Ioan Badulescu

L3
M1
Agrégation

Anneaux, corps, polynômes et théorie de Galois

Cours et exercices corrigés

ellipses

Partie 1

Anneaux et corps

Chapitre 1

Rappels sur les anneaux et les corps

1.1. Conventions et premières définitions

Dans ce livre,

- tous les anneaux ont une unité (élément neutre pour la multiplication), notée souvent 1 (ou 1_A si l'anneau s'appelle A), qui est différente de l'élément neutre pour l'addition, noté souvent 0,

- tous les morphismes d'anneaux sont unitaires par définition (c'est-à-dire envoient l'unité sur l'unité) ; un morphisme d'un anneau dans lui-même est appelé **endomorphisme** et, s'il est bijectif, **automorphisme**,

- une partie d'un anneau A est un sous-anneau de A si elle est un anneau pour les opérations de A *et a la même unité. Ainsi,* $\mathbb{Z} \times \{0\}$ *n'est pas un sous-anneau de* $\mathbb{Z} \times \mathbb{Z}$ *bien que ce soit un anneau pour les opérations induites par celles de* $\mathbb{Z} \times \mathbb{Z}$,

- la notion d'idéal sera utilisée seulement dans le cas d'un anneau commutatif,

- on appelle **algèbre à division** un anneau dans lequel tout élément non nul est inversible, et on garde le nom **corps** pour une algèbre à division *commutative.* [1]

Si X est une partie d'un anneau commutatif A, alors l'idéal (respectivement le sous-anneau) de A **engendré par** X est par définition l'intersection de tous les idéaux (respectivement les sous-anneaux) de A qui contiennent X. Le sous-corps de A engendré par X peut être défini de la même façon, à condition qu'il existe au moins un sous-corps de A qui contient X. Si $a \in A$, l'idéal engendré par a est noté (a) ; il est égal à aA, l'ensemble des produits de a par les éléments de A. Un idéal engendré par un seul élément est dit **principal**.

Un idéal I d'un anneau commutatif A est dit **propre** s'il n'est pas égal à A. Alors I est propre si et seulement s'il ne contient aucun élément inversible. On peut faire le quotient A/I et obtenir un anneau pour tout idéal propre I de A. Le quotient peut être défini dans le cas $I = A$, mais c'est alors un ensemble à un élément et ne peut donc pas être muni d'une structure d'anneau. En pratique, le quotient A/A n'est jamais utilisé.

1. Une des différences importantes entre les corps et les algèbres à division est le fait qu'un polynôme de degré n à coefficients dans un corps a au plus n racines dans le corps, alors que, par exemple, le polynôme $X^2 + 1$ a une infinité de racines dans l'anneau des quaternions $\mathbb{H}$ (qui sera défini au chapitre suivant).

Soient A un anneau commutatif et I un idéal propre de A. On dit que I est **premier** si pour tous $a, b \in A$, si $ab \in I$, alors on a $a \in I$ ou $b \in I$. On dit que I est **maximal** si I n'est strictement inclus dans aucun idéal propre de A. Un résultat classique affirme qu'*un idéal I propre de A est principal si et seulement si A/I est un anneau intègre, et maximal si et seulement si A/I est est un corps*. En particulier, *un idéal maximal est toujours premier*.

Dans un anneau commutatif A on a la formule

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

pour tous $a, b \in A$ et tout $n \in \mathbb{N}^*$ (démonstration facile par récurrence sur n). On fait la convention qu'une somme d'éléments de A indexée sur l'ensemble vide vaut 0, et un produit d'éléments de A indexé sur l'ensemble vide vaut 1. En particulier, pour tout élément x de A on a $x^0 = 1$, et à titre d'exemple (car aucun intérêt théorique) la formule ci-dessus peut s'appliquer à $n = 0$.

Si A est un anneau, l'ensemble des éléments inversibles de A est un groupe pour la multiplication de A, noté $A^\times$. La notation A^* désigne l'ensemble $A\backslash\{0\}$.

Le cardinal d'un ensemble X est noté $|X|$.

Si p est un nombre premier, l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps, noté $\mathbb{F}_p$.

1.2. Propriétés des morphismes

Si $f : A \to B$ est un morphisme d'anneaux, on note $\ker(f)$ ou $\ker f$ le noyau de f et $Im(f)$ ou Imf l'image de f. Supposons que A et B sont commutatifs. On a alors

- $\ker(f)$ est un idéal propre de A et $Im(f)$ est un sous-anneau de B,
- le morphisme f est injectif si et seulement si $\ker f$ est réduit à $\{0\}$,
- si A est un corps, le morphisme f est toujours injectif, puisque le seul idéal propre d'un corps est $\{0\}$,
- si B est un anneau intègre, alors $\ker(f)$ est un idéal premier (exercice) ; si, de plus, A est principal, alors $\ker(f)$, étant premier, est soit nul, soit maximal engendré par un élément irréductible de A (ceci sera appliqué aux anneaux $A = \mathbb{Z}$ et $A = K[X]$, où K est un corps).

Remarque. S'il existe toujours au moins un morphisme de groupes entre deux groupes donnés, il n'en est pas de même pour les anneaux. Par exemple, il n'existe pas de morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{Z}$, ni de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$.

Si A est un anneau commutatif et I est un idéal propre de A on appelle **projection canonique** sur A/I le morphisme $p_I : A \to A/I$ défini par $x \mapsto \bar{x}$. L'image par p_I d'un idéal de A est un idéal de A/I. Il s'ensuit que, si I, J sont deux idéaux de A tels que $I \subset J$, alors J/I est un idéal de A/I. L'application qui envoie la classe de x modulo I sur la classe de x modulo J

est un morphisme $p_{I,J}$ de A/I dans A/J. Le noyau de ce morphisme est l'idéal J/I.

Rappelons le **théorème d'isomorphisme**, admis ici : *Si A et B sont des anneaux commutatifs, si $f : A \to B$ est un morphisme d'anneaux, alors l'application $\bar{f} : A/\ker(f) \to Im(f)$, donnée par $\bar{a} \mapsto f(a)$, est bien définie et c'est un isomorphisme d'anneaux.* La preuve de ce résultat est assez facile.

Plus généralement, *si $f : A \to B$ est un morphisme d'anneaux commutatifs et I, J sont des idéaux propres de A et B respectivement tels que $f(I) \subset J$, on peut définir $\bar{f} : A/I \to B/J$ par $f(\bar{a}) = \widehat{f(a)}$, où la barre désigne les classes dans A modulo I et le chapeau les classes dans B modulo J. De plus, $\bar{f}$ est un morphisme d'anneaux.* Pour démontrer que $\bar{f}$ est bien définie et c'est un morphisme, on peut noter K le noyau du morphisme $p_J \circ f : A \to B/J$ et appliquer le théorème d'isomorphisme à ce morphisme pour obtenir une application $h : A/K \to B/J$; on compose ensuite à gauche avec $p_{I,K} : A/I \to A/K$, après avoir noté que $I \subset K$.

La question se pose parfois de savoir si deux anneaux sont isomorphes ou pas. Il n'y a pas de méthode générale pour répondre à ce genre de question. Voici toutefois deux conseils : quand il faut démontrer un isomorphisme et que l'un des deux anneaux est un quotient, on applique le théorème d'isomorphisme ; quand on veut démontrer un non isomorphisme, on exhibe souvent une équation qui a plus de solutions dans l'un des anneaux que dans l'autre. Voici deux exemples : on veut montrer que

(a) $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et

(b) $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Réponse : (a) L'application f de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ qui envoie k sur (a, b) où a est la classe de k modulo 2 et b est la classe de k modulo 3 est un morphisme d'anneaux (facile). Le noyau de f est l'ensemble des entiers divisibles par 2 et 3, c'est donc $6\mathbb{Z}$. Par le théorème d'isomorphisme, $\mathbb{Z}/6\mathbb{Z}$ est alors isomorphe à l'image de f dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Cette image a alors 6 éléments (comme $\mathbb{Z}/6\mathbb{Z}$) ; elle est donc égale à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ tout entier.

(b) Si un tel isomorphisme f existait, le nombre des x tels que $x+x = 0$ devrait être le même dans les deux anneaux, parce que f et f^{-1} transformeraient un élément x qui vérifie $x + x = 0$ en un élément y qui vérifie $y + y = 0$; or, ce nombre est deux dans $\mathbb{Z}/4\mathbb{Z}$ et quatre dans $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. (Ou bien : le nombre des x tels que $x^2 = x$ est deux dans $\mathbb{Z}/4\mathbb{Z}$ et quatre dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

Il y a des situations où l'on peut montrer plus rapidement que deux anneaux ne sont pas isomorphes ; par exemple s'ils sont finis mais de cardinal différent, ou si l'un est dénombrable et l'autre ne l'est pas (comme $\mathbb{Z}$ et $\mathbb{R}$) parce que dans ces deux cas, il n'y a simplement pas de bijection possible entre les deux anneaux ; ou bien *si un des anneaux est un corps et l'autre ne l'est pas*, ou *si un des anneaux est intègre mais l'autre ne l'est pas* (ces deux derniers cas se ramènent à une équation qui n'a pas « le même nombre de solutions »

dans les deux anneaux, à savoir l'équation $xy = 1$ pour la *corporalité* et respectivement $xy = 0$ pour l'*intégrité*).

1.3. Corps des fractions

Soit A un anneau commutatif intègre. Alors il existe un corps F avec les propriétés suivantes :

- F contient A et

- tout sous-corps de F qui contient A est égal à F.

On dit alors que F est « **un corps des fractions** de A ».

La preuve de l'existence d'un tel corps est la suivante, facile à se rappeler en pensant comment on passe de $\mathbb{Z}$ à $\mathbb{Q}$. Sur l'ensemble $A \times A^*$ on définit la relation d'équivalence $(a, b) \equiv (c, d)$ si $ad = bc$. On note $Fr(A)$ l'ensemble quotient. On note $\frac{a}{b}$ la classe de (a, b). On munit $Fr(A)$ de l'addition $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et de la multiplication $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$, en montrant qu'elles sont bien définies. Alors $Fr(A)$ est un corps. Souvent on s'arrête ici, après avoir fait la remarque « on peut identifier A à un sous-anneau de $Fr(A)$ en utilisant le morphisme injectif d'anneaux $a \mapsto \frac{a}{1}$ de A dans $Fr(A)$ ». Cela veut dire que A n'est pas inclus dans $Fr(A)$, mais on peut tout simplement noter F l'ensemble obtenu à partir de $Fr(A)$ en remplaçant tout élément $\frac{a}{1}$ de $Fr(A)$ par l'élément a, et que F est cette fois un corps qui contient A et qui est un corps des fractions de A, si les opérations sur F sont définies à partir de celles de $Fr(A)$ en remplaçant $\frac{a}{1}$ par a dans les opérations où elle apparaît.

Voici quelques propriétés des corps des fractions.

(1) *Si F est un corps des fractions de A et K est un corps et $h : A \to K$ est un morphisme injectif d'anneaux, alors h se prolonge de façon unique à un morphisme de corps $H : F \to K$*, la formule étant $H(\frac{a}{b}) = h(a)h(b)^{-1}$.

(2) *Deux corps des fractions de A sont toujours isomorphes par un isomorphisme qui prolonge l'identité de A* (découle de (1)).

(3) *Si $f : A \to B$ est un morphisme injectif d'anneaux, si F_A est un corps des fractions de A et F_B est un corps des fractions de B, alors f se prolonge de façon unique en un morphisme de corps $F_A \to F_B$* (passer par le morphisme (injectif) composé $A \to B \to F_B$, et puis (2)).

(4) *Si K est un corps et A est un sous-anneau de K, alors le sous-corps de K engendré par A est un corps des fractions de A.*

1.4. L'anneau $\mathbb{Z}$ et son arithmétique

Rappelons quelques propriétés bien connues de $\mathbb{Z}$ qui peuvent servir dans ce livre :

- si $a, b \in \mathbb{Z}$ on dit que a **divise** b et on écrit $a|b$ s'il existe $a' \in \mathbb{Z}$ tel que $aa' = b$; l'entier a' est alors unique avec cette propriété si $a \neq 0$; ainsi, tous les entiers divisent 0 et 0 divise un seul élément de $\mathbb{Z}$, à savoir 0 ;

- si $a|b$ et $|b| < |a|$ alors $b = 0$; si $a|b$ et $b|a$, alors $a = \pm b$;

- si $a, b \in \mathbb{Z}$ et $b \neq 0$, il existe dans $\mathbb{Z}$ une division euclidienne de a par b ;

- si $a, b \in \mathbb{Z}^*$, il existe un pgcd et un ppcm pour a et b, uniques si on les prend positifs ; on dit que a et b sont premiers entre eux si leur pgcd est 1 ;

- si $a, b \in \mathbb{Z}^*$, alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$ (**théorème de Bézout**) ; si, de plus, $a, b \geq 2$, il existe un et un seul couple $(u, v) \in \mathbb{N}^* \times \mathbb{N}^*$ tels que $u < a$, $v < b$ et $ua - vb = 1$;

- si $a, b, c \in \mathbb{N}^*$, si a divise bc et est premier avec b, alors a divise c (**lemme de Gauss**) ; si un nombre premier divise un produit, alors il divise l'un des termes du produit ;

- il existe une infinité de nombres premiers dans $\mathbb{N}$; tout élément de $\mathbb{N}^*$ a une « décomposition unique en produit de nombres premiers », c'est-à-dire qu'il s'écrit comme un produit de nombres premiers, écriture unique à l'ordre près ; un nombre premier p apparaît dans la décomposition de n en produit de nombres premiers si et seulement si p divise n ;

- deux éléments de $\mathbb{N}^*$ sont premiers entre eux si et seulement s'il n'existe pas de nombre premier qui apparaît dans la décomposition des deux ;

- les éléments premiers de $\mathbb{Z}$ en termes de théorie des anneaux sont non seulement les nombres premiers de $\mathbb{N}$, mais aussi leurs opposés pour l'addition ;

- tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$; un tel idéal non nul $I = n\mathbb{Z}$ est premier si et seulement s'il est maximal, si et seulement si n est un nombre premier, si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Certaines propriétés des nombres entiers qui semblent évidentes doivent néanmoins être systématiquement démontrées, à partir des propriétés données ci-dessus. N'oubliez jamais d'appliquer Bézout quand l'hypothèse vous parle de deux nombres premiers entre eux. Si vous êtes à court d'idées, tentez toujours votre chance en décomposant en produit de nombres premiers.

Exemples de preuves. (1) Soient a, b, m, n des entiers strictement positifs. Alors a^m et b^n sont premiers entre eux si et seulement si a et b sont premiers entre eux.

Preuve : Si a et b ne sont pas premiers entre eux, il existe $d > 1$ qui divise à la fois a et b. Le même d divise a^m et b^n. Donc a^m et b^n ne sont pas premiers entre eux.

Si a^m et b^n ne sont pas premiers entre eux, il existe un nombre premier p qui divise à la fois a^m et b^n. On utilise alors que si un nombre premier divise un produit il divise l'un des termes du produit. On en déduit que p divise a et p divise b, qui ne peuvent donc pas être premiers entre eux.

