

Divisibilité dans un anneau et application à l'analyse Diophantienne

REFICE Zoubida

2017-2018

Table des matières

Introduction	1
1 Notions élémentaires	3
1.1 Notions générales sur les anneaux	3
1.1.1 Quelques définitions	3
1.1.2 Corps	5
1.1.3 Anneau des polynômes	6
1.2 Idéaux et leur opérations	8
1.2.1 Idéaux	9
1.2.2 Opérations sur les idéaux	11
1.2.3 Anneau quotient	11
1.3 Divisibilité	13
1.3.1 pgcd et ppcm	14
1.3.2 Élément irréductible	16
1.3.3 Homomorphisme d'anneaux	17
2 Anneaux particuliers	19
2.1 Anneau principal	19
2.2 Anneau euclidien	21
2.3 Anneau factoriel	23
3 Quelques équations diophantiennes	26
3.1 Equation du premier ordre	27
3.2 Equations de degré supérieures	32
3.3 Système d'équations diophantiennes linéaires	37
Conclusion	40
Bibliographie	41

Introduction

Le mathématicien, comme tout être humain, il est confronté à des problèmes difficiles à résoudre dans son travail. Parmi les problèmes les plus importants et les plus actifs qui sont rencontrés par de nombreux mathématiciens est "comment résoudre des équations diophantiennes". Une équation diophantienne, en mathématique, est une équation polynômiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers, éventuellement rationnels, les coefficients étant eux-mêmes également entiers. Ce type d'équation doit son nom à Diophante d'Alexandrie, mathématicien grec du III^{ème} siècle B.C, auteur des Arithmétiques, traitant de questions de cette nature.

Résoudre une telle équation signifie d'abord décider si elle a ou non des solutions, quand elle en a il faut ensuite dire si leur ensemble est fini ou non, et pour la résoudre complètement il faut enfin déterminer toutes les solutions.

Si l'expression du problème posé est parfois simple, les méthodes de résolution peuvent devenir complexes. Carl Friedrich Gauss, au XIX^{ème} siècle, écrivait de la théorie des nombres que « son charme particulier vient de la simplicité des énoncés jointe à la difficulté des preuves. »

Certaines équations diophantiennes ont demandé pour leur résolution les efforts conjugués de nombreux mathématiciens sur plusieurs siècles. Gauss se plaignait « des efforts démesurés que lui a coûté la détermination d'un signe d'un radical dans la théorie des nombres ; bien d'autres choses ne l'ont pas retenu autant de jours que cette question l'a retenu d'années. » Le dernier théorème de Fermat est un exemple archétypal ; il est conjecturé par Pierre de Fermat et démontré en 1994 par Andrew Wiles, après 357 ans d'efforts de la part de nombreux mathématiciens. Et parmi les méthodes nécessaires de résolutions de ces équations est les anneaux avec leur applications . Pour cette importance, j'intéressé à mon mémoire pour étudier certaines

de ces équations et son résolutions par utilisé la théorie des anneaux.

Ce mémoire est réparti en trois chapitres :

Le premier chapitre consiste en un rappel des notions élémentaires de grande importance pour la théorie des anneaux utilisées par la suite : anneau, sous-anneau, corps, idéal, pgcd, ppcm, élément irréductible, et notion de la divisibilité dans un anneau...etc.

Dans le second chapitre, on fait une étude sur anneaux particuliers ; anneau principal, euclidien et anneau factoriel, ainsi que certaines de leurs propriétés .

Dans le troisième chapitre, on s'intéresse au résolution de quelques équations diophantiennes.

Chapitre 1

Notions élémentaires

Dans ce chapitre on présente des notions élémentaires pour la théorie des anneaux.

1.1 Notions générales sur les anneaux

Cette section présente des notions fondamentales concernant les anneaux, avec des exemples et quelques propriétés importantes.

1.1.1 Quelques définitions

Définition 1.1 (*Anneau*)

Un anneau $(A, +, \cdot)$ est un ensemble non vide A muni de deux opérations (lois) binaires notées respectivement "+" et "." telles que :

1. $(A, +)$ soit un groupe commutatif;
2. la loi "." est associative, c'est-à-dire $\forall a, b, c \in A$ on a : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
3. la loi "." est distributive par rapport à la loi "+", c'est-à-dire

$$\forall a, b, c \in A, \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

Remarques 1.1

- Si de plus la loi "." est commutative, c'est-à-dire $\forall a, b \in A, \quad a \cdot b = b \cdot a$ on dit que l'anneau A est commutatif.

- L'élément neutre pour "+" est appelé zéro de A et noté 0.
- Si la loi "." possède un élément neutre, il est noté 1 et l'anneau A est dit unitaire.

Exemples 1.1

1. $(\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire.

Il en est de même pour $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$.

2. $(M_n(R), +, \cdot)$, est un anneau non commutatif pour l'addition et la multiplication des matrices.
3. $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ est un anneau commutatif avec $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ pour l'addition et la multiplication induites de celles de $(\mathbb{R}, +, \times)$.

Définition 1.2 (*Diviseurs du zéro*)

Soit A un anneau. Un élément $a \neq 0$ de A est dit diviseur de zéro s'il existe un élément $b \neq 0$ de A tel que $a.b = 0$ ou $b.a = 0$.

Exemples 1.2

1. Pour $\mathbb{Z}/6\mathbb{Z}$, les éléments $\bar{2}$ et $\bar{3}$ sont des diviseurs de zéro.
2. Dans l'anneau $M_2(\mathbb{R})$ l'élément $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix}$ sont des diviseurs de zéro.

Définition 1.3 (*Anneau intègre*)

Un anneau A est intègre s'il ne possède pas de diviseur de zéro, c'est-à-dire pour $a, b \in A$, $a.b = 0 \Rightarrow a = 0$ ou $b = 0$.

Ou bien d'une façon équivalente pour $a, b \in A$; $a \neq 0$ et $b \neq 0 \Rightarrow a.b \neq 0$.

Exemples 1.3

1. \mathbb{Z} , \mathbb{Q} , \mathbb{R} , et \mathbb{C} sont des anneaux intègres.
2. $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.
3. $M_n(\mathbb{R})$ n'est pas intègre, (par exemple $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$).

Définition 1.4 (*Elément unité*)

Un élément $a \in A$ est appelé inversible ou élément unité s'il existe un élément b de A tel que $a.b = 1$ et $b.a = 1$. L'élément b est dit l'inverse de a et noté a^{-1} .

Exemples 1.4

1. Pour l'anneau \mathbb{Z} , les éléments inversibles (unités) sont 1 et -1 .

De façon général dans tout anneau unitaire 1 et -1 sont des éléments unités.

2. Pour \mathbb{R} , tout réel non nul est inversible.

3. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \}$, les éléments unités de $\mathbb{Z}/6\mathbb{Z}$ sont $\bar{1}$ et $\bar{5}$.

Proposition 1.1

Soient A un anneau unitaire et $U(A)$ l'ensemble des unités de A . Alors $(U(A), \cdot)$ est un groupe appelé groupe des unités de A .

Démonstration

On a $U(A) \subset A$

- La loi " \cdot " est interne dans $U(A)$

Soit $a, b \in U(A)$. Alors, $\exists x, y \in A$ tels que
$$\begin{cases} a \cdot x = 1 \text{ et } x \cdot a = 1 \\ b \cdot y = 1 \text{ et } y \cdot b = 1 \end{cases}$$

On a $(ab) \cdot (xy) = 1$ et $(xy) \cdot (ab) = 1$ et comme $xy \in A$ on a $(ab) \in U(A)$

- La loi " \cdot " est associative dans A , à fortiori dans $U(A)$;
- $1 \in U(A)$ l'élément neutre;
- Si $a \in U(A)$, $\exists x \in A$, tel que $a \cdot x = 1$ et $x \cdot a = 1$. Alors $a^{-1} = x \in U(A)$.

Donc $(U(A), \cdot)$ est un groupe. ■

1.1.2 Corps**Définition 1.5**

Un anneau $(A, +, \cdot)$ commutatif et unitaire, est appelé un corps si, $(A \setminus \{0\}, \cdot)$ est un groupe.

C'est-à-dire tout élément non nul est inversible.

Exemples 1.5

1. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps commutatifs.
2. Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.
3. Les quaternions $H = \{a + bi + cj + dk ; a, b, c, d \in \mathbb{R}\}$ avec l'addition et la multiplication tels que $i^2 = j^2 = k^2 = -1$ et $ij = -ji = k$ est un corps non commutatif.

Remarques 1.2

- Tout corps est un anneau intègre.
- Si \mathbb{k} est un corps, alors $U(\mathbb{k}) = \mathbb{k} - \{0\} = \mathbb{k}^*$.
- Soit $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ est un anneau intègre
 $\Leftrightarrow n$ est un premier

1.1.3 Anneau des polynômes

Soit A un anneau, X une indéterminée (symbole).

Définition 1.6

Un polynôme d'indéterminée X et à coefficients dans A est une somme formelle

$$a_0 + a_1X + a_2X^2 + a_3X^3 + \dots + a_nX^n + \dots,$$

avec $\forall i \geq 0$, $a_i \in A$ et $a_i = 0$ pour $i \geq i_0$ (certaine indice i_0).

Définition 1.7

L'ensemble de tous les polynômes d'indéterminée X et à coefficients dans A est noté $A[X]$.

