Cours de Bac 2 en mathématiques
Un premier contact avec la Théorie des Nombres
Souvenir 2009-2010

Anne-Marie Simon
Université libre de Bruxelles Faculté des Sciences
Département de mathématiques

première version : 9 mai 2009
deuxième version : 4 mai 2010
corrigée le 10 novembre 2010

Table des matières

Chapitre 0

Introduction

0.1 Introduction générale

La théorie des nombres ou arithmétique a pour objet les nombres entiers naturels ainsi que leurs généralisations, les nombres rationnels, les nombres algébriques et plus particulièrement les entiers algébriques.

La théorie des nombres étudie aussi les équations diophantiennes, équations polynomiales à coefficients entiers ou rationnels, dont on recherche les solutions entières ou rationnelles. La plus célèbre d'entre elle est l'équation de Fermat $x^n + y^n = z^n$, dont l'histoire est longue. Dans la marge d'un livre, Fermat ($XVII^{\text{ième}}$) avait annoncé sans preuve que cette équation ne possède pas de solutions entières non triviales pour $n \geqslant 3$, bien que par la suite il ne fit plus allusion qu'au cas où $n = 3$. On a donné à cet énoncé de Fermat le nom de « grand théorème de Fermat », bien qu'en l'absence de preuve ce grand théorème n'était qu'une conjecture. Le cas $n = 3$ du grand théorème de Fermat fut prouvé par Euler en 1753, d'autres encore furent prouvés dans le courant du $XIX^{\text{ième}}$ et du $XX^{\text{ième}}$ siècle, amenèrent les mathématiciens à étudier plusieurs anneaux de nombres, dont la plupart ne sont ni principaux ni factoriels. Pour remédier à l'absence d'une factorisation unique dans ces anneaux de nombres, Kummer et Dedekind ont développé la théorie des idéaux. Au dernier quart du $XX^{\text{ième}}$ siècle on a remarqué que la « *conjecture* » de Fermat est équivalente à une conjecture très significative concernant certaines courbes du plan réel, ce qui a ramené l'attention sur cet énoncé de Fermat. Le cas général du grand théorème de Fermat, resté très longtemps à l'état de conjecture, fut finalement démontré par Wiles à la fin du $XX^{\text{ième}}$ siècle (la preuve de Wiles dépasse largement le cadre de ces notes).

L'équation $x^2 + y^2 = n$, où n est un nombre naturel donné, est plus accessible ; grâce à la connaissance des propriétés de l'anneau des entiers de Gauss $\mathbb{Z}[i]$, et aussi à celle des corps finis, nous pourrons montrer pour quelles valeurs de n cette équation a des solutions entières (théorème des

deux carrés).

Ceci nous indique que l'étude des nombres entiers naturels est aussi liée à l'étude de certains sous-anneaux du corps des complexes.

La recherche des solutions entières de l'équation de Pell-Fermat

$$x^2 - ny^2 = 1$$

(n étant un entier naturel qui n'est pas un carré) passe par des considérations géométriques sur le plan réel et fournit des informations sur certains anneaux d'entiers algébriques.

Ces quelques exemples montrent que, pour résoudre des questions très simples concernant les entiers naturels $1, 2, 3, \cdots$, il est utile d'élargir le cadre dans lequel on travaille. Ils montrent aussi que ces questions très simples sont aussi des questions concernant des tas d'objets mathématiques.

Quant au contenu de ces notes, il sera très modeste et assez bien décrit par la table des matières.

Nos premières promenades nous emmènent au pays des corps quadratiques. La première d'entre elles, consacrée au nombre d'or, offre l'opportunité d'introduire ou de rappeler quelques notions fondamentales, de suggérer les thèmes des sections suivantes. Elle nous amène aussi à discuter la dépendance intégrale, fondamentale en théorie des nombres.

Au second chapitre nous commençons l'étude de certains anneaux de nombres et nous introduisons les normes et traces pour un corps de nombres quelconque.

Au troisième chapitre nous étudions les extensions de corps en vue d'obtenir une autre vision de la norme pour les extensions non quadratiques et nous regardons un peu les corps cyclotomiques. Nous y explorons au passage la structure des corps finis car ceux-ci interviennent aussi en théorie des nombres (les quotients non triviaux d'anneaux d'entiers algébriques sont finis et parmi eux certains sont des corps finis).

Le dernier chapitre, prolongeant le second, est consacré à l'étude de la structure de l'anneau des entiers d'un corps de nombres.

Avertissement. Les notes qui suivent sont les notes d'un cours donné en 2009 et 2010 aux étudiants de Bac 2 en mathématique de l'Université libre de Bruxelles (24 heures de cours et autant d'exercices). Elles ont été rédigées en fonction des étudiants participant à ce cours. Plusieurs faits importants ont été présentés en exercices, ceux-ci sont désigné par une astérisque *.

Comme nous l'avons dit, ce premier contact avec les nombres sera modeste. On peut trouver plus d'informations sur les thèmes abordés ici dans le joli petit livre de Pierre Samuel [7] qui nous a partiellement inspiré.

Nous supposons une légère familiarité avec les groupes, les anneaux, les modules ainsi qu'avec leurs propriétés exposées au premier cours d'algèbre du Bac en mathématique de l'Université libre de Bruxelles. Certaines de ces notions et propriétés sont rappelées au moment où on désire les utiliser.

D'autres sont brièvement rappelées dans les sections suivantes, à ne consulter qu'en cas de besoin, si ce n'est celle sur les conventions et celle nous emmenant vers les nombres.

0.2 Conventions et notations

0.2.1. Conventions. Dans ces notes, les anneaux sont tous supposés **commutatifs unitaux** (sauf mention expresse du contraire) et les homomorphismes d'anneaux considérés ici sont tous des homomorphismes d'anneaux unitaux, ce qui signifie qu'ils appliquent le neutre multiplicatif du premier anneau sur le neutre multiplicatif du second. Par sous-anneau d'un anneau B nous entendrons toujours un sous-anneau A de B qui contient le neutre multiplicatif de B. Par corps nous entendrons toujours un corps commutatif (dans notre terminologie, les corps non commutatifs, comme celui des quaternions, sont appelés corps gauches ou algèbres à division).

0.2.2. Notations.

$\mathbb{N}$ désigne l'ensemble des nombres naturels, 0 y compris, $\mathbb{N} = \{0, 1, 2, \cdots\}$. Les nombres naturels seront aussi appelés entiers naturels.

$\mathbb{N}_0 = \{1, 2, \cdots\}$ désigne l'ensemble des entiers naturels positifs.

$\mathbb{Z}$ désigne l'anneau des entiers, $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$. Les éléments de $\mathbb{Z}$ seront appelés entiers rationnels, pour les distinguer parmi les entiers algébriques que nous allons définir en 0.9.3.

$\mathbb{Z}_0$ désigne l'ensemble des entiers rationnels non nuls.

$\mathbb{Q}$ désigne le corps des nombres rationnels.

$\mathbb{R}$ désigne le corps des nombres réels.

$\mathbb{C}$ désigne le corps des nombres complexes.

Le **groupe des inversibles** d'un anneau A sera désigné par $A^\times$.

Si K est un corps, $K^\times$ désigne donc le groupe $(K \setminus \{0\}, \cdot)$ et est souvent appelé **le groupe multiplicatif du corps** K.

L'anneau des polynômes en une indéterminée X à coefficients dans un anneau A sera noté $A[X]$. L'anneau des polynômes à coefficients dans A en les indéterminées $X_1, X_2, \cdots, X_n$ sera noté $A[X_1, X_2, \cdots, X_n]$.

Si A est un sous-anneau de l'anneau B, $A \subset B$, et si $b_1, \cdots, b_n \in B$, le sous-anneau de B engendré par A et les b_i sera désigné par $A[b_1, \cdots, b_n]$; ses éléments sont les expressions polynomiales en les b_i à coefficients dans A.

Définitions et observations 0.2.3. Un **domaine** ou **anneau intègre** est un anneau non nul, commutatif comme tous les anneaux considérés ici, et où le produit de deux éléments non nuls est non nul.

Remarque 0.2.4. Un anneau commutatif non nul A est un domaine si et seulement si tout élément non nul de A est **simplifiable** :

$$\forall a, x, y \in A, a \neq 0, \quad ax = ay \Rightarrow x = y,$$

autrement dit si, $\forall a \in A$, $a \neq 0$, la fonction

$$a\cdot : A \to A, a \mapsto ax$$

est injective.

Exemples 0.2.5. L'anneau $\mathbb{Z}$ des entiers rationnels et les corps sont des domaines.

Tout anneau de polynômes à coefficients dans un domaine est un domaine.

La plupart des domaines ne sont pas des corps, mais tout domaine fini est un corps.

Nous utiliserons souvent l'axiome du choix que voici et dont on ne peut guère se passer en algèbre.

0.2.6. L'axiome du choix dit qu'étant donné un ensemble $\mathcal{E}$ d'ensembles non vides, il est possible de choisir un élément dans chacun d'entre eux. Plus précisément, il dit qu'il existe une fonction de choix $c : \mathcal{E} \to \bigcup \mathcal{E}$ telle que $\forall A \in \mathcal{E}, c(A) \in A$.

0.3 Congruences, idéaux et anneaux quotients

Définition 0.3.1. Un **idéal** de l'anneau (commutatif) A est une partie $\mathfrak{I}$ de A telle que

(i) $\mathfrak{I}$ est un sous-groupe du groupe additif $(A, +)$,

(ii) $\forall x \in A$, on a $x\mathfrak{I} := \{xy \mid y \in \mathfrak{I}\} \subset \mathfrak{I}$.

Un **idéal propre** de l'anneau A est un idéal de A distinct de A.

Remarque 0.3.2. Soit A un anneau. A et $\{0\}$ sont des idéaux de A, souvent appelés idéaux triviaux.

Un idéal $\mathfrak{I}$ de A est propre si et seulement si $\mathfrak{I} \cap A^\times = \varnothing$.

Exemple 0.3.3. (i) Le **noyau** d'un homomorphisme d'anneaux $f : A \to B$, défini par $\ker(f) = \{x \in A \mid f(x) = 0\}$, est un idéal de A, propre dès que B est non nul.

(ii) Le seul idéal propre d'un corps est l'idéal nul. Et donc tout homomorphisme d'un corps dans un anneau non nul est injectif.

Définitions et observations 0.3.4. Toute intersection d'idéaux de l'anneau A est un idéal de A.

Si P est une partie quelconque de A, l'intersection des idéaux de A contenant P est donc le plus petit idéal de A contenant P, on dira de cette intersection qu'elle est l'**idéal engendré** par P, on la désignera parfois par $id\ell(P)$.

L'idéal d'un anneau A engendré par ses éléments $a_1, \cdots, a_n$ sera simplement désigné par $(a_1, \cdots, a_n)$ quand il n'y a pas ambiguïté sur l'anneau dans lequel on travaille. Comme nos anneaux sont supposés commutatifs, $\forall a \in A$ nous avons $(a) = aA$. En général nous avons $(a_1, \cdots, a_n) = a_1A + \cdots + a_nA$.

Un **idéal principal** de l'anneau A est un idéal pouvant être engendré par un seul élément de A, donc de la forme $(a) = aA$, où $a \in A$.

Lemme 0.3.5. *Soit A un anneau non nul, commutatif comme tous les anneaux que nous considérons ici.*

Alors A est un corps si et seulement si l'idéal nul est son seul idéal propre.

Définitions et observations 0.3.6. Soit $\mathfrak{I}$ un idéal de l'anneau A.

La **classe latérale** d'un élément $a \in A$ selon $\mathfrak{I}$ est la partie $a + \mathfrak{I}$ de A.

Ces classes latérales forment une partition de A :

$$\forall a \in A \qquad a \in a + \mathfrak{I} \neq \varnothing$$

$$A = \bigcup_{a \in A} (a + \mathfrak{I}) \quad \text{et} \quad (a + \mathfrak{I}) \cap (a' + \mathfrak{I}) \neq \varnothing \Leftrightarrow (a + \mathfrak{I}) = (a' + \mathfrak{I}).$$

Notons aussi : $\quad (a + \mathfrak{I}) = (a' + \mathfrak{I}) \quad \Leftrightarrow \quad (a - a') \in \mathfrak{I}$.

Définitions et observations 0.3.7. Définissons maintenant l'**anneau quotient** $A/\mathfrak{I}$ de A par son idéal $\mathfrak{I}$.

En tant qu'ensemble $A/\mathfrak{I} = \{a + \mathfrak{I} \mid a \in A\}$. L'addition et la multiplication y sont définies comme suit : $\forall a, b \in A$,

$$(a + \mathfrak{I}) \bar{+} (b + \mathfrak{I}) = (a + b) + \mathfrak{I} \quad \text{et} \quad (a + \mathfrak{I}) \bar{\cdot} (b + \mathfrak{I}) = (ab) + \mathfrak{I}.$$

Évidemment il convient de vérifier d'abord que ces opérations sont bien définies, que, si $(a + \mathfrak{I}) = (a' + \mathfrak{I})$ et $(b + \mathfrak{I}) = (b' + \mathfrak{I})$, alors $(a + b) + \mathfrak{I} = (a' + b') + \mathfrak{I}$ et $(ab) + \mathfrak{I} = (a'b') + \mathfrak{I}$. Ceci ne présente aucune difficulté. En effet on a :

$(a + \mathfrak{I}) = (a' + \mathfrak{I}) \quad$ et $\quad (b + \mathfrak{I}) = (b' + \mathfrak{I})$

$\Leftrightarrow a - a' \in \mathfrak{I} \quad$ et $\quad b - b' \in \mathfrak{I}$

$\Rightarrow (a + b) - (a' + b') \in \mathfrak{I} \quad$ et $\quad (ab - a'b') = (a(b - b') + (a - a')b') \in \mathfrak{I}$

$\Leftrightarrow (a + b) + \mathfrak{I} = (a' + b') + \mathfrak{I} \quad$ et $\quad (ab) + \mathfrak{I} = (a'b') + \mathfrak{I}$.

Ceci étant fait, on voit aisément que ces opérations munissent $A/\mathfrak{I}$ d'une structure d'anneau, de neutre additif $0 + \mathfrak{I} = \mathfrak{I}$ et de neutre multiplicatif $1 + \mathfrak{I}$, et que la projection naturelle

$$p : A \to A/\mathfrak{I} : a \mapsto a + \mathfrak{I}$$

est un homomorphisme surjectif d'anneaux de noyau $\mathfrak{I}$.

Dans la pratique il est souvent commode d'écrire $\bar{a} = a + \mathfrak{I}$ pour éviter des lourdeurs d'écriture, et aussi d'omettre la barre sur les opérations.

0.3.8. *Conclusion.* Le noyau d'un homomorphisme d'anneaux est un idéal de son domaine et réciproquement tout idéal d'un anneau A est noyau d'un homomorphisme de domaine A. Les idéaux sont aux anneaux ce que les sous-groupes normaux sont aux groupes.

Exemple 0.3.9. Soit n un nombre naturel, $n \geqslant 2$. L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est un anneau fini, de n éléments que voici : $0+\mathbb{Z}, 1+\mathbb{Z}, \cdots, (n-1)+\mathbb{Z}$. On l'appelle l'anneau des entiers modulo n, ou l'anneau des restes de la division par n, on le désigne souvent par $\mathbb{Z}_n$ et on omet même souvent la barre au dessus de ses éléments, écrivant simplement $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$.

L'anneau $\mathbb{Z}/12\mathbb{Z}$ mérite de s'appeler l'anneau de l'horloge.

L'anneau $\mathbb{Z}/1\mathbb{Z}$ est l'anneau nul.

Si le nombre naturel p est premier, l'anneau $\mathbb{Z}_p$ est un corps souvent désigné par $\mathbb{F}_p$.

Si le nombre naturel $n \geqslant 2$ n'est pas premier, l'anneau $\mathbb{Z}_n$ n'est pas intègre, il comprend deux éléments non nuls dont le produit est nul.

0.3.10. Quotients d'anneaux de polynômes.

Soit K un corps, commutatif comme tous les corps considérés ici, et soit $P \in K[X]$ un polynôme de degré $n \geqslant 1$.

On peut diviser tout polynôme de $K[X]$ par P, obtenir un quotient et un reste de degré $< n$:

$$\forall T \in K[X] \quad \exists! Q \in K[X] \quad \exists! R \in K[X] \quad \text{tels que}$$

$$T = PQ + R \quad \text{et} \quad \text{degré(R)} < \text{degré(P)}.$$

(Par convention le degré du polynôme nul est $-\infty$.)

Il s'en suit que toute classe latérale $T + PK[X]$ comprend un et seul polynôme de degré $< n = \text{degré}(P)$, à savoir le reste de la division de T par P.

En particulier la fonction composée

$$K \xrightarrow{i} K[X] \xrightarrow{p} K[X]/PK[X],$$

où i désigne l'inclusion naturelle et p la projection naturelle, est un homomorphisme d'anneaux injectifs, nous permettant d'identifier K à son image dans l'anneau quotient $K[X]/PK[X]$, de voir K comme un sous-anneau de $K[X]/PK[X]$.

Désignons maintenant par x la classe latérale $X + PK[X]$, autrement dit $x = p(X)$. Avec cette notation nous avons, $\forall T \in K[X], \quad p(T) =$

$T + PK[X] = T(x)$. Mais aussi nous voyons que les éléments de l'anneau quotient $K[X]/PK[X]$ s'écrivent de façon unique sous la forme

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \quad \text{où} \quad a_0, a_1, \cdots, a_{n-1} \in K.$$

Ces éléments s'additionnent et se multiplient de la façon habituelle. En ce qui concerne la multiplication, comme le produit de deux polynômes de degré inférieur à n peut être de degré supérieur ou égal à n, pour écrire un produit sous la forme désirée il convient de tenir compte de la relation

$$p(P) = P(x) = 0,$$

x est une « racine » de P dans l'anneau quotient $K[X]/PK[X]$.

Notons encore qu'une restriction de la multiplication munit $K[X]/PK[X]$ d'une structure d'espace vectoriel sur K, de dimension n et de base $1, x, \cdots, x^{n-1}$.

Traitons un cas particulier : $P = X^3 - 2 \in \mathbb{Q}[X]$
Nous avons $\mathbb{Q}[X]/(X^3-2)\mathbb{Q}[X] = \{a + bx + cx^2 \mid a, b, c \in \mathbb{Q}\}$ et

$$x^3 - 2 = 0 \quad \text{d'où} \quad x^3 = 2 \quad \text{et} \quad x^4 = 2x.$$

Nous avons aussi : $\forall a, b, c, a', b', c' \in \mathbb{Q}$

$(a + bx + cx^2) + (a' + b'x + c'x^2) = (a + a') + (b + b')x + (c + c')x^2$ et

$(a + bx + cx^2) \cdot (a' + b'x + c'x^2)$
$= aa' + (ab' + a'b)x + (ac' + a'c + bb')x^2 + (bc' + b'c)x^3 + cc'x^4$
$= (aa' + 2bc' + 2b'c) + (ab' + a'b + 2cc')x + (ac' + a'c + bb')x^2.$

On peut se demander sous quelle condition l'anneau quotient $K[X]/PK[X]$ est intègre.

Si le polynôme P de degré n est produit de deux polynômes de degré strictement inférieur à n, alors $K[X]/PK[X]$ n'est pas intègre (Si $P = P_1P_2$, où degré(P_1), degré(P_2) < degré(P), dans le quotient $K[X]/PK[X]$ nous avons $0 = P(x) = P_1(x)P_2(x)$ et $P_1(x) \neq 0 \neq P_2(x)$).

Si le polynôme P de degré n n'est pas produit de deux polynômes de degré strictement inférieur à n, nous verrons rapidement que $K[X]/PK[X]$ est un corps.

Dans l'exemple traité ci-haut, le polynôme $X^3 - 2$ de $\mathbb{Q}[X]$ n'est pas produit de deux polynômes de degré < 3 dans $\mathbb{Q}[X]$ (il n'a pas de facteur de degré 1 car $2^{\frac{1}{3}} \notin \mathbb{Q}$), l'anneau quotient $\mathbb{Q}[X]/(X^3-2)\mathbb{Q}[X]$ est un corps.

Vocabulaire 0.3.11. La terminologie suivante est courante en théorie des nombres.

Soit A un anneau et soit $a \in A$. Nous dirons que deux éléments x et y de A sont **équivalents modulo** a (ou **congrus modulo** a) et nous écrirons

$$x \cong y \text{ modulo a} \qquad \text{si} \qquad x - y \in aA,$$

autrement dit si x et y ont même image dans l'anneau quotient A/aA par la projection naturelle $A \to A/aA : z \mapsto z + aA$.

Plus généralement, soit $\mathfrak{A}$ un idéal de l'anneau A. Nous dirons que deux éléments x et y de A sont équivalents modulo $\mathfrak{A}$ (ou congrus modulo $\mathfrak{A}$) et nous écrirons $\quad x \cong y$ modulo $\mathfrak{A} \quad$ si $x - y \in \mathfrak{A}$.

0.3.12. *Application.* Pour montrer qu'une équation polynomiale à coefficients entiers n'a pas de solution dans $\mathbb{Z}$, il suffit de montrer qu'elle n'a pas de solutions modulo un naturel bien choisi. Cette méthode est parfois efficace. En voici un exemple très simple.

Les nombres naturels de la forme $4n + 3$ *ne sont pas des carrés.*

Pour voir ceci, il nous suffit de montrer que l'équation $3 + 4x = y^2$ n'a pas de solution dans $\mathbb{Z}$. Si elle en avait une, nous aurions un nombre $y \in \mathbb{Z}$ tel que $y^2 \cong 3$ modulo 4 et l'image de 3 dans l'anneau $\mathbb{Z}_4$ serait un carré. Or ce n'est pas le cas, dans l'anneau $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ nous avons $0^2 = 0, 1^2 = 1, 2^2 = 0, 3^2 = 1$.

0.4 pgcd et ppcm dans un domaine

La multiplication dans un domaine nous fournit une relation entre les éléments de ce domaine.

Définitions et observations 0.4.1. Soit a et b deux éléments d'un domaine A.

(i) Nous dirons que a **divise** b dans A et nous écrirons $a \mid b$ s'il existe $m \in A$ tel que $b = am$. Dans ce cas, nous dirons aussi que a est un **diviseur** de b et que b est un **multiple** de a.

La relation « divise » dans A est réflexive et transitive, c'est une relation de préordre.

De plus, $\quad a \mid b \qquad \Rightarrow \qquad \forall t \in A, \quad at \mid bt.$

(ii) Si $a \mid b$ et $b \mid a$ dans A, nous dirons que a et b sont **associés** dans A et nous écrirons $a \sim b$.

La relation « être associés » est une relation d'équivalence dans A.

(iii) Si $a \mid b$ et si a n'est pas associé à b dans A, nous dirons que a est un **diviseur strict** de b.

Remarques 0.4.2. Soit A un domaine.

(i) $\forall x \in A$ on a $1 \mid x \mid 0$ et
$x \mid 1 \quad \Leftrightarrow \quad x \sim 1 \quad \Leftrightarrow \quad x \in A^\times$
$0 \mid x \quad \Leftrightarrow \quad x \sim 0 \quad \Leftrightarrow \quad x = 0.$

(ii) Soient a, b, u des éléments du domaine A.

$$a \sim b \quad \Leftrightarrow \quad \exists e \in A^\times \quad \text{tel que} \quad a = be$$

$$au \sim a \quad \Leftrightarrow \quad au \mid a$$

Si $a \neq 0$ alors $au \sim a \quad \Leftrightarrow \quad au \mid a \quad \Leftrightarrow \quad u \in A^\times$

(iii) $$a \mid b \quad \Leftrightarrow \quad bA \subset aA$$

$$a \sim b \quad \Leftrightarrow \quad aA = bA$$

a est un diviseur strict de $b \quad \Leftrightarrow \quad bA \subsetneq aA$.

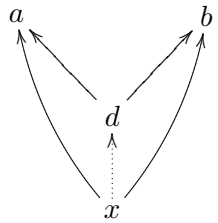
(iv) $\forall t \in A$, $t \neq 0$ on a : $\quad a \mid b \quad \Leftrightarrow \quad at \mid bt$.

Représentation graphique. On indiquera que $a \mid b$ en traçant une flèche allant d'un point représentant a à un point représentant b.

Définitions et observations 0.4.3. Soit A un domaine et soient $a, b \in A$.

(i) Un élément d de A est un **plus grand commun diviseur (pgcd)** de a et b dans A si

$$d \mid a \quad d \mid b \quad \text{et si ,} \quad \forall x \in A, \quad (x \mid a \text{ et } x \mid b) \Rightarrow (x \mid d).$$



Dans ce cas, on écrit $d \sim \text{pgcd}(a, b)$ ou $d \sim (a \wedge b)$. Ceci est justifié par la remarque suivante.

Si d et d' sont deux pgcd de a et b, alors $d \sim d'$ et tout autre élément $d'' \sim d$ est encore un pgcd de a et b.

Le pgcd de deux éléments, quand il existe, est défini à multiplication par un inversible près.

(ii) La connaissance des pgcd permet de retrouver la relation divise :

$$a \mid b \quad \Leftrightarrow \quad a \wedge b \sim a.$$

(iii) On définit un pgcd d'un nombre fini $a_1, \cdots, a_n$ d'éléments de A de la même façon. Si d est un pgcd de ces éléments on écrit $d \sim \text{pgcd}(a_1, \cdots, a_n)$ ou $d \sim (a_1 \wedge \cdots \wedge a_n)$. Notons que l'ordre dans lequel on écrit les a_i est sans importance, la « loi finitaire pgcd » est commutative.

Elle est aussi associative : si $a_1, \cdots, a_n$ et $b_1, \cdots, b_m$ sont deux parties finies du domaine A admettant chacune un pgcd, alors

$$(a_1 \wedge \cdots \wedge a_n) \wedge (b_1 \wedge \cdots \wedge b_m) \sim (a_1 \wedge \cdots \wedge a_n \wedge b_1 \wedge \cdots \wedge b_m)$$

dés que l'un de ces deux éléments existe.

Définition 0.4.4. Les éléments a et b du domaine A sont dits **premiers entre eux** si $1 \sim \text{pgcd}(a, b)$.

Exemples 0.4.5. Deux éléments quelconques de l'anneau $\mathbb{Z}$ des entiers rationnels (resp. de l'anneau $K[X]$ des polynômes en une indéterminée X à coefficients dans un corps K) ont toujours un pgcd que l'on peut calculer par la méthode des divisions successives.

Notons que $\mathbb{Z}^\times = \{1, -1\}$, que $K[X]^\times = K^\times = K \setminus \{0\}$.

Dans le cas de l'anneau $\mathbb{Z}$ des entiers rationnels, parmi les deux pgcd de deux entiers on convient de choisir celui qui est positif.

Dans le cas de l'anneau $K[X]$ des polynômes en une indéterminée X à coefficients dans un corps K, parmi les pgcd de deux polynômes on convient de choisir celui d'entre eux dont le coefficient du terme de degré le plus élevé est 1.

En général, l'axiome du choix nous permet de choisir, pour tout couple (a, b) d'éléments d'un anneau quelconque A admettant un pgcd dans A, l'un quelconque de ses pgcd et de le désigner par $\text{pgcd}(a, b)$. Une fois ce choix fait, le pgcd de deux éléments, quand il existe, est défini comme étant un élément de A.

Proposition 0.4.6. *Supposons que les éléments $a_1, \cdots, a_n$ du domaine A admettent un* pgcd*, disons $d \sim (a_1 \wedge \cdots \wedge a_n)$, supposons aussi que $d \neq 0$, ce qui sera le cas si l'un des a_i est non nul, et écrivons $a_i = da'_i$, $a'_i \in A$, $1 \leqslant i \leqslant n$. Alors*

(i) $(a'_1 \wedge \cdots \wedge a'_n) \sim 1$.

(ii) Soit encore $t \in A$ et supposons que les éléments $a_1 t, \cdots, a_n t$ du domaine A admettent aussi un pgcd, disons $z \sim (a_1 t \wedge \cdots \wedge a_n t)$.

Alors $z \sim dt$.

Démonstration. (i) Si u est un diviseur commun des a'_i, alors ud est un diviseur commun des $a'_i d = a_i$, d'où $ud \mid d$ et $u \sim 1$.

(ii) Si $t = 0$ alors $z = 0$ et $dt = 0$, notre assertion est évidente.

Supposons donc $t \neq 0$. Comme dt est un diviseur commun des $a_i t$, nous avons $dt \mid z$ et nous pouvons écrire $z = dtu$. Par ailleurs nous avons aussi des éléments $a_i'' \in A$ tels que $a_i t = z a_i''$, $1 \leqslant i \leqslant n$.

Dès lors $a_i t = dtua_i''$. En simplifiant par t on obtient $a_i = dua_i''$. Ainsi l'élément du de A est un diviseur commun des a_i, d'où $du \mid d$, $u \in A^\times$ et $dt \sim dtu = z \sim (a_1 t \wedge \cdots \wedge a_n t)$. □

Corollaire 0.4.7. *Soit A un domaine dans lequel tout couple d'éléments admet un* pgcd*, et soit $a, b, c \in A$.*

Si $a \mid bc$ et si $\operatorname{pgcd}(a, b) \sim 1$*, alors $a \mid c$.*

Démonstration. De $a \mid bc$ et $\operatorname{pgcd}(a, b) \sim 1$ on déduit
$a \mid \operatorname{pgcd}(ac, bc) \sim c$. □

Définitions et observations 0.4.8. Soit A un domaine et soient encore $a_1, \cdots, a_n \in A$.

Un élément c de A est un **plus petit commun multiple (ppcm)** dans A des a_i, $1 \leqslant i \leqslant n$, si c est un multiple commun des a_i et si tout multiple commun des a_i est multiple de c, c.-à-d. si

$$(\forall i, 1 \leqslant i \leqslant n) \text{ on a} \quad (a_i \mid c \quad \text{et} \quad \forall y \in A \quad (a_i \mid y \Rightarrow (c \mid y)),$$

autrement dit si

$$cA = \bigcap_{1 \leqslant i \leqslant n} a_i A.$$

On écrit alors $c \sim \operatorname{ppcm}(a_1, \cdots, a_n)$ ou $c \sim (a_1 \vee \cdots \vee a_n)$, ce qui est permis car, si c et c' sont deux ppcm des a_i, alors $c \sim c'$ et tout autre élément $c'' \sim c$ est encore un ppcm des a_i.

Le ppcm de deux éléments, quand il existe, est défini à multiplication par un inversible près et la « loi finitaire ppcm » est commutative et associative.

Mais ici encore l'axiome du choix nous permet de choisir, pour tout couple (a, b) d'éléments de l'anneau A admettant un ppcm dans A, l'un quelconque de ses ppcm et de le désigner par $\operatorname{ppcm}(a, b)$, de sorte qu'une fois ce choix fait, le ppcm de deux éléments, quand il existe, est défini comme étant un élément de A.

Proposition 0.4.9. *Soit A un domaine dans lequel tout couple d'éléments admet un pgcd.*

Alors tout couple d'éléments admet aussi un ppcm *dans A et, $\forall a, b \in A$, on a*

$$\operatorname{pgcd}(a, b) \cdot \operatorname{ppcm}(a, b) \sim ab.$$

Démonstration. Soit $d \sim \operatorname{pgcd}(a, b)$. Si $d = 0$ alors $a = 0 = b$ et aussi $0 = \operatorname{ppcm}(a, b)$, la proposition est évidente.

Supposons donc $d \neq 0$ et écrivons $a = da_1$ et $b = db_1$.

Il suffit de montrer que $da_1 b_1 \sim \operatorname{ppcm}(a, b)$.

Remarquons d'abord que $da_1b_1 = ab_1 = a_1b$ est un multiple de a et de b.

Soit maintenant $y \in A$ tel que $a \mid y$ et $b \mid y$. Nous devons montrer que $da_1b_1 \mid y$. Écrivons $y = aa' = bb'$. Il vient $y = da_1a' = db_1b'$, d'où $a_1a' = b_1b'$ et $a_1 \mid b_1b'$. Comme $\text{pgcd}(a_1, b_1) \sim 1$, 0.4.6, on a $a_1 \mid b'$, 0.4.7, et $da_1b_1 \mid db_1b' = bb' = y$. □

0.5 Domaines principaux et domaines factoriels

Définition 0.5.1. Un **anneau principal** est un anneau dont tous les idéaux sont principaux.

Un **domaine principal** est un domaine dont tous les idéaux sont principaux.

Exemple 0.5.2. L'anneau $\mathbb{Z}$ des entiers rationnels et l'anneau $K[X]$ des polynômes en une indéterminée X à coefficients dans un corps K sont des domaines principaux (ceci a probablement été vu au premier cours d'algèbre, en cas d'oubli, on peut se reporter à 1.1.12).

Les domaines principaux ont des propriétés de factorisation très agréables. La première d'entre elles concerne les plus grands communs diviseurs.

Théorème 0.5.3. Relation de Bezout pour les domaines principaux. *Deux éléments quelconques a et b d'un domaine principal A ont toujours un* pgcd.

Si $d \sim \text{pgcd}(a, b)$, alors $dA = aA + bA = id\ell(a, b)$ et il existe $s, t \in A$ tels que

$$d = as + bt.$$

Démonstration. Comme A est principal, l'idéal $\text{id}\ell(a, b) = aA + bA$ de A est principal, engendré par un élément $d \in A : aA + bA = dA$. Montrons que $d \sim \text{pgcd}(a, b)$.

Comme $a, b \in aA + bA = dA$, on a $d \mid a$ et $d \mid b$. D'autre part, comme $d \in aA + bA$, on peut écrire $d = as + bt$ pour certains $s, t \in A$. On observe alors que tout élément x de A divisant à la fois a et b divise aussi d. □

Continuons notre inspection des éléments d'un domaine.

Définitions 0.5.4. (i) Un élément a du domaine A est dit **irréductible** dans A si a est non nul non inversible et si $a = bc$, où $b, c \in A$, implique que b ou c est inversible dans A.

Autrement dit un élément irréductible du domaine A est un élément non nul non inversible qui n'est divisible que par ses associés ou par des inversibles de A.

(ii) Un élément a du domaine A est dit **premier** dans A si a est non nul non inversible et si, $\forall b, c \in A, \quad a \mid bc \Rightarrow a \mid b$ ou $a \mid c$.

Ces deux notions ne sont pas étrangères l'une à l'autre.

Proposition 0.5.5. *(i) Tout élément premier d'un domaine A est irréductible dans A.*

(ii) Dans un domaine principal, plus généralement dans un domaine A ou tout couple d'éléments admet un pgcd, tout élément irréductible dans A est premier dans A.

Démonstration. (i) Soit p un élément premier du domaine A et soit $p = bc$, où $b, c \in A$. Alors p divise bc et, comme p est premier, p divise l'un au moins des deux facteurs b ou c, disons $p \mid b$. Mais alors $b = np$ pour un certain $n \in A$ et $p = npc$, d'où $nc = 1$ et $c \in A^\times$.

(ii) Soit a un élément irréductible du domaine A dans lequel tout couple d'éléments admet un pgcd. Si $a \mid bc$, où $b, c \in A$, et si $a \nmid b$, alors $\text{pgcd}(a, b) \sim 1$. On obtient avec 0.4.7 que $a \mid c$. □

Remarque 0.5.6. Si on veut uniquement prouver qu'un élément irréductible d'un domaine principal A est premier dans A on peut aussi utiliser la relation de Bezout 0.5.3. Si l'élément $a \in A$ est irréductible dans le domaine principal A, si $a \mid bc$ et si $a \nmid b$, alors $\text{pgcd}(a, b) \sim 1$ et on a : $1 = sa + tb$, pour certains $s, t \in A$. Il vient : $c = sac + tbc$ et $a \mid c$.

Exemples 0.5.7. (i) Les éléments irréductibles de $\mathbb{Z}$ sont les $\pm p$, où p est un nombre premier naturel. Ce sont aussi les éléments premiers de $\mathbb{Z}$.

(ii) Soit K un corps et X une indéterminée. Un polynôme P de $K[X]$ de degré 2 ou 3 sans racines dans K est irréductible dans $K[X]$, et aussi premier dans $K[X]$ puisque $K[X]$ est un domaine principal.

(iii) Dans l'anneau $K[t]$ des polynômes en une indéterminée t à coefficients dans un corps K considérons le sous-anneau $A = K[t^2, t^3]$.

On a : $t^2 \mid (t^3)^2$ dans A mais $t^2 \nmid t^3$ dans A, t^2 n'est pas premier dans A.

Cependant t^2 est irréductible dans A car la seule façon d'écrire t^2 comme produit d' éléments non inversibles dans $K[t]$ est d'écrire $t^2 = (ct) \cdot (c^{-1}t)$, où $c \in K^\times$, et que $ct \notin A$.

Le domaine A n'est donc pas principal.

Dans le cas où K est le corps des réels, l'anneau A correspond à la courbe du plan réel d'équations paramétriques

$$\begin{cases} x &= t^3 \\ y &= t^2 \end{cases}$$

d'équation cartésienne $y^3 = x^2$. Le fait que A ne soit pas principal est lié au fait que cette courbe a un point singulier à l'origine.

(iv) La théorie des nombres offre aussi de nombreux exemples d'éléments irréductibles non premiers (cf. 1.1.14), de domaines non principaux.

Voici une caractérisation des éléments premiers.

Proposition 0.5.8. *Soit a un élément non nul d'un domaine A. Alors*
a est premier dans $A \Leftrightarrow$ l'anneau quotient A/aA est intègre.

Démonstration. Désignons par $\overline{x}$ l'image d'un élément quelconque $x \in A$ par l'homomorphisme naturel $A \to A/aA$, autrement dit écrivons $\overline{x} = x + aA$. Avec ces notations nous avons $\overline{x} = \overline{0} \Leftrightarrow x \in aA \Leftrightarrow a|x$. Rappelons encore que, $\forall x, y \in A$, on a $\overline{x}.\overline{y} = \overline{xy}$ et $\overline{x} + \overline{y} = \overline{x+y}$. De plus, les éléments de $\overline{A} = A/aA$ sont tous de la forme $\overline{x}$, où $x \in A$.

$\Rightarrow$. Si a est premier dans A, il est non inversible par définition, on a donc $aA \neq A$ et $\overline{A}$ est non nul. Nous avons aussi : $\forall x, y \in A$

$$(\overline{x}.\overline{y} = \overline{0}) \Leftrightarrow (a|xy) \Rightarrow (a|x \text{ ou } a|y) \Leftrightarrow (\overline{x} = \overline{0} \text{ ou } \overline{y} = \overline{0}),$$

ce qui signifie que l'anneau non nul $\overline{A} = A/aA$ est intègre.

$\Leftarrow$. Si l'anneau $\overline{A} = A/aA$ est intègre, il est non nul par définition, $aA \neq A$ et a est non inversible dans A. Nous avons aussi : $\forall x, y \in A$

$$(a|xy) \Leftrightarrow (\overline{x}.\overline{y} = \overline{xy} = \overline{0}) \Rightarrow (\overline{x} = \overline{0} \text{ ou } \overline{y} = \overline{0}) \Leftrightarrow (a|x \text{ ou } a|y),$$

ce qui signifie que l'élément non inversible a de A est premier dans A. □

Corollaire 0.5.9. *Soit a un élément non nul d'un domaine A.*
Si a n'est pas irréductible dans A alors l'anneau quotient A/aA n'est pas intègre.

Dans le cas où le domaine A est principal nous pouvons dire plus.

Proposition 0.5.10. *Soit A un domaine principal et soit $0 \neq a \in A$. Alors :*
a est premier dans $A \Leftrightarrow$ l'anneau quotient A/aA est un corps.

Démonstration. Si a est n'est pas premier dans A l'anneau quotient A/aA n'est pas intègre (voir 0.5.8), à fortiori n'est pas un corps.

Supposons maintenant que a est premier dans A et reprenons les notations introduites en 0.5.8. Soit $x \in A$ tel que $\overline{x} \neq \overline{0}$, autrement dit tel que $x \notin aA$. Alors $\text{pgcd}(a, x) \sim 1$ car a est premier et à fortiori irréductible dans A, voir 0.5.5. Nous avons donc des éléments $s, t \in A$ tels que $1 = as + xt$, voir la relation de Bezout pour les domaines principaux 0.5.3. Prenons les images dans le quotient A/aA. Comme $\overline{a} = \overline{0}$ il vient $\overline{1} = \overline{x}\overline{t}$, ce qui montre que $\overline{x}$ est inversible dans l'anneau quotient $\overline{A} = A/aA$. □

Avec 0.5.10 nous retrouvons le fait bien connu que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un premier naturel.

Les considérations précédentes nous permettent de retrouver aussi un résultat sans doute déjà rencontré, mais important en théorie des nombres.

Corollaire 0.5.11. *Soit K un corps et soit $F \in K[X]$ un polynôme de degré positif.*

Si F n'est pas irréductible dans $K[X]$, l'anneau quotient $K[X]/FK[X]$ n'est pas intègre.

Si F est irréductible dans $K[X]$, l'anneau quotient $K[X]/FK[X]$ est un corps.

Il est temps d'élargir la classe des domaines principaux tout en mettant en évidence ses propriétés de factorisation.

Définition 0.5.12. Un domaine **factoriel** est un domaine A où tout élément non nul non inversible est produit d'éléments irréductibles de A, et ce de façon essentiellement unique, ce qui signifie que, pour tout $a \in A$, $0 \neq a \notin A^\times$, on peut écrire

$$a = p_1 p_2 \cdots p_r \quad \text{où les } p_i \text{ sont irréductibles dans } A,$$

et que, si $a = q_1 q_2 \cdots q_s$ est une autre factorisation de a en produits d' irréductibles q_j, alors $r = s$ et on a une permutation σ de l'ensemble d'indices $\{1, 2, \cdots, r\}$ telle que $p_i \sim q_{\sigma(i)}, \quad 1 \leqslant i \leqslant r$.

Le nombre r est alors appelé la *longueur* de la factorisation de a.

Proposition 0.5.13. *Dans un domaine factoriel, tout couple d' éléments possède un* pgcd.

Démonstration. Soit $a, b \in A$. Si l'un des éléments a ou b est nul ou inversible, l'existence du pgcd(a, b) est évidente. Supposer donc que a et b sont tous deux non nuls non inversibles et regardons leur factorisation. Posant comme d'habitude $x^0 = 1$ nous pouvons écrire

$$a = u \prod_{1 \leqslant i \leqslant n} p_i^{r_i} \quad \text{et} \quad b = v \prod_{1 \leqslant i \leqslant n} p_i^{s_i}$$

où $u, v \in A^\times$, où les p_i sont des éléments irréductibles non associés deux à deux et où les exposants r_i, s_i sont des naturels $\geqslant 0$.

Remarquons d'abord que $a \mid b$ si et seulement si, $\forall i, 1 \leqslant i \leqslant n$, $r_i \leqslant s_i$.

En général et quels que soient nos exposants prenons pour chaque i le naturel $\ell_i = \text{minimum}\{r_i, s_i\}$. Il suffit d'observer avec notre remarque que le produit $\prod_{1 \leqslant i \leqslant n} p_i^{\ell_i}$ est un pgcd de a et b. □

Voici d'autres caractérisations des domaines factoriels.

Théorème 0.5.14. *Soit A un domaine où tout élément non nul non inversible est produit d'éléments irréductibles. Les conditions suivantes sont équivalentes :*

(i) A est factoriel,

(ii) tout couple d'éléments de A admet un pgcd*,*

(iii) tout élément irréductible de A est premier dans A.

Démonstration. $(i) \Rightarrow (ii)$ Ceci est dans 0.5.13.

$(ii) \Rightarrow (iii)$ Ceci est dans 0.5.5.

$(iii) \Rightarrow (i)$ Soient deux factorisations de l'élément non nul non inversible a de A

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

où les p_i et les q_j sont irréductibles dans A. Nous devons montrer que $r = s$ et qu'il existe une permutation σ de l'ensemble d'indices $\{1, \cdots, s\}$ telle que $p_i \sim q_{\sigma(i)}$.

Si $r = 1$, alors $s = 1$ et c'est terminé.

Supposons maintenant $r > 1$. Alors $s > 1$. Comme p_1 est premier par hypothèse et que $p_1 \mid q_1 q_2 \cdots q_s$ on a que p_1 divise un des q_i ; quitte à permuter nos facteurs nous pouvons supposer que $p_1 \mid q_1$. Mais alors $p_1 \sim q_1$ et $q_1 = up_1$ pour un certain $u \in A^\times$. Nous simplifions par p_1, nous écrivons $uq_2 = q_2' \sim q_2$, nous obtenons $p_2 \cdots p_r = q_2' \cdots q_s$ et nous terminons par une induction sur le nombre r de facteurs intervenant dans la première factorisation. □

Remarque 0.5.15. On peut aussi montrer que tout élément irréductible d'un domaine factoriel est premier sans passer par les pgcd, en argumentant comme suit. Si l'élément irréductible a du domaine factoriel A divise le produit bc, $b, c \in A$, on a $bc = ma$ pour un certain $m \in A$ et on écrit les éléments b, c et m comme produit d'irréductibles. L'unicité de la factorisation de l'élément $bc = ma$ nous indique que a est associé à au poins un des facteurs irréductibles de b ou de c, donc que $a \mid b$ ou $a \mid c$.

(En mathématique comme partout les façons d'argumenter sont nombreuses.)

Reste à montrer que tout domaine principal est factoriel. Au vu de 0.5.5 et 0.5.14 il suffit de montrer que tout élément non nul non inversible d'un domaine principal est produit d'éléments irréductibles.

Notons que le cas de l'anneau $\mathbb{Z}$ des entiers et celui d'un anneau de polynômes $K[X]$ en une indéterminée X à coefficient dans un corps commutatif se traitent assez facilement. Il suffit de procéder par induction sur la valeur absolue dans le premier cas, sur le degré dans le second.

Pour le cas général nous utiliserons l'axiome du choix de façon essentielle.

Théorème 0.5.16. *Tout domaine principal est factoriel.*

Démonstration. Soit A un domaine principal. Au vu de 0.5.5 et 0.5.14 il suffit de montrer l'existence des factorisations.

Remarquons d'abord que la réunion d'une suite croissante quelconque d'idéaux de A

$$a_0A \subseteq a_1A \subseteq \cdots \subseteq a_nA \subseteq \cdots$$

est un idéal de A, donc de la forme bA pour un certain $b \in A$. De plus, comme $b \in bA = \bigcup_{n\in\mathbb{N}} a_nA$, nous avons que $b \in a_iA$ pour un certain $i \in \mathbb{N}$. Mais alors

$$\bigcup_{n\in\mathbb{N}} a_nA = bA \subseteq a_iA \subseteq a_{i+1}A \subseteq \cdots \subseteq \bigcup_{n\in\mathbb{N}} a_nA$$

$$\text{et} \quad a_iA = a_{i+1}A = \cdots = \bigcup_{n\in\mathbb{N}} a_nA,$$

ce qui s'exprime en disant que la suite stationne en a_iA.

On retient que toute suite croissante d'idéaux du domaine principal A est stationnaire.

Ceci étant nous procédons par l'absurde. Supposons que l'ensemble E des éléments non nuls non inversibles de A qui ne sont pas produit d'un nombre fini d'éléments irréductibles soit non vide. Tout élément $x \in E$ peut s'écrire $x = yz$, où $y, z \notin A^\times$ et où au moins un des deux facteurs y, z est dans E (sinon $x = yz$ serait produit d'un nombre fini d'éléments irréductibles). Avec l'axiome du choix nous pouvons choisir, pour tout $x \in E$, un diviseur strict $c(x)$ de x appartenant à E, ce qui fournit une fonction $c : E \to E$.

Dès lors partons d'un élément quelconque x_0 de E et posons $x_i = c^i(x_0)$. Nous obtenons une suite d'éléments $x_0, x_1, \cdots, x_n \cdots$ et aussi une suite strictement croissante d'idéaux

$$x_0A \subsetneq x_1A \subsetneq \cdots x_nA \subsetneq \cdots$$

en contradiction avec le fait que toute suite croissante d'idéaux est stationnaire. □

0.5.17. *Conclusion.* Si on parvient à exhiber un élément irréductible non premier d'un domaine donné, on aura montré que ce domaine n'est ni principal ni factoriel (0.5.5 , 0.5.14).

0.6 Factorisation d'homomorphismes

Théorème 0.6.1. Théorème de l'homomorphisme.

Si $f : A \to B$ est un homomorphisme d'anneaux, son noyau $ker(f) = \{x \in A \mid f(x) = 0\}$ est un idéal de A et son image $im(f) = \{f(x) \mid x \in A\}$ est un sous-anneau de B.

Les classes latérales $x+ker(f)$, où $x \in A$, sont les classes de l'équivalence associée à la fonction f :

$$x + ker(f) = \{y \in A \mid f(y) = f(x)\}.$$

Ainsi la fonction f induit une bijection

$$\bar{f} : A/ker(f) \to im(f), : x + ker(f) \mapsto f(x).$$

On voit rapidement que cette bijection est un isomorphisme d'anneaux, s'inscrivant dans un diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/ker(f) & \xrightarrow{\bar{f}} & im(f) \end{array}$$

$$f = i \circ \bar{f} \circ p$$

où p est la projection naturelle de A sur son quotient $A/ker(f)$, où i est l'injection naturelle de $im(f)$ dans B et où la fonction$\bar{f}$ définie ci-dessus est un isomorphisme.

Exemple 0.6.2. Rappelons que, si A est un sous-anneau de l'anneau B et si $b \in B$, la fonction d'**évaluation** en b,

$$e_b : A[X] \to B, P \mapsto P(b)$$

est un homomorphisme d'anneaux dont l'image est $A[b]$. L'évaluation en b induit donc un isomorphisme $\overline{e_b} : A/\ker(e_b) \xrightarrow{\sim} A[b]$.

Si de plus $b \in A$, alors $\ker(e_b) = (X - b)A[X]$.

Voici une première application de ce théorème.

Proposition 0.6.3. *(i) Soit m et n deux nombres naturels premiers entre eux. Alors l'homomorphisme naturel*

$$f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n : z \mapsto (z_m, z_n)$$

est surjectif et induit un isomorphisme d'anneaux

$$\mathbb{Z}_{mn} \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n$$

(ii) Soit K un corps commutatif et soit $P, Q \in K[X]$ deux polynômes premiers entre eux. Alors l'homomorphisme naturel

$$g : K[X] \to (K[X]/PK[X]) \times (K[X]/QK[X]) : T \mapsto (T+PK[X], T+QK[X])$$

est surjectif et induit un isomorphisme d'anneaux

$$K[X]/PQK[X] \xrightarrow{\sim} (K[X]/PK[X]) \times (K[X]/QK[X])$$

Démonstration. (i) Comme m et n sont premiers entre eux nous avons $\ker(f) = mn\mathbb{Z}$. D'où $\#\mathrm{Im}(f) = \#\mathbb{Z}/\ker(f) = mn$. Mais $\mathrm{Im}(f) \subset \mathbb{Z}_m \times \mathbb{Z}_n$ et nous avons aussi $\#(\mathbb{Z}_m \times \mathbb{Z}_n) = mn$. Donc $\mathrm{Im}(f) = Z_m \times \mathbb{Z}_n$, f est surjectif et on conclut avec le théorème.

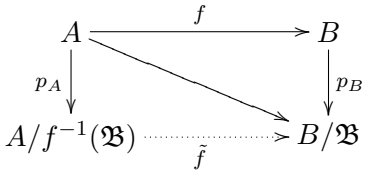
(ii) Cette seconde assertion se démontre à peu près comme la première. Comme P et Q sont premiers entre eux nous avons $\ker(g) = PQK[X]$ et $\mathrm{Im}(g) \simeq K[X]/\ker(g) = K[X]/PQK[X]$ est un espace vectoriel sur K de dimension $(\deg(P) + \deg(Q)$.