(2) Il n'existe pas de nombres entiers non nuls a et b tels que $a\sqrt[3]{20} = b$.

Preuve : supposons par l'absurde que $20a^3 = b^3$, avec $a, b \in \mathbb{Z}^*$. Quitte à multiplier par -1, on suppose que a et b sont positifs. La puissance de 5 dans a^3 est divisible par 3, et pareil pour b^3. Alors dans la décomposition de $20a^3$ la puissance de 5 est congrue à 1 modulo 3, tandis que dans celle de b^3 elle est

congrue à 0 modulo 3. Cela contredit l'unicité de la décomposition en produit de nombres premiers de l'entier $20a^3 = b^3$.

(3) Si p est un nombre premier et k est un entier tel que $1 \leq k \leq p-1$, alors p divise C_p^k.

Preuve : On a $k!(n-k)!C_p^k = p! = p(p-1)!$. Donc p divise $k!(n-k)!C_p^k$. Or, p ne divise aucun des nombres $1, 2, ..., k$ et aucun des nombres $1, 2, ..., n-k$ qui lui sont inférieurs. Donc p divise C_p^k par le lemme de Gauss.

$\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. Tout élément strictement positif de $\mathbb{Q}$ s'écrit de façon unique sous la forme $\frac{a}{b}$, avec $a, b \in \mathbb{N}^*$ premiers entre eux. Voici un résultat utile que nous présentons aussi pour mettre en évidence un exemple de preuve :

Exemple. Soient $m, n \in \mathbb{N}^*$ tels que $\text{pgcd}(m, n) = 1$ et $\frac{m}{n}$ est le carré d'un nombre rationnel. Alors m et n sont des carrés de nombres entiers.

Preuve : On écrit $\frac{m}{n} = (\frac{a}{b})^2$, où $a, b \in \mathbb{N}^*$ sont premiers entre eux. On a alors $mb^2 = na^2$. Comme m est premier avec n, on a $m|a^2$ par le lemme de Gauss. Comme a est premier avec b, a^2 est premier avec b^2 (le (1) plus haut) et donc $a^2|m$ par le lemme de Gauss. Comme $m|a^2$ et $a^2|m$ on a $m = \pm a^2$. Mais m et a^2 sont positifs, donc $m = a^2$. Alors, en simplifiant, on trouve aussi $n = b^2$.
En particulier, *un nombre entier qui est le carré d'un nombre rationnel est le carré d'un nombre entier.*

Pour tout $n \in \mathbb{N}^*$, on note $\phi(n)$ le nombre des entiers strictement positifs inférieur à n qui sont premiers avec n. La fonction $\phi : \mathbb{N}^* \to \mathbb{N}^*$ ainsi définie s'appelle **indicatrice d'Euler**. Elle a une formule utile : si $n = \prod_{i=1}^{s} p_i^{m_i}$ est la décomposition de n en produit de nombres premiers, alors on a

$$\phi(n) = \prod_{i=1}^{s}(p_i^{m_i} - p_i^{m_i-1}) = n\prod_{i=1}^{s}(1 - \frac{1}{p_i}).$$

Par exemple, $\phi(15) = 8$ et $\phi(122) = 60$.

1.5. Arithmétique dans les anneaux intègres

Soit A un anneau commutatif intègre. Alors dans A on peut « simplifier » par les éléments non nuls. C'est-à-dire que, si $a, b, c \in A$ et $ab = ac$, alors on a $a(b-c) = 0$ et, si $a \neq 0$, alors $b = c$ (on a simplifié $ab = ac$ par a pour trouve $b = c$). Cela n'a pas lieu par exemple dans l'anneau non intègre $\mathbb{Z}/6\mathbb{Z}$, où on a $\bar{2}\bar{1} = \bar{2}\bar{4}$.

Si $a, b \in A$ on dit que a **divise** b s'il existe $c \in A$ tel que $ac = b$. On écrit alors $a|b$. Si $a, b \in A$, on dit que a et b sont **associés** s'il existe un élément inversible $u \in A^\times$ tel que $a = ub$, ou, pareil, si $a|b$ et $b|a$.

Si $a \in A\backslash\{0\}$, on dit que a est **irréductible** s'il vérifie :

(i) a n'est pas inversible et

(ii) si $x, y \in A$ sont tels que $xy = a$, alors soit x est inversible, soit y est inversible.

Si $a \in A\backslash\{0\}$ on dit que a est **premier** s'il vérifie :

(i) a n'est pas inversible et

(ii) si $x, y \in A$ sont tels que $a|xy$, alors $a|x$ ou $a|y$. En particulier, tout élément premier est irréductible.

Soient $x, y \in A\backslash\{0\}$, où A est un anneau commutatif intègre.

On dit que x, y admettent **un plus petit commun multiple** (ppcm) s'il existe $m \in A$ tel que $x|m$, $y|m$, et tout élément m' de A tel que $x|m'$ et $y|m'$ vérifie $m|m'$. Un tel m est alors unique à multiplication par un élément inversible près. On dit que m est un plus petit commun multiple (un ppcm) de x et y. Si on écrit $\alpha = \text{ppcm}(x, y)$ on lit « α est un ppcm de x et y ».

On dit que x, y admettent **un plus grand commun diviseur** (pgcd) s'il existe $d \in A$ tel que $d|x$, $d|y$, et tout élément d' de A tel que $d'|x$ et $d'|y$ vérifie $d'|d$. Un tel d est alors unique à multiplication par un élément inversible près. On dit que d est un plus grand commun diviseur (un pgcd) de x et y. Si on écrit $\beta = \text{pgcd}(x, y)$, on lit « β est un pgcd de x et y ».

On dit que x et y sont **premiers entre eux** si tout élément de A qui divise à la fois x et y est inversible. Cela équivaut à $1 = \text{pgcd}(x, y)$.

Ces définitions se font par analogie avec $\mathbb{Z}$. Toutefois, dans $\mathbb{Z}$ tout irréductible est premier et il existe toujours un ppcm et un pgcd. Ce n'est pas le cas de tout anneau intègre. De plus, dans $\mathbb{Z}$, si on déclare que le ppcm est positif, alors il est unique, et pareil pour le pgcd.

Exemples : (1) Soit $\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5},\ a, b \in \mathbb{Z}\}$ vu comme un sous-anneau de $\mathbb{R}$. Alors $\sqrt{5}$ est premier dans $\mathbb{Z}[\sqrt{5}]$. En effet, si $\sqrt{5}$ divise $(a+b\sqrt{5})(c+d\sqrt{5})$, alors en faisant les multiplications on voit qu'on a $\sqrt{5}$ divise ac. Cela se traduit par $\sqrt{5}(u+v\sqrt{5}) = ac$, et on voit qu'on doit avoir $u = 0$ et $5|ac$ dans $\mathbb{Z}$. Comme 5 est premier, on a $5|a$ ou $5|c$, donc $\sqrt{5}|a + b\sqrt{5}$ ou $\sqrt{5}|c + d\sqrt{5}$.

(2) Soit $\mathbb{Z}[\sqrt{6}] := \{a + b\sqrt{6},\ a, b \in \mathbb{Z}\}$ vu comme un sous-anneau de $\mathbb{R}$. Alors $\sqrt{6}$ n'est pas premier dans $\mathbb{Z}[\sqrt{6}]$, parce qu'il divise $6 = 2\times 3$, sans diviser ni 2 ni 3. En effet, $2 = \sqrt{6}(a+b\sqrt{6})$ implique $a = 0$ et ensuite 6 divise 2. Même type de preuve pour 3.

(3) Soit A la partie de $\mathbb{Q}$ formée des quotients $\frac{a}{2^n}$, où $a \in \mathbb{Z}$ et $n \in \mathbb{N}$. Alors A est un anneau intègre et 2 est inversible dans A. 6 est premier dans A. En effet, il est associé à 3, et, si 3 divise $\frac{a}{2^n}\frac{b}{2^m}$ dans A, alors 3 divise ab dans $\mathbb{Z}$, donc 3 divise a ou b dans $\mathbb{Z}$, d'où 3 divise $\frac{a}{2^n}$ ou $\frac{b}{2^m}$ dans A.

(4) 2 est irréductible dans l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers. En effet, si on écrit $2 = PQ$, alors par les degrés on doit avoir $P, Q \in \mathbb{Z}$.

Or, dans $\mathbb{Z}$ on sait que $2 = PQ$ implique P ou Q est pair. En revanche, 2 n'est pas irréductible dans $\mathbb{R}[X]$, parce qu'il est inversible.

1.6. Caractéristique. Conséquences

Pour tout anneau A, il existe un et un seul morphisme $f : \mathbb{Z} \to A$. On écrit souvent n pour $f(n)$, puisqu'il n'y a pas d'ambiguïté suite à l'unicité de f. En particulier, si $a \in A$ et $n \in \mathbb{N}^*$, $na = \underbrace{a + a + ... + a}_{n \text{ fois}}$. La formule du binôme de Newton

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

qui fonctionne dans tout anneau commutatif, a un sens à la lumière de cette convention, c'est-à-dire que C_n^k désigne ici l'élément $1 + 1 + ... + 1$ de A, où le nombre de 1 dans la somme est $\frac{n!}{k!(n-k)!}$ (qui est un entier).

Soit A un anneau. Si $f : \mathbb{Z} \to A$ est l'unique morphisme d'anneaux, l'image Imf est le sous-anneau de A engendré par 1, et c'est un anneau commutatif, inclus dans tout sous-anneau de A. On l'appelle parfois l'**anneau premier de** A. En tant que sous-groupe additif de $(A, +)$ c'est le sous-groupe de $(A, +)$ engendré par 1. Le théorème d'isomorphisme donne $A/\ker f \simeq Imf$. Le noyau $\ker f$ de f est un idéal propre de $\mathbb{Z}$. Il est donc de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}\backslash\{1\}$. On dit alors que A est de **caractéristique** n. Si $n \neq 0$, n est le plus petit entier strictement positif tel que $n1 = 0$. On a alors $na = 0$ pour tout $a \in A$, parce que $na = (n1)\, a$ par distributivité. Dans ce cas, la caractéristique n de A est tout simplement l'ordre de 1 dans le groupe additif $(A, +)$. Si $n = 0$, alors une somme non vide de 1 dans A ne vaut jamais 0, autrement dit 1 est d'ordre infini dans le groupe $(A, +)$. *Si A est intègre (en particulier si A est un corps), alors on sait que* $\ker f$ *est un idéal premier. Dans ce cas, n est soit nul, soit un nombre premier.*

Conséquences. Soit K un corps.

(a) Puisque K est intègre, la caractéristique de K est soit nulle, soit un nombre premier.

(b) Par définition, la caractéristique de K est nulle si et seulement si le morphisme de $\mathbb{Z}$ dans K est injectif. Dans ce cas, par la propriété du corps des fractions, ce morphisme se prolonge à un morphisme injectif de $\mathbb{Q}$ dans K. L'image est un sous-corps de K isomorphe à $\mathbb{Q}$.

(c) Si la caractéristique de K est un nombre premier p, alors le noyau de $f : \mathbb{Z} \to K$ est l'idéal (p), et donc l'image de f est (par le théorème d'isomorphisme) un sous-corps de K isomorphe à $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$. Si on note ce corps K_0, alors K est muni naturellement d'une structure de K_0-espace vectoriel, la multiplication des éléments de K (vecteurs) par des éléments de K_0 (scalaires) étant tout simplement la multiplication dans K. Dès lors, si K est fini, c'est un K_0-espace vectoriel de dimension finie, disons n, et donc

isomorphe, en tant qu'espace vectoriel, avec K_0^n. Donc K a p^n éléments. Nous avons obtenu :

le cardinal d'un corps fini est toujours une puissance d'un nombre premier.

Par exemple, il n'existe pas de corps qui ait 36 éléments, ou 100 éléments, puisque 36 et 100 ne sont pas des puissances d'un nombre premier.

Nous dédierons une section à part aux corps finis.

1.7. L'endomorphisme de Frobenius

Théorème – définition. *Soit A un anneau commutatif de caractéristique p non nulle. On suppose que p est un nombre premier (c'est forcément le cas si A est intègre). Alors pour tous $x, y \in A$ on a $(x+y)^p = x^p + y^p$. L'application $f : A \to A$ définie par $f(x) = x^p$ est un endomorphisme d'anneau, dit* **endomorphisme de Frobenius**.

Démonstration. Grâce qu binôme de Newton, on écrit

$$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} C_p^k x^k y^{p-k}.$$

Pour tout k entier entre 1 et $p-1$, on a p divise C_p^k (voir l'exemple (3) de la section « L'anneau $\mathbb{Z}$ et son arithmétique »). Donc $C_p^k = 0$ dans A. D'où $f(x+y) = f(x) + f(y)$. On a par ailleurs $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$ et $f(1) = 1^p = 1$. □

Soit A un anneau commutatif dont la caractéristique est un nombre premier p. Si $\mathrm{Frob}_A : A \to A$ est l'endomorphisme de Frobenius, alors pour tout $n \in \mathbb{N}^*$ on a $\mathrm{Frob}_A^n : x \mapsto x^{p^n}$ (où la puissance est par rapport à la composition). $\mathrm{Frob}_A^n : x \mapsto x^{p^n}$ est un endomorphisme de A.

1.8. Anneaux finis. Les corps $\mathbb{F}_p$

Soit A un anneau fini. La caractéristique de A est l'ordre de 1 dans le groupe $(A; +)$, ce qui prouve que la caractéristique de A est finie et divise le cardinal de A. Si cette caractéristique est un nombre premier p, par le même raisonnement vu pour les corps finis (à savoir A est un espace vectoriel de dimension finie sur son sous-corps engendré par 1) on obtient que *le cardinal de A est forcément de la forme p^n.*

On a également la classique :

Proposition 1.1. *Soit A un anneau fini intègre. Alors A est une algèbre à division.*

Démonstration. Soit $x \in A$, $x \neq 0$. Soit $f : A \to A$ l'application définie par $f(a) = xa$ pour tout $a \in A$. Par distributivité, f est un endomorphisme du groupe $(A, +)$. Puisque A est intègre et x est non nul, on a que $xa = xb$ implique $a = b$, donc f est injectif. L'anneau A est de cardinal fini et f est injectif, donc f est surjectif. Alors 1_A appartient à l'image, ce qui implique que x a un inverse a à droite. De la même façon on montre que x a un inverse b à gauche. De plus, $a = b$ car $b = b(xa) = (bx)a = a$ par associativité. Donc x est inversible.

Remarque. Il sera montré à la section « Théorème de Wedderburn » du chapitre 4 qu'une algèbre à division finie est forcément un corps, c'est-à-dire est commutative.

