Introduction à l'arithmétique

Master I commun Orléans-Tours

Année universitaire 2014-2015

Table des matières

Chapitre 1

Introduction

Comme l'indique son éthymologie ($\alpha\rho\iota\tau\mu o\varsigma$ signifiant nombre en grec), l'arithmétique est la science des nombres et son origine remonte au moins à l'antiquité grecque. Elle s'est longtemps développée autour des différentes tentatives pour résoudre certaines équations diophantiennes. Rappelons qu'il s'agit d'équations algébriques à une ou plusieurs inconnues dont on cherche à déterminer les éventuelles solutions entières ou au contraire à établir l'absence de solution. Le début de leur étude systématique remonte au moins à Diophante (aux alentours du III-ième sciècle de notre ère). La plus connue est sans doute l'équation

$$x^n + y^n = z^n \tag{1.1}$$

où $n \geq 2$ est un entier et $x, y, z \in \mathbb{Z}$. L'existence d'une infinité de solutions à l'équation $x^2+y^2 = z^2$ est généralement attribuée à l'école de Pythagore (vers 570 avant notre ère) bienqu'il semble que sa résolution ait déjà été connue par les Babyloniens 1000 auparavant. Nous verrons que les les solutions sont les triplets Pythagoriciens

$$(x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2)$$

où r, s sont des entiers positifs, premiers entre eux et de parité opposée.

Les notions de *corps et d'anneaux* sont quant à elles beaucoup plus récentes. Elles émergent progressivement à partir du XVI-ième siècle de l'étude des équations algébriques et de la recherche d'une démonstration du grand théorème de Fermat infirmant l'existence d'un triplet d'entiers non nuls solution à l'équation (1.1) dès lors que $n \geq 3$. Les anneaux sont alors essentiellement vus comme des ensembles de nombres généralisant les nombres entiers.

Pour ce qui concerne l'arithmétique des polynômes, l'idée d'associer une lettre par exemple X à un ensemble de nombres date au moins des travaux de Diophante au III-ième siècle. A l'origine les nombres considérés sont des entiers ou des rationnels. Cette idée est généralisée aux nombres irrationnels par la civilisation arabe, à partir du VIII-ième siècle. Bienque la contruction soit encore rudimentaire, elle permet aux mathématiciens de la Renaissance de résoudre toutes les équations polynomiales jusqu'au degré 4. Au XVIIe siècle apparaît un premier formalisme, celui des fonctions. Le symbole X est vu comme une variable et le polynôme comme une fonction. Cette approche permet notamment à Gauss d'obtenir la première preuve complète du théorème de d'Alembert-Gauss montrant qu'un polynôme à coefficients complexe de degré n a exactement n racines (éventuellement multiples) dans $\mathbb{C}$.

Une question de Vandermonde au XVIIIe siècle remet à l'honneur le concept de polynôme formel faisant usage d'une indéterminée X pouvant s'additionner et se multiplier, mais qui n'est pas vu

comme une fonction. C'est finalement Gauss qui a l'idée de considérer les polynômes comme des équivalents de nombres entiers, avec une division euclidienne, l'équivalent des nombres premiers et une décomposition unique en facteurs premiers. En langage moderne, Gauss considère l'anneau des polynômes $\mathbb{C}[X]$. Ce n'est qu'au XX-ième siècle que la notion d'anneau de polynômes est dégagée de façon totalement rigoureuse.

Les chapitres qui suivent consistent en une introduction à l'arithmétique, sujet extrêmement vaste. Nous renvoyons le lecteur à la bibliographie pour des approfondissements.

Chapitre 2

Rappels sur les anneaux

2.1 Quelques définitions et exemples incontournables

Soit A un ensemble non vide et $+, \cdot$ deux lois de composition internes sur A.

Définition 2.1.1 *L'ensemble A est un anneau lorsque les propriétés suivantes sont vérifiées*

1. *L'ensemble $(A, +)$ est un groupe abélien,*
2. *la loi $\cdot$ est associative,*
3. *la loi $\cdot$ est distributive par rapport à la loi $+$ c'est-à-dire que pour tous a, α, α' dans A, on a $a \cdot (\alpha + \alpha') = a \cdot \alpha + a \cdot \alpha'$ et $(\alpha + \alpha') \cdot a = \alpha \cdot a + \alpha' \cdot a$.*

On notera 0 l'élément neure de la loi $+$. Lorsque la loi $\cdot$ possède un élément neutre (souvent noté 1), on dit que l'anneau est *unitaire*. Lorsque la loi $\cdot$ est commutative, A sera dit commutatif.

Si A est unitaire, on dit que l'élément $a \in A$ possède un inverse lorsqu'il existe un élément $a' \in A$ tel que $a \cdot a' = a' \cdot a = 1$. Dans ce cas, l'inverse est unique (pourquoi ?) et

$$\mathbb{U}(A) = \{a \in A \mid a \text{ est inversible}\}$$

est un groupe pour la loi $\cdot$ d'élément neutre 1 (à vérifier). Lorsque $\mathbb{U}(A)$ contient tous les éléments de A sauf 0, on dit que A est un *corps*. Noter également que l'on a pour tout $a \in A$ et $a' \in A$

$$a \cdot a' = (0 + a) \cdot a' = 0 \cdot a + a \cdot a'$$

ce qui implique en simplifiant par $a \cdot a'$ que $0 \cdot a = 0$. De même $a \cdot 0 = 0$. On dit que 0 est un élément *absorbant*.

L'anneau A est *intègre* lorsque

$$\forall a, b \in A, \text{ on a } ab = 0 \text{ ssi } a = 0 \text{ ou } b = 0.$$

Lorsque A n'est pas intègre, un élément $a \neq 0$ pour lequel il existe un élément $b \neq 0$ avec $ab = 0$ s'appelle un diviseur de 0. Lorsqu'un anneau A est intègre, on peut construire son corps des fractions $\text{frac}(A)$ en mimant la contruction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

Les exemples d'anneaux sont très nombreux et divers :

Exemples.

- $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire intègre pour l'addition et la multiplication des entiers et $\mathbb{U}(\mathbb{Z}) = \{\pm 1\}$.
- L'ensemble des matrices carrées à coefficients dans $\mathbb{R}$ est un anneau unitaire (non commutatif et non intègre) pour l'addition et la multiplication des matrices et $\mathbb{U}(M_n(\mathbb{R})) = GL_n(\mathbb{R})$.
- L'ensemble $\mathcal{C}$ des fonctions continues $f : \mathbb{R} \to \mathbb{R}$ est un anneau commutatif unitaire non intègre pour l'addition et la multiplication des fonctions et $\mathbb{U}(\mathcal{C}) = \{f \in \mathcal{C} \mid f(x) \neq 0 \ \forall x \in \mathbb{R}\}$.
- L'ensemble des polynômes $\mathbb{Z}[X]$ est un anneau commutatif unitaire intègre pour l'addition et la multiplication des polynômes et $\mathbb{U}(\mathbb{Z}[X]) = \{\pm 1\}$.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps (mais pas $\mathbb{Z}$!).

Remarque 2.1.2

1. *Attention, dans un anneau, il peut y avoir des éléments non inversibles (penser par exemple à 3 dans $\mathbb{Z}$).*
2. *Dans un anneau commutatif, les identités remarquables telles que $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^k$ restent vraies. Ce n'est plus le cas dans un anneau non commutatif où on a seulement par exemple $(a+b)^2 = a^2 + ab + ba + b^2$.*

Soit A un anneau. Un sous-anneau de l'anneau unitaire A est une partie $B \subset A$ qui est elle même un sous-anneau unitaire. Cela revient à dire que $(B, +, 0)$ est un sous-groupe de $(A, +, 0)$ qui contient 1 stable par la multiplication dans A (si b et b' dont dans B, alors $b \cdot b'$ est aussi dans B). Très souvent, pour montrer qu'un ensemble est un anneau, on montre qu'il s'agit d'un sous-anneau d'un anneau déjà connu.

Soient $(A, +, \cdot)$ et $(B, \oplus, \otimes)$ deux anneaux unitaires. On note 0_A et 1_A (resp. 0_B et 1_B) les éléments neutres pour $+$ et $\cdot$ dans A (resp. pour $\oplus$ et $\otimes$ dans B).

Définition 2.1.3 *Un morphisme d'anneaux de A vers B est une application $f : A \to B$ telle que $f(1_A) = 1_B$ et pour tout a et a' dans A on ait*

1. $f(a + a') = f(a) \oplus f(a')$,
2. $f(a \cdot a') = f(a) \otimes f(a')$.

Puisque f est en particulier un morphisme de groupe, on a $f(0_A) = 0_B$. On note $\ker f = \{a \in A \mid f(a) = 0\}$. Les notions d'endomorphismes ($A = B$), d'isomorphismes (f est bijective), d'automorphisme ($A = B$ et f est bijective) se définissent comme pour les groupes. En particulier f est injective ssi $\ker f = \{0\}$.

Exemple 1 *Soit $A \in M_n(\mathbb{R})$. On définit un morphisme d'anneaux $f : \mathbb{R}[X] \to M_n(\mathbb{R})$ en posant $f(P) = P(A)$ où $P = a_0 + a_1 X + \cdots + a_n X^n$ est un polynôme de $\mathbb{R}[X]$ et $P(A) = a_0 I_n + a_1 A + \cdots + a_n A^n$.*

exercice 1 *Soit $f : A \to B$ un morphisme d'anneaux unitaires. Vérifier que $f^{-1}(B)$ est un sous-anneau de A et $\operatorname{Im} f = f(A)$ un sous-anneau de B.*

Hypothèse 1 *Dans la suite, les anneaux considérés seront tous supposés commutatifs et unitaires.*

2.2 Idéaux et anneaux (commutatifs) quotients

La notion d'*idéal* est centrale pour les anneaux. Soit I un sous-ensemble non vide de A.

Définition 2.2.1 *On dit que $I \subset A$ est un idéal si I est un sous-groupe de $(A, +)$ tel que $aI \subset I$ pour tout $a \in A$.*

Cela signifie que tous les produits de la forme ax avec $a \in A$ et $x \in I$ sont dans I. Noter que si un idéal I contient un élément inversible, alors $I = A$ car alors $1 \in I$. Attention à ne pas confondre la notion d'idéal avec celle de sous anneau. Dans un idéal, le produit $ax \in I$ dès lors que a ou x est dans I.

Dans un anneau, les idéaux engendrés par un seul élément sont dits *principaux*. On note alors (a) l'idéal enjendré par l'élément a. Les éléments de (a) sont les multiples de a, autrement dit

$$(a) = \{ax \mid x \in A\}.$$

Un anneau dans lequel tous les idéaux sont principaux est dit *principal*.

Exemple 2

- *Pour tout entier n, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de $\mathbb{Z}$.*
- *Soit $\alpha \in \mathbb{C}$ et $I(\alpha) = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$. Alors $I(\alpha)$ est un idéal de $\mathbb{Q}[X]$.*
- *Le noyau d'un morphisme d'anneaux $f : A \to B$ est un idéal de A. En effet, c'est un sous-groupe puisque f est aussi un morphisme de groupes et pour $a \in A, x \in \ker f$ on a $f(ax) = f(a)f(x) = 0_B$. Donc $ax \in \ker f$.*

exercice 2 *Soient I et J deux idéaux de A. Montrer que*

$$I \cap J \text{ et } I + J = \{i + j \mid i \in I, j \in J\}$$

sont des idéaux de A.

Pour tout $a \in A$, on note $\overline{a} := a + I$ la classe de a pour la relation d'équivalence $a \sim a'$ ssi $a - a' \in I$.

Proposition 2.2.2 *L'addition et la multiplication*

$$\overline{a} + \overline{b} = \overline{a + b} \text{ et } \overline{a}\overline{b} = \overline{ab}$$

sont bien définies dans $A/\sim$. Elles confèrent à $A/\sim$ un structure d'anneau commutatif unitaire appelé quotient de A par I et noté A/I.

Preuve. Pour l'addition, il suffit d'utiliser la notion de groupe quotient. En effet A est un groupe abélien pour l'addition et I est un sous groupe (forcément normal). Pour la multiplication, l'idée est de poser $\overline{a} \times \overline{b} = \overline{ab}$. Nous devons pour cela vérifier que le résultat ne dépend pas des représentants choisis dans les classes $\overline{a}$ et $\overline{b}$. Soient donc $a, a' \in \overline{a}$ et $b, b' \in \overline{b}$. Nous devons montrer que $\overline{ab} = \overline{a'b'}$ ce qui revient à dire que $ab - a'b'$ doit être dans I. Or $ab - a'b' = (a - a')b + (b - b')a'$ (ici on utilise que A est commutatif). Comme $a - a' \in I$ et $b - b' \in I$, on a bien $ab - a'b' \in I$. □

Exemple 3

1. *Pour tout entier n, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de $\mathbb{Z}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est alors défini comme l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.*
2. *Dans $\mathbb{Z}/3\mathbb{Z}$, nous avons les tables d'addition et de multiplication suivantes*

$$\begin{array}{|c|c|c|c|} \hline + & \overline{\mathbf{0}} & \overline{\mathbf{1}} & \overline{\mathbf{2}} \\ \hline \overline{\mathbf{0}} & \overline{0} & \overline{1} & \overline{2} \\ \overline{\mathbf{1}} & \overline{1} & \overline{2} & \overline{0} \\ \overline{\mathbf{2}} & \overline{2} & \overline{0} & \overline{1} \\ \hline \end{array} \quad et \quad \begin{array}{|c|c|c|c|} \hline \times & \overline{\mathbf{0}} & \overline{\mathbf{1}} & \overline{\mathbf{2}} \\ \hline \overline{\mathbf{0}} & \overline{0} & \overline{\mathbf{0}} & \overline{\mathbf{0}} \\ \overline{\mathbf{1}} & \overline{\mathbf{0}} & \overline{1} & \overline{2} \\ \overline{\mathbf{2}} & \overline{\mathbf{0}} & \overline{2} & \overline{1} \\ \hline \end{array}$$

3. *De façon analogue, si $P \in \mathbb{Z}[X]$, l'idéal $(P) = P\mathbb{Z}[X]$ des multiples de P permet de définir l'anneau quotient $\mathbb{Z}[X]/P\mathbb{Z}[X] = \mathbb{Z}[X]/(P)$.*