Mais $\mathrm{Im}(g)$ est un sous-espace vectoriel de $(K[X]/PK[X]) \times (K[X]/QK[X])$ et $(K[X]/PK[X]) \times (K[X]/QK[X])$ est aussi un espace vectoriel sur K de dimension $(\deg(P) + \deg(Q)$. On conclut avec un argument de dimension : $\mathrm{Im}(g) = (K[X]/PK[X]) \times (K[X]/QK[X])$. □

La proposition suivante est une conséquence du théorème de l'homomorphisme. On l'utilise souvent de manière implicite.

Proposition 0.6.4. *Soit $f : A \twoheadrightarrow B$ un homomorphisme surjectif d'anneaux et soit $\mathfrak{B}$ un idéal de B.*

Alors $f^{-1}(\mathfrak{B}) := \{x \in A \mid f(x) \in \mathfrak{B}\}$ est un idéal de A et f induit un isomorphisme $\tilde{f}$ comme indiqué dans le diagramme commutatif suivant

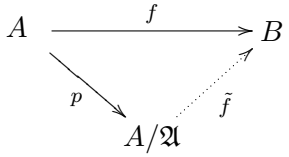


où p_A et p_B désignent les projections naturelles ($ker(p_B \circ f) = f^{-1}(\mathfrak{B})$).

Si $\mathfrak{B} = (b_1, \cdots, b_n)$, si $a_1, \cdots, a_n$ sont des éléments de A tels que $f(a_i) = b_i$ et si $ker(f) = (c_1, \cdots, c_r)$, alors $f^{-1}(\mathfrak{B}) = (a_1, \cdots, a_n, c_1, \cdots, c_r)$.

De plus, la fonction qui applique un idéal $\mathfrak{B}$ de B sur l'idéal $f^{-1}(\mathfrak{B})$ de A est une bijection entre l'ensemble des idéaux de B et celui des idéaux de A contenant $ker(f)$. Nous dirons de cette bijection qu'elle est induite par f.

Théorème 0.6.5. Propriété universelle des anneaux quotients. *Pour tout homomorphisme d'anneaux $f : A \to B$ s'annulant sur un idéal $\mathfrak{A}$ de A il existe un unique homomorphisme $\tilde{f} : A/\mathfrak{A} \to B$ tel que $\tilde{f} \circ p = f$, où p désigne la projection naturelle*



Cet homomorphisme est défini par $\tilde{f}(a+\mathfrak{A}) = f(a)$ *et* $ker(\tilde{f}) = p(ker(f))$.

Corollaire 0.6.6. *Soit* $\mathfrak{B} \subset \mathfrak{C}$ *deux idéaux de l'anneau* A.
Alors $\mathfrak{C}/\mathfrak{B} := \{c+\mathfrak{B} \mid c \in \mathfrak{C}\}$ *est un idéal de l'anneau quotient* $A/\mathfrak{B}$ *et*

$$(A/\mathfrak{B})/(\mathfrak{C}/\mathfrak{B}) \tilde{\to} A/\mathfrak{C}.$$

0.7 Caractéristique d'un anneau

Définition 0.7.1. La **caractéristique** d'un anneau est l'ordre de 1 dans le groupe $(A,+)$ si cet ordre est fini, 0 sinon. Nous la désignerons par $\mathrm{char}(A)$.

Observation 0.7.2. (i) Dans un anneau A de caractéristique positive n on a donc $na = n1.a = 0$ pour tout $a \in A$.

(ii) Rappelons que, pour tout anneau A, il existe un et un seul homomorphisme de l'anneau $\mathbb{Z}$ des entiers dans A

$$u_A : \mathbb{Z} \to A : z \mapsto z1$$

Le noyau de cet homomorphisme est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$, pour un certain $n \in \mathbb{N}$. On remarque alors :

$$\mathrm{char}(A) = n \Leftrightarrow \ker(u_A) = n\mathbb{Z}.$$

Ceci a quelques conséquences.

(iii) Tout anneau de caractéristique nulle contient naturellement un sous-anneau isomorphe à $\mathbb{Z}$.

Tout corps de caractéristique nulle contient naturellement un sous-corps isomorphe à $\mathbb{Q}$.

Tout anneau de caractéristique positive n contient naturellement un sous-anneau isomorphe à $\mathbb{Z}_n$.

La caractéristique d'un corps est soit nulle soit un nombre premier naturel p.

Tout corps de caractéristique positive p contient naturellement un sous-corps isomorphe à $\mathbb{Z}_p$ (p est un nombre premier).

La caractéristique d'un anneau fini est toujours positive

0.8 Modules

Nous aurons aussi à utiliser le langage des modules.

Définitions 0.8.1. Soit A un anneau. Un **A-module** est un groupe commutatif $(M, +)$ muni d'une multiplication scalaire par les éléments de l'anneau A, c.-à-d. d'une fonction

$$A \times M \to M : (a, w) \mapsto aw$$

telle que, $\forall a, b \in A, \quad \forall v, w \in M$, on a :
$a(v + w) = av + aw, \quad (a + b)v = av + bv \quad$ (double distributivité),
$a(bv) = (ab)v \quad$ (associativité mixte),
$1v = v$.

Si $A = K$ est un corps un A-module n'est donc rien d'autre qu'un espace vectoriel sur le corps K (un K-vectoriel).

Un **homomorphisme de A-modules** est un homomorphisme de groupes $f : M \to M'$ tel que, $\forall a \in A, w \in M, f(aw) = af(w)$.

Un **sous-A-module** du A-module M est un sous-groupe M' de M tel que, $\forall w \in M'$ et $\forall a \in A$, on aie $aw \in M'$.

Définitions 0.8.2. Une partie G d'un A-module M est dite **génératrice** si tout élément w de M peut s'écrire comme combinaison linéaire à coefficients dans A d'éléments de G

Un A-module **de type fini** est un A-module possédant une partie génératrice finie.

Un A-module **cyclique** est un A-module pouvant être engendré par un seul élément.

Une partie L d'un A-module M est dite **libre** ou **linéairement indépendante** si, pour tout $n > 0$, toute suite finie $w = (w_1, \cdots, w_n)$ d'éléments de L distincts deux-à-deux et toute suite finie $a = (a_1, \cdots, a_n)$ d'éléments de l'anneau A,

$$\left(\sum_{i=1}^{n} a_i w_i = 0 \right) \Rightarrow (\forall i, 1 \leqslant i \leqslant n, \quad a_i = 0).$$

Une partie B d'un A-module M est une **base** de M si B est à la fois génératrice et libre.

Un A-module M est **libre** s'il possède une base.

Le **rang** d'un A-module libre est le cardinal d'une quelconque de ses bases. (Ceci a un sens : comme A est un anneau *commutatif* , on peut montrer que toutes les bases d'un A-module libre M ont même cardinal.)

Dans le cas où le A-module M a aussi une structure de module sur d' autres anneaux, ce qui est courant, il convient de préciser à laquelle de ces structures nos vocables se rapportent. Plutôt que dire d'une partie P de

M qu'elle est une partie génératrice, libre ou base du A-module M, nous dirons parfois plus simplement qu'elle est une partie A-génératrice, A-libre ou A-base de M. Par exemple, $\mathbb{C}$ a une structure de $\mathbb{C}$-module et aussi de $\mathbb{R}$-module, $\{1\}$ est une $\mathbb{C}$-base de $\mathbb{C}$, $\{1, i\}$ en est une $\mathbb{R}$-base.

Remarques 0.8.3. Soit A un anneau.

(i) Quand l'anneau A n'est pas un corps, la plupart des A-modules ne sont pas libres.

(ii) A et A^n peuvent être vu comme A-modules. Les sous-A-modules de l'anneau A sont ses idéaux.

(iii) Les A-modules libres de type fini et de rang n sont les A-modules isomorphes à A^n.

(iv) Tout A-module de type fini est une image homomorphe d'un A-module libre de type fini.

Plus précisément, si le A-module M est engendré par ses éléments $w_1, \cdots, w_n$, la fonction

$$A^n \to M : (a_1, \cdots, a_n) \mapsto \sum_{i=1}^{n} a_i w_i$$

est un homomorphisme surjectif de A-modules.

(vi) Si le A-module M est annulé par un idéal $\mathfrak{A}$ de A (ce qui signifie que, $\forall a \in \mathfrak{A}$ et $\forall w \in M$, on a $aw = 0$), alors M a aussi une structure de $A/\mathfrak{A}$-module, définie par $\bar{a}w = aw$, où $\bar{a}$ désigne l'image de a par la projection naturelle $A \to A/\mathfrak{A}$.

(vii) Tout groupe commutatif $(M, +)$ a une structure de $\mathbb{Z}$-module définie comme suit : $\forall w \in M$, $\forall n \in \mathbb{N}_0$, on écrit

$$nw = \underbrace{w + \ldots + w}_{n \text{ fois}}, \quad 0w = 0, \quad (-n)w = n(-w).$$

(Les vérifications $\forall w, w' \in M, \forall z, z' \in \mathbb{Z}$, $(z + z')w = (zw + z'w)$, $(zz')w = z(z'w)$, $z(w + w') = (zw + zw')$, $1w = w$ sont immédiates.)

(viii) Tout homomorphisme entre A-modules libres de type fini peut se décrire par une matrice à entrées dans A, après le choix d'une base de chacun des modules concernés.

Nous désignerons par $A^{m\times n}$ l'ensemble des matrices à m lignes et n colonnes à entrées dans l'anneau A. Nous désignerons aussi par I_n la matrice identique de $A^{n\times n}$: $I_{n_{ij}} = \delta_{ij}$.

0.8.4. Rappels d'algèbre linéaire. (i) Soit A un anneau et soit f un endomorphisme d' un A-module M libre de type fini et de rang n, soit encore $e = (e_1, e_2, \cdots, e_n)$ une base de ce A-module. Les $f(e_i)$ s'écrivent de façon unique comme combinaisons linéaires à coefficients dans A des e_k :

$f(e_i) = \sum_k f_{ki} e_k$. Les f_{ki} sont les entrées d'une matrice $F_e \in A^{n\times n}$ dont on peut prendre la trace, le déterminant et le polynôme caractéristique :

$$\mathrm{Tr}(F_e) = \sum_i f_{ii} \in A, \quad \det(F_e) \in A, \quad \mathrm{Char}_{F_e} = \det(XI_n - F_e) \in A[X].$$

Notons que Char_{F_e} ainsi défini est un polynôme unitaire de $A[X]$.

Si $u = (u_1, u_2, \cdots, u_n)$ est une autre base de M : $u_j = \sum_k c_{kj} e_k$, les c_{kj} sont les entrées d'une matrice inversible $C_{u(e)} \in A^{n\times n}$ appelée matrice du changement de base et la matrice F_u décrivant l'endomorphisme f de M dans la base u est liée à la matrice F_e par la relation $F_u = C_{u(e)}^{-1} F_e C_{u(e)}$.

Or, $\forall G, H \in A^{n\times n}$, on a $\det(GH) = \det(G)\det(H)$ et $\mathrm{Tr}(GH) = \mathrm{Tr}(HG)$. Il en résulte que $\mathrm{Tr}(F_e)$, $\det(F_e)$, Char_{F_e} ne dépendent que de l'endomorphisme f et non de la base choisie pour décrire f par une matrice. Nous pouvons donc définir **la trace, le déterminant et le polynôme caractéristique de l'endomorphisme** f par

$$\mathrm{Tr}(f) = \mathrm{Tr}(F_e), \quad \det(f) = \det(F_e), \quad \mathrm{Char}_f = \mathrm{Char}_{F_e}.$$

Développons les déterminants et écrivons

$$\mathrm{Char}_f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \quad a_i \in A.$$

On obtient $\mathrm{Tr}(f) = -a_{n-1}$ et $\det(f) = (-1)^n a_0$.

(ii) Rappelons encore le théorème de Cayley-Hamilton : $\mathrm{Char}_f(f) = 0$.

(iii) Voici une façon rapide de traiter les changements de base : pour bénéficier de la notation matricielle écrivons les coefficients à droite et non gauche, écrivons $f(e_i) = \sum_k e_k f_{ki}$ et $u_j = \sum_k e_k c_{kj}$. En notation matricielle ceci se réecrit :

$$f(e) = e \cdot F_e \quad u = e \cdot C_{u(e)} \quad \text{d'où}$$

$$f(u) = f(e) \cdot C_{u(e)} = e \cdot F_e \cdot C_{u(e)} = u \cdot C_{u(e)}^{-1} \cdot F_e \cdot C_{u(e)} \quad \text{et}$$

$$F_u = C_{u(e)}^{-1} F_e C_{u(e)}.$$

(iv) Pour terminer ce premier rappel, observons qu'une matrice $C \in A^{n\times n}$ est inversible dans l'anneau des matrices $A^{n\times n}$ si et seulement si $\det(C) \in A^\times$.

0.8.5. Second rappel d'algèbre linéaire. Soit A un anneau et soit M un A-module. Nous désignerons par M^* le **dual** du module M :

$$M^* := \mathrm{Hom}_A(M, A).$$

Les éléments de M^* sont souvent appelés des formes A-linéaires sur M.

Si M est un A-module libre de type fini, alors M^* est aussi un un A-module libre de type fini. Plus précisément, si $e = (e_1, \cdots, e_n)$ est une base de M, alors les formes $e_i^* \in M^*$ définies par $e_i^*(e_j) = \delta_{ij}$ forment une base de M^* appelée base duale de la base e et le plus souvent notée e^*.

Définitions 0.8.6. (i) On définit la **somme directe** de deux A-modules M_1 et M_2 par

$$M_1 \oplus M_2 = \{(w_1, w_2) \mid w_1 \in M_1, w_2 \in M_2\}$$

l'addition et la multiplication scalaire étant définie composante par composante.

(ii) Nous dirons aussi qu'un A-module M est somme directe de ses deux sous-A-modules M_1 et M_2, et nous écrirons $M = M_1 \oplus M_2$ si l'homomorphisme

$$M_1 \oplus M_2 \to M : (w_1, w_2) \mapsto w_1 + w_2$$

est bijectif, autrement dit si $\quad M = M_1 + M_2 \quad$ et si $\quad M_1 \cap M_2 = \{0\}$.

Dans ce cas, nous dirons que M_1 (et aussi M_2) est un **sommant direct** de M.

Remarque 0.8.7. Si $M = M_1 \oplus M_2$, si M_1 est libre de rang r_1 et si M_2 est libre de rang r_2, alors M est libre de rang $r = r_1 + r_2$.

0.8.8. Si M' est un sous-A-module du A-module M, le groupe quotient M/M' est naturellement muni d'une structure de A-module par : $\forall a \in A, \forall w \in M, \quad a \cdot (w + M') = aw + M'$. On dispose aussi d'un théorème de l'homomorphisme pour les modules : les théorèmes et propositions 0.6.1, 0.6.5, 0.6.4 admettent une version module. Rappelons aussi les isomorphismes suivants.

Théorème 0.8.9. *Soit M un A-module et M_1, M_2 deux sous-A-modules de M. Alors*

(i) $$(M_1 + M_2)/M_2 \simeq M_1/(M_1 \cap M_2.$$

(ii) Si $M_1 \subset M_2$, alors M_2/M_1 est un sous-A-module de M/M_1 et

$$(M/M_1)/(M_2/M_1) \simeq M/M_2.$$

0.9 Vers les nombres

Le premier objet de la théorie des nombres est l'étude des entiers naturels. Depuis l'antiquité on sait que tout entier naturel $n > 1$ est produit de

nombres premiers et ce de façon unique (à l'ordre des facteurs près, dans un produit, nous pouvons toujours permuter deux facteurs puisque la multiplication est commutative). Euclide a utilisé cette propriété des naturels pour montrer qu'il existe une infinité de nombres premiers. Cette propriété a aussi été utilisée pour montrer l'irrationnalité de certains nombres, dont $\sqrt{2}$.

Théorème 0.9.1. *(Euclide) Parmi les nombres naturels il existe une infinité de nombres premiers.*

Démonstration. Procédons par l'absurde et supposons qu'on n'aie qu'un nombre fini de nombres premiers. Soient alors $p_1, p_2, \cdots, p_k$ ces nombres et regardons le nombre $n = p_1 \cdot p_2 \cdots p_k + 1$. Ce nombre $n > 1$ n'est divisible par aucun des p_i, par aucun nombre premier, et n'est pas produit de nombres premiers. Cette contradiction termine la preuve. □

Voici une autre propriété remarquable des entiers naturels et rationnels.

Théorème 0.9.2. *(Petit théorème de Fermat) Soit p un nombre premier.*
(i) Pour tout $x \in \mathbb{Z}_p$ on a $x^p = x$.
(ii) Pour tout $a \in Z$, $a^p - a$ est multiple de p,
autrement dit $a^p \cong a$ modulo p.
(iii) Pour tout $a \in Z$ tel que $\text{pgcd}(a, p) = 1$, $a^{p-1} - 1$ est multiple de p,
autrement dit $a^{p-1} \cong 1$ modulo p.

Démonstration. (i) Les éléments non nuls du corps $\mathbb{Z}_p$ forment un groupe multiplicatif d'ordre $p - 1$. Comme l'ordre d'un élément d'un groupe divise l'ordre du groupe, tout élément non nul x de $\mathbb{Z}_p$ satisfait l'équation $x^{p-1} = 1$. Multiplions par x, on obtient l'égalité $x^p = x$, qui est aussi vraie pour $x = 0$.

(ii), (iii) Ces deux assertions sont une conséquence directe de la première. □

Vocabulaire 0.9.3. Un **nombre algébrique** est un nombre complexe x pour lequel on a une relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, où les a_i sont des nombres rationnels. Si de plus les a_i sont des nombres entiers, on dit que x est un **entier algébrique**.

Les entiers rationnels sont évidemment des entiers algébriques. Ce ne sont pas les seuls. Par exemple, les nombres $\sqrt{2}$, $\sqrt{3}$, $e^{\frac{2\pi i}{n}}$ sont des entiers algébriques, notons que $e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$.

Définition 0.9.4. Le **polynôme minimal** (sur $\mathbb{Q}$) d'un nombre algébrique α est le **polynôme unitaire** $P \in \mathbb{Q}[X]$ de degré minimum s'annulant en α.

(Un polynôme unitaire est un polynôme dont le degré du terme le plus élevé est 1.)

Le polynôme minimal du nombre algébrique α est aussi l'unique polynôme unitaire engendrant l'idéal principal $\ker(e_\alpha)$ où e_α est l'homomorphisme d'évaluation $\quad \mathbb{Q}[X] \to \mathbb{C} : T \mapsto T(\alpha)$.

– –

0.9.5. Exercice*. (i) Soit p un nombre premier naturel et regardons les coefficients binomiaux $\left(\begin{array}{c} p \\ i \end{array} \right) = \dfrac{p!}{i!(p-i)!}$. On a

$$\left(\begin{array}{c} p \\ i \end{array} \right) \cong 0 \text{ modulo } p \quad \text{pour} \quad 1 \leqslant i \leqslant p-1.$$

(ii) Soit encore $n \in \mathbb{N}_0$. Plus généralement on a

$$\left(\begin{array}{c} p^n \\ i \end{array} \right) \cong 0 \text{ modulo } p \quad \text{pour} \quad 1 \leqslant i \leqslant p^n-1.$$

0.9.6. Exercice*. Soit $m, n \in \mathbb{N}_0$ et soit X une indéterminée. On a

$$(i) \quad X^m - 1 = (X-1)(X^{m-1} + X^{m-2} + \cdots + X + 1),$$

$$(ii) \quad m \mid n \Rightarrow (X^m - 1) \mid (X^n - 1) \quad \text{dans} \quad \mathbb{Z}[X].$$

0.9.7. Exercice*. Montrer : $\sqrt{5} \notin \mathbb{Q}$.

Plus généralement, montrer que, si d est un entier naturel qui n'est pas carré d'un autre naturel, alors $\sqrt{d} \notin \mathbb{Q}$.

0.9.8. Exercice. Montrer que $\sqrt{2}+\sqrt{3}$ est un nombre algébrique, et même un entier algébrique, calculer son polynôme minimal sur $\mathbb{Q}$.

Montrer que $\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$, que $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ a une structure d'espace vectoriel sur $\mathbb{Q}$ de dimension 4.

Chapitre 1

Premières promenades

Nos premières promenades nous emmèneront au pays des corps quadratiques.

1.1 Le nombre d'or φ

Le rapport entre deux longueurs ou réels positifs a, b est dit parfait si

$$\frac{a+b}{a} = \frac{a}{b}$$

Le nombre d'or, désigné par φ, est ce rapport parfait. Calculons-le.

De $\varphi = \frac{a+b}{a} = \frac{a}{b}$, il vient $1 + \frac{b}{a} = \frac{a}{b}$, $\varphi = 1 + \frac{1}{\varphi}$ et $\varphi^2 = \varphi + 1$, φ est racine de l'équation $t^2 - t - 1 = 0$. Comme φ est positif, nous obtenons

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1,618...$$

Notons que l'équation $t^2 - t - 1 = 0$ a une seconde racine φ', on a $\varphi + \varphi' = 1$ et $\varphi' = 1 - \varphi$.

Regardons l'inverse de φ. De $\varphi^2 - \varphi = 1$ on déduit $\varphi^{-1} = \varphi - 1$.

Regardons maintenant les puissances de φ.

$$\begin{array}{lcl}
\varphi^1 & = & 1\varphi \\
\varphi^2 & = & 1\varphi + 1 \\
\varphi^3 & = & 2\varphi + 1 \\
\varphi^4 & = & 3\varphi + 2 \\
\varphi^5 & = & 5\varphi + 3 \\
\varphi^6 & = & 8\varphi + 5 \\
 & \vdots & \\
\varphi^n & = & u_n\varphi + v_n \quad \text{pour certains } u_n, v_n \in \mathbb{N}
\end{array}$$

On peut montrer que les suites u_n et v_n sont liées par $u_n = v_{n+1}$, que la suite des $u_n, n \geqslant 1$ est la suite de Fibonacci définie par la récurrence :

$$u_1 = 1, u_2 = 1 \quad \text{et} \quad u_{n+1} = u_n + u_{n-1} \text{ pour } n \geqslant 1.$$

Si la suite de Fibonacci apparaît dans la suite des puissances du nombre d'or φ, notons que le nombre d'or φ apparaît aussi dans la suite de Fibonacci :

$$\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \varphi.$$

Notons que Fibonacci, alias Leonardo di Pisa (1180-1250), est l'un des premiers depuis l'antiquité à étudier les propriétés des nombres et à en découvrir de nouvelles (il a entre autres observé que si deux nombres naturels sont sommes de deux carrés, leur produit l'est aussi).

Le nombre d'or a ses fans, il a fait couler beaucoup d'encre, on en trouve un bon aperçu dans Wikipedia. On le rencontre en de nombreux endroits, en géométrie dans le pentagone régulier (voir l'exercice 1.1.15), dans l'étude de certaines spirales, ... Tout ceci nous indique que la théorie des nombres a de nombreuses ramifications, en algèbre, en géométrie, en analyse.

Mais ce qui nous importe ici est que le nombre d'or φ, satisfaisant la relation $\varphi^2 - \varphi - 1 = 0$, est un entier algébrique, et nous nous proposons maintenant d'étudier le sous-anneau $\mathbb{Z}[\varphi]$ de $\mathbb{Q}[\sqrt{5}]$.

Observation 1.1.1. (a) Le nombre $\varphi = \frac{1+\sqrt{5}}{2}$ satisfait la relation

$$\varphi^2 - \varphi - 1 = 0$$

φ est un entier algébrique, son polynôme minimal sur $\mathbb{Q}$ est le polynôme $X^2 - X - 1$ ($\sqrt{5} \notin \mathbb{Q}$).

(b) Comme les puissances de φ sont des combinaisons linéaires à coefficients entiers de 1 et φ, nous avons $\mathbb{Z}[\varphi] = \{a + b\varphi \mid a, b \in \mathbb{Z}\}$.

(c) $\mathbb{Z}[\varphi]$ a aussi une structure de $\mathbb{Z}$-module. Comme les nombres φ et $\sqrt{5}$ ne sont pas rationnels, ils sont linéairement indépendants sur $\mathbb{Z}$.

En tant que $\mathbb{Z}$-module, $\mathbb{Z}[\varphi]$ est donc un $\mathbb{Z}$-module libre de rang 2, de base $(1, \varphi)$.

(d) $\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}[\varphi] \subset \mathbb{Q}[\sqrt{5}]$, ces inclusions sont strictes.

(e) $\mathbb{Q}[\varphi] = \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, en tant que $\mathbb{Q}$-vectoriel, $\mathbb{Q}[\sqrt{5}]$ admet pour base $(1, \sqrt{5})$, et aussi $(1, \varphi)$.

De plus, $\mathbb{Q}[\sqrt{5}]$ est un sous-corps du corps des nombres réels.

(Si $0 \neq a+b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, où $a, b \in \mathbb{Q}$, nous avons $(a-b\sqrt{5}) \neq 0, a^2-5b^2 \neq 0$ et alors $\frac{1}{a+b\sqrt{5}} = \frac{a-b\sqrt{5}}{(a+b\sqrt{5})(a-b\sqrt{5})} = \frac{a-b\sqrt{5}}{a^2-5b^2} \in \mathbb{Q}[\sqrt{5}]$.)

(f) $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}[\varphi]$ est le corps des fractions de $\mathbb{Z}[\sqrt{5}]$ et de $\mathbb{Z}[\varphi]$.

Observation 1.1.2. $\mathbb{Z}[\varphi] \simeq \mathbb{Z}[X]/(X^2 - X - 1)$.

Pour voir ceci, regardons l'homomorphisme d'évaluation

$$e_\varphi : \mathbb{Q}[X] \to \mathbb{R}, P \mapsto P(\varphi).$$

Nous avons $\text{im}(e_\varphi) = \mathbb{Q}[\varphi]$ et $\ker(e_\varphi) = (X^2 - X - 1)\mathbb{Q}[X]$.

Nous avons aussi $e_\varphi(\mathbb{Z}[X]) = \mathbb{Z}[\varphi]$.

De plus, $\ker(e_\varphi) \cap \mathbb{Z}[X] = (X^2 - X - 1)\mathbb{Z}[X]$ car la division d'un polynôme de $\mathbb{Z}[X]$ par un polynôme unitaire de $\mathbb{Z}[X]$ donne toujours un quotient et un reste dans $\mathbb{Z}[X]$.

On conclut en appliquant le théorème de l'homomorphisme pour les anneaux, $\text{dom}(f)/\ker(f) \simeq \text{im}(f)$, à la restriction de e_φ à $\mathbb{Z}[X]$.

Proposition 1.1.3. *Définissons une transformation σ de $\mathbb{Q}[\sqrt{5}]$ par*

$$\sigma : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{5}], a + b\sqrt{5} \mapsto a - b\sqrt{5}.$$

Cette transformation σ est un Q-automorphisme involutif de $\mathbb{Q}[\sqrt{5}]$, c.à-d. un automorphisme fixant les éléments de $\mathbb{Q}$ et tel que $\sigma^2 = 1$.

De plus, $\forall \alpha \in \mathbb{Q}[\sqrt{5}]$, nous avons : $\alpha = \sigma(\alpha) \Leftrightarrow \alpha \in \mathbb{Q}$.

Nous avons $\sigma(\varphi) = 1 - \varphi$ et donc $\sigma(\mathbb{Z}[\varphi]) = \mathbb{Z}[\varphi]$.

*Cet automorphisme σ sera appelé l'***automorphisme de conjugaison de** $\mathbb{Q}[\sqrt{5}]$.

Démonstration. Un simple calcul suffit. □

Remarque 1.1.4. Dans la preuve de la proposition ci-dessus, pour prouver que σ est un automorphisme, on peut éviter de calculer et procéder comme suit.

Soit $\mathbb{Q}[X]$ l'anneau des polynômes en une indéterminée X à coefficients dans $\mathbb{Q}$. Les homomorphismes d'évaluation

$$e_{(\sqrt{5})} : \mathbb{Q}[X] \to \mathbb{R} : P \mapsto P(\sqrt{5})$$

$$e_{(-\sqrt{5})} : \mathbb{Q}[X] \to \mathbb{R} : P \mapsto P(-\sqrt{5})$$

ont pour image $\mathbb{Q}[\sqrt{5}]$ et pour noyau $(X^2 - 5)\mathbb{Q}[X]$. Désignons par x l'image de X par la projection naturelle $\mathbb{Q}[X] \to \mathbb{Q}[X]/(X^2 - 5)\mathbb{Q}[X]$. Avec cette notation nos évaluations induisent deux isomorphismes décrits ci-dessous

$$\tau_1 : \mathbb{Q}[X]/(X^2 - 5)\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{5}] : a + bx \mapsto a + b\sqrt{5}$$

$$\tau_2 : \mathbb{Q}[X]/(X^2 - 5)\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{5}] : a + bx \mapsto a - b\sqrt{5}$$

On observe que $\sigma = \tau_2 \circ \tau_1^{-1}$, donc σ est un automorphisme.

Définitions 1.1.5. On définit la **norme** d'un élément α de $\mathbb{Q}[\sqrt{5}]$ par

$$N(\alpha) = \alpha\sigma(\alpha).$$

On définit aussi la **trace** d'un élément α de $\mathbb{Q}[\sqrt{5}]$ par

$$T(\alpha) = \alpha + \sigma(\alpha).$$

Insistons sur le fait que la norme et la trace que nous venons d'introduire ne sont définies que pour les nombres appartenant à $\mathbb{Q}[\sqrt{5}]$, et surtout qu'elles dépendent de l'appartenance de ces nombres à $\mathbb{Q}[\sqrt{5}]$.

Propriétés 1.1.6. $N(\alpha) \in \mathbb{Q}, \quad N(\alpha) = 0 \Leftrightarrow \alpha = 0, \quad N(1) = 1.$
La norme est multiplicative : $\forall \alpha, \beta \in \mathbb{Q}[\sqrt{5}], N(\alpha\beta) = N(\alpha)N(\beta)$.
$T(\alpha) \in \mathbb{Q}$.
Si $\alpha = a + b\sqrt{5}$, où $a, b, \in \mathbb{Q}$, on a $N(\alpha) = a^2 - 5b^2$ et $T(\alpha) = 2a$.

Remarque 1.1.7. $N(\alpha)$ et $T(\alpha)$ définissent α à conjugaison près : α et $\sigma(\alpha)$ sont les deux racines du polynôme $X^2 - T(\alpha)X + N(\alpha) \in \mathbb{Q}[X]$.

Remarques 1.1.8. Si $\alpha \in \mathbb{Z}[\varphi]$, alors $N(\alpha), T(\alpha) \in \mathbb{Z}$.
Plus précisément, si $\alpha = a + b\varphi$, où $a, b \in \mathbb{Z}$, on a
$N(\alpha) = (a + \frac{1}{2}b)^2 - \frac{5}{4}b^2 = a^2 + ab - b^2 \quad$ et $\quad T[\alpha) = 2a + b.$
Ceci joint à la remarque précédente montre que tous les éléments de $\mathbb{Z}[\varphi]$ sont des entiers algébriques.

Proposition 1.1.9. *Un élément de $\mathbb{Z}[\varphi]$ (resp. de $\mathbb{Z}[\sqrt{5}]$) est inversible dans $\mathbb{Z}[\varphi]$ (resp. dans $\mathbb{Z}[\sqrt{5}]$) si et seulement si $N(\alpha) = \pm 1$.*

Démonstration. Soit $\alpha \in \mathbb{Z}[\varphi]$.
Si α est inversible dans $\mathbb{Z}[\varphi]$, il existe un nombre $\beta \in \mathbb{Z}[\varphi]$ tel que $\alpha\beta = 1$. Prenons les normes. Dans l'anneau $\mathbb{Z}$ des entiers naturels nous obtenons
$N(\alpha)N(\beta) = 1, \quad$ donc $\quad N(\alpha) = \pm 1 \quad$ car $\quad \mathbb{Z}^\times = \{\pm 1\}.$
Réciproquement, si $N(\alpha) = \pm 1$, alors $\alpha \neq 0$, $\sigma(\alpha) \neq 0$ et
$\frac{1}{\alpha} = \frac{\sigma(\alpha)}{\alpha\sigma(\alpha)} = \pm\sigma(\alpha) \in \mathbb{Z}[\varphi].$
L'argument vaut aussi pour $\mathbb{Z}[\sqrt{5}]$ (car $\sigma(\mathbb{Z}[\sqrt{5}]) = \mathbb{Z}[\sqrt{5}]$). □

Grâce à la norme, nous pourrons montrer que $\mathbb{Z}[\varphi]$ est principal. Quelques préliminaires seront utiles.

Définition 1.1.10. Un **domaine euclidien** est un domaine E pour lequel on a une fonction

$$\nu : E \to \mathbb{N}$$

satisfaisant les conditions suivantes :
(i) $\forall x \in E$, $\nu(x) = 0 \Leftrightarrow x = 0$,
(ii) $\forall a, b \in E, b \neq 0$, on a : $a|b \Rightarrow \nu(a) \leqslant \nu(b)$,
(iii)$\forall a, b \in E, b \neq 0, \quad \exists \quad q, r \in E$ tels que $a = bq + r$ et $\nu(r) < \nu(b)$.
Une telle fonction ν est parfois appelée **norme euclidienne** pour E.

Exemples 1.1.11. L'anneau des entiers $\mathbb{Z}$ est euclidien pour la fonction valeur absolue.

L'anneau $K[X]$ des polynômes en une indéterminée X à coefficients dans un corps K est aussi euclidien pour la fonction définie par $\nu(P) = 2^{\deg P}$. (Par convention le degré du polynôme nul est $-\infty$ et $2^{-\infty} = 0$.)

Signalons toutefois qu'l existe plusieurs définitions de domaine euclidien, plus ou moins équivalentes. Mais toutes conduisent au résultat suivant, parfois utile pour reconnaître des domaines principaux.

Théorème 1.1.12. *Tout domaine euclidien E est principal.*

Démonstration. Soit $\mathfrak{A}$ un idéal de E. Si l'idéal $\mathfrak{A}$ est nul, il est principal, engendré par 0. Si l'idéal $\mathfrak{A}$ est non nul, soit ν une norme euclidienne pour E et prenons dans $\mathfrak{A}$ un élément $b \neq 0$ tel que, $\forall x \in \mathfrak{A}, x \neq 0$, on aie $\nu(b) \leqslant \nu(x)$ (notons qu'un tel élément b existe car toute partie de $\mathbb{N}_0$ possède un minimum). Comme $b \in \mathfrak{A}$, nous avons $bE \subset \mathfrak{A}$. Montrons que cette inclusion est en fait une égalité. Pour tout $y \in \mathfrak{A}$, nous pouvons écrire $y = bq + r$, où $q, r \in E$, où $\nu(r) < \nu(b)$. Mais alors nous avons $r = y - bq \in \mathfrak{A}$ et $r = 0$ par le choix de b. Il en résulte que $y = bq \in bE$, que $\mathfrak{A} \subset bE$. Donc $\mathfrak{A} = bE$ est un idéal principal. □

Avec 1.1.12 nous retrouvons le fait bien connu que l'anneau des entiers et tout anneau de polynômes en un indéterminée X à coefficients dans un corps sont des domaines principaux. Et nous obtenons une agréable propriété de l'anneau $\mathbb{Z}[\varphi]$.

Proposition 1.1.13. *L'anneau $\mathbb{Z}[\varphi]$ est euclidien et donc principal.*

Démonstration. Pour tout $\alpha \in \mathbb{Q}[\varphi]$, posons $\nu(\alpha) = |N(\alpha)|$. Nous savons que $0 \leqslant \nu(\alpha) \in \mathbb{Q}$ et que, si $\alpha \in \mathbb{Z}[\varphi]$, $\nu(\alpha) \in \mathbb{N}$.

Nous avons donc une fonction $\nu : \mathbb{Z}[\varphi] \to \mathbb{N}, \alpha \mapsto \nu(\alpha)$ et il suffit de montrer que cette fonction est une norme euclidienne pour le domaine $\mathbb{Z}[\varphi]$.

(i) Nous avons bien $\nu(\alpha) = 0 \Leftrightarrow \alpha = 0$.

(ii) Soit $\alpha, \beta \in \mathbb{Z}[\varphi], \beta \neq 0$. Si $\alpha | \beta$ dans $\mathbb{Z}[\varphi]$, nous avons un $\gamma \in \mathbb{Z}[\varphi]$ tel que $\beta = \alpha\gamma$. Comme la norme et la fonction ν sont multiplicatives, nous avons $\nu(\beta) = \nu(\alpha)\nu(\gamma)$ et, comme cette dernière égalité a lieu dans $\mathbb{N}_0$, nous avons aussi $\nu(\alpha) \leqslant \nu(\beta)$.

(iii) Montrons d'abord qu'on peut approcher tout élément $\gamma_1 \in \mathbb{Q}[\varphi]$ par un élément $\gamma \in \mathbb{Z}[\varphi]$ de façon que $\nu(\gamma_1 - \gamma) < 1$.

Soit donc $\gamma_1 = a_1 + b_1\varphi, \quad a_1, b_1 \in \mathbb{Q}$. Commençons par approcher les rationnels a_1 et b_1 par des entiers et écrivons $a_1 = a + c, \quad b_1 = b + d$, où $a, b \in \mathbb{Z}$ et où $|c|, |d| \leqslant \frac{1}{2}$ (notons que le choix des entiers a, b n'est pas toujours unique). Ceci fait, posons $\gamma = a + b\varphi$ et remarquons que ce γ est l'élément cherché de $\mathbb{Z}[\varphi]$. En effet, majorons $\nu(\gamma_1 - \gamma)$, on a :

$0 \leqslant \nu(\gamma_1 - \gamma) = \nu(c + d\varphi) = |(c + \frac{d}{2})^2 - 5\frac{d^2}{4}| \leqslant (\frac{3}{4})^2 + \frac{5}{4}.\frac{1}{4} = \frac{14}{16} < 1$

Ceci étant, soit $\alpha, \beta \in \mathbb{Z}[\varphi], \beta \neq 0$. Alors $\frac{\alpha}{\beta} = \gamma_1 \in \mathbb{Q}[\varphi]$. On approche γ_1 par un $\gamma \in \mathbb{Z}[\varphi]$ de façon que $\nu(\gamma_1 - \gamma) < 1$, on écrit $\rho = \beta(\gamma_1 - \gamma)$ et on obtient $\alpha = \beta\gamma + \rho$, où γ et $\rho = \alpha - \beta\gamma$ sont dans $\mathbb{Z}[\varphi]$, où $\nu(\rho) = \nu(\beta)\nu(\gamma_1 - \gamma) < \nu(\beta)$. □

L'exemple ci-dessous montrera que le sous-anneau $\mathbb{Z}[\sqrt{5}]$ de $\mathbb{Z}[\varphi]$ n'est ni principal ni factoriel, il n'a pas de bonnes propriétés de factorisation et c'est pourquoi on lui préfère $\mathbb{Z}[\varphi]$.

Cet exemple indiquera aussi quelques tactiques utiles pour reconnaître si un nombre est irréductible, premier ou non. Pour le comprendre, il convient de se rappeler les définitions d'éléments irréductibles et d'éléments premiers (0.5.4), la caractérisation des éléments premiers 0.5.8 ainsi que les propriétés des domaines principaux et factoriels exposées au chapitre précédent, en particulier celle-ci : *tout élément irréductible d'un domaine principal ou factoriel est premier*, 0.5.5.

1.1.14. Exemple type. (a) Le nombre 2 est irréductible dans $\mathbb{Z}[\sqrt{5}]$ mais n'est pas premier dans $\mathbb{Z}[\sqrt{5}]$. L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est ni factoriel ni principal.

(b) Le nombre 2 est premier dans $\mathbb{Z}[\varphi]$.

Démonstration. (a)(i) Soit une factorisation $2 = \alpha\beta$ dans $\mathbb{Z}[\sqrt{5}]$, $\alpha, \beta \in \mathbb{Z}[\sqrt{5}]$. Prenons les normes, il vient $N(2) = 4 = N(\alpha)N(\beta)$. Comme cette dernière égalité a lieu dans l'anneau $\mathbb{Z}$ on a

$$N(\alpha) = \begin{cases} \pm 1 \\ \pm 2 \\ \pm 4 \end{cases}$$

Si $N(\alpha) = \pm 1$, alors α est inversible dans $\mathbb{Z}[\sqrt{5}]$.
Si $N(\alpha) = \pm 4$, alors $N(\beta) = \pm 1$ et β est inversible dans $\mathbb{Z}[\sqrt{5}]$.
Par ailleurs, $N(\alpha) = \pm 2$ est impossible. Voyons ceci. Écrivons $\alpha = a + b\sqrt{5}$ où $a, b \in \mathbb{Z}$. Si $N(\alpha) = a^2 - 5b^2 = \pm 2$, nous obtenons $a^2 \cong \pm 2$ modulo 5, ce qui signifie que les images de 2 et de -2 dans le corps $\mathbb{Z}_5$ sont des carrés. Or ceci n'est pas, dans $\mathbb{Z}_5$, 2 et $-2 = 3$ ne sont pas des carrés (les carrés de $\mathbb{Z}_5$ sont les éléments $0, 1, 4$).

Nous venons de montrer que 2 est irréductible dans $\mathbb{Z}[\sqrt{5}]$.

(a)(ii) Regardons l'égalité $(1+\sqrt{5})(-1+\sqrt{5}) = 4 = 2.2$ faisant intervenir des nombres de $\mathbb{Z}[\sqrt{5}]$. Dans $\mathbb{Z}[\sqrt{5}]$, 2 divise le produit $(1 + \sqrt{5})(-1 + \sqrt{5})$ mais ne divise aucun des deux facteurs $(1 + \sqrt{5})$ et $(-1 + \sqrt{5})$ car $\frac{1 \pm \sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$. Le nombre 2 n'est donc pas premier dans $\mathbb{Z}[\sqrt{5}]$.

(a)(iii) Comme l'anneau $\mathbb{Z}[\sqrt{5}]$ possède un élément irréductible non premier, il n'est ni factoriel ni principal.

(b) Pour montrer que 2 est premier dans $\mathbb{Z}[\varphi]$ il nous suffit de montrer que l'anneau quotient $\mathbb{Z}[\varphi]/2\mathbb{Z}[\varphi]$ est intègre (voir 0.5.8).

Rappelons d'abord 1.1.2 :

$$\mathbb{Z}[\varphi] \simeq \mathbb{Z}[X]/(X^2 - X - 1).$$

Avec 0.6.4 nous avons :

$$\mathbb{Z}[\varphi]/2\mathbb{Z}[\varphi] \simeq \mathbb{Z}[X]/(2, X^2 - X - 1) \simeq \mathbb{Z}_2[X]/(X^2 - X - 1).$$

Et nous avons que $\mathbb{Z}_2[X]/(X^2 - X - 1)$ est un corps de 4 éléments, puisque le polynôme $(X^2 - X - 1)$, qui est de degré 2 et n'a pas de racine dans $\mathbb{Z}_2$, est irréductible dans $\mathbb{Z}_2[X]$.

(On aurait pu montrer par un calcul direct que 2 est irréductible dans $\mathbb{Z}[\varphi]$, donc aussi premier dans $\mathbb{Z}[\varphi]$ puisque $\mathbb{Z}[\varphi]$ est principal. Mais nous rencontrerons d'autres anneaux de nombres qui ne sont pas principaux, la tactique utilisée ci-haut sera donc utile pour voir si un de leurs éléments est premier ou non.)

Remarquons que les nombres intervenant dans l'égalité

$$(1 + \sqrt{5})(-1 + \sqrt{5}) = 4 = 2.2$$

appartiennent aussi à $\mathbb{Z}[\varphi]$, mais que cette fois 2 divise $(1 + \sqrt{5})$ dans $\mathbb{Z}[\varphi]$ car $\frac{1+\sqrt{5}}{2} = \varphi \in \mathbb{Z}[\varphi]$.

En fait, les nombres $2, (1 + \sqrt{5})$ et $(-1 + \sqrt{5})$ sont associés dans $\mathbb{Z}[\varphi]$. ($(1 + \sqrt{5}) = 2\varphi, (-1 + \sqrt{5}) = 2(\varphi - 1)$, φ et $\varphi - 1$ sont inversibles dans $\mathbb{Z}[\varphi]$.) □

– – – – – – – – – – – – – – – – –

1.1.15. Exercices*. Le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ et le pentagone régulier.

(a) Dans un cercle de rayon 1, calculer la longueur d de la corde sous-tendue par un angle au centre γ, en fonction de $\cos\gamma$.

(b) Posons $\theta = \frac{2\pi}{5}$ et $\alpha = e^{i\theta}$.

De $\alpha^5 = 1$, déduire $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. Utiliser cette relation pour calculer $\cos\theta$. Remarquer que $\cos\theta \in \mathbb{Q}[\varphi]$.

(c) Calculer la longueur ℓ du coté du pentagone régulier inscrit à un cercle de rayon 1. Remarquer que $\ell^2 \in \mathbb{Z}[\varphi]$.

(d) Indiquer une construction à la règle et au compas du pentagone régulier inscrit à un cercle donné.

(e) Calculer la longueur L d'une grande diagonale d'un pentagone régulier, ainsi que le rapport L/ℓ.

(Vérifier aussi que $L/\ell = \varphi$.)

(f) Calculer la longueur ℓ' du coté d'un décagone régulier inscrit à un cercle de rayon 1.

(g) Les nombres ℓ et ℓ' sont-ils dans $\mathbb{Z}[\varphi]$?

(Solutions partielles : $d^2 = 2 - 2\cos\gamma$, $\cos\theta = t$ satisfait la relation $4t^2 + 2t - 1 = 0$, $\cos\theta = \frac{-1+\sqrt{5}}{4} = \frac{\varphi-1}{2}$, $\ell^2 = 3 - \varphi$, $L^2 = 2 + \varphi$, $L^2/\ell^2 = \varphi + 1 = \varphi^2$, $\cos\frac{2\pi}{10} = \frac{\varphi}{2}$, $\ell'^2 = (2 - \varphi) = (\varphi - 1)^2$.)

1.1.16. Exercices. Soit à nouveau ℓ la longueur du coté du pentagone régulier inscrit à un cercle de rayon 1 et rappelons que $\ell^2 = 3 - \varphi$.

Quel est le polynôme minimal de ℓ sur $\mathbb{Q}$?

(Réponse : $X^4 - 5X^2 + 5$.)

1.1.17. Exercice. Le nombre d'or et la suite de Fibonacci.

Soit $u_o, u_1 \in \mathbb{R}$. Ces deux nombres sont les premiers termes d'une suite de nombres réels $u_0, u_1, u_2, \cdots, u_n, \cdots$ définie par la récurrence :

$$\forall n \geqslant 1, \quad u_{n+1} = u_n + u_{n-1}.$$

Nous avons donc :

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$$

Calculer les valeurs propres et les vecteurs propres de la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. En déduire une formule donnant u_n en fonction de u_0 et u_1.

1.1.18. Exercices.(a) Les nombres $\sqrt{5}, 3, 7, 11, 13$ sont-ils irréductibles dans $\mathbb{Z}[\sqrt{5}]$?

(Pour 11, regarder $(4 + \sqrt{5})(4 - \sqrt{5})$.)

1.1.19. Exercice. Montrer que $\mathbb{Z}[\varphi]/7\mathbb{Z}[\varphi]$ est un corps de 49 éléments. En déduire que 7 est premier dans $\mathbb{Z}[\varphi]$.

(Indication : observer que $\mathbb{Z}[\varphi]/7\mathbb{Z}[\varphi] \simeq \mathbb{Z}_7[X]/(X^2 - X - 1)$ et observer que le polynôme $X^2 - X - 1$ n'a pas de racines dans $\mathbb{Z}_7$ pour conclure).

1.2 Dépendance algébrique et intégrale

Dépendance algébrique.

Définitions et observations 1.2.1. Si K est un sous-corps du corps L, nous dirons que L est une **extension** du corps K.

Toute extension L du corps K a une structure d'espace vectoriel sur K, la dimension de L en tant que K-vectoriel est appelée **degré de L sur K** et notée **[L : K]**. Si ce degré est fini, nous dirons que L est une **extension finie** de K.

Soit L une extension du corps K. Un élément x de L est dit **algébrique sur K** si x est racine d'un polynôme non nul à coefficients dans K. Dans ce cas, l'ensemble des polynômes $T \in K[X]$ tels que $T(x) = 0$ est un idéal non nul de l'anneau $K[X]$. Comme K est un corps et que $K[X]$ est un domaine principal, cet idéal est engendré par un unique polynôme unitaire, appelé **polynôme minimal de x sur K** et noté $\mathbf{Min}_{K,x}$.

Une **extension algébrique** du corps K est une extension de K dont tous les éléments sont algébriques sur K.

Une **sous-K-extension** de l'extension L du corps K est un sous-corps de L contenant K.

Observation 1.2.2. Toute extension finie du corps K est algébrique sur K.

En effet, soit L une extension finie de K, $[L : K] = n \in \mathbb{N}_0$, et soit y un élément quelconque de L. Les $n+1$ éléments $1, y, y^2, \cdots, y^n$ sont linéairement dépendants sur K et toute relation non triviale de dépendance linéaire entre les $1, y, y^2, \cdots, y^n$ sur K est aussi une relation de dépendance algébrique de y sur K, y est donc algébrique sur K.

Si $P = \mathrm{Min}_{K,y}$ est le polynôme minimal de y sur K, on a donc $\deg(P) \leqslant [L : K]$.

Nous pourrons en dire davantage : avec 1.2.8 nous aurons aussi que $\deg(P) \mid [L : K]$.

Remarques 1.2.3. Soit L une extension du corps K et soit $0 \neq x \in L$ un élément algébrique sur K.

Soit encore $P := \mathrm{Min}_{K,x} = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ le polynôme minimal de x sur K, où les $a_i \in K$, où $n = \deg(P) \geqslant 1$.

(a) Le sous-anneau $K[x]$ de L engendré par x et K est un espace vectoriel sur K de dimension n, de base $1, x, x^2, \cdots, x^{n-1}$.

(b) Le polynôme $P = \mathrm{Min}_{K,x}$ est aussi le polynôme unitaire de $K[X]$ de degré minimum s'annulant en x.

(c) Le polynôme $P = \mathrm{Min}_{K,x}$ est un élément irréductible de $K[X]$, en particulier son terme indépendant a_0 est non nul.

(Si $P = P_1P_2$ est une factorisation de P dans $K[X]$, en évaluant en x nous obtenons dans L l'égalité $0 = P_1(x)P_2(x)$. Un des deux éléments $P_1(x)$, $P_2(x)$ du corps L est donc nul, disons $P_1(x) = 0$. Mais alors $\deg(P_1) \geqslant \deg(P)$. Comme $\deg(P) = \deg(P_1) + \deg(P_2)$, il vient $\deg(P_1) = \deg(P)$ et $\deg(P_2) = 0$, donc $0 \neq P_2 \in K$, P_2 est inversible dans K et dans $K[X]$.)

(d) $x^{-1} \in K[x]$

(Nous avons $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$. Réecrivons cette égalité : $x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = -a_0$. Comme $a_0 \neq 0$, nous avons $x^{-1} = (-a_0)^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in K[x]$.)

(e) x^{-1} est algébrique sur K et a pour polynôme minimal le polynôme $P' = X^n + a_0^{-1}a_1X^{n-1} + \cdots a_0^{-1}a_{n-1}X + a_0^{-1}$.