La notation $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ *quand* p *est premier* a déjà été vue à la première section de ce chapitre. $\mathbb{F}_p$ est un corps. Par exemple parce que c'est un anneau fini, et qu'il est intègre puisque $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Il est possible de prouver que $\mathbb{F}_p$ est un corps par le théorème de Bézout dans $\mathbb{Z}$, preuve proposée en exercice. Il est facile de voir que $\mathbb{F}_p$ est de caractéristique p. L'endomorphisme de Frobenius est ici égal tout simplement à l'identité ; c'est-à-dire, tout élément x de $\mathbb{F}_p$ vérifie $x^p = x$; en effet, si $x = 0$, on a $x^p = x$ et que, si $x \neq 0$, alors x est un élément du groupe $\mathbb{F}_p \backslash \{0\}$ et vérifie donc $x^{p-1} = 1$ par le théorème de Lagrange. Le fait que l'endomorphisme de Frobenius de $\mathbb{F}_p$ soit l'identité est équivalent au petit théorème de Fermat dans $\mathbb{Z}$.

1.9. Exercices

Exercice 1. Soit K un corps. On cherche le nombre d'éléments distincts x de K tels que $x^2 = 1$. Montrer que la réponse est « un si $\mathrm{car}(K) = 2$ et deux si $\mathrm{car}(K) \neq 2$ ».

Exercice 2. Montrer qu'un produit de corps n'est jamais un corps.

Exercice 3. Montrer qu'il n'existe pas de morphisme entre deux corps de caractéristiques différentes.

Exercice 4. Soit $f : A \to B$ un morphisme d'anneaux. Montrer que, si B est intègre, alors $\ker(f)$ est un idéal premier de A.

Exercice 5. Soit $f : A \to B$ un morphisme d'anneaux.

(a) Montrer que, si J est un idéal de B, alors $f^{-1}(J)$ est un idéal de A.

(b) Montrer que, si I est un idéal de A et f est surjectif, alors $f(I)$ est un idéal de B.

(c) Montrer par un contrexemple précis que, si f n'est pas surjectif, il se peut que l'image par f d'un idéal de A ne soit pas un idéal de B.

Exercice 6. Montrer qu'il n'existe pas de morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{Q}$, ni de $\mathbb{Q}$ dans $\mathbb{Z}$.

Exercice 7. Soit K un corps inclus dans $\mathbb{Q}$. Montrer que $K = \mathbb{Q}$.

Exercice 8. Soit K un corps tel que le seul sous-corps de K est K lui-même. Montrer que si K est infini alors il est isomorphe à $\mathbb{Q}$, et si K est fini, alors il est isomorphe à l'un des corps $\mathbb{F}_p$.

Exercice 9. (a) Dresser les tables d'addition et de multiplication d'un anneau à deux éléments.

(b) Supposons qu'il existe un corps K à quatre éléments, qu'on note $0, 1, a, b$. Montrer que la caractéristique de K est 2. Dresser la table d'addition de K et ensuite la table de multiplication de K (utiliser que K et $K^\times$ sont des groupes, et le fait que K est de caractéristique 2).

Exercice 10. Posons $A := \{a + b\sqrt{2}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$, comme sous-ensemble de $\mathbb{R}$.

(a) Montrer que A est un sous-anneau de $\mathbb{R}$.

(b) Montrer que A n'est pas isomorphe à $\mathbb{Z} \times \mathbb{Z}$.

(c) Montrer que l'idéal I de A engendré par $\sqrt{2}$ est maximal. Montrer que A/I est isomorphe à $\mathbb{F}_2$.

(d) Montrer que, si $a, b \in \mathbb{Z}$ sont tels que $3|a^2 - 2b^2$, alors $3|a$ et $3|b$. En déduire que l'idéal J engendré par 3 est premier. En déduire que le quotient A/J est un corps. Quelle est sa caractéristique ? Quel est son cardinal ?

Exercice 11. Soient E, K deux corps finis de caractéristique p tels que $K \subset E$. On a vu en cours que $|K| = p^n$ pour un $n \in \mathbb{N}^*$ et $|E| = p^m$ pour un $m \in \mathbb{N}^*$. En s'inspirant de la preuve même de ce résultat de cours, montrer que n divise m.

Exercice 12. Soit A un anneau fini à p éléments ou p est un nombre premier. Montrer que A est un corps.

Exercice 13. Soient $m, n \in \mathbb{N}^* \backslash \{1\}$ deux nombres premiers entre eux. On sait qu'il existe une relation de Bézout $um + vn = 1$ avec $u, v \in \mathbb{Z}^*$. À partir de cette relation, montrer qu'il existe un couple d'entiers (u', v') tel que $1 \leq u' \leq n - 1$, $1 \leq v' \leq m - 1$ et $u'm - v'n = 1$. Montrer également qu'il existe un couple d'entiers (u'', v'') tel que $|u''| \leq \frac{n}{2}$, $|v''| \leq \frac{m}{2}$ et $u''m + v''n = 1$.

Exercice 14. Donner un exemple de deux anneaux non isomorphes dont les corps des fractions sont isomorphes.

Exercice 15. Soit $\mathbb{F}$ un corps fini à 27 éléments. Quels sont les éléments x de $\mathbb{F}$ qui vérifient $x^3 = 1$?

Exercice 16. Si A est un anneau commutatif, montrer que A est un corps si et seulement si A possède exactement deux idéaux. Si K, L sont deux corps, quels sont les idéaux de l'anneau $K \times L$?

Exercice 17. Soient A, B, C, D quatre corps.

(a) On suppose que les anneaux $A \times B$ et $C \times D$ sont isomorphes. Montrer que A est isomorphe à C ou à D.

(b) Donner un exemple de morphisme d'anneaux de $\mathbb{R} \times \mathbb{R}$ dans $\mathbb{R} \times \mathbb{R}$ qui n'est pas un isomorphisme.

Exercice 18. Soit A un anneau. On rappelle que le centre de A, noté $Z(A)$, est par définition l'ensemble des éléments de A qui commutent (pour la multiplication) avec tous les éléments de A. Montrer que $Z(A)$ est un sous-anneau de A. Si A est une algèbre à division, montrer que $Z(A)$ est un corps.

Exercice 19. Soit A un anneau.

(a) Si $f : A \to A$ est un endomorphisme de A, montrer que l'ensemble A_f des points fixes de f, (définis par $f(x) = x$), est un sous-anneau de A. Si A est un corps, montrer que A_f est un corps.

(b) Soit E un ensemble non vide d'endomorphismes de A. Soit A_E l'ensemble des éléments x de A qui vérifient $f(x) = g(x)$ quels que soient f et g dans E. Montrer que A_E est un sous-anneau de A. Si A est un corps, montrer que A_E est un corps.

Exercice 20. Soit p un nombre premier. Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps en utilisant le théorème de Bézout dans $\mathbb{Z}$.

Pourquoi $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps quand n n'est pas un nombre premier ?

Exercice 21. Soit n un entier qui est un cube dans $\mathbb{Q}$. Montrer que n est un cube dans $\mathbb{Z}$.

Exercice 22. Soit $n \in \mathbb{N}^*$ un entier qui n'est pas un carré. On pose alors $\mathbb{Q}(\sqrt{n}) := \{a + b\sqrt{n}, \quad a, b \in \mathbb{Q}\}$.

(a) Montrer que $\mathbb{Q}(\sqrt{n})$ est un corps, et que c'est le sous-corps de $\mathbb{R}$ engendré par $\sqrt{n}$ (c'est-à-dire l'intersection de tous les sous-corps de $\mathbb{R}$ qui contiennent $\sqrt{n}$).

(b) Montrer que $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas isomorphes.

(c) Si $m, n \in \mathbb{N}^*$ ne sont pas des carrés, montrer que $\mathbb{Q}(\sqrt{m}) \simeq \mathbb{Q}(\sqrt{n})$ si et seulement si $\frac{m}{n}$ est un carré dans $\mathbb{Q}$.

Exercice 23. Soient A un anneau commutatif et X une partie de A. On rappelle que, dans A, une somme indexée sur l'ensemble vide est égale à 0, et un produit indexé sur l'ensemble vide est égal à 1.

(a) Montrer que l'idéal engendré par X est l'ensemble des sommes $\sum_{i \in I} a_i x_i$ où I est un ensemble fini et pour tout $i \in I$ on a $a_i \in A$ et $x_i \in X$.

(b) Montrer que le sous-anneau de A engendré par X est l'ensemble des sommes de produits d'éléments de X et des éléments opposées à ces éléments.

(c) Savez-vous identifier l'idéal de A engendré par l'ensemble vide ? Et le sous-anneau de A engendré par l'ensemble vide ?

Exercice 24. Soit A un anneau et soit $g \in A^\times$. Montrer que $x \mapsto gxg^{-1}$ est un automorphisme de l'anneau A.

Exercice 25. Soit A un anneau commutatif. Montrer les éléments de $A^\times$ qui sont de la forme $a^2 + b^2$ avec $a, b \in A$ forment un sous-groupe de $A^\times$.

Exercice 26. Si K est un corps, montrer que $(K, +)$ et $(K^\times, \times)$ ne sont pas isomorphes.

Exercice 27. Soit K un corps de caractéristique p. Montrer que l'ensemble $\{x^p, x \in K\}$ est un sous-corps de K.

Exercice 28. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps. Montrer que f est l'identité.

Exercice 29. (a) Si K est un corps et $x \in K$ est différent de 0 et 1, montrer que

$$x^2 = x + ((x-1)^{-1} - x^{-1})^{-1}.$$

(b) En déduire que, si K et K' sont des corps de caractéristique différente de 2, alors une application $f : K \to K'$ qui vérifie

- $f(1) = 1$,
- $f(x + y) = f(x) + f(y) \quad \forall x, y \in K$,
- $f(x^{-1}) = f(x)^{-1} \quad \forall x \in K^\times$,

est un morphisme de corps.

Exercice 30. Soient A un anneau et B une partie de A telle que B est stable par l'addition et la multiplication de A et c'est un anneau pour ces opérations. Il a été vu dans le cours ($A = \mathbb{Z} \times \mathbb{Z}$ et $B = \mathbb{Z} \times \{0\}$) que B n'est pas forcément un sous-anneau de A. Montrer que, si A est intègre, alors B est forcément un sous-anneau de A.

Exercice 31. Soient $a, b, c, n \in \mathbb{N}^*$ tels que $ab = c^n$. Si a et b sont premiers entre eux, montrer que a est la puissance n-ième d'un nombre entier (et b aussi).

Exercice 32. Soit K le sous-corps de $\mathbb{R}$ engendré par $\sqrt{3} + \sqrt{2}$. Montrer que K contient $\mathbb{Q}$. Montrer que K contient $\sqrt{2}$ et $\sqrt{3}$. Montrer que K est aussi le sous-corps de $\mathbb{R}$ engendré par $X = \{\sqrt{2}, \sqrt{3}\}$.

Exercice 33. (Théorème d'indépendance de Dedekind). [2] Soient G un groupe et K un corps. Supposons qu'il existe n morphismes de groupes différents que nous notons $\chi_1, \chi_2, ..., \chi_n$ de G dans $K^\times$ et n éléments $\lambda_1, \lambda_2, ..., \lambda_n$ de K tels que $\sum_{k=1}^{n} \lambda_k \chi_k = 0$. Montrer que tous les λ_k sont nuls. (Autrement dit : les morphismes de groupes de G dans $K^\times$ forment une famille libre du K-espace vectoriel des applications de G dans K.)

Exercice 34. Montrer qu'un produit d'anneaux $A \times B$ n'est jamais un anneau intègre.

Exercice 35. Soit A un anneau. On suppose qu'il existe dans A un élément x différent de 0 et 1 tel que $x^2 = x$.

(a) Montrer que $(1 - x)^2 = (1 - x)$.

(b) Montrer que $xA := \{xa, a \in A\}$ et $(1 - x)A := \{(1 - x)a, a \in A\}$ sont de anneaux pour les opérations de A (mais avec un élément neutre différent).

(c) Montrer que l'anneau A est isomorphe à l'anneau produit $xA \times (1-x)A$.

(d) Donner un exemple d'anneau qui contient un élément x différent de 0 et 1 tel que $x^2 = x$.

Voici maintenant quelques exercices sur l'arithmétique dans les anneaux intègres. Les anneaux de polynômes seront étudiés en détail dans les chapitres 3 et 4.
Dans tout ce qui suit, A est un anneau commutatif intègre.

Exercice 36. Soient $a, b \in A\backslash\{0\}$ tels que $a|b$. On écrit $ac = b$. Montrer que c est unique avec cette propriété (que $ac = b$).

Exercice 37. Soit $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers. Montrer que 2 est premier dans $\mathbb{Z}[X]$.

Exercice 38. Prouver les affirmations :

(a) Un élément de A est inversible si et seulement s'il divise tous les éléments de A. Si x divise un inversible, x lui-même est inversible.

(b) Si $a, b \in A\backslash\{0\}$, alors a et b sont associés si et seulement si $a|b$ et $b|a$.

2. Ce résultat sera utilisé plus loin dans le livre.

(c) Un élément a de A est irréductible si et seulement si a n'est pas inversible et les seuls diviseurs de a sont les inversibles et les éléments associés à a.

(d) Montrer qu'un élément premier est toujours irréductible.

Exercice 39. Montrer que, dans A, un idéal engendré par un élément inversible est égal à A, et un idéal engendré par un élément premier est un idéal premier.

Exercice 40. (a) Soit $n \in \mathbb{N}^*$ tel que n n'est pas un carré. Montrer que $\mathbb{Z}[\sqrt{n}] := \{a + b\sqrt{n}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$ est un sous-anneau intègre de $\mathbb{R}$.

(b) Dans $\mathbb{Z}[\sqrt{n}]$, montrer que $a+b\sqrt{n} = c+d\sqrt{n}$ avec $a, b, c, d \in \mathbb{Z}$ implique $a = c$ et $b = d$. En déduire que $f : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}[\sqrt{n}]$ définie par la formule $f(a+b\sqrt{n}) = a-b\sqrt{n}$ est bien définie et c'est un morphisme bijectif d'anneaux.

(c) Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}[i\sqrt{n}] := \{a + ib\sqrt{n}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$ est un sous-anneau intègre de $\mathbb{C}$.

Exercice 41. Dans l'anneau $\mathbb{Z}[i]$, est-ce que i est un élément premier ? Et 2 ? Et 3 ? (Indication : penser à multiplier par la quantité conjuguée dans $\mathbb{C}$.)

Exercice 42. Partons de l'égalité $2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ dans $\mathbb{Z}[i\sqrt{3}]$. Montrer que 2 est irréductible dans $\mathbb{Z}[i\sqrt{3}]$ (même indication que l'exercice précédent). Montrer que 2 ne divise ni $1 + i\sqrt{3}$ ni $1 - i\sqrt{3}$, et en déduire que 2 n'est pas premier.

Exercice 43. (a) Montrer que l'ensemble des entiers qui s'écrivent $2u + 3v$ avec $u, v \in \mathbb{N}$ est égal à $\mathbb{N}\backslash\{1\}$.

(b) Montrer que le sous-anneau B de $\mathbb{Z}[X]$ engendré par $\{X^2, X^3\}$ est égal à l'ensemble des polynômes de $\mathbb{Z}[X]$ pour lequel le coefficient de X est nul.