Soit $p(X) \in A[X]$, avec $a_i = 0$ pour $i > n$, $p(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$

Définition 1.8

Si $a_n \neq 0$, on dit que $p(X)$ est de degré n , et on écrit :

$$\deg(p) = d^\circ p = n.$$

Si $a_0 = a_1 = \dots = a_n = 0$, $p(X)$ est le polynôme nul.

Anneau $A[X]$

Sur $A[X]$ on définit deux lois internes :

- addition (1^{ère} loi)

$$f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

$$g(X) = b_0 + b_1X + b_2X^2 + \dots + b_sX^s$$

$$(f + g)(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \dots$$

- multiplication (2^{ème} loi)

$$(f \cdot g)(X) = c_0 + c_1X + c_2X^2 + \dots + a_kX^k, \text{ tels que}$$

$$c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0,$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0, \dots, c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0$$

Théorème 1.1

L'ensemble $A[X]$ muni des lois précédentes est un anneau.

Remarques 1.3

- Si A est commutatif, alors $A[X]$ est commutatif.
- Si A est unitaire d'élément unité 1, alors $A[X]$ est unitaire d'élément unité

$$1 = 1 + 0X + 0X^2 + \dots$$

- Si A est intègre, alors $A[X]$ est intègre.
- $U(A[X]) = U(A)$.

Définition 1.9 (Anneau de Gauss)

L'ensemble $\mathbb{Z}[i] = \{x + iy; x, y \in \mathbb{Z} \text{ et } i^2 = -1\} \subset \mathbb{C}$, avec l'addition et la multiplication induites de celle de $(\mathbb{C}, +, \times)$ est un anneau appelé anneau des entiers de Gauss.

Les éléments unités de $\mathbb{Z}[i]$ sont $\{1, -1, i, -i\}$.

Caractéristique d'un anneau

Définition 1.10

Soit A un anneau commutatif et unitaire. On dit que A est de caractéristique n et on écrit $Car(A) = n$ si $n \cdot x = 0_A, \forall x \in A$ et n est le plus petit entier naturel non

nul qui vérifié cette propriété. En résumant la caractéristique d'un anneau intègre est soit zéro ou soit un entier premier.

Exemples 1.6

1. $A = \mathbb{Z}$; $Car(\mathbb{Z}) = 0 = Car(\mathbb{Q}) = Car(\mathbb{R}) = Car(\mathbb{C})$.
2. $A = \mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$; $Car(\mathbb{Z}/5\mathbb{Z}) = 5$.

Dédinition 1.11 (*Sous-Anneau*)

Soient $(A, +, \cdot)$ un anneau et S une partie non vide de A . On dit que S est un sous-anneau de A si $(S, +, \cdot)$ est lui même un anneau avec les opérations de A .

Exemples 1.7

1. $(2\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Z}, +, \times)$.
2. $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
3. On a une chaîne de sous-anneaux classiques : $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
4. $\mathbb{Z}[i] = \{n + mi; m, n \in \mathbb{Z} \text{ et } i^2 = -1\}$ et $\mathbb{Q}[i] = \{p + qj; p, q \in \mathbb{Q} \text{ et } j^2 = -1\}$ avec l'addition et la multiplication naturelles sont des sous-anneaux de \mathbb{C} .

Proposition 1.2

Soient A un anneau et $S \subset A$. On dit que S est un sous-anneau de A si, et seulement si :

- $\forall x, y \in S, (S, +), x - y \in S$;
- $\forall x, y \in S, x \cdot y \in S$.

Remarque 1.4

Soit A un anneau unitaire. On appelle sous-anneau unitaire de A tout sous-anneau de A qui contient 1_A .

1.2 Idéaux et leur opérations

Dans cette section on étudie une partie très importante d'un anneau : idéaux, avec quelques opérations définies sur eux.

1.2.1 Idéaux

Définition 1.12 (*Idéal*)

Soit A un anneau commutatif et unitaire. Un idéal (bilatère) d'un anneau A est une partie I non vide de A telle que :

1. $\forall x, y \in I$, on a $x - y \in I$;
2. $\forall a \in A, \forall x \in I$, $a \cdot x \in I$ et $x \cdot a \in I$.

Exemples 1.8

1. $A = \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de \mathbb{Z} .

Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$, $n \geq 0$.

2. Soit A un anneau, $\{0\}$ et A sont des idéaux de A .

Remarques 1.5

- Tout idéal I de A est un sous-anneau de A , mais la réciproque est fausse en général.
- Si A est un corps, les seuls idéaux de A sont $\{0\}$ et A .

Définition 1.13 (*Idéal premier*)

Un idéal I de A est dit premier, si :

1. $I \neq A$;
2. si $xy \in I$, alors $x \in I$ ou $y \in I$.

Exemple 1.9

$A = \mathbb{Z}$, $I = p\mathbb{Z}$, p est premier

- $p\mathbb{Z} \neq \mathbb{Z}$;
- supposons que $xy \in p\mathbb{Z}$ donc $p|xy \Rightarrow (p|x \text{ ou } p|y) \Rightarrow (x \in p\mathbb{Z} \text{ ou } y \in p\mathbb{Z})$

donc $p\mathbb{Z}$, p premier, est un idéal premier de \mathbb{Z} .

Définition 1.14 (*Idéal maximal*)

Un idéal I de A est maximal si :

1. $I \neq A$;
2. Si J est un idéal de A et $I \subset J$, alors $J = I$ ou $J = A$.

Exemples 1.10

1. $A = \mathbb{Z}$, $I = p\mathbb{Z}$; p est premier. On a $p\mathbb{Z} \neq \mathbb{Z}$,
soit $J = a\mathbb{Z}$ un idéal de \mathbb{Z} tel que $p\mathbb{Z} \subset a\mathbb{Z}$, alors $a|p \Rightarrow (a = 1 \text{ ou } a = p) \Rightarrow$
($J = \mathbb{Z}$ ou $J = I = p\mathbb{Z}$). Donc $p\mathbb{Z}$ est un idéal maximal de \mathbb{Z} .
2. $A = \mathbb{Z}$, $I = 6\mathbb{Z}$, $6\mathbb{Z}$ n'est pas un idéal maximal car $6\mathbb{Z} \subset 2\mathbb{Z}$.

Définition 1.15 (*Idéal principal*)

Un idéal est dit principal lorsqu'il est engendré par un seul élément a de A ; il est de la forme $\{ax; x \in A\}$ et noté aA ou (a) .

Proposition 1.3

1. $1 \in I \iff I = A$.
2. Soit $x \in U(A)$,

$$x \in I \iff I = A$$

Démonstration

1. (\Rightarrow) Supposons que $1 \in I$. Comme $I \subset A$, il suffit de montrer que $A \subset I$.

Soit $x \in A$ et $1 \in I$ et comme I est un idéal de A alors $x \cdot 1 = 1 \cdot x = x \in I$

Donc $A \subset I$.

L'implication (\Leftarrow) est évidente. ■

2. Soit $x \in U(A)$

(\Rightarrow) Si $x \in I$ avec $x \in U(A)$, alors $\exists y \in A$ tel que $x \cdot y = y \cdot x = 1$

Il résulte que $1 \in I$, donc $I = A$.

L'implication (\Leftarrow) est évidente. ■

1.2.2 Opérations sur les idéaux

Soit A un anneau commutatif unitaire.

- **Somme d'idéaux** : Soient I et J deux idéaux de A . La somme de I et J est l'idéal $I + J = \{i + j ; i \in I \text{ et } j \in J\}$.

De même $I_1 + I_2 + \dots + I_n = \{i_1 + i_2 + \dots + i_n ; i_k \in I_k, k = \overline{1, n}\}$ est un idéal de l'anneau A .

Remarque 1.6

$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, $d = \text{pgcd}(n, m)$ par exemple : $5\mathbb{Z} + 24\mathbb{Z} = \mathbb{Z}$, $\text{pgcd}(5, 24) = 1$.

Définition 1.16

1. Deux idéaux I et J de A sont étrangers si $I + J = A$.
2. Les idéaux I_1, I_2, \dots, I_n sont étrangers deux-à-deux si $\forall i \neq j, I_i + I_j = A$.

- **Intersection d'idéaux** : $I \cap J = \{x \in A ; x \in I \text{ et } x \in J\}$ est un idéal de l'anneau A .

De façon général si $(I_\alpha)_{\alpha \in \Lambda}$ est une famille d'idéaux de A , alors $\cap_{\alpha \in \Lambda} I_\alpha$ est un idéal de A .

- **Produit d'idéaux** : $I \cdot J = \{\sum_{i=1}^n a_i b_i ; n \in \mathbb{N}^*, a_i \in I \text{ et } b_i \in J\}$ est un idéal de A .

1.2.3 Anneau quotient

Définition 1.17 (*Anneau quotient*)

Soient A un anneau commutatif et unitaire et I un idéal de A . Pour $a \in A$, on définit la partie ; $a + I = \{a + x ; x \in I\}$ appelée la classe de a modulo l'idéal I .

Définition 1.18

On définit sur A la relation binaire suivante :

$$a \mathfrak{R} b \Leftrightarrow a - b \in I$$

\mathfrak{R} est une relation d'équivalence sur A .

la réflexivité : $a \mathfrak{R} a$, car $a - a = 0 \in I$.

la symétrie : $a \mathfrak{R} b \Leftrightarrow a - b \in I \Leftrightarrow -(a - b) \in I \Leftrightarrow b - a \in I \Leftrightarrow b \mathfrak{R} a$.

la transitivité :

$(a \mathfrak{R} b \text{ et } b \mathfrak{R} c) \Leftrightarrow (a - b \in I \text{ et } b - c \in I) \Rightarrow (a - b) + (b - c) \in I \Rightarrow a - c \in I$ ce qui implique $a \mathfrak{R} c$.