(Divisons l'égalité $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ par x^n. Il vient $1 + a_{n-1}(\frac{1}{x}) + \cdots + a_1(\frac{1}{x})^{n-1} + a_0(\frac{1}{x})^n = 0$. Ceci montre que $x^{-1} = \frac{1}{x}$ est aussi algébrique sur K, que $P'(x^{-1}) = 0$. Le degré du polynôme minimal de x^{-1} sur K est donc inférieur ou égal au degré du polynôme minimal de x sur K. En permutant le rôle de x et de x^{-1}, nous obtenons finalement que le degré du polynôme minimal de x^{-1} sur K est égal au degré du polynôme minimal de x sur K. On en déduit que P' est le polynôme minimal de x^{-1} sur K.)

(f) $K[x]$ est un corps et une extension algébrique finie de K, $[K[x] : K] = \deg(\mathrm{Min}_{K,x})$.

(Soit $0 \neq y$ un élément quelconque de $K[x]$. Comme $K[x]$ est un K-vectoriel de dimension n, on remarque d'abord comme en 1.2.2 que y est algébrique sur K. Avec ce qui précède on a ensuite $y^{-1} \in K[y] \subset K[x]$.)

1.2.4. Voici une façon plus conceptuelle de montrer que le polynôme minimal P sur K d'un élément non nul x algébrique sur K (appartenant à une extension L de K) est irréductible dans $K[X]$ et que $K[x]$ est un corps.

L'homomorphisme évaluation $e_x : K[X] \to L, T \mapsto T(x)$ a pour noyau l'idéal (P) et pour image le sous-anneau $K[x]$ de L, il induit donc un isomorphisme $\overline{e_x} : K[X]/(P) \xrightarrow{\sim} K[x]$. Comme L est un corps, le sous-anneau $K[x]$ de L est intègre. Il en résulte que le polynôme P est un élément irréductible de $K[X]$, voir 0.5.11, et que finalement $K[x] \simeq K[X]/(P)$ est un corps, voir à nouveau 0.5.11.

Notons encore que $K \subset K[X]/(P)$, que $K[X]/(P)$ est une extension de K. Notons aussi que $\overline{e_x}$ est un **K-isomorphisme**, ce qui signifie que $\overline{e_x}$ est un isomorphisme tel que, pour tout $a \in K$, $\overline{e_x}(a) = a$.

Terminons par quelques informations dont nous ferons peu d'usage.

Définition 1.2.5. On dit q'un corps K est **algébriquement clos** si tout polynôme non constant $F \in K[X]$ a au moins une racine dans K ou, de façon équivalente, si tout polynôme non constant $F \in K[X]$ est produit de polynômes de degré 1.

D'Alembert avait déjà donné une preuve presque complète du fait fondamental suivant, Gauss en a donné une preuve complète.

Théorème 1.2.6. Théorème fondamental de l'algèbre. *(Gauss d'Alembert) Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Signalons aussi sans preuve.

Théorème 1.2.7. *Tout corps peut se plonger dans un corps algébriquement clos.*

Plus précisément, pour tout corps K il existe une extension algébriquement close Ω_K de K qui est algébrique sur K. Une telle extension est unique à K-isomorphisme près et est appelée la **clôture algébrique** *de K.*

– –

1.2.8. Exercice*. Soit B un sous-anneau de l'anneau C et A un sous-anneau de B : $A \subset B \subset C$.

Supposons que B, en tant que A-module, soit engendré par ses éléments $(z_1, \cdots, z_m)$ et que C, en tant que B-module, soit engendré par ses éléments $(y_1, \cdots, y_n)$. Alors les éléments $y_i z_j$ de C engendrent C en tant que A-module.

Si de plus les éléments $(z_1, \cdots, z_m)$ de B forment une base de B en tant que A-module et si les éléments $(y_1, \cdots, y_n)$ de C forment une base de C en tant que B-module, alors les éléments $y_i z_j$ de C forment une base de C en tant que A-module.

En particulier, si L_1 est une extension finie du corps L_0 et L_2 une extension finie de L_1, alors L_2 est une extension finie de L_0 et

$$[L_2 : L_1] \cdot [L_1 : L_0] = [L_2 : L_0].$$

1.2.9. Exercice*. Soit L une extension du corps K.

Montrer que l'ensemble $\overline{K}$ des éléments de L algébriques sur K est un sous-corps de L contenant K.

Si de plus L est algébriquement clos, montrer que $\overline{K}$ est aussi algébriquement clos (donc que $\overline{K}$ est la clôture algébrique de K).

(Indication partielle : si x et y sont deux éléments de L algébriques sur K, $x \neq 0$, regarder les inclusions $K \subset K[x] \subset K[x][y] = K[x, y] \subset L$ et utiliser 1.2.2, 1.2.3 et 1.2.8 pour montrer que $x \pm y$, xy et x^{-1} sont algébriques sur K.)

1.2.10. Exercice. Tout corps algébriquement clos est infini.

(Indication. Si $K = \{a_1, a_2, \cdots, a_n\}$ est un corps fini, le polynôme $(X - a_1)(X - a_2) \cdots (X - a_n)$ de $K[X]$ a-t'il des racines dans K ?)

1.2.11. Exercice. Calculer le polynôme minimal sur $\mathbb{Q}$ de $1/(\sqrt{2}+\sqrt{3})$, en utilisant le polynôme minimal de $\sqrt{2}+\sqrt{3}$ obtenu en 0.9.8.

– –

Dépendance intégrale.

Nous venons d'introduire le vocabulaire de la dépendance algébrique. Introduisons maintenant celui, plus général, de la dépendance intégrale.

Définitions 1.2.12. Soit A un sous-anneau de l'anneau B.

Un élément $b \in B$ est dit **entier sur** A (ou intégralement dépendant sur A) si on a une relation $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$, où les éléments $a_{n-1}, \cdots, a_1, a_0 \in A$. Une telle relation est alors appelée une **relation d'intégrale dépendance** de b sur A.

Si tous les éléments de B sont entiers sur A, on dit que B est entier sur A.

La dépendance intégrale est donc une généralisation de la dépendance algébrique. (Notons que tout élément $a \in A$ est entier sur A, on a la relation $a - a = 0$.)

Nous voulons d'abord généraliser 1.2.2. Pour cela, nous utiliserons les déterminants, disponibles pour tout anneau commutatif et dont la définition et les propriétés ont été vues au cours d'algèbre linéaire. Rappelons seulement ceci.

Rappel 1.2.13. Soit $G = (g_{ij})$ une matrice carrée $n \times n$ à entrées g_{ij} dans un anneau A (rappelons que dans ces notes tous les anneaux sont supposés commutatifs). Soit G_{ij} le déterminant de la matrice $(n-1)\times(n-1)$ obtenue à partir de la matrice G par suppression de la $i^{\text{ième}}$ ligne et de la $j^{\text{ième}}$ colonne et rappelons le développement du déterminant de G selon la $i^{\text{ième}}$ colonne :

$$\det(G) = \sum_k (-1)^{i+k} G_{ki} g_{ki}, \quad 1 \leqslant i \leqslant n.$$

Nous avons aussi

$$0 = \sum_k (-1)^{i+k} G_{ki} g_{kj} \quad \text{si } i \neq j$$

car cette expression est le déterminant d'une matrice dont deux colonnes sont égales (la $i^{\text{ième}}$ et la $j^{\text{ième}}$).

Posons maintenant $\tilde{g}_{ik} = (-1)^{i+k} G_{ki}$, les $\tilde{g}_{ik}$ sont les entrées d'une matrice $\tilde{G}$, transposée de la matrice des cofacteurs de G avec leur signe.

Avec ces notations nos équations se réécrivent

$$\tilde{G}.G = \det(G).I_n,$$

où I_n désigne la matrice identique $n \times n$.

Rappelons que, si A est un sous-anneau de l'anneau B, une restriction de la multiplication munit B d'une structure de A-module.

Proposition 1.2.14. *Soit A un sous-anneau d'un anneau B. Si B muni de sa structure de A-module est un A-module de type fini, alors B est entier sur A.*

Plus précisément, soit $w_1, \cdots, w_n$ une partie génératrice du A-module B. Pour tout $x \in B$ nous avons un système d'équations

$$xw_i = \sum_{j=1}^{n} c_{ij} w_j, \quad 1 \leqslant i \leqslant n$$

où les $c_{ij} \in A$. Voyons ces c_{ij} comme les entrées d'une matrice $C \in A^{n\times n}$.

Alors le polynôme caractéristique $\det(XI_n - C)$ de la matrice C fournit une relation de dépendance intégrale de x sur A : $\det(xI_n - C) = 0$.

Démonstration. Réécrivons le système d'équations :

$$1 \leqslant i \leqslant n, \quad \sum_{j=1}^{n} (\delta_{ij} x - c_{ij}) w_j = 0,$$

où δ_{ij} est le symbole de Kronecker.

Réécrivons encore ce système sous forme matricielle :

$$(xI_n - C) \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad .$$

Posons $xI_n - C = G$ et multiplions notre dernière équation à gauche par la matrice $\tilde{G}$ introduite au paragraphe précédent. Comme $\tilde{G}.G = \det(G).I_n$, il vient :

$$\det(G) I_n \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{et} \quad \forall i, 1 \leqslant i \leqslant n,\ \det(G).w_i = 0.$$

Comme l'élément 1 de B s'écrit aussi $1 = \sum_{i=1}^{n} a_i w_i$, avec $a_i \in A$, on obtient encore $\det(G).1 = 0$ et finalement $\det(G) = 0$. On remarque que $\det(G)$ est le polynôme caractéristique de la matrice C évalué en x et que son développement fournit une relation de dépendance intégrale de x sur A. □

(Remarquer l'analogie entre la proposition précédente et le théorème de Cayley-Hamilton en algèbre linéaire. En fait, la proposition précédente et le théorème de Cayley-Hamilton sont deux cas particuliers d'un fait plus général concernant les endomorphismes des A-modules de type fini.)

Notre proposition est le principal ingrédient du critère très utile que voici.

Théorème 1.2.15. *Soit A un sous-anneau de l'anneau B et soit $b \in B$.*

Les conditions suivantes sont équivalentes.

(i) b est entier sur A,

(ii) $A[b]$ est un A-module de type fini,

(iii) Il existe un sous-anneau B' de B tel que $A[b] \subset B' \subset B$ et tel que B' soit un A-module de type fini.

Lorsque ces conditions sont satisfaites, $A[b]$ est entier sur A.

Démonstration. (i) $\Rightarrow$ (ii) est aisé, (ii) $\Rightarrow$ (iii) est trivial et (iii) $\Rightarrow$ (i) découle de 1.2.14.

La dernière assertion est une conséquence directe de ces équivalences. □

Rappelons le fait suivant, déjà observé en 1.2.8.

Lemme 1.2.16. *Soit B un sous-anneau d'un anneau C et soit encore A un sous-anneau de B, $A \subset B \subset C$.*

Si B est un A-module de type fini et si C est un B-module de type fini, alors C est un A-module de type fini.

Corollaires 1.2.17. *Soit A un sous-anneau de l'anneau B.*

(i) Si x et y sont des éléments de B entiers sur A, alors $x+y, x-y$ et xy sont aussi entiers sur A.

(ii) L'ensemble des éléments de B entiers sur A est un sous-anneau de B contenant A, appelé **fermeture intégrale** *de A dans B.*

Démonstration. Remarquer que $x \pm y, xy \in A[x,y]$, appliquer 1.2.16 à la suite $A \subset A[x] \subset A[x,y] = A[x][y]$ et conclure avec 1.2.15. □

Proposition 1.2.18. *(Transitivité de la dépendance intégrale) Soit A, B, C trois anneaux tels que $A \subset B \subset C$.*

Supposons que B est entier sur A et que C est entier sur B.

Alors C est entier sur A.

Démonstration. Une relation d'intégrale dépendance de l'élément $c \in C$ sur B fait intervenir un nombre fini d'éléments $b_0, \cdots, b_n$ de B. Cet élément c est donc aussi entier sur le sous-anneau $A_1 := A[b_1, \cdots, b_n]$ de B et $A_1[c]$ est un A_1-module de type fini, 1.2.15. Comme les b_i sont entiers sur A l'anneau $A_1 = A[b_1, \cdots, b_n]$ est un A-module de type fini (1.2.15 joint à un usage itéré de 1.2.16). Avec à nouveau 1.2.16 on obtient que l'anneau $A_1[c]$ est un A-module de type fini et on conclut avec 1.2.15 que c est entier sur A. □

Corollaire 1.2.19. *Soit B un anneau. Désignons par $\mathbb{S}ousAnn(B)$ l'ensemble des sous-anneaux de B, et, pour tout $A \in \mathbb{S}ousAnn(B)$, désignons par $\overline{A}$ la fermeture intégrale de A dans B. Nous obtenons une fonction*

$$\mathbb{S}ousAnn(B) \to \mathbb{S}ousAnn(B) : A \mapsto \overline{A}$$

qui a les propriétés suivantes :
(i) elle est expansive : $A \subset \overline{A}$,
(ii) croissante : $A_1 \subset A_2 \Rightarrow \overline{A_1} \subset \overline{A_2}$,
(iii) idempotente : $\overline{A} = \overline{\overline{A}}$.

La proposition suivante joue un grand rôle dans la dépendance intégrale.

Proposition 1.2.20. *Soit A un sous-anneau d'un domaine B tel que B soit entier sur A. Alors*
(i) tout élément a de A inversible dans B est inversible dans A ($a^{-1} \in B \Rightarrow a^{-1} \in A$),
(ii) A est un corps si et seulement si B est un corps.

Démonstration. (i) Soit $a \in A$ un élément inversible dans B : $a^{-1} = \frac{1}{a} \in B$.
Come B est entier sur A nous avons une relation d'intégrale dépendance

$$(\frac{1}{a})^n + c_{n-1}(\frac{1}{a})^{n-1} + \cdots + c_1(\frac{1}{a}) + c_0 = 0 \quad \text{où les } c_i \in A.$$

Multiplions cette relation par a^{n-1}, réarrangeons, il vient

$$\frac{1}{a} = -(c_{n-1} + c_{n-2}a + \cdots + c_1a^{n-2} + c_0a^{n-1} \in A).$$

(ii) Si B est un corps, on déduit de (i) que A est un corps.
Réciproquement, supposons que A soit un corps et soit $0 \neq b \in B$. Nous avons une relation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0 \quad \text{où les } a_i \in A.$$

Quitte à simplifier par une puissance convenable de b, ce qui est permis puisque que B est un domaine, nous pouvons supposer $a_0 \neq 0$. Dès lors

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)(-a_0^{-1}) = 1,$$

ce qui montre que b est inversible dans B. □

Rappelons que tout domaine se plonge dans son corps des fractions.

Définitions 1.2.21. La **clôture intégrale** d'un domaine A est la fermeture intégrale de A dans son corps de fractions.

Un **domaine intégralement clos** est un domaine égal à sa clôture intégrale.

Exemple 1.2.22. Avec la transitivité de la dépendance intégrale 1.2.18 nous obtenons.

La clôture intégrale A' d'un domaine A est un domaine intégralement clos.

Plus généralement, si A est un sous-anneau d'un corps K, la fermeture intégrale de A dans K est un domaine intégralement clos.

Plus généralement encore, si A est un sous-anneau d'un domaine intégralement clos B, la fermeture intégrale de A dans B est un domaine intégralement clos.

Le premier anneau que nous avons rencontré, l'anneau $\mathbb{Z}$ des entiers, est un domaine intégralement clos. Plus généralement nous avons.

Proposition 1.2.23. *Tout domaine factoriel est intégralement clos.*

Démonstration. Soit A un domaine factoriel de corps des fractions K et $c \in K$ un élément entier sur A. Nous devons montrer que $c \in A$. Nous pouvons écrire $c = \frac{a}{b}$, où $a, b \in A$, $b \neq 0$ et nous avons une relation

$$(\frac{a}{b})^n + d_{n-1}(\frac{a}{b})^{n-1} + \cdots + d_0 = 0 \quad \text{où les } d_i \in A.$$

Multiplions par b^n, il vient

$$a^n = -(bd_{n-1}a^{n-1} + \cdots + b^n d_0)$$

ce qui montre que b divise a^n. Mais A est un domaine factoriel et tout facteur premier p de b, divisant a^n, divise aussi a. Par simplifications successives de la fraction $\frac{a}{b}$ on obtient finalement $\frac{a}{b} = a' \in A$. □

Nous avons donc une première hiérarchie des domaines

$$\text{euclidien} \Rightarrow \text{principal} \Rightarrow \text{factoriel} \Rightarrow \text{intégralement clos.}$$

1.2.24. *Application à la théorie des nombres.*

Indiquons maintenant le rôle de la dépendance intégrale et des domaines intégralement clos en théorie des nombres.

La théorie des nombres s'intéresse entre autres aux **corps de nombres**, c.à-d. aux sous-corps de $\mathbb{C}$ de degré fini sur $\mathbb{Q}$ ou, ce qui revient au même, aux extensions finies de $\mathbb{Q}$ (nous verrons plus tard en 3.3.2 que toute extension finie de $\mathbb{Q}$ peut se plonger dans $\mathbb{C}$). Les éléments d'un corps de nombres K sont donc des nombres algébriques (sur $\mathbb{Q}$). Parmi ceux-ci, certains sont des entiers algébriques (entiers sur $\mathbb{Z}$).

Si K est un corps de nombres, l'ensemble des éléments de K entiers sur $\mathbb{Z}$ est un sous-anneau de K appelé l'**anneau des entiers de K**, souvent désigné par $\mathcal{O}_K$, $\mathcal{O}_K$ est donc la fermeture intégrale de $\mathbb{Z}$ dans K.

Voici quelques premières remarques à ce sujet, la première étant un cas particulier de 1.2.22.

Remarques 1.2.25. Soit K un corps de nombres et soit $\mathcal{O}_K$ l'anneau des entiers de K. Nous avons :

(a) $\mathcal{O}_K$ est un domaine intégralement clos,

(b) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ car $\mathbb{Z}$ est intégralement clos, $\mathcal{O}_K \subsetneq K$.

(c) K est le corps des fractions de $\mathcal{O}_K$. Plus précisément, pour tout $x \in K$, il existe $c \in \mathbb{Z}, c \neq 0$ tel que $cx \in \mathcal{O}_K$.

(Soit $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ une relation de dépendance algébrique de x sur $\mathbb{Q}$, $a_i \in \mathbb{Q}$. Les a_i sont des fractions que nous pouvons réduire au même dénominateur. Écrivons donc $a_i = \frac{b_i}{c}$ où $b_i, c \in \mathbb{Z}$ où $c \neq 0$. Multiplions notre relation par c^n, nous obtenons la relation $(cx)^n + b_{n-1}(cx)^{n-1} + b_{n-2}c(cx)^{n-2} + \cdots + b_1c^{n-2}(cx) + b_0c^{n-1} = 0$ qui montre que $cx \in \mathcal{O}_K$.)

(d) Si $\mathfrak{A}$ est un idéal non nul de $\mathcal{O}_K$, alors $\mathfrak{A} \cap \mathbb{Z}$ est un idéal non nul de $\mathbb{Z}$. (Si $\mathfrak{A}$ est non nul, soit $0 \neq x \in \mathfrak{A}$. Nous avons une relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, où les $a_i \in \mathbb{Z}$. Quitte à simplifier par x, on peut supposer $a_0 \neq 0$. Et alors $0 \neq a_0 = -(x^n + a_{n-1}x^{n-1} + \cdots + a_1x) \in \mathbb{Z} \cap \mathfrak{A}$.

1.2.26. Dernière remarque. De tout ce qui précède et en particulier de 1.2.23 il résulte que, si le corps de nombres K possède un sous-anneau A entier sur Z, factoriel et dont K est le corps des fractions, alors $A = \mathcal{O}_K$.

Par exemple, nous avons vu en section 1 que le sous-anneau $\mathbb{Z}[\varphi]$ de $\mathbb{Q}[\sqrt{5}]$ est principal et donc factoriel, que ses éléments sont des entiers algébriques. On conclut que $\mathbb{Z}[\varphi]$ est la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}[\sqrt{5}]$. Ceci explique entre autres pourquoi ce sous-anneau $\mathbb{Z}[\varphi]$ de $\mathbb{Q}[\sqrt{5}]$ est préférable à $\mathbb{Z}[\sqrt{5}]$, qui n'est ni intégralement clos, ni factoriel, ni principal.

Notons qu'en général $\mathcal{O}_K$ est rarement factoriel, cependant il est, en quelque sorte, le « *meilleur* » sous-anneau du corps de nombres K.

– –

1.2.27. Exercices*. Pour tout corps de nombres K, $\mathcal{O}_K^\times \cap \mathbb{Z} = \mathbb{Z}^\times$.

(Indication : en cas d'oubli de 1.2.20, commencer comme ceci :
$n \in \mathbb{N}_0$ inversible dans $\mathcal{O}_K \Rightarrow \frac{1}{n} \in \mathcal{O}_K \cap \mathbb{Q} \Rightarrow$ ...)

1.2.28. Exercices*. Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K et soit γ un élément premier de l'anneau $\mathcal{O}_K$.

Alors $O_K/\gamma\mathcal{O}_K$ est un corps.

(Indication. Observer que l'idéal $(\gamma\mathcal{O}_K \cap \mathbb{Z})$ de $\mathbb{Z}$ est non nul et qu'on a un homomorphisme injectif

$$\mathbb{Z}/(\gamma\mathcal{O}_K \cap \mathbb{Z}) \hookrightarrow \mathcal{O}_K/\gamma\mathcal{O}_K.$$

En déduire que $\mathbb{Z}/(\gamma\mathcal{O}_K \cap \mathbb{Z})$ est intègre et que $\gamma\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain nombre premier naturel p.

Observer encore que $\mathcal{O}_K/\gamma\mathcal{O}_K$ est entier sur le corps $\mathbb{Z}/p\mathbb{Z}$ et conclure avec 1.2.20.)

Observer l'analogie entre ce résultat et 0.5.10, notons cependant que l'anneau des entiers d'un corps de nombres n'est pas toujours principal.

Information : nous verrons plus tard que $O_K/\gamma\mathcal{O}_K$ est en fait un corps fini.

1.2.29. Exercices. Rappelons le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$.

(a) Montrer que $\mathbb{Z}[\varphi]$ est la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}[\sqrt{5}]$.

(Indication : se rappeler que les éléments de $\mathbb{Z}[\varphi]$ sont des entiers algébriques, se rappeler aussi que $\mathbb{Z}[\varphi]$ est principal et donc intégralement clos.)

(b) En déduire une nouvelle preuve du fait que $\mathbb{Z}[\sqrt{5}]$ n'est ni intégralement clos ni factoriel.

1.3 Corps quadratiques

Un **corps quadratique** est une extension de $\mathbb{Q}$ de degré 2 sur $\mathbb{Q}$.

Proposition 1.3.1. *Les corps quadratique sont les corps isomorphes à un sous corps de $\mathbb{C}$ de la forme $\mathbb{Q}[\sqrt{d}]$, où d est un entier rationnel sans facteur carré, $d \neq 0, 1$.*

(si $d < 0$, $\sqrt{d}$ désigne ici l'une quelconque des racines complexes du polynôme $X^2 - d = 0$, le plus souvent nous prendrons la racine $i\sqrt{-d}$.)

Démonstration. Soit d un entier rationnel sans facteur carré, $d \neq 0, 1$. Comme l'équation $X^2 - d = 0$ n'a pas de solution dans $\mathbb{Q}$, le polynôme $X^2 - d$ est un polynôme irréductible de $\mathbb{Q}[X]$ et l'anneau quotient $\mathbb{Q}[X]/(X^2 - d)$ est un corps, extension de $\mathbb{Q}$ de degré 2. De plus, l'homomorphisme d'évaluation

$$e_{\sqrt{d}} : \mathbb{Q}[X] \to \mathbb{C} : P \mapsto P(\sqrt{d})$$

a pour noyau l'idéal $(X^2 - d)$ et induit un isomorphisme

$$\overline{e_{\sqrt{d}}} : \mathbb{Q}[X]/(X^2 - d) \xrightarrow{\sim} \mathbb{Q}[\sqrt{d}],$$

$\mathbb{Q}[\sqrt{d}]$ est donc un corps quadratique.

Réciproquement, si K est un corps quadratique et si $x \in K \setminus \mathbb{Q}$, nous avons $\mathbb{Q} \subsetneq \mathbb{Q}[x] \subset K$ et donc $\mathbb{Q}[x] = K$ pour des raisons de degré. Le polynôme minimal de x sur $\mathbb{Q}$ est donc de degré 2, il s'écrit $X^2 + bX + c$ ($b, c \in \mathbb{Q}$) et a pour racines dans $\mathbb{C}$ les nombres $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$. L' évaluation des polynômes de $\mathbb{Q}[X]$ en une de ces racines fournit encore un isomorphisme $K = \mathbb{Q}[x] \simeq \mathbb{Q}[\frac{-b \pm \sqrt{b^2 - 4c}}{2}] = \mathbb{Q}[\sqrt{b^2 - 4c}]$. D'autre part, le nombre rationnel $b^2 - 4c$ peut s'écrire $b^2 - 4c = \frac{u^2 d}{v^2}$, où $u, v, d \in \mathbb{Z}$, $v \neq 0$, et où $d \neq 0, 1$ est un entier rationnel sans facteur carré. Avec ces notations on obtient $K \simeq \mathbb{Q}[\sqrt{b^2 - 4c}] = \mathbb{Q}[\sqrt{d}]$. □

Convention de section. Dans la suite de cette section, d sera toujours un un entier rationnel $\neq 0, 1$ et sans facteur carré.

Commençons par traiter $\mathbb{Q}[\sqrt{d}]$ comme nous avons traité $\mathbb{Q}[\sqrt{5}]$ en section 1.

Proposition 1.3.2. *Définissons une transformation σ de $\mathbb{Q}[\sqrt{d}]$ par*

$$\sigma : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}], a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

Cette transformation σ est un Q-automorphisme involutif de $\mathbb{Q}[\sqrt{d}]$, c.à-d. un automorphisme fixant les éléments de $\mathbb{Q}$ et tel que $\sigma^2 = 1$.

De plus, $\forall \alpha \in \mathbb{Q}[\sqrt{d}]$, nous avons : $\alpha = \sigma(\alpha) \Leftrightarrow \alpha \in \mathbb{Q}$.

*Cet automorphisme σ sera appelé l'***automorphisme de conjugaison de** $\mathbb{Q}[\sqrt{d}]$.

Démonstration. Un simple calcul suffit. On peut aussi utiliser les deux isomorphismes $\overline{e_{\sqrt{d}}}$ et $\overline{e_{-\sqrt{d}}}$ indiqués dans la preuve de 1.3.1. □

Définitions 1.3.3. On définit la **norme** d'un élément α de $\mathbb{Q}[\sqrt{d}]$ par

$$N(\alpha) = \alpha\sigma(\alpha).$$

On définit aussi la **trace** d'un élément α de $\mathbb{Q}[\sqrt{d}]$ par

$$T(\alpha) = \alpha + \sigma(\alpha).$$

Remarque 1.3.4. Si $d > 0$, alors $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$ et on dit que $\mathbb{Q}[\sqrt{d}]$ est un **corps quadratique réel**.

Si $d < 0$, $\mathbb{Q}[\sqrt{d}] \not\subset \mathbb{R}$ mais $\mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$, on dit alors que $\mathbb{Q}[\sqrt{d}]$ est un **corps quadratique imaginaire**. Dans ce cas, l'automorphisme de conjugaison de $\mathbb{Q}[\sqrt{d}]$ est la restriction à $\mathbb{Q}[\sqrt{d}]$ de l'automorphisme de conjugaison usuel du corps des complexes et la norme d'un nombre $\alpha \in \mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$ est le carré de son module tandis que la trace de α est deux fois sa partie réelle.

Propriétés 1.3.5. (i) Soit $\alpha = a + b\sqrt{d}$, où $a, b \in \mathbb{Q}$. On a

$$N(\alpha) = a^2 - db^2 \in \mathbb{Q} \quad \text{et} \quad T(\alpha) = 2a \in \mathbb{Q}, \quad N(\alpha) = 0 \Leftrightarrow \alpha = 0.$$

(ii) La norme est multiplicative : $\forall \alpha, \beta \in \mathbb{Q}[\sqrt{d}], N(\alpha\beta) = N(\alpha)N(\beta)$.

Autrement dit la fonction norme est un homomorphisme de monoïdes multiplicatifs et fournit un homomorphisme de groupes

$$N : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times, \alpha \mapsto N(\alpha)$$

(rappelons que, pour tout corps K, $K^\times$ désigne le groupe multiplicatif des éléments non nuls de K).

(iii) La fonction trace

$$T : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}, \alpha \mapsto T(\alpha)$$

est une application linéaire de $\mathbb{Q}$-vectoriels.

(iv) $N(\alpha)$ et $T(\alpha)$ définissent α à conjugaison près : α et $\sigma(\alpha)$ sont les deux racines du polynôme $X^2 - T(\alpha)X + N(\alpha) \in \mathbb{Q}[X]$. Ce dernier polynôme est donc le polynôme minimal $\mathrm{Min}_{\mathbb{Q},\alpha}$ de α sur $\mathbb{Q}$ dès que $\alpha \notin \mathbb{Q}$.

L'anneau des entiers $\mathcal{O}_d$ du corps $\mathbb{Q}[\sqrt{d}]$.

Proposition 1.3.6. *(i)* $\mathcal{O}_d \cap \mathbb{Q} = \mathbb{Z}$.

(ii) $\sigma(\mathcal{O}_d) = \mathcal{O}_d$.

(iii) $\forall \alpha \in \mathbb{Q}[\sqrt{d}]$ *on a :*

$$\alpha \in \mathcal{O}_d \Leftrightarrow N(\alpha) \text{ et } T(\alpha) \in \mathbb{Z} \quad \Leftrightarrow \quad Min_{\mathbb{Q},\alpha} \in \mathbb{Z}[X].$$

(iv) $\forall \alpha \in \mathcal{O}_d$, α *est inversible dans* $\mathcal{O}_d \Leftrightarrow N(\alpha) = \pm 1$.

Démonstration. (i) Ceci est dans 1.2.25.

(ii) L'image par σ d'une relation d'intégrale dépendance pour un élément $\alpha \in \mathcal{O}_d$ est une relation d'intégrale dépendance pour $\sigma(\alpha)$.

(iii) $\alpha \in \mathcal{O}_d \Rightarrow \alpha, \sigma(\alpha) \in \mathcal{O}_d \Rightarrow N(\alpha), T(\alpha) \in \mathcal{O}_d \cap \mathbb{Q} = \mathbb{Z} \Rightarrow \mathrm{Min}_{\mathbb{Q},\alpha} \in \mathbb{Z}[X] \Rightarrow \alpha \in \mathcal{O}_d$

(la première implication découle de (ii), la seconde de la définition de la norme, de la trace et de (i), la troisième de (1.3.5 (iv)) et la quatrième est évidente.

(iv) Soit $\alpha, \beta \in \mathcal{O}_d$ tels que $\alpha\beta = 1$. Alors $N(\alpha)N(\beta) = N(1) = 1$ et, comme cette dernière égalité a lieu dans l'anneau $\mathbb{Z}$ des entiers rationnels, on obtient $N(\alpha) \in \mathbb{Z}^\times = \{1, -1\}$.

Par ailleurs, $\forall \alpha \in \mathcal{O}_d$, on a :

$$N(\alpha) = \alpha\sigma(\alpha) = \pm 1 \qquad \Rightarrow \qquad \alpha^{-1} = \pm\sigma(\alpha) \in \mathcal{O}_d. \qquad \square$$

Théorème 1.3.7. *Soit* $\mathcal{O}_d$ *l'anneau des entiers du corps* $\mathbb{Q}[\sqrt{d}]$.

(i) Si $d \cong 2$ *ou* 3 *modulo* 4, *alors* $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$,

(ii) Si $d \cong 1$ *modulo* 4, *alors* $\mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *et les éléments de* $\mathcal{O}_d$ *sont de la forme* $\frac{a+b\sqrt{d}}{2}$, *où* $a, b \in \mathbb{Z}$, *où* a *et* b *sont tous deux pairs ou tous deux impairs.*

Dans tous les cas, $\mathcal{O}_d$ *est un* $\mathbb{Z}$*-module libre de rang 2, de base* $(1, \sqrt{d})$ *dans le premier cas et de base* $(1, \frac{1+\sqrt{d}}{2})$ *dans le second.*

Démonstration. Soit $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$. Nous savons avec 1.3.6 que les conditions pour que $\alpha \in \mathcal{O}_d$ sont

$$2a \in \mathbb{Z} \quad \text{et} \quad a^2 - db^2 \in \mathbb{Z}.$$

Si $a \in \mathbb{Z}$, alors $db^2 \in \mathbb{Z}$ et aussi $b \in \mathbb{Z}$ car d n'a pas de facteurs carrés qui pourraient se simplifier avec un éventuel facteur du dénominateur de la fraction rationnelle b^2.

Si $a \notin \mathbb{Z}$, posons $2a = u$ Alors $u \in \mathbb{Z}$ et u est impair. Posons encore $2b = v$. La seconde condition multipliée par 4 s'écrit : $u^2 - dv^2 \in 4\mathbb{Z}$. Comme plus haut ceci implique que $v \in \mathbb{Z}$, et aussi que v est impair car u est impair. Ceci implique aussi que $d \cong 1$ modulo 4 car pour les nombres impairs u et v nous avons $u^2 \cong 1 \cong v^2$ modulo 4. Pour terminer notons que, si u et v sont impairs et si $d \cong 1$ modulo 4, alors $u^2 - dv^2 \in 4\mathbb{Z}$.

Ce qui précède nous donne la description des éléments de $\mathcal{O}_d$ dans tous les cas. Les autres assertions en découlent aisément. $\square$

1.3.8. Question. *Quels sont les domaines principaux parmi les $\mathcal{O}_d$?*

Dirichlet fut sans doute le premier à voir clairement que l'anneau des entiers d'un corps quadratique n'est pas toujours factoriel.

La situation pour les corps quadratiques imaginaires est aujourd'hui connue.

Soit $d < 0$ un entier rationnel sans facteur carré.

L'anneau $\mathcal{O}_d$ est euclidien pour sa norme pour les valeurs $d = -1, -2, -3, -7, -11$ (voir l'exercice 1.3.19). Ainsi, pour ces valeurs de d, $\mathcal{O}_d$ est un domaine principal et factoriel.

Pour les valeurs $d = -5, -6, -10$, $\mathcal{O}_d$ n'est ni principal ni factoriel.

Pour les autres valeurs négatives de d, autrement pour $d \leqslant -13$, nous pourrons voir que l'anneau $\mathcal{O}_d$ n'est pas euclidien (exercice 2.4.20). Mais parmi ces valeurs, les domaines principaux restant correspondent aux valeurs $-19, -43, -67, -163$.

Ces valeurs de $d < 0$ ont été déterminées par Gauss, sans preuves. La dernière étape de la preuve de ceci fut seulement obtenue en 1967.

La situation pour les corps quadratiques réels n'est pas entièrement élucidée. On sait que $\mathcal{O}_d$ est euclidien pour la valeur absolue de sa norme pour les valeurs $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. En outre $\mathcal{O}_d$ est principal pour « beaucoup d'autres valeurs » de d, mais on ignore encore si ces valeurs de d sont en nombre infini et on ne connaît même pas une bonne façon d'aborder ce problème.

Le groupe des inversibles $\mathcal{O}_d^\times$ de l'anneau des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}]$.

1.3.9. Si $d < 0$, $\mathcal{O}_d$ est assez pauvre en inversibles, le groupe $\mathcal{O}_d^\times$ est un groupe cyclique fini, voir l'exercice 1.3.24.

Si $d > 0$, $\mathcal{O}_d$ est mieux fourni en inversibles. Par exemple, pour $d = 5$, l'anneau des entiers $\mathcal{O}_5$ de $\mathbb{Q}[\sqrt{5}]$ est l'anneau $\mathbb{Z}[\varphi]$ étudié en section 1 (où $\varphi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or) et nous avons vu que φ est inversible dans $\mathbb{Z}[\varphi]$. Les puissances de φ sont donc aussi inversibles dans $\mathbb{Z}[\varphi]$. Mais $1 < \varphi \in \mathbb{R}$, les puissances de φ sont donc distinctes deux à deux et le groupe $\mathcal{O}_5^\times$ est infini. Que pouvons-nous dire de plus, que pouvons-nous dire en général ?

Si $d > 0$, les nombres 1 et -1 sont évidemment des inversibles de $\mathcal{O}_d$, mais ce ne sont pas les seuls. Nous avons le résultat suivant, déjà énoncé par Fermat sous une autre forme, et dont nous postposons la démonstration à la dernière section de ce chapitre car elle fait appel à un autre cercle d'idées que celui développé jusqu'à présent.

Proposition 1.3.10. *Soit $d > 1$ un entier naturel sans facteur carré. L'anneau $\mathcal{O}_d$ des entiers du corps $\mathbb{Q}[\sqrt{d}]$ possède un inversible $\varepsilon \neq \pm 1$.*

Sachant ceci, nous allons pouvoir préciser la structure du groupe $\mathcal{O}_d^\times$.

Remarques 1.3.11. Soit $d > 1$ un entier naturel sans facteur carré et soit $\varepsilon \neq \pm 1$ un inversible de $\mathcal{O}_d$. Alors les quatre nombres $\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ sont aussi des inversibles de $\mathcal{O}_d$, ils sont réels, deux d'entre eux sont positifs et l'un d'entre eux, le plus grand des quatre, est strictement supérieur à 1. Écrivons $\varepsilon = a + b\sqrt{d}$, (où $a, b \in \mathbb{Z}$ si $d \not\equiv 1$ modulo 4, où $a, b \in \frac{1}{2}\mathbb{Z}$ si $d \cong 1$ modulo 4), ces quatre nombres sont les nombres $\pm a \pm b\sqrt{d}$, le plus grand d'entre eux est donc le nombre $|a| + |b|\sqrt{d}$. Remarquons encore que $a \neq 0 \neq b$ puisque $\varepsilon \neq \pm 1$.

Proposition 1.3.12. *Soit $d > 1$ un entier naturel sans facteur carré.*

*(i) L'ensemble des inversibles de $\mathcal{O}_d$ strictement supérieurs à 1 possède un minimum appelé l'***unité fondamentale** *de $\mathbb{Q}[\sqrt{d}]$.*

(ii) Si ε est l'unité fondamentale de $\mathbb{Q}[\sqrt{d}]$, les inversibles de $\mathcal{O}_d$ sont les nombres $\pm\varepsilon^z$, où $z \in \mathbb{Z}$.

(iii) Le groupe $\mathcal{O}_d^\times$ est isomorphe au groupe $(\mathbb{Z}_2, +) \times (\mathbb{Z}, +)$.

Démonstration. (i) Avec 1.3.10 et la première remarque en 1.3.11 on sait que $\mathcal{O}_d$ possède un inversible $\varepsilon > 1$. Si n est un entier naturel suffisamment grand, l'ensemble

$$E_n = \{\varepsilon \in \mathcal{O}_d^\times \mid 1 < \varepsilon < n\}$$

est donc non vide et il nous suffit de montrer qu'il est fini, car alors cet E_n aura un minimum qui sera l'unité fondamentale cherchée.

Soit donc $\varepsilon \in E_n$. Comme ε est inversible dans $\mathcal{O}_d$, nous avons

$$N(\varepsilon) = \varepsilon\sigma(\varepsilon) = \pm 1 \quad \text{et} \quad -1 < \sigma(\varepsilon) < 1.$$

Additionnant nos inégalités nous obtenons

$$0 < T(\varepsilon) = \varepsilon + \sigma(\varepsilon) < n + 1.$$

Comme $T(\varepsilon) \in \mathbb{Z}$ puisque ε est entier sur $\mathbb{Z}$, nous voyons que $T(\varepsilon)$ ne peut prendre qu'un nombre fini de valeurs quand ε parcourt E_n. Or chacun de nos $\varepsilon \in E_n$ est racine du polynôme $X^2 - T(\varepsilon)X + N(\varepsilon) = X^2 - T(\varepsilon)X \pm 1$. Comme ces polynômes sont en nombre fini notre ensemble E_n est aussi fini.

(ii) Soit maintenant ε l' unité fondamentale de $\mathbb{Q}[\sqrt{d}]$. Soit encore $\gamma > 1$ un inversible de $\mathcal{O}_d$ et soit n le plus grand entier naturel tel que $\varepsilon^n \leqslant \gamma$. Nous avons donc $\varepsilon^n \leqslant \gamma < \varepsilon^{n+1}$. En divisant par ε^n nous obtenons $1 \leqslant \varepsilon^{-n}\gamma < \varepsilon$. Comme $\varepsilon^{-n}\gamma$ est un inversible de $\mathcal{O}_d$ on en déduit que $\gamma = \varepsilon^n$ par la minimalité de ε. On termine la preuve avec la remarque précédant notre proposition.

(iii) Conséquence de (ii). □

1.3.13. Décrivons maintenant une méthode pour calculer l'unité fondamentale d'un corps quadratique réel.

Si $d \not\equiv 1$ modulo 4, $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ et l'unité fondamentale s'écrit $\varepsilon = a_1 + b_1\sqrt{d}$, où $a_1, b_1 \in \mathbb{N}_0$ (voir 1.3.11). Nous écrivons alors $\varepsilon^n = a_n + b_n\sqrt{d}$ et nous observons que les suites a_n et b_n sont strictement croissantes. Comme $N(\varepsilon) = a_1^2 - db_1^2 = \pm 1$, il nous suffit pour obtenir l'unité fondamentale de prendre le plus petit entier positif b tel que $db^2 \pm 1$ soit un carré.

Le cas où $d \cong 1$ modulo 4 se traite à peu près de la même façon. Dans ce cas $\mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et l'unité fondamentale s'écrit $\varepsilon = \frac{a_1+b_1\sqrt{d}}{2}$, où a_1 et b_1 sont des entiers, tous deux pairs ou tous deux impairs. Nous avons alors $a_1^2 - db_1^2 = \pm 4$. Un petit raisonnement montre qu'ici aussi il suffit, pour obtenir l'unité fondamentale, de prendre le plus petit entier positif b_1 tel que $db_1^2 \pm 4$ soit un carré .

Dans la pratique, l'unité fondamentale est parfois longue à repérer par la méthode indiquée ci-dessus, car l'unité fondamentale peut correspondre à une très grande valeur de b (ou de b_1). Mais il existe d'autres méthodes pour repérer cette unité fondamentale. L'une d'elles est fondée sur la théorie des fractions continues et était déjà connue des mathématiciens Indiens il y a au moins dix siècles. Ce qui est amusant avec cette dernière méthode, c'est que l'on sait depuis très longtemps que, s'il existe une unité fondamentale (autrement dit si la proposition 1.3.10 est vraie), alors la méthode la fournit, et même assez rapidement. Mais l'existence d'une unité fondamentale, ou, ce qui revient au même, l'existence d'une solution entière à l'équation $x^2 - dy^2 = \pm 1$, n'est pas évidente. Fermat en avait vraisemblablement une preuve et Lagrange (1736-1813) fut le premier à publier une telle preuve en 1768. Pour plus d'information sur le sujet nous renvoyons à [5].

Exemple 1.3.14. Dans le cas où $d = 5$ étudié en section 1, on a $5 \cdot 1 - 4 = 1$, on en déduit que l'unité fondamentale de $\mathbb{Q}[\sqrt{5}]$ est le nombre d'or.

Ce que deviennent les premiers naturels dans l'anneau $\mathcal{O}_d$.

1.3.15. Soit p un nombre premier naturel, autrement dit un élément premier de l'anneau $\mathbb{Z}$. On peut se demander si p est encore premier dans $\mathbb{Z}[\sqrt{d}]$, autrement dit si l'anneau quotient $\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$ est intègre. Comme $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$, on a avec 0.6.4

$$\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d, p) \simeq \mathbb{Z}_p[X]/(X^2 - d).$$

Comme $\mathbb{Z}_p$ est un corps, nous voyons donc que p est premier dans $\mathbb{Z}[\sqrt{d}]$ si et seulement si d n'est pas un carré modulo p.

Si $p \not\equiv 1$ modulo 4, $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_d$ est l'anneau des entiers du corps $\mathbb{Q}[\sqrt{d}]$.

Dans le cas où $d \cong 1$ modulo 4, on a $\mathbb{Z}[\sqrt{d}] \subsetneq \mathcal{O}_d$ et on peut aussi se demander si p reste premier dans $\mathcal{O}_d$. Traitons d'abord le cas où p est impair.

Comme les éléments de $\mathcal{O}_d$ sont alors les éléments de la forme $\frac{a+b\sqrt{d}}{2}$, où $a, b \in \mathbb{Z}$, où a et b sont tous deux pairs ou tous deux impairs, on observe d'abord que $p\mathcal{O}_d \cap \mathbb{Z}[\sqrt{d}] = p\mathbb{Z}[\sqrt{d}]$. On observe ensuite que tout élément de $\mathcal{O}_d$ est équivalent modulo p à un élément de $\mathbb{Z}[\sqrt{d}]$ ($\forall a, b \in \mathbb{Z}, \frac{(2a+1)+(2b+1)\sqrt{d}}{2} - p\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}]$). On en déduit que l'inclusion $\mathbb{Z}[\sqrt{d}] \hookrightarrow \mathcal{O}_d$ induit, après passage aux quotients, un isomorphisme $\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \xrightarrow{\sim} \mathcal{O}_d/p\mathcal{O}_d$. À nouveau, le nombre premier impair p est premier dans $\mathcal{O}_d$ si et seulement si d n'est pas un carré modulo p.

Le cas $p = 2$ se traite séparément, est proposé en exercice (1.3.23).

Rassemblons nos observations et la conclusion de 1.3.23.

Proposition 1.3.16. *(i) Soit p un premier naturel impair. On a :*

$$\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \simeq \mathcal{O}_d/p\mathcal{O}_d$$

p est premier dans $\mathcal{O}_d \Leftrightarrow p$ est premier dans $\mathbb{Z}[\sqrt{d}] \Leftrightarrow d$ n'est pas un carré modulo p.

(ii) 2 est premier dans $\mathcal{O}_d \Leftrightarrow d \cong 5$ modulo 8.

– –

1.3.17. Exercice*. Démontrer que l' anneau $\mathbb{Z}[i]$ est euclidien et donc principal. (Ce résultat est du à Gauss et depuis l'anneau $\mathbb{Z}[i]$ est connu sous le nom de *l'anneau des entiers de Gauss*.)

(Indication : visualiser $\mathbb{Z}[i]$ dans le plan complexe et procéder comme en 1.1.13.)

1.3.18. Exercice*. (i) Observer que le domaine $\mathbb{Z}[i\sqrt{5}]$ est intégralement clos.

(ii) Montrer que 2 et 3 sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$.

(iii) Regarder le produit $(1 + i\sqrt{5}).(1 - i\sqrt{5}) = 6$. En déduire que 2 et 3 ne sont pas premiers dans $\mathbb{Z}[i\sqrt{5}]$, que le domaine intégralement clos $\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal.

(iv) Identifier les anneaux quotients $\mathbb{Z}[i\sqrt{5}]/2\mathbb{Z}[i\sqrt{5}]$ et $\mathbb{Z}[i\sqrt{5}]/3\mathbb{Z}[i\sqrt{5}]$, observer qu'ils ne sont pas intègres.

(v) Montrer que 11 est premier dans $\mathbb{Z}[i\sqrt{5}]$.

(Indication : utiliser la tactique de 1.1.14.)

(vi) Déterminer l'unité fondamentale de $\mathbb{Z}[i\sqrt{5}]$.

1.3.19. Exercice*. Soit $d < 0$ un entier rationnel sans facteurs carrés.

(i) Montrer que, pour les valeurs de $d = -1, -2, -3, -7, -11$, l'anneau $\mathcal{O}_d$ est euclidien pour sa norme et donc principal.

(Indication. Rappelons qu'il suffit de montrer qu'on peut approcher tout nombre $\gamma_1 \in \mathbb{Q}[\sqrt{d}]$ par un nombre $\gamma \in \mathcal{O}_d$ de façon que $N(\gamma_1 - \gamma) < 1$.

Ceci est assez simple à voir pour les valeurs de $d = -1, -2, -3$.

Pour les valeurs de $d = -7, -11$, observons que les nombres de $\mathcal{O}_{(-11)}$ (ou ceux de $\mathcal{O}_{(-7)}$) se disposent dans le plan complexe comme les sommets de triangles tous égaux ($-11 \cong -7 \cong 1$ modulo 4). Calculez le rayon r du cercle circonscrit au triangle du plan complexe de sommets $(0, 1, \frac{1+i\sqrt{11}}{2})$, observez que $r < 1$ et que ceci suffit pour conclure. Idem avec 7 en place de 11.)

(ii) Montrer que, pour les valeurs de $d = -5, -6, -10$, l'anneau $\mathcal{O}_d$ n'est pas principal, à fortiori n'est pas euclidien.

1.3.20. Exercice. Démontrer que les anneaux $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ et l'anneau $\mathcal{O}_{13}$ des entiers du corps $\mathbb{Q}[\sqrt{13}]$ sont euclidiens et donc principaux.

1.3.21. Exercice. Observer que $8 + 3\sqrt{7}$ est inversible dans $\mathbb{Z}[\sqrt{7}]$.

Observer aussi que $8 + 3\sqrt{7}$ est l'unité fondamentale de $\mathbb{Q}[\sqrt{7}]$.

1.3.22. Exercice. Quelle est l'unité fondamentale de $\mathbb{Q}[\sqrt{3}]$, de $\mathbb{Q}[\sqrt{6}]$, de $\mathbb{Q}[\sqrt{11}]$, de $\mathbb{Q}[\sqrt{13}]$?

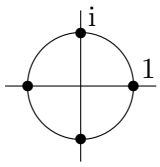
1.3.23. Exercice*. Soit d un entier rationnel sans facteur carré, $d \neq 0, 1$.

Écrire le polynôme minimal de $\frac{1+\sqrt{d}}{2}$ sur $\mathbb{Q}$ et observer que ce polynôme appartient à $\mathbb{Z}[X]$ si et seulement si $d \cong 1$ modulo4.

Soit encore $\mathcal{O}_d$ l'anneau des entiers du corps $\mathbb{Q}[\sqrt{d}]$.

Montrer que 2 est premier dans $\mathcal{O}_d$ si et seulement si $d \cong 5$ modulo 8.

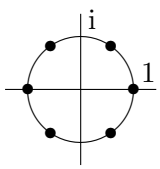
1.3.24. Exercice*. (i) Déterminer le groupe des inversibles de $\mathbb{Z}[i]$ et observer que c'est un groupe cyclique d'ordre 4.



(ii) Pour $d = -3$, l'anneau des entiers de $\mathbb{Q}[i\sqrt{3}]$ est l'anneau $\mathbb{Z}[\zeta]$, où $\zeta = \frac{-1+i\sqrt{3}}{2}$.

Déterminer les inversibles de $\mathbb{Z}[\zeta]$ et représenter-les dans le plan complexe.

Observer que le groupe des inversibles de $\mathbb{Z}[\zeta]$ est un groupe cyclique d'ordre 6.



(iii) Soit encore d un entier rationnel sans facteur carré, $d \neq 0, 1$. Montrer que, pour $d < -1, d \neq -3$, les seuls inversibles de l'anneau $\mathcal{O}_d$ des entiers de $\mathbb{Q}[\sqrt{d}]$ sont ± 1, que le groupe des inversibles de $\mathcal{O}_d$ est cyclique d'ordre deux.

1.3.25. Exercice*. Soit $\zeta = \frac{-1+i\sqrt{3}}{2}$.

(a) Représenter les éléments de $\mathbb{Z}[\zeta]$ dans le plan de Gauss.

