A, sur lequel on ne fait aucune hypothèse particulière et on a une suite d'éléments (x_i) avec $x_0 = x$, $x_1 = y$ et

$$x_{i+1} = x_{i-1} - q_i x_i, \quad i \geqslant 1$$

où les q_i sont des éléments de A. Par construction, l'idéal $\mathrm{A}x_i + \mathrm{A}x_{i+1}$ est indépendant de i, donc égal à $\mathrm{A}x + \mathrm{A}y$. Si $x_{n+1} = 0$, on a alors $\mathrm{A}x_n = \mathrm{A}x + \mathrm{A}y$, ce qui implique que x_n est un pgcd de x et y dans A.

Le pas élémentaire de l'algorithme transforme le couple (x_{i-1}, x_i) en (x_i, x_{i+1}). En notation matricielle, on a

$$\begin{bmatrix} x_i \\ x_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} x_{i-1} \\ x_i \end{bmatrix}$$

et par inversion

$$\begin{bmatrix} x_{i-1} \\ x_i \end{bmatrix} = \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_i \\ x_{i+1} \end{bmatrix}.$$

On a par conséquent les relations

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_n \\ x_{n+1} \end{bmatrix},$$

$$\begin{bmatrix} x_n \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Les polynômes continuants d'Euler

Définissons par récurrence des polynômes à coefficients entiers positifs en les variables q_i par $\mathrm{Q}_{-1} = 0$, $\mathrm{Q}_0 = 1$ et

$$\mathrm{Q}_{i+1}(q_1, \ldots, q_{i+1}) = q_{i+1}\mathrm{Q}_i(q_1, \ldots, q_i) + \mathrm{Q}_{i-1}(q_1, \ldots, q_{i-1}).$$

On a ainsi

$$\begin{aligned} \mathrm{Q}_1 &= q_1, \\ \mathrm{Q}_2 &= 1 + q_1q_2, \\ \mathrm{Q}_3 &= q_1 + q_3 + q_1q_2q_3, \\ \mathrm{Q}_4 &= 1 + q_1q_2 + q_1q_4 + q_3q_4 + q_1q_2q_3q_4. \end{aligned}$$

Exercice 2.15. [B] — Prouver qu'on a

$$\mathrm{Q}_n(1, \ldots, 1, 1) = \mathrm{F}_{n+1}, \quad \mathrm{Q}_n(1, \ldots, 1, 2) = \mathrm{F}_{n+2}.$$

[*hint*]

Exercice 2.16. [B] — Pour toute famille (q_i) d'entiers > 0, on a

$$\mathrm{F}_n + \prod_{1 \leqslant i \leqslant n} q_i \leqslant \mathrm{Q}_n(q_1, \ldots, q_n) \leqslant \prod_{1 \leqslant i \leqslant n} (q_i + 1).$$

[*hint*]

Lemme 2.30. *On a, pour tout* $n \geqslant 1$,

$$\begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \mathrm{Q}_n(q_1, \ldots, q_n) & \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1}) \\ \mathrm{Q}_{n-1}(q_2, \ldots, q_n) & \mathrm{Q}_{n-2}(q_2, \ldots, q_{n-1}) \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} = (-1)^n \begin{bmatrix} \mathrm{Q}_{n-2}(q_2, \ldots, q_{n-1}) & -\mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1}) \\ -\mathrm{Q}_{n-1}(q_2, \ldots, q_n) & \mathrm{Q}_n(q_1, \ldots, q_n) \end{bmatrix}.$$

Exercice 2.17. [B] — Vérifier ce lemme. Montrer qu'on a

$$\begin{aligned} \mathrm{Q}_{n+m}(q_1, \ldots, q_{n+m}) &= \mathrm{Q}_n(q_1, \ldots, q_n)\mathrm{Q}_m(q_{n+1}, \ldots, q_{n+m}) \\ &+ \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1})\mathrm{Q}_{m-1}(q_{n+2}, \ldots, q_{n+m}), \end{aligned}$$

et en particulier

$$\mathrm{Q}_{n+1}(q_1, \ldots, q_{n+1}) = q_1\mathrm{Q}_n(q_2, \ldots, q_{n+1}) + \mathrm{Q}_{n-2}(q_3, \ldots, q_{n+1}).$$

En déduire

$$\mathrm{Q}_n(q_n, \ldots, q_1) = \mathrm{Q}_n(q_1, \ldots, q_n).$$

[*hint*]

EXERCICE 2.18. [A] — On a

$$\mathrm{Q}_n(q_1,\dots,q_n)\mathrm{Q}_{n-2}(q_2,\dots,q_{n-1})-\mathrm{Q}_{n-1}(q_2,\dots,q_n)\mathrm{Q}_{n-1}(q_1,\dots,q_{n-1}) = (-1)^n.$$

[*hint*]

EXERCICE 2.19. [C] — Donner une expression générale pour Q_n. [*hint*]

On a par conséquent

$$\begin{aligned} x &= \mathrm{Q}_n(q_1,\dots,q_n)x_n + \mathrm{Q}_{n-1}(q_1,\dots,q_{n-1})x_{n+1},\\ y &= \mathrm{Q}_{n-1}(q_2,\dots,q_n)x_n + \mathrm{Q}_{n-2}(q_2,\dots,q_{n-1})x_{n+1},\\ x_n &= (-1)^{n-2}\mathrm{Q}_{n-2}(q_2,\dots,q_{n-1})x + (-1)^{n-1}\mathrm{Q}_{n-1}(q_1,\dots,q_{n-1})y. \end{aligned}$$

En particulier, si l'algorithme s'arrête au bout de n pas, c'est-à-dire si $x_{n+1} = 0$, alors $x_n = d$ sera un pgcd de $x_0 = x$ et $x_1 = y$ et on aura explicitement

$$\begin{aligned} x &= d\,\mathrm{Q}_n(q_1,\dots,q_n),\\ y &= d\,\mathrm{Q}_{n-1}(q_2,\dots,q_n),\\ d &= (-1)^{n-2}\mathrm{Q}_{n-2}(q_2,\dots,q_{n-1})x + (-1)^{n-1}\mathrm{Q}_{n-1}(q_1,\dots,q_{n-1})y. \end{aligned}$$

2.3.3. L'algorithme d'Euclide étendu

Reprenons les notations précédentes : on a $x_0 = x$, $x_1 = y$,

$$x_{i+1} = x_{i-1} - q_i x_i, \quad 1 \leqslant i \leqslant n,$$

$x_n = d$ et $x_{n+1} = 0$. Comme on l'a déjà vu dans le cas des entiers, le mécanisme décrit permet aussi de calculer des éléments a et b tels que $d = ax + by$. Plus généralement, supposons x et y donnés sous la forme

$$x = x_0 = a_0 u + b_0 v, \quad y = x_1 = a_1 u + b_1 v.$$

Il est alors immédiat qu'on aura pour tout i la relation $x_i = a_i u + b_i v$ avec

$$a_{i+1} = a_{i-1} - q_i a_i, \quad b_{i+1} = b_{i-1} - q_i b_i.$$

Si on prend initialement $u = x$ et $y = v$, avec $a_0 = b_1 = 1$ et $a_1 = b_0 = 0$, on obtiendra $x_i = a_i x + b_i y$ et en particulier $d = x_n = a_n x + b_n y$.

En fait, cela revient à faire fonctionner l'algorithme sur des vecteurs à trois composantes de la forme $\vec{v}_i = (x_i, a_i, b_i)$ avec

$$\vec{v}_0 = (x, 1, 0), \quad \vec{v}_1 = (y, 0, 1), \quad \vec{v}_{i+1} = \vec{v}_{i-1} - q_i \vec{v}_i.$$

Lorsque n est tel que $x_{n+1} = 0$, on a $\vec{v}_n = (d, a, b)$, avec $d = ax + by$ et $\mathrm{A}d = \mathrm{A}x + \mathrm{A}y$. C'est ce que l'on appelle *« l'algorithme d'Euclide étendu »*. Notons au passage l'écriture matricielle :

$$\begin{bmatrix} x_i & a_i & b_i \\ x_{i+1} & a_{i+1} & b_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} x_{i-1} & a_{i-1} & b_{i-1} \\ x_i & a_i & b_i \end{bmatrix}$$

qui donne en définitive

$$\begin{bmatrix} d & a & b \\ 0 & ? & ? \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} x & 1 & 0 \\ y & 0 & 1 \end{bmatrix}.$$

EXERCICE 2.20. [C] — Que valent les deux points d'interrogation ci-dessus ? [*hint*]

EXERCICE 2.21. [A] — On a $a_i b_{i+1} - a_{i+1} b_i = (-1)^i$ et

$$\begin{aligned} a &= (-1)^n \mathrm{Q}_{n-2}(q_2, \ldots, q_{n-1}) \\ b &= (-1)^{n-1} \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1}). \end{aligned}$$

[*hint*]

EXERCICE 2.22. [A] — Les éléments a et b sont étrangers (au sens fort : il existe e et f avec $ae + bf = 1$), pourquoi ? [*hint*]

Dans un anneau euclidien, on obtient donc les règles suivantes, qui réécrivent un couple d'éléments (x, y) de A en un triplet (d, a, b) où d est un pgcd de x et de y et où $d = ax + by$.

ALGORITHME 2.31. — *Algorithme d'Euclide étendu, version symétrique*

Entrées : éléments x et y. *Sorties :* éléments d, a et b avec $d = \mathrm{pgcd}(x, y)$ et $ax + by = d$.

Règles :

$$\begin{array}{lrcl} & (x, y) & \mapsto & (x, 1, 0, y, 0, 1) \\ [u \neq 0] : & (u, a', b', v, a, b) & \mapsto & (v - qu, a - qa', b - qb', u, a', b') \\ & & & \text{avec } q = v \div u \\ [u = 0] : & (u, a', b', v, a, b) & \mapsto & (v, a, b) \end{array}$$

EXERCICE 2.23. [B] — Vérifier directement la validité de cet algorithme. [*hint*]

Comme dans le cas des entiers, on a la variante suivante :

ALGORITHME 2.32. — *Algorithme d'Euclide étendu, version dissymétrique*

Entrées : éléments x et y. *Sorties :* éléments d et a avec $d = \mathrm{pgcd}(x, y)$ et $ax \equiv d \ [\mathtt{mod}\ y]$.