La projection canonique $p : A \to A/I$ qui associe à tout $a \in A$ sa classe $\overline{a}$ est un morphisme surjectif d'anneaux tel que $\ker f = I$. Plus généralement si $f : A \to B$ est un morphisme d'anneaux, alors $\ker f$ est un idéal et l'application

$$\overline{f} : \begin{cases} A/\ker f \to B \\ \overline{a} \longmapsto f(a) \end{cases}$$

est bien définie. Pour le voir, il faut vérifier que $f(a)$ ne dépend pas du représentant $a \in \overline{a}$ choisi. Mais si $a' \in \overline{a}$, nous avons $a - a' \in \ker f$ et donc $f(a) = f(a')$. Comme f est un morphisme d'anneaux, $\overline{f}$ aussi et on a $\operatorname{Im} f = \operatorname{Im} \overline{f}$. On obtient en particulier le théorème d'isomorphisme :

Proposition 2.2.3 *Soit $f : A \to B$ un morphisme d'anneaux. Alors $A/\ker f$ est isomorphe à $\operatorname{Im} f \subset B$.*

Exemple 4 *Soit $f : \mathbb{Q}[X] \to \mathbb{C}$ défini par $f(P) = P(i)$ pour tout $P \in \mathbb{Q}[X]$. On vérifie que $\ker f = (X^2+1)$ (idéal engendré par X^2+1). Par ailleurs, $\operatorname{Im} f = \{a + ib \mid (a,b) \in \mathbb{Q}^2\}$. Donc $\mathbb{Q}[X]/(X^2+1) \simeq \mathbb{Q}[i]$ avec $\mathbb{Q}[i] = \{a + ib \mid (a,b) \in \mathbb{Q}^2\}$.*

Lemme 2.2.4 *Soit A un anneau commutatif unitaire. Alors A est est un corps ssi ses seuls idéaux sont A et $\{0\}$.*

Preuve. Si A est un corps et I un idéal de A distinct de $\{0\}$, alors I contient au moins un élément inversible et donc $1 \in I$ et finalement $A = I$. Réciproquement si A et $\{0\}$ sont les seuls idéaux de A, pour tout x non nul dans A on a $(x) = A$. Donc $1 \in (x)$ ce qui signifie qu'il existe $y \in A$ tel que $xy = yx = 1$. Donc tout élément non nul de A est inversible et A est un corps. □

2.3 Idéaux maximaux

Un idéal I de l'anneau commutatif A est maximal (pour l'inclusion) si les seuls idéaux de A qui contiennent I sont I et A. Autrement dit, pour tout idéal J de A tel que

$$I \subset J \subset A$$

on a $I = J$ ou $I = A$.

Exemple 5

1. *Dans $\mathbb{Z}$, l'idéal $2\mathbb{Z}$ est maximal. En effet si J est un idéal de $\mathbb{Z}$ contenant $2\mathbb{Z}$ et au moins un nombre impair $n = 2k+1$, il contient 1 et donc $I = \mathbb{Z}$! Nous verrons dans le chapitre suivant qu'il est très facile de déterminer tous les idéaux maximaux de $\mathbb{Z}$.*
2. *Dans $\mathbb{Q}[X]$, l'idéal (X^2) n'est pas maximal car nous avons $(X^2) \subsetneq (X) \subsetneq \mathbb{Q}(X)$. Là encore, nous verrons que les idéaux maximaux de $\mathbb{Q}[X]$ sont très faciles à décrire.*

La notion d'idéal maximal est très importante à cause du théorème suivant :

Théorème 2.3.1 *Soit A un anneau commutatif unitaire et I un idéal de A disctinct de A. Alors A/I est un corps si et seulement si I est un idéal maximal.*

Preuve. D'après le Lemme 2.2.4, il s'agit de montrer que les seuls idéaux de A/I sont $\{\overline{0}\}$ et A/I. Soit donc $\overline{J}$ un idéal de A/I. Nous avons vu que la projection canonique $p : A \to A/I$ qui associe à tout $a \in A$ sa classe $\overline{a}$ est un morphisme surjectif d'anneaux. Donc $p^{-1}(\overline{J})$ est un idéal de A. Notons $J = p^{-1}(\overline{J})$ cet idéal. Nous avons

$$J = p^{-1}(\overline{J}) = \{a \in A \mid p(a) = \overline{a} \in \overline{J}\}.$$

Mais par définition de A/I, pour tout $a \in I$, $p(a) = \overline{0} \in \overline{J}$. On voit donc que l'idéal I est contenu dans J.

Supposons maintenant que I est maximal. Alors comme $I \subset J$ nous avons $I = J$ ou $J = A$. Dans le premier cas, $\overline{J} = p(I) = \{\overline{0}\}$. Dans le deuxième $\overline{J} = p(A) = A/I$. Ainsi $\{\overline{0}\}$ et A/I sont les seuls idéaux de A/I qui est par conséquent un corps.

Suposons pour terminer que A/I est un corps. Soit J un idéal de A tel que $I \subset J \subset A$. Alors $\overline{J} = p(J)$ est un idéal du corps A/I. Donc on a $\overline{J} = \{\overline{0}\}$ ou bien $\overline{J} = A/I = \operatorname{Im} p$. Dans le premier cas, $J = \ker p = I$ et dans le second $J = p^{-1}(A/I) = A$.□

Ce théorème va nous servir très souvent dans la suite.

Exemple 6

1. *$\mathbb{Z}/2\mathbb{Z}$ est un corps puisque $2\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$.*
2. *$\mathbb{Q}[X]/(X^2)$ n'est pas un corps. On le vérifie facilement en remarquant que $\overline{X}^2 = \overline{X^2} = \overline{0}$ dans $\mathbb{Q}[X]/(X^2)$, donc $\mathbb{Q}[X]/(X^2)$ n'est même pas intègre.*

Chapitre 3

L'anneau $\mathbb{Z}$ et ses anneaux quotients

3.1 Division euclidienne et idéaux de $\mathbb{Z}$

Nous admettrons le théorème suivant en apparence innocent mais dont la preuve rigoureuse demande un peu de travail. Notamment elle utilise le fait que toute partie non vide de $\mathbb{N}$ possède un élément minimal et la construction de $\mathbb{Z}$ à partir de $\mathbb{N}$.

Théorème 3.1.1 (Divison euclidienne des entiers) *Soient a et b deux entiers non nuls de $\mathbb{Z}$. Il existe un unique couple (q, r) dans $\mathbb{Z}^2$ tel que*

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

On dit que $\mathbb{Z}$ est un anneau Euclidien.

Rappellons que la division euclidienne permet aussi de calculer le développement décimal d'un rationnel de $\mathbb{Q}$ à n'importe quel ordre. Nous verrons aussi qu'elle confère à $\mathbb{Z}$ la structure d'un *anneau Euclidien*. Ce type d'anneau se définit comme suit.

Définition 3.1.2 *Soit A un anneau commutatif unitaire intègre et une application $\varphi : A\backslash\{0\} \to \mathbb{N}$. On dit que A est euclidien pour le stathme φ si pour tout $a \in A$ et $b \in B \setminus \{0\}$, il existe q et r dans A tels que*

$$a = bq + r \text{ et } r = 0 \text{ où } \varphi(r) < \varphi(b).$$

Notamment $\mathbb{Z}$ est un anneau euclidien pour le stathme valeur absolue. Noter que (q, r) n'est pas supposé unique dans la définition.

exercice 3 *Montrer que les nombres rationnels sont ceux dont le développement décimal est périodique.*

On dit que a est divisible par b lorsque le reste de la division euclidienne vaut 0, autrement dit lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = bq$. Dans ce cas b divise a ce que l'on note $b \mid a$. Un entier p qui n'est divisible que par ± 1 et $\pm p$ est dit premier.

Proposition 3.1.3

1. *Les seuls idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (donc $\mathbb{Z}$ est un anneau principal).*

2. $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. En particulier $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $n = \pm m$.

3. Pour $n \neq \pm 1$, l'idéal $n\mathbb{Z}$ est maximal si et seulement si n est premier.

Preuve. 1 : Soit I un idéal non réduit à $\{0\}$ de $\mathbb{Z}$. Alors $I \cap \mathbb{N}^*$ est non vide. Notons n l'élément minimal de $I \cap \mathbb{N}^*$. Pour tout a dans I, la division euclidienne de a par n donne des entiers q et r tels que $a = nq + r$ et $0 \leq r < n$. Mais alors $r = a - nq$ est dans I puisque I est un idéal. Comme $n = \min I \cap \mathbb{N}^*$ et $r < n$, on doit avoir $r = 0$. Ainsi a est-il dans $n\mathbb{Z}$. Nous avons montré que $I \subset n\mathbb{Z}$. Nous avons aussi $n\mathbb{Z} \subset I$ puisque $n \in I$ et I est un idéal. Finalement $I = n\mathbb{Z}$ comme souhaité.
2 : Si $n\mathbb{Z} \subset m\mathbb{Z}$, on doit avoir $n \in m\mathbb{Z}$ donc $m \mid n$. Réciproquement si $m \mid n$, il existe q tel que $n = qm$ et donc $n \in m\mathbb{Z}$ ce qui entraîne que $n\mathbb{Z} \subset m\mathbb{Z}$.
3 : Supposons n premier dans $\mathbb{N}$. Soit I idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. D'après le point 1, on peut supposer $I = m\mathbb{Z}$ avec $m > 0$. On a donc $n\mathbb{Z} \subset m\mathbb{Z}$ et d'après le point 2, $m \mid n$. Donc, puisque m est premier, $m = n$ et alors $I = n\mathbb{Z}$ ou bien $m = 1$ et alors $I = \mathbb{Z}$. L'idéal $n\mathbb{Z}$ est bien maximal. Réciproquement si $n\mathbb{Z}$ est maximal et $m > 0$ divise n, nous avons $n\mathbb{Z} \subset m\mathbb{Z}$. Cela implique que $n\mathbb{Z} = m\mathbb{Z}$ et alors $n = m$ ou bien $m\mathbb{Z} = \mathbb{Z}$ et alors $m = 1$. □

En utilisant le Théorème 2.3.1 et le théorème précédent, on obtient le corollaire suivant :

Corollaire 3.1.4 *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

3.2 Théorème fondamental de l'arithmétique

Notons $\mathcal{P}$ l'ensemble des entiers naturels premiers. L'ensemble de tous les nombres premiers est donc $\mathcal{P} \cup (-\mathcal{P})$.

Lemme 3.2.1 *Soit $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Si n n'est pas premier, il existe $p \in \mathcal{P}$ tel que p divise n.*

Preuve. On peut suposer n positif. Si on note $D = \{\text{diviseurs } d \text{ de } n \text{ tel que } 1 < d < n\} \subset \mathbb{N}$, on a l'alternative :

- Soit $D = \emptyset$ et alors n est premier.
- Soit $D \neq \emptyset$ et D a un plus petit élément p_1. Alors p_1 est premier car si $p_1 = q_1 r_1$ avec $q_1 < p_1$, alors $q_1 | n$ donc p_1 n'est pas le plus petit élément de D.

□

Proposition 3.2.2 *$\mathcal{P}$ est un ensemble infini.*

Preuve. Supposons par l'absurde que $\mathcal{P}$ est fini et contient N éléments. Posons $\mathcal{P} = \{p_1 < p_2 < \cdots < p_N\}$ la liste ordonnée des éléments de $\mathcal{P}$ et considérons l'entier $a = p_1 \times \cdots \times p_N + 1$. Comme $a > p_N$, l'entier a n'est pas premier. D'après le lemme précédent, il admet un diviseur premier $p \in \mathcal{P}$. On doit donc avoir p qui divise a et aussi $p_1 \times \cdots \times p_N$. Mais alors comme $1 = a - p_1 \times \cdots \times p_N$, on obtient que p divise 1 ce qui est impossible. Donc $\mathcal{P}$ est infini.□

Lemme 3.2.3 (d'Euclide) *Si p premier divise le produit $a_1 \dots a_n$ où $n \geq 2$ alors il existe un entier k tel que $p | a_k$.*

Preuve. Là encore, on peut supposer tous les entiers positifs. Comme p divise $a_1 \dots a_n$, on a $\overline{a_1 \dots a_n} = \overline{a_1} \cdots \overline{a_n} = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Mais comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il est intègre et cela implique que l'un au moins des $\overline{a_k}$ vaut $\overline{0}$ c'est à dire que $p \mid a_k$. □

Corollaire 3.2.4 *Si p premier divise le produit $q_1 \dots q_n$ où $n \geq 1$ et tous les q_i sont des nombres premiers alors il existe i tel que $p = \pm q_i$.*

Théorème 3.2.5 (fondamental de l'arithmétique) *Soit n un entier non nul. Alors il existe un nombre $\varepsilon \in \{\pm 1\}$ et une suite $(p_i, \alpha_i)_{1 \leq i \leq r}$ d'éléments de $\mathcal{P} \times \mathbb{N}^*$ tout deux uniques tels que*

$$n = \varepsilon p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Preuve. Il suffit de le démontrer pour les nombres positifs. On procède en deux temps :
Existence :
D'après le Lemme 3.2.1, soit n est premier et on a fini, soit il existe un facteur premier p_1 pour n et il existe n_1 tel que $n = n_1 p_1$. On recommence alors avec n_1 :
Ou bien n_1 est premier et on a fini,
Ou bien on trouve p_2 qui divise n_2 et $n = p_1 p_2 n_2$.
Ou bien n_2 est premier et on a fini ou bien il existe un p_3 premier qui divise n_2. Si le procédé ne devait pas s'arrêter, on construirait une suite strictement décroissante (car 1 n'est pas premier) d'entiers n_i tous strictement supérieurs à 1. C'est bien sûr impossible et le procédé ci-dessus se termine en un nombre fini d'opérations.
Unicité : Supposons qu'il existe une deuxième suite $q_1, \dots, q_l$ de premiers de $\mathcal{P}$ telle que

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l.$$

On veut montrer que $l = k$ et que pour tout $i \in \{1, \dots, k\}$, il existe un indice j_i de sorte que $p_i = q_{j_i}$. On utilise le corollaire ci-dessus : p_1 divise $q_1 q_2 \dots q_l$. Donc il existe i_1 tel que $p_1 = q_{i_1}$. On simplifie par p_1 et une récurrence sur k vu comme le plus petit entier m tel que n s'écrive comme produit de m entiers donne le résultat en utilisant bien sur que si $k = 1$ le procédé ci-dessus indique que $1 = q_1 \dots q_l$ ce qui dit que chaque q_j est inversible , impossible donc $l = k = 1$.□

3.3 PPCM et PGCD

3.3.1 Definition et lien avec les idéaux

D'après le théorème précédent, tout entier $a \in \mathbb{Z}$ se décompose de façon unique sous la forme

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

où les $v_p(a)$ son nuls sauf un nombre fini d'entre eux. L'entier $v_p(a)$ s'appelle la *valuation p-adique* de a. Il est alors clair que

$$a \mid b \Longleftrightarrow v_p(a) \leq v_p(b) \text{ pour tout } p \in \mathcal{P}.$$