(b) Le polynôme minimal de ζ sur $\mathbb{Q}$ est $X^2 + X + 1$,

$$\mathbb{Z}[\zeta] \simeq \mathbb{Z}[X]/(X^2 + X + 1)\mathbb{Z}[X].$$

(c) Se rappeler que $\mathbb{Z}[\zeta]$ est un domaine euclidien et donc principal.

(d) Observer : $X^2 + X + 1 = (X - \zeta)(X - \zeta^2)$.

En déduire : $3 = (1 - \zeta)(1 - \zeta^2)$.

Observer aussi : $\sigma(\zeta) = \zeta^2 = -1 - \zeta$.

(e) Montrer que $1 - \zeta$ et $1 - \zeta^2$ sont irréductibles et associés dans $\mathbb{Z}[\zeta]$.

En déduire que $3 = \varepsilon(1 - \zeta)^2$, où ε est un inversible de $\mathbb{Z}[\zeta]$.

(f) Observer : $X^3 + 1 = (X + 1)(X + \zeta)(X + \zeta^2)$.

En déduire que, si X et Y sont deux indéterminées, alors

$$X^3 + Y^3 = (X + Y)(X + \zeta Y)(X + \zeta^2 Y).$$

1.3.26. Exercice. Soit encore $\zeta = \frac{-1+i\sqrt{3}}{2}$.
Identifier les quotients $\mathbb{Z}[\zeta]/2\mathbb{Z}[\zeta]$ et $\mathbb{Z}[\zeta]/5\mathbb{Z}[\zeta]$.
Montrer que 2 et 5 sont premiers dans $\mathbb{Z}[\zeta]$.

1.4 Le symbole de Legendre

Les problèmes abordés à la fin de la section précédente montrent l'intérêt de savoir si un entier rationnel d est un carré modulo un premier naturel p. Commençons donc par regarder les carrés dans le groupe multiplicatif $\mathbb{Z}_p^\times$ des éléments non nuls du corps $\mathbb{Z}_p$. Si $p = 2$, tous les éléments de $\mathbb{Z}_2$ sont des carrés et il n'y a rien à dire. C'est pourquoi on s'intéresse ici aux **premiers naturels impairs**.

Proposition 1.4.1. *Soit p un premier naturel impair.*

(i) Le groupe $\mathbb{Z}_p^\times$ est un groupe d'ordre $p-1$, $\forall x \in \mathbb{Z}_p^\times$ on a $x^{p-1} = 1$.

(ii) $C_p = \{x^2 \mid x \in \mathbb{Z}_p^\times\}$ est un sous groupe de $\mathbb{Z}_p^\times$ d'ordre $\frac{p-1}{2}$.

(iii) $\forall a \in \mathbb{Z}_p^\times, \quad a^{\frac{p-1}{2}} = \pm 1$.

(iv) $\forall a \in \mathbb{Z}_p^\times, \quad a^{\frac{p-1}{2}} = 1 \Leftrightarrow a \in C_p$.

Démonstration. (i) Évident, l'ordre d'un élément divise l'ordre du groupe.

(ii) La fonction $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times, x \mapsto x^2$ est un homomorphisme de groupes ($\mathbb{Z}_p^\times$ est commutatif) dont l'image est C_p. Les éléments 1 et $-1 = p-1$ sont dans $\ker(f)$ et $1 \neq -1$ car p est impair.

Par ailleurs, l'équation $\quad x^2 - 1 = 0 \quad$ a au plus deux solutions dans le corps $\mathbb{Z}_p$.

Nous avons donc $\ker(f) = \{1, -1\}$ et $C_p \simeq \mathbb{Z}_p^\times / \ker(f)$ est un groupe d'ordre $\frac{p-1}{2}$.

(iii) $\forall a \in \mathbb{Z}_p^\times$ on a $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1$, d'où $a^{\frac{p-1}{2}} \in \ker(f) = \{1, -1\}$.

(iv) Regardons l'homomorphisme $g : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times, x \mapsto x^{\frac{p-1}{2}}$.

D'une part nous avons $C_p \subset \ker(g)$ (car $g(x^2) = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$), donc $\ker(g)$ contient au moins $\frac{p-1}{2}$ éléments.

D'autre part, $\ker(g)$ contient au plus $\frac{p-1}{2}$ éléments car l'équation $x^{\frac{p-1}{2}} - 1 = 0 \quad$ a au plus $\frac{p-1}{2}$ solutions dans le corps $\mathbb{Z}_p$.

On en déduit que $\ker(g)$ contient exactement $\frac{p-1}{2}$ éléments, que $\ker(g) = C_p$. □

Introduisons maintenant le symbole de Legendre.

Définition 1.4.2. Soit p un premier naturel impair. Pour tout $a \in \mathbb{Z}$ on définit le **symbole de Legendre** par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si} \quad a \notin p\mathbb{Z} \quad \text{et si} \quad a \text{ est un carré modulo } p \\ -1 & \text{si} \quad a \notin p\mathbb{Z} \quad \text{et si} \quad a \text{ n'est pas un carré modulo } p \\ 0 & \text{si} \quad a \in p\mathbb{Z} \end{cases}$$

Remarque 1.4.3. D'après la définition, $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p : $\forall z \in \mathbb{Z}$, on a $\left(\frac{a+zp}{p}\right) = \left(\frac{a}{p}\right)$

Avec 1.4.1 nous obtenons.

Proposition 1.4.4. *Soit p un premier naturel impair. $\forall a \in \mathbb{Z}$ on a*

$$\left(\frac{a}{p}\right) \cong a^{\frac{p-1}{2}} \text{ modulo } p.$$

Corollaires 1.4.5. *Soit p un premier naturel impair.*

(i) $\forall a, b \in \mathbb{Z}$ *on a* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(iii) (-1 *est un carré modulo* p) $\Leftrightarrow$ ($p \cong 1$ *modulo* 4).

(iv) (-1 *n'est pas un carré modulo* p) $\Leftrightarrow$ ($p \cong 3$ *modulo* 4).

Bien que nous ne soyons pas encore en mesure de calculer aisément $\left(\frac{a}{p}\right)$ pour a quelconque, nous avons déjà quelques premières retombées. Combinant 1.4.5 (iv) avec 1.3.16 et rappelant que $2 = (1+i)(1-i)$ n'est pas premier dans $\mathbb{Z}[i]$ nous obtenons.

Corollaire 1.4.6. *Soit p un premier naturel. Ce nombre p est premier dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$ si et seulement si $p \cong 3$ modulo 4.*

Retournons maintenant vers les entiers naturels et voyons quels sont ceux qui sont somme de deux carrés. Comme $a^2+b^2 = (a+bi)(a-bi)$, nous pourrons tirer avantage de notre connaissance de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, nous savons que $\mathbb{Z}[i]$ est principal (1.3.17).

Théorème 1.4.7. *(Fermat, 1601-1665) Soit p un premier naturel impair.*
Ce nombre p est somme de deux carrés dans $\mathbb{N}$ si et seulement si

$$p \cong 1 \text{ modulo } 4.$$

Si cette condition est satisfaite, p s'écrit de façon unique comme somme de deux carrés.

Démonstration. Si $p = a^2 + b^2$, où $a, b \in \mathbb{N}$, un et un seul des deux nombres a, b est pair, disons $a = 2a', b = 2b'+1$, où $a', b' \in \mathbb{N}$. On a alors $p = 4a'^2 + 4b'^2 + 4b' + 1 \cong 1$ modulo 4.

Réciproquement, supposons $p \cong 1$ modulo 4. Alors p n'est pas premier dans le domaine principal $\mathbb{Z}[i]$ (1.4.6) et peut y écrire $p = \alpha\beta$, où α et β sont des éléments non inversibles de $\mathbb{Z}[i]$. Prenons les normes. Nous obtenons dans $\mathbb{N}$ l'égalité

$$N(p) = p^2 = N(\alpha)N(\beta)$$

où $N(\alpha) \neq 1 \neq N(\beta)$ car α et β ne sont pas inversibles.

On a donc $N(\alpha) = N(\beta) = p$. Comme α est de la forme $\alpha = a + bi$ $(a, b \in \mathbb{Z})$ nous obtenons $N(\alpha) = p = a^2 + b^2$ (par simplification nous obtenons aussi $\beta = \sigma(\alpha) = a - bi$).

L'unicité de l'écriture de p comme somme de deux carrés résulte alors de l'unicité, à facteurs inversibles près, de la factorisation d'un nombre de $\mathbb{Z}[i]$ en produits de premiers dans le domaine principal $\mathbb{Z}[i]$. □

Remarque 1.4.8. La preuve de 1.4.7 fournie ici n'est sans doute pas celle imaginée par Fermat, qui aimait travailler avec sa méthode de descente infinie. Une fois qu'on a le résultat, on peut se demander comment trouver la solution entière de l'équation $p = x^2 + y^2$ lorsque $p \cong 1$ modulo 4. Il existe plusieurs méthodes, Legendre (1808) en a fourni une basée sur la théorie des fractions continues.

Voici maintenant un critère pour qu' un entier naturel quelconque soit somme de deux carrés.

Remarquons d'abord avec Fibonacci que l'ensemble des sommes de deux carrés naturels est stable pour la multiplication :

$(a^2 + b^2)(a'^2 + b'^2) = N(a + bi)N(a' + b'i) = N((a + bi)(a' + b'i))$

$= (aa' - bb')^2 + (ab' + a'b)^2$.

Remarquons encore que $2 = 1 + 1$ est aussi somme de deux carrés.

Théorème 1.4.9. Sommes de deux carrés. *Soit n un entier naturel, $n > 1$, et soit $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ sa décomposition en facteurs premiers, où les p_i sont des premiers distincts deux à deux, où $r_i \in \mathbb{N}$.*

Ce nombre n est somme de deux carrés si et seulement si , $\forall i \quad 1 \leqslant i \leqslant s$,

$$(p_i \cong 3 \text{ modulo } 4) \Rightarrow (r_i \in 2\mathbb{N}).$$

Démonstration. Si la condition sur les facteurs premiers de n est satisfaite, alors n est produit de nombres qui sont sommes de deux carrés et n est lui-même somme de deux carrés.

Réciproquement, soit $n = a^2 + b^2$, où $a, b \in \mathbb{N}$. Si $c = \text{pgcd}(a, b)$, on a que $c|n^2$ et nous pouvons diviser par c^2. Posons $n' = \frac{n}{c^2}, a' = \frac{a}{c}, b' = \frac{b}{c}$, il vient $\text{pgcd}(a', b') = 1$ et $n' = a'^2 + b'^2$. Remarquons aussi que n' s'écrit $n' = p_1^{r'_1} p_2^{r'_2} \cdots p_s^{r'_s}$, où les nouveaux exposants r'_i sont tels que $r_i - r'_i \in 2\mathbb{N}$. Pour prouver notre proposition, il nous suffit donc de prouver que les facteurs premiers impairs de n' sont tous $\cong 1$ modulo 4.

Soit donc q un facteur premier impair de n', alors $a'^2 + b'^2 \cong 0$ modulo q. De plus, comme $\text{pgcd}(a', b') = 1$, q ne divise ni a' ni b'. Désignons maintenant par $\overline{(.)}$ les images modulo q. Dans le corps $\mathbb{Z}/q\mathbb{Z}$ nous avons $\overline{a'} \neq \overline{0} \neq \overline{b'}$ et $-1 = \frac{\overline{a'}^2}{\overline{b'}^2}$ est un carré, d'où $q \cong 1$ modulo 4 au vu (1.4.5 (iii). □

En travaillant avec des quaternions plutôt qu'avec des entiers de Gauss, Lagrange (1736-1813) a démontré un siècle plus tard un autre théorème également annoncé par Fermat (théorème que nous ne démontrerons pas).

Théorème 1.4.10. *(Lagrange, 1770) Tout nombre naturel est somme de quatre carrés.*

La condition « $p \cong 1$ modulo 4 » a été souvent rencontrée, le résultat suivant, autre retombée de nos considérations sur le symbole de Legendre, n'est donc pas sans intérêt.

Proposition 1.4.11. *Il existe une infinité de premiers naturels p tels que $p \cong 1$ modulo 4.*

Démonstration. Procédons par l'absurde et supposons qu'il n'y aie qu'un nombre fini de premiers naturels $p \cong 1$ modulo 4. Soit alors $p_1, p_2, \cdots, p_k$ ces nombres, regardons le nombre naturel $n = 4(p_1 \cdot p_2 \cdots p_k)^2 + 1$ et l'un de ses facteurs premiers q.

D'une part, ce nombre n est impair et n'est divisible par aucun des p_i, donc $q \cong 3$ modulo 4.

D'autre part nous avons $0 \cong 4(p_1 \cdot p_2 \cdots p_k)^2 + 1$ modulo q, ce qui signifie que -1 est un carré modulo q et implique $q \cong 1$ modulo 4 (1.4.5(iii)).

Cette contradiction termine la preuve. □

Signalons cependant que la proposition précédente n'est qu'un cas très particulier d'un résultat général (et plus dur à prouver) du à Dirichlet (1805-1853).

Théorème 1.4.12. *(Dirichlet) Soit a et m des entiers naturels premiers entre eux.*

Il existe une infinité de nombres premiers $p \cong a$ modulo m.

Si p et q sont des nombres premiers naturels impairs distincts, les symboles de Legendre $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ sont reliés par la loi de réciprocité quadratique. Cette loi avait déjà été énoncée par Legendre, mais Gauss fut le premier à en fournir une preuve complète. Préparons nous à l'établir.

Lemme 1.4.13. *Soit p un nombre premier naturel impair et soit a un nombre entier rationnel non divisible par p.*

L'image d'un nombre $z \in \mathbb{Z}$ dans le corps $\mathbb{Z}_p$ sera désignée par $\overline{z}$. Posons

$$p_1 = \frac{p-1}{2}, \quad H = \{1, 2, \cdots, p_1\} \subset \mathbb{Z} \quad \textit{et} \quad \overline{H} = \{\overline{1}, \overline{2}, \cdots, \overline{p}_1\} \subset \mathbb{Z}_p.$$

Comme les éléments de $\overline{H}$ forment « la première moitié » des éléments non nuls de $\mathbb{Z}_p$ nous pouvons écrire dans le corps $\mathbb{Z}_p$

$$\forall i, 1 \leqslant i \leqslant p_1, \qquad \overline{i}.\overline{a} = \varepsilon_i.\overline{h}_i \qquad \textit{où} \qquad \varepsilon_i = \pm 1 \qquad \textit{et} \qquad h_i \in H.$$

(i) Avec ces notations on a :

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{p_1} \varepsilon_i$$

(ii) Si x est un nombre rationnel, nous désignons par $\lfloor x \rfloor$ sa partie entière : $\lfloor x \rfloor = max\{z \in \mathbb{Z} \mid z \leqslant x\}$. Avec ces notations on a aussi :

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \lfloor \frac{2ia}{p} \rfloor}$$

Démonstration. (i) Montrons d'abord que les $\overline{h}_i$ figurant dans les égalités $(\overline{i}.\overline{a} = \varepsilon_i.\overline{h}_i \quad 1 \leqslant i \leqslant p_1)$ sont distincts deux à deux.

Si $\overline{h}_i = \overline{h}_j$, alors $\overline{i}^2\overline{a}^2 = \overline{j}^2\overline{a}^2$ et $\overline{i} = \pm\overline{j}$ car $\overline{a} \neq \overline{0}$. Mais $\overline{i}, \overline{j} \in \overline{H}$ et $\overline{H}$ désigne la « première moitié » des éléments non nuls de $\mathbb{Z}_p$. On en déduit $\overline{i} = \overline{j}$ et $i = j$.

Ainsi, quand i parcourt H, $\overline{h}_i$ parcourt $\overline{H}$.

Ceci étant, nous faisons le produit de nos p_1 égalités $\overline{i}.\overline{a} = \varepsilon_i.\overline{h}_i$ et nous obtenons

$$\overline{a}^{p_1} \prod_{i=1}^{p_1} \overline{i} = \prod_{i=1}^{p_1} \overline{i}\overline{a} = \prod_{i=1}^{p_1} \varepsilon_i \prod_{i=1}^{p_1} \overline{h}_i = \prod_{i=1}^{p_1} \varepsilon_i \prod_{i=1}^{p_1} \overline{i}$$

En simplifiant par $\prod_{i=1}^{p_1} \overline{i}$ on obtient $\overline{a}^{p_1} = \prod_{i=1}^{p_1} \varepsilon_i$ et l'égalité en (i) puisque $\left(\frac{a}{p}\right) \cong a^{p_1}$ modulo p (1.4.4).

(ii) Relevons nos égalités $\overline{i}.\overline{a} = \varepsilon_i.\overline{h}_i$ dans $\mathbb{Z}$. Dans l'anneau $\mathbb{Z}$ nous obtenons

$$ia = \varepsilon_i h_i + c_i p \qquad \text{où} \qquad c_i \in \mathbb{Z} \qquad 1 \leqslant i \leqslant p_1.$$

Regardons la partie entière de $\frac{2ia}{p}$.

$$\text{Si } \varepsilon_i = 1 \text{ on a} \qquad \frac{2ia}{p} = \frac{2h_i}{p} + 2c_i \qquad \lfloor \frac{2ia}{p} \rfloor = 2c_i \in 2\mathbb{Z}.$$

$$\text{Si } \varepsilon_i = -1 \text{ on a} \qquad \frac{2ia}{p} = \frac{p - 2h_i}{p} + 2c_i - 1 \qquad \lfloor \frac{2ia}{p} \rfloor = 2c_i - 1 \in 2\mathbb{Z} + 1.$$

Le tout ensemble donne $\varepsilon_i = (-1)^{\lfloor \frac{2ia}{p} \rfloor}$. On remplace dans l'égalité (i) et on obtient l'égalité (ii). □

Voici une formule complémentaire.

Proposition 1.4.14. *Soit p un nombre premier naturel impair. Alors*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Démonstration. Nous posons comme précédemment $p_1 = \frac{p-1}{2}$ et nous commençons par regarder le symbole de Legendre $\left(\frac{2a}{p}\right)$ lorsque a est un entier rationnel *impair* non divisible par p.

Comme a est impair $a + p$ est pair et on a

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{\frac{a+p}{2}}{p}\right).$$

Comme $\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{2}{p}\right) = 1$ on obtient avec les notations du lemme précédent :

$$\left(\frac{2a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \lfloor \frac{i(a+p)}{p} \rfloor} = (-1)^{\sum_{i=1}^{p_1} i + \sum_{i=1}^{p_1} \lfloor \frac{ia}{p} \rfloor} = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{i=1}^{p_1} \lfloor \frac{ia}{p} \rfloor} \quad *$$

(la première égalité résulte du lemme précédant, la seconde est un simple calcul sur les exposants et la troisième vient de l'égalité bien connue $\sum_{i=1}^{p_1} i = \frac{p_1(p_1+1)}{2} = \frac{(p-1)(p+1)}{8}$).

Dans l' égalité $*$ nous remplaçons a par 1, nous observons que $\lfloor \frac{i}{p} \rfloor = 0$ pour $i \in \{1, \cdots, p_1\}$ et nous obtenons notre assertion. □

Lemme 1.4.15. *Soit p un nombre premier naturel impair et soit a un nombre entier rationnel impair non divisible par p. En posant comme précédemment $p_1 = \frac{p-1}{2}$ on a encore :*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \lfloor \frac{ia}{p} \rfloor}$$

Démonstration. Comme $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right)$ et comme $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ on obtient notre égalité en simplifiant l'égalité $*$ de la proposition précédente par $\left(\frac{2}{p}\right)$. □

Et voici enfin notre loi.

Théorème 1.4.16. *(Loi de réciprocité quadratique.) Soit $p \neq q$ deux nombres premiers naturels impairs. Alors*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Démonstration. Posons encore $p_1 = \frac{p-1}{2}$ et $q_1 = \frac{q-1}{2}$. Considérons les ensembles

$$S_1 = \{(i,j) \in \mathbb{N}^2 \mid 1 \leqslant i \leqslant p_1 \quad 1 \leqslant j \leqslant q_1 \quad qi > pj\}$$

$$S_2 = \{(i,j) \in \mathbb{N}^2 \mid 1 \leqslant i \leqslant p_1 \quad 1 \leqslant j \leqslant q_1 \quad qi < pj\}$$

Posons $$s_1 = \#S_1 \quad \text{et} \quad s_2 = \#S_2.$$

Comme $qi \neq pj$ quand $1 \leqslant i \leqslant p_1$ et $1 \leqslant j \leqslant q_1$ on a :

$$s_1 + s_2 = p_1 \cdot q_1$$

Comptons maintenant les éléments de S_1. Pour chaque $i \in \{1, 2, \cdots, p_1\}$ on a

$$qi > pj \Leftrightarrow j \leqslant \lfloor \frac{qi}{p} \rfloor.$$

Comme $\lfloor \frac{qi}{p} \rfloor \leqslant q_1$ quand $1 \leqslant i \leqslant p_1$ on obtient :

$$s_1 = \sum_{i=1}^{p_1} \lfloor \frac{qi}{p} \rfloor \qquad \text{et par symétrie} \qquad s_2 = \sum_{j=1}^{q_1} \lfloor \frac{pj}{q} \rfloor$$

Avec la formule du lemme précédent on obtient alors

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{s_1} \cdot (-1)^{s_2} = (-1)^{s_1+s_2} = (-1)^{p_1 \cdot q_1}$$

ce qui termine la preuve. □

Ces formules sont efficaces pour calculer le symbole de Legendre et décider si un nombre premier naturel reste premier dans l'anneau $\mathcal{O}_d$ des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}]$.

Exemple 1.4.17. $\left(\frac{45}{163}\right) = \left(\frac{5}{163}\right)\left(\frac{3}{163}\right)^2 = \left(\frac{5}{163}\right) = (-1)^{2\times 81}\left(\frac{163}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1).$

Le premier naturel 163 reste premier dans $\mathcal{O}_{45}$.

La loi de réciprocité quadratique est aussi utile pour voir quand une équation du type

$$x^2 + ay^2 = p, \quad a \in \mathbb{Z}, \quad p \text{ premier naturel impair}$$

admet une solution en entiers naturels. Ce genre de problèmes appartient à la théorie des formes quadratiques et c'est au départ de ces problèmes que Legendre a découvert la loi.

– –

1.4.18. Exercice. Soit p un premier naturel impair.
Montrer : $\left(\frac{2}{p}\right) = 1 \quad \Leftrightarrow \quad p \cong \pm 1$ modulo 8.

1.4.19. Exercice. Calculer $\left(\frac{57}{61}\right), \quad \left(\frac{72}{163}\right).$

1.4.20. Exercice. Calculer $\left(\frac{11}{19}\right)$, 19 est-il premier dans l'anneau des entiers de $\mathbb{Q}[\sqrt{11}]$?

1.4.21. Exercice. L'équation $x^2 + 2y^2 = p$, où p est un premier naturel impair.
(a) Montrer que $\mathbb{Z}[i\sqrt{2}]$ est principal.
(b) Montrer : $\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \cong 1$ ou 3 modulo 8.
(c) Soit p est un premier naturel impair.
Montrer que l'équation $x^2 + 2y^2 = p$ a une solution entière si et seulement si $p \cong 1$ ou 3 modulo 8. (Ceci est un des résultats de Fermat.)
Quand l'équation $x^2 - 2y^2 = p$ a-t'elle une solution entière ?

1.4.22. Exercice. Soit p un premier naturel impair.
(a) Montrer que $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.
(b) Montrer : $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \cong 1$ modulo 3.

1.4.23. Exercice. Soit p un premier naturel, $p > 3$.

Montrer que l'équation $x^2 + 3y^2 = p$ a une solution dans $\mathbb{N}$ si et seulement si $p \cong 1$ modulo 3. (Ceci est encore un résultat du à Fermat.)

(Indication. (a) Se rappeler que l'anneau des entiers de $\mathbb{Q}[i\sqrt{3}]$ est $\mathbb{Z}[\zeta]$, où $\zeta = \frac{-1+i\sqrt{3}}{2}$, se rappeler aussi que $\mathbb{Z}[\zeta]$ est principal.

(b) Se rappeler : $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \cong 1$ modulo 3.

(c) Se rappeler :

$$\left(\frac{-3}{p}\right) = 1 \Rightarrow p \text{ est non premier et non irréductible dans } \mathbb{Z}[\zeta].$$

(d) Observer que , si $p = N(a + b\zeta)$, alors $p = N(\zeta(a + b\zeta)) = N(\zeta^2(a + b\zeta))$.)

1.4.24. Exercice. Montrer qu'il existe une infinité de nombres premiers $\cong 1$ modulo 6.

(Indication. Procéder par l'absurde. Si $p_1, \cdots, p_k$ sont les seuls nombres premiers $\cong 1$ modulo 6, regarder les facteurs premier possibles du nombre $n = 4(p_1 \cdot p_2 \cdots p_k)^2 + 3$

Soit q un tel facteur. Remarquer d'abord que q est impair, que $q \neq 3$. Observer d'une part que $\left(\frac{-3}{q}\right) = 1$, donc que $q \cong 1$ modulo 3. Observer d'autre part que $q \cong 5$ modulo 6. En déduire une contradiction.)

1.5 L'équation $x^n + y^n = z^n$, $n = 2, 3, 4$

L'équation $x^2+y^2 = z^2$ est liée au théorème de Pythagore et ses solutions en entiers naturels sont connues depuis l'antiquité. Elles étaient apparemment déjà connues des Babyloniens il y a de ça plus de 3500 ans.

Théorème 1.5.1. *Les entiers naturels $x, y, z \in \mathbb{N}_0$ satisfont la relation*

$$x^2 + y^2 = z^2$$

si et seulement si $\exists$ $d, u, v \in \mathbb{N}_0$ *avec* $pgcd(u, v) = 1$ *tels que*

$$x = d(u^2 - v^2), \quad y = 2duv, \quad z = d(u^2 + v^2)$$

(à une permutation près de x et y).

Démonstration. Il est clair qu'un triple de naturels positifs de la forme $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$ est solution de l'équation $x^2 + y^2 = z^2$. Reste à montrer qu'il n'y en a pas d'autres.

Quand nous avons trois nombres naturels formant une solution de l'équation $x^2 + y^2 = z^2$, nous les divisons par leur plus grand commun diviseur d et nous obtenons une nouvelle solution (x, y, z) de l'équation où cette fois $\text{pgcd}(x, y, z) = 1$. Les nombres x, y et z sont alors premiers entre eux deux à deux, ils ne sont pas tous pairs, ils ne sont pas non plus tous impairs et un seul d'entre eux est pair. Ce ne peut être z qui est pair car la situation (x impair, y impair et z pair) donnerait $x^2 \cong y^2 \cong 1$ modulo 4, $z^2 \cong 0$ modulo 4 et $1 + 1 \cong 0$ modulo 4, ce qui est absurde.

Donc un et un seul des deux nombres x et y est pair. Quitte à permuter le rôle de x et y nous pouvons supposer que c'est y qui est pair. Nous sommes dans la situation

$$x \text{ impair} \qquad y \text{ pair} \qquad z \text{ impair .}$$

Dans cette situation les nombres $z + x$ et $z - x$ sont aussi pair. Écrivons

$$y = 2y' \qquad z + x = 2a \qquad z - x = 2b \qquad y', a, b \in \mathbb{N}_0$$

Avec ces notations nous avons $a + b = z$ et $a - b = x$, comme $\text{pgcd}(x, z) = 1$ on a aussi $\text{pgcd}(a, b) = 1$.

L'équation $x^2 + y^2 = z^2$ peut aussi s'écrire

$$y^2 = z^2 - x^2 = (z + x)(z - x) \qquad \text{ou} \qquad y'^2 = ab.$$

Comme $\text{pgcd}(a, b) = 1$ tout facteur premier de y', intervenant deux fois dans la factorisation de y'^2, intervient aussi deux fois dans la factorisation d'un des deux nombres a et b. On en déduit que a et b sont des carrés, on écrit :

$$a = u^2 \qquad b = v^2 \qquad u, v \in \mathbb{N}_0$$

et on a alors $x = u^2 - v^2 \quad y = 2uv \quad z = u^2 + v^2 \quad \text{pgcd}(u, v) = 1$.

On termine la preuve en multipliant cette solution par le pgcd d de la solution initiale. □

Avec cette description des solutions de l'équation $x^2+y^2 = z^2$ et quelques astuces Fermat arrive au résultat suivant (on peut en trouver une preuve dans [7]).

Théorème 1.5.2. *(Fermat.) L'équation $x^4 + y^4 = z^2$ n'a pas de solutions dans $\mathbb{Z}_0$.*

En particulier l'équation $x^4 + y^4 = z^4$ n'a pas non plus de solutions dans $\mathbb{Z}_0$,

Remarque 1.5.3. Si $n = 4m \in 2\mathbb{N}_0$ l'équation $x^n + y^n = z^n$ peut se réecrire $(x^m)^4 + (y^m)^4 = (z^m)^4$ et n'a donc pas non plus de solutions dans $\mathbb{Z}_0$.

Si $n = pm \in p\mathbb{N}_0$, où p est un nombre premier naturel, l'équation $x^n + y^n = z^n$ peut se réecrire $(x^m)^p + (y^m)^p = (z^m)^p$.

Pour démontrer l'assertion de Fermat qui dit que l'équation $x^n + y^n = z^n$ n'a pas de solutions dans $\mathbb{Z}_0$ quelle que soit la valeur du nombre naturel $n \geqslant 3$, il suffit donc de montrer qu'elle n'a pas de solution pour $n = p$ un nombre premier impair.

Ceci fut finalement démontré par Wiles à la fin du $XX^{\text{ième}}$ du siècle : il suppose que l'équation $x^n + y^n = z^n$ a une solution $(a, b, c) \in \mathbb{Z}_0^3$, à une telle solution il associe une cubique plane (une courbe d'équation $P(X, Y) = 0$ où $P \in \mathbb{Z}[X, Y]$ est un polynôme de degré 3 dont les coefficients proviennent de la solution (a, b, c)) et montre ensuite qu'une telle cubique ne peut exister. Sa preuve dépasse largement le cadre de ces notes, mais ceci nous indique qu'un simple problème sur les entiers rationnels peut trouver sa solution dans la géométrie.

Ici nous nous occuperons seulement de l'équation $x^3 + y^3 = z^3$.

Pour cela nous allons travailler dans l'anneau $\mathbb{Z}[\zeta]$, où $\zeta = \frac{-1+i\sqrt{3}}{2}$ est une racine $3^{\text{ième}}$ de l'unité dans $\mathbb{C}$, et , pour $\alpha, \beta \in \mathbb{Z}[\zeta]$, nous exploiterons la factorisation

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta)$$

obtenue en 1.3.25. Nous avons déjà travaillé dans l'anneau $\mathbb{Z}[\zeta]$, rappelons ceci.

Rappels 1.5.4. (1.3.24, 1.3.25). Soit $\zeta = \frac{-1+i\sqrt{3}}{2}$.

(i) $\zeta^3 = 1$ et le polynôme minimal de ζ sur $\mathbb{Q}$ est $X^2 + X + 1$.

(ii) Soit $a + b\zeta \in \mathbb{Z}[\zeta]$, $a, b \in \mathbb{Z}$. Alors

$$N(a + b\zeta) = (a - \frac{b}{2})^2 + 3\frac{b^2}{4} = a^2 - ab + b^2.$$

(iii) $\mathbb{Z}[\zeta]$ est un domaine principal et donc factoriel, les éléments de $\mathbb{Z}[\zeta]$ sont produits d'irréductibles, et ce de façon essentiellement unique.

(iv) Les inversibles de $\mathbb{Z}[\zeta]$ sont les éléments $1, -1, \zeta, -\zeta, \zeta^2, -\zeta^2$, ils forment un groupe cyclique d'ordre 6 et sont tous de norme 1.

(v) $3 = (1 - \zeta)(1 - \zeta^2)$.

(vi) $1 - \zeta$ et $1 - \zeta^2$ sont irréductibles et associés dans $\mathbb{Z}[\zeta]$
(car $N(1 - \zeta) = 3 = N(1 - \zeta^2)$ et $-\zeta(1 - \zeta^2) = (1 - \zeta)$).

(vii) Posons $\lambda = 1 - \zeta$, nous avons $3 \sim \lambda^2$.

Le nombre $\lambda = 1 - \zeta$, irréductible dans $\mathbb{Z}[\zeta]$, va jouer un rôle essentiel.

Proposition 1.5.5. *Reprenons les notations de 1.5.4 : $\lambda = 1 - \zeta$.*

(i) Tout élément de $\mathbb{Z}[\zeta]$ est équivalent à 0, 1 ou -1 modulo λ.
Plus précisément, $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta] \simeq \mathbb{Z}_3$.

(ii) $\forall \delta \in \mathbb{Z}[\zeta]$, $\delta \cong \delta^3$ modulo λ.

(iii) Soit $\delta \in \mathbb{Z}[\zeta]$. Si $\delta \cong \pm 1$ modulo λ, alors $\delta^3 \cong \pm 1$ modulo λ^3

Démonstration. (i) L'homomorphisme d'évaluation

$$e_\zeta : \mathbb{Z}[X] \to \mathbb{Z}[\zeta] : P \mapsto P(\zeta)$$

est surjectif, il a pour noyau l'idéal $(X^2 + X + 1)$ de $\mathbb{Z}[X]$ et $e_\zeta(1 - X) = \lambda$.
On en déduit : $\mathbb{Z}[X]/(X^2 + X + 1, 1 - X) \simeq \mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta]$.
Par ailleurs, l'homomorphisme d'évaluation

$$e_1 : \mathbb{Z}[X] \to \mathbb{Z} : P \mapsto P(1)$$

est surjectif, il a pour noyau l'idéal $(1 - X)$ de $\mathbb{Z}[X]$ et $e_1(X^2 + X + 1) = 3$.
On en déduit : $\mathbb{Z}[X]/(X^2 + X + 1, 1 - X) \simeq \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}_3$.

(ii) Conséquence de (i) et du petit théorème de Fermat 0.9.2 : $\forall x \in \mathbb{Z}_3$, nous avons $x^3 = x$.

(iii) Si $\delta \cong \pm 1$ modulo λ, on a $\delta = \pm 1 + \lambda\gamma$ pour un certain $\gamma \in \mathbb{Z}[\zeta]$. Tenant compte de ce que $3 \sim \lambda^2$, il vient $\delta^3 = \pm 1 + 3\lambda\gamma + 3(\pm 1)\lambda^2\gamma^2 + \lambda^3\gamma^3 = \pm 1 + \lambda^3\gamma'$ pour un certain $\gamma' \in \mathbb{Z}[\zeta]$ qu'il est inutile d'expliciter. □

Théorème 1.5.6. *L'équation $\alpha^3 + \beta^3 = \gamma^3$ n'a pas de solution non triviale dans $\mathbb{Z}[\zeta]$, à fortiori n'a pas de solution dans $\mathbb{Z}_0$.*

Démonstration. Supposons que les nombres non nuls α, β, γ de $\mathbb{Z}[\zeta]$ satisfassent la relation $\alpha^3 + \beta^3 = \gamma^3$. Quitte à diviser α, β, γ par leur pgcd, nous pouvons supposer α, β, γ premiers entre eux dans leur ensemble et donc premiers entre eux deux à deux.

Première étape. Montrons d'abord qu'un des trois nombres α, β, γ est divisible par λ.

Modulo λ nous avons $\alpha + \beta \cong \gamma$ modulo λ (1.5.5) et nous pouvons écrire $\gamma = (\alpha + \beta) + \lambda\tau$ pour un certain $\tau \in \mathbb{Z}[\zeta]$. Portons ceci dans notre équation, il vient $\alpha^3 + \beta^3 = (\alpha + \beta)^3 + 3\lambda\tau(\alpha + \beta)^2 + 3\lambda^2\tau^2(\alpha + \beta) + \lambda^3\tau^3$. Comme $\lambda^2 \sim 3$ nous en déduisons $0 = 3\alpha^2\beta + 3\alpha\beta^2 + 3\lambda\tau'$ pour un certain $\tau' \in \mathbb{Z}[\zeta]$ qu'il est inutile d'expliciter. En simplifiant par 3 nous obtenons $\alpha\beta(\alpha + \beta) \cong 0$ modulo λ, $\alpha\beta\gamma \cong 0$ modulo λ, ce qui signifie qu'au moins un des trois nombres α, β, γ est divisible par λ.

Étape intermédiaire. Notre équation peut aussi s'écrire $\alpha^3 + (-\gamma)^3 = (-\beta)^3$, au signe près les trois nombres α, β, γ peuvent y être permutés. Nous savons qu'un et un seul des trois nombres α, β, γ est divisible par λ et nous pouvons supposer que c'est γ. Nous écrivons alors $\gamma = \lambda^m\gamma_0$ où $m \in \mathbb{N}_0$ et où γ_0 n'est pas divisible par λ. Nous avons maintenant trois nombres non nuls α, β, γ_0 deux à deux premiers entre eux, dont aucun n'est divisible par λ, et satisfaisant l'équation $\alpha^3 + \beta^3 = \lambda^{3m}\gamma_0^3$. Il nous suffit de montrer que ceci est impossible.

Deuxième étape. Nous allons montrer plus, nous allons montrer qu'il n'existe pas de nombres non nuls $\alpha, \beta, \gamma_0 \in \mathbb{Z}[\zeta]$ deux à deux premiers entre eux, dont aucun n'est divisible par λ, et satisfaisant une équation de la forme

$$\alpha^3 + \beta^3 = \varepsilon\lambda^{3m}\gamma_0^3 \quad \text{où } m \geqslant 1 \text{ et où } \varepsilon \in \mathbb{Z}[\zeta]^\times.$$

Nous allons procéder par l'absurde, nous supposons que de tels nombre existent et nous prenons une équation de ce type où l'exposant $m \in \mathbb{N}_0$ est *minimum*.

Nous factorisons le premier membre, il vient :

$$(\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta) = \varepsilon\lambda^{3m}\gamma_0^3.$$

Regardons la différence entre deux des trois facteurs $(\alpha + \beta), (\alpha + \zeta\beta), (\alpha + \zeta^2\beta)$. Pour $0 \leqslant i < j \leqslant 2$, nous avons

$$(\alpha + \zeta^i\beta) - (\alpha + \zeta^j\beta) = \zeta^i\beta(1 - \zeta^{j-i}) \sim \beta\lambda.$$

Regardons maintenant le pgcd de deux de ces trois facteurs.

Si χ est un diviseur commun des deux nombres $(\alpha + \zeta^i\beta)$ et $(\alpha + \zeta^j\beta)$, χ divise aussi leur différence, on a $\chi|\beta\lambda$.

Mais χ divise aussi $\zeta^{-i}(\alpha+\zeta^i\beta)-\zeta^{-j}(\alpha+\zeta^j\beta) = -\zeta^{-j}(1-\zeta^{j-i})\alpha \sim \alpha\lambda$, on a $\chi|\alpha\lambda$.

Comme α et β sont premiers entre eux, nous avons aussi $\chi|\lambda$.

Mais $\mathbb{Z}[\zeta]$ est un domaine factoriel, l'élément irréductible λ, divisant $\lambda^{3m}\gamma_0$, divise au moins un des trois facteurs $(\alpha + \beta), (\alpha + \zeta\beta), (\alpha + \zeta^2\beta)$.

Comme λ divise aussi la différence entre deux de ces trois facteurs, il les divise tous les trois. On en déduit que $\text{pgcd}((\alpha + \zeta^i\beta), (\alpha + \zeta^j\beta)) \sim \lambda$, que les trois facteurs $(\alpha + \beta), (\alpha + \zeta\beta), (\alpha + \zeta^2\beta)$ sont divisibles par λ et qu'un seul d'entre eux peut être divisible par λ^2.

Nous avons donc $\frac{(\alpha+\zeta^i\beta)}{\lambda} \in \mathbb{Z}[\zeta]$, $0 \leqslant i \leqslant 2$. La différence entre deux quelconques des trois nombres $\frac{(\alpha+\zeta^i\beta)}{\lambda} \in \mathbb{Z}[\zeta]$ est associée à β et donc non divisible par λ. Les images de ces trois nombres dans le quotient $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta] \simeq \mathbb{Z}_3$ sont donc distinctes deux à deux. Comme $\#(\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta] \simeq \mathbb{Z}_3) = 3$, 1.5.5, l'une au moins de ces images est nulle, ce qui signifie qu'au moins un des trois nombres $(\alpha+\beta), (\alpha+\zeta\beta), (\alpha+\zeta^2\beta)$ est divisible par λ^2, et que $m \geqslant 2$.

Quitte à remplacer β par $\zeta\beta$ ou $\zeta^2\beta$, ce qui n'affecte pas l'équation de départ, nous pouvons supposer que c'est $\alpha + \beta$ qui est divisible par λ^2.

Nous écrivons alors

$$\begin{array}{rcl} \alpha + \beta & = & \lambda^{3m-2}\delta_0 \\ \alpha + \zeta\beta & = & \lambda\delta_1 \\ \alpha + \zeta^2\beta & = & \lambda\delta_2 \end{array}$$

Ici nos nouveaux nombres $\delta_0, \delta_1, \delta_2$ sont deux à deux premiers entre eux et non divisibles par λ. En portant ceci dans l'équation de départ et en simplifiant, il vient

$$\delta_0\delta_1\delta_2 = \varepsilon\gamma_0^3.$$

On en déduit que les δ_i sont associés à des cubes, que $\delta_i \sim \tau_i^3$ pour certains $\tau_i \in \mathbb{Z}[\zeta]$. On a donc

$$\begin{array}{rcl} \alpha + \beta & = & \lambda^{3m-2}\tau_0^3\varepsilon_0 \\ \alpha + \zeta\beta & = & \lambda\tau_1^3\varepsilon_1 \\ \alpha + \zeta^2\beta & = & \lambda\tau_2^3\varepsilon_2 \end{array}$$

où $\varepsilon_0, \varepsilon_1, \varepsilon_2$ sont inversibles.

On multiplie la première équation par ζ, la seconde par ζ^2, on additionne le tout et, tenant compte de $\zeta^2 + \zeta + 1 = 0$, on obtient

$$0 = \lambda^{3m-2}\tau_0^3\zeta\varepsilon_0 + \lambda\tau_1^3\zeta^2\varepsilon_1 + \lambda\tau_2^3\varepsilon_2.$$

On divise par $\lambda\varepsilon_2$, il vient

$$\lambda^{3(m-1)}\tau_0^3\varepsilon' = \tau_1^3\eta + \tau_2^3$$

où ε', η sont des inversibles qu'il est inutile d'expliciter.

Nous sommes presque au bout de nos peines, il nous suffit maintenant de prouver que l'inversible η figurant dans la dernière équation est un cube pour obtenir une égalité du même type que celle du départ de cette seconde étape, mais où l'exposant m est remplacé par $m-1$, contredisant le choix de m.

Voyons donc ce dernier point.

Comme les τ_i ne sont pas divisibles par λ, que $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta] \simeq \mathbb{Z}_3$ (1.5.5(i)), nous avons $\tau_i \cong \pm 1$ modulo λ et aussi $\tau_i^3 \cong \pm 1$ modulo λ^3 (1.5.5(iii)). Compte tenu de ceci et de $m \geqslant 2$ notre dernière équation donne :

$$(\pm 1)\eta + (\pm 1) \cong 0 \text{ modulo } \lambda^3, \quad \eta \cong \pm 1 \text{ modulo } \lambda^3.$$

Puisque $\lambda^2 \sim 3$, nous avons aussi

$$\eta \cong \pm 1 \text{ modulo } 3, \quad \eta = \pm 1 + 3(a + b\zeta), \text{ pour certains } a, b \in \mathbb{Z}.$$

Comme η est inversible nous obtenons

$$1 = N(\eta) = (3a \pm 1 - \frac{3b}{2})^2 + 3\frac{9b^2}{4}.$$

On en déduit $b = 0$, puis $a = 0$ et enfin $\eta = \pm 1 = (\pm 1)^3$. □

1.6 L'équation de Pell-Fermat

1.6.1. L'équation de Pell-Fermat (qui n'a rien à voir avec Pell) est l'équation

$$x^2 - ny^2 = \pm 1$$

où n est un entier naturel >1 qui n'est pas un carré.

Fermat nous dit que cette équation a une infinité de solutions en nombres naturels. En particulier elle a dans $\mathbb{Z}$ une solution $(x, y) \neq (\pm 1, 0)$. Comme $x^2 - ny^2 = (x + y\sqrt{n})(x - y\sqrt{n})$, ceci signifie que l'anneau $\mathbb{Z}[\sqrt{n}]$ possède un élément inversible $\neq \pm 1$, résultat plus ou moins annoncé en 1.3.10 dans le cas où n est un entier naturel sans facteurs carrés. Notons que, si n a un facteur carré, c.à-d. si $n = c^2 d$, où d est lui un entier naturel >1 sans facteur carré, alors $\mathbb{Z}[\sqrt{n}] = \mathbb{Z}[c\sqrt{d}] = \{a + bc\sqrt{d} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau et un sous-$\mathbb{Z}$-module libre de rang 2 de $\mathcal{O}_d$, de base $(1, c\sqrt{d})$.

Notre but dans cette section est de démontrer ce résultat de Fermat. Nous utiliserons la norme définie sur $\mathbb{Q}[\sqrt{d}]$ et le fait que $N(\mathbb{Z}[c\sqrt{d}]) \subset \mathbb{Z}$. La démarche sera la suivante. Quelques considérations géométriques et analytiques sur l'espace euclidien $\mathbb{R}^n$ nous permettrons de construire une suite $\alpha_i \in \mathbb{Z}[c\sqrt{d}], i \in \mathbb{N}_0$, d'éléments distincts deux-à-deux et dont la valeur absolue de la norme est inférieure à un un nombre réel donné suffisamment grand. Pour conclure, on utilisera le fait que, pour tout nombre naturel q, l'ensemble $\mathcal{I}_q$ des idéaux de $\mathbb{Z}[c\sqrt{d}]$ de la forme $\{\alpha\mathbb{Z}[c\sqrt{d}] \mid \alpha \in \mathbb{Z}[c\sqrt{d}] \text{ et } |N(\alpha)| = q\}$ est fini.

Commençons donc par quelques résultats concernant l'espace $\mathbb{R}^n$. Ici $\mathbb{R}^n$ est vu à la fois comme groupe commutatif (ou $\mathbb{Z}$-module) et comme espace vectoriel réel ; sa base canonique, en tant qu'espace vectoriel réel, sera désignée par $e = (e_1, \cdots, e_n)$. De plus, $\mathbb{R}^n$ est muni de son produit scalaire usuel : $(a_1, \cdots, a_n) \cdot (b_1, \cdots, b_n) = \sum_i a_i b_i$. Ce produit scalaire munit $\mathbb{R}^n$ d'une structure d'espace métrique et d'une relation d'orthogonalité pour lesquelles les vecteurs e_i de la base canonique sont de longueur 1 et orthogonaux deux-à-deux. Nous dirons d'un élément de $\mathbb{R}^n$ qu'il est un « *point* » ou un « *vecteur* » de $\mathbb{R}^n$ selon l'humeur du moment.

Définitions 1.6.2. Un sous-groupe discret de $\mathbb{R}^n$ est un sous-groupe de $\mathbb{R}^n$ engendré par m vecteurs linéairement indépendants (sur $\mathbb{R}$) de $\mathbb{R}^n$, $m \leqslant n$.

Un **réseau** de $\mathbb{R}^n$ est un sous-groupe H de $\mathbb{R}^n$ engendré par exactement n vecteurs linéairement indépendants $u_1, \cdots, u_n$ de $\mathbb{R}^n$. Ces n vecteurs forment donc une base du $\mathbb{R}$-vectoriel $\mathbb{R}^n$ et une base de H en tant que $\mathbb{Z}$-module. Nous dirons alors que $u = (u_1, \cdots, u_n)$ est une **$\mathbb{Z}$-base** de H.

1.6.3. Propriété. Si H est un sous-groupe discret de $\mathbb{R}^n$, alors, pour toute partie bornée B de $\mathbb{R}^n$, $B \cap H$ est fini.

(En fait, on peut montrer que cette propriété caractérise les sous-groupes discrets de $\mathbb{R}^n$. Rappelons qu'une partie B de $\mathbb{R}^n$ est bornée s'il existe $r_1, \cdots, r_n \in \mathbb{R}$ tels que, $\forall x = (x_1, \cdots, x_n) \in B$, on a : $-r_i \leqslant x_i \leqslant r_i$.)

Définitions et observations 1.6.4. Soit H un réseau de $\mathbb{R}^n$. Pour chaque $\mathbb{Z}$-base $u = (u_1, \cdots, u_n)$ de H on construit le parallélotope semi-ouvert

$$P_u = \{\sum_i r_i u_i \mid \forall i, 1 \leqslant i \leqslant n, \quad r_i \in \mathbb{R} \quad \text{et} \quad 0 \leqslant r_i < 1\}.$$

appelé **domaine fondamental** de H.

Tout comme les translatés $z + [0, 1[$, où z parcourt $\mathbb{Z}$, forment une partition de $\mathbb{R}$, les translatés $h + P_u$, où h parcourt H, forment une partition de $\mathbb{R}^n$. Tout point x de $\mathbb{R}^n$ appartient donc à un et un seul des translatés de P_u par les vecteurs de H.

Le **volume** ou **mesure** d'une partie S de $\mathbb{R}^n$ est défini par $\mu(S) = \int \cdots \int_S dx_1 dx_2 \cdots dx_n$ quand cette intégrale existe, autrement dit quand S est mesurable (ici les coordonnées sont prises par rapport à la base canonique de $\mathbb{R}^n$).

Si u_i est le point de coordonnées $(u_{1i}, \cdots, u_{ni})$, les u_{ij} sont les entrées d'une matrice $U \in \mathbb{R}^{n\times n}$ et la formule des changements de variables dans les intégrales multiples nous donne $\mu(P_u) = |\det(U)|$. Si $u' = (u'_1, \cdots, u'_n)$ est une autre $\mathbb{Z}$-base de H, on a $u' = uC$, où $C \in \mathbb{Z}^{n\times n}$ est une matrice inversible dans l'anneau de matrices $\mathbb{Z}^{n\times n}$, et où donc $\det(C) = \pm 1$. La formule des changements de variables dans les intégrales multiples nous donne alors $\mu(P_u) = |\det(C)|\mu(P_{u'}) = \mu(P'_u)$. Ceci montre que le volume d'un domaine fondamental de H est indépendant de la $\mathbb{Z}$-base de H choisie pour le construire et nous permet de définir la **maille** $v(H)$ du réseau H comme étant le volume d'un quelconque de ses domaines fondamentaux.

Théorème 1.6.5. *(Minkowsky.) Soit H un réseau de $\mathbb{R}^n$ et S une partie mesurable de $\mathbb{R}^n$ de volume $\mu(S) > v(H)$.*

Alors S comprend deux éléments distincts x et y tels que $x - y \in H$.

Démonstration. Soit u une $\mathbb{Z}$-base de H. Comme les translatés par les éléments de H d'un domaine fondamental de H forment une partition de $\mathbb{R}^n$ nous avons $S = \bigcup_{h\in H}(S \cap (h + P_u))$ et les pièces intervenant dans cette réunion sont disjointes. Par l'additivité de la mesure on en déduit

$$\mu(S) = \sum_{h\in H} \mu(S \cap (h + P_u)).$$

Mais nos volumes sont invariants par translations, on a aussi

$$\mu(S \cap (h + P_u)) = \mu((S - h) \cap P_u).$$

De l' hypothèse sur S on déduit que les parties $((S - h) \cap P_u)$ de $\mathbb{R}^n$ ne sont pas toutes disjointes, qu'il existe deux éléments distincts h_1 et h_2 de H tels que $(S - h_1) \cap (S - h_2) \cap P_u) \neq \varnothing$. Nous avons donc deux éléments $x, y \in S$ tels que $x - h_1 = y - h_2$, tels que $0 \neq x - y = h_1 - h_2 \in H$. □

Corollaire 1.6.6. *Soit encore H un réseau de $\mathbb{R}^n$ et soit cette fois S une partie mesurable de $\mathbb{R}^n$, convexe et symétrique par rapport à l'origine.*

Si $\mu(S) > 2^n v(H)$, alors $S \cap H$ comprend un point autre que 0.