(c) Montrer que, dans l'anneau intègre B, X^5 et X^6 n'ont pas de pgcd.

1.10. Annexe : Anneaux principaux et factoriels ; $\mathbb{Z}[i]$

Dans la première sous-section nous énonçons les résultats, dans la seconde nous prouvons les résultats énoncés dans la première, et dans la troisième nous étudions l'anneau $\mathbb{Z}[i]$ et nous montrons comme application du fait que cet anneau est principal le théorème des deux carrés.

1.10.1. Définitions et énoncé des résultats.

Définition. On dit qu'un anneau commutatif A est **euclidien** si

(a) A est intègre et

(b) il existe un application $N : A \to \mathbb{N}$ telle que $N(a) = 0$ si et seulement si $a = 0$ et, pour tous $a, b \in A\backslash\{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et

$N(r) < N(b)$. Il n'est pas demandé à q et r d'être unique. Une telle application N est appelée un **stathme** sur A.

Définition. On dit qu'un anneau commutatif A est **principal** si
(a) A est intègre et
(b) tout idéal de A est principal.

Définition. On dit qu'un anneau commutatif A est **factoriel** si
(a) A est intègre et
(b) il existe un ensemble $\mathcal{P}$ d'éléments irréductibles de A tels que :
(i) tout élément $x \in A\backslash\{0\}$ admet une décomposition $x = u\prod_{i=1}^{k} p_i^{a_i}$ avec $u \in A^\times$, $a_i \in \mathbb{N}^*$ et $p_i \in \mathcal{P}$ distincts,
(ii) si un élément $x \in A\backslash\{0\}$ admet deux décompositions $x = u\prod_{i=1}^{k} p_i^{a_i} = u'\prod_{j=1}^{k'} q_j^{b_j}$ avec $u, u' \in A^\times$, $a_i, b_j \in \mathbb{N}^*$ et $p_i \in \mathcal{P}$ distincts et $q_j \in \mathcal{P}$ distincts, alors on a $k = k'$, $u = u'$, et il existe une permutation σ de $\{1, 2, ..., k\}$ telle que $p_i = q_{\sigma(i)}$ et $a_i = b_{\sigma(i)}$.

Commentaires sur les anneaux factoriels. Soit A un anneau factoriel.
(1) On peut écrire tout élément a d'un anneau factoriel $a = u\prod_{p\in\mathcal{P}} p^{a_p}$, avec $u \in A^\times$ et les $a_p \in \mathbb{N}$ tous nuls sauf un nombre fini. Avec cette notation, si $a = u\prod_{p\in\mathcal{P}} p^{a_p}$ et $b = u'\prod_{p\in\mathcal{P}} p^{b_p}$, on a $ab = uu'\prod_{p\in\mathcal{P}} p^{a_p+b_p}$.
(2) Si K est le corps des fractions de A, alors tout élément x de K s'écrit $x = u\prod_{p\in\mathcal{P}} p^{a_p}$, avec $u \in A^\times$ et les $a_p \in \mathbb{Z}$ tous nuls sauf un nombre fini.
(3) Soit $\mathcal{P}$ comme dans la définition. Alors $\mathcal{P}$ contient un et un seul élément de chaque classe d'association d'éléments irréductibles de A. Aussi, si $\mathcal{P}'$ est un ensemble d'éléments de A contenant un représentant de chaque classe d'association d'éléments irréductibles de A et rien d'autre, $\mathcal{P}'$ vérifie aussi les conditions de la définition. On dit qu'un tel $\mathcal{P}'$ est un système minimal de générateurs irréductibles. On dira par la suite « soit $(A, \mathcal{P})$ un anneau factoriel », sous-entendu que A est un anneau factoriel et $\mathcal{P}$ est un système minimal de générateurs irréductibles.

Exemples. Un corps est toujours un anneau euclidien pour le stathme qui vaut 1 sur tout élément non nul. Voici trois types classiques moins triviaux d'anneaux euclidiens :
(1) L'anneau $\mathbb{Z}$. On posera $N(x) = |x|$.
(2) L'anneau $K[X]$ où K est un corps. On posera $N(P) = \deg P + 1$ si $P \neq 0$.
(3) L'anneau $\mathbb{Z}[i] := \{a + ib,\ a, b \in \mathbb{Z}\}$ comme sous-anneau de $\mathbb{C}$. On pose ici $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$.

Il existe une famille importante d'anneaux factoriels, à savoir les anneaux de polynômes à coefficients dans un anneau factoriel.

THÉORÈME 1.2. *Soit A un anneau principal.*

(a) *Le théorème de Bézout fonctionne dans A : si $a, b \in A$ sont premiers entre eux, alors il existe $u, v \in A$ tels que $au + bv = 1$,*

(b) *Dans A, tout idéal premier non nul est maximal.*

Remarques. Dans un anneau factoriel *le théorème de Bézout n'est pas toujours vrai.* Dans $\mathbb{Z}[X]$ [3], par exemple, $P_1 = X$ et $P_2 = X + 2$ sont premiers entre eux, mais tout polynôme de la forme $uP_1 + vP_2$ avec $u, v \in \mathbb{Z}[X]$ aura un terme constant pair quels que soient $u, v \in \mathbb{Z}[X]$.

Dans un anneau factoriel, *un idéal premier non nul n'est pas toujours maximal.* Dans $\mathbb{Z}[X]$, par exemple, l'idéal (X) est premier non nul, mais il est inclus strictement dans $(2, X)$. Et $(2, X)$ est un idéal propre parce qu'il ne contient pas 1, étant l'ensemble des polynômes de $\mathbb{Z}[X]$ dont le terme constant est pair.

THÉORÈME 1.3. *Un anneau euclidien est toujours principal.*

THÉORÈME 1.4. *Un anneau principal est toujours factoriel.*

Contrexemples. Un anneau principal n'est pas forcément euclidien. Un anneau factoriel n'est pas forcément principal. Un anneau commutatif intègre n'est pas forcément factoriel.

Il n'est pas facile de trouver des anneaux principaux non euclidiens. Dans le livre *Cours d'algèbre* de Daniel Perrin, il est montré que $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est principal sans être euclidien (section II.5) ainsi que $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ (exercice 4, page 63).

L'anneau $\mathbb{Z}[X]$ est factoriel, mais il n'est pas principal. L'idéal $(X, 2)$ engendré par X et 2, qui est aussi égal à l'ensemble des polynômes de $\mathbb{Z}[X]$ dont le coefficient constant est pair, n'est pas principal. En effet, supposons par l'absurde que l'idéal $(2, X)$ est principal, engendré par un polynôme $P \in \mathbb{Z}[X]$. Alors P est un polynôme dont le coefficient constant est pair et qui divise 2. Alors $P = \pm 2$, mais ± 2 ne divise pas X. Contradiction.

L'anneau $\mathbb{Z}[i\sqrt{3}] := \{a + bi\sqrt{3},\ a, b \in \mathbb{Z}\}$ est intègre (parce que inclus dans $\mathbb{C}$) mais pas factoriel, puisqu'on a $(1 + i\sqrt{3})(1 - i\sqrt{3}) = 4 = 2 \cdot 2$ alors que $(1 + i\sqrt{3})$, $(1 - i\sqrt{3})$ et 2 sont irréductibles et non associés (exercice 38), donc il n'y a pas unicité de la décomposition de 4.

THÉORÈME 1.5. *Si $(A, \mathcal{P})$ est un anneau factoriel (à plus forte raison si A est principal), alors, si $a = u \prod_{p \in \mathcal{P}} p^{a_p} \in A \backslash \{0\}$ et $b = u' \prod_{p \in \mathcal{P}} p^{b_p} \in A \backslash \{0\}$ avec $u, u' \in A^\times$, on a :*

(a) *$a | b$ si et seulement si $a_p \leq b_p$ pour tout $p \in \mathcal{P}$.*

(b) *$d := \prod_{p \in \mathcal{P}} p^{min(a_p, b_p)}$ est un pgcd de a et b.*

3. Nous admettons que $\mathbb{Z}[X]$ est factoriel. Cela sera prouvé au chapitre 4.

(c) $m := \prod_{p\in\mathcal{P}} p^{max(a_p,b_p)}$ *est un ppcm de* a *et* b.

(d) *Dans* A*, tout élément irréductible est premier.*

(e) *On a dans* A *le lemme de Gauss : soient* $a, b, c \in A$ *tels que* a *divise* bc *mais* a *est premier avec* b*. Alors* a *divise* c*.*

Remarques. Si A est principal, si $m = \text{ppcm}(x, y)$ on a $(x) \cap (y) = (m)$, et si $d = \text{pgcd}(x, y)$ on a $(x, y) = (d)$.

Il existe des anneaux dans lesquels il n'existe pas de pgcd (ppcm). Par exemple, dans l'anneau $\mathbb{R}[X^2, X^3]$ des polynômes dont le coefficient de X est nul, en cherchant un pgcd de X^5 et X^6 on s'aperçoit que les diviseurs de X^5 sont, à un inversible près, $1, X^2$ et X^3, qui divisent tous X^6. Mais X^2 ne divise pas X^3 (ni l'inverse) donc le pgcd ne peut être ni X^2 ni X^3 (ni évidemment 1). On conclut que X^5 et X^6 n'admettent pas de pgcd.

1.10.2. Démonstrations.

Démonstration du théorème 1.2. (a) Rappelons que, si $a, b \in A$, on a $(a, b) = \{ua+vb,\ u, v \in A\}$. Soient a et b premiers entre eux. Posons $(a, b) = (x)$ (A est principal). Comme x divise a et b il doit être inversible. Donc $(x) = A$. Alors $1 \in (a, b)$. Donc 1 s'écrit $ua + vb$.

(b) Soit $I = (p)$ un idéal premier non nul. Donc $p \neq 0$. Si $p|xy$ alors $xy \in I$, donc $x \in I$ ou $y \in I$ donc $p|x$ ou $p|y$. Nous avons trouvé que p est premier. Soit alors $x \notin I$. Alors p ne divise pas x. Donc, parmi les diviseurs non inversibles de p aucun ne divise x, ce qui implique $\text{pgcd}(x, p) = 1$. On peut alors écrire une équation de Bézout $up+vx = 1$ par (a). Cette relation implique que l'idéal (x, p) contient 1, donc $(x, p) = A$. Donc, pour tout $x \notin I$, l'idéal engendré par I et x est égal à A. Donc I est maximal. □

Démonstration du théorème 1.3 (euclidien implique principal). Soit A un anneau euclidien. Soit I un idéal de A et montrons que I est principal. Si $I = \{0\}$ alors $I = (0)$ et il est principal. Si $I \neq \{0\}$, l'image par N de l'ensemble non vide $I\backslash\{0\}$ est une partie non vide de $\mathbb{N}$ et a donc un plus petit élément. Soit alors $x \in I\backslash\{0\}$ qui vérifie : pour tous $y \in I\backslash\{0\}$, on a $N(y) \geq N(x)$. Montrons que $I = (x)$. En effet, si $z \in I\backslash\{0\}$, écrivons $z = qx + r$ avec $N(r) < N(x)$. Mais $r \in I$ car $r = z - qx$ et $x, z \in I$. Par choix de x de stathme minimale, on doit avoir $r = 0$. Donc $x|z$. Ainsi, x divise tous les éléments de I, d'où $I = (x)$. □

Démonstration du théorème 1.4 (principal implique factoriel). Soit A un anneau principal.

Démontrons l'existence de la décomposition. Disons qu'un élément $x \in A$ qui n'est pas inversible est **décomposable** si x est irréductible ou peut s'écrire comme un produit d'éléments irréductibles. Supposons par l'absurde qu'il existe un élément $a \in A$ qui n'est pas décomposable. Puisque a n'est pas irréductible,

il peut s'écrire comme un produit $a = a_1 a_1'$ d'éléments a_1 et a_1' qui ne sont ni inversibles, ni associés à a. Si a_1 et a_2 sont décomposables, alors a l'est. Donc au moins l'un des éléments a_1 et a_1' n'est pas décomposable. Disons que c'est a_1. On a alors $(a) \subsetneq (a_1)$ parce que a_1 divise a et a ne divise pas a_1. On applique le même procédé à (a_1). On construit alors récursivement une suite infinie d'idéaux $(a), (a_1), (a_2), ..., (a_n), ...$ telle que $(a_i) \subsetneq (a_{i+1})$. La réunion de tous ces idéaux est un idéal I de A (facile). Il est engendré par un élément b, parce que A est principal. Alors b appartient à l'un des idéaux (a_k). Mais alors on a $(a_k) \subset (b)$ et $(b) \subset (a_k)$. Donc $I = (a_k)$ et la suite est stationnaire. Contradiction. Il n'existe pas d'élément de A qui ne soit pas décomposable.

Soit C l'ensemble des éléments irréductibles de A. Pour chaque classe d'association dans C choisissons un élément, et soit $\mathcal{P}$ l'ensemble de ces représentants. Puisque tout élément de A se décompose en produit d'éléments inversibles ou irréductibles, il s'ensuit que tout élément de A est associé à un produit d'éléments de $\mathcal{P}$.

Montrons maintenant l'unicité de la décomposition.

LEMME 1.6. *Dans un anneau principal A, tout élément irréductible est premier.*

Démonstration du lemme. Soit $a \in A$ irréductible. Soient $x, y \in A$ tels que $a|xy$. On pose $(a, x) = (m)$, en particulier $m|a$. Comme a est irréductible, m est inversible ou m est associé à a. Si m est associé à a, comme $m|x$, on a $a|x$. Si m est inversible, cela veut dire que $(a, x) = (1)$ et donc il existe $u, v \in A$, $ua + vx = 1$. Alors $uay + vxy = y$, et comme $a|xy$, on a $a|y$. Nous avons prouvé que $a|x$ ou $a|y$. □

Supposons maintenant une égalité $x = u \prod_{i=1}^{k} p_i^{a_i} = u' \prod_{j=1}^{k'} q_j^{b_j}$ avec $u, u' \in A^\times$, $a_i, b_j \in \mathbb{N}^*$ et $p_i \in \mathcal{P}$ distincts et $q_j \in \mathcal{P}$ distincts. On procède par récurrence sur $n := \sum_{i=1}^{k} a_i$. Si $n = 0$, x est inversible et il n'y a pas de q_i car un inversible n'est jamais divisible par un non inversible. L'unicité en découle. Si $n > 1$, alors p_k divise $u' \prod_{j=1}^{k'} q_j^{b_j}$. Par le lemme précédent, p_k est premier, donc il doit diviser l'un des q_j. Comme q_j est irréductible, ils sont associés. Comme on a choisi dans $\mathcal{P}$ un représentant de chaque classe, on a $p_k = q_j$. On simplifie alors l'égalité et on applique l'hypothèse de récurrence. □

Démonstration du théorème 1.5. (a) Si $a|b$, on écrit $b = at$. Alors, si $t = v \prod_{p \in \mathcal{P}} p^{t_p}$, on a $at = uv \prod_{p \in \mathcal{P}} p^{a_p + t_p}$. Par unicité de la décomposition, on doit avoir $uv = u'$ et $a_p + t_p = b_p$, d'où $a_p \leq b_p$ car $t_p \geq 0$. La réciproque est évidente.