On dispose alors d'une notion naturelle de ppcm et de pgcd en posant

$$\text{ppcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\sup(v_p(a), v_p(b))} \text{ et } \text{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\inf(v_p(a), v_p(b))}.$$

Lorsque $\text{pgcd}(a,b) = 1$, on dit que a et b sont *premiers entre eux.*

Proposition 3.3.1

1. $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = a \times b$.
2. $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a,b)\mathbb{Z}$
3. $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a,b)\mathbb{Z}$.
4. *Théorème de Bachet-Bézout : il existe deux entiers u et v tels que $au + bv = \text{pgcd}(a,b)$.*

Preuve. L'assertion 1 découle immédiatement des définitions puisque

$$\sup(v_p(a), v_p(b)) + \inf(v_p(a), v_p(b)) = v_p(a) + v_p(b).$$

Pour les assertions 2 et 3, comme on sait que $a\mathbb{Z} \cap b\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$ qui est principal, il existe d et m dans $\mathbb{N}$ tels que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. L'entier m est un multiple de a et b donc $\text{ppcm}(a,b) \mid m$. Par ailleurs, $\text{ppcm}(a,b) \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ donc $m \mid \text{ppcm}(a,b)$. On a bien $m = \text{ppcm}(a,b)$. Comme $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$, l'entier d divise a et b. Donc $d \mid \text{pgcd}(a,b)$. Par ailleurs, comme $a\mathbb{Z} \subset \text{pgcd}(a,b)\mathbb{Z}$ et $b\mathbb{Z} \subset \text{pgcd}(a,b)\mathbb{Z}$, nous avons

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset \text{pgcd}(a,b)\mathbb{Z}.$$

Donc $\text{pgcd}(a,b) \mid d$. On a bien $d = \text{pgcd}(a,b)$. L'assertion 4 découle de la 3. □

Remarque 3.3.2 *Les entiers u et v apparaissant dans le théorème de Bachet-Bézout ne sont pas uniques. Noter également que si u et v sont tels que $au + bv = \delta$, alors* $\text{pgcd}(a,b)$ *divise δ. En particulier, dès que l'on a trouvé u et v tels que $au + bv = 1$, on a* $\text{pgcd}(a,b) = 1$.

Le corollaire bien pratique suivant se déduit immédiatement.

Corollaire 3.3.3 (Lemme de Gauss) *Soient a et b deux entiers et k un entier divisant ab. Alors si k divise ab en étant premier avec b, il divise a.*

3.3.2 L'algorithme d'Euclide

On se donne deux entiers a et b relatifs dont on veut déterminer le PGCD et aussi un couple (u,v) réalisant l'identé de Bachet-Bézout plus haut. On commence par choisir a et b naturels avec $b \leq a$ car $\text{pgcd}(a,b) = \text{pgcd}(-a,b) = \text{pgcd}(b,a)$.

De deux choses l'une

- Ou bien $b|a$ et $\text{pgcd}(a,b) = b$ et on a terminé,
- Ou bien $b \nmid a$ et en effectuant la division euclidienne de a par b on trouve un quotient q et un reste $0 < r < b$. Mais comme $a = bq + r$ nous avons $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$ ce qui d'après la définition du PGCD de a et de b devient $\text{pgcd}(a,b) = \text{pgcd}(b,r)$

On a donc la "descente" suivante :
Posons $r_0 = r$

$$a = bq_0 + r_0 \quad r_0 < b, \quad \text{pgcd}(a,b) = \text{pgcd}(b,r_0)$$
$$b = r_0 q_1 + r_1 \quad r_1 < r_0, \quad \text{pgcd}(a,b) = \text{pgcd}(r_0,r_1)$$

Tant que $r_k \neq 0$ faire

$$(\forall k \geq 1) \quad r_{k-1} = r_k q_{k+1} + r_{k+1} \quad r_{k+1} < r_k, \quad \text{pgcd}(a,b) = \text{pgcd}(r_k, r_{k+1})$$

et l'algorithme s'arrête quand $r_m = 0$ ce qui signifie que $\text{pgcd}(a, b) = r_{m-1}$.
En remontant les équations :

$$\text{pgcd}(a,b) = r_{m-1} = r_{m-3} - r_{m-2}q_{m-1} = r_{m-5} - r_{m-4}q_{m-3} - q_{m-1}(r_{m-4} - r_{m-3}q_{m-2}) = \cdots = ua + bv$$

Remarque : Comme $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, on peut voir que $q_{k+2} = [\frac{r_k}{r_{k+1}}]$.

On peut alors écrire une procédure sous forme récursive
pgcd $:= proc(a, b)$
- Si $(b > a)$ alors $\text{pgcd}(b, a)$
- sinon si $b = 0$ alors retourner a
- sinon $r := a - b[\frac{a}{b}]$; calculer $\text{pgcd}(b, r)$
- fin si

Pour évaluer le coût il faut imaginer la pire des situations autrement dit le cas où l'algorithme se déroule avec des quotients qui sont toujours 1. Si on suppose que $r_{m+1} = 0$, on a

$$\begin{aligned} r_m &= r_{m-1} = 1 \\ r_{m-2} &= r_m + r_{m-1} \\ r_i &= r_{i+1} + r_{i+2} \\ b &= r_0 + r_1 \\ a &= b + r_0 \end{aligned}$$

et on reconnait les relations de récurrence de la suite de Fibonaci. Grâce à cette remarque , on peut démontrer (cf Demazure) que l'algorithme d'Euclide pour calculer $\text{pgcd}(a, b)$ avec $0 < b \leq a$ prend au plus $\frac{3}{2}\ln(b) + 1$ étapes.

Exemple 7 *Déterminer* $\text{pgcd}(5, 123)$ *et les coefficients de Bézout (qui valent* -49 *et* 2*) en utilisant l'algorithme d'Euclide.*

3.4 Congruences et anneaux $\mathbb{Z}/n\mathbb{Z}$

Pour tout entier $n \in \mathbb{Z}$, on rappelle que $\equiv$ désigne la relation d'équivalence définie sur $\mathbb{Z}$ par

$$a \equiv b \bmod n \iff b - a \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} \mid b - a = kn.$$

Noter également que si r est le reste de la division euclidienne de a par b, on a $a \equiv r \bmod n$. En pratique faire des calculs "modulo n" ou dans $\mathbb{Z}/n\mathbb{Z}$ revient essentiellement à la même chose. Notamment les propriétés

$$\begin{cases} a \equiv b \bmod n \\ a' \equiv b' \bmod n \end{cases} \implies a + a' \equiv b + b' \bmod n \text{ et } aa' \equiv bb' \bmod n$$

qui peuvent facilement se démontrer à partir de la définition de $\equiv$ sont équivalentes au fait que l'addition et la multiplication sont bien définies dans $\mathbb{Z}/n\mathbb{Z}$. De façon plus générale toute proposition portant sur les congruences modulo n admet une forme équivalente dans $\mathbb{Z}/n\mathbb{Z}$. Dans ce qui suit, on utilisera le plus souvent la structure d'anneau dans $\mathbb{Z}/n\mathbb{Z}$ qui permet une rédaction moins lourde. Le lecteur est encouragé à chercher des preuves alternatives n'utilisant que les congruences.

exercice 4 *Soit p un nombre premier. Sans utiliser que $\mathbb{Z}/p\mathbb{Z}$ est un corps, redémontrer à l'aide de congruence le Lemme d'Euclide*[1] *: si $p \mid ab$ alors $p \mid a$ ou $p \mid b$ (on pourra raisonner par l'absurde et utiliser la division euclidienne par p).*

3.4.1 Inversibles modulo n

Proposition 3.4.1

1. *Les éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{a}$ telles que* $\mathrm{pgcd}(a, n) = 1$.
2. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est un nombre premier.*
3. *Les générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. L'élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible ssi il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{au} = \overline{1}$. Cela revient à $au - 1 \in n\mathbb{Z}$. Autrement dit $\overline{a}$ est inversible ssi il existe $u, v \in \mathbb{Z}$ tels que $au - 1 = n(-v)$. Cette équalité se reécrit sous la forme $au + nv = 1$. Or, d'après le théorème de Bézout sur les entiers, on sait que l'existence d'une telle identité équivaut à a et n premiers entre eux. Ainsi $\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{a} \mid \mathrm{pgcd}(a, n) = 1\}$. En particulier $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi tous les nombres $\{1, \ldots, n-1\}$ sont premiers avec n, autrement dit, si n est premier (on savait déjà que n premier implique que $\mathbb{Z}/n\mathbb{Z}$ est un corps). Pour démontrer la dernière assertion, on observe que $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ ssi le groupe engendré par $\overline{a}$ contient $\overline{1}$ (puisque $\overline{1}$ engendre clairement $\mathbb{Z}/n\mathbb{Z}$). Cela revient à dire qu'il existe un entier k tel que $k\overline{a} = \overline{k}\overline{a} = \overline{1}$, autrement dit que $\overline{a}$ est inversible. □

Remarque 3.4.2 *Noter que la preuve ci-dessus permet de déterminer l'inverse d'un élément de $\mathbb{Z}/n\mathbb{Z}$ lorsqu'il existe : il suffit de déterminer les coefficients de Bézout correspond grâce à l'algorithme d'Euclide. Par exemple $\overline{5}$ est inversible dans $\mathbb{Z}/8\mathbb{Z}$. Par ailleurs, on a $8 \times 2 - 5 \times 3 = 1$. Donc l'inverse de $\overline{5}$ est $\overline{-3} = \overline{5}$ ce que l'on vérifie aussi en calculant $\overline{5} \times \overline{5} = \overline{25} = \overline{1}$.*

Pour tout n, *l'indicatrice d'Euler* $\varphi(n)$ désigne le nombre d'entiers entre 1 et n premiers avec n. D'après ce qui précède

$$\mathrm{card}((\mathbb{U}(\mathbb{Z}/n\mathbb{Z})) = \varphi(n).$$

Comme $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ est un groupe fini pour $\times$, le théorème de Lagrange permet d'obtenir le corollaire suivant (théorème d'Euler pour n quelconque et petit théorème de Fermat pour n premier) :

Corollaire 3.4.3 *Pour tout entier a premier avec n, on a $a^{\varphi(n)} \equiv 1 \bmod n$.*

exercice 5 *Soit p un nombre premier. Nous allons rémontrer sans utiliser les résultats sur les groupes le petit théorème de Fermat $a^p \equiv a \bmod p$ en procédant par récurrence sur a.*

1. *Vérifier que le théorème est vrai pour $a = 0$ et 1.*
2. *Montrer que $(a + 1)^p \equiv a + 1 \bmod p$.*
3. *Conclure.*

[1] Cela permet d'obtenir une preuve plus élémentaire du théorème fondamental de l'arithmétique sans utiliser de structure quotient.

3.4.2 Lemme chinois

La proposition suivante est connue sous le nom de Lemme chinois.

Proposition 3.4.4 *Si p et q sont premiers entre eux, on a un* ***isomorphisme d'anneaux***

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Preuve. On considère l'application suivante :

$$\begin{array}{rccc} \theta: & \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ & m & \mapsto & (m(\mathrm{mod}\, p), m(\mathrm{mod}\, q)) \end{array}$$

Il est facile de voir qu'il s'agit d'un morphisme d'anneaux :

$$\theta(m+m') = \theta(m) + \theta(m') \text{ et } \theta(mm') = \theta(m)\theta(m')$$

de noyau $pq\mathbb{Z}$. En effet, $\theta(m) = 0$ signifie que $p \mid m$ et $q \mid m$. Donc $\mathrm{pgcd}(p,q) = pq$ divise m. Comme θ est de plus surjectif, les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes d'après la Proposition 2.2.3. □

Là encore, on peut énoncer le lemme chinois en termes de congruence : si p et q sont premiers, le système de congruences

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}$$

admet une unique solution dans $\{0, 1, \ldots, pq-1\}$. Pour résoudre ce système, il suffit de déterminer e_1 et e_2 tels que

$$\begin{cases} e_1 \equiv 0 \bmod p \\ e_1 \equiv 1 \bmod q \end{cases} \text{ et } \begin{cases} e_2 \equiv 1 \bmod p \\ e_2 \equiv 0 \bmod q \end{cases}.$$

On aura alors

$$x = ae_1 + be_2.$$

Maintenant e_1 et e_2 sont donnés par l'identité de Bézout pour p et q : $pu + qv = 1$. En effet

$$\begin{cases} pu \equiv 0 \bmod p \\ pu \equiv 1 \bmod q \end{cases} \text{ et } \begin{cases} qv \equiv 1 \bmod p \\ qu \equiv 0 \bmod q \end{cases}.$$

Donc $e_1 = pu$ et $e_2 = qv$.

Il est également facile de voir que ses résultat s'étendent immédiatement aux cas où on considère une suite $p_1, \ldots, p_r$ de nombres *deux à deux premiers entre eux*[2]. Nous avons alors

$$\mathbb{Z}/p_1 \cdots p_r\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$$

et une unique solution dans $\{0, 1, \ldots, p_1 \cdots p_r - 1\}$ au système de congruences

$$\begin{cases} x \equiv a_1 \bmod p_1 \\ \vdots \\ x \equiv a_r \bmod p_r \end{cases}$$

[2] Noter que les nombres $p_1, \ldots, p_r$ ne sont pas supposés premiers. En revanche, l'hypothèse que les nombres sont premiers entre eux, c'est à dire sans facteur commun, ne suffit pas (prendre $3, 6$ et 8 par exemple).

exercice 6 *Une bande de* 17 *pirates s'est emparée d'un nombre* n *de pièces d'or identiques. Ils décident de se les partager équitablement et de donner le reste au capitaine qui devrait alors recevoir* 3 *pièces. Une bagarre éclate et* 6 *d'entre-eux sont tués. Le capitaine devrait alors recevoir* 4 *pièces. Dans un naufrage ultérieur, seul le butin,* 7 *pirates dont leur capitaine sont sauvés et le partage laisse finalement* 5 *pièces à ce dernier. Quel est le nombre minimal de pièces d'or* n *possible ?*

3.4.3 Calcul de $\varphi(n)$

Nous sommes maintenant en mesure de calculer $\varphi(n)$ pour n'importe quel entier n. Pour cela observons tout d'abord que si p est un nombre premier et $\alpha \geq 1$ un entier naturel, nous avons

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

Pour le voir, il suffit d'enlever à l'ensemble des entiers compris entre 1 et p^α (qui comporte p^α éléments) l'ensemble de ceux qui sont divisibles par p. Ce dernier ensemble comporte $p^{\alpha-1}$ éléments puisque les diviseurs de p sont $p, 2p, 3p$ etc et forment une progression arithmétique de raison p. Pour terminer il suffit d'observer que grâce au lemme chinois, nous avons également

$$\varphi(pq) = \varphi(p)\varphi(q)$$

dès que p et q sont premiers entre eux.