Démonstration. Regardons la partie $S' = \frac{1}{2}S$.

Nous avons $\mu(S') = 2^{-n}\mu(S) > v(H)$ et donc S' comprends deux éléments distincts x et y tels que $0 \neq x - y \in H$, 1.6.5. Mais alors $2x, 2y \in S$ et aussi $0 \neq x - y = \frac{1}{2}(2x + (-2y)) \in S$ car S est symétrique par rapport à l'origine et convexe. □

Les corps quadratiques imaginaires se plongent naturellement dans le plan de Gauss $\mathbb{C}$. Pour les corps quadratiques réels, nous allons utiliser leur automorphisme de conjugaison σ de façon à en obtenir aussi une « *représentation géométrique* ».

Proposition 1.6.7. *Soit $d > 1$ un entier naturel sans facteur carré et soit $\mathbb{Q}[\sqrt{d}]$ le corps quadratique réel correspondant. La fonction*

$$\tilde{\sigma} : \mathbb{Q}[\sqrt{d}] \to \mathbb{R}^2 : \alpha \mapsto (\alpha, \sigma(\alpha))$$

est un homomorphisme injectif d'anneaux, à fortiori de $\mathbb{Z}$-modules.

Si de plus M est un sous-$\mathbb{Z}$-module libre de rang 2 de $\mathbb{Q}[\sqrt{d}]$, alors $\tilde{\sigma}(M)$ est un réseau de $\mathbb{R}^2$.

Démonstration. Comme σ est un automorphisme du corps $\mathbb{Q}[\sqrt{d}]$ la première assertion est évidente.

Pour montrer la seconde, soit (α, β) une base du $\mathbb{Z}$-module M. Comme $\tilde{\sigma}$ est un homomorphisme injectif nous avons que $\tilde{\sigma}(M)$ est un sous-$\mathbb{Z}$-module libre de $\mathbb{R}^2$, de base $\tilde{\sigma}(\alpha), \tilde{\sigma}(\beta)$. Il nous reste à montrer que les vecteurs $\tilde{\sigma}(\alpha)$ et $\tilde{\sigma}(\beta)$ de $\mathbb{R}^2$ sont linéairement indépendants sur $\mathbb{R}$. Si ce n'était pas le cas nous aurions $\frac{\alpha}{\beta} = \frac{\sigma(\alpha)}{\sigma(\beta)} = \sigma(\frac{\alpha}{\beta})$ et donc $\frac{\alpha}{\beta} \in \mathbb{Q}$, 1.3.2, ce qui est impossible car les nombres α et β, étant linéairement indépendants sur $\mathbb{Z}$, sont aussi linéairement indépendants sur $\mathbb{Q}$. □

Lemme 1.6.8. *Soit M un sous-$\mathbb{Z}$-module libre de rang 2 du corps quadratique réel $\mathbb{Q}[\sqrt{d}]$ tel que tous les nombres de M soient entiers sur $\mathbb{Z}$ et soit un nombre réel $c > v(\tilde{\sigma}(M)$.*

Alors M comprend une infinité dénombrable de nombres non nuls $\alpha_n, n \in \mathbb{N}$, distincts deux-à-deux et tels que $|N(\alpha_n)| < c$.

Démonstration. À tout nombre réel $r > 0$ associons le rectangle de $\mathbb{R}^2$ défini par

$$B_r = \{(x, y) \in \mathbb{R}^2 \mid |x| < r \text{ et } |y| < cr^{-1}\}.$$

Ces rectangles sont convexes, symétriques par rapport à l'origine et leur volume satisfait $v(B_r) = 2^2 c > 2^2 v(\tilde{\sigma}(M)$. Comme $\tilde{\sigma}(M)$ est un réseau de $\mathbb{R}^2$, 1.6.7, il existe un nombre non nul $\alpha_r \in M$ tel que $\tilde{\sigma}(\alpha_r) \in B_r$, 1.6.6.

Occupons-nous d'abord de la norme de ces nombres. Nous avons :

$$1 \leqslant |N(\alpha_r)| = |\alpha_r| \cdot |\sigma(\alpha_r)| < c$$

la première inégalité provenant du fait que α_r est entier sur $\mathbb{Z}$ et non nul, la seconde de la description de B_r.

Occupons-nous maintenant de la valeur absolue de ces nombres, les inégalités ci-dessus nous donnent

$|\alpha_r| = |N(\alpha_r)| \cdot |\sigma(\alpha_r)|^{-1} \geqslant |\sigma(\alpha_r)|^{-1} > rc^{-1}$, d'où

$$rc^{-1} < |\alpha_r| < r.$$

Fixons maintenant un nombre réel positif r_0, considérons la suite des nombres réels $r_n = c^n r_0, n \in \mathbb{N}$, et la suite des nombres α_{r_n} correspondants. Ces nombres α_{r_n} de M sont distincts deux-à-deux car ils se situent comme suit sur la droite réelle

$$r_0c^{-1} < |\alpha_{r_0}| < r_0 = r_1c^{-1} < |\alpha_{r_1}| < r_1 \cdots < r_ic^{-1} < |\alpha_{r_i}| < r_i = r_{i+1}c^{-1} \cdots .$$

□

Le lemme suivant est valable pour tout corps quadratique, réel ou non, et est un cas très particulier d'un résultat (2.4.14) concernant tous les corps de nombres.

Lemme 1.6.9. *Soit $\mathcal{O}$ un sous-anneau du corps quadratique $\mathbb{Q}[\sqrt{d}]$ qui, en tant que $\mathbb{Z}$-module, est un $\mathbb{Z}$-module libre de rang 2, et soit q un entier naturel non nul.*

Alors l'ensemble d'idéaux $\mathfrak{I}_q = \{\alpha\mathcal{O} \mid \alpha \in \mathcal{O} \text{ et } |N(\alpha)| = q\}$ de $\mathcal{O}$ est fini.

Démonstration. Comme $\mathcal{O}$ est entier sur $\mathbb{Z}$, 1.2.14, nous avons, $\forall \alpha \in \mathcal{O}$, $N(\alpha), T(\alpha) \in \mathbb{Z}$ et $N(\alpha) = -\alpha^2 + T(\alpha)\alpha$ (voir 1.3.6 et 1.3.5), d'où $N(\alpha) \in \alpha\mathcal{O}$. Il suffit donc de montrer que l'ensemble des idéaux de $\mathcal{O}$ contenant q est fini.

Comme $\mathcal{O}/q\mathcal{O}$ a aussi une structure de $\mathbb{Z}/q\mathbb{Z}$-module de type fini pouvant être engendré par deux éléments, ce module $\mathcal{O}/q\mathcal{O}$ est une image homomorphe de $(\mathbb{Z}/q\mathbb{Z})^2$ (cf. 0.8.3). En particulier $\mathcal{O}/q\mathcal{O}$ est un anneau fini (de cardinal $\leqslant q^2$) et n'admet qu'un nombre fini d'idéaux. Pour terminer, rappelons que les idéaux de $\mathcal{O}/q\mathcal{O}$ sont en bijection avec les idéaux de $\mathcal{O}$ contenant q. □

Proposition 1.6.10. *Les sous-anneaux $\mathbb{Z}[c\sqrt{d}], \mathbb{Z}[\sqrt{d}]$ et $\mathcal{O}_d$ du corps quadratique réel $\mathbb{Q}[\sqrt{d}]$ admettent un inversible $\varepsilon \neq \pm 1$.*

En particulier l'équation de Pell-Fermat admet une infinité de solutions dans $\mathbb{Z}$.

Démonstration. Les sous-anneaux $\mathbb{Z}[c\sqrt{d}], \mathbb{Z}[\sqrt{d}]$ et $\mathcal{O}_d$ ont ceci en commun qu'ils sont tous trois des $\mathbb{Z}$-modules libres de rang 2, entiers sur $\mathbb{Z}$ (voir 1.2.14), et nous pouvons appliquer 1.6.8 à l'un quelconque d'entre eux, nommons-le $\mathcal{O}$. Nous obtenons une infinité dénombrable de nombres non nuls $\alpha_n \in \mathcal{O}$ dont la valeur absolue de la norme est inférieure à un réel c suffisamment grand. Comme les $|N(\alpha_n)| \in \mathbb{N}_0$, nous avons aussi un nombre naturel non nul $q < c$ et parmi nos α_n une infinité dénombrable de nombres β_n avec $|N(\beta_n)| = q$. Mais les idéaux $\beta_n\mathcal{O}$ sont en nombre fini, 1.6.9. Parmi les β_n nous avons donc deux nombres $\beta_i \neq \pm\beta_j$ avec $\beta_i\mathcal{O} = \beta_j\mathcal{O}$. Écrivons alors $\beta_i = \varepsilon\beta_j$, on a $N(\varepsilon) = \pm 1$ et ε est un inversible de $\mathcal{O}$ différent de $\neq \pm 1$.

Dès lors les puissances ε^n de ε sont aussi des inversibles de $\mathcal{O}$ et elles sont distinctes deux-à-deux puisque ε est un nombre réel $\neq \pm 1$. Dans le cas où $\mathcal{O} = \mathbb{Z}[c\sqrt{d}]$ chacun de ces ε^n fournit une solution entière de l'équation de Pell-Fermat. □

Remarque 1.6.11. Comme en 1.3.12 on peut définir l'unité fondamentale de $\mathbb{Z}[\sqrt{n}]$.

Si l'unité fondamentale de $\mathbb{Z}[\sqrt{n}]$ est de norme (-1) les deux équations $x^2 - ny^2 = 1$ et $x^2 - ny^2 = -1$ ont une infinité de solutions entières.

Si l'unité fondamentale de $\mathbb{Z}[\sqrt{n}]$ est de norme 1, alors, $\forall \varepsilon \in \mathbb{Z}[\sqrt{n}]^\times$ on a $N(\varepsilon) = 1$ et seule l'équation $x^2 - ny^2 = 1$ admet des solutions entières (en nombre infini).

Chapitre 2

Anneaux d'entiers algébriques

Les anneaux qui nous occupent ici sont les sous-anneaux d'un corps de nombres K qui, en tant que $\mathbb{Z}$-modules, sont libres de type fini, de rang $[K : \mathbb{Q}]$. De tels anneaux seront appelés « *ordres* » de K. Pour les observer, un peu de bagage algébrique sera utile.

Les remarques qui suivent auront aussi quelques retombées sur les corps quadratiques. Nous pourrons déterminer entre autres les valeurs de $d < 0$ pour lesquelles l'anneau $\mathcal{O}_d$ des entiers de $\mathbb{Q}[\sqrt{d}]$ est euclidien (2.4.20).

2.1 Anneaux et modules noethériens

Commençons par un préambule sur les ensembles ordonnés en relation avec l'axiome du choix 0.2.6.

Lemme 2.1.1. *Dans un ensemble ordonné $(E, \prec)$, les conditions suivantes suivantes sont équivalentes :*

(i) Toute suite croissante $x_1 \prec x_2 \prec \cdots \prec x_n \prec \cdots$ dans E est stationnaire, ce qui signifie qu'il existe $k \in \mathbb{N}$ tel que $\forall n \geqslant k$ on aie $x_k = x_n$,

(ii) Toute partie non vide P de E possède un élément maximal.

Démonstration. (i) $\Rightarrow$ (ii). Soit $\varnothing \neq P \subset E$ et supposons que P ne possède pas d'élément maximal. Pour tout $x \in P$ nous pouvons donc choisir (avec l'axiome du choix) un élément $c(x) \in P$ tel que $x \prec c(x)$ et $x \neq c(x)$, ce qui nous donne une fonction $c : P \to P$. Prenons un élément quelconque $x_0 \in P$. Cette fonction c nous fournit une suite strictement croissante au départ de $x_0 : x_0 \prec c(x_0) \prec c(c(x_0)) \prec \cdots \prec c^n(x) \prec \cdots$, en contradiction avec la condition (i).

(ii) $\Rightarrow$ (i). Les termes de la suite croissante $x_1 \prec x_2 \prec \cdots \prec x_n \prec \cdots$ forment une partie non vide de E qui possède un maximal, disons x_k. Ceci implique que notre suite stationne en ce maximal x_k. □

Nous sommes prêts à introduire les conditions de « finitude » sur les modules qui nous intéressent. Elles concernent l'ensemble des sous-modules d'un module M, ensemble qui s' ordonne par inclusion.

Théorème 2.1.2. *Soit A un anneau et M un A-module. Les conditions suivantes suivantes sont équivalentes :*

(i) Tout sous-module de M est de type fini,

(ii) Toute suite croissante de sous-modules de M :

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

est stationnaire,

(iii) Tout ensemble non vide de sous-modules de M possède un maximal.

Démonstration. (i) $\Rightarrow$ (ii). Soit $M' = \bigcup_{n\in\mathbb{N}_0} M_n$, M' est un sous-module de M, donc engendré par un nombre fini d'éléments, disons par ses éléments $w_1, \cdots, w_r$. Chacun de ces w_j appartient à un des sous-modules de la suite, disons $w_j \in M_{i(j)}, i(j) \in \mathbb{N}_0, 1 \leqslant j \leqslant r$. Comme ces w_j sont en nombre fini, ils appartiennent tous au plus grand des $M_{i(j)}$, à savoir M_k, où $k = \max\{i(j) \mid 1 \leqslant j \leqslant r\}$. On a donc $M' \subset M_k \subset M'$, d'où $M' = M_k$ et notre suite stationne en M_k.

(ii) $\Leftrightarrow$ (iii). Découle de 2.1.1

(iii) $\Rightarrow$ (i). Soit N un sous-module de M et soit $\mathcal{S}_N$ l'ensemble des sous -modules de type fini de N. $\mathcal{S}_N \neq \varnothing$ car $\{0\} \in \mathcal{S}_N$. Donc $\mathcal{S}_N$ comprend un sous-module maximal, disons N'. Mais alors, $\forall x \in N$, $N' + Ax$ est aussi un sous-module de type fini de N : $N' + Ax \in \mathcal{S}_N$. On en déduit que $N' + Ax = N'$ par la maximalité de N', que $x \in N'$. On a donc $N = N'$ et N est de type fini. □

Définition 2.1.3. Un **A-module est dit A-noethérien** (ou simplement noethérien quand ceci ne prête pas à confusion) s'il satisfait l'une des trois conditions équivalentes du théorème 2.1.2.

Un **anneau A est dit noethérien** s'il est noethérien en tant que A-module, autrement dit si tous ses idéaux sont de type fini.

Exemples 2.1.4. L'anneau des entiers $\mathbb{Z}$ et plus généralement les anneaux principaux sont des anneaux noethériens, ce ne sont pas les seuls.

Lemme 2.1.5. *Soit N un A-module et soit N' un sous-A-module de N.*

Si N' et N/N' sont de type fini, alors N est aussi de type fini.

Démonstration. Soit $w_1, \cdots, w_r$ des éléments de N dont les images dans le quotient N/N' engendrent ce quotient, soit encore $v_1, \cdots, v_s$ une partie génératrice de N'. Il suffit de remarquer que les éléments $w_1, \cdots, w_r, v_1, \cdots, v_s$ engendrent N. □

Proposition 2.1.6. *Soit M un A-module et soit $M' \subset M$ un sous-A-module de M. Alors :*

$$M \text{ est noethérien } \Leftrightarrow M' \text{ et } M/M' \text{ sont noethériens .}$$

Démonstration. (i) $\Rightarrow$. Ceci est assez clair d'après la définition.

(ii) $\Leftarrow$. Soit N un sous-A-module de M. L'A-module $(N + M')/M'$ est un sous-A-module de M/M', il est donc de type fini. Mais $(N + M')/M' \simeq N/(N \cap M')$ et $N \cap M'$ est aussi de type fini en tant que sous-A-module de M'. On conclut avec 2.1.5. □

Corollaire 2.1.7. *(i) La somme directe de deux A-modules A-noethériens est A-noethérien.*

(ii) Tout module de type fini sur un anneau noethérien A est A-noethérien.

Démonstration. La première assertion est une conséquence directe de 2.1.6.

Pour obtenir la dernière, notons d'abord qu'un A-module libre de type fini sur un anneau noethérien A est A-noethérien (en tant que somme directe finie de modules A-noethériens). Rappelons ensuite que tout A-module de type fini peut se voir comme quotient d'un A-module libre de type fini (0.8.3). □

Les anneaux noethériens sont nombreux, comme l'indique le résultat fondamental suivant que nous ne démontrerons pas ici puisque 2.1.7 suffira à nos explorations des nombres.

Théorème 2.1.8. *(Théorème de la base d'Hilbert). Si A est noethérien, tout anneau de polynômes $A[X_1, \cdots, X_n]$ en un nombre fini d'indéterminées $X_1, \cdots, X_n$ est un anneau noethérien.*

En particulier, si K est un corps, $K[X_1, \cdots, X_n]$ et tous les quotients de $K[X_1, \cdots, X_n]$ sont des anneaux noethériens.

– – – – – – – – – – – – – – – – – –

2.1.9. Exercice. Montrer que tout élément non nul non inversible d'un domaine noethérien A est produit d'un nombre fini d'éléments irréductibles de A.

2.1.10. Exercice. On dit qu'un idéal $\mathfrak{A}$ d'un anneau A est **irréductible** si $\mathfrak{A}$ est un idéal propre de A et si $\mathfrak{A}$ n'est pas intersection de deux idéaux strictement plus grands que lui :

$$\mathfrak{A} \subsetneq A \quad \text{et} \quad \mathfrak{A} = \mathfrak{B} \cap \mathfrak{C} \Rightarrow \mathfrak{A} = \mathfrak{B} \text{ ou } \mathfrak{A} = \mathfrak{C}.$$

Montrer que dans un anneau noethérien tout idéal propre est intersection d'un nombre fini d'idéaux irréductibles.

2.2 Modules de type fini sur un domaine principal

Nous commencerons par regarder les modules libres de type fini ainsi que leurs sous-modules

2.2.1. Rappels et notations. Soit A un anneau et soit L un A-module libre de type fini et de rang n, de base $e = (e_1, e_2, \cdots, e_n)$. Tout élément w de L s'écrit donc de façon unique $w = a_1e_1 + a_2e_2 + \cdots + a_ne_n$, où les $a_i \in A$. Nous dirons que a_i est la $i^{\text{ième}}$ coordonnée de w dans la base e de L et nous utiliserons les « projections associées à la base e » définies par

$$p_i : M \to A : w = a_1e_1 + a_2e_2 + \cdots + a_ne_n \mapsto a_i.$$

Notons que les $p_i \in L^* := \mathrm{Hom}_A(L, A)$ ($p_i = e_i^*$ dans les notations de 0.8.5).

Notons encore que la fonction

$$A^n \to L : (a_1, \cdots, a_n) \mapsto a_1e_1 + a_2e_2 + \cdots + a_ne_n$$

est un isomorphisme de A-modules.

Remarque 2.2.2. Soit A un domaine et soit L un A-module libre. Soit encore $0 \neq w \in L$.

(i) La fonction $m_w : A \to L : a \mapsto aw$ est un homomorphisme injectif de A-modules, le sous-A-module Aw de L engendré par w est un A-module libre de rang 1, isomorphe à A en tant que A-module.

(En particulier, si $0 \neq a \in A$, l'idéal Aa de A est un A-module libre de rang 1.)

(ii) Il existe $f \in L^*$ tel que $f(w) \neq 0$.

(iii) Si w fait partie d'une base de L, il existe $f \in L^*$ tel que $f(w) = 1$.

(Pour cette dernière remarque (iii), il n'est pas nécessaire de supposer que A est un domaine.)

Voici une première information sur les sous-modules des modules libres.

Proposition 2.2.3. *Soit A un domaine principal, soit L un A-module libre de type fini et de rang n et soit M un sous-A-module de L.*

Alors M est libre de rang $m \leqslant n$.

Démonstration. Soit $e = (e_1, e_2, \cdots, e_n)$ une base de L et soit L_r le sous-A-module de L engendré par les éléments $e_1, e_2, \cdots, e_r$, $r \leqslant n$. Nous avons donc une chaîne de sous-modules libres de L

$$L_1 \subset \cdots \subset L_r \subset \cdots \subset L_n = L, \quad \mathrm{rang}(L_r) = r.$$

Soit encore

$$M_r = M \cap L_r.$$

Comme $M_1 \subset L_1 \simeq A$, M_1 est isomorphe à un idéal de A. Et comme A est un domaine principal, nous avons que M_1, s'il n'est pas nul, est un A-module libre de rang 1 (cf. 2.2.2).

Nous procédons ensuite par induction sur le rang de L. Soit donc $r < n$, supposons avoir déjà prouvé que le sous-module M_r de L_r est libre de rang $\leqslant r$ et montrons qu'alors M_{r+1} est libre de rang $\leqslant r+1$. Utilisons les projections p_i associées à la base e.

Notons que $p_{r+1}(M_{r+1})$ est un idéal de A, donc principal, disons $p_{r+1}(M_{r+1}) = a_{r+1}A$.

Si $a_{r+1} = 0$, alors $M_{r+1} = M_r$ est libre de rang $\leqslant r$.

Si $a_{r+1} \neq 0$, soit $w \in M_{r+1}$ tel que $p_{r+1}(w) = a_{r+1}$. Pour tout $x \in M_{r+1}$ nous avons $p_{r+1}(x) = ca_{r+1}$ pour un certain $c \in A$ et alors $p_{r+1}(x - cw) = 0$, ce qui implique $x - cw \in M_r$. Nous avons donc

$$M_{r+1} = Aw + M_r.$$

D'autre part il est clair que $Aw \cap M_r = \{0\}$ (on a même $Aw \cap L_r = \{0\}$).

Nous avons donc $M_{r+1} = Aw \oplus M_r$. Comme Aw est libre de rang 1, on en déduit que M_{r+1} est libre de rang $\leqslant r+1$. □

La proposition précédente reste valable si on y supprime l'hypothèse « type fini ». Sa preuve nécessite alors une induction transfinie, c.-à d. une induction sur les ordinaux et quelques rudiments de la théorie des ensemble.

Nous pouvons dire plus, dans la situation de 2.2.3 nous pouvons trouver une base du A-module libre L bien adaptée à son sous-module M.

Théorème 2.2.4. *Soit A un domaine principal et soit L un A-module libre de type fini et de rang n. Soit encore M un sous-A-module de L.*

Alors il existe une base $(u_1, u_2, \cdots, u_n)$ de L et des éléments non nuls de A : $a_1 \mid a_2 \mid \cdots \mid a_r$, $r \leqslant n$, tels que les éléments $a_1u_1, a_2u_2, \cdots, a_ru_r$ forment une base de M.

Démonstration. Si $M = \{0\}$ il n'y a rien à faire, supposons donc M non nul.

L'image de M par une forme linéaire $g \in L^*$ est un idéal de A, donc un idéal principal. L'ensemble d'idéaux $\mathfrak{I} = \{g(M) \mid g \in L^*\}$ est un ensemble non vide ordonné par inclusion, et il possède un maximal car tout anneau principal est noethérien. Soit alors $f_1 \in L^*$ tel que $f_1(M)$ est un maximal de $\mathfrak{I}$, soit $a_1 \in A$ tel que $f_1(M) = Aa_1$ et soit encore $w_1 \in M$ tel que $f_1(w_1) = a_1$. Notons que $a_1 \neq 0$ car M est non nul.

Montrons d'abord que, $\forall g \in L^*$, $g(w_1) \in Aa_1$. Pour cela, regardons $d \sim \mathrm{pgcd}(f_1(w_1), g(w_1))$. Comme A est un domaine principal, nous avons des éléments $s, t \in A$ tels que $d = sf_1(w_1) + tg(w_1)$. Mais $sf_1(w_1) + tg(w_1) = (sf_1 + tg)(w_1)$ et $(sf_1 + tg) \in L^*$. Les inclusions $Aa_1 \subset Ad \subset (sf_1 + tg)(M)$ nous donnent $Aa_1 = Ad$ par la maximalité de Aa_1 dans $\mathfrak{I}$, ce qui entraîne $g(w_1) \in Aa_1$.

Soit maintenant $e = (e_1, \cdots, e_n)$ une base quelconque de L et écrivons w_1 comme combinaison linéaire des e_i ; $w_1 = \sum_i b_i e_i$. Comme $b_i = p_i(w_1)$, où les p_i sont les projections associées à la base e de L, nous avons $b_i \in Aa_1$ et nous avons des éléments $c_i \in A$ tels que $b_i = a_1 c_i$.

Écrivons encore $u_1 = \sum_i c_i e_i$. Avec ces notations nous avons

$$w_1 = a_1 u_1, \quad a_1 = f_1(w_1) = a_1 f_1(u_1), \quad \text{d'où} \quad f_1(u_1) = 1.$$

Montrons maintenant que

$$L = Au_1 \oplus \ker(f_1) \quad \text{et} \quad M = Aw_1 \oplus (\ker(f_1) \cap M).$$

Pour tout $v \in L$ écrivons

$$v = f_1(v)u_1 + (v - f_1(v)u_1).$$

Comme $f_1(v - f_1(v)u_1) = f_1(v) - f_1(v)f_1(u_1) = 0$, nous obtenons $L = Au_1 + \ker(f)$. Si de plus $v \in M$ alors $f_1(v) \in f_1(M) = Aa_1$ et $f_1(v)u_1 \in Aa_1u_1 = Aw_1$. On a donc aussi $M = Aw_1 + (\ker(f_1) \cap M)$. Par ailleurs, si $v \in Au_1 \cap \ker(f_1)$, on a $v = au_1$ pour un certain $a \in A$ et alors $0 = f_1(v) = af_1(u_1) = a$, d'où $a = 0$ et $v = 0$. Ceci montre que nos sommes sont directes.

Continuons par induction sur le rang n de L. Si $n = 1$, $L \simeq A$ et notre théorème est évident. Supposons donc le théorème prouvé pour les A-modules libres de rang $n-1$. Comme le sous-A-module $L_2 := \ker(f_1)$ de L est un A-module libre (2.2.3) de rang $n-1$ (0.8.7), l'hypothèse d'induction appliquée à ce module libre L_2 et à son sous-module $M_2 := \ker(f_1) \cap M$ nous fournit une base $u_2, \cdots, u_r$ de L_2 et une suite d'éléments non nuls $a_2 \mid a_3 \mid \cdots \mid a_r$ de A telle que les éléments $a_2u_2, \cdots, a_ru_r$ forment une base de M_2.

Reste à prouver que $a_1 \mid a_2$. Prolongeons la forme linéaire $f_2 \in L_2^*$ utilisée pour trouver u_2 en une forme linéaire f_2' sur L en posant $f_2'(u_1) = 1$. Pour cette forme $f_2' \in L^*$ nous avons $f_2'(w_1) = f_2'(a_1u_1) = a_1$. Ainsi $f_2'(M) \supseteq Aa_1$. Mais l'idéal Aa_1 est maximal dans l'ensemble d'idéaux $\mathfrak{I}$ introduit en début de preuve. On a donc $f_2'(M) = Aa_1$ et aussi $a_2 \in Aa_1$, ce qui termine la preuve. □

Remarque 2.2.5. Dans la situation de 2.2.4 on peut aussi montrer l'unicité de la suite $a_1 \mid a_2 \mid \cdots \mid a_r$, à multiplication par des inversibles près.

Tout ceci nous donne une première information sur la structure des modules de type fini sur un domaine principal.

Corollaire 2.2.6. *Tout module de type fini sur un domaine principal A est isomorphe à un module de la forme*

$$\bigoplus_{i=1}^{r} (A/a_iA) \bigoplus A^m$$

où les a_i sont des éléments non nuls de A.

Démonstration. Dans la situation de 2.2.4 nous avons

$$L/M \simeq \bigoplus_{i=1}^{r}(A/a_iA) \bigoplus A^{n-r}.$$

Rappelons maintenant que tout module N de type fini peut se voir comme quotient d'un module libre de type fini : si $\{w_1, w_2, \cdots, w_n\}$ est une partie génératrice finie de N, l'homomorphisme

$$f : A^n \to N : (a_1, \cdots, a_n) \mapsto a_1w_1 + a_2w_2 + \cdots + a_nw_n$$

est surjectif et induit un isomorphisme $N \simeq A^n/\ker(f)$. On conclut en appliquant le théorème 2.2.4 au module libre A^n et à son sous-module $\ker(f)$. □

Dans le cas où le domaine principal A est l'anneau des entiers rationnels, nous obtenons encore une information bien utile.

Corollaire 2.2.7. *Soit M un $\mathbb{Z}$-module libre de type fini et soit $f : M \to M$ un endomorphisme injectif de M.*

Alors $\det(f) \neq 0$*, $M/f(M)$ est fini et* $\#(M/f(M)) = |\det(f)|$.

Démonstration. Comme f est injectif, $M \simeq f(M)$ et $f(M)$ est un sous-module libre de type fini de M, de même rang que M. Il existe donc une base $u = (u_1, \cdots, u_n)$ de M ($n = \text{rang}(M)$) et des entiers naturels non nuls $c_1, \cdots, c_n$ tels que les c_iu_i forment une base de $f(M)$. On en déduit :

$$M/f(M) \simeq \bigoplus_{i=1}^{n}\mathbb{Z}/c_i\mathbb{Z} \quad \text{et} \quad \#(M/f(M)) = c_1 \cdot c_2 \cdots c_n.$$

Par ailleurs les $f(u_1), \cdots, f(u_n)$ forment aussi une base de $f(M)$ et nous avons une matrice inversible $C \in \mathbb{Z}^{n\times n}$ telle que

$$(c_1u_1, \cdots, c_nu_n) = (f(u_1), \cdots, f(u_n)) \cdot C.$$

Soit maintenant F la matrice de f dans la base u :

$$(f(u_1), \cdots, f(u_n)) = (u_1, \cdots, u_n) \cdot F.$$

Il vient

$$(c_1u_1, \cdots, c_nu_n) = (u_1, \cdots, u_n) \cdot F \cdot C \quad \text{et} \quad \text{diag}(c_1, \cdots, c_n) = F \cdot C$$

où $\text{diag}(c_1, \cdots, c_n)$ désigne la matrice diagonale dont les entrées sur la diagonale principale sont $c_1, \cdots, c_n$. On conclut : $c_1 \cdots c_n = |\det(f)|$ car $\det(C) = \pm 1$, C étant une matrice inversible de $\mathbb{Z}^{n\times n}$. □

Voici quelques corollaires intéressants pour nos nombres.

Corollaires 2.2.8. *Soit A un anneau.*

(i) Si, en tant que $\mathbb{Z}$-module, A est un $\mathbb{Z}$-module de type fini, alors A est un anneau noethérien.

Plus précisément, si A, en tant que $\mathbb{Z}$-module, peut être engendré par n éléments, alors tout idéal de A peut aussi être engendré en tant qu'idéal par n éléments (non nécessairement distincts).

En particulier tout idéal de $\mathbb{Z}[\sqrt{d}]$ ou de l'anneau $\mathcal{O}_d$ des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}]$ peut être engendré par 1 ou 2 éléments.

(ii) Si de plus A est un domaine et si, en tant que $\mathbb{Z}$-module, A est un $\mathbb{Z}$-module libre de rang n, alors tout idéal non nul $\mathfrak{A}$ de A est aussi, en tant que $\mathbb{Z}$-module, un $\mathbb{Z}$-module libre de rang n.

Démonstration. (i) Soit $a_1, \cdots, a_n$ des éléments de A engendrant A en tant que $\mathbb{Z}$-module. Nous avons un homomorphisme surjectif de $\mathbb{Z}$-modules :

$$f : \mathbb{Z}^n \to A : (z_1, \cdots, z_n) \mapsto \sum_{i=1}^{n} z_i a_i.$$

Un idéal $\mathfrak{A}$ de l'anneau A est aussi un sous-$\mathbb{Z}$-module de A et $f^{-1}(\mathfrak{A})$ est un sous-$\mathbb{Z}$-module du $\mathbb{Z}$-module libre $\mathbb{Z}^n$. Le $\mathbb{Z}$-module $f^{-1}(\mathfrak{A})$ peut donc être engendré par $m \leqslant n$ éléments, 2.2.3 ou 2.2.4, et par conséquent $\mathfrak{A}$ peut aussi être engendré en tant que $\mathbb{Z}$-module, à fortiori en tant qu'idéal, par $m \leqslant n$ éléments.

(ii) Soit $0 \neq a \in \mathfrak{A}$. Nous avons un isomorphisme de A-modules $A \simeq aA$ et des inclusions $aA \subset \mathfrak{A} \subset A$. On conclut encore avec 2.2.3 ou 2.2.4 appliqués au $\mathbb{Z}$-module libre A et à son sous-$\mathbb{Z}$-module $\mathfrak{A}$, on a $\mathrm{rang}(A) = \mathrm{rang}(aA) \leqslant \mathrm{rang}(\mathfrak{A}) \leqslant \mathrm{rang}(A)$.

□

Retournons au cas général des modules de type fini M sur un domaine principal. Leur décomposition en somme directe obtenue en 2.2.6 va pouvoir se raffiner. La proposition suivante a sans doute été vue au premier cours d'algèbre dans le cas où $A = \mathbb{Z}$.

Proposition 2.2.9. *Soit A un domaine principal et b, c deux éléments non nuls de A premiers entre eux. L'homomorphisme naturel d'anneaux*

$$p : (A, +, \cdot) \to (A/bA, +, \cdot) \times (A/cA, +, \cdot) : x \mapsto (x + bA, x + cA)$$

est surjectif induit un isomorphisme d'anneaux

$$A/bcA, +, \cdot) \xrightarrow{\sim} (A/bA, +, \cdot) \times (A/cA, +, \cdot).$$

Démonstration. Nous avons $\ker(p) = bA \cap cA = \text{ppcm}(b,c)A = bcA$ car b et c sont premiers entre eux. Il nous suffit donc de montrer que p est surjectif. Comme b et c sont premiers entre eux nous avons deux éléments $s, t \in A$ tels que $1 = sb + tc$. Reste à observer que, $\forall x, y \in A$, $p(tcx + sby) = (x + bA, y + cA)$. □

Remarque 2.2.10. Dans la preuve ci-dessus et dans le cas où A est l'anneau $\mathbb{Z}$ des entiers naturels, on peut aussi montrer que l'homomorphisme naturel p ci-dessus est surjectif en utilisant un argument de finitude : comme p induit une injection de $\mathbb{Z}/bc\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$ et comme ces deux anneaux ont même nombre d'éléments, à savoir $|bc|$, cette injection est bijective.

Combinant 2.2.6 et 2.2.9 on obtient.

Corollaire 2.2.11. *Tout module de type fini sur un domaine principal A est somme directe d'un module libre de type fini et d'un nombre fini de modules cycliques de la forme A/p^rA, où p est un élément premier de A et où $r \in N_0$.*

En particulier tout groupe commutatif fini est somme directe d'un nombre fini de groupes cycliques de la forme $\mathbb{Z}/p^r\mathbb{Z}$, où p est un premier naturel et où $r \in N_0$.

On obtient aussi un petit résultat concernant les groupes commutatifs finis.

Corollaire 2.2.12. *Soit $(M, +)$ un groupe commutatif fini d'ordre n. Si p est un diviseur premier de n, alors M contient un élément d'ordre p.*

Démonstration. Au vu de 2.2.11 il suffit de remarquer que le groupe additif $(\mathbb{Z}/p^r\mathbb{Z}, +)$ $(r \geqslant 1)$ comprend un élément d'ordre p, à savoir $p^{r-1} + \mathbb{Z}$. □

Notons cependant que ce dernier corollaire n'est qu'une petite partie des théorèmes de Sylow, valables pour tout groupe fini, commutatif ou non.

Voici une dernière information, utile mais non indispensable. Avant de la formuler, rappelons que l'**annulateur** d'un A-module M est l'idéal $\text{Ann}_A(M) := \{a \in A \mid \forall w \in M, aw = 0\}$

Proposition 2.2.13. *Soit A un domaine principal et M un A-module tel que l'idéal $\text{Ann}_A(M)$ soit non nul. Soit a un générateur de cet idéal et soit encore $a = bc$ une factorisation de a, où b et c sont des éléments de A premiers entre eux. Écrivons*

$$M_{(b)} = \{w \in M \mid bw = 0\} \quad \text{et} \quad M_{(c)} = \{w \in M \mid cw = 0\}.$$

Alors

(i) $M_{(b)}$ et $M_{(c)}$ sont des sous-A-modules de M,

(ii) $M = M_{(b)} \oplus M_{(c)}$,

(iii) $\mathrm{Ann}_A(M_{(b)}) = bA \quad \text{et} \quad \mathrm{Ann}_A(M_{(c)}) = cA.$

Démonstration. (i) Ceci est assez clair : 0 est un élément de $M_{(b)}$ et de $M_{(c)}$ et, $\forall w_1, w_2 \in M, \forall x \in A$,
$(bw_1 = 0 \text{ et } bw_2 = 0) \Rightarrow (b(w_1 \pm w_2) = 0 \text{ et } b(xw_1) = xbw_1 = 0)$.

(ii) Comme b et c sont premiers entre eux nous pouvons écrire $1 = sb+tc$ pour certains $s, t \in A$.

Si $w \in M_{(b)} \cap M_{(c)}$ on a $w = 1w = (sb + tc)w = sbw + tcw = 0$, ce qui prouve $M_{(b)} \cap M_{(c)} = \{0\}$.

D'autre part, pour tout $w \in M$ on a $w = bsw + ctw$. Mais $c(bsw) = asw = 0$ et $b(ctw) = atw = 0$, donc $bsw \in M_{(c)}$ et $ctw \in M_{(b)}$. Ceci prouve que $M = M_{(b)} + M_{(c)}$.

Le tout ensemble donne $M = M_{(b)} \oplus M_{(c)}$.

(iii) Soit $b', c' \in A$ tels que

$$\mathrm{Ann}_A(M_{(b)}) = b'A \quad \text{et} \quad \mathrm{Ann}_A(M_{(c)}) = c'A.$$

Nous avons : $b \in b'A$ et $c \in c'A$, nous pouvons écrire

$$b = b'u_1 \quad c = c'u_2$$

où $u_1, u_2 \in A$.

Comme $M = M_1 + M_2$ nous avons aussi $b'c' \in \mathrm{Ann}_A(M) = aA$ et nous pouvons écrire

$$b'c' = au_3$$

où $u_3 \in A$. Il vient :

$$b'c' = au_3 = bcu_3 = b'c'u_1u_2u_3 \quad \text{et} \quad u_1u_2u_3 = 1$$

car $b'c' \neq 0$. On en déduit que u_1, u_2, u_3 sont inversibles dans A et que $bA = b'A$, $cA = c'A$. □

On pourrait en dire davantage concernant les modules de type fini sur un domaine principal, mais ce qui précède suffira amplement à nos besoins.

– – – – – – – – – – – – – – – – –

2.2.14. Exercice. Soit $L = \mathbb{Z}^2$ et soit M le sous-$\mathbb{Z}$-module de L engendré par $v_1 = (2, 4)$ et $v_2 = (2, 10)$.

Remarquer : $\forall f \in L^*$, $f(M) \subset 2\mathbb{Z}$ et $p_1(v_1) = 2$ (notation comme en 2.2.1).

Déterminer comme en 2.2.4 une base $u = (u_1, u_2)$ du $\mathbb{Z}$-module L et des entiers $a_1, a_2 \in \mathbb{Z}$ tels que (a_1u_1, a_2u_2) soit une base du $\mathbb{Z}$-module M.

Identifier le $\mathbb{Z}$-module quotient L/M.

2.2.15. Exercice. Soit A un anneau et supposons qu'il aie la propriété suivante :« tout sommant direct d'un A-module libre de type fini est libre de type fini » (c'est le cas pour les domaines principaux en vertu de 2.2.3).

Soit alors L un A-module libre de rang n, de base $(e_1, \cdots, e_n)$ et soit $v = \sum_i a_i e_i \in L$. Les conditions suivantes sont équivalentes :

(i) v fait partie d'une base de L,

(ii) $\exists f \in L^*$ tel que $f(v) = 1$,

(iii) $Aa_1 + \cdots Aa_n = A$.

2.2.16. Exercice. L'anneau $\mathbb{Z}_6$ est somme directe de ses deux idéaux $(2) \simeq \mathbb{Z}_3$ et $(3) \simeq \mathbb{Z}_2$, mais ces idéaux ne sont pas des $\mathbb{Z}_6$-modules libres. Noter que $\mathbb{Z}_6$ est un anneau principal mais non un domaine principal.

2.3 Compléments sur les domaines factoriels

Ces compléments nous permettrons de montrer que le polynôme minimal d'un entier algébrique quelconque a tous ses coefficients dans $\mathbb{Z}$ (fait que nous savions déjà pour les entiers d'un corps quadratique).

Par ailleurs, les polynômes irréductibles jouent un grand rôle dans la théorie des nombres. Le polynôme minimal sur $\mathbb{Q}$ d'un nombre algébrique est irréductible dans $\mathbb{Q}[X]$ et réciproquement tout polynôme irréductible de $\mathbb{Q}[X]$ est le polynôme minimal sur $\mathbb{Q}$ d'une quelconque de ses racines complexes. Avoir un critère d'irréductibilité sera donc utile.

Rappelons que des éléments $a_1, a_2, \cdots, a_n$ d'un domaine factoriel A ont un plus grand commun diviseur (pgcd). Certes, ce pgcd n'est défini qu'à multiplication près par un inversible de A. Néanmoins nous pouvons choisir une fois pour toute un pgcd pour n'importe quelle famille finie d'éléments de A, ce que nous ferons avec l'axiome du choix.

Définition 2.3.1. Soit A un domaine factoriel.

Le **contenu** d'un polynôme non nul

$$F = a_n X^n + a_{n-1} X^{n-1} + \cdots a_1 X + a_0 \in A[X]$$

est défini par

$$\mathrm{cont}(F) = \mathrm{pgcd}(a_1, a_2, \cdots, a_n).$$

Un polynôme **primitif** est un polynôme non constant $F \in A[X]$ tel que $\mathrm{cont}(F) \sim 1$.

Voici un leme essentiel

Lemme 2.3.2. *(Lemme de Gauss). Soit A un domaine factoriel.*
Le produit de deux polynômes primitifs de $A[X]$ est primitif.
Plus généralement : $\forall F, G \in A[X], \quad \mathrm{cont}(FG) \sim \mathrm{cont}(F)\mathrm{cont}(G)$.

Démonstration. Soit $F = f_s X^s + \cdots + f_1 X + f_0$ et $G = g_r X^r + \cdots + g_1 X + g_0$ deux polynômes primitifs de $A[X]$ et soit p un élément premier quelconque de A. Il nous faut montrer que p ne divise pas tous les coefficients du produit FG. Comme F et G sont primitifs, cet élément p ne divise pas tous les coefficients de F, ni tous ceux de G. Soit alors

$$i = \mathrm{minimum}\{k \in \mathbb{N} \mid p \nmid f_k\} \quad \text{et} \quad j = \mathrm{minimum}\{k \in \mathbb{N} \mid p \nmid g_k\}$$

et regardons le coefficient du terme de degré $i + j$ du produit FG. Ce coefficient est une somme

$$\cdots + f_{i-1} g_{j+1} + f_i g_j + f_{i+1} g_{j-1} + \cdots \quad .$$

Nous remarquons que p divise tous les termes de cette somme sauf un, à savoir le terme $f_i g_j$. Donc p ne divise pas cette somme. Ceci termine la preuve de la première assertion. Notons que la seconde est une conséquence assez directe de la première et des propriétés des pgcd. □

Proposition 2.3.3. *Soit A un domaine factoriel de corps des fractions K et soit $F \in A[X]$ un polynôme primitif.*

(i) Supposons que $F = P_1 \cdot P_2$, où $P_1, P_2 \in K[X]$.

Alors il existe un élément non nul $k \in K$ tels que kP_1 et $k^{-1}P_2$ soient deux polynômes primitifs de $A[X]$.

(ii) F est irréductible dans $A[X] \Leftrightarrow F$ est irréductible dans $K[X]$.

Démonstration. (i) Prenons dans A un multiple commun non nul c_1 des dénominateurs des coefficients de P_1 et un multiple commun non nul c_2 des dénominateurs des coefficients de P_2, de sorte que $c_1P_1, c_2P_2 \in A[X]$. Nous obtenons dans $A[X]$ et A :

$$c_1c_2F = (c_1P_1)(c_2P_2) \quad c_1c_2 = \mathrm{cont}(c_1P_1) \cdot \mathrm{cont}(c_2P_2) \quad \text{et}$$

$$F = \frac{c_1P_1}{\mathrm{cont}(c_1P_1)} \cdot \frac{c_2P_2}{\mathrm{cont}(c_2P_2)}.$$

Le nombre $k = \frac{c_1}{\mathrm{cont}(c_1P_1)}$ fait l'affaire.

Pour terminer, de $\mathrm{cont}(kP_1)\mathrm{cont}(k^{-1}P_2) \sim \mathrm{cont}(F) \sim 1$ on déduit $\mathrm{cont}(kP_1) \sim 1 \sim \mathrm{cont}(k^{-1}P_2)$.

(ii) découle de (i).

□

Avec cette dernière proposition et un peu de réflexion on obtient le résultat suivant.

Théorème 2.3.4. *Soit A un domaine factoriel de corps de fractions K.*

Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.

L'anneau $A[X]$ est un domaine factoriel.

Application aux entiers algébriques.

Nous savions déjà que le polynôme minimal d'un entier d'un corps quadratique appartient à $\mathbb{Z}[X]$.

Avec 2.3.3 on voit que ceci reste vrai pour les entiers d'un corps de nombres quelconque.

Corollaire 2.3.5. *Soit K un corps de nombre et soit $\alpha \in K$ un nombre entier sur $\mathbb{Z}$.*

Alors le polynôme minimal $P := Min_{\mathbb{Q},\alpha}$ de α sur $\mathbb{Q}$ appartient à $\mathbb{Z}[X]$.

De plus, l'anneau $\mathbb{Z}[\alpha]$ est un $\mathbb{Z}$-module libre de rang $n = [\mathbb{Q}[\alpha] : \mathbb{Q}]$.

Démonstration. Soit F un polynôme unitaire de $\mathbb{Z}[X]$ s'annulant en α. Comme P engendre l'idéal des polynômes de $\mathbb{Q}[X]$ s'annulant en α, on a un polynôme $T \in \mathbb{Q}[X]$ tel que $F = PT$. Avec 2.3.3 appliqué à l'anneau $\mathbb{Z}$ on obtient un nombre rationnel non nul k tel que $kP, k^{-1}T \in \mathbb{Z}[X]$. Soit a (respectivement b) le coefficient du terme de dégré le plus élevé de kP (respectivement de $k^{-1}T$). Par construction ces nombres $a, b \in \mathbb{Z}$ et, comme F est unitaire, on obtient $ab = 1$ d'où $a = \pm 1$. Comme P est aussi unitaire il vient $k = a = \pm 1$ et $P = \pm kP \in \mathbb{Z}[X]$.

Puisque le polynôme minimal P de α sur $\mathbb{Z}$ est un polynôme unitaire à coefficients entiers, disons de degré n, on a que les nombres $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ forment non seulement une base du $\mathbb{Q}$-vectoriel $\mathbb{Q}[\alpha]$, mais aussi une base du $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$. □

Un critère d'irréductibilité.

Proposition 2.3.6. *(Critère d'Eisenstein). Soit A un domaine factoriel de corps de fractions K et soit $F \in A[X]$ un polynôme de degré positif, $F = a_n X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0, n \geqslant 1, a_n \neq 0$.*

S'il existe un élément premier p de A tel que

$$p \nmid a_n, \quad p \mid a_i \text{ pour } 0 \leqslant i < n, \quad p^2 \nmid a_0$$

alors F est irréductible dans $K[X]$.

Démonstration. Écrivons $a_i = a_i' \mathrm{cont}(F)$ et notons qu'un élément $p \in A$ comme dans l'énoncé ne divise pas $\mathrm{cont}(F)$. Un tel élément p divise donc les éléments a_i' pour $0 \leqslant i < n$ et $p^2 \nmid a_0'$. Quitte à diviser F par son contenu, nous pouvons donc supposer et nous supposons que F est primitif dans $A[X]$.

Dès lors, procédons par l'absurde. Supposons que F n'est pas irréductible dans $K[X]$. Alors F n'est pas non plus irréductible dans $A[X]$ (cf. 2.3.3) et nous avons $F = GH$, où G et H sont des polynômes de degré positifs de $A[X]$.

Écrivons

$$G = g_r X^r + \cdots + g_1 X + g_0, \quad H = h_s X^s + \cdots + h_1 X + h_0,$$

où $g_r \neq 0, \quad h_s \neq 0, \quad r + s = n, \quad r, s \geqslant 1$.

Nous avons $a_0 = g_0 h_0$. Comme a_0 est divisible par p et non par p^2, p divise un et un seul des deux facteurs g_0, h_0 de a_0, disons $p \mid g_0, p \nmid h_0$.

Nous allons montrer par induction que $p \mid g_i$ pour tout $i, 0 \leqslant i \leqslant r$, ce qui amènera une contradiction puisque $a_n = g_r h_s$ n'est pas divisible par p.

Supposons que nous ayons déjà démontré que $p \mid g_0, \cdots g_{k-1}$, où $k \leqslant r$, et montrons qu'alors $p \mid g_k$. Nous avons $a_k = g_k h_0 + g_{k-1} h_1 + \cdots \cong g_k h_0$ modulo p, et , comme $k < n$, nous avons par hypothèse que $p \mid a_k$. Nous avons donc aussi $p \mid g_k h_0$ et, comme $p \nmid h_0$, on en déduit $p \mid g_k$. □

Exemples 2.3.7. Les polynômes $10X^7 - 12X^4 + 3$ et $X^{15} - 6$ sont irréductibles dans $\mathbb{Q}[X]$.

Si $d \neq 0, \pm 1$ est un entier rationnel sans facteurs carrés, le polynôme $X^n - d$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \geqslant 1$.

(Remarquer que pour n=2 on retrouve $\sqrt{d} \notin \mathbb{Q}$).

Exemple 2.3.8. Montrons que, pour tout premier naturel p, le polynôme

$$F = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots X + 1$$

est irréductible dans $\mathbb{Q}[X]$.

Ici, le critère d'Eisenstein ne s'applique pas directement, mais il nous suffit de montrer que $F(Y+1)$ est irréductible.

$$F(Y+1) = \frac{(Y+1)^p - 1}{Y} = \frac{Y^p + pY^{p-1} + \cdots + \binom{p}{i} Y^{p-i} + \cdots + pY}{Y}$$

$$= Y^{p-1} + pY^{p-2} + \cdots + \binom{p}{i} Y^{p-i-1} + \cdots + p.$$

Nous rappelons que les coefficients binomiaux $\binom{p}{i}$ sont divisibles par p pour $1 \leqslant i \leqslant p-1$ et nous concluons avec le critère d'Eisenstein que $F(Y+1)$ et $F(X)$ sont irréductibles dans $\mathbb{Q}[X]$.