(b) et (c) découlent directement de (a).

(d) a déjà été montré (lemme précédent).

(e) Écrivons $c = u'' \prod_{p\in\mathcal{P}} p^{c_p}$. Alors $a|bc$ implique $a_p \leq b_p + c_p$ pour tout p par (a). Mais, si $a_p \neq 0$, alors $b_p = 0$ parce que, sinon, p serait un diviseur commun non inversible de a et b ; alors, quand $a_p \neq 0$, on a $a_p \leq c_p$. Mais, quand $a_p = 0$, on a $a_p = 0 \leq c_p$. Ainsi, $a_p \leq c_p$ pour tout p, et donc $a|c$ par (a). □

1.10.3. Application : étude de l'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés. Cette sous-section utilise le corps $\mathbb{C}$ qui sera officiellement défini au chapitre 2. On note $\mathbb{Q}(i)$ le sous-ensemble de $\mathbb{C}$ formé de nombres complexes $a + ib$ tels que $a, b \in \mathbb{Q}$. Alors $\mathbb{Q}(i)$ est stable par addition et multiplication ; c'est donc un sous-anneau de $\mathbb{C}$. C'est en fait un sous-corps de $\mathbb{C}$ comme on peut le vérifier en écrivant, pour $(a, b) \in \mathbb{Q}\backslash\{(0, 0)\}$,

$$\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} \in \mathbb{Q}(i).$$

On pose :

$$N : \mathbb{Q}(i) \to \mathbb{Q}_+, \qquad N(z = a + ib) := z\bar{z} = a^2 + b^2.$$

On appelle N la **norme** sur $\mathbb{Q}[i]$. Elle est multiplicative au sens où on a $N(zz') = N(z)N(z')$ (facile à vérifier avec la formule $N(z) = z\bar{z}$).

On note $\mathbb{Z}[i]$ le sous-ensemble de $\mathbb{C}$ formé de nombres complexes $a+ib$ tels que $a, b \in \mathbb{Z}$. Il est facile de vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{Q}[i]$. La restriction de la norme N à $\mathbb{Z}[i]$ est une application multiplicative $N : \mathbb{Z}[i] \to \mathbb{N}$. Son image est le sous-ensemble de $\mathbb{N}$ formé des sommes de deux carrés.

THÉORÈME 1.7. (a) *L'anneau $\mathbb{Z}[i]$ est euclidien, donc principal.*

(b) *Le corps des fractions de $\mathbb{Z}[i]$ est $\mathbb{Q}(i)$.*

(c) *Les éléments inversibles de $\mathbb{Z}[i]$ sont les éléments de norme 1, à savoir $\{1, -1, i, -i\}$.*

(d) *Un nombre premier $p \in \mathbb{N}$ est un élément premier de $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \mod 4$.*

Démonstration. (a) Montrons que N est un stathme pour $\mathbb{Z}[i]$. Soient $a, b \in \mathbb{Z}[i]$ tels que $b \neq 0$. Soit $x := \frac{a}{b} \in \mathbb{C}$. Écrivons $x = u + iv$. Tout nombre réel est a distance de au plus $\frac{1}{2}$ d'un entier. Posons alors $q := u' + iv'$ tel que u' et v' sont des entiers et $|u' - u| \leq 1/2$, $|v' - v| \leq 1/2$. On a alors une écriture $a = qb + r$, où $q \in \mathbb{Z}[i]$ et $r := a - bq \in \mathbb{Z}[i]$. Puisque $a = bx = bq + r$, on a $r = b(x - q)$, donc $N(r) = N(b)N(x - q)$. Comme $N(x - q) < 1$ puisque $(u - u')^2 + (v - v')^2 \leq 1/2$, on a $N(r) < N(b)$.

(b) On a vu que $\mathbb{Q}(i)$ était un corps, et il est évident que $\mathbb{Z}[i] \subset \mathbb{Q}(i)$. Il est immédiat que tout élément de $\mathbb{Q}(i)$ est le quotient de deux éléments de $\mathbb{Z}[i]$ (même d'un élément de $\mathbb{Z}[i]$ par un entier de $\mathbb{Z}$), ce qui achève la preuve.

(c) Si z est de norme 1, on a $z\bar{z} = 1$. Comme $z \in \mathbb{Z}[i]$ implique $\bar{z} \in \mathbb{Z}[i]$ on a que z est inversible dans $\mathbb{Z}[i]$. Réciproquement, si $z \in \mathbb{Z}[i]^\times$, alors il existe $u \in \mathbb{Z}[i]$ tel que $zu = 1$. Mais la norme étant multiplicative, $N(zu) = 1$ implique

$N(z)N(u) = 1$ et, comme les deux sont des entiers positifs, $N(z) = N(u) = 1$. D'où $z = a + ib$, avec soit $a = \pm 1$ et $b = 0$, soit $a = 0$ et $b = \pm 1$.

(d) Soit $p \in \mathbb{N}$ premier tel que $p \equiv 3 \mod 4$. Supposons par l'absurde que p n'est pas premier dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est principal, p n'est pas irréductible. Écrivons $p = zu$, avec z et u non inversibles, donc $N(z) > 1$ et $N(u) > 1$. On a $p^2 = N(p) = N(z)N(u)$. Comme cette relation a lieu dans $\mathbb{N}$, et que p est premier, on doit avoir $p = N(z) = N(u)$. Mais une norme $N(z)$ est une somme de deux carrés, qui ne peut *jamais* être congrue à 3 modulo 4 (un carré est congru à 0 ou 1 modulo 4). Donc p est irréductible ; il est alors premier, parce que l'anneau $\mathbb{Z}[i]$ est principal par (a).

Si $p = 2$, on voit que $p = (1 + i)(1 - i)$ et que $N(1 + i) = N(1 - i) = 2$, ce qui implique que $1 + i$ et $1 - i$ ne sont pas inversibles ; donc 2 n'est pas premier.

Soit maintenant $p \in \mathbb{Z}$ premier tel que $p \equiv 1 \mod 4$. $\mathbb{Z}/p\mathbb{Z}$ est un corps, et l'équation $x^{-1} = x$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, qui équivaut à $x^2 = 1$, a pour solutions $\bar{1}$ et $-\bar{1}$. Alors le produit de tous les éléments du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ vaut $-\bar{1}$, parce que à part $\pm\bar{1}$ chaque élément se regroupe avec son inverse. En passant dans $\mathbb{Z}$, cela se traduit par *la relation de Wilson* $p|(p-1)! + 1$.

Puisque $p - k \equiv -k \mod p$, on a

$$(p-1)! \equiv (1 \times 2 \times ... \times \frac{p-1}{2})((-1) \times (-2) \times ... \times (-\frac{p-1}{2})) \mod p.$$

Puisque le nombre de signes moins est pair parce que $p \equiv 1 \mod 4$, cela vaut aussi $((\frac{p-1}{2})!)^2 \mod p$. Ainsi, il existe $y \in \mathbb{N}$ tel que $(p-1)! \equiv y^2 \mod p$ ($y = (\frac{p-1}{2})!$). Alors la relation de Wilson implique p divise $y^2 + 1$ dans $\mathbb{Z}$; donc dans $\mathbb{Z}[i]$. Mais dans $\mathbb{Z}[i]$ on peut alors écrire $p|(y + i)(y - i)$. Supposons par l'absurde que p est premier dans $\mathbb{Z}[i]$. Alors p divise $y + i$ ou $y - i$. Mais $p(a + ib) = pa + ipb$, et pb ne peut être égal ni à 1, ni à -1. Donc p ne divise ni $y + i$, ni $y - i$. Donc p n'est pas un élément premier de $\mathbb{Z}[i]$. □

COROLLAIRE 1.8. **(Le théorème des deux carrés)**. *Soit $p \in \mathbb{Z}$ un nombre premier. p s'écrit comme somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.*

Démonstration. Si $a, b \in \mathbb{Z}$, alors $a^2 + b^2$ est toujours congru à 0, 1 ou 2 modulo 4. Donc, si $p \equiv 3 \mod 4$, il n'est pas une somme de deux carrés.

Si $p = 2$, on a $p = 1^2 + 1^2$.

Si $p \equiv 1 \mod 4$, on a vu que p n'était pas un élément premier de $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est principal, p est réductible. Écrivons $p = zu$ avec z, u non inversibles, donc $N(z) > 1$ et $N(u) > 1$. On a $p^2 = N(p) = N(z)N(u)$. Comme dans $\mathbb{N}$ l'élément p est premier, on doit avoir $p = N(z) = N(u)$. Une norme $N(z)$ ($z \in \mathbb{Z}[i]$) est toujours une somme de deux carrés par définition, donc p est une somme de deux carrés. □

Chapitre 2

Le corps $\mathbb{C}$ et l'anneau $\mathbb{H}$ des quaternions

2.1. Construction de $\mathbb{C}$. Racines n-ièmes

2.1.1. Construction de $\mathbb{C}$. Le $\mathbb{R}$-espace vectoriel $\mathbb{R}^2$ est de dimension 2. On note $(1, i)$ sa base canonique, de sorte que tout élément z de $\mathbb{R}^2$ s'écrira de façon unique sous la forme $z = a + bi$ avec $a, b \in \mathbb{R}$. On dit que a est la **partie réelle de** z, notée $\Re(z)$, et b est la **partie imaginaire de** z, notée $\Im(z)$. On définit une multiplication sur $\mathbb{R}^2$ de la façon suivante : on pose d'abord que $1 \times 1 = 1$, $1 \times i = i \times 1 = i$ et $i \times i = -1$; ensuite, cette multiplication s'étend de façon unique à $\mathbb{R}^2$ si on impose qu'elle soit distributive par rapport à l'addition. On obtient une multiplication commutative qui vérifie $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, et dont l'élément neutre est 1. On laisse en exercice la vérification du fait que cette multiplication est aussi associative, et qu'on obtient sur $\mathbb{R}^2$ une structure d'anneau. On note $\mathbb{C}$ l'anneau obtenu. Les éléments $z = a + bi$ tels que $b = 0$ forment un sous-corps de $\mathbb{C}$ qu'on identifie avec $\mathbb{R}$ (si cette affirmation vous pose problème, voir la proposition 3.1). On écrit $a + bi$ aussi sous la forme $a + ib$ quand cela nous arrange (puisque cette écriture facilite la lecture de la forme trigonométrique définie plus loin).

Si $z \in \mathbb{C}$, $z = a+bi$, on pose $\bar{z} = a-bi$. Il est facile de vérifier que $z \mapsto \bar{z}$ est un automorphisme de l'anneau $\mathbb{C}$, appelé **conjugaison complexe** ou parfois simplement **conjugaison** quand il est clair de quoi il s'agit. On appelle $\bar{z}$ le **conjugué** de z. Le conjugué du conjugué de z est toujours z.

On définit l'application **module** $|\ | : \mathbb{C} \to \mathbb{R}_+$ par la formule

$$|a + ib| := \sqrt{a^2 + b^2}.$$

On a alors $|z| := \sqrt{z\bar{z}}$ pour tout $z \in \mathbb{C}$. On voit facilement alors que $|z| = 0$ si et seulement si $z = 0$ et que $|zz'| = |z||z'|$ pour tous $z, z' \in \mathbb{C}$. En particulier, on a que tout élément z non nul de $\mathbb{C}$ est inversible, et son inverse est $\frac{\bar{z}}{|z|^2}$. Donc $\boxed{\mathbb{C} \textit{ est un corps}}$. Notons l'inégalité dite « triangulaire » $|z+z'| \leq |z|+|z'|$ pour tous $z, z' \in \mathbb{C}$, et sa version $|z + z'| \geq |z| - |z'|$. L'application module $z \mapsto |z|$ induit par restriction un morphisme de groupes surjectif de $\mathbb{C}^\times$ dans $\mathbb{R}_+^*$.

Un élément de $\mathbb{C}$ s'appelle **nombre complexe**, et $\mathbb{C}$ est le **corps des nombres complexes**.

2.1.2. Forme trigonométrique. Si θ est un nombre réel, le nombre complexe $z = \cos(\theta) + i\sin(\theta)$ est de module 1. Réciproquement, un résultat d'analyse nous dit que, si a, b sont deux nombres réels tels que $a^2 + b^2 = 1$, alors il existe un et un seul nombre réel $\theta \in [0, 2\pi[$ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$. Maintenant, tout nombre complexe z non nul s'écrit de façon unique sous la forme rz', où $r \in \mathbb{R}_+^*$ et $|z'| = 1$. En effet, pour montrer l'existence d'une telle écriture il suffit de poser $r := |z|$ et $z' := \frac{z}{|z|}$, et pour montrer l'unicité on remarque qu'une telle écriture $z = rz'$ implique $|z| = r$ en passant aux modules ; ensuite, évidemment, $z' = \frac{z}{r} = \frac{z}{|z|}$. Quand on écrit $z = r(\cos(\theta) + i\sin(\theta))$, on dit qu'on a écrit z **sous forme trigonométrique**. On dit que θ est un **argument** de z. Si θ est un argument de z, les autres arguments de z s'obtiennent de θ en ajoutant des multiples entiers de 2π. On note parfois le nombre $\cos(\theta) + i\sin(\theta)$ par $e^{i\theta}$.

L'avantage non négligeable d'écrire les nombres complexes sous forme trigonométrique est le suivant : les formules trigonométriques classiques pour le sinus d'une somme et le cosinus d'une somme montrent que, quels que soient $\theta, \theta' \in \mathbb{R}$, on a

$$(\cos(\theta) + i\sin(\theta))(\cos(\theta') + i\sin(\theta')) = \cos(\theta + \theta') + i\sin(\theta + \theta').$$

Aussi, $e^{i\theta}e^{i\theta'} = e^{i(\theta+\theta')}$. Si on connaît la forme trigonométrique de deux nombres complexes $z_1 = r_1(\cos(\theta_1) + i\sin(\theta_1))$ et $z_2 = r_2(\cos(\theta_2) + i\sin(\theta_2))$, on a donc la forme trigonométrique de leur produit, $z_1z_2 = r(\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2))$, où $r = r_1r_2$.

Par opposition avec la « forme trigonométrique », on appelle **forme algébrique** d'un nombre complexe son écriture initiale sous la forme $a + bi$.

2.1.3. Racines de l'unité. Si $n \in \mathbb{N}^*$, on appelle **racine n-ième de l'unité** dans $\mathbb{C}$ tout nombre complexe z tel que $z^n = 1$. On appelle **racine de l'unité** tout nombre complexe z tel qu'il existe $n \in \mathbb{N}^*$ tel que z soit une racine n-ième de l'unité.

Si on fixe n et on note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité, alors $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^\times$. Pour le montrer, il suffit de remarquer que

- $1^n = 1$, et
- si z, z' vérifient $z^n = z'^n = 1$ alors $(zz')^n = 1$ et $(z^{-1})^n = 1$.