Proposition 3.4.5 *Soit* n *un entier naturel. alors*

$$\varphi(n) = \prod_{p\in\mathcal{P}, p|n} p^{v_p(n)-1}(p-1) = n \prod_{p\in\mathcal{P}, p|n} \left(1 - \frac{1}{p}\right).$$

exercice 7 *On choisit au hasard suivant la loi uniforme un entier entre* 1 *et* n*. Montrer que la probabilité qu'il soit premier avec* n *ne dépend que de l'ensemble des diviseurs premiers de* n *et pas des valuations associées.*

Chapitre 4

Les anneaux de polynômes

4.1 Quelques définitions et propriétés élémentaires

Etant donné A un anneau commutatif unitaire intègre, on note $A[X]$ l'anneau des polynômes en l'indéterminée X à coefficients dans A. On note $d(P)$ le degré du polynôme $P \in A[X]$. Par convention $d(0) = -\infty$. Comme A est intègre, on a pour P et Q deux polynômes de $A[X]$

$$d(PQ) = d(P) + d(Q).$$

En particulier $A[X]$ est lui aussi un anneau intègre. Attention, cela devient faux si A n'est pas intègre. Par exemple dans $\mathbb{Z}/4\mathbb{Z}[X]$, on a $(2X)^2 = 0$. Dans la suite, on supposera donc que A est intègre. On veillera par ailleurs à ne pas confondre un polynôme $P \in A[X]$ avec la fonction polynomiale correspondante

$$f_P : \begin{cases} A \to A \\ x \longmapsto P(x). \end{cases}$$

La fonction polynomiale peut en effet être nulle alors que P n'est pas nul.
Exemple. $A = \mathbb{Z}/3\mathbb{Z}$ et $P(X) = X(X^2 - 1) \in \mathbb{Z}/3\mathbb{Z}[X]$. Alors $f_P(x) = 0$ pour tout $x \in \mathbb{Z}/3\mathbb{Z}$. Pourtant P n'est pas le polynôme nul.

Proposition 4.1.1 *Les éléments inversibles de $A[X]$ sont les constantes inversibles, autrement dit $U(A[X]) = U(A)$.*

Preuve. Soit P inversible dans $A[X]$. Il existe $Q \in A[X]$ tel que $PQ = 1$. Comme A est intègre, on a alors que $d(P) + d(Q) = 0$. Donc $d(P) = d(Q) = 0$ et P est une constante inversible.□

De façon plus générale si $X_1, \ldots, X_n$ est un ensemble d'indéterminées (supposées algébriquement indépendantes), $A[X_1, \ldots, X_n]$ est l'anneau des polynômes sur A en les variables $X_1, \ldots, X_n$.

Exemple. $P(X, Y) = X^2Y + XY + Y^2$ peut être vu comme un élément de $\mathbb{Z}[X, Y]$.

Proposition 4.1.2 (division euclidienne) *Soit P non nul dans $A[X]$ de **coefficient dominant inversible**. Alors pour tout $F \in A[X]$, il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et $d(R) < d(Q)$.*

Preuve. On peut supposer que P est unitaire (i.e son coefficient dominant vaut 1). Posons $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Notons (P) l'idéal engendré par P (c'est-à-dire, l'ensemble des multiples

de P). Soit $B := A/(P)$ et x l'image de X par la projection canonique. Il suffit de montrer que tout élément de B est combinaison linéaire à coefficients dans A de $1, x, \ldots, x^{n-1}$. En fait, il suffit même de le faire pour tous les monômes $x^i, i \geq 0$. Cela découle immédiatement par récurrence de la relation $x^n = -(a_{n-1}x^{n-1} + \cdots + a_0)$ vraie dans B.
On peut aussi éviter le passage au quotient en raisonnant par récurrence à l'aide de l'algorithme de la division euclidienne des polynômes.
□

Puisque tous les éléments non nuls d'un corps sont inversibles, on obtient le corollaire fondamental suivant.

Corollaire 4.1.3 *Si K est un corps, alors $K[X]$ est* euclidien *relativement au degré des polynômes c'est-à-dire qu'étant donnés deux polynômes F et Q, il existe un unique polynôme R tel que $F = PQ + R$ et $d(R) < d(Q)$.*

Corollaire 4.1.4 *Si K est un corps, et I un idéal de de $K[X]$ il existe un polynôme P tel que $I = (P) = PK[X]$, c'est-à-dire que I contient exatement les multiples de P. Autrement $K[X]$ est un anneau principal.*

Preuve. On procède comme pour les idéaux de $\mathbb{Z}$. Si $I = \{0\}$, $P = 0$ convient. Si $I \neq \{0\}$, soit P unitaire de degré minimal positif dans I. Pour tout $U \in I$, on effectue la division euclidienne de P par U ce qui donne $U = PQ + R$ avec $d(R) < d(U)$. Mais $R = U - PQ$ donc $R \in I$. Comme $d(R) < d(P)$, on a $R = 0$ et donc $U = PQ \in (P)$. Cela montre que $I \subset (P)$. Comme $P \in I$, on a aussi $(P) \subset I$ et finalement $I = (P)$.

Remarque 4.1.5 *Attention, si A n'est pas un corps, l'anneau $A[X]$ n'est pas principal. Par exemple l'idéal I engendré dans $\mathbb{Z}[X]$ par 2 et X contient exactement les polynômes de la forme*

$$2a_0 + a_1X + \cdots + a_nX^n$$

avec $n > 1$ et $a_0, \ldots, a_n$ dans $\mathbb{Z}$. Ce n'est pas un idéal premier car si $I = (P)$ on aurait $P/2$ et $P \mid X$. Donc $P = \pm 1$ et $I = \mathbb{Z}[X]$ ce qui est faux (par exemple $1 + X \notin I$).

exercice 8 *Montrer que $A[X]$ est principal si et seulement si A est un corps.*

exercice 9 *Que vaut* $\mathrm{frac}(K[X])$ *le corps des fractions de $K[X]$?*

4.2 Irréductibilité

Soit A un anneau intègre.

Définition 4.2.1 *Un polynôme $P \in A[X]$ est dit irréductible lorsque pour tout polynômes Q_1 et Q_2, l'égalité $P = Q_1Q_2$ entraîne que Q_1 ou Q_2 est inversible, autrement dit Q_1 ou Q_2 est dans $U(A)$.*

Proposition 4.2.2 *Soit K un corps et $P \in K[X]$. Alors $K[X]/(P)$ est un corps si et seulement si P est irréductible.*

Preuve. D'après le Théorème 2.3.1, il suffit de démontrer que l'idéal (P) est maximal ssi P est irréducible. Supposons P irréducible et I idéal de $K[X]$ contenant(P). D'après le corollaire précédent, on peut supposer $I = (Q)$ avec $Q \in K[X]$. On a donc $(P) \subset (Q)$ et $Q \mid P$. Puisque P est irréducible on a donc $P = cQ$ avec $c \in K$ et alors $I = (P)$ ou bien $Q = c \in K$ et alors $I = K[X]$. L'idéal (P) est bien maximal. Réciproquement si (P) est maximal et $Q \in K[X]$ divise P, nous avons $(P) \subset (Q)$. Cela implique que $(P) = (Q)$ et alors $P = cQ$ avec $c \in K[X]$ ou bien $(Q) = K[X]$ et alors $Q = c \in K[X]$. Donc P est irréductible. □

Corollaire 4.2.3 (Lemme d'Euclide pour les polynômes) *Soit P un polynôme irréducibles de $K[X]$ divisant le produit Q_1Q_2 de deux polynômes de $K[X]$. Alors P divise Q_1 ou Q_2.*

Preuve. Dans le corps $K[X]/(P)$ on a $\overline{Q_1Q_2} = \overline{Q_1Q_2} = \overline{0}$. Donc, comme $K[X]/(P)$ est intègre, $\overline{Q_1} = \overline{0}$ ou $\overline{Q_2} = \overline{0}$, autrement dit P divise Q_1 ou Q_2.□

Il peut être difficile de prouver qu'un polynôme de $A[X]$ est irréductible. Rappelons quelques faits élémentaires mais très utiles dont la justification est laissée en exercice.

1. Les polynômes $X - a$ avec $a \in A$ sont irréductibles dans $A[X]$.
2. Si $P(X) \in A[X]$ et $a \in A$ sont tels que $P(a) = 0$ (on dit que a est racine de P), alors $X - a$ divise P dans $A[X]$ (cela découle de la division euclidienne de P par $X - a$ dont le reste est une constante).
3. Un polynôme qui n'a pas de racine peut ne pas être irréductible. Par exemple $P(X) = (X^2 + 1)^2$ n'a pas de racine dans $\mathbb{Z}[X]$ mais n'est pas irréductible.
4. Un polynôme de degré 3 qui n'est pas irréductible dans $K[X]$ où K est un corps possède nécessairement une racine.
5. Un polynôme de degré n admet au plus n racines (ce qui n'est plus vrai si A n'est pas intègre).

On dit que deux polynômes irréductibles P et Q de $A[X]$ sont associés[1] si il existe $a \in U(A)$ tel que $P = aQ$. Cela définit une relation d'équivalence sur les polynômes irréductibles. Lorsque $A = K$ est un corps, chaque classe contient un unique polynôme unitaire. Nous noterons

$$\mathcal{P} = \{P \in K[X] \text{ irréductibles et unitaires}\}.$$

exercice 10 *En s'inspirant de la preuve de la Proposition 3.2.2, démontrer que les polynômes apparaissant dans $\mathcal{P}$ sont en nombre infini.*

Théorème 4.2.4 (Factorisation) *Soit K un corps et P un polynôme de $K[X]$. Alors il existe $c \in K$ et une suite $(P_i, \alpha_i)_{1 \leq i \leq r}$ d'éléments de $\mathcal{P} \times \mathbb{N}^*$ tout deux uniques tels que*

$$P = cP_1^{\alpha_1} \cdots P_r^{\alpha_r}.$$

Preuve. La preuve découle du Lemme d'Euclide pour les polynômes de façon totalement analogue à celle du Théorème 3.2.5. □

[1] De façon générale, deux éléments a et a' d'un anneau commutatif A sont associés si il existe un inversible u tel que $a' = ua$. La relation $\sim$ définie par $a \sim a'$ ssi a et a' sont associés est une relation d'équivalence.

Remarque 4.2.5 *Les résultats dans $K[X]$ sont très similaires à ceux obtenus dans $\mathbb{Z}$. C'est du au fait que ces deux anneaux sont Euclidiens. En fait, on peut démontrer des résultats analogues dans n'importe quel anneau principal. Les preuves sont essentiellements les mêmes. Le théorème fondamental de décomposition découle du lemme d'Euclide qui lui même provient du fait que dans un anneau principal pour n'importe quel idéal $I = (P)$, il y équivalence entre I est maximal et P est irréductible.*

exercice 11 *Définir les notions de PPCM et PGCD de deux polynomes de $K[X]$ à partir du théorème précédent. Puis montrer que pour A et B dans $K[X]$ on a encore*

$$(A) + (B) = (\text{pgcd}(A, B)) \text{ et } (A) \cap (B) = (\text{ppcm}(A, B)).$$

Comment peut-on adapter l'algorithme d'Euclide au calcul de $\text{pgcd}(A, B)$ *?*

4.3 Groupe des inversibles d'un corps commutatif fini

Soit K un corps commutatf fini. Son groupe des inversibles $U(K)$ est alors un groupe multiplicatif abélien fini. Nous allons démontrer qu'il s'agit nécessairement d'un groupe cyclique. Rappelons tout d'abord le Lemme suivant.

Lemme 4.3.1 *Soit G un groupe abélien fini et $x_1, x_2, \ldots, x_k$ des éléments de G d'ordres repectifs $m_1, \ldots, m_k$ premiers entre eux deux à deux. Alors leur produit $x = x_1 \cdots x_k$ a pour ordre $m = m_1 \cdots m_k$.*

Preuve. Nous allons procéder par récurrence sur k. Le lemme est clair pour $k = 1$. Supposons le lemme vrai pour $k-1$. Notons m' l'ordre de x. Nous avons $x^m = x_1^m \cdots x_k^m = 1$ puisque G est abélien et m est multiple de tous les m_i. Donc $m' \mid m$. De même $x_1^{m'} \cdots x_k^{m'} = 1$ et $x_k^{m'} = (x_1 \cdots x_{k-1})^{-m'}$. Donc $x_k^{m'}$ est dans le groupe engendé par $x_1 \cdots x_{k-1}$. Mais par notre hypothèse de récurrence, $x_1 \cdots x_{k-1}$ est d'ordre $m_1 \cdots m_{k-1}$. Puisque x_k est d'ordre m_k, on en déduit que l'ordre de $x_k^{m'}$ divise en même temps m_k et $m_1 \cdots m_{k-1}$. Il est donc égal à 1, autrement dit $x_k^{m'} = 1$ et m' est un multiple de m_k. On a aussi $(x_1 \cdots x_{k-1})^{-m'} = 1$ ce qui implique que m' est un multiple de $m_1, \ldots, m_{k-1}$. Finalement $m \mid m'$ et puisque $m' \mid m$, on a bien $m = m'$.□

exercice 12 *Justifier que le lemme devient faux si les ordre considérés ne sont plus premiers entre eux.*

Théorème 4.3.2 *Soit K un corps fini commutatif d'ordre k. Alors le groupe $U(K)$ est cyclique d'ordre $k - 1$.*

Preuve. Remarquons tout d'abord que si $x \in U(K)$ est d'ordre $n = p^\alpha m$ avec p ne divisant pas m, alors x^m est d'odre p^α. En effet $(x^m)^{p^\alpha} = x^{mp^\alpha} = 1$ et si $(x^m)^k = 1$, on a $p^\alpha m \mid mk$. Donc $p^\alpha \mid k$ et mk est un multiple de n. Puisque K est fini, l'ensemble $E = \{p_1, \ldots, p_r\}$ des entiers premiers qui apparaissent dans la décomposition des ordres des éléments de $U(K)$ est fini. Notons α_i la plus grande valuation possible en p_i des ordres des éléments de $U(K)$. D'après la remarque qui précède, $U(K)$ possède au moins un élément x_i d'ordre $p_i^{\alpha_i}$ pour tout $i = 1, \ldots, r$. Alors, le lemme précédent assure que $g = x_1 \cdots x_r$ est d'ordre $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Il s'esnsuit que $U(K)$ contient le groupe cyclique $\langle g \rangle$ engendré par g qui possède a éléments. En particulier, $\text{card}(U(G)) \geq a$. Par

définition de a, nous avons $x^a = 1$ pour tout $x \in U(K)$. Donc tous les éléments de $U(K)$ sont racines du polynôme $X^a - 1 \in K[X]$. Or ce polynôme n'a au plus que a racines distinctes ce qui impose que $\text{card}(U(K)) \leq a$. Finalement, on a $\text{card}(U(A)) = a$ et donc $U(K) = \langle g \rangle$ est cyclique.□