Soit $a \in A$

$$\begin{aligned}\bar{a} &= \{b \in A; b \mathfrak{R} a\} = \{b \in A; b - a \in I\} \\ &= \{b \in A; b - a = x, x \in I\} \\ &= \{b \in A; b = a + x, x \in I\} \\ &= \{a + x; x \in I\} = a + I\end{aligned}$$

Notation

$$A/I = A/\mathfrak{R} = \{\bar{a}; a \in A\} = \{a + I, a \in A\}.$$

Sur A/I on définit les deux lois internes :

- $(a + I) + (b + I) = a + b + I$.
- $(a + I) \cdot (b + I) = a \cdot b + I$.

C'est-à-dire $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Théorème 1.2

L'ensemble A/I pour les lois internes définies ci-dessus est un anneau appelée l'anneau quotient de A sur I .

Proposition 1.4

Soient A un anneau et I un idéal de A . On a :

- 1.** *L'anneau A/I est intègre \Leftrightarrow L'idéal I est premier.*
- 2.** *L'anneau A/I est un corps \Leftrightarrow L'idéal I est maximal.*

Corollaire 1.1

Tout idéal maximal est un idéal premier.

1.3 Divisibilité

Cette section précise quelques définitions et propriétés de la divisibilité dans un anneau intègre.

Définition 1.19

Soit $a, b \in A$. On dit que a divise b , et on écrit $a|b$, s'il existe $c \in A$ tel que ;
 $b = a \cdot c$.

Exemples 1.11

1. $A = \mathbb{Z}$, $-2|10$.
2. $A = \mathbb{Q}[x]$, $x + 1|x^2 - 1$.
3. $A = \mathbb{Z}/7\mathbb{Z}$, $\bar{3}|\bar{5}$.
4. $A = \mathbb{Z}[i]$, $(2 + i)|(7 + i)$.

Définition 1.20

On dit que deux éléments a et b de A sont associés, et on écrit $a \sim b$, si $a|b$ et $b|a$.

Exemples 1.12

1. $A = \mathbb{Z}$, 2 et -2 sont associés.
2. $A = \mathbb{R}$, chaque deux éléments non nuls sont associés.

Proposition 1.5

Soit A un anneau commutatif et unitaire.

1. $a|b \Leftrightarrow (b) \subset (a)$
2. $a \sim b \Leftrightarrow (a) = (b)$
3. si A est intègre, $a \sim b \Leftrightarrow \exists u \in U(A) ; b = au$.

Démonstration

1. $a|b \Leftrightarrow \exists x \in A$ tel que $b = a \cdot x$.

(\Rightarrow) Soit $y \in (b)$, $y = b \cdot z$, $z \in A$. Alors $y = a \cdot x \cdot z$, donc $y \in (a)$.

(\Leftarrow) Supposons que $(b) \subset (a)$

on a $b = b \cdot 1 \in (b) \Rightarrow b \in (a)$, alors $\exists x \in A$ tel que $b = a \cdot x$. Donc $a|b$. ■

2. $a \sim b \Leftrightarrow a|b$ et $b|a$

$\Leftrightarrow (b) \subset (a)$ et $(a) \subset (b)$

$\Leftrightarrow (a) = (b)$. ■

3. A est intègre

(\Rightarrow) Si $a = 0$ et $b \sim a$, alors $b = 0$, et on a, $0 = 0 \cdot u \forall u \in U(A)$.

Supposons $b \neq 0$, ($a \neq 0$), $a \sim b \Leftrightarrow (a|b \text{ et } b|a) \Leftrightarrow (b = a \cdot x, x \in A \text{ et } a = b \cdot y, y \in A)$, donc $b = b \cdot y \cdot x \Rightarrow (y \cdot x - 1)b = 0$ et comme A intègre, on a $y \cdot x = 1$ ce qui implique $x \in U(A)$ et $y \in U(A)$. Donc $b = a \cdot x$, $x \in U(A)$

(\Leftarrow) s'il existe $u \in U(A)$ tel que $b = a \cdot u \Rightarrow a|b$ (*)

D'autre part on a $b \cdot u^{-1} = a \Rightarrow b|a$. (**)

De (*) et (**) $a \sim b$. ■

1.3.1 pgcd et ppcm

Définition 1.21 (*pgcd*)

Soient a et b deux éléments de A . Un plus grand commun diviseur de a et b est un élément d de A tel que :

1. $d|a$ et $d|b$;

2. si $c \in A$ avec $c|a$ et $c|b$, alors $c|d$.

Et on écrit $d = \text{pgcd}(a, b) = (a, b) = a \wedge b$.

Exemples 1.13

1. $A = \mathbb{Z}$, $a = 15$ et $b = 20$;

5 est un *pgcd* de 15 et 20, et -5 est un autre *pgcd* de 15 et 20.

2. $A = \mathbb{Q}[x]$, $a = f(x) = x^2 - 2x + 1$ et $b = g(x) = x^2 - 1$

$x - 1$ est un *pgcd* de $f(x)$ et $g(x)$.

Remarque 1.7

d est un *pgcd* de a et b si, et seulement si, $(a) + (b) = (d)$.

Proposition 1.6

Si d_1 et d_2 sont deux *pgcd* de a et b , alors d_1 et d_2 sont associés.

Démonstration

On a :

$$\begin{cases} (a) + (b) = (d_1) \\ (a) + (b) = (d_2) \end{cases} \Rightarrow (d_1) = (d_2)$$

donc d_1 et d_2 sont associés. ■

Définition 1.22

On dit que a_1, a_2, \dots, a_n ; $n \geq 2$ sont premiers entre eux ou étrangers si $\text{pgcd}(a_1, a_2, \dots, a_n)$ est un élément inversible, ce qui revient à dire que leur *pgcd* est égal 1.

Définition 1.23 (*ppcm*)

Soient a et b deux éléments de A . Un plus petit commun multiple de a et b est un élément m de A tel que :

1. $a|m$ et $b|m$;

2. si $c \in A$ avec $a|c$ et $b|c$, alors $m|c$.

On écrit $m = \text{ppcm}(a, b)$.

Exemple 1.14

$A = \mathbb{Z}$, $a = 3$ et $b = 7$; 21 est un *ppcm* de 3 et 7.

1.3.2 Élément irréductible

Définition 1.24

Un élément $p \in A$ est dit irréductible si :

1. $p \neq 0$ et $p \notin U(A)$;
2. si $p = a \cdot b$ avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.

Exemples 1.15

1. $A = \mathbb{Z}$, les éléments irréductibles de \mathbb{Z} sont les éléments $\pm p$ avec p premier.

Car, on a

- $p \neq 0$ et $p \notin U(\mathbb{Z}) = \{-1, 1\}$, car p premier, $p \geq 2$.
- Si $p = a \cdot b$, alors $a|p \Rightarrow a = 1$ ou $a = p$
 - si $a = 1$, donc $a \in U(\mathbb{Z})$.
 - si $a = p \Rightarrow b = 1 \in U(\mathbb{Z})$.

Donc p est irréductible dans \mathbb{Z} .

2. $A = \mathbb{R}[x]$, $f(x) = x^2 + 1$, $f(x)$ est irréductible dans $\mathbb{R}[x]$.
3. $A = \mathbb{C}[x]$, $f(x) = x^2 + 1 = (x + i)(x - i)$, $f(x)$ est réductible dans $\mathbb{C}[x]$.

Proposition 1.7

Soit A un anneau commutatif, unitaire et intègre. $P \in A$ est irréductible dans A si, et seulement si :

1. $p \neq 0$ et $p \notin U(A)$;
2. si $a|p$ alors $a \in U(A)$ ou a est associé à p .

Démonstration

p est irréductible dans A , alors 1 est vérifié.

$$\begin{aligned} a|p &\Leftrightarrow p = a \cdot b; b \in A \\ &\Leftrightarrow a \in U(A) \text{ ou } b \in U(A) \\ &\Leftrightarrow a \in U(A) \text{ ou } a \sim p. \blacksquare \end{aligned}$$

Proposition 1.8

Soit A un anneau commutatif, unitaire et intègre, $p \neq 0$ un élément de A .

1. (p) est premier $\Rightarrow p$ est irréductible.
2. (p) est maximal $\Rightarrow p$ est irréductible.

Démonstration

1. (p) est premier et par l'hypothèse $p \neq 0$, $p \notin U(A)$ car sinon $(p) = A$ ceci contredit (p) est premier.

Supposons $p = a \cdot b$ et $a, b \in A$.

$p \in (p) \Rightarrow a \cdot b \in (p) \Rightarrow a \in (p)$ ou $b \in (p)$.

- Si $a \in (p)$, $a = p \cdot a'$, $a' \in A$, alors $p = p \cdot a' \cdot b$ ce qui implique $p(a' \cdot b - 1) = 0$ et comme A est intègre, on a $a' \cdot b = 1$. Donc on a bien $b \in U(A)$.
- Si $b \in (p)$, de la même façon on trouve $a \in U(A)$.

Donc p est irréductible.

2. (p) est maximal $\Rightarrow (p)$ est premier $\Rightarrow p$ est irréductible. ■

1.3.3 Homomorphisme d'anneaux

Soient A et B deux anneaux.

Définition 1.25

Un homomorphisme d'anneaux est une application $f : A \longrightarrow B$ telle que :

1. $\forall x, y \in A, f(x + y) = f(x) + f(y)$;
2. $\forall x, y \in A, f(x \cdot y) = f(x) \cdot f(y)$.

