Université du Burundi
Institut de Pédagogie Appliquée
Département de mathématiques

Syllabus du cours d'Algèbre commutative

Bac III

Volume horaire: 45 heures

Par

Professeur Aboubacar Nibirantiza

Année Académique:2024-2025

Version de Janvier 2025

Table des Matières

Chapitre 1

Préface

1.1 Contenu-matière

Le cours d'algèbre commutative est destiné aux étudiants de la 3ème année du département de mathématiques de l'Institut de Pédagogie Appliquée (IPA) de l'Université du Burundi. On commence par une introduction générale qui consiste à présenter le but de l'algèbre commutative par rapport à une gamme de branches des mathématiques. On explique brièvement les différentes structures algébriques qu'on va développer dans le corps du présent syllabus.

Ce cours est constitué de dix chapitres suivants: Le premier chapitre est une préface qui décrit le contenu-matière du cours, l'objectif général du cours, les résultats attendus et la méthodologie d'enseignement utilisé dans ce cours. Le second parle des relations d'ordre et d'équivalence. Il a pour but de rappeler certaines définitions et propriétés ainsi que quelques outils de calcul. Le troisième propose aux étudiants le principe de démonstration par récurrence. Dans ces deux précédents chapitres, on donne des exemples sous forme d'exercices résolus et non résolus pour inviter les étudiants à s'entraîner aux outils de calculs.

Dans le quatrième chapitre, on explique les notions algébriques fondamentales telles que les structures de groupe, d'anneaux et d'anneaux intègres. Les étudiants futurs enseignants du fondamental et du post-fondamental doivent maîtriser à fond ces notions parce qu'elles sont vues en premier lieu en premier année du post-fondamental. La notion de corps étant un anneau particulier intervient dans plusieurs branches des mathématiques. On montre dans ce chapitre le lien entre le corps et l'anneau. Dans le chapitre cinq, on montre aux futurs enseignants comment on construit des espaces quotients dans lesquels on étudie des structures où l'on ne s'intéresse qu'à quelques

propriétés bien spécifiques des éléments étudiés. Par exemple :

- l'étude des entiers relatifs où l'on ne s'intéresse qu'à la divisibilité par un entier naturel donné;
- l'étude d'un espace vectoriel affine où l'on ne s'intéresse qu'à la direction de la droite joignant deux points donnés;
- l'étude d'un groupe muni d'un endomorphisme où l'on s'intéresse qu'à l'image des éléments par ce morphisme.

Dans tous ces exemples, le fait que deux éléments x et y aient la même propriété étudiée (en d'autres termes, le fait qu'ils soient équivalents pour la propriété étudiée) peut se traduire par une relation compatible avec les lois qui nous intéressent.

Bref, dans ces espaces quotients, on manipule les éléments appelés classes d'équivalence. Donc les relations d'équivalence consistent à regrouper les éléments d'un ensemble par famille et on définit les opérations habituelles entre ces familles. Cela a pour but de montrer aux futurs enseignants que les opérations habituelles peuvent être définies différemment selon qu'on se trouve dans tel ou tel autre espace.

Dans les chapitres six et sept, nous traitons les notions nous permettant de manipuler avec aisance les différentes opérations de base faisant intervenir les idéaux (la somme et le produit par exemple). Ensuite, manipuler avec aisance les domaines intégrités, domaines euclidiens, domaines à idéaux principaux (plus particulièrement les anneaux de polynômes sur un corps). Nous amenons les étudiants à être capable de reconnaître les différents types d'idéaux (premiers, maximaux, nilpotents, etc.)

Dans le chapitre huit, nous appliquons les notions vues dans les chapitres six et sept au cas de l'anneau des polynômes à une indéterminée et à n indéterminées.

Les chapitres neuf et dix se focalisent sur les anneaux produits et le corps des fractions. On généralise la construction d'un anneau quotient sur un anneau quelconque, c'est qu'on appelle la localisation. On termine dans le chapitre dix par la divisibilité dans un anneau. L'objectif principal dans ce chapitre est l'étude sommaire de la divisibilité dans un cadre plus général que celui déjà bien connu de l'anneau $\mathbb{Z}$. Nous manipulons pour cette étude les anneaux commutatifs intègres, la congruence et les équations de congruences.

1.2 Objectif général du cours

Faire acquérir aux étudiants les fondements de la géométrie algébrique et ceux de la théorie algébrique des nombres et assurer une bonne maîtrise des outils de calcul en algèbre en général et en algèbre commutative en particulier.

1.3 Objectifs spécifiques

À la fin de l'ECUE, l'étudiant devrait être capable de :

a) reconnaître les anneaux, les anneaux intègres et effectuer la divisibilité dans un anneau,

b) définir les idéaux et opérer sur eux,

c) reconnaître les anneaux principaux et maximaux,

d) transférer les idéaux par un morphisme d'anneaux,

e) opérer sur les espaces quotients

f) manipuler les anneaux de polynômes à une indéterminée.