Corollaire 4.3.3 *Pour tout nombre premier p, le groupe $U(\mathbb{Z}/p\mathbb{Z})$ est cyclique d'ordre $p-1$. Une classe $\overline{x}$ d'ordre $p-1$ pour la multiplication s'appelle une racine primitive modulo p.*

exercice 13 *Déterminer les racines primitives modulo $2, 4, 5$ et 7.*

4.4 Polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème 4.4.1 (Dalembert-Gauss) *Un polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine. En particulier, les polynômes non constants irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1.*

Preuve. Il s'agit de montrer que tout polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ unitaire de degré n dans $\mathbb{C}$ a au moins une racine. Cela revient à montrer que l'équation $P(z) = 0$ possède toujours une solution complexe.
Considérons tout d'abord l'équation $x^n = a$ avec $n \geq 1$ un entier et $a \in \mathbb{C}$. Dans ce cas, on sait trouver les solutions. En particulier $z = \sqrt[n]{|a|}\exp(\frac{i\theta}{n})$ avec $\theta = \arg a$ est solution.
Soit maintenant la fonction $f : \mathbb{C} \to \mathbb{R}_{\geq 0}$ telle que $f(z) = |P(z)|$. Il s'agit d'une fonction continue non identiquement nulle puisque $P \neq 0$. L'ensemble $E := f(\mathbb{C})$ est non vide minoré par 0 donc admet une borne inférieure m. Par ailleurs l'inégalité triangulaire montre que

$$|P(z)| \geq |z^n| - \left|a_{n-1}z^{n-1} + \cdots + a_0\right| \geq |z|^n \left(1 - \frac{\left|a_{n-1}z^{n-1} + \cdots + a_0\right|}{|z|^n}\right).$$

On voit donc que $\lim_{|z|\to+\infty} f(z) = +\infty$. La fonction f étant continue, il existe un rayon $r > 0$ tel que $f(z) > m$ dès que z sort de $D(0, r)$ le disque fermé de centre 0 et de rayon r. Ce dernier étant compact, f atteint son minimum m en une valeur z_0, i.e. $f(z_0) = m$. Quitte à remplacer $P(X)$ par $P(X + z_0)$ ce qui ne change rien aux valeurs prises par f, on peut supposer que $z_0 = 0$.
On peut alors écrire $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_kX^k + a_0$ avec $k > 0$ minimal tel que $a_k \neq 0$. On a alors $m = a_0$. Soit c tel que $c^k = -m\overline{a_k}$. Un tel complexe existe puisque les équations de la forme $z^n = a$ ont toujours au moins une solution.
Supposons $m \neq 0$. On définit maintenant la fonction g sur l'intervalle $[0, 1]$ par $g(t) = f(tc)$. Cela donne

$$g(t) = \left|m - m \times |a_k|^2 t^k + c_{k+1}t^{k+1} + \cdots + c_nt^n\right| \text{ où } c_r = a_rc^r, r = k+1, \ldots, n.$$

On a donc en utilisant l'inégalité triangulaire et pour tout $t \in [0, 1]$

$$g(t) \leq m(1 - |a_k|^2 t^k) + t^{k+1}(\left|c_{k+1} + \cdots + c_nt^{n-k-1}\right| \leq$$
$$m(1 - |a_k|^2 t^k) + t^{k+1}M \leq m - m|a_k|^2 t^k \left(1 - \frac{tM}{m|a_k|^2}\right).$$

où $M = |c_{k+1}| + \cdots + |c_n| > 0$. Pour $0 < t \leq \min(1, \frac{m|a_k|^2}{M})$, on voit que $g(t) < m$ ce qui fournit une contradiction. Cela signifie que notre supposition $m \neq 0$ est fausse. Donc $m = 0$ et P admet bien une racine dans $\mathbb{C}$.□

Corollaire 4.4.2 *Les polynômes non constants irréductibles de* $\mathbb{R}[X]$ *sont ceux de degré* 1 *et ceux de degré* 2 *dont le discriminant* Δ *est strictement négatif.*

Exemple. Le polynôme $P(X) = X^4 + 1$ est irréducible dans $\mathbb{Q}[X]$ mais se factorise sous la forme

$$P(X) = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$$

dans $\mathbb{R}[X]$ et sous la forme

$$P(X) = (X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}})$$

dans $\mathbb{C}[X]$.

exercice 14 *Soient* A *et* B *deux polynomes de* $\mathbb{Q}[X]$. *Montrer que* $\text{pgcd}(A, B)$ *est le même si on les considère dans* $\mathbb{Q}[X]$, $\mathbb{R}[X]$ *ou* $\mathbb{C}[X]$.

4.5 Formule de Taylor

Soit K un corps. Dans ce cas, $K[X]$ est un K-espace vectoriel de base $\{X^n \mid n \geq 0\}$. La dérivation Δ dans $K[X]$ est l'application linéaire qui envoie 1 sur 0 et pour $n > 0$, X^n sur nX^{n-1}. On note $\Delta(P) = P'$ le polynôme dérivé de P. Elle vérifie

$$(PQ)' = P'Q + PQ'.$$

Par ailleurs $\ker \Delta = K$ et $\text{Im}\, \Delta = K[X]$. En effet si $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$, on a

$$\Delta^{-1}(\{P\}) = \{\frac{a_n}{n+1}X^{n+1} + \frac{a_{n-1}}{n}X^n + \cdots + a_0 X + c \mid c \in K\}.$$

Pour le voir, il suffit de remarquer que $P - \frac{a_n}{n+1}X^{n+1} + \frac{a_{n-1}}{n}X^n + \cdots + a_0 X \in \ker \Delta$. Pour tout a et $c \in A$, il existe donc un unique polynôme Q dans $\Delta^{-1}(\{P\})$ tel que $Q(a) = c$

Proposition 4.5.1 (Formule de Taylor pour les polynômes) *Soit* K *un corps et* $P \in K[X]$ *de degré* n. *Alors pour tout* $a \in K$, *on a*

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

Preuve. On raisonne par récurrence sur n. Si $n = 0$, $P(X) = P(a)$ et la formule est vraie. Supposons la formule vraie pour tout polynôme de degré $k < n$. Soit P de degré n. On a en appliquant l'hypothèse de récurrence avec $P'(X)$

$$P'(X) = \sum_{k=1}^{n} \frac{P^{(k)}(a)}{(k-1)!}(X - a)^{k-1}.$$

Donc d'après ce qui précède

$$P(X) = \sum_{k=1}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k + P(a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

□

Corollaire 4.5.2 *Un polynôme* $P \in \mathbb{C}[X]$ *a toutes ces racines simples ssi* P *et son polynôme dérivé* P' *sont premiers en eux.*

4.6 Théorème chinois

Théorème 4.6.1 *Soit K un corps, $A_1, A_2, \ldots, A_n$ des polynômes de $K[X]$ et $M_1, \ldots, M_n$, des polynômes premiers entre eux deux à deux. Alors il existe un unique polynôme $P \in K[X]$ vérifiant*

$$\begin{cases} P - A_1 & \in M_1 K[X] \\ P - A_2 & \in M_2 K[X] \\ \vdots & \vdots \\ P - A_n & \in M_n K[X] \end{cases} \qquad d(P) < d(M) \text{ où } M = M_1 \ldots M_n$$

Preuve. C'est la même que pour le Théorème chinois dans $\mathbb{Z}$. Une solution est donnée par :

$$P = A_1 K_1 L_1 + \cdots + A_n L_n K_n$$

où $L_i = M/M_i$ et les polynômes K_i sont donnéss par Bézout en exprimant que les polynômes L_i et M_i sont premiers entre eux :

$$\exists (H_i, K_i) \quad H_i M_i + K_i L_i = 1$$

Puis on fait la division euclidienne de P par M. Il existe donc $Q, R \in K[X]$ avec $d(R) < d(M)$ et $P = MQ + R$ donc $R \equiv P$ modulo M donc R satisfait le système S lui aussi. L'unicité provient du fait que comme les M_i sont premiers entre eux deux à deux, $R \equiv 0[M_i]$ pour tout i entraine que $R \equiv 0[M]$.□

Corollaire 4.6.2

$$K[X]/(M) \simeq K[X]/(M_1) \times \cdots \times K[X]/(M_n)$$

Chapitre 5

Polynômes dans $\mathbb{Z}[X]$

Nous avons vu que tout polynôme à coefficients dans un corps K admettait une factorisation en irréductibles, unique une fois choisi un système de représentants des irréductibles. Cela découle du fait que $K[X]$ est un anneau euclidien. Mais que se passe-t-il pour $\mathbb{Z}[X]$ qui n'est pas un anneau euclidien (puisque ce n'est pas un anneau principal d'après la Remarque 4.1.5) ?

5.1 Polynômes irréductibles et factorisation dans $\mathbb{Z}[X]$

Une première remarque est qu'un polynôme de $\mathbb{Z}[X]$ peut être irréductible dans $\mathbb{Q}[X]$ sans l'être dans $\mathbb{Z}[X]$. Par exemple $P(X) = 2X^2 + 4 = 2(X^2 + 2)$ se factorise de façon non triviale dans $\mathbb{Z}[X]$ puisque 2 n'est pas inversible dans $\mathbb{Z}$ mais ne se factorise pas dans $\mathbb{Q}[X]$ (voir Définition 4.2.1). Cela conduit à la définition suivante. Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. On note $c(P)$ le *contenu* de P défini par $c(P) := \text{pgcd}(a_n, \ldots, a_0) \in \mathbb{N}$. On dit que P est *primitif* lorsque $c(P) = 1$.

Lemme 5.1.1 (dit lemme de Gauss) *Soit P, Q dans $\mathbb{Z}[X]$. Alors $c(PQ) = c(P)C(Q)$.*

Preuve. Supposons tout d'abord $c(P) = c(Q) = 1$. Posons $P(X) = a_nX^n + \cdots + a_0$, $Q(X) = b_mX^m + \cdots + b_0$ et $PQ(X) = v_{n+m}X^{n+m} + \cdots + v_0$. Supposons tout d'abord que $c(PQ) \neq 1$. Alors, il existe p premier tels que $p \mid c(PQ)$. Puisque $c(P) = c(Q) = 1$ il existe i_0 tel que $p \mid a_i$ pour $i < i_0, p \not| a_{i_0}$ et j_0 tel que $p \mid b_j$ pour $j < j_0, p \not| b_{j_0}$. Alors

$$p \mid c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_ib_j = a_{i_0}b_{j_0} + \sum_{i+j=i_0+j_0,(i,j)\neq(i_0,j_0)} a_ib_j.$$

Dans la dernière somme on a $i < i_0$ ou $j < j_0$ ce qui implique que p divise cette somme. Il s'ensuit que p divise $a_{i_0}b_{j_0}$ et donc, d'après le lemme d'Euclide, $p \mid a_{i_0}$ ou $p \mid b_{i_0}$. Ce qui mène à une contradiction.
Dans le cas général, on pose $d = c(P)$, $e = c(Q)$, $P' = P \mid d$ et $Q' = Q \mid e$. Ainsi $c(P') = c(Q') = 1$ donc d'après ce qui précède $c(P'Q') = 1$. Or $PQ = deP'Q'$. Donc $c(PQ) = dec(P'Q') = de$ comme souhaité. □

Proposition 5.1.2 *Les polynômes irréductibles dans $\mathbb{Z}[X]$ sont les nombres premiers $p \in \mathbb{Z}$ et les polynômes $P \in \mathbb{Z}[X]$ primitifs de degré au moins 1 et irréductibles dans $\mathbb{Q}[X]$.*

Preuve. Montrons que les éléments proposés sont effectivement irréductibles. Si p est premier dans $\mathbb{Z}$ et $p = P(X)Q(X)$ dans $\mathbb{Z}[X]$, on doit avoir $d(P) = d(Q) = 0$ car $\mathbb{Z}$ est intègre. Donc p reste irréductible dans $\mathbb{Z}[X]$. Si $P \in \mathbb{Z}[X]$ est irréductible non constant dans $\mathbb{Q}[X]$ et vérifie $P = QR$ dans $\mathbb{Z}[X]$, Q ou R est dans $\mathbb{Q} \setminus \{0\}$. Supposons qu'il s'agisse de R. Comme R est dans $\mathbb{Z}[X]$, on doit avoir $R \in \mathbb{Z}$. Mais alors $c(P) = c(Q)C(R) = 1$ donc $c(R) = R = \pm 1$ et P est bien irréductible. Montrons qu'il s'agit des seuls irréductibles. Si P est irréductible de degré 0, il s'agit nécessairement d'un irréductible de $\mathbb{Z}$. Si P est irréductible de degré au moins 1, on doit avoir $c(P) = 1$. Supposons que l'on ait $P(X) = Q(X)R(X)$ dans $\mathbb{Q}[X]$. On peut écrire $Q(X) = \frac{a}{b}Q'(X)$ et $R(X) = \frac{c}{d}R'(X)$ où Q', R' sont dans $\mathbb{Z}[X]$ et de contenu égal à 1 et a, b, c, d sont dans $\mathbb{Z}$ avec $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. On en déduit que $bdP(X) = abQ'(X)R'(X)$. En passant aux contenus, on obtient puisque $\mathbb{Z}$ est intègre $bd = \pm ac$. Donc $P(X) = \pm Q'(X)R'(X)$ avec P' et Q' dans $\mathbb{Q}[X]$. Or, P étant irréductible dans $\mathbb{Z}[X]$ Q' ou R' vaut ± 1. Les polynômes irréductibles de $\mathbb{Z}[X]$ doivent donc nécessairement le rester dans $\mathbb{Q}[X]$ ce qui termine la preuve.□

Théorème 5.1.3 *L'anneau $Z[X]$ est factoriel. C'est à dire que tout polynôme dans $\mathbb{Z}[X]$ se décompose en produit d'irréductibles et la décomposition est unique modulo le changement de signe de ses facteurs*[1]*.*

Preuve. On commence par montrer l'existence d'une décomposition dans $\mathbb{Z}[X]$. Considérons $P \in \mathbb{Z}[X]$ primitif. Dans $\mathbb{Q}[X]$, on peut écrire $P(X) = P_1(X)^{r_1} \cdots P_k(X)^{r_k}$ où les P_i sont irréductibles dans $\mathbb{Q}[X]$. Posons comme dans la preuve précédente $P_i(X) = \frac{a_i}{b_i}P_i'(X)$ avec $P'(X) \in \mathbb{Z}[X]$ de contenu égal à 1. D'après la proposition précédente, chaque P_i' est irréductible dans $\mathbb{Z}[X]$. On obtient $\prod b_i P(X) = \prod a_i \prod P_i'(X)^{r_i}$. En passant aux contenus, cela implique que $P(X) = \pm \prod P_i(X)^{r_i}$ c'est à dire l'existence d'une décomposition en irréductibles dans $\mathbb{Z}[X]$ pour P. Si P n'est pas primitif, on écrit $P = c(P)P'$ et on décompose P' en irréductibles dans $\mathbb{Z}[X]$ puis $c(P)$ en nombres premiers dans $\mathbb{Z}$. L'unicité de la décomposition dans $A[X]$ découle immédiatement de l'unicité de la décomposition dans $\mathbb{K}[X]$ et du fait que $\mathbb{Z}$ est lui même factoriel. □

Une première méthode pour étudier l'irréductibilité d'un polynôme dans $\mathbb{Z}[X]$ consiste à étudier celle de son image dans $\mathbb{Z}/p\mathbb{Z}[X]$ où p est un entier premier. En effet sous cette hypothèse, on sait que $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre. Si $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$, on note $\overline{P}(X) = \overline{a}_n X^n + \cdots + \overline{a}_0$ son image dans $\mathbb{Z}/p\mathbb{Z}[X]$. Le preuve de la proposition suivante est laissée en exercice.