Règles :

$$\begin{array}{lrcl} & (x, y) & \mapsto & (x, 1, y, 0) \\ [u \neq 0] : & (u, a', v, a) & \mapsto & (v - qu, a - qa', u, a') \text{ avec } q = v \div u \\ [u = 0] : & (u, a', v, a) & \mapsto & (v, a) \end{array}$$

En particulier, cela nous donne un algorithme d'inversion dans l'anneau quotient $\mathrm{A}/(y)$: si d est inversible dans A, alors $x \ \mathtt{mod}\ y$ est inversible, d'inverse $d^{-1} a \ \mathtt{mod}\ y$; sinon, $x \ \mathtt{mod}\ y$ n'est pas inversible.

§ 2.4. Fractions continues

2.4.1. Définition

Supposons maintenant que A soit un corps et soit α dans A. Nous allons appliquer les résultats de 2.3.2 au couple $(\alpha, 1)$, en décalant les indices d'une unité. Nous posons donc $x_{-1} = \alpha$, $x_0 = 1$ et nous supposons données deux suites, (x_i) pour $i \geqslant 2$ et (q_i) pour $i \geqslant 0$, avec

$$x_{i+1} = x_{i-1} - q_i x_i, \quad i \geqslant 0.$$

Tant que x_i n'est pas nul, posons $\alpha_i = x_{i+1}/x_i$. On a au départ $\alpha_0 = x_1 = x_{-1} - q_0 x_0 = \alpha - q_0$ et ensuite

$$\alpha_i = \frac{1}{\alpha_{i-1}} - q_i, \qquad \alpha_{i-1} = \frac{1}{q_i + \alpha_i},$$

ce qui donne

$$\alpha = q_0 + \alpha_0 = q_0 + \frac{1}{q_1 + \alpha_1} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \alpha_2}} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots}}}$$

On appelle une telle expression « fraction continue »[3].

Notons les écritures matricielles

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha_0 \end{bmatrix},$$

et, pour $i \geqslant 1$,

$$\begin{bmatrix} 1 \\ \alpha_{i-1} \end{bmatrix} = \alpha_{i-1} \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha_i \end{bmatrix},$$

ce qui implique

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha_n \end{bmatrix},$$

ce qu'on peut aussi écrire

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_n + \alpha_n & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Utilisant le lemme 2.30, on obtient les deux formules

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} Q_{n+1}(q_0, \ldots, q_n) & Q_n(q_0, \ldots, q_{n-1}) \\ Q_n(q_1, \ldots, q_n) & Q_{n-1}(q_1, \ldots, q_{n-1}) \end{bmatrix} \begin{bmatrix} 1 \\ \alpha_n \end{bmatrix},$$

3. On devrait dire comme en anglais « fraction continuée ». La notion et la définition sont dues à Euler.

et

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} \mathrm{Q}_{n+1}(q_0, \ldots, q_n + \alpha_n) & \mathrm{Q}_n(q_0, \ldots, q_{n-1}) \\ \mathrm{Q}_n(q_1, \ldots, q_n + \alpha_n) & \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

On en déduit :

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} \mathrm{Q}_{n+1}(q_0, \ldots, q_n) + \alpha_n \mathrm{Q}_n(q_0, \ldots, q_{n-1}) \\ \mathrm{Q}_n(q_1, \ldots, q_n) + \alpha_n \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1}) \end{bmatrix},$$

et

$$\begin{bmatrix} \alpha \\ 1 \end{bmatrix} = \alpha_0 \cdots \alpha_{n-1} \begin{bmatrix} \mathrm{Q}_{n+1}(q_0, \ldots, q_n + \alpha_n) \\ \mathrm{Q}_n(q_1, \ldots, q_n + \alpha_n) \end{bmatrix}.$$

En définitive :

PROPOSITION 2.33. — *On a, pour tout entier $n \geqslant 0$,*

$$\alpha = \frac{\mathrm{Q}_{n+1}(q_0, \ldots, q_n) + \alpha_n \mathrm{Q}_n(q_0, \ldots, q_{n-1})}{\mathrm{Q}_n(q_1, \ldots, q_n) + \alpha_n \mathrm{Q}_{n-1}(q_1, \ldots, q_{n-1})} = \frac{\mathrm{Q}_{n+1}(q_0, \ldots, q_n + \alpha_n)}{\mathrm{Q}_n(q_1, \ldots, q_n + \alpha_n)}.$$

2.4.2. Réduites d'une fraction continue

Pour simplifier l'écriture, posons

$$u_i = \mathrm{Q}_{i+1}(q_0, \ldots, q_i), \qquad v_i = \mathrm{Q}_i(q_1, \ldots, q_i),$$

de sorte qu'on a par définition

$$u_{-1} = 1, \quad v_{-1} = 0, \quad u_0 = q_0, \quad v_0 = 1$$
$$u_n = q_n u_{n-1} + u_{n-2}, \quad v_n = q_n v_{n-1} + v_{n-2}.$$

Avec cette notation, la première égalité de la proposition précédente s'écrit

$$\alpha = \frac{u_n + \alpha_n u_{n-1}}{v_n + \alpha_n v_{n-1}}. \tag{2.1}$$

On appelle « réduites »[4] de la fraction continue précédente les expressions r_n obtenues en « négligeant les restes α_n », c'est-à-dire les

$$r_n = \frac{u_n}{v_n} = \frac{\mathrm{Q}_{n+1}(q_0, \ldots, q_n)}{\mathrm{Q}_n(q_1, \ldots, q_n)}.$$

On a par exemple :

$$\begin{aligned} r_0 &= q_0, \\ r_1 &= \frac{u_1}{v_1} = q_0 + \frac{1}{q_1} = \frac{1 + q_0 q_1}{q_1}, \\ r_2 &= \frac{u_2}{v_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = \frac{q_0 + q_0 q_1 q_2 + q_2}{1 + q_1 q_2}. \end{aligned}$$

4. En anglais, on dit « convergents ».

Notons que le déterminant de chacune des matrices 2×2 associées aux q_i est égal à -1. Cela implique $u_{n+1}v_n - u_n v_{n+1} = (-1)^n$, soit

$$r_{n+1} - r_n = \frac{(-1)^n}{v_n v_{n+1}}, \qquad n \geqslant 0. \tag{2.2}$$

On tire de là

$$\begin{aligned} r_{n+1} - r_{n-1} &= (r_{n+1} - r_n) + (r_n - r_{n-1}) \\ &= \frac{(-1)^n}{v_n v_{n+1}} + \frac{(-1)^{n-1}}{v_{n-1} v_n} = \frac{(-1)^{n+1}(v_{n+1} - v_{n-1})}{v_{n-1} v_n v_{n+1}}, \end{aligned}$$

et en définitive

$$r_{n+1} - r_{n-1} = (-1)^{n+1} \frac{q_{n+1}}{v_{n-1} v_{n+1}}, \qquad n \geqslant 1. \tag{2.3}$$

EXERCICE 2.24. [A] — On a

$$r_{n+1} = q_0 + \frac{1}{v_0 v_1} - \frac{1}{v_1 v_2} + \cdots + \frac{(-1)^n}{v_n v_{n+1}}$$

[*hint*]

Enfin, notons que la relation 2.1 peut aussi s'écrire

$$\alpha v_n - u_n = -\alpha_n(\alpha v_{n-1} - u_{n-1}). \tag{2.4}$$

Il s'ensuit que $\alpha v_n - u_n = (-1)^n \alpha_0 \cdots \alpha_n$, soit

$$\alpha - r_n = (-1)^n \frac{\alpha_0 \cdots \alpha_n}{v_n}, \qquad n \geqslant 0. \tag{2.5}$$

REMARQUE 2.34. — Tout ce qui précède est un calcul purement algébrique qu'on peut faire en prenant pour α et les q_i des variables indépendantes.

2.4.3. Réduites et approximations rationnelles

Particularisons maintenant ce qui précède au cas où $\mathrm{A} = \mathbf{R}$. Partons d'un $\alpha \in \mathbf{R}$. Posons

$$q_0 = \lfloor \alpha \rfloor, \quad \alpha_0 = \alpha - q_0$$

et définissons pour chaque entier $i > 0$ les q_i et les α_i par

$$q_{i+1} = \lfloor 1/\alpha_i \rfloor, \quad \alpha_{i+1} = 1/\alpha_i - q_{i+1},$$

tant que α_i n'est pas nul. Notons qu'on a $0 < \alpha_i < 1$ pour tout i, donc $1/\alpha_i > 1$ et les entiers q_i sont > 0.

Si α est un nombre rationnel, on retrouve une version de l'algorithme d'Euclide : il existe n avec $\alpha_n = 0$, et on obtient $\alpha = r_n$. Si α n'est pas

rationnel, l'algorithme ne s'arrête pas et on obtient un développement en fraction continue

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}}, \quad q_i \in \mathbf{N}, \quad q_i > 0. \tag{2.6}$$

En vertu de la relation 2.4, les $\alpha v_n - u_n$ sont de signes alternés et décroissent en valeur absolue. Les réduites $r_n = u_n/v_n$ convergent vers α en vertu de l'inégalité 2.5 et du fait que les v_n augmentent indéfiniment (c'est clair, ils croissent même exponentiellement ; voir aussi l'exercice 2.16).

EXERCICE 2.25. [B] — On choisit arbitrairement une suite $(q_i), i \geqslant 0$ de nombres réels avec $q_i \geqslant 1$ pour $i > 0$. Montrer que la suite des r_n converge vers un nombre réel α. [*hint*]

EXERCICE 2.26. [C] — Même question avec $q_i \geqslant \epsilon > 0$ pour $i > 0$. [*hint*]

EXERCICE 2.27. [B] — La suite des q_n et la suite des r_n se déterminent mutuellement. [*hint*]

EXERCICE 2.28. [C] — Les α tels que $q_0, \ldots, q_n$ soient égaux à des entiers fixés forment un intervalle (ouvert). [*hint*]

On tire des relations (2.5) et (2.3) les inégalités

$$r_0 < r_2 < \cdots < r_{2n} < \cdots < \alpha < \cdots < r_{2n+1} < \cdots < r_3 < r_1.$$

PROPOSITION 2.35. — *On a*

$$|r_n - \alpha| \leqslant \frac{1}{v_n v_{n+1}} < \frac{1}{q_{n+1} v_n^2}, \qquad n \geqslant 0.$$

Démonstration. On a en effet $|r_n - \alpha| \leqslant |r_{n+1} - r_n|$ et on applique (2.2). □

On a donc toujours $|r_n - \alpha| < \frac{1}{v_n^2}$. On a même $|r_n - \alpha| < \frac{1}{2v_n^2}$ dès que q_{n+1} est > 1. En fait, on a cette majoration pour au moins « une réduite sur deux » :

PROPOSITION 2.36. — *On ne peut avoir à la fois* $|r_n - \alpha| \geqslant \frac{1}{2v_n^2}$ *et* $|r_{n+1} - \alpha| \geqslant \frac{1}{2v_{n+1}^2}$.