1.4 Méthodologie d'enseignement

1.4.1 Présentation du cours

Les grandes lignes de chaque chapitre seront présentées sur Power-Point. Ainsi, on explique brièvement le but de chaque chapitre et son utilité comme outils mathématique. On combine diverses méthodes lors de l'enseignement. Il s'agit des méthodes interactive, participative et expositive.

1.4.2 Travaux pratiques et dirigés

On initie les étudiants à faire des présentations sur des thèmes variés en rapport les chapitres vus dans le cours. On leur demande de vérifier manuellement certaines assertions données dans le texte. On propose aussi des exercices corrigés et des exercices non corrigés.

1.4.3 Syllabus du cours

Les étudiants seront indiqués où ils peuvent trouver le présent syllabus (numéro d'enregistrement au répertoire des publications)

1.4.4 Mode d'évaluation

L'évaluation des acquis est constitué de:

- l'évaluation formative sous forme d'interrogations, de devoirs à domicile ou de travaux pratiques et dirigés qui représente 40% des notes.
- un examen écrit à la fin du semestre qui vaut 60% des notes.

Chapitre 2

Relations d'ordre et relations d'équivalence

Les relations d'ordre et d'équivalence sont importantes en mathématiques. Les relations d'ordre mettent un ordre parmi les éléments d'un ensemble tandis que les relations d'équivalence consistent à regrouper les éléments d'un ensemble par famille.

2.1 Définitions

Définition 1. *Une relation sur un ensemble E est un sous-ensemble R de l'ensemble $E \times E$, produit cartésien de E par lui-même.*

Par exemple, si E={Habitants de Bujumbura}, on peut prendre pour R le sous-ensemble

$$\{(x, y) : x \quad \text{et } y \quad \text{sont habitants de Bujumbura de même nom}\}.$$

Un autre exemple est $E = \mathbb{Z}$ et $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \,\text{pair}\}$

On notera xRy plutôt que le couple (x, y) pour dire que x et y sont en relation.

Définition 2. *Soit E un ensemble et R une relation sur E. On dit que R est une relation d'ordre si R a les trois propriétés suivantes:*

- *Pour tout $x \in E$, on a xRx, on dit que R est réflexive,*
- *Pour tous $x, y \in E$, si xRy et yRx impliquent $x = y$, alors on dit que R est antisymétrique,*

- *Pour tous $x, y \in E$, si xRy et yRz impliquent xRz, alors on dit que R est transitive.*

Les deux exemples suivants sont fondamentaux.

Exemple 1. *Si on prend $E = \mathbb{N}$ ou bien $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et on définit*

$$R = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq y\},$$

cet ordre est appelé ordre naturel. Il est facile de vérifier les trois propriétés de la définition.

Exemple 2. *Soit X un ensemble quelconque et $E = P(X)$, l'ensemble des sous-ensembles de X. On définit la relation d'inclusion, notée $\subseteq$ dans E. Il est facile de voir que*

- *pour tout $A \in E$, on a $A \subseteq A$,*
- *pour tous $A, B \in E$, $A \subseteq B$ et $B \subseteq A$ impliquent que $A = B$,*
- *pour tous $A, B; C \in E$, $A \subseteq B$ et $B \subseteq C$ impliquent que $A \subseteq C$.*

Par analogie avec l'exemple 1, on note souvent un ordre par $\leq$ au lieu de R.

Définition 3. *Une relation d'ordre $\leq$ sur un ensemble E est totale si pour tous x, y dans E, $x \leq y$ ou $y \leq x$.*

Cela signifie que deux éléments quelconques de E sont toujours comparables pour l'ordre $\leq$. Si l'ordre n'est pas total, on dit souvent ordre partiel.

Définition 4. *Soit E un ensemble muni d'un ordre $\leq$ et A un sous-ensemble de E. On dit que A a un maximum ou un plus grand élément s'il y a dans A un élément a tel que $\forall x \in A, x \leq a$.*

On définit de manière analogue un minimum ou plus petit élément.

Définition 5. *Soit E un ensemble muni d'un ordre $\leq$ et A un sous-ensemble de E. on dit que $a \in A$ est un élément maximal de A si*

$$\forall b \in A, a \leq b \Rightarrow a = b.$$

En d'autres termes termes, $a < b$, i.e. $a \leq b$ et $a \neq b$ avec $b \in A$ est impossible.

On définit de manière analogue un élément minimal. Bien sûr tout maximum est maximal mais la réciproque est fausse.

Exemple 3.
- *Soit $E = P(X)$. Le minimum de E est l'ensemble vide $\emptyset$ et le maximum X.*
- *Soit $X = \{x, y, z\}$ et A le sous-ensemble de E défini par*

$$A = \{\{x, \{y\}, \{z\}, \{y, z\}, \{z, x\}, \{x, y\}\} = P(X) \setminus \{\emptyset, X\}.$$

On voit que A n'a ni minimum ni maximum. Cependant les singletons $\{x\}, \{y\}$ et $\{z\}$ sont des éléments minimaux et $\{x, z\}, \{x, y\}$ et $\{y, z\}$ sont des éléments maximaux de A.