Proposition 5.1.4 *Soit $P \in \mathbb{Z}[X]$ de degré n et $\overline{P}$ son image dans $\mathbb{Z}/p\mathbb{Z}[X]$. On suppose de plus que $d(\overline{P}) = n$. Si $\overline{P}$ est irréducitble dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

On prendra garde que l'irréductibilité de P obtenue est sur $\mathbb{Q}$ et pas sur $\mathbb{Z}$ en général. Par exemple $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$ mais l'est dans $\mathbb{Z}/3\mathbb{Z}[X]$ puisque $\mathbb{Z}/3\mathbb{Z}$ est un corps.

Exemple 8 *Le polynôme $P(X) = X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$. En effet, modulo 2, on a $P(X) = X^3 + X + 1$ qui est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$ puisque de degré 3 sans racine. Il est de plus primitif.*

Voici un autre critère permettant de démontrer l'irréductibilité d'un polynôme de $\mathbb{Z}[X]$.

[1] Un anneau A est dit factoriel lorsque tout élément de A se décompose en produit d'irréductibles et que la décomposition est unique à multiplication de ses facteurs par les inversibles de A près.

Proposition 5.1.5 (critère d'Eisenstein) *On considère un polynôme $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ et $p \in \mathbb{Z}$ un nombre premier tel que $p \nmid a_n$, $p \mid a_i$ pour $i = 0, \ldots, n-1$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Q}[X]$ (donc aussi dans $\mathbb{Z}[X]$ si $c(P) = 1$).*

Preuve. Si P n'est pas irréductible dans $\mathbb{Q}[X]$, on peut écrire $P(X) = Q(X)R(X)$ avec P, Q dans $\mathbb{Z}[X]$ non constants. On a donc $Q(X) = b_qX^q + \cdots + b_0$ et $R(X) = c_rX^r + \cdots + c_0$ avec $0 < q, r < n$. Dans $\mathbb{Z}/p\mathbb{Z}[X]$ on a donc

$$\overline{P}(X) = \overline{a}_nX^n = (\overline{b}_qX^q + \cdots + \overline{b}_0)(\overline{c}_rX^r + \cdots + \overline{c}_0).$$

Mais $\mathbb{Z}/p\mathbb{Z}[X]$ est euclidien, donc factoriel. L'unicité de la décomposition et les inégalités $0 < q, r < n$ montrent que X divise à la fois $\overline{Q}$ et $\overline{R}$. Donc $\overline{b}_0 = \overline{c}_0 = 0$. Mais alors p^2 divise $a_0 = b_0c_0$ contrairement à l'hypothèse.□

Exemple 9

1. *Soit p un nombre premier. Alors $P(X) = X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}[X]$. Il suffit de poser $X = Y + 1$ et d'appliquer le critère précédent avec p.*
2. *Soit $a \in \mathbb{Z}$ tel que $v_p(a) = 1$ pour au moins un nombre premier p. Alors $X^n - a$ est irréductible dans $\mathbb{Z}[X]$.*

5.2 Polynômes cyclotomiques

Rappelons que les racines dans $\mathbb{C}$ du polynôme $X^n - 1$ sont les éléments du groupe cyclique $C_n = \{1, \zeta, \zeta^2, \ldots \zeta^{n-1}\} =< \zeta >$ où $\zeta = exp(\frac{2i\pi}{n})$. On sait que

$$f : \begin{cases} (C_n, \times) \to (\mathbb{Z}/n\mathbb{Z}, +) \\ \xi^k \mapsto \overline{k} \end{cases}$$

est un isomorphime de groupes cycliques. D'après la Proposition 3.4.1 on sait donc que les générateurs de C_n sont les ζ^k avec $(k, n) = 1$ et qu'il y en a $\varphi(n)$. Ces générateurs sont appelées *racines primitives n-ièmes de l'unité*. Posons

$$\Delta_n = \{\zeta^k, 0 \leq k \leq n-1, (k, n) = 1\}.$$

Observons que pour tout diviseur d de n, C_d est un sous-groupe de C_n. En effet si $z^d = 1$ avec $z \in \mathbb{C}$, alors $z^n = (z^d)^{\frac{n}{d}} = 1$. On a donc $\Delta_d \subset C_d \subset C_n$ pour tout diviseur d de n. Par ailleurs si d et d' divisent n, $\Delta_d \cap \Delta_{d'} = \emptyset$. Finalement si $z^n = 1$, il existe un unique diviseur d de n tel que $z \in \Delta_d$, c'est l'ordre de z dans le groupe C_n. Tout cela montre que

$$C_n = \bigsqcup_{d|n} \Delta_d \tag{5.1}$$

où la réunion est disjointe. En particulier, nous avons

$$n = \sum_{d|n} \varphi(d).$$

Définition 5.2.1 *Le polynôme unitaire* $\Phi_n(X) = \prod_{\omega \in \Delta_n} (X - \omega)$ *est appelé polynôme cyclotomique d'indice* n. *Son degré vaut* $\varphi(n)$. *En particulier, si* p *est un nombre premier, ona*

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1.$$

exercice 15 *Donner les polynômes cyclotomiques* $\Phi_1, \Phi_2, \Phi_3, \Phi_4$.

Théorème 5.2.2

1. *On a la factorisation*
$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$
2. *Pour tout entier* $n \in \mathbb{N}^*$, Φ_n *est un polynôme unitaire de* $\mathbb{Z}[X]$.
3. *Pour tout* $n \geq 2$ *nous avons* $\Phi_n(0) = 1$ *et* $X^{\varphi(n)}\Phi_n(\frac{1}{X}) = \Phi_n(X)$.

Preuve. L'assertion 1 découle de la décomposition (5.1). Elle permet le calcul par récurrence des polynômes Φ_n. En effet, on a

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d(X)}. \tag{5.2}$$

Il est clair que $\Phi_1(X) = X - 1$ et $\Phi_2(X) = X + 1$ sont unitaires dans $\mathbb{Z}[X]$. Supposons par récurrence que $\Phi_k(X)$ $n > k \geq 2$ soit unitaire dans $\mathbb{Z}[X]$ et $\Phi_k(0) = 1$. Alors, $\prod_{d|n, d<n} \Phi_d(X)$ est unitaire. La division euclidienne de $X^n - 1$ par $\prod_{d|n, d<n} \Phi_d(X)$ assure que $\Phi_n(X)$ est unitaire dans $\mathbb{Z}[X]$. D'après (5.2) on a de plus et $\Phi_n(0) = 1$ puisque $\Phi_1(0) = -1$. Par ailleurs,

$$X^{\varphi(n)}\Phi_n(\frac{1}{X}) = \prod_{\omega \in \Delta_n} (1 - \omega X) = -(1)^{\varphi(n)} \prod_{\omega \in \Delta_n} \omega \prod_{\omega \in \Delta_n} (X - \omega^{-1}).$$

Mais $\Phi_n(0) = -(1)^{\varphi(n)} \prod_{\omega \in \Delta_n} \omega = 1$ et $\prod_{\omega \in \Delta_n} (X - \omega^{-1}) = \prod_{\omega \in \Delta_n} (X - \omega)$ puisque Δ_n est stable par passage à l'inverse. □

Théorème 5.2.3 *Les polynômes cyclotomiques* Φ_n *sont irréductibles sur* $\mathbb{Z}$ *(donc aussi sur* $\mathbb{Q}$*).*

Preuve. Admis provisoirement (cf cours d'algèbre du second semestre) □.

Chapitre 6

Résolutions d'équations dans $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

6.1 Equations diophantiennes du premier ordre

Du nom de Diophante (né entre 200 et 214 et mort vers 284/298 av JC). Résoudre une équation Diophantienne consiste à chercher des solutions entières (ou rationnelles) à des équations polynomiales à coefficients entiers ou rationnels. On va se concentrer pour le moment sur les équations du 1er ordre.

Théorème 6.1.1 *L'équation Diophantienne du* 1*er ordre*

$$bx - ay = c, \ \text{où } a, b, c \in \mathbb{Z} \tag{6.1}$$

admet des solutions si et seulement si d, le PGCD de a et b, divise c.

Dans ce cas, l'ensemble des solutions de (6.1) est donné par :

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + k \begin{pmatrix} \frac{a}{d} \\ \frac{b}{d} \end{pmatrix}, \quad k \in \mathbb{Z}$$

Preuve : La condition d divise c est nécessaire car $c = bx - ay$ signifie que $c \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Elle est suffisante car si d divise c il existe un entier m tel que $c = dm$ donc $c \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ donc il, existe x_0 et y_0 tels que $c = ay_0 + bx_0$.
Pour trouver un tel couple, on peut toujours

1. Trouver (u, v), par l'algorithme d'Euclide, tels que $bu - av = d$.
2. Poser $x_0 = um$ et $y_0 = vm$.

Reste à trouver toutes les solutions : soit (x_0, y_0) comme ci-dessus et (x, y) un autre couple solution. On a donc

$$b(x - x_0) = a(y - y_0)$$

On divise par le pgcd d et si on note a' et b' tels que $a = da'$ et $b = b'd$, on obtient

$$b'(x - x_0) = a'(y - y_0).$$

Mais maintenant a' et b' sont premiers entre eux car un facteur commun q aux deux nombres diviserait a et b et dq diviserait a et b donc diviserait d. Ce qui contredirait la définition de d. Donc le Lemme de Gauss dit que a' divise $(x - x_0)$ tandis que b' divise $(y - y_0)$. Donc si $k \in \mathbb{Z}$ vérifie $x - x_0 = ka'$ l'équation donne que $y - y_0 = kb'$. □

6.2 Triplets pythagoriciens

Un triplet pythagoricien est une solution de l'équation diophantienne d'inconnues x, y, z

$$z^2 = x^2 + y^2.$$

On dit que le triplet est primitif lorsque $\text{pgcd}(x, y, z) = 1$. Il est clair qu'il suffit de déterminer les triplets primitifs, les autres étant obtenus par multiplication par un facteur commun.

Théorème 6.2.1 *Les triplets Pythagoriciens primitifs (x, y, z) sont tels que x et y ont une parité opposée. De plus, si on suppose x impair, ils sont de la forme*

$$(x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2)$$

où r, s sont des entiers premiers entre eux et de parité opposée.

Preuve. On vérifie sans peine que $(r^2 - s^2, 2rs, r^2 + s^2)$ est un triplet pythagoricien. Comme r et s sont de parité opposée, r^2 et s^2 aussi. Donc $r^2 - s^2$ et $r^2 + s^2$ sont impairs. Si p premier divise $r^2 - s^2, 2rs$ et $r^2 + s^2$, nous avons $p > 2$. Mais alors $p \mid r$ et $p \mid s$ et on a une contradiction. Donc, $(r^2 - s^2, 2rs, r^2 + s^2)$ est primitif.
Réciproquement, donnons nous (x, y, z) un triplet primitif. Notons tout d'abord que l'on peut supposer x, y et z dans $\mathbb{N}$ qui à changer les signes. Nous avons alors $x \leq z$. Observons maintenant que x et y sont de parité opposée. En effet si x et y étaient pairs, il en serait de même pour z et (x, y, z) ne serait plus primitif. Maintenant si x et y étaient impairs, on aurait $x \equiv \pm 1 \bmod 4$ et $y \equiv \pm 1 \bmod 4$. Mais alors $x^2 \equiv y^2 \equiv 1 \bmod 4$ et $z^2 \equiv 2 \bmod 4$ ce qui est impossible car $\overline{0}$ et $\overline{1}$ sont les seuls carrés dans $\mathbb{Z}/4\mathbb{Z}$. On peut donc supposer que y est pair et x est impair. Dans ce cas z est également impair. On a alors

$$y^2 = (z - x)(z + x).$$

Soit $p > 2$ un nombre premier divisant $z - x$ et $z + x$. Alors $p \mid y^2$ et donc $p \mid y$. De plus $p \mid 2x$ et $p \mid 2z$ ce qui contredit le fait que (x, y, z) est primitif. Donc 2 est le seul diviseur premier commun à $z - x$ et $z + x$. Posons

$$y^2 = 4\frac{z - x}{2}\frac{z + x}{2}.$$

Alors comme $\frac{z-x}{2}$ et $\frac{z+x}{2}$ sont premiers entre-eux, ce sont des carrés. Posons

$$r = \sqrt{\frac{z + x}{2}} \text{ et } s = \sqrt{\frac{z - x}{2}}.$$

Alors r et s sont premiers entre eux puisque c'est le cas pour r^2 et s^2. Finalement r et s sont de parité opposée car, dans le cas contraire, r^2 et s^2 auraient la même parité et $z = r^2+s^2, x = r^2-s^2, y = 2rs$ seraient tous pairs ce qui contredirait le fait que (x, y, z) est primitif.□

6.3 Loi de réciprocité quadratique

Dans $\mathbb{Z}/p\mathbb{Z}$ et p premier impair, l'ensemble des solutions de l'équation du second degré

$$\overline{a}X^2 + \overline{b}X + \overline{c} = 0 \text{ avec } \overline{a} \neq \overline{0}$$

se décrit à l'aide du discriminant $\overline{\Delta} = \overline{b}^2 - 4\overline{ac}$. En effet on a encore

$$\overline{a}X^2 + \overline{b}X + \overline{c} = \overline{a}\left(X - \overline{b}(\overline{2}\overline{a})^{-1}\right)^2 + \overline{\Delta}(\overline{4}\overline{a}^2)^{-1}.$$

Donc

$$S = \begin{cases} \emptyset \text{ si } \overline{\Delta} \text{ n'est pas un carré dans } \mathbb{Z}/p\mathbb{Z}, \\ \{\overline{b}(\overline{2}\overline{a})^{-1}\} \text{ si } \overline{\Delta} = \overline{0}, \\ \{(-\overline{b} \pm \overline{\delta})(\overline{2}\overline{a})^{-1}\} \text{ si } \overline{\Delta} = \overline{\delta}^2 \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

Il est donc important de savoir si $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$ est un carré. Le problème étant trivial si $p = 2$, nous supposerons $p > 2$.