Démonstration. En effet cela impliquerait

$$\frac{1}{v_n v_{n+1}} = |r_n - r_{n+1}| > \frac{1}{2v_n^2} + \frac{1}{2v_{n+1}^2},$$

ce qui est impossible, puisque s'écrivant aussi $(v_n - v_{n+1})^2 \leqslant 0$, donc $v_{n+1} = v_n$. □

REMARQUE 2.37. — On verra ci-dessous (corollaire 2.39) que si u et v sont deux entiers avec $v > 0$ et $\left|\frac{u}{v} - \alpha\right| < \frac{1}{2v^2}$, il existe n avec $u = u_n$ et $v = v_n$, donc $\frac{u}{v} = r_n$. On peut aussi prouver que, sur trois réduites successives, il y en a au moins une qui vérifie l'inégalité $|r_n - \alpha| < \frac{1}{\sqrt{5}v_n^2}$.

Si v est un entier > 0 quelconque, il existe $u \in \mathbf{Z}$ (d'ailleurs unique, on a supposé α irrationnel) avec $|u - \alpha v| < 1/2$, ce qu'on peut écrire aussi $\left|\frac{u}{v} - \alpha\right| < \frac{1}{2v}$. Pour un v quelconque, on ne peut a priori espérer mieux. Lorsque $v = v_n$ est le dénominateur d'une réduite de α, on vient de voir qu'on peut trouver $u = u_n$ avec $|u - \alpha v| < \frac{1}{v}$, ce qui est bien meilleur. Les réduites r_n sont en fait *les meilleures approximations rationnelles* de α : elles donnent les minimums successifs de la suite double $|u - \alpha v|$, ordonnée suivant les v croissants, comme le montre le résultat suivant.

PROPOSITION 2.38. — *Fixons $n > 1$ et soient u et v deux entiers, avec $0 < v < v_{n+1}$. On a alors*

$$|u - \alpha v| \geqslant |u_n - \alpha v_n|,$$

et l'égalité n'est atteinte que pour $u = u_n$ et $v = v_n$.

Démonstration. Il existe un entier $j \leqslant n$ avec $v_j \leqslant v < v_{j+1}$. Écrivons alors

$$\begin{bmatrix} v \\ u \end{bmatrix} = \begin{bmatrix} v_{j+1} & v_j \\ u_{j+1} & u_j \end{bmatrix} \begin{bmatrix} b \\ a \end{bmatrix}$$

avec a et b entiers, ce qui est toujours possible puisque la matrice écrite est de déterminant ± 1. On a en particulier $v = v_{j+1}b + v_j a$, ce qui implique nécessairement $ab \leqslant 0$ et $a \neq 0$. On a par ailleurs, en vertu de 2.4,

$$u - \alpha v = b(u_{j+1} - \alpha v_{j+1}) + a(u_j - \alpha v_j) = (-b\alpha_{j+1} + a)(u_j - \alpha v_j).$$

Puisque a et b sont de signes contraires avec $a \neq 0$, on a $\left|-b\alpha_{j+1} + a\right| = |b|\alpha_{j+1} + |a| \geqslant 1$, ce qui donne en définitive

$$|u - \alpha v| \geqslant (|b|\alpha_{j+1} + |a|)\left|u_j - \alpha v_j\right| \geqslant |u_n - \alpha v_n|.$$

Cela prouve l'inégalité annoncée. Pour qu'il y ait égalité, il faut qu'on ait à la fois $j = n$ et $|b|\alpha_{j+1} + |a| = 1$. Mais puisque $a \neq 0$, cela implique $b = 0$ et $a = \pm 1$, et en définitive $v = v_n$ et $u = u_n$. □

COROLLAIRE 2.39. — *Soit u et $v > 0$ deux entiers avec $|\alpha - u/v| < \frac{1}{2v^2}$. Alors u/v est l'une des réduites de α.*

Démonstration. Il existe n avec $v_n \leqslant v < v_{n+1}$. D'après la proposition, on a

$$|u_n - \alpha v_n| \leqslant |u - \alpha v| < \tfrac{1}{2v} \leqslant \tfrac{1}{2v_n}.$$

Cela implique $|vu_n - \alpha v v_n| < 1/2$ et de même $|uv_n - \alpha v v_n| < 1/2$. L'inégalité triangulaire donne alors $|vu_n - uv_n| < 1$, donc $vu_n = uv_n$ et en définitive $u/v = u_n/v_n = r_n$. □

2.4.4. Exemples classiques

Résumons les résultats obtenus. Les réduites r_n sont les meilleures approximations rationnelles du nombre irrationnel α et l'on a

$$r_n < \alpha < r_n + \frac{1}{q_{n+1}v_n^2} \quad \text{pour } n \text{ pair},$$
$$r_n - \frac{1}{q_{n+1}v_n^2} < \alpha < r_n \quad \text{pour } n \text{ impair}.$$

Ainsi, une réduite sera d'autant plus proche de α que q_{n+1} sera plus grand. En termes imagés, pour avoir une excellente approximation, il faut « couper la fraction continue juste avant un grand quotient ».

EXERCICE 2.29. [B] — Une publication médicale annonce un traitement nouveau d'une maladie rare, efficace dans 29, 41 % des cas. Combien de malades ont fait l'objet de l'expérience ? [*hint*]

Le nombre d'or

Le premier cas est celui du nombre d'or $\phi = (\sqrt{5}+1)/2$. Il satisfait aux deux relations $\lfloor \phi \rfloor = 1$ et $1/(\phi-1) = \phi$. On obtient ainsi un développement en fraction continue dont tous les quotients sont égaux à 1 :

$$\phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+\cdots}}}.$$

Les réduites de ϕ sont les quotients successifs de nombres de Fibonacci :

$$r_0 = \frac{1}{1}, \quad r_1 = \frac{2}{1}, \ldots, \quad r_{n-1} = \frac{\mathrm{F}_{n+1}}{\mathrm{F}_n}$$

de sorte qu'on a

$$\left| \phi - \frac{\mathrm{F}_{n+1}}{\mathrm{F}_n} \right| < \frac{1}{\mathrm{F}_n \mathrm{F}_{n+1}}.$$

Approximations de π

Un exemple est historiquement bien connu, celui de $\pi = 3.1415926535\cdots$. Le développement en fraction continue de π est

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1+\cdots}}}}}$$

et ses réduites successives sont

$$r_0 = 3, r_1 = 22/7, r_2 = 333/106, r_3 = 355/113, \ldots$$

Cela donne les meilleures approximations rationnelles[5] successives de π :

$$\begin{aligned} \frac{22}{7} - \frac{1}{15\times 7^2} &< \pi < \frac{22}{7} \\ \frac{333}{106} &< \pi < \frac{333}{106} + \frac{1}{106^2} \\ \frac{355}{113} - \frac{1}{292\times 113^2} &< \pi < \frac{355}{113} \end{aligned}$$

Ainsi, $355/113$ est une remarquable approximation de π, non seulement parce que c'en est une réduite, mais en plus parce que le quotient suivant, $q_4 = 292$, est particulièrement élevé. Le même phénomène se produit pour $22/7$, à cause de $q_2 = 15$, mais pas pour $333/106$.

Calendriers

D'autres exemples viennent de l'astronomie. Notons respectivement A et L l'année tropique et la lunaison, exprimées en jours. On a

$$\mathrm{A} = 365,2421989\ldots, \qquad \mathrm{L} = 29,530588\ldots$$

a) Parmi les réduites de la lunaison, se trouve $6585/223$. En 223 lunaisons, il y a presque exactement 6585 jours, soit 18 ans et 11 jours (s'il y a 4 bissextiles parmi les 18 années — 10 jours s'il y en a 5). Cette durée est le *« saros »*. Au bout d'un saros, les phénomènes lunaires (phases de la lune, éclipses) se reproduisent périodiquement en première approximation ; il y a 42 éclipses de lune et 42 éclipses de soleil dans un saros.

b) Parmi les réduites du rapport L/A, il y a $19/235$; en 19 ans, il y a presque exactement 235 lunaisons. C'est le *« cycle de Meton »* qui sert de base au calcul de la date de Pâques dans le calendrier ecclésiastique grégorien.

c) Enfin, les premières réduites de l'année tropique sont

$$365 + \frac{1}{4}, \quad 365 + \frac{7}{29}, \quad 365 + \frac{8}{33}, \quad 365 + \frac{31}{128}.$$

La première est bien connue : c'est celle qui donne naissance à *l'année julienne* de $365,25$ jours (une année sur quatre est bissextile). Les autres ne semblent pas utilisées[6]. La durée de *l'année grégorienne*, soit $365 + 1/4 - 1/100 + 1/400 = 365 + 97/400$ (une année bissextile sur quatre, les années centenaires non bissextiles, sauf les quadricentenaires) n'est pas une réduite et est une mauvaise approximation. On a en effet

5. L'approximation $22/7$ figure chez Archimède, l'approximation $355/113$ chez Adrien Métius (1625). Les deux étaient connues des chinois au cinquième siècle.