Application. Comme le polynôme $X^{p-1} + X^{p-2} + \cdots X + 1$ est irréductible dans $\mathbb{Q}[X]$ et s'annule en $e^{\frac{2\pi i}{p}}$, il est le polynôme minimal sur $\mathbb{Q}$ de $e^{\frac{2\pi i}{p}}$ et $[\mathbb{Q}[e^{\frac{2\pi i}{p}}] : \mathbb{Q}] = p - 1$.

Les corps de nombres de la forme $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$, où $n \in \mathbb{N}_0$, ont leur rôle à jouer et méritent un nom, ils sont appelés « *corps cyclotomiques* ».

Rappelons le rôle joué par le corps cyclotomique $\mathbb{Q}[e^{\frac{2\pi i}{3}}]$ dans l'équation de Fermat $X^3 + Y^3 = Z^3$.

– – – – – – – – – – – – – – – – – –

2.3.9. Exercice*. Soit k un corps, t une indéterminée et soit $A = k[t]$. Soit encore $K = k(t)$ le corps des fractions de A.

Pour tout $n \geqslant 1$, le polynôme

$$X^n - t$$

est irréductible dans $K[X]$.

(Noter que t est un élément premier du domaine factoriel A.)

2.3.10. Exercice. Soit X et Y deux indéterminées et $c \in \mathbb{R}$, $c \neq 0, 1$.

Le polynôme

$$F = Y^2 - X(X-1)(X-c)$$

est irréductible dans $\mathbb{C}[X, Y]$.

(Noter que X, $X-1$ et $X-c$ sont des éléments premiers du domaine factoriel $\mathbb{C}[X]$, non associés deux-à-deux.)

Le polynôme $Y^2 - X^3$ est aussi irréductible dans $\mathbb{C}[X, Y]$.

(Il suffit de remarquer que X^3 n'est pas un carré dans le corps des fractions $\mathbb{C}(X)$ de $\mathbb{C}[X]$.)

2.4 Normes, Traces et Ordres

Définitions 2.4.1. Soit A un sous-anneau de l'anneau B et supposons que B est un A-module libre de type fini. La multiplication par un élément $x \in B$ fournit un endomorphisme

$$x\cdot : B \to B : z \mapsto xz$$

du A-module B dont nous pouvons prendre la trace, le déterminant et le polynôme caractéristique (0.8.4).

On définit alors la **trace**, la **norme** et le **polynôme caractéristique** de l' élément $x \in B$ relativement à l'inclusion $A \subset B$ par

$$\mathrm{Tr}_{B/A}(x) = \mathrm{Tr}(x\cdot), \quad N_{B/A}(f) = \det(x\cdot), \quad \mathrm{Char}_{B/A,x} = \mathrm{Char}_{(x\cdot)},$$

Propriétés 2.4.2. (i) La fonction

$$\mathrm{Tr}_{B/A} : B \to A : x \mapsto \mathrm{Tr}_{B/A}(x)$$

est une application A-linéaire, c.à-d. un homomorphisme de A-modules.

(ii) La fonction

$$N_{B/A} : B \to A : x \mapsto N_{B/A}(x)$$

est multiplicative : $\forall x, y \in B, \quad N_{B/A}(xy) = N_{B/A}(x)N_{B/A}(y)$.

(iii) $\forall c \in A, \qquad \mathrm{Tr}_{B/A}(c) = nc \quad$ et $\quad N_{B/A}(c) = c^n$
où n est le rang du A-module libre B.

(iv) $\mathrm{Char}_{B/A,x}$ est un polynôme unitaire de $A[X]$.

De plus, on remarque avec 0.8.4 que

$$\text{si} \quad \mathrm{Char}_{B/A,x} = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

$$\text{alors} \quad \mathrm{Tr}_{B/A}(x) = -a_{n-1} \quad \text{et} \quad N_{B/A}(x) = (-1)^n a_0.$$

(v) En conséquence du théorème de Cayley-Hamilton ou de 1.2.14 on a

$$\mathrm{Char}_{B/A,x}(x) = 0.$$

(vi) Si $A = K$ et $B = L$ sont des corps, on a aussi

$$N_{L/K}(x) = 0 \Leftrightarrow x = 0.$$

Insistons sur le fait que les normes, traces et polynômes caractéristiques introduits ci-dessus dépendent effectivement de l'inclusion $A \subset B$. Ceci est déjà clair avec la remarque en (2.4.2, (iii)) que nous pouvons généraliser.

Proposition 2.4.3. *Soit $A \subset B \subset C$ trois anneaux tels que B soit un A-module libre de rang n_1 et C un B-module libre de rang n_2.*

Alors, $\forall b \in B$ nous avons :

$$Char_{C/A,b} = (Char_{B/A,b})^{n_2} \quad N_{C/A}(b) = (N_{B/A}(b))^{n_2} \quad T_{C/A}(b) = n_2(T_{B/A}(b)).$$

Démonstration. Soient $(e_1, \cdots, e_{n_1})$ une base du A-module libre B et $(u_1, \cdots, u_{n_2})$ une base du B-moule libre C. Les $u_i e_j$ forment alors une base de C en tant que A-module (1.2.8), numérotons-les dans l'ordre lexicographique $((u_1e_1, u_1e_2, \cdots, u_1e_{n_1}, u_2e_1, \cdots))$et regardons la matrice de la transformation $(b\cdot)$ de C dans cette base ainsi numérotée. Nous obtenons une matrice de la forme

$$F = \begin{pmatrix} G & 0 & 0 & \cdots & 0 \\ 0 & G & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & G \end{pmatrix},$$

où G désigne la matrice de la transformation $(b\cdot)$ du A-module libre B dans sa base $(e_1, \cdots, e_{n_1})$.

Prenons les traces et déterminants, on obtient : $\mathrm{Tr}(F) = n_2\mathrm{Tr}(G)$, $\det(F) = \det(G)^{n_2}$ et $\det(XI_{n_1n_2} - F) = \det(XI_{n_1} - G)^{n_2}$, ce qui termine la preuve □

Nous appliquons ceci aux extensions finies de corps. Si L est une extension finie du corps K, nous obtenons une relation entre le polynôme caractéristique $\mathrm{Char}_{L/K,x}$ d'un élément quelconque $x \in L$ et son polynôme minimal $\mathrm{Min}_{K,x}$ sur K

Corollaire 2.4.4. *Soit L une extension finie du corps K, $\forall x \in L$ on a :*

$$Char_{L/K,x} = (Min_{K,x})^m,$$

où $m = [L : K[x]]$.

Démonstration. Il suffit d' appliquer 2.4.3 aux inclusions $K \subset K[x] \subset L$, en remarquant que degré$(\mathrm{Char}_{K[x]/K,x}) = [K[x] : K] =$ degré$(\mathrm{Min}_{K,x})$ et que, comme $\mathrm{Char}_{K[x]/K,x}$ est un polynôme unitaire s'annulant en x, il est égal à $\mathrm{Min}_{K,x}$. □

Ceci donne aussi des informations sur les entiers d'un corps de nombres. En combinant 2.4.4 avec 2.3.5 et 2.4.2 on obtient.

Corollaire 2.4.5. *Soit K un corps de nombres. Si le nombre α de K est entier sur $\mathbb{Z}$, alors*

$$\mathrm{Min}_{\mathbb{Q},\alpha} \text{ et } \mathrm{Char}_{K/\mathbb{Q},\alpha} \in Z[X] \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \text{ et } N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}.$$

2.4.6. Avant de continuer, il convient de remarquer que, dans le cas des corps quadratiques, extensions de Q de degré 2, les traces et normes définies ici coïncident avec les traces et normes définies au premier chapitre. En effet, soit $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ un élément du corps quadratique $\mathbb{Q}[\sqrt{d}]$, où $d \neq 0, 1$ est un entier rationnel sans facteur carré. La matrice de la transformation $\alpha\cdot$ de $\mathbb{Q}[\sqrt{d}]$ dans la base $(1, \sqrt{d})$ de $\mathbb{Q}[\sqrt{d}]$ sur $\mathbb{Q}$ est la matrice $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$. On a donc

$$\mathrm{Tr}_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(\alpha) = 2a \quad \text{et} \quad N_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(\alpha) = a^2 - db^2.$$

Dans le cas d'un corps de nombres quelconque, c.à-d. d'une extension finie K de $\mathbb{Q}$, ce qui précède nous donne la définition des normes $N_{K/\mathbb{Q}}$ et traces $\mathrm{Tr}_{K/\mathbb{Q}}$.

Mais il conviendra aussi de restreindre ces normes et traces à des sous-anneaux convenables de K.

Définition 2.4.7. Soit K un corps de nombres, $[K : \mathbb{Q}] = n$.

Un **ordre** de K est un sous-anneau $\mathcal{O}$ de K qui, en tant que $\mathbb{Z}$-module, est un $\mathbb{Z}$-module libre de type fini et de rang $n = [K : \mathbb{Q}]$.

Exemple 2.4.8. (i) Soit $d \neq 0, 1$ un entier rationnel sans facteur carré. Les anneaux $\mathbb{Z}[\sqrt{d}]$, $\mathcal{O}_d$ et $\mathbb{Z}[c\sqrt{d}]$ $(0 \neq c \in \mathbb{Z})$ sont des ordres du corps quadratique $\mathbb{Q}[\sqrt{d}]$.

(ii) Plus généralement soit α un nombre algébrique entier sur $\mathbb{Z}$, autrement dit un entier algébrique. Alors l'anneau $\mathbb{Z}[\alpha]$ est un ordre du corps de nombres $\mathbb{Q}[\alpha]$, cf. 2.3.5.

2.4.9. Premières propriétés des ordres. Soit $\mathcal{O}$ un ordre du corps de nombres K. On a :

(i) $\mathcal{O}$ est entier sur $\mathbb{Z}$ (1.2.14) : $\mathcal{O}$ est un sous-anneau de l'anneau des entiers $\mathcal{O}_K$ de K.

(Nous verrons plus tard que $\mathcal{O}_K$ est lui-même un ordre de K, donc est l'ordre maximum de K.)

De plus, tout idéal de $\mathcal{O}$ peut être engendré par $n = [K : \mathbb{Q}]$ éléments (2.2.8), $\mathcal{O}$ est un anneau noethérien.

(ii) Comme des éléments de K linéairement indépendants sur $\mathbb{Z}$ sont aussi linéairement indépendants sur $\mathbb{Q}$, toute base de $\mathcal{O}$ en tant que $\mathbb{Z}$-module est aussi une base de K en tant que $\mathbb{Q}$-vectoriel et, $\forall \alpha \in K, \exists c \in \mathbb{Q}, c \neq 0$ tel que $c\alpha \in \mathcal{O}$. En particulier K est le corps des fractions de $\mathcal{O}$.

(iii) Au vu de (ii), nous pouvons utiliser une base du $\mathbb{Z}$-module libre $\mathcal{O}$ pour calculer nos normes, traces et polynômes caractéristiques : si $\alpha \in \mathcal{O}$, la matrice représentant l'endomorphisme $\alpha\cdot$ du $\mathbb{Q}$-vectoriel K dans une telle base aura ses entrées dans $\mathbb{Z}$ ($\alpha \cdot \mathcal{O} \subset \mathcal{O}$ car $\mathcal{O}$ est un anneau). On retrouve un fait déjà remarqué en 2.4.5 :

$$\forall \alpha \in \mathcal{O} \qquad N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \qquad \mathrm{Char}_{K/\mathbb{Q},\alpha} \in \mathbb{Z}[X].$$

Ceci a des conséquences intéressantes.

Proposition 2.4.10. *Soit $\mathcal{O}$ un ordre du corps de nombres K et soit $\alpha \in \mathcal{O}$. Alors :*

$$\alpha \in \mathcal{O}^\times \quad \Leftrightarrow \quad N_{K/\mathbb{Q}}(\alpha) = \pm 1.$$

Démonstration. $\Rightarrow$ Soit $\beta \in \mathcal{O}$ tel que $\alpha\beta = 1$. Alors $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = 1$ et, comme cette égalité a lieu dans $\mathbb{Z}$, on en déduit $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

$\Leftarrow$ Si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ le polynôme caractéristique de α est de la forme $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X \pm 1$, où les $a_i \in \mathbb{Z}$, (2.4.2(iv) et 2.4.5), et, comme il s'annule en alpha (2.4.2(v)), on obtient : $\alpha^{-1} = \pm(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) \in \mathcal{O}$. □

Théorème 2.4.11. *Soit $\mathcal{O}$ un ordre du corps de nombres K.*

(i) Tout quotient de $\mathcal{O}$ par un idéal non nul est un anneau fini.

(ii) Pour tout $\alpha \in \mathcal{O}$, $\alpha \neq 0$, on a :

$$|N_{K/\mathbb{Q}}(\alpha)| = \#(\mathcal{O}/\alpha\mathcal{O}).$$

Démonstration. (i) est une conséquence directe de (ii) car tout idéal non nul comprend un élément non nul !

Et (ii) est un cas particulier de 2.2.7. En effet, par définition de la norme nous avons $N_{K/\mathbb{Q}}(\alpha) = \det(\alpha\cdot)$ et, comme $0 \neq \alpha \in \mathcal{O}$, $\alpha\cdot$ est un endomorphisme injectif du $\mathbb{Z}$-module libre $\mathcal{O}$. □

Ceci nous amène à étendre la notion de normes aux idéaux (l'idée étant de remplacer l'étude des nombres par celle des idéaux).

Définition 2.4.12. La norme d'un idéal non nul $\mathfrak{A}$ d'un ordre $\mathcal{O}$ d'un corps de nombres K est définie par $N(\mathfrak{A}) = \#(\mathcal{O}/\mathfrak{A})$, $N(\mathfrak{A}) \in \mathbb{N}$.

Pour un idéal principal de $\mathcal{O}$ on a donc $N(\alpha\mathcal{O}) = |N_{K/\mathbb{Q}}(\alpha)|$.

Lemme 2.4.13. *Soit $\mathfrak{A}$ un idéal non nul d'un ordre $\mathcal{O}$ d'un corps de nombres K.*

Alors l'entier naturel $N(\mathfrak{A}) \in \mathfrak{A}$.

Démonstration. Soit $n = N(\mathfrak{A})$ et désignons par $\overline{(\cdot)}$ les images modulo $\mathfrak{A}$. Comme le groupe additif $(\overline{\mathcal{O}}, +) = (\mathcal{O}/\mathfrak{A}, +)$ est un groupe fini de n éléments, l'ordre de chacun de ses éléments divise n. En particulier on a : $n \cdot \bar{1} = \bar{0}$, autrement dit $n = n \cdot 1 \in \mathfrak{A}$. □

Voici un premier résultat de finitude (généralisant 1.6.9).

Proposition 2.4.14. *Soit $\mathcal{O}$ un ordre du corps de nombres K et soit $q \in \mathbb{N}_0$.*
L'ensemble des idéaux non nuls de $\mathcal{O}$ de norme q est fini.

Démonstration. Si $\mathfrak{A}$ est un idéal de $\mathcal{O}$ de norme q on a $q \in \mathfrak{A}$ (2.4.13). Comme $\mathcal{O}/q\mathcal{O}$ est un anneau fini (de q^n éléments si $n = [K : \mathbb{Q}]$), il n'a qu'un nombre fini d'idéaux. Mais les idéaux de $\mathcal{O}/q\mathcal{O}$ sont en bijection avec les idéaux de $\mathcal{O}$ contenant $q\mathcal{O}$, ces derniers sont donc en nombre fini. À fortiori les idéaux de $\mathcal{O}$ de norme q sont aussi en nombre fini. □

Reste à montrer que l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres est un ordre de K et donc le plus grand ordre de K.

Nous utiliserons la trace, qui va nous fournir une forme bilinéaire bien utile. D'abord quelques rappels.

2.4.15. Rappels d'algèbre bilinéaire.
Soit A un anneau et M un A-module.

(i) Une **forme A-bilinéaire** b sur M est une fonction

$$b : M \times M \to A : (v, w) \mapsto b(v, w)$$

telle que, pour tout $v, w \in M$, les fonctions

$$b(v, \cdot) : M \to A : w \mapsto b(v, w) \quad \text{et} \quad b(\cdot, w) : M \to A : v \mapsto b(v, w)$$

soient des formes A-linéaires sur M.

Cette forme est dite **symétrique** si, pour tout $v, w \in M$,

$$b(v, w) = b(w, v).$$

(ii) Supposons maintenant que M soit un A-module libre de type fini et soit $e = (e_1, \cdots, e_n)$ une base de M. Une forme bilinéaire b sur M est alors entièrement déterminée par les éléments $b_{ij} = b(e_i, e_j)$ de A. Ces b_{ij} sont les entrées d'une matrice $B_e \in A^{n\times n}$ appelée *matrice de la forme A-bilinéaire b dans la base e.*

Écrivons maintenant nos coefficients à droite comme en 0.8.4. Si $v = \sum e_i v_i$ et $w = \sum e_i w_i$ sont deux éléments de M nous avons :

$$b(v, w) = \sum_{i,j} v_i b_{ij} w_j = (v_1, \cdots, v_n) \cdot B_e \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

(iii) Si u est une autre base de M : $u_j = \sum_k e_k c_{kj}$, les c_{kj} sont les entrées d'une matrice inversible $C_{u(e)} \in A^{n\times n}$ et la matrice B_u de la forme b dans la base u est liée à la matrice B_e par

$$B_u = C_{u(e)}^t B_e C_{u(e)}$$

où $C_{u(e)}^t$ désignée la transposée de la matrice $C_{u(e)}$.

Il s'en suit que $\det(B_u) = \det(B_e)c^2$ où $c = \det(C_{u(e)}) \in A^\times$. L'idéal de A engendré par $\det(B_u)$ ne dépend donc que de la forme bilinéaire b et pas de la base choisie la représenter par une matrice.

On définit alors le **discriminant** de la forme b comme étant l'idéal de A engendré par $\det(B_e)$. Notons que, dans le cas où $A = \mathbb{Z}$, le nombre $\det(B_e)$ est lui aussi indépendant de la base choisie pour représenter la forme bilinéaire b par une matrice.

(iv) Supposons maintenant que $A = K$ est un corps et que $M = V$ est un espace vectoriel de dimension finie sur K, de base $e = (e_1, \cdots, e_n)$,

Une forme K-bilinéaire b sur V est dite **non dégénérée** ou **régulière** si

$$\forall v \in V, v \neq 0 \quad \exists w \in V \quad \text{ tel que } \quad b(v,w) \neq 0,$$

autrement dit si l'application linéaire

$$K^{1\times n} \to K^{1\times n} : v \mapsto vB_e$$

est injective.

Une forme K-bilinéaire b sur V est donc régulière si et seulement si la matrice B_e est inversible, autrement dit si $\det(B_e) \neq 0$. Dans ce cas $u = e \cdot B_e^{-1}$ est une autre base de V satisfaisant $b(e_i, u_j) = \delta_{ij}$ (si $u_j = \sum_k e_k c_{kj}, b(e_i, u_j) = \sum_k b_{ik} c_{kj}$). Une telle base u satisfaisant $b(e_i, u_j) = \delta_{ij}$ est unique et sera appelée « **base duale de la base e relativement à la forme b** ».

Proposition 2.4.16. *Soit K un corps de nombre de degré n sur $\mathbb{Q}$. La fonction*

$$T : K \times K \to \mathbb{Q} : (x,y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

est une forme $\mathbb{Q}$-bilinéaire symétrique et régulière, naturellement appelée **forme trace** *sur K.*

Démonstration. La bilinéarité et la symétrie de T découlent des propriétés de la trace.

Pour voir que T est régulière il suffit de remarquer que, si $0 \neq x \in K$, on a $T(x, x^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = n \neq 0$. □

Théorème 2.4.17. *Soit K un corps de nombre de degré n sur $\mathbb{Q}$.*

Alors l'anneau $\mathcal{O}_K$ des entiers de K est un ordre de K, autrement dit $\mathcal{O}_K$, en tant que $\mathbb{Z}$-module, est un $\mathbb{Z}$-module libre de type fini et de rang n.

Démonstration. Avec (1.2.25,c) nous savons déjà que que $\mathcal{O}_K$ contient une base $e = (e_1, \cdots, e_n)$ de K sur $\mathbb{Q}$. Soit maintenant u la base duale de cette base relativement à la forme T, la base u telle que $\mathrm{Tr}_{K/\mathbb{Q}}(e_i u_j) = \delta_{ij}$. Au vu de 2.2.3 il suffit de montrer que $\mathcal{O}_K$ est contenu dans le sous-$\mathbb{Z}$ module M de K engendré par les u_i. Soit donc z un élément quelconque de $\mathcal{O}_K$. Nous avons $e_i z \in \mathcal{O}_K$ et donc $\mathrm{Tr}_{K/\mathbb{Q}}(e_i z) \in \mathbb{Z}$, 2.4.5.

Par ailleurs z s'écrit $z = c_1 u_1 + c_2 u_2 + \cdots + c_n u_n$, où les $c_i \in \mathbb{Q}$ et nous avons aussi $\mathrm{Tr}_{K/\mathbb{Q}}(e_i z) = T(e_i, z) = \sum_k c_k T(e_i, u_k) = \sum_k c_k \delta_{ik} = c_i$. Donc les $c_i \in \mathbb{Z}$ et $\mathcal{O}_K \subset M$. □

Joignant ceci à 2.4.9 on obtient.

Corollaire 2.4.18. *L'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres K est noethérien.*

Si $[K : \mathbb{Q}] = n$ les idéaux de $\mathcal{O}_K$ peuvent être engendrés par n éléments.

2.4.19. Le théorème précédent et les remarques en 2.4.15 nous permettent de définir le **discriminant** d'un corps de nombres K comme étant le déterminant de la matrice représentant la forme trace introduite en 2.4.16 dans une $\mathbb{Z}$-base quelconque de l'anneau $\mathcal{O}_K$ de ses entiers.

– – – – – – – – – – – – – – – – –

2.4.20. Exercice*. *Où l'on voit quels sont les corps quadratiques imaginaires dont l'anneau des entiers est euclidien.*

Soit $d \neq 0, 1$ un entier rationnel sans facteur carré, désignons par $\mathcal{O}_d$ l'anneau des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}]$ et écrivons simplement $N = N_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}$.

(i) Si l'anneau $\mathcal{O}_d$ est euclidien et si $d < -3$, $\mathcal{O}_d$ comprend un élément non nul non inversible β tel que $N(\beta) \leqslant 3$.

(Indication. Il convient de se rappeler que, pour $d < -3$, $\mathcal{O}_d^\times = \{1, -1\}$. Si ν est une norme euclidienne pour $\mathcal{O}_d$, prenons parmi les éléments non nuls non inversibles de $\mathcal{O}_d$ un élément β pour lequel $\nu(\beta)$ est minimum. Observons alors que le reste de la division par un tel β des éléments de $\mathcal{O}_d$ est soit nul, soit inversible et conclure $\#(\mathcal{O}_d/\beta\mathcal{O}_d \leqslant 3$.)

(ii) Si $d \leqslant -13$, pour tout élément non nul non inversible α de $\mathcal{O}_d$ on a $N(\alpha) > 3$.

(iii) On en déduit que, pour $d < -11$, les anneaux $\mathcal{O}_d$ ne sont pas euclidiens.

Rappelons que le cas où $-11 \leqslant d \leqslant -1$ a été traité en 1.3.19, les seules valeurs négatives de d pour lesquelles $\mathcal{O}_d$ est euclidien sont donc les valeurs $-1, -2, -3, -7, -11$. Rappelons aussi 1.3.8 pour information.

2.4.21. Exercice. Calculer le discriminant du corps quadratique $\mathbb{Q}[\sqrt{d}]$ en fonction de d.

2.4.22. Exercice. Soient x, y deux éléments d'une extension finie L du corps K. Si x et y ont même polynôme minimal sur K alors

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{L/K}(y) \text{ et } N_{L/K}(x) = N_{L/K}(y).$$

2.4.23. Exercice*. Soit $L = K[x]$ une extension finie de K de degré n et soit

$$P = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$$

le polynôme minimal de x sur K. Observer :

$$P = \mathrm{Char}_{L/K,x} \quad \mathrm{N}_{L/K}(x) = (-1)^n c_0 \quad \mathrm{Tr}_{L/K}(x) = -c_{n-1}.$$

Écrire la matrice de la transformation K-linéaire $(x\cdot)$ de L dans la base $(1, x, x^2, \cdots, x^{n-1})$ de L sur K.

Cette matrice est appelée la *matrice compagnon* du polynôme P et P est son polynôme caractéristique.

Chapitre 3

Extension de corps

Dans ce chapitre nous continuons à rassembler quelques-uns des outils nécessaires à l'exploration des corps de nombres de degré supérieur à 2, de façon à obtenir une autre interprétation des normes et traces. Nous nous tournons ensuite vers les corps cyclotomiques et au passage nous explorons la structure des corps finis.

3.1 Corps de déploiement

Convention de section. Dans cette section, K désigne toujours un corps.

Définitions et observations 3.1.1. Nous dirons qu'un polynôme de degré positif $F \in K[X]$ se **déploie** dans une extension L de K si F est produit de facteurs de degré 1 dans $L[X]$, autrement dit si on a des éléments $a_1, a_2, \cdots, a_n \in L$ tel que

$$F = c(X - a_1)(X - a_2)\cdots(X - a_n)$$

où $0 \neq c \in K$ est le coefficient du terme de degré le plus élevé de F. Les a_i sont alors les racines de F dans L ($F(a_i) = 0$) et sont algébriques sur K.

Dans ce cas, F se déploie aussi dans la sous-K-extension finie $E = K[a_1, a_2, \cdots, a_n]$ de L. De plus, cette sous-K-extension E est la plus petite sous-K-extension de L où F se déploie. Nous dirons alors que E est un **corps de déploiement** de F sur K.

Remarque terminologique. Les « corps de déploiement » sont aussi appelés par certains auteurs « corps de rupture » (splitting field en anglais) ou même « corps des racines », cette dernière appellation étant toutefois un peu ambiguë. Nous préférons notre terminologie : le terme « déploiement » évoque l'ouverture, la joie, la fête, tandis que le terme « rupture » n'évoque rien d'agréable.

Il est facile de construire un corps de déploiement sur K d'un polynôme $F \in K[X]$.

Théorème 3.1.2. *(Existence des corps de déploiement.) Tout polynôme de degré positif $F \in K[X]$ possède un corps de déploiement E sur K tel que $[E : K] \leqslant n!$, où $n = \deg(F)$.*

Démonstration. Nous procédons par induction sur le degré de F.

Si F est de degré 1 il n'y a rien à faire.

Sinon, supposons le théorème vrai pour les polynômes dont le degré est strictement plus petit que celui de F et montrons qu'alors il est vrai pour F.

Prenons un facteur irréductible F_1 de F dans $K[X]$, formons le quotient $L_1 := K[X]/F_1K[X]$ et désignons par x l'image de X dans ce quotient. Nous savons que $L_1 = K[x]$ et que L_1 est un corps, extension finie de K, $[L_1 : K] = \text{degré}(F_1) \leqslant \text{degré}(F)$. Comme x est une racine de F_1 et aussi de F dans L_1 nous pouvons écrire $F = (X - x)G$, où $G \in L_1[X]$. L'hypothèse d'induction nous fournit un corps de déploiement E de G sur L_1 tel que $[E : L_1] \leqslant \text{degré}(G)! = (n-1)!$. On conclut en observant que E est aussi un corps de déploiement de F sur K et que $[E : K] = [E : L_1][L_1 : K] \leqslant n!$. □

Remarque 3.1.3. Si on dispose d'une extension algébriquement close Ω de K on obtient aussi un corps de déploiement sur K d'un polynôme $F \in K[X]$ en prenant $E = K[a_1, a_2, \cdots, a_n]$, où les a_i sont les racines de F dans Ω. Mais la preuve de l'existence d'une extension algébriquement close d'un corps quelconque commence toujours par le premier pas de la preuve de 3.1.2

Ce théorème facile va permettre une petite généralisation et une autre preuve de 2.3.5.

Proposition 3.1.4. *Soit A un domaine intégralement clos, K son corps des fractions et soit L une extension algébrique de K. Soit encore $x \in L$.*

Si x est entier sur A, alors son polynôme minimal P sur K appartient à $A[X]$ et toute autre racine de P dans n'importe quelle extension L' de K est entière sur A.

De plus on a aussi $\text{Char}_{L/K,x} \in A[X]$ *et* $\text{Tr}_{L/K}(x), N_{L/K}(x) \in A$

Démonstration. Comme l'élément x de L est entier sur A, il satisfait une relation de dépendance intégrale sur A et on a un polynôme unitaire $G \in A[X]$ s'annulant en x. Mais ce polynôme G, s'annulant en x, est divisible par P et toute racine de P est aussi racine de G, donc entière sur A.

Ceci étant, soit maintenant E un corps de déploiement de P sur K. On peut écrire $P = (X - a_1)(X - a_2) \cdots (X - a_n)$, où les $a_1, a_2, \cdots, a_n \in E$ sont les racines de P dans E (non nécessairement distinctes). En développant, on observe que les coefficients de P, qui sont des sommes de produits des

$\pm a_i$, appartiennent à $A[a_1, a_2, \cdots, a_n]$. Comme les a_i sont entiers sur A, les coefficients de P sont aussi entiers sur A (1.2.17). Mais les coefficients de P appartiennent au corps des fractions K de A et A est intégralement clos ; puisque ces coefficients sont entiers sur A ils sont dans A.

L' assertion concernant le polynôme caractéristique s'obtient avec 2.4.4 et celles sur la norme et la trace avec 2.4.2(iv). □

Nous allons maintenant montrer que, quelque soit la manière de construire un corps de déploiement du polynôme F de $K[X]$ sur K, le résultat est toujours le même, ce qui signifie que, si E et E' sont deux corps de déploiement sur K du même polynôme F il existe un **K-isomorphisme** $\sigma : E \xrightarrow{\sim} E'$ (rappelons qu'un K-isomorphisme entre deux extensions E, E' de K est un isomorphisme $\sigma : E \xrightarrow{\sim} E'$ tel que, pour tout $x \in K$, $\sigma(x) = x$). Comme cette preuve consiste à prolonger des isomorphismes il sera utile d'introduire un second corps $\tilde{K}$ isomorphe à K.

3.1.5. *Préparatif.* Soit $\sigma : K \xrightarrow{\sim} \tilde{K}$ un isomorphisme de corps.

Cet isomorphisme σ se prolonge immédiatement en un un isomorphisme $\sigma_X : K[X] \xrightarrow{\sim} \tilde{K}[X]$. Désignons par $\tilde{F}$ l'image par σ_X d'un polynôme $F \in K[X]$. On remarque que σ_X induit un isomorphisme $\overline{\sigma} : K[X]/(F) \xrightarrow{\sim} \tilde{K}[X]/(\tilde{F})$ qui prolonge σ, plus précisément on a un diagramme commutatif

$$\begin{array}{ccccc} K & \longrightarrow & K[X] & \xrightarrow{p} & K[X]/(F) \\ {\scriptstyle\sigma}\downarrow & & {\scriptstyle\sigma_X}\downarrow & & \downarrow{\scriptstyle\overline{\sigma}} \\ \tilde{K} & \longrightarrow & \tilde{K}[X] & \xrightarrow{\tilde{p}} & \tilde{K}[X]/(\tilde{F}) \end{array}$$

où p et $\tilde{p}$ sont les projections naturelles.

Lemme 3.1.6. *(Premier pas des prolongements.)*

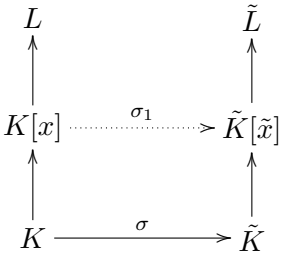
Soit $\sigma : K \xrightarrow{\sim} \tilde{K}$ un isomorphisme de corps et soient $K \subset L$ et $\tilde{K} \subset \tilde{L}$ deux extensions algébriques de corps.

Soit encore $x \in L$ et soit $F = Min_{K,x}$ le polynôme minimal de x sur K. Nous reprenons les notations de 3.1.5.

(i) Pour tout homomorphisme $\tau : K[x] \to \tilde{L}$ prolongeant σ. $\tau(x)$ est racine du polynôme $\tilde{F} \in \tilde{K}[X]$.

(ii) Pour toute racine $\tilde{x}$ de $\tilde{F}$ dans $\tilde{L}$, il existe un unique isomorphisme $\sigma_1 : K[x] \to \tilde{K}[\tilde{x}]$ prolongeant σ et tel que $\sigma_1(x) = \tilde{x}$.

Ceci s'inscrit donc dans un diagramme commutatif

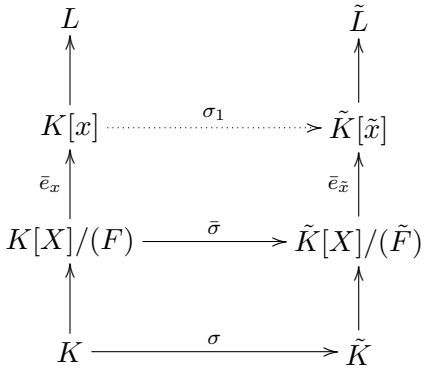


où les flèches verticales représentent les inclusions naturelles.

(iii) Le nombre r d'homomorphismes $\tau : K[x] \to \tilde{L}$ prolongeant σ est exactement le nombre des racines du polynôme $\tilde{F}$ dans $\tilde{L}$, d'où $r \leqslant$ degré(F).

Démonstration. (i) Comme $F(x) = 0$ et que τ est un homomorphisme, on a aussi $\tau(F(x)) = 0$ et $0 = \tau(F(x)) = (\tilde{F})(\tau(x))$

(ii) Les évaluations en x et en $\tilde{x}$ nous fournissent des isomorphismes $\bar{e}_x$ et $\bar{e}_{\tilde{x}}$ indiqués dans le diagramme commutatif suivant, et il suffit de prendre $\sigma_1 = \bar{e}_{\tilde{x}} \circ \overline{\sigma} \circ {\bar{e}_x}^{-1}$.



L'unicité de σ_1 satisfaisant les conditions requises est évidente.

(iii) Ceci est une conséquence directe de (i) et (ii). □

3.1.7. Voici une remarque évidente que nous utiliserons souvent. Si E est un corps de déploiement sur K d'un polynôme $F \in K[X]$ et si E' est une sous-K-extension de E, E est aussi un corps de déploiement de F sur E'.

Théorème 3.1.8. *(Unicité des corps de déploiement.) Soit $F \in K[X]$ un polynôme de degré positif et soit $\sigma : K \xrightarrow{\sim} \tilde{K}$ un isomorphisme de corps,*

Soit encore E un corps de déploiement sur K de F et soit $\tilde{E}$ un corps de déploiement sur $\tilde{K}$ du polynôme $\tilde{F} \in \tilde{K}[X]$ (notation comme en 3.1.5).

Alors σ se prolonge en un isomorphisme $\sigma' : E \xrightarrow{\sim} \tilde{E}$.

$$\begin{array}{ccc} E & \xrightarrow{\sigma'} & \tilde{E} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & \tilde{K} \end{array}$$

En particulier on a $[E : K] = [\tilde{E} : \tilde{K}]$.

Démonstration. Nous procédons par induction sur le degré de F. Si $deg(F) = 1$, on a $E = K$, $\tilde{E} = \tilde{K}$ et il n'y a rien à faire. Supposons avoir démontré le théorème pour les polynômes dont le degré est strictement inférieur à celui de F et montrons-le pour F.

Supposons donc $\deg(F) > 1$ et prenons un facteur irréductible F_1 de F. Tout comme F, ce F_1 se déploie dans E, il a une racine x dans E et son correspondant $\tilde{F}_1$ dans $\tilde{K}[X]$, qui est un facteur irréductible de $\tilde{F}$, a aussi une racine $\tilde{x}$ dans $\tilde{E}$. Le lemme 3.1.6 nous fournit alors un isomorphisme $\sigma_1 : K[x] \xrightarrow{\sim} \tilde{K}[\tilde{x}] : x \mapsto \tilde{x}$ prolongeant σ. Mais x est aussi une racine de F et nous avons une factorisation $F = (X - x)G$ où $G \in K[x][X]$. Prenant l'image de cette factorisation par l'isomorphisme σ_{1X} (notation comme en 3.1.5) il vient $\tilde{F} = (X - \tilde{x})\sigma_{1X}(G)$. On remarque alors que E (resp. $\tilde{E}$) est un corps de déploiement de G sur $K[x]$ (resp. de $\sigma_{1X}(G)$ sur $K[\tilde{x}]$) et on conclut par l'hypothèse d'induction. □

Le corps de déploiement d'un polynôme F peut aussi être le corps de déploiement d'un autre polynôme G. Par exemple, $\mathbb{Q}[\sqrt{5}]$ est le corps de déploiement sur $\mathbb{Q}$ du polynôme $X^2 - 5$, et aussi du polynôme $X^2 - X - 1$. Mais nous allons voir que les corps de déploiement ont d'agréables propriétés, indépendantes du polynôme dont ils sont le corps de déploiement. C'est pourquoi on introduit un nouveau vocable.

Définition 3.1.9. Une extension E de K est dite **normale** si E est le corps de déploiement sur K d'un polynôme $F \in K[X]$.

Voici une propriété essentielle des extensions normales et aussi un critère de normalité.

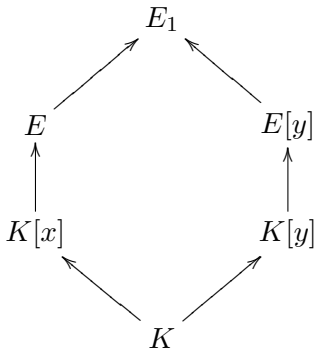
Théorème 3.1.10. *Soit E une extension finie de K. Les conditions suivantes sont équivalentes :*

(i) E est une extension normale de K,

(ii) tout polynôme irréductible G de $K[X]$ ayant une racine dans E se déploie dans E.

Démonstration. (i) ⇒ (ii) Soit G un polynôme irréductible de $K[X]$ ayant une racine x dans E, soit E_1 un corps de déploiement de G sur $\mathbf{E}$ et soit y une racine quelconque de G dans E_1. Nous devons montrer que $y \in E$.

Regardons le diagramme suivant, où les flèches représentent les inclusions naturelles.



Comme x et y sont deux racines du polynôme irréductible G de $K[X]$, nous avons

$$[K[x] : K] = \deg(G) = [K[y] : K].$$

Et nous avons aussi un K-isomorphisme $\sigma : K[x] \xrightarrow{\sim} K[y]$ (3.1.6).

D'autre part E par hypothèse est un corps de déploiement sur K d'un polynôme $F \in K[X]$. A fortiori E est un corps de déploiement de F sur $K[x]$. Mais $E[y]$ est aussi un corps de déploiement sur $K[y]$ du même polynôme F. Comme $K[x] \simeq K[y]$, on en déduit encore avec 3.1.8 l'égalité

$$[E : K[x]] = [E[y] : K[y]].$$

De tout ceci on déduit :

$$[E : K] = [E : K[x]] \cdot [K[x] : K] = [E[y] : K[y]] \cdot [K[y] : K] = [E[y] : K]$$

Or $E \subset E[y]$ et nous avons aussi :

$$[E[y] : K] = [E[y] : E] \cdot [E : K].$$

Il en résulte $[E[y] : E] = 1$, $E[y] = E$ et $y \in E$.

(Il en résulte aussi $E = E_1 = E[y]$.)

(ii) $\Rightarrow$ (i). Comme E est une extension finie de K, on peut écrire $E = K[a_1, a_2, \cdots, a_n]$. Soit F_i le polynôme minimal de a_i sur K, $1 \leqslant i \leqslant n$. Comme F_i est un polynôme irréductible de $K[X]$ ayant une racine a_i dans E, notre hypothèse nous dit qu'il se déploie dans E. Alors le polynôme $F = F_1 F_2 \cdots F_n$ se déploie aussi dans E. Comme E est engendré sur K par les a_i qui sont des racines de F, E est un corps de déploiement de F sur K. □

Les extensions finies ne sont pas toutes normales. Par exemple l'extension $\mathbb{Q}[2^{\frac{1}{3}}]$ de $\mathbb{Q}$ n'est pas normale, le polynôme irréductible $X^3 - 2$ de $\mathbb{Q}[X]$ y a une racine sans s'y déployer. Mais nous pourrons remédier à cette non normalité. La proposition suivante sera utile.

Proposition 3.1.11. *Toute extension finie L de K est contenue dans une extension normale E de K.*

Et alors tout polynôme irréductible de $K[X]$ ayant une racine dans L se déploie dans cette extension E.

Démonstration. Si $L = K[a_1, a_2, \cdots, a_n]$, prenons comme précédemment les polynômes minimaux F_i des a_i sur K, prenons leur produit $F = F_1F_2 \cdots F_n$ et prenons un corps de déploiement E de F sur L. Comme L est engendré sur K par les a_i qui sont des racines de F, E est aussi un corps de déploiement de F sur K.

La seconde assertion est un corollaire du théorème précédent. □

Remarque 3.1.12. Si E est une extension normale de K, corps de déploiement sur K du polynôme $F \in K[X]$, alors tout K-automorphisme de E induit une permutation des racines de F dans E, 3.1.6, et est entièrement déterminé par son action sur ces racines, car elles engendrent l'extension E de K. Le groupe $\mathrm{Aut}_K(E)$ des K-automorphismes de E apparaît donc comme un sous-groupe du groupe des permutations des racines de F dans E.

Le groupe $\mathrm{Aut}_K(E)$ est donc fini et il sera intéressant de comparer les nombres $\#(\mathrm{Aut}_K(E))$ et $[E : K]$. On devine déjà que

$$\#(\mathrm{Aut}_K(E)) \leqslant [E : K],$$

cependant la présence d'éventuelles « *racines multiples* » pourrait forcer cette inégalité à être stricte. Pouvoir détecter la présence de racines multiples sera très utile.

– – – – – – – – – – – – – – – – –

3.1.13. Exercice. Représenter les racines cubiques de 2 dans le plan complexe et montrer un corps de déploiement E sur $\mathbb{Q}$ du polynôme $X^3 - 2$.

Calculer $[E : \mathbb{Q}]$.

3.1.14. Exercice. Montrer que $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ est une extension normale de $\mathbb{Q}$ de degré 4 et décrire son groupe d'automorphismes.

3.1.15. Exercice. Toute extension de degré 2 d'un corps K est une extension normale de K.

3.1.16. Exercice. *Une extension normale d'une extension normale n'est pas toujours normale.*

Regarder les extensions $\mathbb{Q} \subset \mathbb{Q}[3^{\frac{1}{2}}] \subset \mathbb{Q}[3^{\frac{1}{4}}]$.

$\mathbb{Q}[3^{\frac{1}{2}}]$ est une extension normale de $\mathbb{Q}$,

$\mathbb{Q}[3^{\frac{1}{4}}]$ est une extension normale de $\mathbb{Q}[3^{\frac{1}{2}}]$,

mais $\mathbb{Q}[3^{\frac{1}{4}}]$ n'est pas une extension normale de $\mathbb{Q}$.

(Ceci est à rapprocher d'un fait similaire en théorie des groupes : un sous-groupe normal N_1 d'un sous-groupe normal N_2 d'un groupe G n'est pas nécessairement un sous-groupe normal de G.)

3.1.17. Exercice. Décrire le groupe des automorphismes de $\mathbb{Q}[3^{\frac{1}{4}}]$ et calculer $[\mathbb{Q}[3^{\frac{1}{4}}] : \mathbb{Q}]$.

Montrer un corps de déploiement E sur $\mathbb{Q}$ du polynôme $X^4 - 3$.

3.2 Racines simples, Racines multiples

3.2.1. Soient K un corps, $F \in K[X]$ un polynôme de degré positif et a une racine de F dans une extension L de K, ce qui signifie que $a \in L$ et que $F(a) = 0$, autrement dit que $(X - a)$ divise F dans $L[X]$. Nous pouvons écrire

$$F = (X-a)^r F_1 \quad \text{où} \quad r \in \mathbb{N}_0 \quad F_1 \in L[X] \quad \text{et où} \quad F_1(a) \neq 0.$$

Si $r = 1$, nous dirons que a est une **racine simple** de F.

Si $r > 1$, nous dirons que a est une **racine multiple** de F, de **multiplicité** r.

Commençons par un critère très simple permettant de voir si une racine donnée du polynôme F est simple ou multiple. Une notion de dérivation sera utile.

Définition 3.2.2. Soit A un anneau et soit

$$F = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X].$$

On définit la dérivée de F par

$$d(F) = \sum_{i=1}^{n} i a_i X^{i-1} = n a_n X^{n-1} + \cdots + a_1.$$

Notons qu'ici A est un anneau quelconque qui peut ne rien avoir à faire avec le corps des réels, il peut même être fini. Notre dérivée est donc purement formelle, elle n'en a pas moins les propriétés usuelles.

Propriétés 3.2.3. Un simple calcul montre que, pour tous $F, G \in A[X]$, pour tout $a \in A$ on a :

$$d(F+G) = d(F) + d(G), \quad d(aF) = a d(F),$$
$$d(FG) = d(F)G + F d(G), \quad d(a) = 0.$$

Notons aussi que, si A est un sous-anneau d'un autre anneau B, les dérivées d'un polynôme $F \in A[X] \subset B[X]$, prises dans $A[X]$ ou $B[X]$, coïncident.

Voici ce petit critère.

Proposition 3.2.4. *Soient K un corps, $F \in K[X]$ un polynôme de degré positif et a une racine de F dans une extension L de K. Alors :*

a est une racine multiple de $F \Leftrightarrow d(F)(a) = 0$.

Démonstration. Écrivons $F = (X-a)^r F_1$, où $r \in \mathbb{N}_0$, $F_1 \in L[X]$ et où $F_1(a) \neq 0$.

Si $r > 1$, on a $d(F) = r(X-a)^{r-1} F_1 + (X-a)^r d(F_1)$ et $d(F)(a) = 0$.

Si $r = 1$, on a $d(F) = F_1 + (X-a) d(F_1)$ et $d(F)(a) = F_1(a) \neq 0$. □

Nous désirons maintenant un critère nous permettant de reconnaître si un polynôme $F \in K[X]$ peut avoir ou non une racine multiple dans une extension de K. Ceci peut être intéressant car depuis Galois on sait qu'il n'existe aucun moyen de calculer les racines d'un polynôme quelconque de degré $\geqslant 5$.

Rappelons que le pgcd de deux polynômes $F, G \in K[X]$ peut se calculer par divisions successives. Il en résulte que, si L est une extension de K, le pgcd de deux polynômes $F, G \in K[X]$ pris dans $L[X]$ est aussi le pgcd de ces deux polynômes pris dans $K[X]$.

Proposition 3.2.5. *Soient K un corps et $F \in K[X]$ un polynôme de degré positif. Les conditions suivantes sont équivalentes :*

(i) les racines de F dans n'importe quelle extension L de K sont toutes simples.

(ii) $\operatorname{pgcd}(F, d(F)) = 1$.

Démonstration. Si le polynôme $F \in K[X]$ possède une racine multiple a dans une certaine extension L de K, les polynômes F et $d(F)$, tous deux divisibles par $(X - a)$ dans $L[X]$ (3.2.4), ne sont pas premiers entre eux.

Si le polynôme F n'a que des racines simples dans toute extension L de K, prenons un corps de déploiement E de F sur K. Le polynôme F s'y factorise complètement, on a

$$F = c(X - a_1)(X - a_2) \cdots (X - a_n)$$

où $0 \neq c \in K$ et où les éléments a_i sont les racines de F dans E, donc distincts deux à deux. On observe alors que

$$d(F)(a_i) = c \prod_{k \neq i} (a_i - a_k) \neq 0,$$

qu'aucun des facteurs $(X - a_i)$ de F ne divise $d(F)$. On en déduit $\operatorname{pgcd}(F, d(F)) = 1$. □

Définition 3.2.6. Soit K un corps. Un polynôme de degré positif $F \in K[X]$ est dit **séparable** si $\operatorname{pgcd}(F, d(F)) = 1$, autrement dit si F n'a que des racines simples dans toute extension de K.

Un élément x d'une extension algébrique L de K est dit séparable sur K ou **K-séparable** si son polynôme minimal sur K est séparable.

Une extension algébrique L de K est dite séparable si tous ses éléments sont séparables sur K.

Observation 3.2.7. Soient $K \subset K_1 \subset L$ trois corps emboîtés et supposons que L est une extension séparable de K.

Alors L est aussi une extension séparable de K_1.

En effet, pour tout $x \in L$, le polynôme minimal $\mathrm{Min}_{K_1,x}$ de x sur K_1 divise dans l'anneau $K_1[X]$ le polynôme minimal $\mathrm{Min}_{K,x}$ de x sur K. Si ce dernier n'a que des racines simples, il en est de même du premier.

Et K_1 est aussi une extension séparable de K.

3.2.8. En caractéristique nulle la dérivée d'un polynôme de degré positif n'est jamais nulle, les polynômes irréductibles sont donc séparables et tout polynôme irréductible de degré n a exactement n racines dans toute extension où il se déploie

En caractéristique positive la situation est un peu plus compliquée car la dérivée d'un polynôme de degré positif peut être nulle ! En effet, soit K un corps de caractéristique p et soit $F = \sum_{i=0}^{n} a_i X^i \in K[X]$. On a :

$$d(F) = 0 \quad \Leftrightarrow \quad (\forall i, 1 \leqslant i \leqslant n, \quad a_i \neq 0 \Rightarrow i \in p\mathbb{N}).$$

Par exemple, pour le polynôme $F = X^6 - 2 \in \mathbb{Z}_3[X]$ on a $d(F) = 0$. Notons qu'on a aussi $2^3 = 2$ et $X^6 - 2 = (X^2 - 2)^3$ dans $\mathbb{Z}_3[X]$, $X^6 - 2$ n'est pas irréductible dans $\mathbb{Z}_3[X]$.

Voici un autre exemple. Soient p un premier naturel et $K = \mathbb{Z}_p(t)$, le corps des fractions de l'anneau $\mathbb{Z}_p[t]$ des polynômes en l'indéterminée t à coefficients dans le corps $\mathbb{Z}_p$. Regardons le polynôme $X^p - t \in K[X]$. Ici aussi on a $d(X^p - t) = 0$, mais cette fois le polynôme $X^p - t$ est irréductible dans $K[X]$ (2.3.9).

Il y a un endomorphisme remarquable sous-jacent à ces phénomènes.

Proposition 3.2.9. *Soit A un anneau de caractéristique p un nombre premier. La fonction*

$$Fr_A : A \to A : x \mapsto x^p$$

est un endomorphisme de A, appelé endomorphisme de **Frobenius** *de A.*

(L'indice A est omis de la notation quand cela ne prête pas à confusion.)

Démonstration. Pour tous $x, y \in A$ on a évidemment $(xy)^p = x^p y^p$ car la multiplication est commutative. Mais on a aussi $(x + y)^p = x^p + y^p$ car les coefficient binomiaux $\binom{p}{i}$ sont multiples de p pour $1 \leqslant i \leqslant p-1$ (0.9.5). □

3.2.10. L'endomorphisme de Frobenius d'un corps K de caractéristique positive p est évidemment injectif. Et il est bijectif si et seulement si tous les éléments de K sont des puissances $p^{\text{ièmes}}$: $\forall x \in K, \exists y \in K, x = y^p$, notons qu'alors l'élément y de K tel que $y^p = x$ est unique. Cette dernière condition est particulièrement intéressante car si elle est satisfaite tout polynôme de degré positif dont la dérivée est nulle est aussi une puissances $p^{\text{ième}}$ ($\sum_{i=n}^{n} a_i^p X^{ip} = (\sum_{i=n}^{n} a_i X^i)^p$), donc non irréductible. Mais alors les polynômes irréductibles sont séparables et la situation reste satisfaisante. Ceci nous amène à une définition propre à formuler nos remarques.