Définition 6.3.1 *Le symbole de Legendre est défini sur $\mathbb{Z}$ par*

$$\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } x \in p\mathbb{Z}, \\ 1 \text{ si } \overline{x} \text{ est un carré dans } U(\mathbb{Z}/p\mathbb{Z}), \\ -1 \text{ sinon.} \end{cases}$$

Proposition 6.3.2

1. *L'application $\rho : U(\mathbb{Z}/p\mathbb{Z}) \to \{\pm 1\}$ telle que $\rho(\overline{x}) = x^{\frac{p-1}{2}} \bmod p$ est bien définie et est un morphisme surjectif de groupes multiplicatifs.*
2. *On a $\rho(\overline{x}) = \left(\frac{x}{p}\right)$ pour tout $x \in \overline{x}$ et tout $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$. En particulier $\ker\rho$ est l'ensemble des carrés de $U(\mathbb{Z}/p\mathbb{Z})$.*
3. *Le symbole de Legendre est multiplicatif*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \ \forall x, y \in \mathbb{Z}.$$

4. *Si $x = x' \bmod p$, on a $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.*
5. *On a l'identité*

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0.$$

Preuve. 1 : L'application est bien définie car $\rho(\overline{x})$ ne dépend pas de $x \in \overline{x}$. Par ailleurs $\rho(\overline{x})^2 = x^{p-1} \bmod p = 1$ donc $\rho(\overline{x}) \in \{\pm 1\}$ d'après le petit théorème de Fermat. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$ d'après le Theorème 4.3.2, ρ est surjectif. En effet si $\overline{\alpha}$ est un générateur de $U(\mathbb{Z}/p\mathbb{Z})$ (racine primitive modulo p), $\rho(\overline{\alpha}) = -1$ (sinon $\overline{\alpha}$ serait d'ordre $\leq \frac{p-1}{2}$). L'application ρ est clairement un morphisme de groupes multiplicatifs. On a par ailleurs $U(\mathbb{Z}/p\mathbb{Z})/\ker\rho \simeq \{\pm 1\}$ donc $\ker\rho$ est d'indice 2 dans $U(\mathbb{Z}/p\mathbb{Z}) = \ker\rho \sqcup (\alpha \ker\rho)$.
2 : Si $\overline{x} = \overline{y}^2$ est un carré, on a $\rho(\overline{x}) = y^{p-1} \bmod p = 1$. Donc $\ker\rho$ contient l'ensemble des carrés de $U(\mathbb{Z}/p\mathbb{Z})$. Par ailleurs cet ensemble vaut $\{1, \overline{\alpha}^2, \overline{\alpha}^4, \ldots, \overline{\alpha}^{p-3}\}$ et possède donc $\frac{p-1}{2}$ éléments. Il s'ensuite que $\ker\rho$ est l'ensemble des carrés de $U(\mathbb{Z}/p\mathbb{Z})$. Par passage au complèmentaire, $\alpha\ker\rho$ est l'ensemble des éléments non carrés de $U(\mathbb{Z}/p\mathbb{Z})$.
3 : Découle de 1 et 2.
4 : Découle de 2.

5 : Nous avons

$$\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{\alpha x}{p}\right)$$

puisque la multiplication par $\overline{\alpha}$ est une bijection de $U(\mathbb{Z}/p\mathbb{Z})$ sur lui-même. D'après la point 3, on a donc

$$\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{\alpha x}{p}\right)=\left(\frac{\alpha}{p}\right)\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=-\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)$$

d'où le résultat. □

Soit θ une racine primitive modulo p (par exemple $\theta=\exp(\frac{2i\pi}{p})$. On définit la somme de Gauss τ par

$$\tau=\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\theta^x.$$

Proposition 6.3.3 *Nous avons* $\tau^2=p\left(\frac{-1}{p}\right)$.

Preuve. Par définition

$$\tau^2=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\theta^{x+y}=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)\theta^{x+y}$$

où la seconde égalité est une conséquence du point 3 de la proposition précédente. Cela donne

$$\tau^2=\sum_{u=0}^{p-1}\sum_{x+y=u \bmod p}\left(\frac{xy}{p}\right)\theta^u=\sum_{u=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x(u-x)}{p}\right)\theta^u=\sum_{u=0}^{p-1}S(u)\theta^u$$

car

$$\sum_{x+y=u \bmod p}\left(\frac{xy}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x(u-x)}{p}\right)$$

d'après le point 5 de la même proposition. Dans ce qui précède, on a posé, pour tout $u\in\{0,\dots,p-1\}$

$$S(u)=\sum_{x=0}^{p-1}\left(\frac{x(u-x)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x(u-x)}{p}\right).$$

On a $S(0)=\sum_{x=1}^{p-1}\left(\frac{-1}{p}\right)=(p-1)\left(\frac{-1}{p}\right)$. Pour $u\neq 0$, on note[1] x^{-1} l'unique entier de $\{1,\dots,p-1\}$ tel que $xx^{-1}=1 \bmod p$. On a alors

$$S(u)=\sum_{x=1}^{p-1}\left(\frac{-x^2(1-x^{-1}u)}{p}\right)$$

[1] Il s'agit d'une notation commode mais un peu trompeuse car x^{-1} n'est pas ici égal à l'inverse de x dans $\mathbb{Z}$ qui n'est pas un entier en général.

puisque pour tout $x = 1, \dots p-1$, $-x^2(1-x^{-1}u) = x(u-x) \bmod p$. Comme le symbole de Legendre est multiplicatif,

$$S(u) = \left(\frac{-1}{p}\right) \sum_{x=1}^{p-1} \left(\frac{1-x^{-1}u}{p}\right) = \left(\frac{-1}{p}\right) \sum_{z=0, z\neq 1}^{p-1} \left(\frac{z}{p}\right)$$

où la dernière égalité vient du fait que $\{(1-x^{-1}u) \bmod p \mid x = 1, \dots p-1\} = \{0, 2, \dots, p-1\}$ car $u \neq 0$ et $x^{-1} \neq 0$. Finalement

$$S(u) = -\left(\frac{-1}{p}\right)$$

en utilisant le point 4 de la proposition précédente. On a donc

$$\tau^2 = S(0) + \sum_{u=1}^{p-1} S(u)\theta^u = \left(\frac{-1}{p}\right)\left(p - 1 - \sum_{u=1}^{p-1} \theta^u\right) = \left(\frac{-1}{p}\right)p$$

puisque $1 + \sum_{u=1}^{p-1} \theta^u = 0$.□

Théorème 6.3.4 *Soient p et q deux nombres premiers impairs disctincts. On a*

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

Preuve. Notons $E = \mathbb{Z}[\theta]$ le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et θ. En utilisant le morphisme de Frobenius dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, nous avons

$$\tau^q = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)\theta^{qx} \bmod qE.$$

En utilisant que le symbole de Legendre est multiplicatif, cela donne

$$\tau^q = \left(\frac{q}{p}\right) \sum_{x=1}^{p-1} \left(\frac{qx}{p}\right)\theta^{qx} \bmod qE$$

de sorte que nous avons $\tau^q = \left(\frac{q}{p}\right)\tau \bmod qE$ puisque la multiplication par q donne une bijection de $\mathbb{F}_p^*$.

Considérons maintenant le nombre

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{q-1}{2}} = (\tau^2)^{\frac{q-1}{2}} = \tau^{q-1}.$$

En mulitipliant par τ^2, on trouve la congruence

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right)\tau^2 = \tau^{q+1} = \left(\frac{q}{p}\right)\tau^2 \bmod qE.$$

D'après la proposition précédente, nous savons que $\tau^2 = \left(\frac{-1}{p}\right)p$ donc comme p et q sont premiers entre eux, τ^2 est inversible dans E/qE. En simplifiant par $\tau^2 \bmod qE$, nous obtenons

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\frac{q}{p}\right)$$

puisque l'égalité modulo qE équivaut à l'égalité pour des valeurs dans $\{\pm 1\}$. Finalement, nous avons

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

□

Proposition 6.3.5 *Pour tout nombre impair p, on a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

exercice 16 *Le but de l'exercice est le calcul de $\left(\frac{2}{p}\right)$ lorsque p est un nombre premier impair. On pose $A = \mathbb{Z}/p\mathbb{Z}[X]/(X^4+1)$ et on note α la classe de X modulo X^4+1. Soit $b = \alpha + \alpha^{-1}$.*

1. *Montrer que $b^2 = \overline{2}$ puis que $\overline{\left(\frac{2}{p}\right)} = b^p \mid b$.*
2. *Montrer que $b^p = \alpha^p + \alpha^{-p}$.*
3. *En déduire que $b^p = b$ si $p \equiv 1 \bmod 8$ ou $p \equiv 7 \bmod 8$ et $b^p = -b$ si $p \equiv 3 \bmod 8$ ou $p \equiv 5 \bmod 8$.*
4. *Conclure.*

Le Théorème et la proposition qui précèdent permettent le calcul du symbole de Legendre.

Exemple 10 *Calculons $\left(\frac{11}{29}\right)$. Nous avons*

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2}{7}\right)^2 = -(-1)^{\frac{7^2-1}{4}} = -1.$$

Donc 11 n'est pas un carré modulo 29.

Chapitre 7

L'anneau euclidien $\mathbb{Z}[i]$

7.1 Division euclidienne dans $\mathbb{Z}[i]$

Notons

$$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\} \subset \mathbb{C}.$$

On définit sur $\mathbb{Z}[i]$ la norme $N(z) = |z|\,|^2$ et on rappelle l'identité dite de *Lagrange* :

$$N(zz') = N(z)N(z').$$

La proposition suivante est immédiate.

Proposition 7.1.1 *L'anneau $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ donc il est commutatif intègre. Par ailleurs si $z \mid z'$ il existe $t \in U(\mathbb{Z}[i])$ tel que $z' = tz$ et donc $N(z)$ divise $N(z')$.*

Théorème 7.1.2 *Soient z et z' dans $\mathbb{Z}[i]$ tels que $z' \neq 0$. Il existe q et r dans $\mathbb{Z}[i]$ tels que*

$$z = qz' + r \text{ et } N(r) < N(z').$$

On dit que l'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Preuve. Le point M d'affixe le nombre complexe $\frac{z}{z'}$ doit appartenir à l'un des carrés $C_{k,l}$ de sommets d'affixes

$$k + il, (k + 1) + il, (k + 1) + i(l + 1), k + i(l + 1)$$

puisque $\mathbb{C} = \cup_{k,l} C_{k,l}$. Chaque carré $C_{k,l}$ est centré en un point $O_{k,l}$ d'affixe $o_{k,l} = (k + \frac{1}{2}) + i(l + \frac{1}{2})$, ce point $O_{k,l}$ est le point le plus éloigné de chaque sommet . Ainsi, il existe, pour z et z' donnés tels que $M \in C_{k,l}$, un sommet $q \in \{k + il, (k + 1) + il, (k + 1) + i(l + 1), k + i(l + 1)\}$ le plus proche de $\frac{z}{z'}$ de sorte que

$$|\frac{z}{z'} - q| \leq |o_{k,l} - q| \leq \frac{\sqrt{2}}{2} < 1.$$

Ce point q n'est pas forcément unique si on est sur un des axes de symétries du carré ou a fortiori si on a par hasard $\frac{z}{z'} = o_{k,l}$ (4 choix équidistants). En multipliant l'inégalité ci-dessus par z' puis en élevant au carré, on obtient :

$$N(z - qz') = \left|z - qz'\right|^2 \leq \frac{|z'|^2}{2} < N(z')$$

ce qui établit, en posant $r = z - qz'$, que l'anneau est euclidien. □

Comme l'anneau est euclidien, il est principal et factoriel donc on a les résultats de décomposition en produits de facteurs irréductibles, unique à l'ordre près des facteurs, et l'existence de ppcm et de pgcd.

7.2 Irréductibles dans $\mathbb{Z}$ et dans $\mathbb{Z}[i]$

Soit p un entier relatif, on peut le voir comme un élément de $\mathbb{Z}[i]$ et on va commencer par décrire les conditions dans lesquelles p serait premier de $\mathbb{Z}$ mais non irréductible dans $\mathbb{Z}[i]$.

Proposition 7.2.1 *Soit p un nombre premier de $\mathbb{Z}$. Alors il y a équivalence entre les assertions suivantes :*

1. *p n'est pas irréductible dans $\mathbb{Z}[i]$,*
2. *il existe un $z \in \mathbb{Z}[i]$ tel que $p = \pm N(z)$,*
3. *-1 est un carré modulo p.*
4. *$p = 2$ ou $p \equiv 1 \bmod 4$*

Preuve.