Nous rappelons la forme trigonométrique des racines n-ièmes de l'unité :

THÉORÈME 2.1. *Si $n \in \mathbb{N}^*$, il existe dans $\mathbb{C}$ exactement n racines n-ièmes de l'unité. Ce sont les nombres complexes $\varepsilon_k := e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$ pour $k = 0, 1, 2, ..., n-1$.*

Démonstration. Les arguments $\frac{2k\pi}{n}$ se trouvent dans $[0, 2\pi[$ et sont distincts. Donc les nombres ε_k qu'ils définissent sont distincts. Par la formule du produit

à partir de la forme trigonométrique on a $\varepsilon_k^n = \cos(2k\pi) + i\sin(2k\pi) = 1$. Réciproquement, supposons qu'un nombre complexe z vérifie $z^n = 1$. Alors $|z|^n = 1$ et donc $|z| = 1$. On peut donc écrire z sous forme trigonométrique $e^{i\theta}$, avec $\theta \in [0, 2\pi[$. Donc $z^n = e^{in\theta}$. Comme $z^n = 1$, on a $n\theta = 2k\pi$, où k est un nombre entier. Donc $\theta = \frac{2k}{n}\pi$. Puisque $\theta \in [0, 2\pi[$, on a $k \in \{0, 1, 2, ..., n-1\}$. □

Les racines de l'unité ont beaucoup de propriétés importantes, dont la preuve sera posée en exercice.

2.1.4. Racines n-ièmes. Soit $n \in \mathbb{N}^*$. Si r est un nombre réel strictement positif, alors il existe un et un seul nombre réel strictement positif a tel que $a^n = r$, et ce nombre est appelé **racine n-ième de** r et noté $\sqrt[n]{r}$ – c'est un résultat d'analyse réelle admis ici (et démontré grâce à l'existence d'une borne sup pour les ensembles non vides bornés de $\mathbb{R}$). Basé sur ce résultat d'analyse réelle et sur le théorème 2.1 voici le résultat pour $\mathbb{C}$:

THÉORÈME 2.2. *Soit z un nombre complexe non nul, de forme trigonométrique $z = r(\cos(\theta) + i\sin(\theta))$. Alors il existe exactement n nombres complexes distincts dont la puissance n-ième vaut z. Ces nombres sont $z_0, z_1, ..., z_{n-1}$, où $z_k = \sqrt[n]{r}(\cos(\frac{\theta+2k\pi}{n}) + i\sin(\frac{\theta+2k\pi}{n}))$.*

Démonstration. On a bien $z_0^n = r(\cos(\theta) + i\sin(\theta)) = z$. On a également $z_k = z_0\varepsilon_k$ pour tout $k = 1, 2, ..., n-1$, où ε_k est la racine n-ième de l'unité définie au théorème 2.1. Alors $z_k^n = z_0^n\varepsilon_k^n = z$; de plus, si $i \neq j$, on a $z_i \neq z_j$ parce que $\varepsilon_i \neq \varepsilon_j$.

Réciproquement, si u est un nombre complexe tel que $u^n = z$, alors le nombre complexe $\varepsilon := \frac{u}{z_0}$ vérifie $\varepsilon^n = \frac{z}{z} = 1$. Par le théorème 2.1, il existe $k \in \{0, 1, 2, ..., n-1\}$ tel que $\frac{u}{z_0} = \varepsilon_k$, et donc $u = z_0\varepsilon_k$, d'où $u = z_k$. □

Les nombres complexes dont la puissance n-ième vaut z s'appellent **racines complexes n-ièmes de** z. Parfois, si z est un nombre complexe, on note $\sqrt[n]{z}$ une racine n-ième de z, en précisant qu'il s'agit d'*une* racine n-ième de z. Les racines 2-ièmes et 3-ièmes s'appellent aussi racines « carrées » et respectivement « cubiques ». Une racine n-ième au sens général (sans qu'un n soit fixé) s'appelle « radical ».

2.2. Équations de degré deux, trois et quatre

Chercher les racines d'un polynôme $P(X) = \sum_{i=0}^{n} a_i X^i$ de degré $n \geq 1$ se dit aussi « résoudre l'équation $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$ de degré n en (l'inconnue) x ». La terminologie « équation » est plus générale, le genre d'équation cité ici étant « polynomial ». Quand l'équation à résoudre

est de degré deux, on l'appelle aussi « équation du second degré ». Dans la suite de cette section nous montrons comment on obtient des formules avec des radicaux pour les racines des polynômes de degré deux, trois et quatre à coefficients dans $\mathbb{C}$. Plus précisément, pour chaque $n = 2, 3, 4$ on verra des formules générales basées sur les opérations élémentaires (addition, soustraction, multiplication, division) et aussi faisant intervenir des racines carrées et cubiques, telles que, si on injecte dans la formule les coefficients du polynôme, on obtient à la sortie les racines du polynôme. Ce genre de formule n'existe pas pour des polynômes de degré cinq ou plus (théorème d'Abel-Ruffini), et ce résultat difficile (d'inexistence) sera montré vers la fin de ce livre grâce à la théorie de Galois. Noter que les racines d'un polynôme P sont les mêmes que les racines du polynôme obtenu de P en divisant par son coefficient dominant, c'est pourquoi nous allons nous concentrer exclusivement sur des polynômes de coefficient dominant égal à 1.

2.2.1. L'équation du second degré. Soit $P(X) = X^2 + aX + b$ un polynôme à coefficients dans $\mathbb{C}$. On pose $\Delta := a^2 - 4b$ (Δ est le **discriminant** de P). Soit $\sqrt{\Delta}$ une racine carrée de Δ dans $\mathbb{C}$. On pose $x_1 := \frac{1}{2}(-a + \sqrt{\Delta})$ et $x_2 := \frac{1}{2}(-a - \sqrt{\Delta})$. Alors $P(X) = (X - x_1)(X - x_2)$ (vérification facile). Puisque $\mathbb{C}$ est intègre, P s'annule en un nombre complexe x si et seulement si $x = x_1$ ou $x = x_2$.

Les nombres complexes x_1 et x_2 sont confondus si et seulement si $\Delta = 0$. Donc P a deux racines complexes si $\Delta \neq 0$ et une seule si $\Delta = 0$. Quand a et b sont réels, on voit que x_1 et x_2 sont tous les deux réels si $\Delta \geq 0$, et non réels conjugués si $\Delta < 0$.

La formule $P(X) = (X - x_1)(X - x_2)$ montre que $a = -(x_1 + x_2)$ et $b = x_1 x_2$, et permet de répondre à la **question :** peut-on trouver deux nombres complexes dont on connaît la somme s et le produit p ? **Réponse :** oui, ces nombres existent et sont forcément les nombres x_1 et x_2 associés comme plus haut au polynôme $P(X) = X^2 - sX + p$.

Exemple. On veut trouver deux nombres complexes dont la somme et le produit valent 1. Par ce qui précède, ce sont les racines du polynôme $X^2 - X + 1$. Il s'agit de

$$x_1 = \frac{1 + i\sqrt{3}}{2} \qquad \text{et} \qquad x_2 = \frac{1 - i\sqrt{3}}{2}.$$

Aussi, *si a, b, c, d sont des nombres complexes tels que $a+b = c+d$ et $ab = cd$ (même somme et même produit), alors $\{a, b\} = \{c, d\}$*. En effet, si la somme est s et le produit est p, il s'agit forcément des racines de $P(X) = X^2 - sX + p$.

2.2.2. L'équation du troisième degré. Soit $P \in \mathbb{C}[X]$ le polynôme $P(X) = X^3 + aX^2 + bX + c$. On peut alors écrire P sous la forme $P(X) = (X + \frac{a}{3})^3 - \frac{a^2}{3}X - \frac{a^3}{27} + bX + c$. En posant $X = Y - \frac{a}{3}$ dans la formule

de P, on obtient un polynôme $Y^3 - \frac{a^2}{3}(Y - \frac{a}{3}) - \frac{a^3}{27} + b(Y - \frac{a}{3}) + c$ en Y, dont le coefficient de Y^2 est manifestement nul. Or, si on sait calculer les racines de ce polynôme, on sait en obtenir celles de P (en soustrayant $\frac{a}{3}$). Autrement dit, il suffit d'avoir des formules pour les racines de tout polynôme unitaire de degré trois en X dont le coefficient de X^2 est nul pour en déduire des formules pour les racines de tout polynôme de degré trois. Supposons donc que $a = 0$ et cherchons les racines du polynôme $P(X) = X^3 + bX + c$.

Supposons d'abord que $b = 0$. Alors les racines de P sont les racines 3-ièmes de $-c$. Laissons donc de côté ce cas, et supposons par la suite que $b \neq 0$.

L'idée est de partir de l'identité $(u + v)^3 = u^3 + v^3 + 3uv(u + v)$, vraie pour tout couple de nombres complexes u, v. Si on pose $x = u + v$ on a $x^3 = u^3 + v^3 + 3uvx$. Cela montre que, si on trouve u et v tels que $3uv = -b$ et $u^3 + v^3 = -c$, alors $P(u + v) = 0$ et on aura trouvé une racine de P.

Partons à la recherche de u et v tels que $3uv = -b$ et $u^3 + v^3 = -c$. Posons $u^3 = U$ et $v^3 = V$. On sait alors grâce à la sous-section précédente (« L'équation du second degré ») trouver U et V tels que $UV = -\frac{1}{27}b^3$ et $U + V = -c$: U et V sont les solutions de $t^2 + ct - \frac{1}{27}b^3$. On sait les calculer dans $\mathbb{C}$ (puisque c'est une équation du second degré en t) : il s'agit de

$$U = -\frac{c}{2} + \frac{1}{2}\sqrt{\frac{1}{27}(27c^2 + 4b^3)} \qquad \text{et} \qquad V = -\frac{c}{2} - \frac{1}{2}\sqrt{\frac{1}{27}(27c^2 + 4b^3)}.$$

où $\sqrt{\frac{1}{27}(27c^2 + 4b^3)}$ désigne une racine carrée de $\frac{1}{27}(27c^2 + 4b^3)$ dans $\mathbb{C}$. Notons u une racine cubique de U dans $\mathbb{C}$. Puisque $UV = -\frac{1}{27}b^3$ et b est non nul, on a $U \neq 0$ et donc $u \neq 0$. Posons $v := \frac{-b}{3u}$. Alors v est une racine cubique de V dans $\mathbb{C}$. Maintenant u et v vérifient effectivement les relations voulues $3uv = -b$ et $u^3 + v^3 = -c$ et donc $x_1 := u + v$ est une racine de P. On peut trouver deux autres formules qui donnent en général les deux « autres » racines (mais qui peuvent être confondues), en posant $j = e^{\frac{2\pi i}{3}}$ (racine cubique de l'unité) : ce sont $x_2 = ju + \frac{-b}{3ju} = ju + j^2v$ et $x_3 = j^2u + \frac{-b}{3j^2u} = j^2u + jv$.

Les formules trouvées marchent aussi quand $b = 0$, au sens suivant : quand $b = 0$ on a soit $U = 0$ et $V = -c$, soit $U = -c$ et $V = 0$. Les racines de $P(X) = X^3 + c$, qui sont alors les racines cubiques de $-c$, sont encore des sommes d'une racine cubique de U et une racine cubique de V.

Par un calcul à partir des formules de x_1, x_2 et x_3 on obtient

$$(X - x_1)(X - x_2)(X - x_3) = X^3 - 3uvX - (u^3 + v^3) = P(X).$$

Donc $P(x_1) = P(x_2) = P(x_3) = 0$, et $P(x) \neq 0$ pour tout $x \in \mathbb{C}\backslash\{x_1, x_2, x_3\}$.

On pose $\Delta := -(4b^3 + 27c^2)$

On peut vouloir savoir combien de racines distinctes a P dans $\mathbb{C}$. La réponse est la suivante : *quand $\Delta \neq 0$, P a trois racines distinctes ; quand $\Delta = 0$, P a une seule racine si $b = c = 0$ et deux sinon.* Montrons-le.

Quand $b = c = 0$, la seule racine est 0 et on a par ailleurs $\Delta = 0$. Quand $b = 0$ et $c \neq 0$, P a trois racines distinctes puisque $-c$ a trois racines cubiques distinctes dans $\mathbb{C}$, et clairement $\Delta \neq 0$. Supposons pour ce paragraphe et le suivant que $b \neq 0$. Les nombres x_1, x_2, x_3 ont été définis par des sommes $u+v$, $u'+v'$ et respectivement $u''+v''$, avec les relations $uv = u'v' = u''v'' = -\frac{b}{3}$. S'il y a deux qui sont égaux, par exemple $x_1 = x_2$, alors u et v ont la même somme et le même produit que u' et v'. La discussion faite ci-dessus à la sous-section « L'équation du second degré » montre que $\{u, v\} = \{u', v'\}$. Or, on a aussi $u \neq u'$ parce que $U \neq 0$ (en effet, $U = 0$ implique $b = 0$), donc on en déduit $u = v'$. Alors $u^3 = v'^3$, donc $U = V$. Il s'ensuit que $\Delta = 0$. Donc, *si deux nombres parmi x_1, x_2 et x_3 sont égaux, alors* $\Delta = 0$. Dans ce cas, il ne se peut pas que les trois soient égaux. En effet, par le même raisonnement plus haut on devrait avoir $u = v'$ et $u = v''$, d'où $v' = v''$, soit $V = 0$. Mais $V = 0$ implique $b = 0$, et on a supposé que ce n'était pas le cas.

Montrons la réciproque, à savoir que, si $\Delta = 0$, alors deux parmi les nombres x_1, x_2, x_3 sont égaux. En effet, si $\Delta = 0$, on a $U = V$. On peut écrire $u' = ju$ et $u'' = j^2u$, et alors de $uv = u'v' = u''v''$ on en déduit $v' = j^2v$ et $v'' = jv$. Les trois nombres x_1, x_2, x_3 sont alors $u + v$, $ju + j^2v$ et $j^2u + jv$. De $U = V$ on a que v est égal soit à u, soit à ju, soit à j^2u. Dans le premier cas on a $x_2 = x_3$, dans le deuxième cas on a $x_1 = x_2$ et dans le troisième cas on a $x_1 = x_3$.

Le nombre complexe $\Delta := -(4b^3 + 27c^2)$ s'appelle **discriminant** du polynôme (ou de l'équation associée), et joue un rôle analogue au Δ de l'équation du second degré pour l'équation du troisième degré. Il sera montré en exercice que, si notre polynôme P a des coefficients réels, alors le signe de Δ nous dit combien de racines réelles a P. On verra plus tard une définition générale du discriminant, comme le résultant d'un polynôme et de sa dérivée.

2.2.3. L'équation du quatrième degré. Soit P un polynôme unitaire de degré 4, $P(X) = X^4 + \alpha X^3 + \beta X^2 + \gamma X + \delta$. Si on pose $X = Y - \frac{1}{4}a$, on a $P(X) = Q(Y)$ avec Q un polynôme unitaire de degré 4 dont le coefficient de Y^3 est nul. Si on donne des formules pour les racines de Q on en déduit par translation avec $-\frac{1}{4}a$ les racines de P. C'est pourquoi, à partir de maintenant *on cherche les racines d'un polynôme P de la forme* $P(X) = X^4 + aX^2 + bX + c$.