6. Euler donne un développement en fraction continue de A, mais comme il utilise une autre valeur approchée, il obtient après $8/33$ la réduite $55/227$.

$$\frac{97}{100} = 0,2425, \qquad |97 - 400 \times 0,2421989\ldots| = 0,120\ldots$$

tandis que par exemple

$$\frac{31}{128} = 0,2421875, \qquad |31 - 128 \times 0,2421989\ldots| = 0,00146\ldots$$

Comme de plus, on a $31/128 = 1/4 - 1/128$, on voit qu'on obtiendrait un calendrier bien plus exact que le calendrier grégorien (qui, comme on le voit ci-dessus, dérive d'un jour en environ $400/0,12 = 10000/3$ années, soit moins de 3400 ans) en décidant simplement que les années multiples de 128 ne sont pas bissextiles (ce qui donnerait une dérive d'un jour en environ $128/0,00146$ années, soit plus de 87000 ans). C'est bien entendu ce que n'aurait pas manqué de faire Grégoire XIII si l'astronomie travaillait en numération binaire et non en numération décimale !

Gammes

D'autres exemples viennent enfin de l'harmonie. L'harmonie « naturelle » est basée sur les rapports 2 (octave), 3/2 (quinte) et 5/4 (tierce), donc sur les nombres $\gamma = \log(3/2) = 0,584962\ldots$ et $\theta = \log(5/4) = 0,321928\ldots$, tels que $2^\gamma = 3/2$ et $2^\theta = 5/4$. Comme γ et θ sont irrationnels, il est impossible d'en tirer une échelle discrète des sons. Les premières réduites de γ sont

$$1, \frac{1}{2}, \frac{3}{5}, \frac{7}{12}, \frac{24}{41}, \frac{31}{53}, \ldots$$

La réduite 7/12 donne la gamme tempérée. On peut obtenir des gammes discrètes plus proche de la gamme naturelle en divisant l'octave en 41 ou 53 degrés égaux. Le choix de 53 est meilleur en ce que 17/53 est une assez bonne approximation de θ : on a en effet $53\theta = 17,062\ldots$, tandis que $41\theta = 13,199\ldots$. Notons au passage que les premières réduites de θ sont

$$\frac{1}{3}, \frac{9}{28}, \frac{19}{59}, \ldots$$

et qu'on a

$$3\theta = 0,96\ldots, \quad 28\theta = 9,014\ldots, \quad 59\theta = 18,994\ldots.$$

§ 2.5. Fractions continues des irrationnelles quadratiques

Soit n un entier > 0 qui n'est pas un carré parfait. Nous nous proposons de prouver que le développement en fraction continue de $\sqrt{n}$ est périodique et de donner pour le calculer un algorithme *rationnel*, c'est-à-dire ne nécessitant pas de calculs sur des nombres réels.

Commençons par donner une variante de la construction des fractions continues, qui nous sera utile. Notons f l'application définie sur les nombres réels non entiers et à valeurs dans les nombres réels > 1 telle que

$$f(\alpha) = \frac{1}{\alpha - \lfloor \alpha \rfloor}.$$

On a donc $\alpha = \lfloor \alpha \rfloor + 1/f(\alpha)$. Itérant tant qu'il est possible, on obtient

$$\alpha = \lfloor \alpha \rfloor + \frac{1}{\lfloor f(\alpha) \rfloor + \frac{1}{\lfloor f(f(\alpha)) \rfloor + \cdots}}.$$

Le raccord avec les notations antérieures se fait par les relations

$$q_i = \lfloor f^i(\alpha) \rfloor, \quad \alpha_i = 1/f^{i+1}(\alpha).$$

Nous allons démontrer notamment que pour $\alpha = \sqrt{n}$, il existe $\mathrm{N} > 0$ tel que $f^{\mathrm{N}+1}(\alpha) = f(\alpha)$, donc que la suite des q_i, pour $i > 0$, est périodique de période N. Par exemple, pour $n = 2$, on a $f(\sqrt{2}) = 1/(\sqrt{2}-1) = \sqrt{2}+1$ et $f(\sqrt{2}+1) = 1/(\sqrt{2}-1) = \sqrt{2}+1$, ce qui donne $q_0 = 1$ et $q_i = 2$ pour $i > 0$.

On fixe dans la suite l'entier n et on note q_0 sa racine carrée entière par défaut :

$$q_0 = \lfloor \sqrt{n} \rfloor > 0,$$

de sorte qu'on a $q_0^2 < n \leqslant q_0^2 + 2q_0$.

2.5.1. Un calcul préliminaire

Nous allons considérer des matrices à coefficients entiers de la forme

$$\mathrm{M} = \begin{bmatrix} -e & c \\ c & d \end{bmatrix}.$$

Nous dirons que M est *spéciale* ou que le triplet d'entiers (c, d, e) est *spécial* si l'on a

$$c^2 + de = n, \quad 0 \leqslant q_0 - c < d \leqslant q_0 + c.$$

Les inégalités ci-dessus impliquent $c > 0$, $d > 0$ et $c \leqslant q_0$.

Exercice 2.30. [A] — Le triplet $(q_0, 1, n - q_0^2)$ est spécial. [*hint*]

Exercice 2.31. [B] — Supposons $d > 0$ et $0 \leqslant c \leqslant q_0$. Alors l'inégalité $q_0 - c < d$ équivaut à $e \leqslant q_0 + c$ et l'inégalité $d \leqslant q_0 + c$ équivaut à $q_0 - c < e$. Ainsi, (c, d, e) est spécial si et seulement si (c, e, d) est spécial. [*hint*]

On notera que, n étant fixé, il n'existe qu'un nombre fini de triplet spéciaux : pour chaque c compris entre 1 et q_0, d doit être un diviseur de $n - c^2$ et e est alors déterminé.

Puisque $c^2 \leqslant q_0^2 < n$, on a $de > 0$, donc $e > 0$. Par ailleurs, on a $(\sqrt{n}+c)(\sqrt{n}-c) = de$, posons

$$\alpha = \frac{\sqrt{n}+c}{e} = \frac{d}{\sqrt{n}-c}.$$

On dira qu'un nombre réel α est *spécial* s'il peut s'écrire sous la forme précédente pour un triplet spécial (c,d,e). On notera que ce triplet est alors uniquement déterminé : si $(\sqrt{n}+c)/e = (\sqrt{n}+c')/e'$, on a $(e'-e)\sqrt{n} = ec' - ce'$ donc $e = e'$, puisque $\sqrt{n}$ est supposé irrationnel. On en déduit $c = c'$, puis $de = n - c^2 = d'e$, donc $d = d'$. On dira que α est associé à la matrice M. Les nombres spéciaux sont en nombre fini.

> EXERCICE 2.32. [A] — (suite de l'exercice 2.31) Si α est spécial, alors $\overline{\alpha} = e\alpha/d$ est spécial. [*hint*]

LEMME 2.40. — *a*) *Si α est spécial, associé à la matrice* M, *on a* $1 \leqslant \lfloor\alpha\rfloor \leqslant 2q_0$. *Si* $\lfloor\alpha\rfloor = 2q_0$, *alors* $\alpha = \sqrt{n} + q_0$.

b) *Si α est spécial, associé à la matrice* M, *alors $f(\alpha)$ est spécial, associé à la matrice*

$$\mathrm{M}' = -\begin{bmatrix} \lfloor\alpha\rfloor & 1 \\ 1 & 0 \end{bmatrix} \mathrm{M} \begin{bmatrix} \lfloor\alpha\rfloor & 1 \\ 1 & 0 \end{bmatrix}.$$

c) *Si α et β sont spéciaux et si $f(\alpha) = f(\beta)$, alors $\alpha = \beta$.*

Démonstration. Posons

$$q = \lfloor\alpha\rfloor = \lfloor\frac{q_0+c}{e}\rfloor.$$

On a par hypothèse $d \geqslant q_0 - c$, donc $d \geqslant \sqrt{n} - c$. Puisque $de = (\sqrt{n}-c)(\sqrt{n}+c) > 0$, il en résulte $0 < e \leqslant \sqrt{n}+c$, donc $0 < e \leqslant q_0 + c$. Le nombre rationnel $\frac{q_0+c}{e}$ est donc $\geqslant 1$ et, puisqu'on a $c \leqslant q_0$ et $e \geqslant 1$, il est $\leqslant 2q_0$. Sa partie entière q est donc comprise entre 1 et $2q_0$. Pour qu'on ait $q = 2q_0$, il faut qu'on ait à la fois $c = q_0$ et $e = 1$. Cela démontre a).

Par ailleurs, $f(\alpha) = 1/(\alpha - q) = 1/((\sqrt{n}+c-qe)/e)$, soit $f(\alpha) = \frac{e}{\sqrt{n}-c'}$, avec $c' = qe - c$. Comme $(\sqrt{n}+c')(\sqrt{n}-c') = n - c'^2 = n - c^2 + 2qce - q^2e^2 = de + 2qce - q^2e^2$, on obtient en définitive

$$f(\alpha) = \frac{\sqrt{n}+c'}{g} = \frac{e}{\sqrt{n}-c'}$$

avec $c' = qe - c$ et $g = d + 2qc - q^2e$. Un calcul immédiat donne

$$\begin{bmatrix} q & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -e & c \\ c & d \end{bmatrix}\begin{bmatrix} q & 1 \\ 1 & 0 \end{bmatrix} = -\begin{bmatrix} -g & c' \\ c' & e \end{bmatrix},$$

Par construction, on a $q \leqslant (q_0+c)/e < q+1$, ce qui s'écrit $qe \leqslant q_0 + c < qe + e$, ou encore $0 \leqslant q_0 - c' \leqslant e$. Par ailleurs, puisqu'on a $q \geqslant 1$, on a $e \leqslant qe = c + c' \leqslant q_0 + c'$. Ainsi, le triplet (c', e, g) est spécial et on a démontré b).

Pour prouver c), il faut montrer que connaissant (c', e, g), on peut déterminer (c, d, e). Il suffit évidemment de déterminer c. On doit avoir $d \leqslant q_0 + c$ et $c = qe - c'$ pour un certain q. Mais la relation $d \leqslant q_0 + c$ équivaut à $d < \sqrt{n} + c$, donc à $e > \sqrt{n} - c$, donc à $e > q_0 - c$ et enfin à $c > q_0 - e$. Ainsi, on doit avoir $q_0 - e < c \leqslant q_0$, ce qui s'écrit aussi $q_0 - c' - e < qe \leqslant q_0 - c'$. Cela détermine q comme la partie entière par excès de $(q_0 - c')/e$ et achève la démonstration. □

EXERCICE 2.33. [B] — Posons $\alpha = \sqrt{n} + q_0$. Alors, avec les notations de l'exercice 2.31, on a $\overline{\alpha} = 1/(\sqrt{n} - q_0)$ et $f(\overline{\alpha}) = \alpha$. [*hint*]

EXERCICE 2.34. [C] — Soient α et β deux nombres spéciaux. Avec les notations de l'exercice 2.31, si $f(\alpha) = \overline{\lambda}$, alors $f(\beta) = \overline{\alpha}$ et $\lfloor \alpha \rfloor = \lfloor \lambda \rfloor$. [*hint*]

2.5.2. L'énoncé

PROPOSITION 2.41. — *Si α est spécial, le développement en fraction continue de α est périodique : il existe un entier* $\mathrm{N} > 0$ *avec* $f^{\mathrm{N}}(\alpha) = \alpha$. *De plus, pour tout quotient q de ce développement, on a* $1 \leqslant q \leqslant 2q_0$.