Proposition 1.9

Soit $f : A \longrightarrow B$ un homomorphisme d'anneau.

1. Si S un sous-anneau d'un anneau A , alors $f(S)$ est un sous-anneau de B .
2. $\text{Ker}(f) = \{x \in A ; f(x) = 0_B\}$ est un idéal de A appelé le noyau de f .

Démonstration

1. Soient $x = f(s) \in f(S)$ et $y = f(t) \in f(S)$.

- $x - y = f(s) - f(t) = f(s - t)$ et $s - t \in S$.
- $x \cdot y = f(s) \cdot f(t) = f(s \cdot t)$ et $s \cdot t \in S$.

Donc $f(S)$ est un sous-anneau de B . ■

2. Soient $x, y \in \text{Ker}(f)$ et $a \in A$.

- $f(x - y) = f(x) - f(y) = 0_B - 0_B = 0_B$, alors $x - y \in \text{Ker}(f)$.
- $f(ax) = f(a) \cdot f(x) = f(a) \cdot 0_B = 0_B$, alors $ax \in \text{Ker}(f)$.
- $f(xa) = f(x) \cdot f(a) = 0_B \cdot f(a) = 0_B$, alors $xa \in \text{Ker}(f)$.

Donc $\text{Ker}(f)$ est un idéal de A . ■

Chapitre 2

Anneaux particuliers

Dans ce chapitre, on étudie quelques notions attachées aux anneaux intègres et commutatifs.

2.1 Anneau principal

Définition 2.1

Un anneau A commutatif et unitaire est un anneau principal si, A est intègre et si tout idéal de A est principal.

Exemples 2.1

1. \mathbb{Z} est un anneau principal, car \mathbb{Z} est intègre et tout idéal de \mathbb{Z} est de la forme :
$$n\mathbb{Z} = (n), n \geq 0.$$
2. Si \mathbb{k} est un corps commutatif, l'anneau $\mathbb{k}[X]$ est principal.

Proposition 2.1

Soit A un anneau principal, pour tout a et b dans A , un pgcd de a et b existe.

Démonstration

Soit $(a, b) \in A^2$, $(a) + (b)$ est un idéal de A et comme A est principal alors, il existe $d \in A$ tel que $(a) + (b) = (d)$. Donc d est un pgcd (a, b) . ■

Proposition 2.2

Soit A un anneau principal, on a :

(p) est premier $\Leftrightarrow (p)$ est maximal $\Leftrightarrow p$ est irréductible.

Démonstration

On a dans n'importe quel anneau intègre,

$$\left\{ \begin{array}{l} (p) \text{ est maximal} \Rightarrow p \text{ est irréductible.} \\ (p) \text{ est premier} \Rightarrow p \text{ est irréductible.} \\ (p) \text{ est maximal} \Rightarrow (p) \text{ est premier.} \end{array} \right.$$

Alors il suffit de montrer que : p est irréductible $\Rightarrow (p)$ est maximal.

p est irréductible $\Rightarrow p \notin U(A) \Rightarrow (p) \neq A$.

- Soit I un idéal de A tel que $(p) \subset I$.

A est principal $\Rightarrow \exists a \in A$ tel que $I = (a)$.

$(p) \subset (a)$, c'est-à-dire $a|p \Rightarrow a \in U(A)$ ou $a \sim p$

· si $a \in U(A) \Rightarrow (a) = I = A$

· si $a \sim p \Rightarrow (a) = I = (p)$

alors on a bien (p) est maximal.

Donc (p) est maximal $\Leftrightarrow p$ est irréductible.

Ce qui implique p est irréductible $\Rightarrow (p)$ est premier.

Alors p est irréductible $\Leftrightarrow (p)$ est premier. ■

Proposition 2.3

Soit A un anneau principal, p est irréductible dans A . Si $p|ab \Rightarrow p|a$ ou $p|b$.

Démonstration

Supposons que p ne divise pas a , soit $\lambda = \text{pgcd}(a, p)$, alors $\lambda|p$, par suite $\lambda \in U(A)$ ou $\lambda \sim p$.

Si $\lambda \sim p \Rightarrow \lambda = p \cdot \varepsilon$ tel que $\varepsilon \in U(A)$, donc on a aussi p est un $\text{pgcd}(a, p)$, ce qui implique que $p|a$ contradiction.

Donc $\lambda \in U(A)$, alors a et p sont étrangers. D'après le théorème de Bézout il existe $x, y \in A$; $ax + py = 1$ ce qui implique $abx + pby = b$. Donc on a bien $p|b$. ■

En général, si p est irréductible $p|a_1 a_2 \dots a_n \Rightarrow \exists i_0 = \overline{1, n}$ tel que $p|a_{i_0}$.

2.2 Anneau euclidien

La difficulté de définir une division sur un anneau est que l'anneau considéré n'est pas nécessairement un ensemble ordonné. C'est pour cela qu'il nous faut recourir à une fonction qui nous permettra de plonger les éléments de notre anneau dans \mathbb{N} qui est ordonné.

Définition 2.2 (Dévision euclidienne)

Soit $(A, +, \cdot)$ un anneau. On dit que A est muni d'une division euclidienne s'il existe une application φ

$\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$, telle que :

1. $\forall a, b \in A^*, \varphi(a) \leq \varphi(ab)$.

2. Pour $(a, b) \in A \times A^*$, il existe $(q, r) \in A^2$ tels que :

$a = bq + r$, avec $r = 0$ ou $(r \neq 0 \text{ et } \varphi(r) < \varphi(b))$.

(q est le quotient de la division euclidienne de a par b et r est le reste).

On dit parfois que l'application φ est un stathme euclidien.

Définition 2.3

On dit qu'un anneau A est euclidien s'il est intègre et possède une division euclidienne (stathme euclidien).

Exemples 2.2

1. $A = \mathbb{Z}$, $\varphi : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$

$$x \longmapsto \varphi(x) = |x|$$

\mathbb{Z} est un anneau euclidien.

2. \mathbb{k} corps, $A = \mathbb{k}[x]$, $\varphi : (\mathbb{k}[x]) \setminus \{0\} \longrightarrow \mathbb{N}$

$$g(x) \longmapsto \deg(g)$$

$\mathbb{k}[x]$ est un anneau euclidien.

3. $\mathbb{Z}[i]$ avec le stathme φ tel que $\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{N}$,

$$a + ib \longmapsto a^2 + b^2$$

est un anneau euclidien.

Théorème 2.1

Tout anneau euclidien est un anneau principal.

Démonstration

Soit I un idéal de A .

- Si $I = \{0\}$, alors $I = (0)$.
- Supposons que $I \neq \{0\}$

soit $x_0 \in I$, $x_0 \neq 0$ tel que $\varphi(x_0) = \min_{x \in I} (\varphi(x))$ où φ est le stathme de A (*)

Montrons que $(x_0) = I$.

" \subset " $x_0 \in I$, on a $(x_0) = \{x_0 \cdot a, a \in A\}$

Comme $x_0 \in I$, alors $\Rightarrow x_0 \cdot a \in I$ pour tout $a \in A \Rightarrow (x_0) \subset I$.

" \supset " Soit $x \in I$; $x \neq 0$

A est euclidien $\Rightarrow \exists q, r \in A$ tels que $x = x_0 q + r$, avec $r = 0$ ou $\varphi(r) < \varphi(x_0)$.

Supposons que $\varphi(r) < \varphi(x_0)$, on a $r = x - x_0 q$. $x \in I$, $x_0 \in I$ et $q \in A$, alors $r \in I$, le fait $r \in I$ et $\varphi(r) < \varphi(x_0)$ contredit la définition de x_0 (selon (*)). On a nécessairement $r = 0$, alors $x = x_0 q \in (x_0) \Rightarrow I \subset (x_0)$. Donc $I = (x_0)$. ■

Théorème 2.2 (Algorithme d'Euclide).

Soit a, b deux éléments d'un anneau euclidien A avec b non nul.

On écrit des divisions euclidiennes successives,

$$a = bq_1 + r_1 ; \text{ tel que } \varphi(r_1) < \varphi(b)$$

$$b = r_1 q_2 + r_2 ; \text{ tel que } \varphi(r_2) < \varphi(r_1)$$

$$r_1 = r_2 q_3 + r_3 ; \text{ tel que } \varphi(r_3) < \varphi(r_2)$$

$$\vdots \qquad \qquad \qquad \vdots$$

$$r_{k-2} = r_{k-1} q_k + r_k \text{ tel que } \varphi(r_k) < \varphi(r_{k-1})$$

$$r_{k-1} = r_k q_{k+1} + 0.$$

Si $r_1 = 0$, alors $b = \text{pgcd}(a, b)$; sinon $r_k = \text{pgcd}(a, b)$.

Exemples 2.3

1. On calcule le $\text{pgcd}(713, 253)$

$$713 = 2 \times 253 + 207 \quad , \quad a = 713, b = 253, r_1 = 207$$

$$253 = 1 \times 207 + 46 \quad , \quad r_2 = 46$$

$$207 = 4 \times 46 + 23 \quad , \quad r_3 = 23$$

$$46 = 2 \times 23 + 0 \quad , \quad r_4 = 0$$

Le dernier reste non nul est le pgcd . Alors $\text{pgcd}(713, 253) = 23$.