L'idée est d'écrire $P(X)$ comme une différence de deux carrés, sous la forme $P(X) = (X^2 + \alpha)^2 - (\beta X + \gamma)^2$, ce qui mènerait à deux équations du second degrés données par $x^2 + \alpha = \pm(\beta x + \gamma)$. Or, pour tout $u \in \mathbb{C}$ on a

$$P(X) = (X^2 + \frac{u}{2})^2 - \Big((u - a)X^2 - bX + (\frac{u^2}{4} - c)\Big).$$

On veut donc choisir u de façon à ce que la grosse parenthèse soit le carré d'un polynôme, ce qui équivaut à ce que son discriminant (en tant que équation du second degré) soit nul. Or, ce discriminant est nul si et seulement si on a

$b^2 = 4(u-a)(\frac{u^2}{4} - c)$. On reconnaît là une équation du troisième degré en u qui a une solution, que nous notons u_0, donnée par des racines carrées et cubiques grâce à la théorie de l'équation du troisième degré de la sous-section précédente. Alors on s'est ramené à

$$(x^2 + \frac{u_0}{2})^2 = (u_0 - a)(x - t)^2,$$

où $t = \frac{b}{2(u_0-a)}$. Si m est une racine carrée de $u_0 - a$ dans $\mathbb{C}$, l'équation initiale est équivalente à : $x^2 + \frac{u_0}{2} = m(x-t)$ ou $x^2 + \frac{u_0}{2} = -m(x-t)$, qui sont deux équations du second degré en x qu'on sait résoudre par des formules. Les quatre racines (pas forcément distinctes) peuvent donc être exprimées à partir des coefficients initiaux à l'aide de sommes, produits, soustractions, divisions et racines carrées et cubiques, puisque ce sont les opérations qu'on a utilisées à chaque étape de l'algorithme.

2.3. $\mathbb{C}$ est algébriquement clos

Dans cette section on montre que tout polynôme $P \in \mathbb{C}[X]$ non constant a au moins une racine dans $\mathbb{C}$. On dit qu'un tel corps est **algébriquement clos**, mais il en existe dans la littérature d'autres définitions équivalentes comme il sera vu plus tard.

Si $Z = (z_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{C}$, on dit que Z **converge** (dans $\mathbb{C}$) si les suites réelles $(\Re(z_n))_{n\in\mathbb{N}}$ et $(\Im(z_n))_{n\in\mathbb{N}}$ convergent dans $\mathbb{R}$, et alors la **limite** de la suite Z est par définition $a + ib$ où $a = \lim\limits_{n\to\infty} \Re(z_n)$ et $b = \lim\limits_{n\to\infty} \Im(z_n)$. On note cette limite $\lim\limits_{n\to\infty} z_n$. On a $\lim\limits_{n\to\infty} z_n = z$ si et seulement si dans $\mathbb{R}$ on a $\lim\limits_{n\to\infty} |z - z_n| = 0$.

Nous allons admettre le lemme suivant, qui dit en somme que les fonctions polynômiales non constantes de $\mathbb{C}$ dans $\mathbb{C}$ sont continues et tendent vers l'infini quand la variable complexe tend vers l'infini. La démonstration n'est pas difficile, mais nous voulons éviter d'alourdir cette section avec des notions qui ne seront pas utilisées ailleurs.

Lemme 2.3. *Soit $P \in \mathbb{C}[X]$ un polynôme non constant (vu ici comme fonction de $\mathbb{C}$ dans $\mathbb{C}$).*

(a) *Si $Z = (z_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{C}$ telle que $\lim\limits_{n\to\infty} z_n = z$, alors on a $\lim\limits_{n\to\infty} P(z_n) = P(z)$.*

(b) *Quel que soit $M \in \mathbb{R}$, il existe $R \in \mathbb{R}$ tel que $\max(|\Re(z)|, |\Im(z)|) > R$ implique $|P(z)| > M$.*

Théorème 2.4. *Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Alors P a au moins une racine dans $\mathbb{C}$.*

Démonstration. Posons $P(X) = \sum_{j=0}^{n} a_j X^j$. Par le lemme, il existe R tel que, si $\max(|\Re(z)|, |\Im(z)|) \geq R$, alors on a $|P(z)| \geq |a_0| = |P(0)|$. En particulier, si $K := \{z, |\Re(z)| \leq R, |\Im(z)| \leq R\}$ on a $\inf_{z\in\mathbb{C}} |P| = \inf_{z\in K} |P|$, car $0 \in K$.

Montrons que $\inf_{z\in K} |P|$ est atteint en un point de K. Soit (z_n) une suite contenue dans K telle que

$$\lim_{n\to\infty} |P(z_n)| = \inf_{z\in K} |P|.$$

De la suite réelle $(\Re(z_n))$ (incluse dans l'intervalle fermé borné $[-R, R]$) on peut extraire une sous-suite convergente $(\Re(z_{\sigma(n)}))$ de limite $a \in [-R, R]$; de la sous-suite correspondante $(\Im(z_{\sigma(n)}))$ de $(\Im(z_n))$ (incluse aussi dans $[-R, R]$) on peut extraire une sous-suite convergente $(\Im(z_{\sigma(\tau(n))}))$ de limite $b \in [-R, R]$. On pose $u_n = \Re(z_{\sigma(\tau(n))}) + i\Im(z_{\sigma(\tau(n))})$. Alors la limite de la suite complexe (u_n) est le nombre complexe $a+bi$, et par le (b) du lemme on a $|P(a+bi)| = \lim_{n\to\infty} |P(u_n))|$. Mais, comme u_n est une sous-suite de z_n, on a aussi $\lim_{n\to\infty} |P(u_n)| = \inf_{z\in K} |P|$. Donc $|P(a + bi)| = \inf_{z\in K} |P| = \inf_{z\in\mathbb{C}} |P|$.

Montrons maintenant que $\inf_{z\in K} |P| = 0$. Quitte à remplacer $P(z)$ par $P(z + a + bi)$, on peut supposer que le inf est touché en 0. C'est donc $|a_0|$. Si $a_0 = 0$ on a fini, car $P(0) = 0$. Supposons par l'absurde que $a_0 \neq 0$. Quitte à multiplier P par $\frac{1}{a_0}$ on peut supposer que $a_0 = 1$. En notant k le plus petit entier strictement positif tel que le coefficient de X^k dans P est non nul, on peut écrire $P(z) = 1 + a_k z^k + a_{k+1} z^{k+1} + ... + a_n z^n$, avec $a_k \neq 0$. Avec nos suppositions, on a $|P(z)| \geq 1$ pour tout $z \in \mathbb{C}$. Nous montrerons que cela mène à une contradiction, en prouvant que, si on approche 0 par la bonne direction, alors on peut trouver une valeur de P de module strictement inférieur à 1. On note x une racine k-ième de $-\frac{1}{a_k}$ et on pose $x_n = \frac{x}{n}$ pour $n \in \mathbb{N}^*$. Alors on a

$$P(x_n) = 1 - \big(\frac{1}{n}\big)^k + \big(\frac{1}{n}\big)^{k+1} Q(\frac{1}{n}),$$

où Q est un polynôme à coefficients complexes. Par le (a) du lemme on a

$$\lim_{n\to\infty} \frac{1}{n} Q(\frac{1}{n}) = 0,$$

parce que la limite de $Q(\frac{1}{n})$ est $Q(0)$.

Soit n assez grand pour que $\frac{1}{n}|Q(\frac{1}{n})| < \frac{1}{2}$. Alors

$$|P(x_n)| \leq |1 - \big(\frac{1}{n}\big)^k| + \big|\big(\frac{1}{n}\big)^{k+1} Q\big(\frac{1}{n}\big)\big| = 1 - \big(\frac{1}{n}\big)^k + \big(\frac{1}{n}\big)^k \big|\frac{1}{n} Q(\frac{1}{n})\big|$$

$$\leq 1 - \big(\frac{1}{n}\big)^k + \frac{\big(\frac{1}{n}\big)^k}{2} = 1 - \frac{\big(\frac{1}{n}\big)^k}{2} < 1.$$

Il existe donc z tel que $|P(z)| < 1$. Contradiction. □

Remarque. On pourrait croire que ce résultat implique l'existence d'une racine n-ième de tout nombre complexe z, en posant $P(X) = X^n - z$. Mais la démonstration que nous en avons donnée utilise à un certain moment l'existence d'une telle racine. C'est pourquoi nous avons dû traiter les racines n-ièmes avant, par la forme trigonométrique. Par ailleurs, il est étonnant de voir à quelle point l'idée que la preuve la plus rapide de « $\mathbb{C}$ est algébriquement clos » serait par le théorème de Liouville en analyse complexe. En effet, ce dernier est plus difficile à démontrer, et sa démonstration la plus simple ne fait que reproduire la présente preuve de « $\mathbb{C}$ est algébriquement clos » en plus compliqué.

2.4. L'anneau $\mathbb{H}$ des quaternions

Soit $\mathbb{H}$ le $\mathbb{R}$-espace vectoriel $\mathbb{R}^4$. On note $1, i, j, k$ la base canonique de $\mathbb{H}$. Un élément $z \in \mathbb{H}$, donné par $z = (a, b, c, d)$ dans cette base, s'écrira sous la forme $z = a + bi + cj + dk$. On définit une multiplication distributive par rapport à l'addition sur $\mathbb{H}$ en décrétant que

* 1 est élément neutre, en particulier $1 \times 1 = 1$, $1 \times i = i \times 1 = i$, $1 \times j = j \times 1 = j$ et $1 \times k = k \times 1 = k$.
* $i^2 = j^2 = k^2 = -1$.
* $ij = k$, $ji = -k$, $jk = i$, $kj = -i$ et $ki = j$, $ik = -i$.

(Pour se rappeler les formules de la dernière ligne pensez que $ij = k$, $jk = i$ et $ki = j$ respectent des permutations circulaires de i, j, k.)
Posons $(a + bi + cj + dk)(a' + b'i + c'j + d'k) = A + Bi + Cj + Dk$. Alors $A = aa' - bb' - cc' - dd'$, $B = ab' + ba' + cd' - dc'$, $C = ac' + a'c - bd' + db'$ et $D = ad' + da' + bc' - cb'$. Nous ne vérifions pas que la multiplication est associative et prions le lecteur de nous croire.

On identifie $\mathbb{R}$ à la partie $\{(a, 0, 0, 0), a \in \mathbb{R}\}$ de $\mathbb{H}$ via l'isomorphisme $a \mapsto (a, 0, 0, 0)$ et on voit $\mathbb{R}$ comme un sous-corps de $\mathbb{H}$ (si cette affirmation vous pose problème, voir la proposition 3.1). $\mathbb{R}$ est alors le centre de $\mathbb{H}$, c'est-à-dire l'ensemble des éléments de $\mathbb{H}$ qui commutent avec tous les éléments de $\mathbb{H}$.

Si $z \in \mathbb{H}$, $z = a + bi + cj + dk$, on pose $\bar{z} = a - bi - cj - dk$. On pose $N : \mathbb{H} \to \mathbb{R}_+$ définie par $N(a+bi+cj+dk) = \sqrt{a^2 + b^2 + c^2 + d^2}$. L'application N s'appelle **norme**. On a aussi $N(z) = \sqrt{z\bar{z}} = \sqrt{\bar{z}z}$ (a priori $z\bar{z}$ est un élément de $\mathbb{H}$, et $N(z)$ est un élément de $\mathbb{R}$, mais $\mathbb{R}$ est inclus dans $\mathbb{H}$ ... depuis le paragraphe précédent).

Proposition 2.5. (a) *La norme est multiplicative, c'est-à-dire qu'on a l'égalité $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{H}$.*

(b) *Tout élément non nul de $\mathbb{H}$ est inversible, c'est-à-dire que $\mathbb{H}$ est donc une algèbre à division.*

(c) *Dans $\mathbb{H}$ on a la formule $\overline{xy} = \bar{y}\bar{x}$*

Démonstration. (a) On utilise la formule plus haut et on calcule séparément les sommes $A^2+B^2+C^2+D^2$ et $(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2)$; on trouve le même résultat.

(b) Si $z \in \mathbb{H}$ est non nul, alors $N(z)$ est un élément non nul de $\mathbb{R}$, donc inversible dans $\mathbb{R}$, donc inversible dans $\mathbb{H}$. Dès lors, $z\bar{z} = N^2(z)$ implique que $\frac{\bar{z}}{N^2(z)}$ est un inverse pour z.

(c) Si x ou y est nul, c'est clair. On suppose que x et y sont non nuls, donc inversibles par (b). On a $\overline{xy}(xy) = N^2(xy)$. On a aussi par ailleurs $\bar{y}\bar{x}(xy) = \bar{y}N^2(x)y = N^2(x)\bar{y}y = N^2(x)N^2(y)$ (on a utilisé que $N(x)$ est un élément de $\mathbb{R}$, et commute donc avec $\bar{y}$). Puisque $N(xy) = N(x)N(y)$ par (a), on trouve $\overline{xy}(xy) = \bar{y}\bar{x}(xy)$. On peut simplifier avec x et y qui sont inversibles et on obtient le résultat. □

L'ensemble $\{\pm 1, \pm i, \pm j, \pm k\}$ est un sous-groupe d'ordre 8 de $\mathbb{H}^\times$. Tous ses éléments à part ± 1 sont d'ordre 4. On l'appelle **groupe des quaternions**.

On trouvera une généralisation de la construction de $\mathbb{H}$ en remplaçant $\mathbb{R}$ par un corps quelconque dans la dernière section du chapitre « Compléments ».

2.5. Exercices

Rappelons la notation $\mathbb{U}_n := \{z \in \mathbb{C}, z^n = 1\}$.

Exercice 1. Si $z \in \mathbb{C}$, $z = a + bi$ avec $a, b \in \mathbb{R}$, montrer :

$$\max(|a|, |b|) \leq |z| \leq |a| + |b| \leq |z|\sqrt{2}.$$

Exercice 2. Si $z, z' \in \mathbb{C}$, montrer que $||z| - |z'|| \leq |z + z'| \leq |z| + |z'|$. Supposons que $z \neq 0$. Montrer alors que la première inégalité est une égalité si et seulement si $z' = \lambda z$ avec $\lambda \in \mathbb{R}_-$, et la seconde inégalité est une égalité si et seulement si $z' = \lambda z$ avec $\lambda \in \mathbb{R}_+$.

Exercice 3. Quelles sont les racines n-ièmes de -1 dans $\mathbb{C}$ (donner la forme trigonométrique).

Exercice 4. Soit ε une racine n-ième de l'unité différente de 1. Montrer que $1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + ... + \varepsilon^{n-1} = 0$.

Exercice 5. Si n est pair et ε est une racine n-ième de l'unité, calculer $\varepsilon + \varepsilon^3 + \varepsilon^5 + \varepsilon^7 + ... + \varepsilon^{n-1}$.