Démonstration. D'après les parties a) et b) du lemme 2.40 précédent, tous les $f^i(\alpha)$ sont spéciaux et de partie entière comprise entre 1 et $2q_0$. Comme les nombres spéciaux sont en nombre fini, il existe deux entiers i et N avec $f^{i+\mathrm{N}}(\alpha) = f^i(\alpha)$. Mais, d'après la partie c) du lemme, cela implique $f^{\mathrm{N}}(\alpha) = \alpha$. □

COROLLAIRE 2.42. — *Soient $q_0, q_1, \ldots$ les quotients du développement en fraction continue de $\sqrt{n}$. Alors la suite des q_i, pour $i > 0$, est périodique. Plus précisément, il existe un entier* $\mathrm{N} > 0$ *tel qu'on ait* $q_i < 2q_0$ *pour* $0 \leqslant i < \mathrm{N}$, $q_{\mathrm{N}} = 2q_0$ *et* $q_{i+\mathrm{N}} = q_i$ *pour* $i > 0$.

En d'autres termes, la suite des quotients est de la forme

$$q_0, q_1, q_2, \ldots, 2q_0, q_1, q_2, \ldots, 2q_0, \ldots$$

où tous les q_i sont $< 2q_0$ sauf ceux pour lesquels i est multiple de N.

Démonstration. Posons $\alpha = \sqrt{n} + q_0$. Alors α est spécial, car il correspond au triplet spécial $(c, d, e) = (q_0, 1, n - q_0^2)$. Le développement en fraction continue de α est donc périodique. Mais ses quotients sont $2q_0, q_1, q_2, \ldots$ De plus, la condition $q_i = 2q_0$ équivaut d'après le lemme 2.40, a), à $f^i(\alpha) = \sqrt{n} + q_0 = \alpha$, donc au fait que i soit une période. □

On appellera N la *période* du développement de $\sqrt{n}$.

On peut prouver que la partie régulière du développement est « palindromique », c'est-à-dire que l'on a $q_{\mathrm{N}-i} = q_i$ pour $0 < i < \mathrm{N}$.

EXERCICE 2.35. [C] — Démontrer cette assertion, à l'aide des exercices 2.33 et 2.34. [*hint*]

2.5.3. L'algorithme

Si l'on applique récursivement le lemme 2.40, on obtient l'algorithme suivant de calcul du développement de $\sqrt{n}$.

Partant de

$$d_{-1} = n, \quad c_{-1} = 0, \quad d_0 = 1,$$

on construit par récurrence pour tout entier $i \geqslant 0$ (on a toujours $d_i > 0$, ce qui justifie l'introduction de q_i) les entiers

$$q_{i+1} = \lfloor \frac{q_0 + c_i}{d_{i+1}} \rfloor, \quad c_i = q_i d_i - c_{i-1}, \quad d_{i+1} = d_{i-1} + 2c_{i-1}q_i - d_i q_i^2.$$

La construction des c_i des d_i équivaut à la définition matricielle :

$$\begin{bmatrix} -d_{i+1} & c_i \\ c_i & d_i \end{bmatrix} = -\begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -d_i & c_{i-1} \\ c_{i-1} & d_{i-1} \end{bmatrix}\begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.7}$$

Alors les q_i sont les quotients successifs du développement en fraction continue de $\sqrt{n}$. Plus précisément, si l'on pose $\alpha_0 = \sqrt{n} - q_0$ et $\alpha_i = \frac{1}{\alpha_{i-1}} - q_i$ pour $i > 0$, on a pour tout $i \geqslant 0$, $q_i = \lfloor 1/\alpha_{i-1} \rfloor$ et

$$0 < \alpha_i = \frac{\sqrt{n} - c_i}{d_i} = \frac{d_{i+1}}{\sqrt{n} + c_i} < 1. \tag{2.8}$$

Ainsi, à chaque pas, on obtient $(\alpha_i)^{-1}$ sous la forme $\frac{\sqrt{n}+c}{d}$; pour en prendre la partie entière, on remplace d'abord $\sqrt{n}$ par sa partie entière q_0 et on prend la partie entière q_{i+1} de la fraction ainsi trouvée ; on pose alors $\alpha_{i+1} = (\alpha_i)^{-1} - q_{i+1}$.

On s'arrête lorsqu'on trouve un N tel que $\alpha_N = \alpha_0$, c'est-à-dire $c_N = q_0$ et $d_N = 1$. On verra d'ailleurs ci-dessous (proposition 2.44) que la condition $d_N = 1$ a elle seule implique $\alpha_N = \alpha_0$. On trouve automatiquement $q_N = 2q_0$ d'après ce qui précède.

Traitons comme exemple le cas $n = 13$. Le calcul procède comme suit :

$i = 0$	$\alpha = \sqrt{13}$	$q_0 = 3$	$\alpha_0 = \sqrt{13} - 3$
$i = 1$	$\frac{1}{\alpha_0} = \frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4}$	$q_1 = \lfloor 3 + \frac{3}{4} \rfloor = 1$	$\alpha_1 = \frac{\sqrt{13}-1}{4}$
$i = 2$	$\frac{1}{\alpha_1} = \frac{4}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{3}$	$q_2 = \lfloor \frac{4}{3} \rfloor = 1$	$\alpha_2 = \frac{\sqrt{13}-2}{3}$
$i = 3$	$\frac{1}{\alpha_2} = \frac{3}{\sqrt{13}-2} = \frac{\sqrt{13}+2}{3}$	$q_3 = \lfloor \frac{5}{3} \rfloor = 1$	$\alpha_3 = \frac{\sqrt{13}-1}{3}$
$i = 4$	$\frac{1}{\alpha_3} = \frac{3}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{4}$	$q_4 = \lfloor \frac{4}{4} \rfloor = 1$	$\alpha_4 = \frac{\sqrt{13}-3}{3}$
$i = 5$	$\frac{1}{\alpha_4} = \frac{4}{\sqrt{13}-3} = \sqrt{13} + 3$	$q_5 = \lfloor 3 + 3 \rfloor = 6$	$\alpha_5 = \sqrt{13} - 3 = \alpha_0$

On obtient ainsi la suite des quotients $(3, 1, 1, 1, 1, 6, 1, \ldots)$ et une pé-

riode N = 5. La réduite r_5 vaut $3 + 1/s$, où s est la quatrième réduite du nombre d'or, soit $s = F_5/F_4 = 5/3$. On a donc $r_5 = 18/5$.

EXERCICE 2.36. [B] — Soit a un entier > 0. Calculer les développements en fraction continue de $\sqrt{a^2+1}$ et $\sqrt{a^2+2}$. Application à $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$ et $\sqrt{6}$. [*hint*]

EXERCICE 2.37. [N] — Écrire dans le langage de votre choix un algorithme calculant le développement en fraction continue de $\sqrt{n}$ et ses réduites. On effectuera sur les expressions de la forme $\frac{\sqrt{n}+c}{d}$ avec c, d entiers des calculs *exacts* comme dans l'algorithme expliqué ci-dessus, et non des calculs approchés. On utilisera la périodicité pour les réduites d'indice $>$ N. [*hint*]

2.5.4. L'équation de Pell-Fermat

On appelle *équation de Pell-Fermat* l'équation

$$x^2 - ny^2 = \pm 1, \tag{2.9}$$

dont on s'intéresse aux solutions entières. On écarte les solutions triviales $x = \pm 1$, $y = 0$. Par ailleurs, on peut changer de signe x et y indépendamment, et il suffit de considérer les cas où x et y sont > 0.

Nous allons voir que le développement en fraction continue de $\sqrt{n}$ permet de construire toutes les solutions.

Notons $\frac{u_i}{v_i}$ les réduites successives de $\sqrt{n}$, de sorte que

$$\begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} u_i & u_{i-1} \\ v_i & v_{i-1} \end{bmatrix},$$

. On a par construction (voir la formule 2.8

$$(-1)^{i+1} \begin{bmatrix} -d_{i+1} & c_i \\ c_i & d_i \end{bmatrix} = \begin{bmatrix} u_i & v_i \\ u_{i-1} & v_{i-1} \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & n \end{bmatrix} \begin{bmatrix} u_i & u_{i-1} \\ v_i & v_{i-1} \end{bmatrix},$$

ce qui donne en particulier :

$$u_i^2 - nv_i^2 = (-1)^{i+1} d_{i+1}. \tag{2.10}$$

Nous allons démontrer le théorème suivant :

THÉORÉME 2.43. — *Soit* N *la période du développement de* $\sqrt{n}$.

a) Pour tout couple d'entiers (x, y) *solution de* 2.9 *avec* $y \neq 0$, *il existe un entier* $k > 0$ *tel que* $x = \pm u_{k\mathrm{N}-1}$, $y = \pm v_{k\mathrm{N}-1}$.

b) Pour tout entier $k > 0$, *on a*

$$u_{k\mathrm{N}-1}^2 - nv_{k\mathrm{N}-1}^2 = (-1)^{k\mathrm{N}}.$$

c) Pour tout entier $k > 0$, *on a*

$$u_{k\mathrm{N}-1} - v_{k\mathrm{N}-1}\sqrt{n} = (u_{\mathrm{N}-1} - v_{\mathrm{N}-1}\sqrt{n})^k.$$

La partie b) du théorème résulte de la proposition plus précise suivante :

PROPOSITION 2.44. — *Soit i un entier > 0. Les conditions suivantes sont équivalentes :*

(i) $i+1$ est multiple de N,
(ii) on a $d_{i+1} = 1$,
(iii) on a $u_i^2 - nv_i^2 = (-1)^{i+1}$,
(iv) on a $u_i^2 - nv_i^2 = \pm 1$.