2. On détermine d le plus grand commun diviseur de $f(x) = 2x^4 + 2$, $g(x) = x^5 + 2$ dans $\mathbb{Z}_3[x]$ et on trouve $s(x), t(x) \in \mathbb{Z}_3[x]$ tels que :

$$d = s(x)(2x^4 + 2) + t(x)(x^5 + 2).$$

Par la division successive, on trouve :

$$x^5 + 2 = (2x)(2x^4 + 2) + (2x + 2) \quad (1)$$

$$2x^4 + 2 = (x^3 + 2x^2 + x + 2)(2x + 2) + 1 \quad (2)$$

$$2x + 2 = (2x + 2) \times 1 + 0 \quad (3)$$

Alors $\text{pgcd}(f(x), g(x)) = 1$.

De l'équation (2) on a

$$\begin{aligned} 1 &= (2x^4 + 2) - (x^3 + 2x^2 + x + 2)(2x + 2) \\ &= (2x^4 + 2) - (x^3 + 2x^2 + x + 2)(x^5 + 2 - (2x)(2x^4 + 2)) \end{aligned}$$

de l'équation (1)

$$1 = (2x^4 + x^3 + 2x^2 + x + 1)(2x^4 + 2) + (2x^3 + x^2 + 2x + 1)(x^5 + 2).$$

Donc,

$$s(x) = 2x^4 + x^3 + 2x^2 + x + 1 \text{ et } t(x) = 2x^3 + x^2 + 2x + 1.$$

2.3 Anneau factoriel

Il y a une importance dans certains anneaux de pouvoir décomposer (de façon essentiellement unique) un élément en produit d'irréductibles. Les anneaux factoriels sont les anneaux intègres possédant cette propriété.

Définition 2.4

Un anneau intègre A est dit factoriel (de factorisation unique) si les deux conditions suivantes sont vérifiées :

1. Pour tout $x \in A$, $x \neq 0$, $x \notin U(A)$, x s'écrit sous la forme :

$$x = p_1 p_2 \dots p_k, \quad k \geq 1, \text{ avec } p_i \text{ irréductible dans } A.$$

2. Si $x = q_1 q_2 \dots q_s$, $s \geq 1$, avec q_j irréductible dans A , est une autre écriture de

$$x \in A|(U(A) \cup \{0\}) \text{ alors } k = s \text{ et } \forall i = \overline{1, k}, \exists j = \overline{1, k} \text{ tel que } p_i \sim q_j.$$

Exemples 2.4

1. \mathbb{Z} est un anneau factoriel.

2. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, car par exemple : $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et $3 \not\sim 2 + i\sqrt{5}$ et $3 \not\sim 2 - i\sqrt{5}$.

Théorème 2.3

Tout anneau principal est factoriel.

Démonstration

A est un anneau intègre car A est principal, dans l'anneau principal A tout élément $x \neq 0$, non inversible est produit fini d'éléments irréductibles. S'il n'en était pas ainsi, alors $x = a_1 b_1$, $a_1 \notin U(A)$ et $b_1 \notin U(A)$, on a $a_1 | x \Rightarrow (x) \subsetneq (a_1)$, l'un des facteurs au moins, a_1 n'étant pas produit fini d'éléments irréductibles. On a pour a_1 une décomposition analogue $a_1 = a_2 b_2$ avec $a_2 \notin U(A)$ et $b_2 \notin U(A)$ on a $a_2 | a_1 \Rightarrow (a_1) \subsetneq (a_2)$ où l'un des facteurs, par exemple a_2 , n'est pas produit fini d'éléments irréductibles. La suite d'éléments a_1, a_2, \dots ainsi mise en évidence, engendre une suite infinie croissante d'idéaux principaux, avec $x = (a_0)$

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

Soit $I = \bigcup (a_i)$, I est un idéal de A alors il existe $a \in A$ tel que $I = (a)$, on a

$$a \in I, \exists i_0 \geq 0 \text{ avec } a \in (a_{i_0}).$$

$$(a_{i_0}) \subset I = (a) \subset (a_{i_0}), \text{ donc } I = (a_{i_0}).$$

De ce fait on voit que $(a_{i_0}) = (a_{i_0+1})$ qui contredit la construction de la suite $(a_i)_{i \geq 0}$ car $(a_{i_0}) \subsetneq (a_{i_0+1})$.

Supposons que x admette deux factorisations : $x = p_1 \dots p_r = q_1 \dots q_s$ en éléments irréductibles. Alors p_1 divise le produit $q_1 \dots q_s$, c'est-à-dire que $q_1 \dots q_s \in p_1 A$. Puisque $p_1 A$ est un idéal premier, il existe $q_i \in p_1 A$, donc, puisque q_i est irréductible, $q_i = u_i p_1$ avec u_i élément inversible.

Nous pouvons écrire après simplification $p_2 \dots p_r = u_i q_1 \dots \hat{q}_i \dots q_s$ (\hat{q}_i signifie que le facteur q_i est omis). Ce qui implique que $\forall i = 2, \dots, r$ on a $p_i \sim q_j$ par récurrence sur r .

Alors $r = s$ et $\forall i = \overline{1, r}, \exists j = \overline{1, s}$ tel que $p_i \sim q_j$.

Donc A est un anneau factoriel. ■

Proposition 2.4

Soit A un anneau factoriel, p est irréductible dans A . Si $p|ab$ alors $p|a$ ou $p|b$.

Démonstration

Soient $a, b, c \in A$ et $p \cdot c = a \cdot b$. Supposons que $a \neq 0, b \neq 0$ et $c \neq 0$ non inversibles.

$p \cdot c_1 c_2 \dots c_n = a_1 a_2 \dots a_m b_1 b_2 \dots b_s$ tel que c_i, a_j, b_t sont irréductibles dans A , alors $p \sim a_{j_0}$ ou $p \sim b_{t_0} \Rightarrow p|a$ ou $p|b$. ■

Proposition 2.5

Si A est un anneau factoriel et $a \in A$, alors :

(a) est un idéal premier $\Leftrightarrow a$ est irréductible.

Démonstration

(\Rightarrow) Il est clair.

(\Leftarrow) Soit a irréductible, c'est-à-dire $a \neq 0$ et $a \notin U(A)$, alors $(a) \neq A$ (*)

soit $xy \in (a) \Rightarrow a|xy \Rightarrow a|x$ ou $a|y$ ceci implique $x \in (a)$ ou $y \in (a)$ (**)

de (*) et (**) l'idéal (a) est un idéal premier. ■

Chapitre 3

Quelques équations diophantiennes

Une des parties les plus passionnantes de la théorie des nombres est les équations diophantiennes. Dans ce chapitre on étudie quelques équations ou des systèmes d'équations diophantiennes, c'est-à-dire d'équations à coefficients et ensemble de solutions contenus dans \mathbb{Z} ou \mathbb{Q} .

Définition 3.1

Une équation diophantienne est une équation polynômiale

$$p(x_1, x_2, \dots, x_n) = 0$$

à coefficients entiers dont on cherche les solutions entières, c'est-à-dire dans \mathbb{Z}^n ou dans \mathbb{Q}^n .

Théorème 3.1 (Théorème de Bézout)

Soient $a, b \in \mathbb{N}$, non tous deux nuls et $d \in \mathbb{N}$. Les propositions suivantes sont équivalentes :

- 1.** *d est le pgcd de a et b ;*
- 2.** *Il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$.*

En particulier, a et b sont premiers entre eux ($\text{pgcd}(a, b) = 1$) si, et seulement si, il existe $u, v \in \mathbb{Z}$; $au + bv = 1$.

Théorème 3.2 (Théorème de Gauss)

Soient a, b et c trois entiers relatifs tels que a divise bc et a est premier avec b , alors a divise c .

Démonstration

Si $a|bc \Rightarrow \exists d$ tel que $bc = ad$ et comme $(a, b) = 1 \Rightarrow \exists u, v \in \mathbb{Z}; au + bv = 1$ ce qui implique $acu + adv = c$, donc $a(cu + dv) = c$. Ce qui prouve que $a|c$. ■

3.1 Equation du premier ordre

Equation $ax + by = c$

Il s'agit de résoudre dans \mathbb{Z} l'équation $ax + by = c$ d'inconnues x et y , les entiers a, b et c étant fixés.

Proposition 3.1

Soient $(a, b) \in \mathbb{Z}$, pas tous les deux nuls, et $c \in \mathbb{Z}$. L'équation $ax + by = c$ a une solution si, et seulement si, $d|c$ tel que $d = \text{pgcd}(a, b)$.

Démonstration

Supposons que l'équation admette une solution (x, y) . Comme d divise a et b , alors $d|(ax + by) = c$. D'où le résultat.

Réciproquement, supposons que $d|c$. Ecrivons $a = da'$, $b = db'$ et $c = dc'$ tels que a', b' et $c' \in \mathbb{Z}$. On sait que $a' \wedge b' = 1$ comme $((a, b) \neq (0, 0), d \neq 0)$ et l'équation est équivalente à $a'x + b'y = c'$. Comme $a' \wedge b' = 1$, $\exists (u, v) \in \mathbb{Z}^2$ tels que $a'u + b'v = 1$ donc $a'uc' + b'vc' = c'$ et le couple $(x, y) = (uc', vc')$ est une solution particulière de l'équation $ax + by = c$. ■

Remarquons que la connaissance d'une solution particulière notée (x_0, y_0) de l'équation $a'x + b'y = c'$ permet la détermination de toutes les autres solutions de l'équation. En effet, (x, y) est une solution si, et seulement si :

$$a'x + b'y = c = a'x_0 + b'y_0$$

C'est-à-dire $a'(x - x_0) = b'(y_0 - y)$

Puis que $a' \wedge b' = 1$ cette égalité équivaut, d'après le lemme de Gauss à l'existence de $k \in \mathbb{Z}$ tel que :

$$(x - x_0) = kb' \text{ et } (y_0 - y) = ka'.$$

L'ensemble des solutions est donc $\mathcal{L} = \{(x_0 + kb', y_0 - ka'); k \in \mathbb{Z}\}$.