Définition 6. *Une relation R sur un ensemble E est une relation d'équivalence si elle est reflexive, transitive et de plus symétrique, i.e, $xRy \Rightarrow yRx$.*

On peut donner plusieurs exemples ici. Si on définit une fonction f sur un ensemble E vers un ensemble F.

Exemple 4. *En définissant la relation sur E par xRy si $f(x) = f(y)$, on peut vérifier que R est une relation d'équivalence.*

Définition 7. *Soit E un ensemble et R une relation d'équivalence sur E. Une classe d'équivalence de R est un sous-ensemble A de E tel qu'il existe a de E vérifiant $A = \{x \in E : xRa\}$. On notera $[a]$ ou $\bar{a}$ une classe d'équivalence de a.*

Le théorème suivant montre qu'avoir une relation d'équivalence sur un ensemble revient à regrouper ses éléments en classes.

Théorème 1. *Soit E un ensemble et R une relation d'équivalence sur E. Alors E est la réunion disjointe des classes d'équivalence pour R.*

Démonstration. Il faut montrer que tout élément de E appartient à une classe d'équivalence, et que deux classes d'équivalence distinctes ont une intersection vide.

1. Si $x \in E$ alors $x \in [x]$ puisque $[x] = \{y \in E : yRx\}$ et que R est réflexive.
2. Soient C_1 et C_2 deux classes d'équivalence. Nous pouvons trouver des éléments x_1, x_2 de E tels que, pour $i = 1, 2$, on ait $C_i = \{y \in E : yRx_i\}$. supposons que C_1 et C_2 n'aient

pas une intersection vide, i.e, il existe $y \in C_1 \cap C_2$. On a alors, par définition de C_1 et C_2, yRx_1 et yRx_2. Par symétrie de R, nous avons x_1Ry et par transitivité, on x_1Rx_2. Nous montrons maintenant que $C_2 \subseteq C_1$. En effet, soit $x \in C_1$. Alors xRx_1. Comme x_1Rx_2, on a aussi xRx_2 par transitivité. Donc $x \in C_2$. Cela signifie que tout élément de C_1 est aussi un élément de C_2. L'inclusion $C_2 \subseteq C_1$ se montre de manière analogue, en utilisant x_2Rx_1. Finalement, nous avons $C_1 = C_2$, ce qui montre que deux classes d'équivalence sont toujours soit d'intersection vide, soit égales. □

2.2 Exercices résolus

1. On définit sur $\mathbb{Z}$ une relation R par xRy si $x - y$ est divisible par 2. Montrer que c'est une relation d'équivalence et déterminer ses classes d'équivalence.

En effet, il est facile de vérifier les trois propriétés de la définition. Il n'y a que deux classes d'équivalences suivantes: $\{x : x \quad \text{est pair}\}$ et $\{x : x \quad \text{est impair}\}$.

2.On considère $E = P(X)$ où X est un ensemble fini et l'on y définit la relation ARB si A et B ont même nombre d'éléments. Montrer que c'est une relation d'équivalence. En effet, on peut utiliser l'exemple 4 pour montrer cela.

Soit $f : E \to \mathbb{N} : A \mapsto |A|$. On a donc

$$f^{-1}(n) = \{A \subseteq X : |A| = n\}.$$

On constate que $f^{-1}(0) = \{\emptyset\}$, et $f^{-1}(n) = \emptyset$ si $n > |X|$, $f^{-1}(m) = \{X\}$ si $|X| = m$. Plus concrètement, si $X = \{a, b, c\}$, $E = \{\{\emptyset\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Il y a quatre classes d'équivalence:$\{\emptyset\}, \{\{a\}, \{b\}, \{c\}\}, \{\{a, b\}, \{a, c\}, \{b, c\}\}$ et $\{\{a, b, c\}\}$.

3. On considère l'ensemble $\mathbb{N}^*$ avec la relation (dite de divisibilité) R définie par aRb s'il existe $n \in \mathbb{N}^*$ tel que $b = na$. Montrer que c'est une relation d'ordre qui n'est pas totale. Trouver les éléments maximaux et minimaux de $A = \{2, 3, 4, ..., 9, 10\}$.

En effet, on a:

(transitivité) Si a divise b et b divise c alors $c = mb$ et $b = na$ d'où $c = (mn)a$ et a divise c.

(antisymétrie) Si a divise b et b divise a alors $b = na$ et $a = mb$ d'où $nm = 1$ et $n = m = 1$, et $a = b$.

(réflexivité) Comme $a = 1.a$ on a bien aRa, pour tout $a \in \mathbb{N}^*$. Cette relation d'ordre n'est pas totale car, par exemple pour $n = 2$ et $m = 3$ on n'a ni n divise m, ni m divise n, i.e. 2 et 3 ne sont pas comparables.

Les éléments minimaux de A sont $2, 3, 5, 7$; les maximaux sont $6, 7, 8, 9, 10$.

Chapitre 3

Raisonnement par récurrence

On veut montrer une propriété qu'ont tous les entiers naturels n, par exemple: "la somme de tous les entiers de 0 à n est égale à $n(n+1)/2$". Comme on considère une propriété quelconque, on va la noter $P(n)$ et lire : n a la propriété P. On veut montrer donc que $P(0)$ est vraie, ainsi que $P(1), P(2) \ldots$ jusqu'à l'infini. On utilise pour cela le raisonnement par récurrence, ou par induction.