Démonstration. On a $u_i^2 - nv_i^2 = (-1)^{i+1} d_{i+1}$ d'après 2.10. Puisque d_{i+1} est > 0, les trois dernières conditions sont équivalentes. Si $i+1$ est multiple de N, on a, d'après 2.8

$$\frac{\sqrt{n} - c_{i+1}}{d_{i+1}} = \alpha_{i+1} = \alpha_0 = \sqrt{n} - q_0,$$

et cela implique $d_{i+1} = 1$. Inversement, si $d_{i+1} = 1$, toujours d'après 2.8, on a $\alpha_i = 1/(\sqrt{n} + c_i)$, donc

$$\alpha_{i+1} = \frac{1}{\alpha_i} - \lfloor \frac{1}{\alpha_i} \rfloor = (\sqrt{n} + c_i) - (q_0 + c_i) = \sqrt{n} - q_0 = \alpha_0,$$

et $i+1$ est multiple de N. □

Démontrons maintenant la partie a) du théorème.

Démonstration. Soient x et y deux entiers > 0 tels que $x^2 - dy^2 = \pm 1$. On a d'abord $|x/y) - \sqrt{n}||x/y + \sqrt{n}| = 1/y^2$, de sorte qu'on a $|x/y - \sqrt{n}| \leqslant 1/2y^2$. D'après le corollaire 2.39, y/x est une réduite u_i/v_i de $\sqrt{n}$. Puisque x et y sont premiers entre eux, cela donne $x = u_i$ et $y = v_i$, ce qui implique $u_i^2 - nv_i^2 = \pm 1$. Alors $i+1$ est multiple de N d'après la proposition précédente. □

Pour démontrer la partie c), nous utiliserons le lemme suivant :

LEMME 2.45. — *Soient* A *une matrice carrée d'ordre* 2 *et $\lambda \in \mathbf{R}$ tels que*

$$\mathrm{A} \cdot \begin{bmatrix} 1 \\ \alpha_0 \end{bmatrix} = \lambda \begin{bmatrix} 1 \\ \alpha_0 \end{bmatrix}.$$

Posons

$$\begin{bmatrix} u' & u \\ v' & v \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \mathrm{A}.$$

Alors $u - v\sqrt{n} = \lambda \det(\mathrm{A})$.

Démonstration. Posons

$$\mathrm{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

La première relation donne $\lambda = a + b\alpha_0$ et $\lambda\alpha_0 = c + d\alpha_0$. Multipliant la première par d, la seconde par $-b$ et ajoutant, on obtient $\lambda(d - \alpha_0 b) = ad - bc = \det(\mathrm{A})$. D'un autre côté, on a $u = q_0 b + d$ et $v = b$, donc $u - v\sqrt{n} = d + v(q_0 - \sqrt{n}) = d - \alpha_0 b$. □

Passons à la démonstration de c) :

Démonstration. Considérons la matrice produit

$$\mathrm{M} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_{\mathrm{N}} & 1 \\ 1 & 0 \end{bmatrix}.$$

On a par définition de la période

$$\mathrm{M} \cdot \begin{bmatrix} 1 \\ \alpha_0 \end{bmatrix} = \lambda \begin{bmatrix} 1 \\ \alpha_0 \end{bmatrix}$$

avec $\lambda = (\alpha_0 \cdots \alpha_n)^{-1}$ et par ailleurs

$$\begin{bmatrix} u_{\mathrm{N}} & u_{\mathrm{N}-1} \\ v_{\mathrm{N}} & v_{\mathrm{N}-1} \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \mathrm{M}.$$

Le lemme précédent donne alors $u_{\mathrm{N}-1} - v_{\mathrm{N}-1}\sqrt{n} = (-1)^{\mathrm{N}}\lambda$. Mais, pour tout entier $k > 0$, on a par périodicité

$$\begin{bmatrix} u_{k\mathrm{N}} & u_{k\mathrm{N}-1} \\ v_{k\mathrm{N}} & v_{k\mathrm{N}-1} \end{bmatrix} = \begin{bmatrix} q_0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \mathrm{M}^k,$$

et par le même raisonnement $u_{k\mathrm{N}-1} - v_{k\mathrm{N}-1}\sqrt{n} = (-1)^{k\mathrm{N}}\lambda^k$. □

On a ainsi achevé la démonstration du théorème.

On voit donc que la connaissance de la réduite $u_{\mathrm{N}-1}/v_{\mathrm{N}-1}$ permet de calculer toutes les solutions : on prend un entier $k > 0$, on considère $u_{\mathrm{N}-1} - v_{\mathrm{N}-1}\sqrt{n}$, on l'élève à la puissance k-ième, on l'écrit sous la forme $a - b\sqrt{n}$, où a et b sont entiers, et on prend $x = \pm a$ et $y = \pm b$. Ce sera une solution de $x^2 - ny^2 = 1$ si k ou N est pair, et une solution de $x^2 - ny^2 = -1$ si k et N sont impairs.

Par exemple, pour $n = 13$, on a $\mathrm{N} = 5$, $r_4 = 18/5$ et $18^2 - 13 \cdot 5^2 = -1$ et les solutions sont données par $x = \pm a$ et $y = \pm b$, avec $a - b\sqrt{13} = (18 - 5\sqrt{13})^k$.

COROLLAIRE 2.46. — *L'équation de Pell-Fermat proprement dite $x^2 - ny^2 = 1$ a toujours des solutions non triviales. Soit (u, v) la plus petite des solutions avec $u > 0$ et $v > 0$. Pour chaque entier $r > 0$, écrivons*

$$(u - v\sqrt{n})^r = x_r - y_r\sqrt{n},$$

avec x_r et y_r entiers. Alors (x_r, y_r) parcourt toutes les solutions à composantes > 0.

Démonstration. Cela résulte directement du théorème : on a $(u, v) = (u_{\mathrm{N}-1}, v_{\mathrm{N}-1})$ si N est pair, $(u, v) = (u_{2\mathrm{N}-1}, v_{2\mathrm{N}-1})$ si N est impair. □

EXERCICE 2.38. [A] — L'équation $x^2 - ny^2 = -1$ n'a de solutions que si N est impair. [*hint*]

EXERCICE 2.39. [B] — Supposons N impair. Décrire toutes les solutions de l'équation $x^2 - ny^2 = -1$. [*hint*]

Une remarque finale. Nous avons vu que les réduites étaient les meilleures approximations rationnelles de $\sqrt{n}$, et qu'une réduite r_i donnée était d'autant meilleure que le quotient suivant q_{i+1} était plus grand. Or, on vient de voir que les plus grands quotients sont justement les $q_{k\mathrm{N}} = 2q_0$ et que les réduites $u/v = r_{k\mathrm{N}-1}$ donnent à $\left|u^2 - nv^2\right|$ la valeur minimum, à savoir 1. D'ailleurs, si u/v est une telle réduite, on $(u - v\sqrt{n})(u + v\sqrt{n}) = \pm 1$, et $u > v\sqrt{n}$. On en tire

$$\left|\frac{u}{v} - \sqrt{n}\right| = \frac{1}{v(u + v\sqrt{n})} < \frac{1}{2\sqrt{n}v^2} < \frac{1}{2q_0v^2},$$

ce qui correspond exactement à l'inégalité de la proposition 2.35.

Solutions des exercices

1.1. — Si un nombre premier divise un produit, il divise l'un des facteurs. [*retour*]

1.2. — On a $b^n \equiv (-1)^n \ [\mathtt{mod}\ b+1]$. Considérer la somme alternée des chiffres de n. [*retour*]

1.3. — On a $1 \neq 0$, donc $1+1 \neq 1$. [*retour*]

1.4. — On multiple la relation par $x+y$, et on raisonne par récurrence sur n. [*retour*]

1.5. — Les multiples $n.1_A$ pour $n \in \mathbf{Z}$. [*retour*]

1.6. — Tout sous-anneau contient 1, donc tous ses multiples entiers. [*retour*]

1.7. — Dire que h_a est injective, c'est dire que a n'est pas diviseur de zéro. Dire que h_a est surjective, ou bijective, c'est dire que a est inversible. [*retour*]

1.8. — Si on met dans S un diviseur de zéro s avec $st = 0$, alors on a $s/1 = 0/t$ et $0/t = 0/1$, donc la relation proposée n'est pas une relation d'équivalence. De toute façon, on ne peut pas plonger A dans un anneau K où s devient inversible, vu la relation $st = 0$. [*retour*]

1.9. — S est formée des couples (m,n) où m *et* n sont non nuls, et on obtient $K = \mathbf{Q} \times \mathbf{Q}$. Plus généralement, la construction proposée est « compatible avec les produits ». [*retour*]

1.10. — $b/a = d/1$. [*retour*]

1.11. — De (i), on déduit que $x \equiv y$ est équivalent à $x - y \in \mathfrak{a}$, où $\mathfrak{a}$ est l'ensemble des éléments équivalents à 0. Pour passer de (ii) à (i), on note que $xy - x'y' = x(y-y') + y'(x-x')$. [*retour*]

1.12. — $\{0\}$ et A sont des idéaux. Si un idéal contient 1, il contient $a = a.1$. [*retour*]

1.13. — Lorsque $m' = am$, avec a inversible. [*retour*]

1.14. — Si $x^n \in \mathfrak{a}$ et $y^m \in \mathfrak{a}$, on a $(x+y)^{n+m-1} \in \mathfrak{a}$ d'après la formule du binôme. [*retour*]

1.15. — La première assertion est un cas particulier de l'exercice précédent. Si x^n est nilpotent, x l'est. [*retour*]

1.16. — On a $xe = x$ pour tout $x \in Ae$. [*retour*]

1.17. — On pourra noter que le produit triple $\mathfrak{a}\mathfrak{b}\mathfrak{c}$ est formé des sommes finies de produits xyz avec $x \in \mathfrak{a}$, $y \in \mathfrak{b}$, $z \in \mathfrak{c}$. [retour]

1.18. — Utiliser la relation $4xy = (x+y)^2 - (x-y)^2$. [retour]

1.19. — Voici un exemple ad-hoc. On prend $A = (\mathbf{Z}/2\mathbf{Z})[X, Y]$ et on considère l'idéal formé des polynômes sans terme constant. [retour]