1. 1) $\Longrightarrow$ 2) Si p n'est pas irréductible dans $\mathbb{Z}[i]$, il existe z et z' qui ne sont pas des unités de $\mathbb{Z}[i]$ de sorte que $p = zz'$. Mais alors $p^2 = N(p) = N(z)N(z')$ et comme z et z' ne sont pas des unités de $\mathbb{Z}[i]$, on doit avoir $p = N(z) = N(z')$ si $p \in \mathbb{N}$ et $p = -N(z)$ sinon.
2. 2) $\Longrightarrow$ 3) S'il existe un $z = x + iy \in \mathbb{Z}[i]$ tel que $p = \pm N(z)$, on a donc $p = \pm(x^2 + y^2)$ et modulo p , $x^2 + y^2 \equiv 0 \bmod p$. Puisque y n'est pas divisible par p, cela signifie que -1 est un carré modulo p. En effet dans $\mathbb{Z}/p\mathbb{Z}$, on a $-\overline{1} = \overline{x}^2(\overline{y}^{-1})^2$.
3. 3) $\Longrightarrow$ 1) Si -1 est un carré modulo p, cela signifie que p divise a^2+1 où a est un représentant de la classe $\bar{a}$ telle que $\bar{a}^2 = -1$ dans $\mathbb{Z}/p\mathbb{Z}$. Comme $a^2 + 1 = (a + i)(a - i)$ et que $\mathbb{Z}[i]$ est euclidien, si p était irréductible, il diviserait $a + i$ ou $a - i$ (Lemme de Gauss) mais si, par exemple, p divise $a+i$ alors $p = \bar{p}$ diviserait $a-i$ donc p diviserait $2a$ et p diviserait $2i$. Donc $N(p) = p^2$ diviserait 4. Mais soit $p = 2$ et donc p n'est pas irréductible ($2 = (1 + i)(1 - i)$) soit p est impair c'est impossible . Donc quoiqu'il arrive, p n'est pas irréductible.
4. L'équivalence entre 3 et 4 vient du fait que lorsque p est impair $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ donc vaut 1 si et seulement si $p \equiv 1 \bmod 4$. □

Corollaire 7.2.2 *Un entier premier p de $\mathbb{Z}$ est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv 3[4]$.*

Corollaire 7.2.3 *Les irréductibles de $\mathbb{Z}[i]$ sont*
-d'une part les nombres premiers de $\mathbb{Z}$ congrus à 3 modulo 4 et leurs associés,
-d'autre part, les éléments $z = a + ib$ pour lesquels $N(z)$ est un nombre premier p de $\mathbb{N}$ égal à 2 ou congru à 1 modulo 4.

Preuve : On considère $z = a + ib$ que l'on suppose irréductible. Si $ab = 0$, on est ramené au cas de $z \in \mathbb{Z}$ à association près. Il est clair que si $z \in \mathbb{Z}$ il ne peut être irréductible que si z est déjà premier dans $\mathbb{Z}$ et alors, la proposition (7.2.1), ou son corollaire, dit que $z \equiv 3 \bmod 4$.

Si $N(z) = a^2 + b^2$ avec $ab \neq 0$, alors on doit avoir nécessairement que $N(z)$ est premier dans $\mathbb{N}$. En effet, sinon, le théorème fondamental de l'arithmétique dans $\mathbb{Z}$ dit que $N(z) = p_1 \dots p_k$ ce qui dans $\mathbb{Z}[i]$ se lit

$$z\bar{z} = p_1 \dots p_k.$$

Mais z étant irréductible, il existe un indice i tel que z divise p_i et bien sûr $\bar{z}$ divise lui aussi p_i. Comme z et $\bar{z}$ ne peuvent être associés (pourquoi ?), le lemme de Gauss dit que $z\bar{z}$ divise p_i mais on a bien sûr que p_i divise $N(z) = z\bar{z}$. Donc $N(z) = p_i$ et le nombre premier $p_i = z\bar{z}$ est donc la somme de deux carrés donc c'est 2 ou bien il est congru à 1 modulo 4. Réciproquement si z dans $\mathbb{Z}[i]$ est tel que $N(z)$ est premier, alors z est irréductible dans $\mathbb{Z}[i]$. En effet si $z = z_1 z_2$, alors $N(z) = N(z_1)N(z_2)$ et donc $N(z_1) = 1$ ou $N(z_2) = 1$. $\square$

Chapitre 8

Anneaux Factoriels

Dans ce chapitre, on suppose que A est un anneau commutatif unitaire intègre.

8.1 Définition d'un anneau factoriel

Définition 8.1.1 *On dit que l'anneau commutatif unitaire intègre A est* factoriel *si pour tout $a \in A$ non nul admet*

- *(E) : une décomposition sous la forme*

$$a = up_1 \cdots p_r \tag{8.1}$$

  où $u \in U(A)$ et $p_1, \ldots, p_r$ sont des irréductibles
- *(U) : la décomposition est unique au sens où $a = vq_1 \cdots q_r$ ssi il existe une permutation $\sigma \in S_r$ telle que p_i et $q_{\sigma(i)}$ soient associés.*

La notion d'anneau factoriel offre une généralisation naturelle du théorème fondamental de l'arithmétique dans $\mathbb{Z}$. Malheureusement, elle est encore trop restrictive pour permettre l'étude d'anneaux aussi simples que

$$\mathbb{Z}[i\sqrt{3}] = \{a + ib \mid a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}.$$

qui n'est pas factoriel puisque $4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ dans cet anneau. Pour étudier ce type d'anneaux non factoriels, il faut introduire une classe d'anneaux plus vaste : les *annneaux de Dedekind*. Nous renvoyons le lecteur à [7] pour leur définition et propriétés qui ne seront pas abordées dans la suite. Noter également la présence d'une condition d'existence et d'une condition d'unicité dans la définition des anneaux factoriels.

Soit A un anneau intègre. On se donne un ensemble P des irréductibles dans A, c'est à dire que l'on fixe un représentant dans chaque classe

$$[p] = \{\varepsilon p \mid \varepsilon \in U(A)\}$$

où p est irréductible. Alors A est un anneau factoriel ssi chaque élément a non nul admet une décomposition unique sous la forme

$$a = u \prod_{p \in P} p^{v_p(a)}$$

où u inversible et les $v_p(a)$ son nuls sauf un nombre fini d'entre eux. L'entier $v_p(a)$ s'appelle la *valuation p-adique* de a. Il est alors clair que

$$a \mid b \Longleftrightarrow v_p(a) \leq v_p(b) \text{ pour tout } p \in P.$$

On dispose alors d'une notion naturelle de ppcm et de pgcd en posant

$$\text{ppcm}(a,b) = \prod_{p\in P} p^{\sup(v_p(a),v_p(b))} \text{ et } \text{pgcd}(a,b) = \prod_{p\in P} p^{\inf(v_p(a),v_p(b))}.$$

Noter que l'on a $(a) \cap (b) = (\text{ppcm}(a,b))$ mais seulement $(a) + (b) \subset (\text{pgcd}(a,b))$ en général si aucune autre hypothèse n'est faite sur l'anneau A.

Exemple 11 *Dans l'anneau $A = \mathbb{R}[X,Y]$, on a $\text{pgcd}(X,Y) = 1$ et $(X) + (Y) \subset \mathbb{R}[X,Y] = (1)$. Cependant, $(X) + (Y) \neq \mathbb{R}[X,Y]$ car $(X) + (Y)$ est un idéal ne contenant pas 1.*

Proposition 8.1.2 *Soit A un anneau intègre où chaque élément a non nul admet une décomposition $a = up_1 \cdots p_r$ du type (8.1). Les assertions suivantes sont équivalentes :*

1. *La décomposition est unique (au sens (U) ci-dessous),*
2. *Si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (lemme d'Euclide).*
3. *Si $a \mid bc$ et si a est premier avec b alors $b \mid c$.*

Preuve : (1) $\Longrightarrow$ (2) : l'assertion 1 signifie que A est factoriel. Dans ce cas $p \mid ab$ signifie que $v_p(ab) > 0$. Comme $v_p(ab) = v_p(a) + v_p(b)$, l'une des deux valuations $v_p(a)$ ou $v_p(b)$ doit être non nulle.

(2) $\Longrightarrow$ (1) : Si $a = up_1 \cdots p_r = vq_1 \cdots q_s$ avec u, v inversibles et $p_1, \ldots, p_r, q_1, \ldots, q_s$ irréductibles, chaque p_i divise l'un des q_j. Comme il s'agit d'irréductibles, cela montre que modulo les inversibles les ensembles $\{p_1, \ldots, p_r\}$ et $\{q_1, \ldots, q_s\}$ sont les mêmes, c'est à dire que la décomposition est unique.

(3) $\Longrightarrow$ (2) est immédiat.

(2) $\Longrightarrow$ (3) : Puisque 2 est vrai, les décompositions des éléments a, b, c sont uniques ce qui entraîne facilement (3) en considérant les valuations. □

exercice 17 *Montrer que l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ est n'est pas factoriel.*

8.2 Liens unissant les différents types d'anneaux déjà rencontrés

Proposition 8.2.1 *Soit A un anneau euclidien. Alors A est principal.*

Preuve : Notons φ le stahme sur l'anneau euclidien A. Soit I un idéal non réduit à $\{0\}$ de A et $a \in A$ non nul tels que $\varphi(a) = \min\{\varphi(\alpha) \mid \alpha \in I\}$.Considérons $\alpha \in I$. La division euclidienne de α par a implique l'existence de q, r dans A tels que $\alpha = aq + r$ et, $\varphi(r) = 0$ ou $\varphi(r) < \varphi(a)$. Comme $r = \alpha - aq$, r est dans I. Par définition de a, on a donc $r = 0$. Cela montre que $I \subset (a)$. La réciproque étant évidente, $I = (a)$ est un anneau principal. □

Proposition 8.2.2 *Soit A un anneau principal. Alors A est factoriel.*

Preuve : La preuve est similaire à celle du Théorème 3.2.5. □

Proposition 8.2.3 *Soit A un anneau factoriel. Alors $A[X]$ est factoriel.*

Preuve : La preuve est similaire à celle du Théorème 5.1.3. Elle est notamment basée sur la généralisation de la notion de contenu d'un polynôme (Voir Perrin). □

8.3 Idéaux premiers

Définition 8.3.1 *Soit I un idéal de l'anneau A. On dit que l'idéal I est premier si pour tout x et y dans A tels que $xy \in I$, on a $x \in I$ ou $y \in I$.*

Attention à ne pas confondre avec la notion d'*élément* irréductible dans A. Par définition, on toujours pour $x \neq 0$ et $x \notin U(A)$

$$(x) \text{ idéal premier} \Longrightarrow x \text{ élément irréductible dans } A$$

En effet si $x = yz$, on a $yz \in (x)$ et donc y ou z est un multiple de x. Supposons $y = xt$, cela donne $x = xtz$ et donc $x(1 - tz) = 0$. Comme A est intègre, on a finalement $tz = 1$ et z est inversible. La réciproque est fausse en général comme nous allons le voir mais vraie dans les anneaux factoriels.

Lemme 8.3.2 *Dans un anneau factoriel, on a l'équivalence*

$$(x) \textit{ idéal premier} \Leftrightarrow x \textit{ élément irréductible dans } A.$$

Preuve : Soit x un élément irréductible, et y, z deux éléments de A tels que $yz \in (x)$. Alors x divise yz. Mais puisque A est factoriel, x divise y ou z d'après la Proposition 8.1.2. Donc $y \in (x)$ ou $z \in (x)$. Cela montre que (x) est un idéal premier.□

Exemple 12 *Dans l'anneau intègre non factoriel $\mathbb{Z}[i\sqrt{3}]$, on voit en utilisant $N(z) = z\overline{z}$ que 2 est irréductible mais (2) n'est pas un idéal premier. En effet $4 = (1 + i\sqrt{3})(1 - i\sqrt{3}) \in (2)$ mais $1 + i\sqrt{3} \notin (2)$ et $1 - i\sqrt{3} \notin (2)$.*

Voici une définition alternative de la notion d'idéal premier qui la rendra plus naturelle.

Lemme 8.3.3 *Soit I un idéal de l'anneau A. Alors A/I est intègre ssi I est un idéal premier.*

Preuve : Il suffit d'observer que pour tout x et y dans A, on a l'équivalence

$$xy \in I \Longleftrightarrow \overline{xy} = \overline{0} \text{ dans } A/I.$$

□

Exemple 13 *Dans $\mathbb{Z}[X]$ l'idéal $(2, X)$ est premier mais n'est pas principal engendré par un élément irréductible. En effet, nous avons déjà vu (voir Remarque 4.1.5) que $(2, X)$ n'était pas principal. Comme $(2, X)$ contient tous les polynômes de la forme $2a_0 + a_1X + \cdots + a_nX_n$ avec $a_0, \ldots, a_n$ dans $\mathbb{Z}$, l'anneau quotient $\mathbb{Z}[X]/(2, X)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ le corps à deux éléments. Il est donc intègre ce qui montre que $I = (2, X)$ est premier.*

Lemme 8.3.4 ***Dans un anneau principal*** *pour tout élément p les équivalences ci-dessous sont vraies :*

$$p \textit{ irréductible} \Longleftrightarrow (p) \textit{ premier} \iff (p) \textit{ maximal.}$$

Cela simplifie énormément les choses. Notamment, le théorème de Bézout est vérifié.

Preuve : Supposons (p) maximal. Alors, $A/(p)$ est un corps d'après le Théorème 2.3.1. Donc $A/(p)$ est intègre et (p) est premier. On alors que p est irréductible d'après ce qui précède. Maintenant, si p est irréductible, comme A est principal (p) est maximal. En effet si $(p) \subset I$ avec I idéal de A, il existe $a \in A$ tel que $I = (a)$. On a alors $(p) \subset (a)$ et a divise p ce qui n'est possible que si $(a) = (p)$ ou $(a) = I$.□

Corollaire 8.3.5 *Soit A un anneau principal. Considérons a, b deux éléments non nuls et $d = \text{pgcd}(a, b)$. Alors $(a) + (b) = (d)$. En particulier, $(a) + (b) = A$ si a et b sont premiers entre eux.*

Preuve : On a déjà vu que $(a) + (b) \subset (d)$ car $a \in (d)$ et $b \in (d)$. Par ailleurs, comme A est principal, il existe e tel que $(a) + (b) = (e)$. On a donc $(e) \subset (d)$ et donc $d \mid e$, $e \mid a$ et $e \mid b$. Par définition de $\text{pgcd}(a, b)$, cela impose que $e = d$. □

Exemple 14 *L'anneau des entiers $\mathbb{Z}$ est euclidien relativement à $v = |\ |$ la valeur absolue. L'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien relativement au stathme N.*

Il existe des anneaux principaux non euclidiens comme par exemple $\mathbb{Z}[\alpha]$ où $\alpha = \frac{1+i\sqrt{19}}{2}$ (voir [6] pour la preuve qui n'est pas immédiate).

Bibliographie

[1] J. Calais, Extension de corps, théorie de Galois, Ellipse (2006).

[2] F. Combes, Algèbre et géométrie, Bréal (2004)

[3] P. Damphouosse, Décrouvrir l'arithmétique, Ellipse (2000).

[4] M. Demazure, Cours d'algèbre Cassini (1997)..

[5] J.M. De Koninc et A. Mercier, Introduction à la théorie des nombres, Edition Québec (1994).

[6] D. Perrin, Cours d'algère, Ellipse (1996).

[7] J-P Serre, Cours d'arithmétique, PUF (1995)