3.1 Principe de récurrence

On veut démontrer une propriété $P(n)$ de tous les entiers naturels. On fait comme suit:

(i) On démontre que $P(0)$ est vraie

(ii) On fait l'hypothèse que $P(n)$ est vraie (hypothèse de récurrence) et on démontre que $P(n+1)$ est vraie. Autrement dit, on démontre que $P(n)$ est vraie implique $P(n+1)$ est vraie.

Ceci étant fait, on est sûr que la propriété est vraie pour tous les entiers: intuitivement en effet, $P(0)$ est vrai par (i), donc $P(1)$ est vraie par (ii), donc $P(2)$ est vraie par (ii), etc...

3.2 Exemple

$P(n)$ est la propriété "la somme des entiers de 0 à n est égale à $n(n+1)/2$. En effet, On a

(i) $P(0)$ est vraie car $0 = 0.(0+1)/2$.
(ii) Supposons que $P(n)$ soit vraie, i.e. $0+1+2+..+n = n(n+1)/2$. De cette égalité on déduit, par addition de $n+1$ de chaque côté:

$$0+1+2+...+n+(n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)) + 2n + 2}{2} = \frac{(n+1)(n+2)}{2}.$$

Pour illustrer le principe de récurrence, démontrons le théorème suivant.

Théorème 2. *Tout sous-ensemble non vide de* $\mathbb{N}$ *a un minimum.*

Démonstration. 1. Nous commençons par démontrer qu'une certaine propriété $P(n)$ est vraie pour tout n dans $\mathbb{N}$. Puis nous verrons que le théorème s'en déduit.
On prend pour $P(n)$ l'énoncé suivant: " tout sous-ensemble de $\mathbb{N}$ qui contient un entier $\leq n$ a un minimum.
Démontrons que $P(n)$ est vrai, en utilisant le principe de récurrence.

> (i) $P(0)$ signifie que si un sous-ensemble de $\mathbb{N}$ contient 0, alors il a un minimum. C'est clair, puisque alors 0 est son minimum. Donc $P(0)$ est vraie. (ii) L'hypothèse de récurrence est: si un sous-ensemble A de $\mathbb{N}$ contient un élément $\leq n$, alors A a un minimum (c'est la propriété $P(n)$).

Nous en déduisons $P(n+1)$: en effet, soit E un sous-ensemble de $\mathbb{N}$ qui contient un élément $\leq n+1$. Si E contient un élément $\leq n$, l'hypothèse de récurrence implique que E a un minimum. Si par contre E ne contient aucun élément $\leq n$, comme il contient un élément $\leq n+1$, il doit contenir $n+1$. Mais alors $n+1$ est son minimum. Ainsi $P(n+1)$ est vraie.

2. Pour finir la preuve du théorème, soit maintenant E un sous-ensemble non vide quelconque de $\mathbb{N}$. Comme E est non vide, il existe $n \in \mathbb{N}$ tel que $n \in E$. Le fait que $P(n)$ est vraie implique alors que E a un minimum.

□

Remarque 1. *On observera où est intervenue l'hypothèse "non vide". Le théorème 2 est faux si l'on omet cette hypothèse.*

3.3 Principe de récurrence: Variante

On laisse tel que (i) et on remplace (ii) par:
(ii') On fait l'hypothèse que $P(0), P(1), \ldots, P(n)$ sont toutes vraies (hypothèse de récurrence),

et on démontre qu'alors $P(n+1)$ est vraie.

Une autre variante consiste, au lieu de commencer par 0, à commencer par un nombre plus grand, comme dans la preuve de l'énoncé suivant. Rappelons d'abord cette définition.

Définition 8. *Un nombre entier est dit premier s'il est* ≥ 2 *et s'il n'est divisible que par* 1 *et par lui-même. Autrement dit, s'il n'a que deux diviseurs:* 1 *et lui-même.*

Théorème 3. *Tout entier naturel* ≥ 2 *est divisible par un entier naturel premier.*

Démonstration. Nous prenons pour $P(n)$ la propriété "n est divisible par un entier naturel premier.

(i) $P(2)$ est vraie car 2 est premier et se divise par lui-même.

(ii) Supposons que $P(2), P(3), \ldots, P(n)$ sont vraies (hypothèse de récurrence). Démontrons que $P(n+1)$ l'est aussi. Si $n+1$ est premier, $P(n+1)$ est vraie. Par contre, si $n+1$ n'est pas premier, il est divisible par un entier naturel a tel que $2 \leq a \leq n$.

L'hypothèse de récurrence implique alors que $P(a)$ est vraie, i.e. a admet un diviseur premier p: nous pouvons donc écrire $a = pq$, où q est un entier naturel, et enfin que $n+1 = ab = pqb$, ce qui montre que $n+1$ est divisible par p premier. Donc $P(n+1)$ est vraie. □

3.4 Exercices résolus

Démontrer par récurrence les assertions suivantes où n est un entier naturel quelconque.