Exercice 6. Soient $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}$ les racines n-ièmes de l'unité, avec $n \geq 2$. Montrer que

$$\varepsilon_0 + \varepsilon_1 + \varepsilon_2 + ... + \varepsilon_{n-1} = 0.$$

Plus généralement, pour tout $k \in \mathbb{N}$, si k n'est pas divisible par n, montrer que

$$\sum_{m=0}^{n-1} \varepsilon_m^k = 0.$$

Que se passe-t-il si $n|k$?

Exercice 7. Soit ε une racine d-ième de l'unité. Montrer alors que ε est racine n-ième de l'unité pour tout entier n non nul divisible par d. Montrer que, si $m, n \in \mathbb{N}^*$, alors $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{\text{pgcd}(m,n)}$.

Exercice 8. Si $n \in \mathbb{N}^*$, montrer que le groupe $\mathbb{U}_n$ est cyclique. Montrer que tout sous-groupe de $\mathbb{U}_n$ est de la forme $\mathbb{U}_d$ avec $d|n$.

Exercice 9. Une racine **primitive** n-ième de l'unité est une racine n-ième z de l'unité telle que $z^m \neq 1$ si $0 < m < n$. Montrer que les racines primitives n-ièmes de l'unité sont les nombres $e^{\frac{2ik\pi}{n}}$ telles que k est premier avec n. Combien de telles racines (distinctes) existe-t-il ?

Exercice 10. Si $z_1, z_2 \in \mathbb{C}$, il n'est en général pas possible de donner une formule trigonométrique satisfaisante de $z_1 + z_2$ en fonction de celles de z_1 et z_2. Mais cela est possible quand $|z_1| = |z_2|$. En passant z_1 en facteur dans $z_1 + z_2$, il suffit de traiter le cas où $z_1 = 1$.

(a) En factorisant par $e^{\frac{i\theta}{2}}$, écrire le nombre complexe $1+e^{i\theta}$ sous une forme $re^{\frac{i\theta}{2}}$ avec r réel. Pareil pour $1 - e^{i\theta}$.

(b) Discuter le signe de r et en déduire la forme trigonométrique des nombres complexes $1 + e^{i\theta}$ et $1 - e^{i\theta}$.

(c) Soient z_1 et z_2 deux nombres complexes non nuls de modules égaux. Donner un argument de $z_1 + z_2$ en fonction de ceux de z_1 et z_2.

Exercice 11. À partir de l'exercice 10, mettre sous une forme simple la fraction $\frac{1-e^{i(n+1)\theta}}{1-e^{i\theta}}$ pour $\theta \in \mathbb{R}\backslash 2\mathbb{Z}\pi$. En déduire une formule pour $\sum_{k=0}^{n} e^{(x+k\theta)i}$, quand x est un nombre réel fixé. En déduire une formule simple pour $\sum_{k=0}^{n} \sin(x + k\theta)$ et ensuite pour $\sum_{k=0}^{n} \cos(x + k\theta)$.

Exercice 12. Posons $j := e^{\frac{2i\pi}{3}}$. Montrer que $j^2 = \bar{j}$. Montrer que $j^3 = \bar{j}^3 = 1$

et $1+j+j^2=0$, et en déduire grâce à la formule du binôme de Newton que

$$(1+1)^n+(1+j)^n+(1+\bar{j})^n=3(C_n^0+C_n^3+C_n^6+...+C_n^{3m}),$$

où m est la partie entière de $\frac{n}{3}$. Mettre le résultat sous une forme simple.

Exercice 13. Calculer la somme $C_n^1+C_n^4+C_n^7+...$ en vous inspirant de l'exercice précédent.

Exercice 14. Calculer

$$C_n^0+C_n^4+C_n^8+...$$

en utilisant $(1+1)^n,(1-1)^n,(1+i)^n,(1-i)^n$ et l'exercice 6. Donner ensuite une formule simple pour $C_n^0+C_n^4+C_n^8+...$, en mettant $1+i$ et $1-i$ sous une forme de type trigonométrique grâce à l'exercice 10.

Exercice 15. Soit $z=a+bi$ un nombre complexe, avec $a,b\in\mathbb{R}$. Exprimer les parties réelles et imaginaires des racines carrées de $a+bi$ en fonction de a et b, en suivant les indications suivantes : à partir de $z=(a'+b'i)^2$, écrire deux équations en les inconnues a' et b' en utilisant l'égalité des modules et l'égalité des parties réelles ; sur les quatre possibilités trouvées pour le nombre $a'+b'i$, décider enfin quelles sont les deux à garder grâce à l'égalité des parties imaginaires.

Calculer sous forme algébrique une racine carrée de $1+i$ et une racine carrée de $1-2i$.

Exercice 16. Soit V le $\mathbb{R}$-espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Soit $x\in\mathbb{R}$. Montrer que, pour tout $n\in\mathbb{N}$, le sous-espace de V engendré par $\{\cos(kx)\}_{0\leq k\leq n}$ et le sous-espace de V engendré par $\{\cos^k(x)\}_{0\leq k\leq n}$ sont confondus.

Exercice 17. Soit $Z(\mathbb{H})$ le centre de l'anneau $\mathbb{H}$ des quaternions, c'est-à-dire l'ensemble des éléments de $\mathbb{H}$ qui commutent avec tous les éléments de $\mathbb{H}$. Montrer que $Z(\mathbb{H})=\mathbb{R}$ (affirmation vue sans preuve dans le cours).

Exercice 18. Soient $\mathbb{H}$ l'anneau des quaternions et $N:\mathbb{H}\to\mathbb{R}_+$ l'application norme. Si $z\in\mathbb{H}$, on pose $\mathrm{tr}(z)=z+\bar{z}$.

(a) Montrer que tout élément z de $\mathbb{H}$ vérifie $z^2-\mathrm{tr}(z)z+N^2(z)=0$. (Noter que tout commute, puisque $\mathrm{tr}(z)$ et $N(z)$ sont des nombres réels.)

(b) En déduire que le polynôme X^2+1 a une infinité de racines dans $\mathbb{H}$.

Exercice 19. Montrer que l'anneau $\mathbb{H}$ des quaternions a une infinité de sous-corps isomorphes à $\mathbb{C}$.

Exercice 20. Si b et c sont des nombres réels et $P(X):=X^3+bX+c$, on veut savoir quand les racines de P sont (toutes) réelles. Soit $\Delta:=-(27c^2+4b^3)$

le **discriminant** de P, de sorte que, si δ est une racine carrée de Δ dans $\mathbb{C}$, les nombres complexes U et V du cours s'écrivent $U = -\frac{c}{2} + i\delta, V = -\frac{c}{2} - i\delta$. Notons x_1, x_2, x_3 les nombres complexes définis comme dans le cours, dont on sait que ce sont les racines de P.

(a) Montrer que, si x est une racine de P, alors son conjugué complexe l'est aussi.

(b) Supposons que $\Delta > 0$. Montrer que x_1, x_2, x_3 sont réels.

(c) Supposons que $\Delta < 0$. Montrer qu'un seul nombre parmi x_1, x_2, x_3 est réel.

Exercice 21. Soit P un polynôme de degré $n \geq 1$ à coefficients complexes qui vérifie $|P(z)| \leq 1$ si $|z| \leq 1$. Montrer que tous les coefficients de P sont de module au plus 1.

Exercice 22. Trouver $a, b \in \mathbb{C}$ tels que $a + b = ab = 5$. Trouver $a, b \in \mathbb{C}$ tels que $a+b = a^2+b^2 = 5$. Trouver $a, b \in \mathbb{C}^*$ tels que $a+b = 2$ et $\frac{1}{a^2} + \frac{1}{b^2} = 6$.

Exercice 23. Soit $n \in \mathbb{N}^*$. Trouver les solutions de l'équation de degré $2n$: $(x^2 + 1)^n - (x + 1)^n = 0$ dans $\mathbb{C}$.

Exercice 24. Soit $n \in \mathbb{N}^*$. On suppose qu'il existe dans $\mathbb{C}$ deux racines n-ièmes de l'unité dont la somme est une racine n-ième de l'unité. Montrer que n est divisible par 6.

Exercice 25. On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1, et $\mathbb{U}_\infty$ l'ensemble de toutes les racines de l'unité (la réunion des $\mathbb{U}_n$ quand n parcourt $\mathbb{N}^*$).

(a) Montrer que $\mathbb{U}$ et $\mathbb{U}_\infty$ sont des sous-groupes de $\mathbb{C}^\times$.

(b) Montrer les isomorphismes de groupes :

$$\mathbb{U} \simeq \mathbb{R}/\mathbb{Z}, \qquad \mathbb{U}_\infty \simeq \mathbb{Q}/\mathbb{Z}, \qquad \mathbb{C}^\times/\mathbb{U} \simeq (\mathbb{R}_+^*, \times).$$

(c) Si $n \in \mathbb{N}^*$, montrer que $\mathbb{C}^\times/\mathbb{U}_n \simeq \mathbb{C}^\times$.

Exercice 26. Montrer que les matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $a, b \in \mathbb{R}$ forment un sous-corps de $M_2(\mathbb{R})$, isomorphe à $\mathbb{C}$.

Exercice 27. Montrer que les matrices de la forme $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ avec $a, b \in \mathbb{C}$ forment un sous-anneau de $M_2(\mathbb{C})$, isomorphe à $\mathbb{H}$.

Exercice 28. Posons $j := e^{\frac{2i\pi}{3}}$. Montrer que $A := \{a + bi,\ a, b \in \mathbb{Q}\}$ et

$B := \{a + bj,\ a, b \in \mathbb{Q}\}$ sont des sous-corps de $\mathbb{C}$ et qu'ils ne sont pas isomorphes.

Partie 2

Polynômes

Chapitre 3

Algèbres. $K[X]$. Étude des polynômes

3.1. Algèbres

3.1.1. Définitions. Soit K un corps. Rappelons qu'un anneau $(A, +, \times)$ est appelé **algèbre sur** K, ou K**-algèbre**, si A est muni d'une structure de K-espace vectoriel où

- l'addition des vecteurs est l'addition de A, et

- la multiplication par des scalaires est compatible avec la multiplication de l'anneau A, au sens suivant : on a $\lambda(a \times b) = (\lambda a) \times b = a \times (\lambda b)$ pour tout $\lambda \in K$ et tous $a, b \in A$.

Une telle K-algèbre A est dite **commutative** (resp. **intègre**) si l'anneau A sous-jacent est commutatif (resp. intègre). On appelle **idéal** de (l'algèbre) A tout idéal de l'anneau A.

Soit K un corps. Soit A une K-algèbre. Un sous-anneau B de A qui est une K-algèbre pour les opérations définies sur A est appelée K**-sous-algèbre** de A ; mais, le plus souvent, K étant fixé, on appelle B simplement « sous-algèbre » de A. L'intersection d'une famille de sous-algèbres de A est encore une sous-algèbre de A. Si U est une partie de A, la **sous-algèbre de** A **engendrée par** U est, par définition, l'intersection de toutes les sous-algèbres de A qui contiennent U.

Un **morphisme de** K**-algèbres** $f : A \to B$ est un morphisme d'anneaux de A dans B qui est K-linéaire. Alors l'image de f est une sous-algèbre de B et le noyau de f (en tant que morphisme d'anneaux, en fait simplement de groupes additifs) est un idéal propre de A. Comme expliqué dans l'exemple (4) ci-dessous, $A/\ker(f)$ a une structure naturelle de K-algèbre et l'isomorphisme d'anneaux $\bar{f} : A/\ker f \to Im(f)$, obtenu par le théorème d'isomorphisme pour les anneaux, est K-linéaire ; c'est donc un isomorphisme de K-algèbres. Si A est une K-algèbre, un morphisme de K-algèbres de A dans A est aussi appelé K**-endomorphisme** de A. Un K**-automorphisme** est un K-endomorphisme bijectif.

3.1.2. Exemples généraux. Soit K un corps.

(1) L'anneau de polynômes $K[X]$ est une K-algèbre commutative intègre pour la multiplication par des scalaires qu'on lui connaît.

(2) Si $n \in \mathbb{N}^*$, l'anneau des matrices $M_n(K)$, est une K-algèbre pour la multiplication par des scalaires qu'on lui connaît. Si $n \geq 2$, l'algèbre $M_n(K)$ n'est ni commutative ni intègre.

(3) Si A est une K-algèbre, le centre $Z(A)$ de l'anneau A, formé des éléments de A qui commutent avec tous les éléments de A, est une K-sous-algèbre de A. Si, de plus, A est une algèbre à division, alors $Z(A)$ est une algèbre à division, et même, étant commutative, un corps.

(4) Soient A une K-algèbre commutative et I un idéal de l'anneau A. Alors I est automatiquement un K-sous-espace vectoriel de A (en effet, si $\lambda \in K$ et $x \in I$, on a $\lambda x = \lambda(1_A x) = (\lambda 1_A)x \in I$, parce que $\lambda 1_A$ est un élément de l'anneau A). Si I est un idéal propre, l'anneau quotient A/I est une K-algèbre pour la structure quotient d'anneau et la structure quotient de K-espace vectoriel. Par exemple, $\mathbb{R}[X]/(X^3+1)$ a une structure de $\mathbb{R}$-algèbre induite par celle de $\mathbb{R}[X]$.

(5) Si A est un anneau commutatif qui contient K, alors A a automatiquement une structure de K-algèbre, où la multiplication par des scalaires de K est donnée par la multiplication dans A. On appelle cette structure la structure **canonique** de K-algèbre de A. Par exemple, $\mathbb{R}$ a une structure canonique de $\mathbb{Q}$-algèbre.

Remarquer toutefois que, même si A contient K, A peut avoir d'autres structures de K-algèbre que la structure canonique. Par exemple, si $K = \mathbb{C}$ et $A = \mathbb{C}$, alors la structure canonique de K-algèbre de A est donnée par une multiplication par des scalaires qui est la multiplication dans $\mathbb{C}$, mais on peut aussi définir une multiplication par des scalaires par la formule $\lambda z := \bar{\lambda} \times z$, où $\times$ est la multiplication dans l'anneau $\mathbb{C}$.

Commentaires. (1) Certains exemples traités plus haut peuvent s'étendre à des algèbres non commutatives en considérant des multiplications par des scalaires à gauche, ou bien à une définition d'algèbre non pas sur un corps mais sur un anneau ; ces généralisations ne sont pas traitées dans le livre présent.

(2) Un autre exemple général d'algèbre (commutative) sur un corps K est l'algèbre des séries formelles à coefficients dans K. Il n'a pas assez de liens avec le livre présent pour être cité ici.

Voici deux autres cas où on obtient des structures d'algèbres de façon tellement courante qu'on oublie parfois d'en donner l'argument :

(1) Si $\kappa : K \to K'$ est un morphisme de corps, si A est une K'-algèbre, alors on obtient une structure de K-algèbre sur A, **par transfert de structure via** κ, en posant $\lambda x := \kappa(\lambda)x$ pour tout $\lambda \in K$ et tout $x \in A$. Par exemple l'anneau $\mathbb{R}[X]$ a une structure de $\mathbb{Q}$-algèbre, via le morphisme d'inclusion de $\mathbb{Q}$ dans