1.20. — Pour la première partie, on remarque que si u divise m, alors $N(u)$ divise $N(m)$ et on détermine explicitement toutes les solutions de $N(u) \leqslant 9$. Pour la seconde, déterminons par exemple l'idéal $\mathfrak{a}\mathfrak{b}$. C'est le plus petit idéal contenant les quatre éléments

$$x = 3(1+\alpha),\ y = 3(1-\alpha),\ z = (1+\alpha)(2-\alpha),\ t = (1-\alpha)(2-\alpha).$$

Mais $z = 7+\alpha$, donc $1+\alpha = z-x-y$ appartient à $\mathfrak{a}\mathfrak{b}$. Inversement, x, y, z et t appartiennent à $(1+\alpha)$: c'est clair pour x et pour z, et c'est aussi vrai pour $y = 6-z$, puisque $6 = (1+\alpha)(1-\alpha)$; enfin, on a $t = -3-3\alpha = -x$. [retour]

1.21. — La seule difficulté apparente concerne les produits ; mais il ne faut pas oublier que le produit de deux idéaux n'est pas l'ensemble des produits d'éléments, mais l'ensemble des sommes de produits d'éléments. [retour]

1.22. — Élever l'identité donnée à la puissance n. [retour]

1.23. — On a $\mathfrak{a}+\mathfrak{b} = Ax_1 + \cdots + Ay_m$, $\mathfrak{a}\mathfrak{b} = Ax_1y_1 + \cdots + Ax_ny_m$ avec tous les mn produits, donc $\mathfrak{a}^2 = Ax_1^2 + \cdots Ax_{n-1}x_n$, avec les n carrés et les $n(n-1)/2$ doubles produits. Il n'y a pas de description simple de l'intersection : comment savoir par exemple si $\mathfrak{a} = \mathfrak{b}$? [retour]

1.24. — Utiliser par exemple la proposition 1.4 ci-dessus. [retour]

1.25. — La condition proposée signifie que tout élément est un multiple entier de l'élément unité, c'est-à-dire que l'application $n \mapsto n.1_A$ est surjective, donc identifie A à un anneau-quotient de $\mathbf{Z}$ (voir ci-dessous). [retour]

1.26. — $f(a) = 0$ implique $f(xa) = f(x)f(a) = 0$. [retour]

1.27. — Considérer le premier coefficient non entier de Q. [retour]

1.28. — La relation $x - y \in \mathfrak{a}$ implique $x - y \in \mathfrak{b}$. [retour]

1.29. — Les parties de $A/\mathfrak{a}$ correspondent par image réciproque aux parties de A qui sont réunions de classes d'équivalence. Les idéaux ont comme image réciproque des idéaux. Il est équivalent de dire qu'un idéal de A est réunion de classes modulo $\mathfrak{a}$ ou qu'il contient $\mathfrak{a}$. [retour]

1.30. — On a $A/(0) = A$. [retour]

1.31. — On a $A/(0) = A$. [retour]

1.32. — Pour $a > 2$, $a^n - 1$ est divisible par $a - 1$. Par ailleurs $a^{mm'} - 1$ est divisible par $a^m - 1$. Si a est impair, $a^n + 1$ est pair ! Si m est impair, $a^{mm'} + 1$ est divisible par $a^{m'} + 1$. [*retour*]

1.33. — Evident. [*retour*]

1.34. — L'application qui associe à un polynôme son terme constant est un homomorphisme surjectif d'anneaux de noyau $\mathfrak{m}$. Par ailleurs, on a $\mathfrak{m}^r = (\mathrm{X}^r)$. [*retour*]

1.35. — Calculer le terme de degré $\deg(\mathrm{P}) + \deg(\mathrm{Q})$ de PQ. [*retour*]

1.36. — Il faut et il suffit que a soit nilpotent. Si $a^n = 0$, alors $1 + a\mathrm{T} + \cdots + a^{n-1}\mathrm{T}^{n-1}$ convient. Inversement, on écrit l'inverse sous la forme $b_0 + \cdots + b_{n-1}\mathrm{T}^{n-1}$, et on prouve que $a^n = 0$. [*retour*]

1.37. — Posons $\mathrm{P} = a_0 + \cdots + a_n\mathrm{X}^n$ et notons b_m le coefficient dominant de Q. On remarque d'abord que, si un scalaire c est tel que $cb_m = 0$, on doit avoir $c\mathrm{Q} = 0$, puisque $(c\mathrm{Q})\mathrm{P} = 0$ et $\deg(c\mathrm{Q}) < \deg(\mathrm{Q})$. Puisque $a_n b_m = 0$, il en résulte que $a_n\mathrm{Q} = 0$. Considérant alors le terme de degré $n + m - 1$ de PQ, on voit que $a_{n-1}b_m = 0$, et on continue ainsi. En définitive, chaque a_i annule Q, donc tout coefficient de Q annule P. [*retour*]

1.38. — Cela implique en effet $h(\mathrm{P}) = \mathrm{P}(a)$. [*retour*]

1.39. — Soit f un tel homomorphisme, on pose $a = f(\mathrm{X})$. [*retour*]

1.40. — $\mathrm{R} = \mathrm{U}(a)$; en dérivant, on obtient $\mathrm{Q}(a) = \mathrm{U}'(a)$. [*retour*]

1.41. — $a' = a + 2c$ et $b' = b - ac - c^2$. [*retour*]

1.42. — C'est l'idéal annulateur de a, formé des $\alpha \in \mathrm{A}$ avec $\alpha a = 0$. [*retour*]

1.43. — Remplacer la deuxième règle par $(\mathrm{Q}, \mathrm{R}, \mathrm{V}) \mapsto (c\mathrm{Q} + \mathrm{A}, c\mathrm{R} - \mathrm{A}, \mathrm{V})$ avec $\mathrm{A} = \mathtt{dom}(\mathrm{R})\mathrm{X}^{\deg(\mathrm{R})-\deg(\mathrm{V})}$. [*retour*]

1.44. — Définir des dérivées divisées $\mathrm{D}^{(r)}$ par $\mathrm{D}^{(r)}(\mathrm{X}^s) = \binom{}{r}\mathrm{X}^{s-r}$, de sorte que la dérivée r-ième usuelle est $r!\mathrm{D}^{(r)}$. Alors l'ordre de a comme racine du polynôme P est le plus petit entier r tel que $(\mathrm{D}^{(r)}\mathrm{P})(a) \neq 0$. Notons au passage la « formule de Taylor »

$$\mathrm{P}(a + \mathrm{X}) = \sum_{r=0}^{\deg(\mathrm{P})} \mathrm{D}^{(r)}(a)\mathrm{X}^r.$$

[*retour*]

1.45. — Il faut « répéter chaque racine autant de fois que sa multiplicité ». [*retour*]

1.46. — Pour chaque i soit $L_i(X)$ le produit des $(X - a_j)/(a_i - a_j)$, étendu aux $j \neq i$. Alors $L_i(a_j) = 0$ pour $j \neq i$ et $L_i(a_i) = 1$. On pose $P = \sum P(a_i)L_i$. [retour]

1.47. — On fixe le développement limité de P à l'ordre r_i en chaque a_i et on cherche P de degré $\sum r_i$. [retour]

1.48. — Il existe deux solutions, que l'on obtient en tronquant à droite les deux suites infinies $\cdots 90625$ et $\cdots 09376$. La première s'obtient en calculant 5^{2^n} modulo 10^n, ce qui donne la suite 5 mod 10, 25 mod 100, 625 mod 1000, etc. La seconde s'obtient par « complément à 1 ». Appliquer la méthode de Newton à partir de 5 mod 10 et 6 mod 10. [retour]

1.49. — Si $f(a) = f'(a)^2 u$ avec $u \in I$, et si on pose $x = -f'(a)u \in f'(a)I$, on a $f(a + x) \in f'(a)^2 I^2 = f'(a + x)^2 I^2$. Recommençant, on trouve au bout de n pas un a_n avec $a_n - a \in f'(a)I$ et $f(a_n) \in f'(a)^2 I^{n+1}$. [retour]

1.50. — On a $u^2 - su + p = 0$, donc $uv = us - u^2 = p$. Inversement, des relations $U + V = s$ et $UV = p$ vraies dans l'anneau-quotient proposé (on note suivant l'usage la classe de U par U et de même pour V), on déduit $U^2 - sU + p = 0$ et $V = U - s$. On tire de là un homomorphisme de cet anneau dans B, qui applique U sur u et V sur v, et on vérifie que c'est un isomorphisme, son inverse étant évident. [retour]

1.51. — On associe à chaque polynôme de l'anneau de départ la fonction qu'il définit sur $\mathbf{F}_2^n$. C'est un homomorphisme d'anneaux, qui s'annule sur l'idéal proposé. Par ailleurs, les produits des 2^n parties de $\{X_1, \ldots, X_n\}$ forment une base de l'espace vectoriel quotient, et leurs images forment une base de l'espace des fonctions. [retour]

1.52. — On envoie B dans l'anneau proposé en posant $a = x + y$ et $X = x$. L'application réciproque envoie x sur X et y sur $a - X$. En partant de l'identité $(x^n + y^n)(x + y) = x^{n+1} + y^{n+1} + xy(x^{n-1} + y^{n-1})$, on obtient une relation de récurrence pour les W_n. Ceux-ci sont d'ailleurs symétriques et peuvent donc se mettre sous la forme $Z_n(x + y, xy)$. On obtient de même une relation de récurrence pour les Z_n à savoir

$$Z_{n+1}(s, p) = sZ_n(s, p) - pZ_{n-1}(s, p) - V_{n-1}(s).$$

[retour]

1.53. — Même méthode que ci-dessus. [retour]

1.55. — L'image est un sous-anneau. [retour]

2.1. — Si $p = xy$ et si p divise x, alors $(x/p).y = 1$. [retour]

2.2. — Pour $r = 1$, alors m et d sont associés à x. Pour $r = 0$, alors m est inversible et $d = 0$. Si $x_i = 0$, alors $m = 0$. Si $x_i = 1$, alors d est inversible. [*retour*]