1. On a toujours
$$0^2 + 1^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

2. On a pour tout n:
$$1 + 2 + 2^2 \ldots + 2^n = 2^{n+1} - 1$$

3. On a également
$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

En effet, pour le premier exercice, on a

$$\begin{aligned} 1^2+\ldots+n^2+(n+1)^2 &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2 \\ &= (n+1)\left(\frac{n(2n+1)}{6}+n+1\right) \\ &= \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)\left((n+1)+1)(2(n+1)+1)\right)}{6}, \end{aligned}$$

qui est la bonne formule avec n remplacé par $n+1$.

Autre preuve: l'identité $(x+1)^3-x^3=3x^2+3x+1$. Posons $x=1,2,\ldots,n$ et sommons:

$$(n+1)^3-1^3=3(1^2+2^2++n^2)+\frac{3n(n+1)}{2}+n.$$

On trouve ensuite: $1^2+2^2+\ldots+n^2$. Pour le deuxième exercice, on écrit

$$1+2+2^2\ldots+2^n+2^{n+1}=2^{n+1}-1+2^{n+1}=2.2^{n+1}-1=2^{(n+1)+1}-1.$$

Enfin, on a:

$$1^3+2^3+\ldots+n^3+(n+1)^3=(1+2+\ldots+n)^2+(n+1)^3.$$

Ainsi, sachant que la somme de tous les entiers de 0 à n vaut $\frac{n(n+1)}{2}$, on écrit

$$\begin{aligned} \left(\frac{n(n+1)}{2}\right)^2+(n+1)^3 &= (n+1)^2\left(\frac{n^2}{4}+n+1\right) \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 \\ &= (1+2+\ldots+n+(n+1))^2. \end{aligned}$$

On peut aussi écrire: $(x+1)^4-x^4=4x^3+6x^2+4x+1$ et sommer de 1 à n.

3.5 Exercices non résolus

Démontrer par récurrence les assertions suivantes pour tout entier naturel n quelconque.

1. $n^3 - n$ est divisible par 3.
2. $2^{2n+1} + 1$ est divisible par 3.
3. $7^n - 3^n$ est divisible par 4.

Chapitre 4

Structure de groupes, anneaux, anneaux intègres, Corps

4.1 Groupes

Définition 9. *Soit E un ensemble. Une loi de composition interne sur E est une fonction $f : E \times E \to E$. On dit aussi une loi de composition ou une opération binaire sur E.*

Définition 10. *Soit M un ensemble muni d'une loi $l : (a, b) \mapsto l(a, b)$. On dit que M est un monoïde si les propriétés suivantes sont satisfaites:*

1. *pour tous a, b, c dans M, on a*

$$l(l(a, b), c) = l(a, l(b, c)).$$

   On dit que la loi de composition l est associative.

2. *Il existe dans M un élément e tel que pour tout élément a dans M, on a*

$$l(a, e) = l(e, a) = a.$$

   On dit que e est un élément neutre de M pour la loi l.

Exemple 5. *Les exercices suivants peuvent être effectués pour vérification.*

1. *Prenons le cas de $M = \mathbb{N}$ et la loi $l(a, b) = a + b$. Il est facile de voir que $\mathbb{N}$ muni de la loi l est un monoïde admettant 0 comme élément neutre.*

2. *Par contre pour* $\mathbb{N}$ *muni de la loi* $l(a,b) = a+b+1$ *n'est pas un monoïde car cette loi n'admet pas d'élément neutre dans* $\mathbb{N}$.

Remarque 2. *Les notations* $l(a,b)$ *sont souvent remplacées par* ab *ou* $a.b$ *qu'on appelle multiplication.*

Définition 11. *Un monoïde est dit commutatif si la loi* l *est commutative, i.e* $l(a,b) = l(b,a)$.

Théorème 4. *Un monoïde a un seul élément neutre*

Démonstration. On suppose que l'unicité existe en deux exemplaires et on montre que ces deux n'en forment en fait qu'un seul. Supposons donc que notre monoïde M ait deux éléments neutres e_1 et e_2, et montrons que $e_1 = e_2$. En utilisant la notation multiplicative, nous avons $e_1 = e_1e_2$ car e_2 est un élément neutre, mais aussi $e_2 = e_1e_2$ car e_1 est un élément neutre. Donc $e_1 = e_2$. Nous dirons donc l'élément neutre d'un monoïde plutôt qu'un élément neutre de M. □

Définition 12. *Soit un monoïde. Un sous-monoïde de* M *est un sous-ensemble* P *de* M *qui contient l'élément neutre de* M *et tel que pour tout* a, b *de* P, *on a* ab.