Définition 3.2.11. Un corps de caractéristique positive est dit **parfait** si son endomorphisme de Frobenius est bijectif, autrement dit est un automorphisme.

Pour éviter des lourdeurs de langage, on dit aussi d'un corps de caractéristique nulle qu'il est parfait.

Les corps parfaits sont nombreux.

Proposition 3.2.12. *Tout corps fini est parfait.*
Tout corps algébriquement clos est aussi parfait.

Comme nous l'avons remarqué en 3.2.8 et 3.2.10 les corps parfaits sont bien aimables.

Proposition 3.2.13. *Si K est un corps parfait, tout polynôme irréductible F de $K[X]$ est séparable et a donc exactement $n := \text{degré}(F)$ racines dans toute extension de K où il se déploie.*
Par conséquent toute extension algébrique d'un corps parfait est séparable.

Réciproquement, on peut montrer qu'un corps dont toute extension algébrique est séparable est parfait, voir 3.2.16.

Terminons par un autre exemple assez significatif.

Exemple 3.2.14. Le polynôme $X^n - 1 \quad (n \in \mathbb{N}_0)$ de $K[X]$ est séparable si la caractéristique de K est nulle ou, dans le cas où K est un corps de caractéristique positive p, si $p \nmid n$.

Dans ces cas, le polynôme $X^n - 1$ a exactement n racines distinctes dans toute extension de K où il se déploie.

– – – – – – – – – – – – – – – – –

3.2.15. Exercice. Soit K un corps non parfait de caractéristique p et soit a un élément de K qui n'est pas une puissance $p^{\text{ième}}$. Regardons le polynôme

$$T = X^p - a.$$

(i) $d(T) = 0$

(ii) Soit b une racine de T dans un corps de déploiement E de T sur K. Comme $b^p = a$ on a

$$T = (X - b)^p, \quad b \text{ est la seule racine de T dans } E \quad \text{et} \quad E = K[b].$$

(iii) T est irréductible dans $K[X]$, $[E : K] = p$ et E n'est pas une extension séparable de K.

(iv) E n'a qu'un seul K-automorphisme, l'automorphisme identique.

3.2.16. Exercice. Un corps est parfait si et seulement si toutes ses extensions algébriques sont séparables.

3.2.17. Exercice. Toute extension finie K_1 d'un corps parfait K est parfaite.

(Indication. On peut commencer par prouver que l'image par Fr_{K_1} d'une base du K-vectoriel K_1 est une partie libre du K-vectoriel K_1. Mais attention : si K est de caractéristique positive, Fr_{K_1} n'est pas une transformation linéaire de K_1 vu comme comme K-vectoriel, Fr_K n'est pas nécessairement l'automorphisme identique de K.

On peut aussi argumenter en utilisant l'exercice 3.2.16.)

3.3 Normes, Traces et Extensions galoisiennes

Quand nous avons étudié les corps quadratiques, nous disposions d'un automorphisme de conjugaison bien pratique. Que pouvons-nous faire pour étudier un corps de nombres quelconque, une extension finie L de $\mathbb{Q}$? Certes on peut regarder les automorphismes de L ; on peut en avoir plusieurs ; mais surtout on peut n'en avoir pas assez. Par exemple le seul automorphisme de $\mathbb{Q}[2^{\frac{1}{3}}]$ est l'automorphisme identique, notons cependant que $\mathbb{Q}[2^{\frac{1}{3}}]$ n'est pas une extension normale de $\mathbb{Q}$.

Nous savons déjà que toute extension finie L d'un corps K est contenue dans une extension normale E de K et qu'alors tout polynôme irréductible de $K[X]$ ayant une racine dans L s'y déploie (3.1.11). Une telle extension va nous permettre de remédier à la situation.

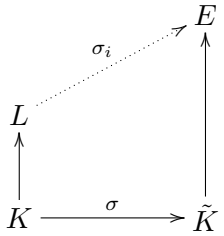
Théorème 3.3.1. *Soit $K \xrightarrow{\sigma} \tilde{K}$ un isomorphisme de corps .*

Soit L une extension finie séparable de K de degré n, soit encore E une extension de $\tilde{K}$ telle que, pour tout polynôme irréductible G de $K[X]$ ayant une racine dans L, le polynôme $\tilde{G} = \sigma_X(G)$ se déploie dans E (notations comme en 3.1.5).

Alors il y a exactement n homomorphismes distincts

$$\sigma_i : L \to E \quad 1 \leqslant i \leqslant n$$

prolongeant σ.



Si $x \in L$, les $\sigma_i(x)$ sont souvent appelés les **conjugués** *de x dans E.*

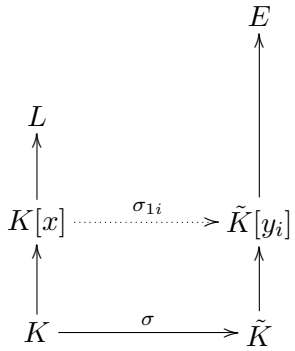
De plus, si P est le polynôme minimal de x sur K, si $r = \deg(P) = [K[x] : K]$ et si $s = [L : K[x]]$, de sorte que $n = sr$, les $\sigma_i(x)$ sont les r racines de $\tilde{P}$ dans E, ces racines toutes distinctes étant chacune répétée s fois.

Démonstration. Nous procédons par induction sur le degré $n = [L : K]$ de l'extension.

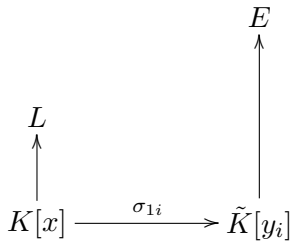
Si $n = 1$, alors $L = K$ et il n'y a rien à faire. Supposons le théorème démontré pour les extensions de degré < n et montrons-le pour les extensions de degré n, $n > 1$.

Si $n > 1$, soit $x \in L \setminus K$, soit P son polynôme minimal sur K et soit $r = \deg(P) = [K[x] : K] > 1$.

Comme P est un polynôme irréductible de $K[X]$ ayant une racine x dans L, notre hypothèse nous dit que $\tilde{P}$ se déploie dans E. Comme par hypothèse P est séparable, $\tilde{P}$ est aussi séparable et a exactement r racines distinctes $y_1, y_2, \cdots, y_r$ dans E. Avec 3.1.6 nous obtenons exactement r isomorphismes $\sigma_{1i} : K[x] \to \tilde{K}[y_i] : x \mapsto y_i$ prolongeant σ $(1 \leqslant i \leqslant r)$.



Pour pouvoir appliquer l'hypothèse d'induction, il nous faut d'abord vérifier que la situation décrite par la partie supérieure du diagramme



satisfait aux hypothèses du théorème.

Voyons ceci. Posons

$$K_1 = K[x] \qquad \tilde{K}_{1i} = \tilde{K}[y_i].$$

Notons d'abord que L est une extension séparable de K_1, 3.2.7. Soit maintenant F_1 un polynôme irréductible de $K_1[X]$ ayant une racine $z \in L$. Il nous faut montrer que le polynôme $\sigma_{1iX}(F_1)$ de $\tilde{K}_{1i}[X]$ se déploie dans E. Mais dans $K_1[X]$ le polynôme F_1 divise le polynôme minimal F de z sur K, nous avons $F = F_1 H$, où $H \in K_1[X]$. Prenons l'image de cette égalité par σ_{1iX}, il vient $\tilde{F} = \sigma_X(F) = \sigma_{1iX}(F_1)\sigma_{1iX}(H)$. Comme $\tilde{F}$ se déploie dans E par hypothèse, il en est de même de son facteur $\sigma_{1iX}(F_1)$.

Ainsi nous sommes en position d'appliquer l'hypothèse d'induction. Chacun des r isomorphismes σ_{1i} obtenus en début de preuve se prolonge en exactement s homomorphismes $K_1 \to E$. Comme tout homomorphisme $L \to E$ restreint à $K[x]$ induit un des isomorphismes σ_{1i}, notre isomorphisme de base σ se prolonge en exactement $sr = n$ homomorphismes $K \to E$. Ceci montre aussi la dernière assertion concernant les $\sigma_i(x)$. □

Corollaire 3.3.2. *Toute extension finie de $\mathbb{Q}$ se plonge dans le corps des complexes.*

En examinant la preuve de 3.3.1, essentiellement basée sur 3.1.6, nous obtenons l'information suivante.

Proposition 3.3.3. *Soient L une extension finie du corps K, $\sigma : K \to \tilde{K}$ un isomorphisme de corps et E une extension de $\tilde{K}$.*

Alors le nombre m d'homomorphismes $L \to E$ prolongeant σ est tel que $m \leqslant [L : K]$.

Pour que $m \neq 0$ il faut que, pour tout polynôme irréductible P de $K[X]$ ayant une racine dans L, le polynôme $\tilde{P}$ aie une racine dans E.

Et $m = [L : K]$ si et seulement si L est une extension séparable de K telle que, pour tout polynôme irréductible P de $K[X]$ ayant une racine dans L, le polynôme $\tilde{P}$ se déploie dans E.

Dans la pratique nous aurons $K = \tilde{K}$, $\sigma = 1_K$ et il sera souvent utile de prendre pour E une extension normale de K contenant l'extension séparable L de K. Les hypothèses du théorème 3.3.1 seront satisfaites, rappelons 3.1.10, et dans ce cas l'injection naturelle de L dans E figurera parmi les σ_i. Le cas où $L = E$ est une extension normale et séparable de K est évidemment le cas idéal.

Définitions 3.3.4. L'extension E du corps K est dite **galoisienne** si elle est une extension normale et séparable de K.

Nous dirons que deux éléments x et y de l'extension galoisienne E de K sont **K-conjugués** s'il existe un K-automorphisme σ de E tel que $\sigma(x) = y$ ou, ce qui revient au même avec 3.3.1, si x et y ont même polynôme minimal sur K.

Le groupe des K-automorphismes de l'extension galoisienne E de K sera appelé **groupe de Galois de E sur K** et sera souvent désigné par $\mathcal{G}al(E/K)$.

Avec 3.3.1 le résultat suivant est presque évident.

Corollaire 3.3.5. *Soit E est une extension galoisienne de degré n du corps K.*

Alors $\mathcal{G}al(E/K)$ est un groupe fini d'ordre n et

$$\{x \in E \mid \forall \sigma \in \mathcal{G}al(E/K), \quad \sigma(x) = x\} = K.$$

Démonstration. Avec 3.3.1 on sait qu'on a exactement n K-endomorphismes $\sigma_i : E \to E$. Ces σ_i sont aussi des transformations linéaires injectives du K-vectoriel de dimension finie E, elles sont donc bijectives.

De plus, si $x \in E \setminus K$, le polynôme minimal de x sur K est de degré >1, il a dans E une racine $y \neq x$ et nous avons, toujours avec 3.3.1, un $\sigma \in \mathcal{G}al(E/K)$ tel que $\sigma(x) = y \neq x$. □

Les extensions galoisiennes ont beaucoup d'autres jolies propriétés et la structure de leur groupe de Galois est du plus haut intérêt, mais ce qui précède suffira à nos premières explorations des nombres.

Comme dans le cas des corps quadratiques, nous pouvons maintenant exprimer les normes et traces introduites en 2.4.1 à l'aide de certains homomorphismes.

Théorème 3.3.6. *Soit K un corps, L une extension séparable de K de degré n et soit*

$$\sigma_i : L \to E \qquad\qquad 1 \leqslant i \leqslant n$$

les n K-homomorphismes distincts de L dans une extension E de K où tout polynôme irréductible de $K[X]$ ayant une racine dans L se déploie.

Alors, $\forall x \in L$, on a

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x) \quad et \quad N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

De plus,

$$\mathrm{Char}_{L/K,x} = (X - \sigma_1(x))(X - \sigma_2(x)) \cdots (X - \sigma_n(x)) = \mathrm{Min}_{K,x}{}^{s},$$

où $\mathrm{Min}_{K,x}$ désigne le polynôme minimal de x sur K et où $s = [L : K[x]]$.

Démonstration. Nous savons déjà que $\mathrm{Char}_{L/K,x} = \mathrm{Min}_{K,x}{}^{s}$, 2.4.4.

Premier cas. Dans le cas où $L = K[x]$, c.-à-d. où $s = 1$ et degré$(\mathrm{Min}_{K,x}) = n$, nous savons aussi aussi que les $\sigma_i(x)$ sont les n racines distinctes de $\mathrm{Min}_{K,x}$, d'où la factorisation $(X - \sigma_1(x))(X - \sigma_2(x)) \cdots (X - \sigma_n(x)) = \mathrm{Min}_{K,x}$. On obtient alors les relations sur la norme et la trace avec 2.4.2(iv).

Cas général. Nous savons avec 3.3.1 que les $\sigma_i(x)$ sont encore les racines de $\mathrm{Min}_{K,x}$, chacune étant cette fois répétées s fois. Le premier cas et l'égalité $\mathrm{Char}_{L/K,x} = \mathrm{Min}_{K,x}{}^{s}$ nous donne alors la factorisation de $\mathrm{Char}_{L/K,x}$; comme dans le premier cas on en déduit les autres relations.

□

– – – – – – – – – – – – – – – – –

3.3.7. Exercice. Montrer que $\mathbb{Q}[e^{\frac{2\pi i}{5}}]$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

Observer que $\mathcal{G}al(\mathbb{Q}[e^{\frac{2\pi i}{5}}]/\mathbb{Q})$ est un groupe cyclique d'ordre 4.

3.3.8. Exercice. Déterminer le corps de déploiement de $2^{\frac{1}{3}}$ sur $\mathbb{Q}$ et montrer que son groupe de Galois est isomorphe au groupe symétrique $\mathcal{S}_3$.

3.3.9. Exercice. Regardons l'extension $\mathbb{Q}[2^{\frac{1}{3}}]$ de $\mathbb{Q}$.

(a) On a : $\mathrm{Tr}_{\mathbb{Q}[2^{\frac{1}{3}}]/\mathbb{Q}}(2^{\frac{1}{3}}) = 0$ et $N_{\mathbb{Q}[2^{\frac{1}{3}}]/\mathbb{Q}}(2^{\frac{1}{3}}) = 2$.

Le nombre $2^{\frac{1}{3}}$ est entier sur $\mathbb{Z}$ et est irréductible dans $\mathcal{O}_{\mathbb{Q}[2^{\frac{1}{3}}]}$.

(b) Plus généralement, soit $\alpha = a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}} \in \mathbb{Q}[2^{\frac{1}{3}}]$, $a, b, c \in \mathbb{Q}$.

Alors $\mathrm{Tr}_{\mathbb{Q}[2^{\frac{1}{3}}]/\mathbb{Q}}(\alpha) = 3a$.

(c) Montrer que $N_{\mathbb{Q}[2^{\frac{1}{3}}]/\mathbb{Q}}(1 - 2^{\frac{1}{3}}) = -1$ et en déduire que $1 - 2^{\frac{1}{3}}$ est inversible dans $\mathcal{O}_{\mathbb{Q}[2^{\frac{1}{3}}]}$.

3.4 Corps finis

Nos pérégrinations nous ont fait rencontrer des corps finis, nous avons même été amenés à en exploiter certaines propriétés. Par ailleurs les corps finis interviennent dans beaucoup d'autres domaines des mathématiques, on les rencontre entre autres en théorie des codes. Ce ne sera donc pas inutile de les regarder d'un peu plus près.

3.4.1. Soit F un corps fini. La caractéristique de F est un nombre premier p et $\mathbb{Z}_p$ est un sous-corps de F (0.7.2). Le corps F a donc une structure d'espace vectoriel sur le corps $\mathbb{Z}_p$. De plus, comme F est fini, F est un espace vectoriel de dimension finie sur $\mathbb{Z}_p$, disons $n = [F : \mathbb{Z}_p]$; on a alors $\#F = p^n$.

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

La première question qui se pose est la suivante. Existe-t'il un corps fini de cardinal une puissance donnée d'un nombre premier p, et, si oui, combien avons-nous de tels corps ? La réponse est ci-dessous.

Théorème 3.4.2. *Soit $q = p^n$ une puissance du nombre premier p, $n \geqslant 1$. Alors il existe un et un seul corps fini F de q éléments, à isomorphisme près.*

Ce corps est souvent désigné par $\mathbb{F}_q$, il est le corps de déploiement sur $\mathbb{Z}_p$ du polynôme $X^q - X$.

Démonstration. (i) *Unicité.* Soit F un corps avec $\#F = q$. Le groupe multiplicatif de F est un groupe d'ordre $q - 1$ et, pour tout $x \in F, x \neq 0$, on a $x^{q-1} = 1$. Il en résulte que, $\forall x \in F$, on a $x^q = x$.Comme $F \supset \mathbb{Z}_p$ ce qui précède montre que les q éléments de F sont les racines du polynôme $X^q - X$ de $\mathbb{Z}_p[X]$, donc que F est le corps de déploiement sur $\mathbb{Z}_p$ du polynôme $X^q - X$. L'unicité de F avec $\#F = q$ résulte alors de l'unicité des corps de déploiement 3.1.8

(ii) *Existence.* Prenons le corps de déploiement E sur $\mathbb{Z}_p$ du polynôme $X^q - X \in \mathbb{Z}_p[X]$ (3.1.2) et regardons l'ensemble $R = \{x \in E \mid x^q = x\}$ des racines du polynôme $X^q - X$ dans E. Comme $d(X^q - X) = -1$, on a $\operatorname{pgcd}((X^q - X), d(X^q - X)) = 1$, le polynôme $X^q - X$ n'a pas de racine multiples (3.2.5) et $\#R = q$.

D'autre part R est un sous-corps de E. En effet, $0, 1 \in R$ et, $\forall x, y \in R$ on a $(xy)^q = x^q y^q = (xy)$, on a aussi $(x \pm y)^q = (x^q \pm y^q) = (x \pm y)$ (voir 0.9.5) et $(x^{-1})^q = (x^q)^{-1} = x^{-1}$.

Il en résulte que R est déjà le corps de déploiement de $X^q - X$ sur $\mathbb{Z}_p$, que $R = E$ est un corps de q éléments.

□

Rappelons que l'endomorphisme de Frobenius d'un corps fini F de caractéristique p

$$Fr_F : F \to F : x \mapsto x^p$$

est un automorphisme de F, que tout corps fini est parfait. Observons encore que, si $F = F_q$, où $q = p^n$ est une puissance du nombre premier p, alors Fr_F est un automorphisme d'ordre n. Comme nous venons de montrer que tout corps fini est un corps de déploiement sur $\mathbb{Z}_p$ d'un certain polynôme, nous obtenons.

Proposition 3.4.3. *Soit $q = p^n$ une puissance du nombre premier p, $n \geqslant 1$, et soit $\mathbb{F}_q$ le corps de q éléments.*

$\mathbb{F}_q$ est une extension galoisienne du corps $\mathbb{Z}_p$, de degré n, et $\mathcal{G}al(\mathbb{F}_q/\mathbb{Z}_p)$ est un groupe cyclique d'ordre n, engendré par l'automorphisme de Frobenius de $\mathbb{F}_q$.

Regardons maintenant le groupe multiplicatif d'un corps fini. Nous allons voir qu'il est toujours cyclique. Ceci est un cas particulier du théorème suivant concernant tous les corps. (Rappelons que dans ces notes tous les corps sont supposés commutatifs.)

Théorème 3.4.4. *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

Démonstration. Soit K un corps et soit G un sous-groupe fini du groupe multiplicatif $K^\times$, disons $\#G = n$. Notons que, pour tout $x \in G$, on a $x^n = 1$ car l'ordre d'un élément d'un groupe divise l'ordre du groupe. Les n éléments de G sont donc les n racines du polynôme $X^n - 1$ dans K.

Si $n = p$ est un nombre premier, alors $G \simeq (\mathbb{Z}_p, +)$ est cyclique.

Si $n = p^r$ est une puissance du nombre premier p, alors G contient un élément d'ordre p^r, car sinon, pour tout $x \in G$, on aurait $x^{p^{r-1}} = 1$, ce qui est impossible car le polynôme $X^{p^{r-1}} - 1$ ne peut avoir p^r racines distinctes dans K. Dans ce cas ci encore G est cyclique.

En général nous procédons par induction sur le nombre de facteurs premiers distincts de n. Écrivons donc $n = n_1 n_2$, où $\text{pgcd}(n_1, n_2) = 1$ et supposons le théorème démontré pour les sous-groupes H de $K^\times$ avec $\#H = n_1$ ou n_2. Comme $\text{pgcd}(n_1, n_2) = 1$, la relation de Bezout dans $\mathbb{Z}$ nous donne des entiers $s, t \in \mathbb{Z}$ tels que $1 = sn_1 + tn_2$.

Soient $\quad G_1 = \{x \in G \mid x^{n_1} = 1\} \quad$ et $\quad G_2 = \{x \in G \mid x^{n_2} = 1\}$.

On remarque rapidement que G_1 et G_2 sont des sous-groupes de G car le groupe G est commutatif et on a :

(i) $G_1 \cap G_2 = \{1\}$ car $x \in G_1 \cap G_2 \Rightarrow x = x^{sn_1+tn_2} = (x^{n_1})^s (x^{n_2})^t = 1$.

(ii) $G_1G_2 = G$. En effet, tout $x \in G$ peut s'écrire $x = (x^{n_1})^s(x^{n_2})^t$, mais $x^{n_1} \in G_2$ car $(x^{n_1})^{n_2} = x^{n_1n_2} = 1$ et aussi $x^{n_2} \in G_1$.

(iii) Nous avons donc $G \simeq G_1 \times G_2$ et $n = \#G = \#G_1 \cdot \#G_2$.

(iv) Par ailleurs nous avons $\#G_i \leqslant n_i$ car le polynôme $X^{n_i} - 1$ a au plus n_i racines dans K.

(v) On déduit de (iii) et (iv) que $\#G_i = n_i$.

(vi) L'hypothèse d'induction nous donne alors un élément $y_1 \in G_1$ d'ordre n_1 et un élément $y_2 \in G_2$ d'ordre n_2. Il nous suffit de montrer que y_1y_2 est d'ordre n. Soit donc $t \in \mathbb{N}_0$ tel que $(y_1y_2)^t = 1$ Alors $y_1^t = (y_2^{-1})^t \in G_1 \cap G_2 = \{1\}$, d'où $y_1^t = y_2^t = 1$, ce qui montre que t est un multiple de n_1 et de n_2, t est donc un multiple de $\mathrm{ppcm}(n_1, n_2)$. Mais $\mathrm{ppcm}(n_1, n_2) = n_1n_2 = n$ car n_1 et n_2 sont premiers entre eux. On en déduit que t est un multiple de n et que y_1y_2 est d'ordre n.

□

Remarque 3.4.5. On aurait pu éviter la dernière partie de la preuve cihaut en utilisant l'isomorphisme de groupes $(\mathbb{Z}_{mn}, +) \xrightarrow{\sim} (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$ valable dès que m et n sont premiers entre eux, 2.2.9.

Remarque 3.4.6. Si G est un sous-groupe fini d'ordre n du groupe multiplicatif d'un corps K, les n éléments de G sont les racines du polynôme $X^n - 1 \in K[X]$, ce polynôme n'a donc pas de racines multiples.

Si K est un corps de caractéristique positive p, on a donc $p \nmid n$.

(En cas d'oubli de la section sur les racines multiples, on peut argumenter comme ceci (en se rappelant 0.9.5). Supposons $\mathrm{char}(K) = p$. Alors $n = pm \Rightarrow X^n - 1 = X^{pm} - 1 = (X^m)^p - 1 = (X^m - 1)^p$ dans $K[X]$, si $n = pm$, le polynôme $X^n - 1 \in K[X]$ a au plus m racines dans K.)

Corollaire 3.4.7. *Soit $q = p^n$ une puissance du nombre premier p, $n \geqslant 1$, et soit $\mathbb{F}_q$ le corps de q éléments.*

Il existe $x \in \mathbb{F}_q$ tel que $\mathbb{F}_q = \mathbb{Z}_p[x]$.

En particulier $\mathbb{Z}_p[X]$ possède un polynôme irréductible de degré n.

Démonstration. Il suffit de prendre pour x un générateur du groupe cyclique $\mathbb{F}_q^\times$. Le polynôme minimal sur $\mathbb{Z}_p$ d'un tel x sera alors le polynôme cherché.

□

– – – – – – – – – – – – – – – – –

3.4.8. Exercice. Déterminer un générateur des groupes cycliques $\mathbb{Z}_7^\times$, $\mathbb{Z}_{11}^\times$.

3.4.9. Exercice. Construire une extension de degré 2 de $\mathbb{Z}_2$ (autrement dit un corps de 4 éléments) et dessiner le graphe de son automorphisme de Frobenius.

Construire aussi un corps de 8 éléments et dessiner le graphe de son automorphisme de Frobenius.

3.4.10. Exercice. Montrer que le polynôme $X^4 + X + 1$ est irréductible dans $\mathbb{Z}_2[X]$.

Dessiner le graphe de l' automorphisme de Frobenius de $\mathbb{F}_{16}$.

3.4.11. Exercice. Montrer que $\mathbb{F}_{16}$ ne possède pas de sous-corps isomorphe à $\mathbb{F}_8$.

3.4.12. Exercice*. *Emboîtement de corps finis.* Soit $q_1 = p^{n_1}$ et $q_2 = p^{n_2}$ deux puissances du nombre premier p ($1 \leqslant n_1 \leqslant n_2$). Alors :

$$\mathbb{F}_{q_1} \hookrightarrow \mathbb{F}_{q_2} \quad \Leftrightarrow \quad n_1 \mid n_2.$$

De plus, si $n_1 \mid n_2$, $\mathbb{F}_{q_2}$ possède un et un seul sous-corps isomorphe à $\mathbb{F}_{q_1}$.

(Suggestion. Pour $\Rightarrow$, regarder les degrés.

Pour $\Leftarrow$, observer que $F = \{x \in \mathbb{F}_{q_2} \mid x^{q_1} = x\}$ est un sous-corps de $\mathbb{F}_{q_2}$. Observer aussi que, si $n_1 \mid n_2$, alors $(X^{n_1} - 1) \mid (X^{n_2} - 1)$, d'où $(q_1 - 1) \mid (q_2 - 1)$ et $(X^{q_1-1} - 1) \mid (X^{q_2-1} - 1)$. En déduire que le polynôme $(X^{q_1-1} - 1)$ se déploie dans $\mathbb{F}_{q_2}$ et que $F \simeq \mathbb{F}_{q_1}$ est le seul corps de $\mathbb{F}_{q_2}$ comprenant q_1 éléments.)

3.4.13. Exercice. Soit p un nombre premier et soit n un naturel non divisible par p.

Montrer qu'il existe une extension finie $\mathbb{F}$ de $\mathbb{Z}_p$ dont le groupe multiplicatif comprend un élément d'ordre exactement n. (Un tel élément sera appelé racine primitive $n^{\text{ième}}$ de l'unité dans F.)

(Indication : utiliser un corps de déploiement du polynôme $X^n - 1$ sur $\mathbb{Z}_p$ et le fait que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.)

3.4.14. Exercice. Soit p un nombre premier impair et soit $\mathbb{F}$ une extension de $\mathbb{Z}_p$ dont le groupe multiplicatif $\mathbb{F}^\times$ possède un élément α d'ordre 8.

Observer : $1+\alpha+\cdots+\alpha^7 = 0$, $1+\alpha^2+\alpha^4+\alpha^6 = 0$, $\alpha+\alpha^3+\alpha^5+\alpha^7 = 0$.
Montrer : $\alpha^4 = \alpha^{-4} = -1$, $\quad (\alpha^2 + \alpha^{-2})^2 = 0$, $\quad \alpha^2 + \alpha^{-2} = 0$.

Poser $y = \alpha + \alpha^{-1}$
Montrer : $y^2 = 2$. Montrer aussi :

$$p \cong \pm 1 \text{ modulo } 8 \Rightarrow y^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = y \Rightarrow y \in \mathbb{Z}_p,$$

$$p \cong \pm 3 \text{ modulo } 8 \Rightarrow y^p = \alpha^3 + \alpha^{-3} = \alpha^3 + \alpha^5 = -y \Rightarrow y \notin \mathbb{Z}_p$$

Se rappeler le symbole de Legendre et conclure

$$\left(\frac{2}{p}\right) = 1 \quad \Leftrightarrow \quad p \cong \pm 1 \text{ modulo } 8.$$

Retrouver la formule $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

3.4.15. Exercice. Soit Ω_p une extension algébriquement close de $\mathbb{Z}_p$.

Montrer que $\tilde{\mathbb{Z}}_p = \{x \in \Omega_p \mid \exists r \in \mathbb{N}_0 \quad x^{p^r} = x\}$ est un sous-corps algébriquement clos de Ω_p.

3.5 Racines de l'unité, Indicateur d'Euler

Convention de section. Dans cette section, K désigne toujours un corps.

Définitions et observations 3.5.1. Soit $a \in K$.

On dit que a est une **racine de l'unité** dans K s'il existe $m \in \mathbb{N}_0$ tel que $a^m = 1$, autrement dit si a est un élément d'ordre fini du groupe multiplicatif $K^\times$..

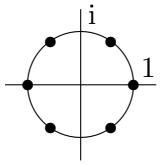
Les racines de l'unité de K forment un sous-groupe du groupe multiplicatif $K^\times$, nous le désignerons par μ^K.

On dit que a est une **racine $n^{\text{ième}}$ de l'unité** dans K si $a^n = 1$.

Les racines $n^{\text{ièmes}}$ de l'unité de K forment un sous-groupe du groupe μ^K, nous le désignerons par μ_n^K.

On dit que a est une **racine primitive $n^{\text{ième}}$ de l'unité** dans K si a est un élément d'ordre n du groupe multiplicatif $K^\times$.

Exemple 3.5.2. (a) Voici les racines $6^{\text{ièmes}}$ de l'unité dans le plan complexe



(b) Le groupe $\mu_n^{\mathbb{C}}$ est un groupe cyclique d'ordre n, $e^{\frac{2\pi i}{n}}$ en est un générateur.

Remarques 3.5.3. (i) Quel que soit le corps K, les groupes μ_n^K sont des sous-groupes finis du groupe multiplicatif $K^\times$: on a $\#\mu_n^K \leqslant n$ car le polynôme $X^n - 1$ a au plus n racines dans K. Les groupes μ_n^K sont toujours des groupes cycliques, 3.4.4.

On peut même montrer que $\#\mu_n^K \mid n$ (voir l'exercice 3.5.18).

(ii) Si G est un sous-groupe fini d'ordre n du groupe multiplicatif $K^\times$, alors $G \subseteq \mu_n^K$ car l'ordre d'un élément divise l'ordre du groupe et, comme $n = \#G \leqslant \#\mu_n^K \leqslant n$, on a même l'égalité $G = \mu_n^K$.

Comme les n éléments de G sont les racines du polynôme $X^n - 1 \in K[X]$, ce polynôme n'a pas de racines multiples. Si K est un corps de caractéristique positive p, on en déduit $p \nmid n$.

(En cas d'oubli de la section sur les racines multiples, on peut argumenter comme ceci (en se rappelant 0.9.5). Supposons $\mathrm{char}(K) = p$. Alors $n = pm \Rightarrow X^n - 1 = X^{pm} - 1 = (X^m)^p - 1 = (X^m - 1)^p$ dans $K[X]$, si $n = pm$, le polynôme $X^n - 1 \in K[X]$ a au plus m racines dans K.)

Occupons-nous maintenant des racines primitives $n^{\text{ièmes}}$ de l'unité d'un corps K quand elles existent. Il peut être utile de les reconnaître, et aussi de les compter.

Observation 3.5.4. Soit K un corps et $n \in \mathbb{N}_0$. Les conditions suivantes sont équivalentes.

(i) K possède une racine primitive $n^{\text{ième}}$ de l'unité.

(ii) μ_n^K est un groupe cyclique d'ordre n, isomorphe au groupe $(\mathbb{Z}_n, +)$. Dans cet isomorphisme, les racines primitives $n^{\text{ièmes}}$ de l'unité correspondent aux générateurs du groupe $(\mathbb{Z}_n, +)$

(iii) Le polynôme $X^n - 1$ se déploie dans K et toutes ses racines sont simples.

(iv) Le polynôme $X^n - 1$ se déploie dans K et, si K est de caractéristique positive p, $p \nmid n$.

La proposition suivante a sans doute été observée au premier cours d'algèbre.

Proposition 3.5.5. *Soit $n \in \mathbb{N}_0$ et $a \in \mathbb{Z}_n$. Les conditions suivantes sont équivalentes.*

(i) a est un générateur du groupe $(\mathbb{Z}_n, +)$,

(ii) $\operatorname{pgcd}(a, n) = 1$,

(iii) a est un inversible de l'anneau $(\mathbb{Z}_n, +, \cdot)$.

Rappelons un cas particulier très utile de 2.2.9.

Proposition 3.5.6. *Soit m et n deux entiers naturels positifs premiers entre eux.*

L'homomorphisme naturel $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_m, +, \cdot) \times (\mathbb{Z}_n, +, \cdot)$ induit un isomorphisme d'anneaux

$$(\mathbb{Z}_{mn}, +, \cdot) \xrightarrow{\sim} (\mathbb{Z}_m, +, \cdot) \times (\mathbb{Z}_n, +, \cdot).$$

et un isomorphisme de groupes multiplicatifs

$$\mathbb{Z}_{mn}^{\times} \xrightarrow{\sim} \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}.$$

Définition 3.5.7. L'indicateur d'Euler d'un nombre naturel positif n est défini par

$$\varphi(n) = \#\{a \in \mathbb{N} \mid 0 \leqslant a < n \text{ et } \operatorname{pgcd}(a, n) = 1\}.$$

3.5.8. Propriétés. (i) Soient p un premier naturel et $r \in \mathbb{N}_0$. On a

$$\varphi(p) = (p - 1), \qquad \varphi(p^r) = (p^r - p^{r-1}) = (p - 1)p^{r-1}.$$

(ii)Si $\operatorname{pgcd}(m, n) = 1$, alors $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Ceci s'exprime en disant que l'indicateur d'Euler est faiblement multiplicatif.

– – – – – – – – – – – – – – – – –

3.5.9. Exercice*. Soit $n > 1$ un entier naturel et soit $\psi = e^{\frac{2\pi i}{n}}$. Ce nombre ψ est donc une racine primitive $n^{\text{ième}}$ de l'unité dans le corps des complexes. Observer :

$$X^n - 1 = \prod_{i=0}^{n-1}(X - \psi^i), \quad X^{n-1} + X^{n-2} + \cdots + X + 1 = \prod_{i=1}^{n-1}(X - \psi^i),$$

$$n = \prod_{i=1}^{n-1}(1 - \psi^i).$$

3.5.10. Exercice*. Soit $n > 1$ un entier naturel et soit $a \in \mathbb{Z}_n$.

Calculer l'ordre de a dans le groupe $(\mathbb{Z}_n, +)$ en fonction de a et de n.

3.5.11. Exercice*. Soit $r > 1$ un entier naturel et soit p un premier naturel.

Montrer que l'élément $(p^{r-1} + 1)$ du groupe $\mathbb{Z}_{p^r}^\times$ est d'ordre p.

Soit encore $n > 1$ un entier naturel divisible par p^2. Montrer que le groupe $\mathbb{Z}_n^\times$ comprend aussi un élément d'ordre p.

3.5.12. Exercice. (a) Calculer l'indicateur d'Euler des nombres 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 55, 64, 10000, etc.

(b) Déterminer toutes les valeurs de n pour lesquelles
$\varphi(n) = 5, \quad \varphi(n) = 6, \quad \varphi(n) = 8, \quad \varphi(n) = 20.$
(Solution partielle : les valeurs demandées se trouvent parmi les nombres 2, 5, 7, 8, 9, 14, 15, 16, 18, 20, 24, 25, 30, 33, 44, 50, 55, 66.)

3.5.13. Exercice*. (a) Si $n > 2$, $\varphi(n)$ est pair.

(b) Si le nombre naturel n est impair, alors $\varphi(2n) = \varphi(n)$.
Si le nombre naturel n est pair, alors $\varphi(2n) = 2\varphi(n)$.

(c) $d \mid n \Rightarrow \varphi(d) \mid \varphi(n)$.

La réciproque est fausse, on a par exemple $\varphi(44) = 20 = \varphi(25)$.

3.5.14. Exercice. Soit $\text{Prem}_n = \{k \in \mathbb{N} \mid 0 \leqslant k < n \text{ et } \text{pgcd}(k, n) = 1\}$. On a, $\forall n \in N, n > 2$

$$\sum_{k \in \text{Prem}_n} k \cong 0 \text{ modulo } n.$$

3.5.15. Exercice. Une généralisation du petit théorème de Fermat, due à Julien Meyer (étudiant au Bac 2 en mathématiques à l'ULB, mars 2009).

Pour tous entiers naturels positifs a et n premiers entre eux, on a

$$a^{\varphi(n)} - 1 \text{ est divisible par } n.$$

3.5.16. Exercice*. Soit $\mu^{\mathbb{C}} = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}_0, z^n = 1\}$; $\mu^{\mathbb{C}}$ est un sous-groupe du groupe $\mathbb{C}^\times$.

Établir un isomorphisme entre les groupe $(\mu^{\mathbb{C}}, .)$ et $(\mathbb{Q}/\mathbb{Z}, +)$.

(Indication : utiliser une restriction de l'homomorphisme de groupes
$(\mathbb{R}, +) \to (\mathbb{C}^\times, .) : x \mapsto e^{2\pi i x}$.)

3.5.17. Exercice*. Soit $\alpha, \beta \in \mu^{\mathbb{C}}$, où α est d'ordre m et β d'ordre n, donc

$$gr(\alpha) = \mu_m^{\mathbb{C}} \quad \text{et} \quad gr(\beta) = \mu_n^{\mathbb{C}}.$$

(a) Si $\text{pgcd}(m, n) = 1$, alors $\quad gr(\alpha) \cap gr(\beta) = \{1\}$

$$\text{et} \quad gr(\alpha \cdot \beta) = gr(\alpha, \beta) = \mu_{mn}^{\mathbb{C}}.$$

(b) Pour tous $d, n \in \mathbb{N}_0$, on a : $\quad d \mid n \Leftrightarrow \mu_d^{\mathbb{C}} \subset \mu_n^{\mathbb{C}}$.

(c) Soit $d = \text{pgcd}(m, n)$ et $r = \text{ppcm}(m, n)$. On a

$$\mu_m^{\mathbb{C}} \cap \mu_n^{\mathbb{C}} = \mu_d^{\mathbb{C}} \quad \text{et} \quad gr(\alpha, \beta) = \mu_m^{\mathbb{C}} \mu_n^{\mathbb{C}} = \mu_r^{\mathbb{C}}.$$

(d) Si m est impair, alors $(-\alpha)$ est un élément de $\mu^{\mathbb{C}}$ d'ordre $2m$.

3.5.18. Exercice*. Pour tout corps K on a : $\quad \#\mu_n^K \mid n$.

(Suggestion : utiliser une extension convenable de K.)

3.6 Les corps cyclotomiques

Un **corps cyclotomique** est un corps de nombres engendré sur $\mathbb{Q}$ par une racine de l'unité dans $\mathbb{C}$.

3.6.1. Soit donc γ une racine de l'unité dans $\mathbb{C}$ et soit n l'ordre de γ dans le groupe $(\mathbb{C}^\times, \cdot)$. Notre γ est une racine primitive $n^{\text{ième}}$ de l'unité dans $\mathbb{C}$ et le corps cyclotomique $\mathbb{Q}[\gamma]$ contient $\mu_n^{\mathbb{C}}$. Ainsi $\mathbb{Q}[\gamma] = \mathbb{Q}[\mu_n^{\mathbb{C}}]$ et $\mathbb{Q}[\gamma]$ est le corps de déploiement sur $\mathbb{Q}$ du polynôme $X^n - 1$. Les corps cyclotomiques sont donc des extensions normales et galoisiennes de $\mathbb{Q}$.

Nous allons déterminer le degré de l'extension $\mathbb{Q}[\gamma]$ de $\mathbb{Q}$ et le polynôme minimal de γ sur $\mathbb{Q}$. Nous verrons que deux racines primitives $n^{\text{ièmes}}$ de l'unité ont même polynôme minimal sur $\mathbb{Q}$ et regarderont certaines propriétés de ce polynôme minimal.

Nous regarderons aussi le groupe des automorphismes de $\mathbb{Q}[\gamma]$.

Nous attaquerons ce problème par la bande.

Définition 3.6.2. Soit $n \in \mathbb{N}_0$ et soit $\mathrm{Prim}(n)$ l'ensemble des racines primitives $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$.

Le $n^{\text{ième}}$ polynôme cyclotomique est défini par

$$\Phi_n = \prod_{\gamma \in \mathrm{Prim}(n)} (X - \gamma).$$

Exemples 3.6.3.

$$\begin{array}{rcc} \Phi_1 & = & X - 1 \\ \Phi_2 & = & X + 1 \\ \Phi_3 & = & X^2 + X + 1 \\ \Phi_4 & = & X^2 + 1 \\ \Phi_5 & = & X^4 + X^3 + X^2 + X + 1 \\ \Phi_6 & = & X^2 - X + 1 \end{array}$$

Remarques 3.6.4. (i) $\deg(\Phi_n) = \varphi(n)$, où $\varphi(n)$ est l'indicateur d'Euler.

$$(ii) X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \prod_{d|n, d \neq n} \Phi_d.$$

$$n = \sum_{d|n} \varphi(d).$$

(iii) Si n=p est un premier naturel, on a

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1$$

De plus Φ_p est un polynôme irréductible de $\mathbb{Z}[X]$ et de $\mathbb{Q}[X]$ (cf. 2.3.8).

Donc Φ_p est le polynôme minimal des racines primitives $p^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$.

Voyons maintenant ce que nous pouvons dire des Φ_n pour un entier naturel n quelconque.

Proposition 3.6.5. *Φ_n est un polynôme unitaire à coefficients dans $\mathbb{Z}$.*

Démonstration. Par induction sur n, en utilisant la deuxième des remarques précédentes. □

Proposition 3.6.6. *Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Soit γ une racine primitive $n^{\text{ième}}$ de l'unité dans $\mathbb{C}$ et soit F le polynôme minimal de γ sur $\mathbb{Q}$; rappelons 2.3.5, F est un polynôme unitaire de $\mathbb{Z}[X]$. Comme $\Phi_n(\gamma) = 0$, on a que $F \mid \Phi_n$ dans $\mathbb{Q}[X]$ et

$$\Phi_n = F \cdot G$$

pour un autre polynôme unitaire $G \in \mathbb{Q}[X]$; on a même $G \in \mathbb{Z}[X]$ car F est unitaire.

Nous devons montrer que $\Phi_n = F$, autrement dit que toute racine primitive $n^{\text{ième}}$ de l'unité γ' dans $\mathbb{C}$ est une racine de F. Rappelons que les racines primitives $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$ sont de la forme γ^k, où $\text{pgcd}(k, n) = 1$. Il suffit donc de montrer que, pour tout nombre premier naturel p *ne divisant pas* n, γ^p est encore une racine de F.

Soit donc p un premier naturel ne divisant pas n. Pour montrer que γ^p est une racine de F nous procédons par l'absurde. Supposons que γ^p n'est pas une racine de F. Alors γ^p est une racine de G. Introduisons un nouveau polynôme G_1 défini par $G_1(X) = G(X^p)$. Comme γ^p est une racine de G on a que γ est une racine de G_1. Les polynômes F et G_1 ont donc une racine commune dans $\mathbb{C}$, ils ne sont pas premiers entre eux et leur pgcd H est un polynôme de degré positif. Comme le pgcd de F et G_1 peut se calculer par divisions successives et comme F et G_1 sont des polynômes unitaires de $\mathbb{Z}[X]$, on remarque avec 2.3.3 que H est un polynôme unitaire de $\mathbb{Z}[X]$ et qu'on a

$$F = H \cdot F' \qquad G_1 = H \cdot G_1'$$

où $F', G_1' \in \mathbb{Z}[X]$ où $F', G_1' \in \mathbb{Z}[X]$.

Réduisons tout ceci modulo p, désignons par $\overline{(\cdot)}$ les images modulo p. Dans l'anneau de polynômes $\mathbb{Z}_p[X]$ nous avons

$$\overline{F} = \overline{H} \cdot \overline{F}' \qquad \overline{G}_1 = \overline{H} \cdot \overline{G}_1' \qquad \text{et aussi} \qquad \overline{G}_1 = \overline{G}^p$$

en vertu du petit théorème de Fermat (0.9.2). Les polynômes $\overline{F}$ et $\overline{G}_1$, ayant un facteur commun $\overline{H}$ de degré positif, ont une racine commune ξ dans une extension convenable de $\mathbb{Z}_p$. Mais alors cette racine commune ξ est aussi une racine de $\overline{G}$ et ξ est une racine multiple du polynôme $\overline{\Phi}_n = \overline{F} \cdot \overline{G} \in \mathbb{Z}_p[X]$. Or ceci est impossible car $\overline{\Phi}_n \mid X^n - 1$ et le polynôme $X^n - 1$ n'a que des racines simples dans toute extension de $\mathbb{Z}_p$ (3.2.14) puisque $p \nmid n$. Cette contradiction termine la preuve. □

Corollaire 3.6.7. *Les racines primitives $n^{ièmes}$ de l'unité dans $\mathbb{C}$ ont toutes Φ_n pour polynôme minimal.*

Corollaire 3.6.8. *Soit γ une racine primitive $n^{ième}$ de l'unité dans $\mathbb{C}$.*

$\mathbb{Q}[\gamma]$ est le corps de déploiement sur $\mathbb{Q}$ du polynôme irréductible Φ_n, et $[\mathbb{Q}[\gamma] : \mathbb{Q}] = \varphi(n)$.

Le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}[\gamma]$ est d'ordre $\varphi(n)$.

Quand σ parcourt l'ensemble des $\mathbb{Q}$-automorphismes de $\mathbb{Q}[\gamma]$, $\sigma(\gamma)$ parcourt l'ensemble des racines primitives $n^{ièmes}$ de l'unité.

Soit p un nombre premier naturel et ψ une racine primitive $p^{\text{ième}}$ de l'unité dans $\mathbb{C}$. En utilisant les normes et les traces nous pourrons montrer en 3.6.14 que l'anneau des entiers du corps cyclotomique $\mathbb{Q}[\psi]$ est l'anneau $\mathbb{Z}[\psi]$.

– – – – – – – – – – – – – – – – –

3.6.9. Exercice. Calculer Φ_8, Φ_9, Φ_{15}.

3.6.10. Exercice. Soit $2 < n \in \mathbb{N}_0$. Alors

$\Phi_n(0) = 1$, le terme indépendant de Φ_n est 1.

3.6.11. Exercice. Parmi les corps cyclotomiques quels sont ceux qui sont quadratiques ?

3.6.12. Exercice*. Soit $n \in \mathbb{N}_0$. Introduisons les notations $\alpha_n = e^{\frac{2\pi i}{n}}$ et $\mathbb{Q}_n = \mathbb{Q}[\alpha_n]$.

(a) Décrire le groupe des automorphismes de $\mathbb{Q}_5$, de $\mathbb{Q}_7$, de $\mathbb{Q}_8$.

(b) Montrer : $\mathcal{G}al(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$.

3.6.13. Exercice. Utilisons les notations de l'exercice précédent.

(a) $d \mid n \Rightarrow \mathbb{Q}_d \subset \mathbb{Q}_n$.

(b) Si n est impair, $\mathbb{Q}_n = \mathbb{Q}_{2n}$.

(c) Si $n = p$ est un premier impair, $\mu^{\mathbb{C}} \cap \mathbb{Q}_p = \mu_{2p}^{\mathbb{C}}$.

3.6.14. Exercice. *L'anneau des entiers des corps cyclotomiques.*

Soit p un nombre premier naturel et soit ψ une quelconque racine primitive $p^{\text{ième}}$ de l'unité dans $\mathbb{C}$. Nous nous proposons de montrer que l'anneau des entiers $\mathcal{O}_p := \mathcal{O}_{\mathbb{Q}[\psi]}$ du corps cyclotomique $\mathbb{Q}_p = \mathbb{Q}[\psi]$ est exactement $\mathbb{Z}[\psi]$ (on sait déjà que $\mathbb{Z}[\psi] \subset \mathcal{O}_p$).

Nous utiliserons la trace et la norme et nous écrirons Tr et N pour $\mathrm{Tr}_{\mathbb{Q}[\psi]/\mathbb{Q}}$ et $N_{\mathbb{Q}[\psi]/\mathbb{Q}}$.

Rappelons d'abord que les $\psi^i, 1 \leqslant i \leqslant p-1$, sont toutes les racines primitives $p^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$, qu'elles ont toutes le même polynôme minimal sur Q, à savoir le polynôme cyclotomique

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{i=1}^{p-1}(X - \psi^i).$$

Les ψ^i sont donc conjugués deux à deux et nous pouvons numéroter les $p-1$ automorphismes de $\mathbb{Q}_p$ de façon que $\sigma_i(\psi) = \psi^i$ (cf. 3.6.7).

Traçons maintenant notre chemin.

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

(ii) Pour $1 \leqslant i \leqslant p-1$, on a $N(1-\psi^i) = p$.

Les nombres $(1-\psi^i)$ sont irréductibles dans $\mathcal{O}_p$ et deux à deux associés dans $\mathcal{O}_p$,

car on a $(1-\psi) \mid (1-\psi^i) = (1-\psi)(1+\psi+\cdots\psi^{i-1})$ et, en permutant les rôles de ψet ψ^i, on a aussi $(1-\psi^i) \mid (1-\psi)$.)

(iii) $(1-\psi)\mathcal{O}_p \cap \mathbb{Z} = p\mathbb{Z}$.

(Avec (i) on a $p\mathbb{Z} \subset (1-\psi)\mathcal{O}_p \cap \mathbb{Z}$. Si cette inclusion était stricte on aurait $(1-\psi)\mathcal{O}_p \cap \mathbb{Z} = \mathbb{Z}$, ce qui est impossible car $(1-\psi)$ n'est pas inversible dans $\mathcal{O}_p$.)

(iv) $\mathrm{Tr}(1) = p-1, \quad \mathrm{Tr}(\psi) = -1, \quad \mathrm{Tr}(1-\psi) = p$

et pour $1 \leqslant i \neq j \leqslant p-1$, $\mathrm{Tr}(\psi^i) = -1$, d'où $\mathrm{Tr}(\psi^i - \psi^j) = 0$.

(v) Pour tout $\gamma \in \mathcal{O}_p$, on a $\mathrm{Tr}(\gamma(1-\psi)) \in p\mathbb{Z}$.

$$(\mathrm{Tr}(\gamma(1-\psi)) = \sum_{1 \leqslant i \leqslant p-1} \sigma_i(\gamma)(1-\psi^i) \in (1-\psi)\mathcal{O}_p \cap \mathbb{Z} = p\mathbb{Z}.)$$

(vi) Les nombres $1, \psi, \psi^2, \cdots, \psi^{p-2}$ forment une base de $\mathbb{Q}_p$ sur $\mathbb{Q}$.

(vii) Si $\gamma = a_0 + a_1\psi + \cdots + a_{p-2}\psi^{p-2} \in \mathcal{O}_p$ $(a_i \in \mathbb{Q})$, alors les $a_i \in \mathbb{Z}$.

(Commençons par montrer que $a_0 \in \mathbb{Z}$.
On a $\quad \gamma(1-\psi) = a_0(1-\psi) + a_1(\psi-\psi^2) + \cdots + a_{p-2}(\psi^{p-2} - \psi^{p-1})$.