2.3. — D'abord, am est un multiple de chacun des ax_i. Réciproquement, tout multiple commun des ax_i est un multiple de a (si la famille est vide, le résultat est clair), donc s'écrit az, et z est un multiple commun des x_i, donc un multiple de m. [*retour*]

2.4. — Puisque d divise x et y, alors $xy/d = x.(y/d) = y.(x/d)$ est un multiple de x et de y. Inversement, soit m un multiple commun de x et y. On a $m = ax$, avec $a \in$ A. Mais y divise alors ax et aussi évidemment ay, donc divise ad d'après l'hypothèse. Ainsi $ad = by$, avec $b \in$ A, ce qui donne $a = b.(y/d)$ et $m = b.(xy/d)$. [*retour*]

2.5. — Tout polynôme divisible par X et par Y est divisible par XY. Par ailleurs, tout élément P(X, Y) de (X) + (Y) est tel que P(0) = 0 (et réciproquement d'ailleurs) et ce n'est pas le cas de 1. [*retour*]

2.6. — 2 est extrémal, mais il divise le produit $(1 + \alpha)(1 - \alpha)$ sans diviser aucun d'entre eux. L'idéal $\mathfrak{a}$ par exemple, n'est pas principal. [*retour*]

2.7. — On démontre la nécessité à partir de la proposition 2.15 ; par ailleurs, la démonstration du théorème 2.19 montre que (a') implique la condition (a) de la définition 2.12. [*retour*]

2.8. — On remarque que (a") est une forme de (a') ; pour (b'), on utilise la proposition 2.11. [*retour*]

2.9. — Non, c'est en fait la même, car pour prouver que les polynômes sur un anneau intègre forment eux-mêmes un anneau intègre, on considère les termes de plus haut degré des deux polynômes qu'on multiplie. [*retour*]

2.10. — Notons d'abord que $\phi(\alpha + \beta\sqrt{d})$ ne peut être nul que si α et β sont nuls (sinon d serait un carré dans $\mathbf{Q}$, donc dans $\mathbf{Z}$). Puisque $u^{-1} = \pm\phi(u)^{-1}\overline{u}$ si $u \neq 0$. on voit que K est un corps. Introduisant un dénominateur commun aux nombres rationnels α et β, on voit que tout élément de K est le quotient d'un élément de A par un entier. Cela implique notamment que K est bien le corps des fractions de A. La relation (E) s'écrit aussi $a/b = q + r/b$ et on a $\phi(r/b) = \phi(r)/\phi(b)$. De là, on déduit l'équivalence de (E) et de la propriété annoncée. Pour tout $x \in$ K, on peut trouver $a \in$ A avec $x - a = \alpha + \beta\sqrt{d}$ tel que $|\alpha| \leqslant 1/2$ et $|\beta| \leqslant 1/2$, ce qui donne $\phi(x - a) =\leqslant 1/4(1 + |d|)$ pour $d < 0$ et $\phi(x - a) =\leqslant 1/4 \sup(1, d)$ pour $d > 0$. [*retour*]

2.11. — pgcd(x, y) est invariant, $\phi(x) + \phi(y)$ diminue. [*retour*]

2.12. — On peut par exemple calculer successivement $d_2 = \operatorname{pgcd}(a_1, a_2)$, puis $d_3 = \operatorname{pgcd}(d_2, a_3)$ et ainsi de suite jusqu'à $d = \operatorname{pgcd}(d_{n-1}, a_n)$. [retour]

2.13. — $\lfloor x + 1/2 \rfloor$ et $\lceil x - 1/2 \rceil$. [retour]

2.14. — La relation $\mathrm{E}(x + n) = \mathrm{E}(x) + n$ est claire. Ainsi, $\mathrm{E}(x) + n = 0$ équivaut à $\mathrm{E}(x + n) = 0$. Si E est croissante, I doit contenir tous les points intermédiaires entre deux points quelconques qu'il contient, donc être un intervalle. Pour que $\mathbf{R}$ soit réunion disjointe de ses translatés, I doit être de la forme $]\alpha - 1, \alpha]$ ou $[-\alpha, 1 - \alpha[$, avec $0 \leqslant \alpha < 1$. [retour]

2.15. — La première égalité résulte de la définition récurrente des nombres de Fibonacci, et la seconde des égalités

$$\begin{aligned} \mathrm{Q}_n(1, \dots, 1, 2) &= 2\mathrm{Q}_{n-1}(1, \dots, 1) + \mathrm{Q}_{n-2}(1, \dots, 1) = 2\mathrm{F}_n + \mathrm{F}_{n-1} \\ &= \mathrm{F}_{n+1} + \mathrm{F}_n = \mathrm{F}_{n+2}. \end{aligned}$$

[retour]

2.16. — On raisonne par récurrence à partir de la définition des polynômes Q_n. [retour]

2.17. — Le lemme se démontre par récurrence sur n. La valeur de Q_{n+m} se calcule en exprimant le produit des $n + m$ matrices correspondantes comme le produit du produit des n premières par le produit des m dernières. La dernière assertion résulte de la précédente : $\mathrm{Q}_n(q_n, \dots, q_1)$ et $\mathrm{Q}_n(q_1, \dots, q_n)$ sont définis par la même récurrence. [retour]

2.18. — C'est un déterminant. [retour]

2.19. — On montrera d'abord que Q_n est une somme, dont tous les coefficients sont égaux à 1, de monômes extraits du produit $q_1 \cdots q_n$, puis on trouvera la règle de sélection de ces monômes : on supprime dans ce produit, de toutes les façons possibles, des couples disjoints de variables successives. [retour]

2.20. — On a une relation

$$\begin{bmatrix} d & a & b \\ 0 & a' & b' \end{bmatrix} = \begin{bmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{bmatrix} \begin{bmatrix} x & 1 & 0 \\ y & 0 & 1 \end{bmatrix}$$

avec $\mathrm{AD} - \mathrm{BC} = (-1)^n$. Calculant les déterminants des deux matrices carrées obtenues en prenant la première colonne et l'une des deux autres, on obtient $da' = -(-1)^n y$, $db' = (-1)^n x$. Donc a' et b' sont au signe près les quotients de y et x par leur pgcd. [retour]

2.21. — Les deux colonnes de droite de la définition matricielle donnent

$$\begin{bmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} a_{i-1} & b_{i-1} \\ a_i & b_i \end{bmatrix},$$

donc

$$\begin{bmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

et on est ramené directement à la définition des polynômes d'Euler. [retour]

2.22. — Cas particulier de l'exercice précédent. Autre raison : dans la définition matricielle de a et b, le déterminant de la matrice carrée de première ligne $a\ b$ vaut ± 1. Autre raison encore : par construction $(-1)^i(a_i b_{i+1} - a_{i+1}b_i)$ est indépendant de i. [retour]

2.23. — Les réécritures respectent les relations $a'x + b'y = u, ax + by = v$, et conservent le pgcd de u et v. On peut remarquer d'ailleurs que $ab' - ba'$ reste invariant au signe près, donc égal à ± 1. [retour]

2.24. — Evident, vu les valeurs des $r_{n+1} - r_n$. [retour]

2.25. — On a $v_n \geqslant n$. Les formules du début du numéro restent valables et donnent $|r_{n+1} - r_n| \leqslant n^{-2}$. [retour]

2.26. — On prouve par récurrence que $v_{2n-1} \geqslant n\epsilon$ et $v_{2n} \geqslant 1 + n(n+1)\epsilon/2$, et on conclut par la même méthode. [retour]

2.27. — Pour $q_1, \ldots, q_i$ fixés, $\mathbf{r}_{i+1}$ est une fonction homographique de q_{i+1}. [retour]

2.28. — En vertu d'une formule donnée précédemment, α est un fonction homographique de α_n. [retour]

2.29. — Les quotients du développement en fraction continue de $0,2941$ sont $3, 2, 2, 195$ à la précision d'une calculette. On peut parier que le nombre donné est

$$\frac{1}{3 + \frac{1}{2 + \frac{1}{2}}},$$

c'est-à-dire $5/17$. [retour]

2.30. — Clair. [retour]

2.31. — Voir la démonstration de la partie a) du lemme 2.40 qui suit. [retour]

2.32. — Il correspond au triplet (c, e, d). [retour]

2.33. — $\overline{\alpha}$ s'écrit $\sqrt{n} + c$, mais $d = 1$ implique $c = q_0$. [retour]

2.34. — Si α correspond à (c, d, e), alors $f(\alpha)$ correspond à (c', e, g), avec comme ci-dessus $c' = qe - c$ et $q = \lfloor \alpha \rfloor = \lfloor (q_0 + c)/e \rfloor$. Alors β correspond à (c'', e, h), avec $c'' = q'e - c' = c + (q' - q)e$ et $q' = \lfloor \beta \rfloor = \lfloor (q_0 + c')/e \rfloor = \lfloor (q_0 + qe - c)/e \rfloor = q + \lfloor (q_0 - c)/e \rfloor$. Il suffit alors de

remarquer que l'on a $0 \leqslant q_0 - c < e$, donc $q' = q$, donc $c'' = c$, donc $(c'', e, h) = (c, e, d)$. [*retour*]

2.35. — Soit α comme ci-dessus. On a $f^{\mathrm{N}}(\alpha) = \alpha$. D'après l'exercice 2.33, cela implique $f^{\mathrm{N}-1}(\alpha) = \overline{\alpha}$. Appliquant l'exercice 2.34, on voit que $f^{n-2}(\alpha) = \overline{f(\alpha)}$ et de proche en proche qu'on a $f^{\mathrm{N}-i}(\alpha) = \overline{f^i(\alpha)}$. Mais cela donne par la même référence $\lfloor f^{\mathrm{N}-i}(\alpha) \rfloor = \lfloor f^i(\alpha) \rfloor$ donc $q_{n-i} = q_i$. [*retour*]

2.36. — Pour $\sqrt{a^2+1}$, on a $q_0 = a$ et $q_1 = q_2 = \cdots = 2a$. Pour $\sqrt{a^2+2}$, on a $q_0 = a, q_1 = q_3 = \cdots = a$ et $q_2 = q_4 = \cdots = 2a$. [*retour*]

2.38. — Conséquence directe du théorème. [*retour*]

2.39. — Même chose que ci-dessus, en prenant les puissances impaires de $u_{\mathrm{N}-1} - v_{\mathrm{N}-1}\sqrt{n}$. [*retour*]

Index