Théorème 5. *Soit* M *un monoïde de loi* l, *et* P *un sous-monoïde. On définit sur* P *la loi* $k : P \times P \to P$ *telle que tous* $a, b \in P$ *on a* $k(a,b) = l(a,b)$. *Avec la loi* k, P *est un monoïde.*

Démonstration. Remarquons d'abord que k est bien une loi sur P. En effet, P est un sous-monoïde, donc pour tous $a, b \in P, l(a,b) \in P$, donc $k(a,b) \in P$. Maintenant, l'associativité de la loi k résulte de celle de l, pour tout $a, b, c \in P$, on a par définition de k:

$$k(k(a,b),c) \quad \text{et} \quad k(a,k(b,c)).$$

On conclut donc par l'associativité de l. De plus, M a un élément neutre e. Celui-ci est dans P, car P est un sous-monoïde. On a alors

$$\forall a \in P, k(a,e) = l(a,e) = a \quad \text{et} \quad k(k(e,a)) = l(e,a) = a,$$

ce qui montre que P est bien un monoïde. □

Définition 13. *Soit* M *un monoïde noté multiplicativement. On dit que* M *est un groupe si tout élément* $a \in M$ *a un inverse (On dit que* a *est inversible dans* M*), i.e. pour tout* $a \in M, \exists b \in M$ *que* $ab = ba = e$ *où* e *est l'élément neutre de* M.

Théorème 6. *Dans un groupe, l'inverse de chaque élément est unique.*

Démonstration. Soit G ce groupe, e son élément neutre, $a \in G$ et b_1, b_2 des inverses de a. On a donc $b_1 = b_1 e$ car e est l'élément neutre et $b_1 = b_1 e = b_1(ab_2)$ car b_2 est inverse de a et

$$b_1 = b_1 e = (b_1 a) b_2$$

par associativité et encore $b_1 = b_1 e = e b_2$ car b_1 est inverse de a, et $b_1 = b_1 e = b_2$. D'où $b_1 = b_2$. On parlera d'inverse d'un élément dans un groupe. Dans un groupe additif, on dit plutôt opposé. □

Définition 14. *Soit G un groupe multiplicatif d'élément neutre* 1. *Un sous-groupe de G est un sous-ensemble H de G tel que*

1. *l'on a* $1 \in H$;
2. *pour tous* $a, b \in H$, *on a* $ab \in H$;
3. *pour tout* $a \in H, a^{-1} \in H$.

On peut énoncer une définition similaire dans le cas additif (on laisse cet exercice aux étudiants).

Théorème 7. *Soit H un sous-groupe du groupe G. Avec la loi $(a, b) \mapsto ab$, héritée de G, H est un groupe.*

On dit souvent que la loi sur H est induite par celle de G. Les exemples suivants sont donnés sous forme d'exercices. Le lecteur intéressé pourra les faire sans aucune difficulté.

1. Soit G un groupe et H un sous-ensemble de G. On peut montrer que H est un sous-groupe si et seulement si on a les propriétés suivantes:

   (i) H est non vide, et

   (ii) pour tous $a, b \in H$, on a $ab^{-1} \in H$.

   En effet, si H est un sous-groupe alors $e \in H$ implique que H est non vide, i.e (i). Pour (ii) soient $a, b \in H$, on a que $b^{-1} \in H$ et $ab^{-1} \in H$.
   Réciproquement, soit $a \in H$ (car $H \neq \emptyset$). On a $aa^{-1} \in H$. On a $eb^{-1} = b^{-1} \in H$. Soit $a, b \in H$ on a que $a, b^{-1} \in H$ et donc par (ii) , $a.(b^{-1})^{-1} = ab \in H$. Ainsi H est un sous groupe.

2. Sur $\mathbb{Q}$, on définit une loi $*$ par : $a * b = ab + a + b$. Montrer que $\mathbb{Q}$ devient un monoïde, d'élément neutre 0. Montrer que tout élément a un inverse, sauf -1. Montrer que $\mathbb{Q} \setminus \{-1\} = \{x \in \mathbb{Q} : x \neq -1\}$ est un sous-monoïde, qui devient un groupe avec la loi induite. Idée: On utilisera le fait que $ab+a+b+1 = (a+1)(b+1)$. En effet, on peut voir que $0 * b = b = b * 0$ pour tout b, donc 0 est le neutre. Ainsi on a $(-1) * b = -1$ pour tout b. Donc -1 n'a pas d'inverse car $(-1) * b = 0$ (le neutre) est impossible. Notez que la fonction $f : \mathbb{Q} \setminus \{-1\} \to \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ définie par $f(x) = x + 1$ est une bijection telle que

$$f(a * b) = ab + a + b + 1 = (a + 1)(b + 1) = f(a)f(b) \text{ et } \quad f(0) = 1.$$

On note ici que 0 est le neutre pour la loi $*$ dans $\mathbb{Q} \setminus \{-1\}$ et 1 est le neutre pour la multiplication usuelle dans $\mathbb{Q}^*$. C'est aussi un exemple d'isomorphisme de groupes.

4.2 Anneaux

Définition 15. *Soit A un ensemble non vide muni de deux opérations notés " $+$ " et "$.$". Le triplet $(A.+, .)$ est un anneau si:*

- *$(A, +)$ est un groupe commutatif*
- *si la loi "$.$" définie pour tous $x, y \in A$ par $x.y \in A$ est associative, distributive par rapport à l'addition et admet un élément unité, i.e. $\exists e \in A, \forall x \in A, x.e = e.x = x$. L'élément unité e sera noté 1_A.*

Proposition 1. *Soit A un anneau commutatif. Soit $a, b \in A$ et $n \in \mathbb{N} \setminus \{0\}$. Alors on a*

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

La démonstration est laissée aux étudiants comme exercice.