D'où $\quad \mathrm{Tr}(\gamma(1-\psi)) = a_0\mathrm{Tr}(1-\psi) = pa_0$, comme $\quad \mathrm{Tr}(\gamma(1-\psi)) \in p\mathbb{Z}$ on a $\quad pa_0 \in p\mathbb{Z} \quad$ et $\quad a_0 \in \mathbb{Z}$.

On a $(\gamma - a_0)\psi^{-1} \in \mathcal{O}_p$ car $\psi^{-1} = \psi^{p-1} \in \mathcal{O}_p$

$$\text{comme } (\gamma - a_0)\psi^{-1} = a_1 + a_2\psi + \cdots + a_{p-2}\psi^{p-3},$$

on en déduit avec ce qui précède que $a_1 \in \mathbb{Z}$. En itérant le procédé on obtient que tous les $a_i \in \mathbb{Z}$.)

(viii) Conclusion : $\quad \mathcal{O}_p = \mathbb{Z}[\psi]$.

3.7 Les nombres pseudo-premiers

Rappelons le petit théorème de Fermat 0.9.2.

Théorème 3.7.1. *Si p est un premier naturel, alors*

$$\forall a \in \mathbb{Z} \text{ tel que } \mathrm{pgcd}(a,p) = 1 \text{ on a } \quad a^{p-1} \cong 1 \text{ modulo } p.$$

On peut se demander si cette propriété des nombres premiers les caractérise, si elle peut fournir un test de primalité. En fait il n'en est rien, ce qui nous amène à formuler une définition.

Définition 3.7.2. Le nombre naturel $n > 1$ est dit **pseudo-premier ou nombre de Carmichael** s'il n'est pas premier et s'il a la propriété suivante :

$$\forall a \in \mathbb{Z} \text{ tel que } \mathrm{pgcd}(a,n) = 1 \text{ on a } \quad a^{n-1} \cong 1 \text{ modulo n.}$$

La propriété pour un nombre naturel n d'être pseudo-premier est en fait une propriété de l'anneau $\mathbb{Z}_n$ des entiers modulo n, et même, au vu de 3.5.5, une propriété du groupe $\mathbb{Z}_n^\times$.

Remarque 3.7.3. *Le nombre naturel $n > 1$ est pseudo-premier si et seulement si l'ordre de tout élément du groupe $\mathbb{Z}_n^\times$ divise $n-1$.*

Mais l'ordre du groupe $\mathbb{Z}_n^\times$ est donné par l'indicateur d'Euler $\varphi(n)$, 3.5.7, que nous pouvons calculer en fonction de la factorisation de n en produit de premiers. Il vient :

Proposition 3.7.4. *Un nombre pseudo-premier n'a pas de facteur carré.*

Démonstration. Soit n un naturel divisible par le carré du nombre premier p. Alors $p \mid \varphi(n)$, (voir 3.5.8), et le groupe $\mathbb{Z}_n^\times$ comprend un élément d'ordre p, (voir 2.2.12 ou 3.5.11). Comme $p \nmid (n-1$ le nombre n n'est pas pseudo-premier. □

Voici maintenant un critère de pseudo-primalité.

Proposition 3.7.5. *(Korselt, 1899) Soit $p_1, \cdots, p_k$ des nombres premiers distincts deux-à-deux, $k > 1$, et soit $n = p_1 \cdots p_k$. Ce nombre n est pseudo-premier si et seulement si*

$$\forall i, \quad 1 \leqslant i \leqslant k, \quad (p_i - 1) \mid (n-1).$$

Démonstration. La structure du groupe $\mathbb{Z}_n^\times$ est connue, avec (3.5.6) nous avons

$$\mathbb{Z}_n^\times \simeq \prod_{1 \leqslant i \leqslant k} \mathbb{Z}_{p_i}^\times$$

Et, comme les groupes $\mathbb{Z}_{p_i}^\times$ sont d'ordre $(p_i - 1)$, l'ordre de tout élément du groupe $\mathbb{Z}_n^\times$ divise $\text{ppcm}((p_1 - 1), (p_2 - 1), \cdots, (p_k - 1))$.

Mais si n satisfait la condition de la proposition, on a

$$\text{ppcm}((p_1 - 1), (p_2 - 1), \cdots, (p_k - 1)) \mid n - 1$$

et on en déduit via 3.7.3 que n est pseudo-premier.

On sait aussi que les groupes $\mathbb{Z}_{p_i}^\times$ sont cycliques d'ordre $(p_i - 1)$, 3.4.4, donc le groupe $\mathbb{Z}_n^\times$ comprend des éléments d'ordre $(p_i - 1)$. Si donc n est pseudo-premier, il satisfait via 3.7.3 la condition de la proposition.

□

Remarque 3.7.6. En reformulant la condition en 3.7.5 on obtient un critère assez rapide à vérifier.

Le nombre naturel $n > 1$ est pseudo-premier si et seulement

$$\forall i, \quad 1 \leqslant i \leqslant k, \qquad n \cong 1 \text{ modulo}(p_i - 1).$$

Corollaire 3.7.7. *(i) Les nombres pseudo-premiers sont impairs.*

(ii) Les nombres pseudo-premiers ont au moins trois facteurs premiers.

Démonstration. (i) Un nombre pair $n > 2$ sans facteur carré a un facteur premier p impair et le nombre pair $(p - 1)$ ne peut diviser le nombre impair $(n - 1)$.

(ii) Si $n = pq$, où $p < q$ sont des premiers impairs, alors
$n \cong p \text{ modulo}(q - 1)$ et $n \ncong 1 \text{ modulo}(q - 1)$. □

Il semble que Carmichael fut le premier à exhiber un nombre pseudo-premier, en 1910 il montra le plus petit pseudo-premier, à savoir le nombre $3 \times 11 \times 17$

Avec (3.7.6) on peut vérifier assez rapidement que les nombres $5 \times 13 \times 17$ et $7 \times 11 \times 13 \times 41$ sont aussi pseudo-premiers.

En 1994 on a pu montrer qu'il existe une infinité de nombres pseudo-premiers, bien que ceux-ci soient assez rares.

Chapitre 4

Les entiers d'un corps de nombres

Le but de ce dernier chapitre est l'étude de la factorisation des idéaux dans l'anneau des entiers d'un corps de nombres. Le cours se terminant, celle-ci sera malheureusement assez incomplète et nous n'aurons guère l'occasion d'en tirer avantage.

Comme d'habitude, il nous faut commencer par rassembler quelques outils. Nos exemples seront principalement pris parmi les corps quadratiques.

4.1 Le premier langage des idéaux

Comme l'anneau des entiers d'un corps de nombres est noethérien, 2.4.18, on peut montrer que tout élément non nul non inversible d'un tel anneau est produit d'un nombre fini d'éléments irréductibles de A (cf. 2.1.9). Malheureusement cette factorisation n'est généralement pas unique. C'est en tentant de remédier à cette situation que Kummer et Dedekind ont introduit la notion d'idéal. Pour cette raison il est utile de s'intéresser non pas tant aux éléments d'un anneau A mais bien à ses idéaux, et de faire avec ceux-ci ce que nous faisions avec les nombres

4.1.1. Rappelons qu'un idéal propre d'un anneau A est un idéal de A distinct de A, autrement dit un idéal ne comprenant pas d'éléments inversibles de A.

La notion d'idéal propre peut donc être vue comme une généralisation de la notion d'élément non inversible.

Parmi les idéaux d'un anneau, certains se comportent un peu comme les nombres premiers.

Définitions 4.1.2. Un idéal $\mathfrak{P}$ d'un anneau A est dit **premier** si $\mathfrak{P}$ est un idéal propre et si, $\forall x, y \in A$,

$$xy \in \mathfrak{P} \Rightarrow x \in \mathfrak{P} \text{ ou } y \in \mathfrak{P}.$$

Un idéal $\mathfrak{M}$ d'un anneau A est dit **maximal** si $\mathfrak{M}$ est un idéal propre de A maximal parmi les idéaux propres de A.

Exemple 4.1.3. (i) Dans un domaine A, un idéal principal non nul pA est premier si et seulement p est un élément premier de A.

Dans un domaine principal A, les idéaux premiers non nuls sont exactement les idéaux engendrés par un élément premier, ce sont aussi les idéaux maximaux de A.

(ii) L'idéal nul de l'anneau A est premier si et seulement si A est intègre.

(iii) Dans l'anneau $K[X, Y]$ des polynômes en deux indéterminées X et Y à coefficient dans un corps K, l'idéal (X) est un idéal premier non maximal.

Rappelons que tous les anneaux et corps considérés ici sont supposés être commutatifs. Et insistons.

Proposition 4.1.4. *(i) Un idéal $\mathfrak{P}$ d'un anneau commutatif A est premier si et seulement si l'anneau quotient $A/\mathfrak{P}$ est intègre.*

(ii) Un idéal $\mathfrak{M}$ d'un anneau commutatif A est maximal si et seulement si l'anneau quotient $A/\mathfrak{M}$ est un corps.

(iii) Tout idéal maximal d'un anneau commutatif est premier.

Démonstration. (i) Cette preuve, en tout point semblable à celle de 0.5.10, est laissée à titre d'exercice.

(ii) Il suffit d'utiliser la bijection entre l'ensemble des idéaux de A contenant $\mathfrak{M}$ et l'ensemble des idéaux du quotient $A/\mathfrak{M}$ fournie par l'homomorphisme naturel

$$A \to A/\mathfrak{M}$$

en se rappelant qu'un corps commutatif est un anneau commutatif non nul dont l'idéal nul est le seul idéal propre.

(iii) Conséquence directe de (i) et (ii). □

Regardons maintenant les idéaux premiers de l'anneau des entiers d'un corps de nombres, la situation y est à peu près la même que dans les domaines principaux.

Proposition 4.1.5. *Soit $\mathfrak{P}$ un idéal premier non nul de l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres K.*

Alors $\mathfrak{P}$ est un idéal maximal de $\mathcal{O}_K$ et le quotient $\mathcal{O}_K/\mathfrak{P}$ est un corps fini.

Démonstration. Observons que $\mathfrak{P} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, propre ($1 \notin \mathfrak{P}$), et non nul (1.2.25). Donc $\mathfrak{P} \cap \mathbb{Z} = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}, n \neq 0, 1$ et l'injection naturelle de $\mathbb{Z}$ dans $\mathcal{O}_K$ induit un homomorphisme injectif

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{P}.$$

Comme $O_K/\mathfrak{P}$ est intègre, il en est de même de $\mathbb{Z}/n\mathbb{Z}$, donc $n = p$ est un nombre premier naturel. Comme $\mathcal{O}_K$ est entier sur $\mathbb{Z}$, $O_K/\mathfrak{P}$ est entier sur $\mathbb{Z}/p\mathbb{Z}$ qui est un corps. On en déduit avec 1.2.20 que $O_K/\mathfrak{P}$ est un corps, on en déduit ensuite avec 4.1.4 que l'idéal $\mathfrak{P}$ est maximal. D'autre part on sait avec 2.4.11 que $O_K/\mathfrak{P}$ est fini. □

Les idéaux premiers et plus spécialement les idéaux maximaux d'un anneau commutatif quelconque jouent un rôle très important. Leur existence est donc essentielle. Pour la montrer en général, nous aurons besoin de quelques notions de la théorie des ensembles.

Commençons par quelques préambules sur les ensembles ordonnés.

Définitions 4.1.6. (i) Un élément x d'un ensemble ordonné $(E, \prec)$ est dit **maximal** si, $\forall y \in E, \quad x \prec y \Rightarrow x = y$.

(ii) Une **chaîne** dans un ordonné $(E, \prec)$ est une partie C de E telle que, $\forall x, y \in C$ on a $x \prec y$ ou $y \prec x$.

(iii) Nous dirons qu'un élément x d'un ordonné $(E, \prec)$ **majore** la partie P de E si, $\forall p \in P$, $p \prec x$. Nous dirons aussi que la partie P de E est majorée si $\{x \in E \mid x \text{ majore } P\} \neq \varnothing$.

(iv) Un **inductif** est un ordonné non vide dont toute chaîne est majorée.

Remarques 4.1.7. Dans un ordonné, un élément maximal n'est pas forcément un maximum. Par exemple, dans l'ordonné par inclusion $(\mathcal{I}_\mathbb{Z}, \subset)$ des idéaux propres de l'anneau des entiers $\mathbb{Z}$, les idéaux maximaux sont les idéaux $p\mathbb{Z}$, où p est un nombre premier. Mais aucun d'entre eux n'est un maximum de $\mathcal{I}_\mathbb{Z}$.

En algèbre, il est difficile de se passer de l'axiome du choix 0.2.6. Il en existe plusieurs formulations, toutes équivalentes dans la théorie classique des ensembles. Une des plus connues est connue sous le nom de lemme, la voici.

Lemme 4.1.8. *(Lemme de Zorn). Tout inductif possède un maximal.*

Voici maintenant un fait simple mais fondamental.

Proposition 4.1.9. *Tout idéal propre $\mathfrak{A}$ d'un anneau A est contenu dans un idéal maximal de A.*

Démonstration. Soit $\mathfrak{A}$ un idéal propre de A. L'anneau A est donc non nul et son élément 1 n'appartient à aucun idéal propre.

Il suffit de montrer que l'ordonné par inclusion $\mathcal{I}_{\mathfrak{a}}$ des idéaux propres de l'anneau A contenant l'idéal $\mathfrak{A}$ est un inductif ; un maximal de $\mathcal{I}_{\mathfrak{a}}$ sera alors un idéal maximal de A contenant $\mathfrak{A}$.

Que $\mathcal{I}_{\mathfrak{a}}$ est un inductif assez clair. En effet la réunion d'une chaîne non vide d'idéaux propres de A est un idéal de A, et même un idéal propre puisque ne comprenant pas 1. Les chaînes non vides de $\mathcal{I}_{\mathfrak{a}}$ y sont donc majorées par leur réunion. Pour terminer, remarquons que la chaîne vide de $\mathcal{I}_{\mathfrak{a}}$ y est majorée par $\mathfrak{A}$. □

Corollaire 4.1.10. *Tout anneau non nul possède un idéal maximal et se surjecte sur un corps.*

Comme les nombres, les idéaux s'additionnent et se multiplient.

Définitions 4.1.11. Soit $\mathfrak{A}$ et $\mathfrak{B}$ deux idéaux de l'anneau A. On définit la somme et le produit de $\mathfrak{A}$ et $\mathfrak{B}$ par

$$\mathfrak{A} + \mathfrak{B} = \{a + b \mid a \in \mathfrak{A} \text{ et } b \in \mathfrak{B}\}$$

$$\mathfrak{A} \cdot \mathfrak{B} = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{A} \text{ et } b_i \in \mathfrak{B}, n \in \mathbb{N}_0\}.$$

On remarque que $\mathfrak{A} + \mathfrak{B}$ et $\mathfrak{A} \cdot \mathfrak{B}$ ainsi définis sont des idéaux de A.

Remarques 4.1.12. (i) $\mathfrak{A} \cdot \mathfrak{B} \subset \mathfrak{A} \cap \mathfrak{B}$, cette inclusion peut être stricte.

Par exemple, dans l'anneau des entiers $\mathbb{Z}$ nous avons

$$n\mathbb{Z} \cdot n\mathbb{Z} = n^2\mathbb{Z} \subsetneq n\mathbb{Z} \text{ pour tout } n \geqslant 1.$$

Et aussi $$4\mathbb{Z} \cdot 6\mathbb{Z} = 24\mathbb{Z} \subsetneq 4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}.$$

(ii) Dans un domaine principal A nous avons : $\forall a, b \in A$,

$$aA \cdot bA = abA \subset aA \cap bA = \text{ppcm}(a, b)A.$$

(iii) L'ensemble $\mathcal{I}_A$ des idéaux d'un anneau A forme un monoïde pour le produit, son neutre est l'idéal impropre A.

(iv) On définit de la même façon la somme et le produit d'un ensemble fini d'idéaux de l'anneau A. Soit $\mathcal{I}_A$ l'ensemble des idéaux de A. Par **convention**, la somme de la partie vide de $\mathcal{I}_A$ est l'idéal nul de A et le produit de la partie vide de $\mathcal{I}_A$ est l'idéal impropre A.

Terminons par une propriété des domaines noethériens qui sera bien utile.

Proposition 4.1.13. *Dans un domaine noethérien, tout idéal non nul contient un produit fini d'idéaux premiers non nuls.*

Démonstration. S'il existe dans le domaine noethérien A un idéal non nul ne contenant pas un produit d'idéaux premiers non nuls, soit $\mathfrak{A}$ un maximal parmi ceux-ci. Cet idéal $\mathfrak{A}$ est un idéal propre (car le domaine A contient un idéal maximal) et il n'est pas premier. Nous avons donc deux éléments $x, y \in A \setminus \mathfrak{A}$ tels que $xy \in \mathfrak{A}$. Les idéaux $xA + \mathfrak{A}$ et $yA + \mathfrak{A}$ de A contiennent strictement $\mathfrak{A}$ et contiennent donc chacun un produit d'idéaux premiers non nuls. Le produit $(xA + \mathfrak{A}) \cdot (yA + \mathfrak{A})$ contient donc aussi un produit d'idéaux premiers non nuls. Mais $(xA+\mathfrak{A})\cdot(yA+\mathfrak{A}) \subset \mathfrak{A}$. Donc $\mathfrak{A}$ lui-même contient un produit d'idéaux premiers non nuls. Cette contradiction termine la preuve. □

– – – – – – – – – – – – – – – – –

4.1.14. Exercice*. Soit $\mathfrak{A}$, $\mathfrak{B}$ et $\mathfrak{P}$ trois idéaux de l'anneau A. Montrer.

$$\text{Si } \mathfrak{P} \text{ est premier et si } \mathfrak{P} \supset \mathfrak{A} \cdot \mathfrak{B} \quad \text{alors} \quad \mathfrak{P} \supset \mathfrak{A} \text{ ou } \mathfrak{P} \supset \mathfrak{B}.$$

(Indication. Si $\mathfrak{P} \not\supseteq \mathfrak{A}$ et $\mathfrak{P} \not\supseteq \mathfrak{B}$, prendre $a \in \mathfrak{A} \setminus \mathfrak{P}$ et $b \in \mathfrak{B} \setminus \mathfrak{P}$ et regarder où se trouve le produit ab.)

4.1.15. Exercice*. Soit $f : A \to B$ un homomorphisme d'anneaux et soit $\mathfrak{P}$ un idéal premier de B.

Montrer que $f^{-1}(\mathfrak{P})$ est un idéal premier de A.

4.1.16. Exercice*. Nous dirons que les idéaux $\mathfrak{A}$ et $\mathfrak{B}$ de l'anneau A sont **étrangers** si $\mathfrak{A} + \mathfrak{B} = A$.

(a) Si les idéaux $\mathfrak{A}$ et $\mathfrak{B}$ de l'anneau A sont étrangers, alors $\mathfrak{A}\cdot\mathfrak{B} = \mathfrak{A}\cap\mathfrak{B}$.

(b) Soient $\mathfrak{A}$ et $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_n$ des idéaux de l'anneau A.
Si $\forall i, 1 \leqslant i \leqslant n, \quad \mathfrak{A} + \mathfrak{B}_i = A$, alors $\mathfrak{A} + \mathfrak{B}_1 \cdot \mathfrak{B}_2 \cdots \mathfrak{B}_n = A$.

(c) Voici une généralisation d'un résultat déjà mentionné dans le cas où $A = \mathbb{Z}$ (cf. 3.5.6).

Si les idéaux $\mathfrak{A}$ et $\mathfrak{B}$ de l'anneau A sont étrangers, alors l'homomorphisme naturel $A \to A/\mathfrak{A} \times A/\mathfrak{B}$ est surjectif et induit un isomorphisme

$$A/(\mathfrak{A} \cdot \mathfrak{B}) \xrightarrow{\sim} A/\mathfrak{A} \times A/\mathfrak{B}.$$

(d) Généralisons encore. Si les idéaux $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_n$ de A sont étrangers

deux à deux, alors

$$A/(\mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_n) \xrightarrow{\sim} \prod_{i=1}^{n} A/\mathfrak{A}_i.$$

(Indication partielle. Si $\mathfrak{A} + \mathfrak{B} = A$ on peut écrire $1 = a + b$, où $a \in \mathfrak{A}$ et $b \in \mathfrak{B}$. On a alors $1 \cong b$ modulo $\mathfrak{A}$ et $1 \cong a$ modulo $\mathfrak{B}$ et, $\forall x, y \in A$, on a : $bx + ay \cong x$ modulo $\mathfrak{A}$ et $bx + ay \cong y$ modulo $\mathfrak{B}$.)

4.1.17. Observation. Soit A un anneau et $a, b, c, d \in A$. Voici quelques égalités au niveau des idéaux de A.

$$(a, ac) = (a) = aA, \quad (a, b) = (a, b + ac), \quad (a, b) \cdot (c, d) = (ac, ad, bc, bd).$$

4.1.18. Dans l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres K nous n'avons généralement pas l'unicité de la factorisation d'un élément non nul non inversible en produit d'éléments irréductibles, bien que nous en ayons l'existence (2.1.9). C'est le cas de $\mathbb{Z}[i\sqrt{5}]$ par exemple. Mais on peut récupérer cette unicité au niveau des idéaux. Nous n'avons pas encore tous les outils nécessaires pour montrer que les idéaux non nuls d'un $\mathcal{O}_K$ y sont produits d'idéaux premiers non nuls de façon unique, mais nous pouvons déjà nous exercer.

Rappelons 1.3.18, dans l'anneau des entiers $\mathbb{Z}[i\sqrt{5}]$ du corps $\mathbb{Q}[i\sqrt{5}]$, nous avons $(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = 2 \cdot 3$, les quatre nombres figurant dans cette égalité sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$ mais ne sont pas premiers dans $\mathbb{Z}[i\sqrt{5}]$. Regardons quelques idéaux de $\mathbb{Z}[i\sqrt{5}]$.

(i) Soit $\mathfrak{P} = (2, 1 + i\sqrt{5})$. Identifier l'anneau quotient $\mathbb{Z}[i\sqrt{5}]/\mathfrak{P}$. Montrer que $\mathfrak{P}$ est un idéal premier maximal non principal de $\mathbb{Z}[i\sqrt{5}]$.

(ii) Vérifier : $(2) = \mathfrak{P}^2$.

(iii) Montrer que les idéaux $\mathfrak{P}_1 = (3, 1 + i\sqrt{5})$ et $\mathfrak{P}_2 = (3, 2 + i\sqrt{5})$ sont deux idéaux maximaux distincts de $\mathbb{Z}[i\sqrt{5}]$.

(iv) Dans $\mathbb{Z}[i\sqrt{5}]$ vérifier qu'on a aussi $(3) = \mathfrak{P}_1 \cdot \mathfrak{P}_2$.

(v) Écrire les idéaux $(1 + i\sqrt{5})$ et $(1 - i\sqrt{5})$ de $\mathbb{Z}[i\sqrt{5}]$ comme produit d'idéaux premiers.

Observer qu'au niveau des idéaux on a

$$(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = \mathfrak{P}^2 \cdot \mathfrak{P}_1 \cdot \mathfrak{P}_2 = (2) \cdot (3).$$

(vi) Écrire chacun des idéaux (7) et $(4, (2 + 2i\sqrt{5}))$ de $\mathbb{Z}[i\sqrt{5}]$ comme produit d'idéaux premiers.

(vii) Soit $\mathfrak{P}' = \{\gamma \in \mathbb{Q}[i\sqrt{5}] \mid \gamma\mathfrak{P} \subset \mathbb{Z}[i\sqrt{5}]$. Observer : $\frac{3}{1+i\sqrt{5}} \in \mathfrak{P}'$, $\mathbb{Z}[i\sqrt{5}] \subsetneq \mathfrak{P}'$.

4.2 Domaines de Dedekind

Convention de section. Dans toute cette section, A est un domaine et K est son corps des fractions.

Pour étudier la factorisation des idéaux il est utile d'élargir le cadre dans lequel on travaille, d'y introduire des idéaux fractionnaires, un peu comme on a introduit les fractions $\frac{2}{3}, \frac{4}{15}, \cdots$ au départ des entiers naturels, ou comme on a introduit le corps des fractions d'un domaine.

Définition 4.2.1. Un **idéal fractionnaire** du domaine A (ou du corps K relativement à A) est un sous-A-module *non nul* $\mathfrak{A}$ de K pour lequel il existe un élément *non nul* d de A satisfaisant $d\mathfrak{A} \subset A$.

Nous dirons d'un tel élément d qu'il est un dénominateur pour $\mathfrak{A}$.

(Les éléments de $\mathfrak{A}$ sont des fractions de la forme $\frac{a}{b}$ $(a, b \in A, \quad b \neq 0)$, et $d\frac{a}{b} = a' \in A \Rightarrow \frac{a}{b} = \frac{a'}{d}$, l'élément d de la définition peut être vu comme un dénominateur commun des éléments de $\mathfrak{A}$.)

Remarques 4.2.2. (i) Tout idéal non nul de A est un idéal fractionnaire de A, les idéaux non nuls de A seront appelés *idéaux entiers.*

(ii) Si $\mathfrak{A}$ est un idéal fractionnaire de A et si d est un dénominateur pour $\mathfrak{A}$, alors $d\mathfrak{A}$ est un idéal entier de A, isomorphe à $\mathfrak{A}$ en tant que A-module.

De plus, comme $\quad d\mathfrak{A} \subset \mathfrak{A} \cap A, \quad$ on a $\quad \{0\} \neq \mathfrak{A} \cap A \quad$ et $\quad \mathfrak{A} \cap A$ est un idéal entier non nul de A.

(iii) Si $\mathfrak{A}$ et $\mathfrak{B}$ sont deux idéaux fractionnaires de A, alors $\mathfrak{A} \cap \mathfrak{B}$ est un idéal fractionnaire de A.

(Il est clair que $\mathfrak{A} \cap \mathfrak{B}$ est un sous-A-module de K car l'intersection de deux sous-modules est un sous-module.

Vérifions d'abord que $\mathfrak{A} \cap \mathfrak{B}$ est non nul. Soit d un dénominateur pour $\mathfrak{A}$ et soit d' un dénominateur pour $\mathfrak{B}$. Alors $d\mathfrak{A}$ et $d'\mathfrak{B}$ sont deux idéaux entiers de A, comme ils ne sont pas nuls leur intersection est aussi non nulle car A est un domaine. Et comme $d\mathfrak{A} \cap d'\mathfrak{B} \subset \mathfrak{A} \cap \mathfrak{B}$ on voit que $\mathfrak{A} \cap \mathfrak{B}$ est aussi non nul.

On termine en observant que d ou d' peut servir de dénominateur pour $\mathfrak{A} \cap \mathfrak{B}$.)

(iv) Pour tout $x \in K, x \neq 0$, xA est un idéal fractionnaire de A, appelé idéal fractionnaire principal.

(v) Si A est un domaine principal, tous les idéaux fractionnaires de A sont principaux.

(Si A est principal, si d est un dénominateur pour l'idéal fractionnaire $\mathfrak{A}$ de A, alors $d\mathfrak{A} = aA$ pour un certain $a \in A$, d'où $\mathfrak{A} = \frac{a}{d}A$.)

(vi) Tout sous-A-module non nul de type fini $\mathfrak{A}$ de K est un idéal fractionnaire de A.

(Si $(x_1, x_2, \cdots, x_n)$ est une partie génératrice du sous-A-module $\mathfrak{A}$ de K, un multiple des dénominateurs des fractions $x_i = \frac{a_i}{b_i}$ sera un dénominateur pour $\mathfrak{A}$.)

Réciproquement, si A est *noethérien*, tout idéal fractionnaire $\mathfrak{A}$ de A est un sous-A-module de type fini de K.

(Si d est un dénominateur pour $\mathfrak{A}$, on a $\mathfrak{A} \simeq d\mathfrak{A}$. Comme $d\mathfrak{A}$ est un idéal entier de A, $d\mathfrak{A}$ est un A-module de type fini.)

Définitions et observations 4.2.3. On définit la somme et le produit de deux idéaux fractionnaires $\mathfrak{A}$ et $\mathfrak{B}$ de l'anneau A comme on a défini la somme et le produit de deux idéaux entiers :

$$\mathfrak{A} + \mathfrak{B} = \{a + b \mid a \in \mathfrak{A} \text{ et } b \in \mathfrak{B}\}$$
$$\mathfrak{A} \cdot \mathfrak{B} = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{A} \text{ et } b_i \in \mathfrak{B}, n \in \mathbb{N}_0\}.$$

On remarque que $\mathfrak{A} \cdot \mathfrak{B}$ et $\mathfrak{A} + \mathfrak{B}$ ainsi définis sont des idéaux fractionnaires de A.

(Il est assez clair que $\mathfrak{A} + \mathfrak{B}$ et $\mathfrak{A} \cdot \mathfrak{B}$ sont des sous-A-modules de K.

$\mathfrak{A} + \mathfrak{B}$ est clairement non nul. $\mathfrak{A} \cdot \mathfrak{B}$ est non nul car le produit de deux éléments non nuls est non nul. Si d est un dénominateur pour $\mathfrak{A}$ et si d' est un dénominateur pour $\mathfrak{B}$. on observe que dd' est un dénominateur pour $\mathfrak{A} \cdot \mathfrak{B}$ et pour $\mathfrak{A} + \mathfrak{B}$.)

4.2.4. Soit $\mathfrak{A}$, $\mathfrak{B}$ et $\mathfrak{C}$ des idéaux fractionnaires. On a :

$$\mathfrak{A} \subset \mathfrak{B} \Rightarrow \mathfrak{A} \cdot \mathfrak{C} \subset \mathfrak{B} \cdot \mathfrak{C}.$$

Notons qu'en général il n'y a pas de relation d'inclusion entre les idéaux fractionnaires $\mathfrak{A} \cdot \mathfrak{B}$ et $\mathfrak{A} \cap \mathfrak{B}$.

4.2.5. Le monoïde des idéaux fractionnaire.

Nous désignerons par $\mathcal{F}rac(A)$ l'ensemble des idéaux fractionnaires du domaine A. La loi « produit » sur $\mathcal{F}rac(A)$ munit $\mathcal{F}rac(A)$ d'une structure de monoïde commutatif, dont le neutre est l'idéal impropre A.

Comme le produit de deux idéaux fractionnaires principaux est un idéal fractionnaire principal ($xA \cdot yA = xyA$), on voit que les idéaux fractionnaires principaux de A forment un sous-monoïde du monoïde $(\mathcal{F}rac(A), \cdot)$. Ils forment même un sous-groupe de $(\mathcal{F}rac(A), \cdot)$ car si xA est un idéal fractionnaire principal, on a $x \neq 0$, $x^{-1} \in K$ et on aussi $xA \cdot x^{-1}A = A$, autrement écrit $(xA)^{-1} = x^{-1}A$.

Dans le cas où A est un corps (donc dans le cas où $A = K$) le monoïde $\mathcal{F}rac(A)$ ne comprend qu'un seul élément, à savoir son neutre A, et il n'y a pas grand-chose à en dire. Ce cas trivial sera souvent écarté.

À tout idéal fractionnaire $\mathfrak{A}$ de A nous allons maintenant associer un autre idéal fractionnaire qui pourra dans certains cas servir d'inverse à $\mathfrak{A}$ dans le monoïde $(\mathcal{F}rac(A), \cdot)$.

Définitions et observations 4.2.6. Pour tout idéal fractionnaire $\mathfrak{A}$ de A on définit

$$\mathfrak{A}' = \{x \in K \mid x\mathfrak{A} \subset A\}.$$

On remarque que $\mathfrak{A}'$ ainsi défini est encore un idéal fractionnaire de A.

(Il est clair que $\mathfrak{A}'$ est un sous-A-module de K, non nul car il comprend un dénominateur de $\mathfrak{A}$. Et tout élément non nul de $\mathfrak{A}$ peut servir de dénominateur pour $\mathfrak{A}'$.)

Remarque 4.2.7. Si l'idéal fractionnaire $\mathfrak{A}$ est inversible dans le monoïde $\mathcal{F}rac(A)$, alors $\mathfrak{A}^{-1} = \mathfrak{A}'$.

(Si $\mathfrak{A}$ est inversible, de $\mathfrak{A} \cdot \mathfrak{A}^{-1} = A$ on déduit $\mathfrak{A}^{-1} \subset \mathfrak{A}'$ et $A = \mathfrak{A} \cdot \mathfrak{A}^{-1} \subset \mathfrak{A} \cdot \mathfrak{A}' \subset A$, d'où $\mathfrak{A} \cdot \mathfrak{A}' = A$ et $\mathfrak{A}^{-1} = \mathfrak{A}'$.)

Propriétés 4.2.8. Pour tous $\mathfrak{A}, \mathfrak{B} \in \mathcal{F}rac(A)$ on a :

$$\begin{array}{ccc} A & = & A' \\ \mathfrak{A} \cdot \mathfrak{A}' & \subset & A \\ \mathfrak{A} & \subset & \mathfrak{A}'' \\ \mathfrak{A} \subset \mathfrak{B} & \Rightarrow & \mathfrak{A}' \supset \mathfrak{B}' \end{array}$$

$$\mathfrak{A} \subset A \quad \Rightarrow \quad (\mathfrak{A}' \supset A \quad \text{et} \quad \mathfrak{A} \subset \mathfrak{A} \cdot \mathfrak{A}' \subset A)$$

$$\begin{array}{ccc} (\mathfrak{A} + \mathfrak{B})' & = & \mathfrak{A}' \cap \mathfrak{B}' \\ (\mathfrak{A} \cdot \mathfrak{B})' & \supset & \mathfrak{A}' \cdot \mathfrak{B}' \end{array}$$

.

Proposition 4.2.9. *Soit A un domaine noethérien dont tout idéal premier non nul est maximal et soit $\mathfrak{A} \in \mathcal{F}rac(A)$. Alors*

$$\mathfrak{A} \subsetneq A \quad \Rightarrow \quad A \subsetneq \mathfrak{A}'.$$

Démonstration. Si A est un corps il n'y a rien à démontrer. Nous supposons donc que notre domaine A n'est pas un corps, autrement dit que les idéaux maximaux de A sont non nuls.

Comme tout idéal propre non nul de A est contenu dans un idéal maximal de A, il suffit de démontrer que, si $\mathfrak{M}$ est un idéal maximal de A, alors $A \subsetneq \mathfrak{M}'$.

Soit $0 \neq a \in \mathfrak{M}$. L'idéal non nul aA de A contient un produit d'idéaux premiers non nuls, 4.1.13, et nous avons

$$\mathfrak{M} \supset aA \supset \mathfrak{P}_1 \cdots \mathfrak{P}_n$$

où les $\mathfrak{P}_i$ sont des idéaux premiers non nuls. Supposons que n est le plus petit naturel tel que aA contienne un produit de n idéaux premiers non nuls. Comme l'idéal maximal $\mathfrak{M}$ est un idéal premier, $\mathfrak{M}$ contient un des $\mathfrak{P}_i$, 4.1.14, disons $\mathfrak{M} \supset \mathfrak{P}_1$. Mais alors $\mathfrak{M} = \mathfrak{P}_1$ par l' hypothèse sur A. Posons maintenant $\mathfrak{B} = \mathfrak{P}_2 \cdots \mathfrak{P}_n$. Avec ces notations nous avons

$$\mathfrak{M} \supset aA \supset \mathfrak{M} \cdot \mathfrak{B} \quad \text{et aussi} \quad aA \not\supseteq \mathfrak{B}$$

par notre hypothèse sur n. Nous avons donc un élément $b \in \mathfrak{B} \setminus aA$.

Mais alors on a

$$a^{-1}b \notin A \quad \text{et aussi} \quad a^{-1}b\mathfrak{M} \subset a^{-1}\mathfrak{B} \cdot \mathfrak{M} \subset a^{-1}aA = A.$$

Donc $a^{-1}b \in \mathfrak{M}'$ et $A \subsetneq \mathfrak{M}'$. □

Pour obtenir de plus jolis résultats sur le monoïde $\mathcal{F}rac(A)$ il nous faut renforcer nos hypothèses.

Définition 4.2.10. Un **domaine de Dedekind** est un domaine noethérien intégralement clos dont tous les idéaux premiers non nuls sont maximaux.

Les domaines principaux sont donc des domaines de Dedekind. Ce ne sont pas les seuls. Nous avons déjà rassemblé plusieurs propriétés de l'anneau des entiers d'un corps de nombres. Avec 1.2.25, 2.4.18 et 4.1.5 nous avons

Théorème 4.2.11. *L'anneau des entiers d'un corps de nombre est un domaine de Dedekind.*

Ce théorème est la raison pour laquelle nous nous intéressons ici aux domaines de Dedekind.

Lemme 4.2.12. *Soit A un domaine de Dedekind et soit $\mathfrak{A} \subset \mathfrak{B}$ deux idéaux propres non nuls de A. Alors*

$$\mathfrak{A} \subsetneq \mathfrak{A} \cdot \mathfrak{B}' \subset A.$$

Démonstration. De $\mathfrak{A} \subset \mathfrak{B} \subsetneq A$ on déduit $A \subsetneq \mathfrak{B}'$ (4.2.9) et

$$\mathfrak{A} = A \cdot \mathfrak{A} \subset \mathfrak{A} \cdot \mathfrak{B}' \subset \mathfrak{B} \cdot \mathfrak{B}' \subset A.$$

Reste à montrer l'essentiel, que l'inclusion $\mathfrak{A} \subset \mathfrak{A} \cdot \mathfrak{B}'$ est stricte. Procédons par l'absurde et supposons $\mathfrak{A} = \mathfrak{A} \cdot \mathfrak{B}'$. La multiplication par un élément $x \in \mathfrak{B}' \setminus A$ se restreint alors en un endomorphisme $x\cdot : \mathfrak{A} \to \mathfrak{A}$ du A-module de type fini $\mathfrak{A}$. Supposons $\mathfrak{A}$ engendré par n éléments, on a comme en 1.2.14 une matrice $C \in A^{n\times n}$ telle que $\det(xI_n - C)\mathfrak{A} = \{0\}$. Comme A est intègre et que $\mathfrak{A}$ est non nul, on en déduit $\det(xI_n - C) = 0$, ce qui entraîne que x est entier sur A et aussi que $x \in A$ puisque A est intégralement clos. Cette contradiction termine la preuve □

Corollaire 4.2.13. *Soit A un domaine de Dedekind qui n'est pas un corps et soit $\mathfrak{M}$ un idéal maximal de A. Alors $\mathfrak{M}$ est inversible dans le monoïde $\mathcal{F}rac(A)$. Plus précisément on a*

$$\mathfrak{M} \cdot \mathfrak{M}' = A \qquad \mathfrak{M}' = \mathfrak{M}^{-1}$$

Démonstration. Comme A n'est pas un corps l'idéal maximal $\mathfrak{M}$ est non nul et appartient à $\mathcal{F}rac(A)$. Dans le lemme précédent on remplace $\mathfrak{A}$ et $\mathfrak{B}$ par $\mathfrak{M}$, on obtient $\mathfrak{M} \subsetneq \mathfrak{M} \cdot \mathfrak{M}' \subset A$ et on en déduit $\mathfrak{M} \cdot \mathfrak{M}' = A$ par la maximalité de $\mathfrak{M}$. □

Dans la situation de ce corollaire nous pouvons donc prendre des puissances positives ou négative de l'idéal maximal $\mathfrak{M}$: pour $n \in N_0$ on définit $\mathfrak{M}^{-n} = (\mathfrak{M}^{-1})^n$ et comme d'habitude on pose $\mathfrak{M}^0 = A$.

Théorème 4.2.14. *Soit A un domaine de Dedekind qui n'est pas un corps et soit $\mathfrak{B}$ un idéal fractionnaire de A, $\mathfrak{B} \neq A$. Alors $\mathfrak{B}$ s'écrit de façon unique sous la forme*

$$\mathfrak{B} = \mathfrak{P}_1^{n_1} \cdot \mathfrak{P}_2^{n_2} \cdots \mathfrak{P}_r^{n_r}$$

où les $\mathfrak{P}_i$ sont des idéaux maximaux de A distinct deux à deux et où $0 \neq n_i \in \mathbb{Z}$.

Si de plus $\mathfrak{B}$ est un idéal entier, alors les $n_i \in \mathbb{N}_0$.

Démonstration. (i) *Existence.*

On a un élément non nul d de A tel que $d\mathfrak{B} \subset A$, tel que $d\mathfrak{B}$ soit un idéal entier de A. Mais dA est aussi un idéal entier de A et on a $\mathfrak{B} = d\mathfrak{B} \cdot d^{-1}A = d\mathfrak{B} \cdot (dA)^{-1}$. Il suffit donc de montrer l'existence de la factorisation pour les idéaux *entiers* non nuls $\mathfrak{B} \neq A$ de A.

Procédons par l'absurde, supposons que l'ensemble $\mathcal{C}$ des idéaux entiers non nuls de A distincts de A qui ne sont pas de la forme donnée dans notre énoncé est non vide. Comme A est noethérien $\mathcal{C}$ admet un maximal, disons $\mathfrak{A}$. Cet idéal $\mathfrak{A}$ n'est pas un idéal maximal de A mais il contenu dans un idéal maximal de A, disons $\mathfrak{A} \subset \mathfrak{P}$. De $\mathfrak{A} \subset \mathfrak{P}$ on déduit $\mathfrak{A} \subsetneq \mathfrak{A} \cdot \mathfrak{P}' \subset A$ (4.2.12). Mais alors le choix de $\mathfrak{A}$ nous dit que $\mathfrak{A} \cdot \mathfrak{P}'$ est de la forme donnée dans l'énoncé. Et comme $\mathfrak{P}' = \mathfrak{P}^{-1}$ (4.2.13), il suffit de multiplier la factorisation de $\mathfrak{A} \cdot \mathfrak{P}'$ par $\mathfrak{P}$ pour obtenir une factorisation de $\mathfrak{A}$. Cette contradiction prouve l'existence de la factorisation.

(ii) *Unicité.*

Supposons que $\mathfrak{B}$ aie deux factorisations. Quitte à autoriser les exposants nuls en convenant comme d'habitude $\mathfrak{P}^0 = A$ on peut écrire

$$\mathfrak{B} = \mathfrak{P}_1^{n_1} \cdot \mathfrak{P}_2^{n_2} \cdots \mathfrak{P}_s^{n_s} = \mathfrak{P}_1^{m_1} \cdot \mathfrak{P}_2^{m_2} \cdots \mathfrak{P}_s^{m_s}$$

où les $\mathfrak{P}_i$ sont des idéaux maximaux de A distincts deux à deux. Il nous faut montrer que $n_i = m_i$ pout tout $i, 1 \leqslant i \leqslant s$. On procède par l'absurde, on suppose qu'il existe un $i, 1 \leqslant i \leqslant s$, tel que $n_i \neq m_i$ et on écrit

$$A = \mathfrak{P}_1^{m_1-n_1} \cdot \mathfrak{P}_2^{m_2-n_2} \cdots \mathfrak{P}_s^{m_s-n_s}$$

Notons qu'ici, nos exposants $m_i - n_i$ ne peuvent être tous strictement positifs car un produit d'idéaux propres est un idéal propre, et ils ne peuvent pas non plus être tous strictement négatifs. En séparant les exposants positifs et les exposants négatifs, en changeant éventuellement la numérotation des $\mathfrak{P}_i$ et en éliminant les éventuels exposants nuls, on obtient deux factorisations

$$\mathfrak{P}_1^{m_1-n_1} \cdot \mathfrak{P}_2^{m_2-n_2} \cdots \mathfrak{P}_k^{m_k-n_k} = \mathfrak{P}_{k+1}^{n_{k+1}-m_{k+1}} \cdot \mathfrak{P}_{k+2}^{n_{k+2}-m_{k+2}} \cdots \mathfrak{P}_t^{n_t-m_t}$$

où cette fois tous les exposants sont strictement positifs. Comme

$$\mathfrak{P}_1 \supset \mathfrak{P}_{k+1}^{n_{k+1}-m_{k+1}} \cdot \mathfrak{P}_{k+2}^{n_{k+2}-m_{k+2}} \cdots \mathfrak{P}_t^{n_t-m_t}$$

on a alors que $\mathfrak{P}_1$ contient un des $\mathfrak{P}_i$ $(k+1 \leqslant i \leqslant t)$ figurant dans le second membre de cette relation (4.1.14), ce qui est impossible puisque $\mathfrak{P}_1$ et $\mathfrak{P}_i$ sont des idéaux premiers maximaux distincts. Cette contradiction termine la preuve. □

Corollaire 4.2.15. *Le monoïde $(\mathcal{F}rac(A), \cdot)$ est un groupe.*

Démonstration. Si $\mathfrak{B} = \mathfrak{P}_1^{n_1} \cdot \mathfrak{P}_2^{n_2} \cdots \mathfrak{P}_r^{n_r}$ alors

$$\mathfrak{P}_1^{-n_1} \cdot \mathfrak{P}_2^{-n_2} \cdots \mathfrak{P}_r^{-n_r} = \mathfrak{B}^{-1}.$$

□

Proposition 4.2.16. *Si A est à la fois un domaine de Dedekind et un domaine factoriel, alors A est principal.*

Démonstration. Si A est un corps il n'y a rien à faire. Supposons donc que A n'est pas un corps.

Comme tout idéal propre de A est produit d'idéaux maximaux, il suffit de montrer que tout idéal maximal est principal.

Soit donc $\mathfrak{P}$ un idéal maximal et soit $0 \neq x \in \mathfrak{P}$, un tel x n'est pas inversible. Comme l'idéal maximal $\mathfrak{P}$ est premier, il comprend un des facteurs irréductibles de x, disons q. Mais l'idéal non nul qA est un idéal premier car dans un domaine factoriel tout élément irréductible est premier, et on a $qA \subset \mathfrak{P}$. Comme par hypothèse tous les idéaux premiers non nuls de A sont maximaux on en déduit que $\mathfrak{P} = qA$ est principal □

Terminons par une dernière définition.

Définition 4.2.17. Soit A un domaine de Dedekind. Le quotient du groupe $(\mathcal{F}rac(A), \cdot)$ par son sous-groupe formé des idéaux fractionnaires principaux est appelé le **groupe des classes de A**. On le note souvent par $\mathcal{C}(A)$.

Un domaine de Dedekind est donc principal si et seulement si son groupe des classes est le groupe neutre.

On pourrait en dire beaucoup plus sur les domaines de Dedekind, sur l'anneau des entiers d'un corps de nombres. On pourrait exploiter la factorisation des idéaux. Mais le cours se termine, il nous reste à renvoyer la lectrice et le lecteur à la littérature, s'ils le désirent, ou à les encourager à prendre un cours plus avancé.

– – – – – – – – – – – – – – – – –

4.2.18. Exercice. Si $\mathfrak{A}$ et $\mathfrak{B}$ sont deux idéaux fractionnaires du domaine A, il n'y a en général pas de relations d'inclusion entre $\mathfrak{A} \cap \mathfrak{B}$ et $\mathfrak{A} \cdot \mathfrak{B}$.

Pour $A = \mathbb{Z}$ vérifier qu'on a :

$$\frac{1}{2}\mathbb{Z} \cap \frac{1}{3}\mathbb{Z} = \frac{3}{6}\mathbb{Z} \cap \frac{2}{6}\mathbb{Z} = \mathbb{Z} \subsetneq \frac{1}{2}\mathbb{Z} \cdot \frac{1}{3}\mathbb{Z} = \frac{1}{6}\mathbb{Z}.$$

Calculer

$$\frac{2}{3}\mathbb{Z} \cap \frac{4}{5}\mathbb{Z} \quad \text{et} \quad \frac{2}{3}\mathbb{Z} \cdot \frac{4}{5}\mathbb{Z}.$$

Vérifier qu'il n'y pas de relation d'inclusion entre ces deux derniers idéaux fractionnaires.

4.2.19. Exercice. Soit A un domaine de Dedekind, soient $\mathfrak{A}$ et $\mathfrak{B}$ deux idéaux fractionnaires de A et soient

$$\mathfrak{A} = \mathfrak{P}_1^{m_1} \cdot \mathfrak{P}_2^{m_2} \cdots \mathfrak{P}_s^{m_s} \quad \text{et} \quad \mathfrak{B} = \mathfrak{P}_1^{n_1} \cdot \mathfrak{P}_2^{n_2} \cdots \mathfrak{P}_s^{n_s}$$

leur factorisation en produits d'idéaux maximaux (les $\mathfrak{P}_i$ sont distinct deux à deux et on autorise les exposants nuls).

(i) Indiquer une condition sur les exposants m_i, n_i pour que $\mathfrak{A} \subset \mathfrak{B}$.

(ii) Écrire la factorisation de $\mathfrak{A} \cap \mathfrak{B}$ et aussi celle de $\mathfrak{A} + \mathfrak{B}$.

(Remarquer que $\mathfrak{A} + \mathfrak{B}$ est le plus petit idéal fractionnaire contenant à la fois $\mathfrak{A}$ et $\mathfrak{B}$.)

4.2.20. Exercice. Soit $d \neq 0, 1$ un entier rationnel sans facteurs carrés et soit $\mathcal{O}_d$ l'anneau des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}]$. Soit encore p un nombre premier naturel.

Montrer qu'il y a trois possibilités pour l'idéal $p\mathcal{O}_d$ de l'anneau $\mathcal{O}_d$:

soit $p\mathcal{O}_d$ est un idéal premier,

soit $p\mathcal{O}_d$ est produit de deux idéaux premiers distincts de $\mathcal{O}_d$,

soit $p\mathcal{O}_d$ est le carré d'un idéal premier de $\mathcal{O}_d$.

4.2.21. Exercice. Dans $\mathbb{Z}[\sqrt{10}]$ on a $(2 + \sqrt{10})(2 - \sqrt{10}) = (-2).3$.

Écrire la factorisation des idéaux principaux engendrés par chacun des quatre nombres $2 + \sqrt{10}$, $2 - \sqrt{10}$, 2 et 3.

Montrer que l'anneau $\mathbb{Z}[\sqrt{10}]$ est un domaine de Dedekind non principal.

4.2.22. Exercice. Soit A un domaine de Dedekind ne possédant qu'un seul idéal maximal.

(i) Montrer que A est principal.

(Suggestion. Montrer d'abord que, $\forall a, b \in A$, on a soit $aA \subset bA$, soit $bA \subset aA$.)

(ii) Si de plus A n'est pas un corps, soit t un générateur de l'unique idéal maximal de A.

Montrer qu'alors tout élément non nul a de A s'écrit de façon unique sous la forme $a = ut^n$, où u est un inversible de A et où $n \in \mathbb{N}$.

(Un tel anneau est souvent appelé anneau de valuation discrète.)

Bibliographie

[1] Z. I. Borevitch et I. R. Chavarevitch, Théorie des Nombres, Gauthier-Villars, Paris (1967).

[2] P. M. Cohn, Algebra, volume 2, John Wiley & Sons (1977).

[3] Simone Gutt et Anne-Marie Simon, cours d'algèbre et premiers exercices d'algèbre.

[4] Serge Lang, Algebra, Addison-Wesley, New-York (1965).

[5] H. W. Lenstra Jr., Solving the Pell equation, Notices of the AMS, volume 49, Number 2 (2002), pp.182-192.

[6] W. Scharlau et H. Opolka, From Fermat to Minkowski, Lectures on the theory of numbers and its Historical Development, Springer (1985).

[7] Pierre Samuel, Théorie algébrique des nombres, Hermann, Paris (1967).

[8] Alexander Schmidt, Einführung in die algebraische Zahlentheorie, Springer, Berlin Heidelberg (2007).

[9] Jean-Pierre Serre, Cours d'Arithmétique, Presses universitaires de France, collection Sup, Paris (1970).