Méthode Résolution de l'équation $ax + by = c$

- Si $a \wedge b$ ne divise pas c , l'équation n'admet aucune solution.
 - Si $(a \wedge b) | c$, écrire $d = a \wedge b$, $a = da'$, $b = db'$ et $c = dc'$ avec a', b' et c' dans \mathbb{Z} .
l'équation est équivalente à $a'x + b'y = c'$.
1. On commence par rechercher une solution particulière (x_0, y_0) en exploitant une relation de Bézout entre a' et b' .
 2. Résoudre l'équation en écrivant qu'un couple (x, y) est solution si, et seulement si, $a'x + b'y = a'x_0 + b'y_0$, i.e, $a'(x - x_0) = b'(y_0 - y)$. On applique ensuite le lemme de Gauss (on a $a' \wedge b' = 1$) pour conclure que les solutions sont les couples d'entiers de la forme $(x_0 + kb', y_0 - ka')$ avec $k \in \mathbb{Z}$.

Exemple 3.1

Résoudre l'équation : $9x + 12y = 3$ avec x et y sont des entiers relatifs.
Avant de commencer vérifions s'il y a des solutions : on détermine $\text{pgcd}(9, 12) = 3$, on peut diviser les trois coefficients de l'équation par 3 :

$$9x + 12y = 3 \Leftrightarrow 3x + 4y = 1 \text{ Or, } \text{pgcd}(3, 4) = 1$$

- **Solution particulière de $3x + 4y = 1$.**

On remarque que $(-1, 1)$ est une solution particulière de cette équation, car $3(-1) + 4(1) = 1$.

- **Solution générale de $3x + 4y = 1$.**

Un couple (x, y) d'entiers est donc solution si, et seulement si :
 $3x + 4y = 3(-1) + 4(1)$, c'est-à-dire $3(x + 1) = 4(-y + 1)$, alors 3 divise $4(-y + 1)$, et comme le $\text{pgcd}(3, 4) = 1$ alors d'après le théorème de Gauss, 3 divise $-y + 1$. Donc il existe $k \in \mathbb{Z}$ tel que $-y + 1 = 3k$.

Pour tout $k \in \mathbb{Z}$, si $-y + 1 = 3k$ alors : $[3(x+1) = 4(-y+1)] \Leftrightarrow [3(x+1) = 4 \times 3k]$ alors $x + 1 = 4k$. Ce qui implique $\forall k \in \mathbb{Z}$, $x = 4k - 1$ et $y = -3k + 1$.
Donc l'ensemble des solutions de $9x + 12y = 3$ est $\{(-1 + 4k, 1 - 3k), k \in \mathbb{Z}\}$.

Exemple 3.2

Résoudre dans \mathbb{Z}^2 l'équation $8x + 12y = 2$.
On a le $\text{pgcd}(8, 12) = 4$ Or, 4 n'est pas un diviseur de 2 donc l'équation n'admet pas de solution dans \mathbb{Z}^2 .

Exemple 3.3

Résoudre l'équation : $630x - 1088y = 20$ avec x et y des entiers relatifs.
Avant de commencer vérifions s'il y a des solutions on détermine $\text{pgcd}(630, 1088) = 2$.
Comme 20 est un multiple de 2, il y a des solutions, donc on peut poursuivre.
Simplifions l'équation par 2, on obtient : $315x - 544y = 10$.

Solution particulière de $315x - 544y = 10$.

On écrit l'algorithme d'Euclide :

$$544 = 315 + 229$$

$$315 = 229 + 86$$

$$229 = 2(86) + 57$$

$$86 = 57 + 29$$

$$57 = 29 + 28$$

$$29 = 28 + 1$$

Puis, on va « remonter » pour aboutir à une égalité du type $1 = 315() + 544()$
Pour cela, on garde 544 et 315 à chaque fois qu'on les trouve puis on remplace les autres nombres par l'égalité « la plus haute » dans l'algorithme.

$$\begin{aligned} 1 &= 29 - 28 \\ &= 86 - 57 - (57 - 29) \\ &= 86 - 2(57) + 29 \\ &= 315 - 229 - 2(229 - 2(86)) + 86 - 57 \\ &= 315 - 3(229) + 5(86) - 57 \\ &= 315 - 3(544 - 315) + 5(315 - 229) - (229 - 2(86)) \end{aligned}$$

$$\begin{aligned}
&= -3(544) + 9(315) - 6(229) + 2(86) \\
&= 9(315) - 3(544) - 6(544 - 315) + 2(315 - 229) \\
&= -9(544) + 17(315) - 2(229) \\
&= -9(544) + 17(315) - 2(544 - 315) = -11(544) + 19(315)
\end{aligned}$$

On a donc : $1 = 315(19) - 544(11)$.

La solution particulière de $315x - 544y = 1$ est donc le couple $(19, 11)$.

Solution particulière de $315x - 544y = 10$.

Puisque $315(19) - 544(11) = 1$ alors en multipliant les deux membres par 10, on obtient : $315(190) - 544(110) = 10$. Donc une solution particulière de $315x - 544y = 10$ est le couple : $(x_0, y_0) = (190, 110)$

Solution générale de $315x - 544y = 10$.

L'équation est vraie pour la solution particulière donc : $315x_0 - 544y_0 = 10$
on veut : $315x - 544y = 10$. Donc : $315x_0 - 544y_0 = 315x - 544y$, c'est-à-dire
 $315(x_0 - x) = 544(y_0 - y)$.

Maintenant,

544 divise $315(x_0 - x)$. Comme 315 et 544 sont premiers entre eux donc par le théorème de Gauss, 544 divise $x_0 - x$. Il existe donc k entier relatif tel que :

$$(x_0 - x) = 544k \text{ ce qui donne : } x = 190 - 544k.$$

On remplace dans l'équation : $315(x_0 - x) = 544(y_0 - y)$

alors, $315(544k) = 544(y_0 - y)$ ce qui implique : $y = 110 - 315k$.

On vérifie que le couple trouvé fonctionne : $315(190 - 544k) - 544(110 - 315k) = 10$.
Les solutions sont donc les couples $(190 - 544k, 110 - 315k)$ avec k entier relatif.

Théorème 3.3

L'algorithme d'Euclide permet de résoudre les congruences linéaires.

Démonstration

On considère une congruence linéaire de la forme $ax \equiv c[b]$, elle a une solution si, et seulement si, l'équation $ax + by = c$ admet des solutions entiers pour x et y . Cette congruence est aussi équivalent l'équation $[a][x] = [b]$ dans \mathbb{Z}_n . ■

Exemple 3.4

Résoudre des systèmes de congruences

$$\text{On veut résoudre } \begin{cases} x \equiv 1[11] \\ x \equiv 3[4] \end{cases}$$

Par définition, il existe u et v entiers relatifs tels que $x = 11u + 1$ et $x = 4v + 3$.

On doit donc résoudre : $11u + 1 = 4v + 3$ c'est-à-dire $11u - 4v = 2$. C'est bien une équation diophantienne .

- Solution particulière : $(u, v) = (2, 5)$
- Solution générale :

On a : $u = 4k + 2$ et $v = 11k + 5$.

Donc $x = 11u + 1 = 11(4k + 2) + 1 = 23 + 44k$.

Utilisation du logiciel Xcas

Dans l'application arithmétique Pour obtenir une solution particulière de l'équation $ax + by = c$, on utilise l'instruction `iabcuv(a, b, c)`. Par exemple pour l'équation $7x + 12y = 1$, On entre dans la barre de saisie : `iabcuv(7, 12, 1)`.

Le résultat affiché est : $(-5, 3)$

Vérification :

$$7 \times (-5) + 12 \times 3 = -35 + 36 = 1.$$

Sinon, Le résultat affiché est : pas de solution, Par exemple l'équation $8x + 12y = 2$ n'admet pas de solution.

Remarque 3.1

Pour télécharger Xcas, allez sur le site :

http://www-fourier.ujf-grenoble.fr/~parisse/install_fr.html

Pour traiter les exemples, il est conseillé d'ouvrir Xcas :

- Sous Windows en installation locale, on clique sur l'icone xcasfr du bureau.
- Sous Linux avec Gnome, on clique sur Xcas du menu Education. Sinon, ouvrir un terminal et taper `xcas &`.
- Sur Mac, cliquez sur Xcas dans le menu Applications du Finder.

Lors de la première utilisation, choisissez Xcas lorsqu'on vous demande de choisir une syntaxe (sauf si vous connaissez le langage Maple). Nous donnons ici seulement le minimum de l'interface à connaître pour commencer à programmer. On consultera plutôt le manuel Débuter en calcul formel ou les autres manuels (menu Aide) pour apprendre à utiliser les fonctionnalités de Xcas en calcul formel, géométrie, tableur, etc..

Equations $a_1x_1+a_2x_2+.... + a_nx_n=c$

Même méthode, avec Bézout on a condition nécessaire et suffisante d'existence des solutions. Par linéarité on casse le problème en solution particulière et solution homogène.