4.3 Sous-anneau

Définition 16. *Soit $(A, +, .)$ un anneau et B un sous-ensemble de A. B est un sous-anneau de A si $(B, +, .)$ est un anneau. Ceci revient à dire*

(*i*) $(B,+)$ *est un sous-groupe de* $(A,+)$, *i.e.* $0_A \in B$ *et pour tous* $x,y \in B$, *on a* $x-y \in B$, *où*

$$x-y = x+(-y).$$

(*ii*) B *est stable pour la multiplication, i.e. pour tous* $x,y \in B$, *on a* $x.y \in B$.

(*iii*) *on a* $1_A \in B$.

Exemple 6. *On peut montrer que* $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$ *est un sous-anneau de* $(\mathbb{C},+,.)$.

4.4 Anneaux intègres

Définition 17. *Soit* A *un anneau non nul.* A *est un anneau intègre si*

$$\forall x,y \in A, x.y = 0 \Rightarrow x = 0 \text{ ou } \quad y = 0.$$

On peut montrer que les ensembles $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ sont des anneaux intègres.

Définition 18. *Soit* A *un anneau non nul et* $a \in A \setminus \{0\}$. *L'élément* a *est un diviseur de zéro s'il existe* $b \in A \setminus \{0\}$ *tel que* $a.b = 0$.

4.5 Corps

Définition 19. *Soit* $(A,+,.)$ *un anneau non nul commutatif et* $a \in A$, a *est inversible pour la multiplication "." s'il existe* a' *tel que* $a'a = 1$. *Si* a' *existe, il est unique et sera noté* a^{-1}. *On note* $A^\times$ *l'ensemble des éléments de* A *inversibles pour la multiplication.*

$$1 \in A^\times \Rightarrow A^\times \neq \emptyset.$$

Exemple 7. *Les ensembles suivants nous donnent les ensembles inversibles de* $\mathbb{Z},\mathbb{Q}$ *et* $\mathbb{R}$ *pour la multiplication respectivement. Il s'agit de:*

- $\mathbb{Z}^\times = \{-1,1\}$,
- $\mathbb{Q}^\times = \mathbb{Q}^*$,
- $\mathbb{R}^\times = \mathbb{R}^*$

Proposition 2. *Soit A un anneau non nul commutatif. Alors $(A^\times, .)$ est un groupe commutatif.*

Démonstration. (i) Soit $a, b \in A^\times$. On doit montrer que $a.b \in A^\times$. On a :

$$(a.b).(a.b)^{-1} = (a.b)(b^{-1}.a^{-1}) = a(b.b^{-1})a^{-1} = a.1.a^{-1} = 1$$

(ii) La multiplication est associative et commutative.

(iii) on a aussi $1 \in A^\times$

(iv) Par définition de $A^\times$, tous les éléments de $A^\times$ sont inversibles.

□

Définition 20. *Soit A un anneau commutatif non nul, A est un corps si $A^\times = A \setminus \{0\}$.*

On peut expliciter cette définition en disant ce qui suit: On appelle corps tout anneau A non nul dans lequel tout élément non nul est inversible.

On dit qu'un corps est commutatif si sa multiplication est commutative. Ainsi pour un corps A on a, $A^\times = A^*$. Si 1 est l'élément unité du groupe multiplicatif $A^\times$, alors 1 est l'élément unité de A. Ainsi un corps possède toujours au moins les deux éléments 0 et 1.

Les notions définies pour les anneaux (intégrité, morphisme, idéal, caractéristique) s'appliquent également aux corps qui sont des anneaux particuliers.

Proposition 3. *Si A est un anneau intègre fini alors A est un corps.*

Démonstration. Soit $a \in A \setminus \{0\}$ (fixé). On considère l'application:

$$\varphi : A \to A : x \mapsto a.x.$$

On montre que φ est injective. Soit $x, x' \in A$ tels que $a.x = a.x'$:

$$a.x = a.x' \Rightarrow a.x - a.x' = 0 \Rightarrow a(x - x') = 0 \Rightarrow x - x' = 0 \Rightarrow x = x'.$$

La condition $x - x' = 0$ montre que $a \neq 0$ et que A est intègre. Comme A est fini, φ est surjective donc il existe $x \in A$ tel que $a.x = 1$. □

4.6 Exercices corrigés

1. Montrer que l'anneau unitaire intègre $(\mathbb{D}, +, \times)$ n'est pas un corps.
2. Montrer que pour tout n non premier, l'espace quotient $(\mathbb{Z}/(n\mathbb{Z}), +, \times)$ n'est pas un corps.

Démonstration. Les réponses à ces questions peuvent être résumées comme suit.