Pour vraiment résoudre, il faut se ramener au problème précédent avec deux inconnues seulement.

3.2 Equations de degré supérieures

Equation de Pythagore : $x^2+y^2=z^2$

Soit (x, y, z) une solution en entiers premiers entre eux. Les nombres x et y ne peuvent être tous deux impairs sinon $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$, d'où $z^2 \equiv 2[4]$.

Contrairement au fait que z^2 est un carré. On a donc après échange éventuel de x et y : x impair, y pair et z impair.

Posons $y = 2y'$, $z + x = 2x'$ et $z - x = 2z'$ où y', x' et z' sont des entiers, car y , $z + x$ et $z - x$ sont pairs. On a alors $y'^2 = x'z'$. tout diviseur commun de x' et z' divise $x = x' - z'$ et $z = x' + z'$, donc x' et z' sont des entiers premiers entre eux ; la décomposition en facteurs premiers de y'^2 montre que x' et z' sont des carrés u^2 et v^2 d'où $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$.

Naturellement, u et v sont premiers entre eux ; sinon x, y et z auraient un facteur premier commun.

Equation de Fermat : $x^n+y^n=z^n$ (le cas $n = 4$)

En vue d'étudier le cas $n = 4$, considérons l'équation diophantienne $x^4 + y^4 = z^2$.

Soit (x, y, z) une solution en entiers premiers entre eux (x^2, y^2, z) est une solution de l'équation de Pythagore et il existe u et v deux entiers premiers entre eux tels que :

$$x^2 = u^2 - v^2, y^2 = 2uv \text{ et } z = u^2 + v^2.$$

(x, v, u) est encore une solution de l'équation de Pythagore et il existe a et b deux entiers premiers entre eux tel que : $x = a^2 - b^2$, $v = 2ab$ et $u = a^2 + b^2$ d'où $y^2 = 4ab(a^2 + b^2)$. puis que a et b sont premiers entre eux, il en est de même de a, b et $a^2 + b^2$, donc la décomposition en facteurs premiers de y^2 montre que a, b et $a^2 + b^2$ sont des carrés, d'où $a = \alpha^2$, $b = \beta^2$ et $a^2 + b^2 = \gamma^2$.

En particulier : $\alpha^4 + \beta^4 = \gamma^2$, c'est-à-dire que (α, β, γ) est une solution de l'équation $x^4 + y^4 = z^2$. Mais $\gamma < \gamma^2 = u < z = u^2 + v^2$. Ainsi, s'il existe une solution (x, y, z) en entiers positifs premiers entre eux, il doit exister une autre solution (α, β, γ) en entiers positifs avec $\gamma < z$.

On peut donc construire une suite (x_n, y_n, z_n) de solutions où la suite (z_n) est strictement décroissante, ce qui est absurde. L'équation $x^4 + y^4 = z^2$ n'admet donc aucune solution positive en nombres entiers.

De l'étude ci dessus, il résulte que l'équation de Fermat $x^4 + y^4 = z^4$ est impossible en nombres entiers. Il suffit d'écrire $x^4 + y^4 = (z^2)^2$.

Equation : $x^2 + 2 = y^3$

Considérons l'anneau $A = \mathbb{Z}[\sqrt{-2}]$, sous anneau de \mathbb{C} , formé des éléments de la forme : $x + y\sqrt{-2}$, avec $x, y \in \mathbb{Z}$.

l'application : $\alpha = x + y\sqrt{-2} \mapsto (x + y\sqrt{-2})(x - y\sqrt{-2}) = x^2 + 2y^2$ est un stathme euclidien.

$$\begin{aligned} \text{L'application : } A &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\ x + y\sqrt{-2} &\longmapsto \bar{x} \end{aligned}$$

est un épimorphisme de noyau $p = \sqrt{-2}A$ d'où $A/p \cong \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z}$ est un anneau intègre et donc p est un idéal premier. Puisque l'anneau A est principal, $\sqrt{-2}$ est un élément irréductible.

Soit q l'idéal engendré par les éléments $x - \sqrt{-2}$ et $x + \sqrt{-2}$. Donc on a bien $x + \sqrt{-2} - (x - \sqrt{-2}) = 2\sqrt{-2} \in q$, c'est-à-dire $(\sqrt{-2})^3 \in q$; q est principal donc nécessairement de la forme $(\sqrt{-2})^m$, $(0 \leq m \leq 3)$.

Si $m \neq 0$, $x + \sqrt{-2} = (a + b\sqrt{-2})\sqrt{-2}$ donc $x = -2b$; si (x, y) est un couple solution de $x^2 + 2 = y^3$, alors $4b^2 + 2 = y^3$ d'où $y^3 \equiv 2[4]$, ce qui est impossible, donc $m = 0$ et $q = A$.

Ainsi, si (x, y) est un couple solution de $x^2 + 2 = y^3$, les éléments $x + \sqrt{-2}$ et $x - \sqrt{-2}$ sont deux éléments étrangers de l'anneau A .

Si $x + y\sqrt{-2}$ est un élément inversible de l'anneau A , $x^2 + 2y^2 = 1$ ce qui implique $x = \pm 1$ et $y = 0$ donc -1 et 1 sont les seules unités de A .

Soit (x, y) est une solution de l'équation $x^2 + 2 = y^3$. On a la factorisation :

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3.$$

Puisque A est factoriel, ceci impose que $x + \sqrt{-2}$ est un cube dans A . D'où :

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 \quad (a, b \in \mathbb{Z}),$$

$$\text{d'où} \quad x = a^3 - 6ab^2;$$

$$1 = (3a^2 - 2b^2)b.$$

Alors $b = \pm 1$; $3a^2 - 2 = \pm 1$.

Donc $a = \pm 1$ et $x = \pm 5$, puis $y = 3$.

Remarque 3.2

Cet exemple illustre une technique utilisée pour la première fois par Euler en 1770. Pour résoudre l'équation de Fermat, $x^3 + y^3 = z^3$, il se ramène à écrire que $p^2 + 3q^2$ est un cube, ce qu'il fait en posant $p + q\sqrt{-3} = (r + s\sqrt{-3})^3$, admettant ainsi que $\mathbb{Z}[\sqrt{-3}]$ est principal, ce qui inexact. Il est possible que dans la «démonstration» de son célèbre théorème, Fermat ait commis une erreur de ce type.

Equation de Pell : $x^2 - dy^2 = \pm 1$

Soit d un entier positif non carré. On cherche des solutions en entiers (x, y) de l'équation $x^2 - dy^2 = \pm 1$. Encore une fois, on cherche surtout des solutions positives, les autres étant obtenues en changeant les signes des solutions positives.

Pour $d = 2$ on a les solutions suivantes de $x^2 - 2y^2 = \pm 1$

$$(x, y) = (1, 1), (3, 2), (7, 5), (17, 12), (41, 29), (99, 70), \dots$$

Pour $d = 3$ on a les solutions suivantes de $x^2 - 3y^2 = \pm 1$

$$(x, y) = (2, 1), (7, 4), (26, 15), (97, 56), \dots$$

Pour étudier l'équation de Pell, on travaille avec l'ensemble

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

On présente quelques propriétés de cet ensemble. C'est ce qu'on appelle un anneau commutatif ou plus précisément un sous-anneau commutatif de \mathbb{R} .

C'est-à-dire, c'est un sous-ensemble de \mathbb{R} contenant 0 et 1 avec les propriétés que les sommes, produits et opposés de membres de $\mathbb{Z}[\sqrt{d}]$ restent dans $\mathbb{Z}[\sqrt{d}]$.

Pour les sommes et opposés, cela est assez évident. Pour les produits, on a

$$(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + (ab' + ba')\sqrt{d}$$

Dans $\mathbb{Z}[\sqrt{d}]$ il y a une opération de conjugaison, définie par :

$$\overline{a + b\sqrt{d}} = a - b\sqrt{d}$$

Cette conjugaison n'est pas la conjugaison complexe car tous ces nombres sont réels, mais elle a beaucoup des mêmes propriétés formelles.

En particulier on a :

$$\begin{aligned}\overline{(a + b\sqrt{d}) + (a' + b'\sqrt{d})} &= \overline{(a + b\sqrt{d})} + \overline{(a' + b'\sqrt{d})} \\ \overline{(a + b\sqrt{d})(a' + b'\sqrt{d})} &= \overline{(a + b\sqrt{d})} \cdot \overline{(a' + b'\sqrt{d})}\end{aligned}$$

La somme des conjuguées est la conjuguée de la somme, et idem pour les produits.

Maintenant on définit la norme d'un membre de $\mathbb{Z}[\sqrt{d}]$ comme suite :

$$\begin{aligned}N(a + b\sqrt{d}) &= (a + b\sqrt{d})\overline{(a + b\sqrt{d})} \\ &= (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= a^2 - db^2 \in \mathbb{Z}.\end{aligned}$$

La norme d'un membre de $\mathbb{Z}[\sqrt{d}]$ est ainsi toujours un entier relatif.

Lemme 3.1

Pour $(a + b\sqrt{d})$ et $(a' + b'\sqrt{d})$ dans $\mathbb{Z}[\sqrt{d}]$ on a

$$N((a + b\sqrt{d})(a' + b'\sqrt{d})) = N(a + b\sqrt{d}) \cdot N(a' + b'\sqrt{d})$$

Démonstration

On a

$$\begin{aligned} N((a + b\sqrt{d})(a' + b'\sqrt{d})) &= (a + b\sqrt{d})(a' + b'\sqrt{d}) \cdot \overline{(a + b\sqrt{d})(a' + b'\sqrt{d})} \\ &= (a + b\sqrt{d})(a' + b'\sqrt{d}) \overline{(a + b\sqrt{d})} \overline{(a' + b'\sqrt{d})} \\ &= (a + b\sqrt{d}) \overline{(a + b\sqrt{d})} (a' + b'\sqrt{d}) \overline{(a' + b'\sqrt{d})} \\ &= N(a + b\sqrt{d}) \cdot N(a' + b'\sqrt{d}). \end{aligned}$$

■

Lemme 3.2

Les solutions (x, y) de l'équation de Pell $x^2 - dy^2 = \pm 1$ correspondent aux éléments $x + y\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ avec $N(x + y\sqrt{d}) = 1$.

Ces $x + y\sqrt{d}$ avec $N(x + y\sqrt{d}) = 1$ s'appellent les unités ou inversibles de $\mathbb{Z}[\sqrt{d}]$.

Corollaire 3.1

Le produit de deux unités de $\mathbb{Z}[\sqrt{d}]$ est une unité. Les puissances d'une unité de $\mathbb{Z}[\sqrt{d}]$ sont des unités.

Par exemple $1 + \sqrt{2}$ est une unité de $\mathbb{Z}[\sqrt{2}]$ car :

$$N(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = 1 - 2 = -1$$

Ses puissances :

$$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2},$$

$$(1 + \sqrt{2})^3 = 7 + 5\sqrt{2},$$

$$(1 + \sqrt{2})^4 = 17 + 12\sqrt{2}, \dots$$

sont aussi des unités. Elles correspondent aux solutions de l'équation de Pell $x^2 - 2y^2 = \pm 1$.

Similairement $2 + \sqrt{3}$ est une unité de $\mathbb{Z}[\sqrt{3}]$ car $N(2 + \sqrt{3}) = 1$.

Ses puissances :

$$(2 + \sqrt{3})^2 = 7 + 4\sqrt{3},$$

$$(2 + \sqrt{3})^3 = 26 + 15\sqrt{3},$$

$$(2 + \sqrt{3})^4 = 97 + 56\sqrt{3}, \dots$$

sont aussi des unités. Elles correspondent aux solutions de l'équation de Pell $x^2 - 3y^2 = \pm 1$.

Théorème 3.4.

Soit $d \geq 2$ un entier positif non carré.

(a) *Il existe une unité $x_0 + y_0\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ avec $x_0 > 0$ et $y_0 > 0$, appelée l'unité*

fondamentale, telle que pour toute unité $x + y\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ avec $x > 0$ et $y > 0$ on a $x_0 + y_0\sqrt{d} \leq x + y\sqrt{d}$.

(b) *Les unités $x + y\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ avec $x > 0$ et $y > 0$ sont les puissances*

positives de l'unité fondamentale $x_0 + y_0\sqrt{d}$.

L'unité fondamentale de $\mathbb{Z}[\sqrt{2}]$ est $1 + \sqrt{2}$. Celle de $\mathbb{Z}[\sqrt{3}]$ est $2 + \sqrt{3}$. Celle de $\mathbb{Z}[\sqrt{5}]$ est $2 + \sqrt{5}$.

3.3 Système d'équations diophantiennes linéaires

On pose $A \in M_{m,n}(\mathbb{Z})$ et $B \in \mathbb{Z}^m$ et on étudie $AX = B$ où $X \in \mathbb{Z}^n$.

Il est facile de plonger dans \mathbb{Q} et de trouver toutes les solutions $X \in \mathbb{Q}^n$: c'est l'ensemble vide ou un sous-espace affine de \mathbb{Q}^n de dimension $n - \text{rg} A$. Mais, trouver les points entiers dans ce sous-espace ne se réduit pas à résoudre séparément chaque équation. On a un exemple :

$$x + y = b \quad , \quad x - y = 0.$$

Chaque équation a une infinité de solutions, mais le système n'en a que si b est pair.

L'idée est d'adapter l'algorithme de Gauss en faisant des divisions euclidiennes plutôt que des quotients exacts : c'est une méthode classique pour démontrer le théorème de la base adaptée.

1. Second membre nul

On se donne $A \in \mathbb{Z}^n$ et on cherche les $X \in \mathbb{Z}^n$ tels que $AX = 0$. C'est un sous-groupe de \mathbb{Z}^n , présenté comme le noyau d'un morphisme de \mathbb{Z} -modules. Résoudre ce système, c'est trouver une représentation paramétrique.

On peut encore dire que ça consiste à présenter le sous-groupe comme l'image d'un (autre) morphisme de \mathbb{Z} -modules. Le lemme suivant n'est qu'une reformulation (d'une étape) du théorème de la base adaptée.

Lemme 3.3

L'ensemble des $X \in \mathbb{Z}^n$, solutions du système homogène $AX = 0$, est un sous-groupe de \mathbb{Z}^n , libre de rang $n - \text{rg}A$, où le rang de A est calculé dans \mathbb{Q}^n .

2. Second membre quelconque : résolution effective

On trouve dans une méthode effective, variante de l'algorithme de Gauss, qui permet de trouver P et Q inversibles (non uniques), et $d_1 | \dots | d_r$ (uniques) tels que

$$Q^{-1}AP = D, \text{ où } D = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix}$$

En gros, on obtient D à partir de A en faisant des opérations élémentaires sur les lignes et les colonnes, et P et Q gardent la trace de ces manipulations. Mais alors, si on pose $X' = P^{-1}X$ et $B' = Q^{-1}B$, on a :

$$AX = B \Leftrightarrow QDP^{-1}X = B \Leftrightarrow DX' = B'.$$

Si $B' = (b'_i) \ i = 1, \dots, n$, il y a une solution si, et seulement, si $d_i | b'_i$ pour $1 \leq i \leq r$, et dans ce cas, les solutions sont : $x'_i = b'_i / d_i$ si $1 \leq i \leq r$, et $x'_i = k_{i-r}$ quelconque si $i \geq r + 1$.

En repassant aux x_i via $X = PX'$, on constate que, s'il n'est pas vide, l'ensemble des solutions est bien de la forme attendue : "sous-espace affine" sous le noyau de A , un groupe isomorphe à \mathbb{Z}^{n-r} .

Conclusion

Les équations diophantiennes sont des équations qui jouent un rôle très important dans l'histoire des mathématiques ; c'est la source de la théorie des nombres.

Dans ce mémoire j'ai étudié quelques techniques élémentaires permettant de résoudre certaines de ces équations par exemple équation linéaire du premier ordre, équations de Pythagore et équation de Fermat... Pour cela j'intéresse à l'étude des anneaux particuliers avec des notions et des théorèmes sur les anneaux, comme la notion de la divisibilité, le pgcd et le ppcm, ainsi que l'identité de Bézout, la division euclidienne et l'algorithme d'Euclide...etc. Et leur principaux résultats pour résoudre quelques équations diophantiennes.

Bibliographie

- [1] **F. ARNAULT et al**, *Mathématiques L3 Algèbre, Cours complet avec 400 tests et exercices corrigés*, Pearson Éducation France, 2009.
- [2] **P. COLMEZ**, *Elément d'analyse et d'algèbre*, École polytechnique, octobre 2009.
- [3] **T. CONNOR et J. VERCROYSSSE**, *Algèbre I Cours pour 2^{ème} année de Bachelier en sciences mathématiques*, année académique 2012-2013, Version du 12 septembre 2012.
- [4] **O. DEBARRE**, *Algèbre 2*, École Normale supérieure, 2012-2013.
- [5] **J-R. Durbin**, *Modern Algebra, An Introduction*, Sixth Edition, The University of Texas at Austin.
- [6] **J-p. ESCOFIER**, *Tout l'algèbre de la licence Cours et exercices corrigés*, premier décembre 2005.
- [7] **D. FREDON et M. MAUMY-BERTRAND et F. BERTRAND**, *Mathématiques Algèbre et géométrie en 30 fiches*, paris 2009.
- [8] **B. GUGGER, D. RICHARD et j. TOMASIK**, *Algorithme d'Euclide et équations diophantiennes*, Université de Clermont1, IUT d'Informatique, 1ère année - 2002-2003.
- [9] **Ch. HOUZEL**, *Introduction à l'histoire de l'analyse diophantienne*, Cahier de séminaire d'histoire des mathématiques 2^{ème} série, tome 3 (1993), p :1-12.
- [10] **L. LADJELAT**, *Cours Master1, Algèbre et Arithmétique*, Université M. Bou-diaf de Msila. Année univ 2016-2017.
- [11] **J-p. MARCO, et L. LAZZARINI**, *Mathématiques L1 Algèbre, Cours complet avec 1000 tests et exercices corrigés*, Pearson Education France, 2007.

- [12] **J-p. MARCO, et PH. THIEULLEN et J. ARTHUR WEIL**, *Mathématiques L2 Algèbre, Cours complet avec 700 tests et exercices corrigés*, Pearson Education France, 2007.
- [13] **F. PERTUOL et M. DREVETON**, *Exemples d'équations diophantiennes*, 10 février 2016.
- [14] **J. QUERRE**, *Cours D'algèbre*, Université Bretagne Occidentale, Masson paris , New york , Barcelene, Milan, 1976.
- [15] **J. ROTMAN**, *A first course in abstract algebra*, University of Illinois at Urbana-Champaign, Third edition.
- [16] **J. WILLIAM GILBERT and W. KEITH NICHOLSON**, *Moderne algebra with applications*, University of Waterloo and University of Calgary, Canada.