1. Il suffit de voir que $(\mathbb{D}, +, \times)$ est un sous anneau du corps $(\mathbb{Q}, +, \times)$ des nombres rationnels. Ce n'est pas un corps: pour le voir il suffit de voir que 3 est un decimal mais que son inverse 1/3 ne l'est pas (plutôt un réel).
2. Il suffit de montrer par un exemple que tout élément non nul de $\mathbb{Z}/(n\mathbb{Z})$ n'est pas inversible quand n n'est pas premier , c'est a dire qu'on n'a pas l'égalité

$$(\mathbb{Z}/(n\mathbb{Z}))^{\times} = (\mathbb{Z}/(n\mathbb{Z})) \setminus \{\overline{0}\}.$$

□

4.7 Exercices non corrigés

1. Montrer que l'intersection de deux sous-groupes H et K de G est un sous-groupe de G.
2. On munit $\mathbb{R}$ de la loi de composition interne $*$ définie par:

$$\forall x, y \in \mathbb{R}, x * y = \sqrt[3]{x^3 + y^3}.$$

Montrer que l'application $x \mapsto x^3$ est un isomorphisme de $(\mathbb{R}^*, *)$ vers $(\mathbb{R}, +)$. En déduire que $(\mathbb{R}, *)$ est un groupe commutatif.

3. On pose $\mathrm{id} = (1,2,3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$; $c_1 = (2,3,4,1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$;
$\alpha = (3,4,1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$; $c_2 = (4,1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

Calculer

i) $c_1 \circ c_2$,

ii) $c_1 \circ c_1$,

iii) $c_1 \circ \alpha$,

iv) $c_2 \circ \alpha$.

4. Montrer que $\mathcal{U} = \{z \in \mathbb{C} : |z| = 1\}$ muni de la multiplication est un sous-groupe de $(\mathbb{C}^*, \times)$.

5. On considère les applications suivantes, de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même.

$$f_1 : x \mapsto x;\ f_2 : x \mapsto 1-x;\ f_3 : x \mapsto \frac{1}{1-x};\ f_4 = x \mapsto \frac{1}{x};\ f_5 : x \mapsto \frac{x}{x-1};\ f_6 : x \mapsto \frac{x-1}{x}$$

On munit l'ensemble $E = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ de la composition des applications.

i) Écrire la table de composition de $(E, \circ)$,

ii) Montrer que $G = (E, \circ)$ est un groupe,

iii) Déterminer tous les sous groupes de G,

6. Montrer que les ensembles suivants d'applications de $\mathbb{C}$ dans $\mathbb{C}$, munis de la loi de composition des applications, sont des groupes

i) $E_1 = \{z \mapsto z + t, t \in \mathbb{Z}\}$

ii) $E_2 = \{z \mapsto e^{i\theta} z,\ \theta \in \mathbb{R}\}$

iii) $E_3 = \{z \mapsto sz + t,\ (s, t) \in \mathbb{C}^* \times \mathbb{C}\}$

Chapitre 5

Espaces quotients

Une relation d'équivalence consiste à regrouper les éléments d'un ensemble par famille. Nous allons définir des nouveaux espaces appelés "espaces quotients" dont les éléments sont ces familles d'éléments et nous définissons les opérations habituelles sur ces espaces nouvellement définis pour obtenir quelques structures algébriques. Nous allons étudier quelques cas particuliers d'espaces quotients.

5.1 Quotient d'un groupe abélien par un sous-groupe

Soient un groupe abélien $(G, +)$ et H un sous-groupe de G. On rappelle qu'on lira x est congru à y modulo H et on écrit $x \equiv y$ ou xRy. On interprète dans le langage courant comme $x$vaut y à un élément de H près (l'élément en question étant la différence $y - x$, qui est dans H si $x \equiv y$.) On peut également comprendre cela comme suit: x est égal à y modulo un élément de H.

Proposition 4. *Si on définit sur G une relation*

$$x \equiv y \iff y - x \in H,$$

alors cette relation ainsi définie est une relation d'équivalence, appelée, relation de congruence modulo H.

Démonstration. Vérifier que $\equiv$ est une relation d'équivalence est immédiat car H contient le neutre 0, c'est-à-dire, $x - x = 0 \in H$ (réflexivité). On sait également que H est stable par passage à l'opposé, c'est-à-dire, si $y - x \in H$ alors $-(y - x) \in H$ ou bien encore $x - y \in H \iff y \equiv x$, donc la symétrie. Ensuite H est stable par addition, c'est-à-dire,

$$\text{si} \quad x \equiv y \quad \text{et} \quad y \equiv z, \quad \text{on a} \quad (y - x) + (z - y) \in H,$$

ce qui donne, $z - x \in H \Longleftrightarrow x \equiv z$, donc la transitivité. □

On notera $\bar{x}$ la classe d'équivalence de x pour la relation $\equiv$. Nous remarquons directement que

$$y \in \bar{x} \Longleftrightarrow \bar{y} = \bar{x} \Longleftrightarrow y - x \in H \Longleftrightarrow y \in x + H,$$

et l'on note l'ensemble des classes d'équivalences de G comme suit

$$G/\sim := G/H := \{\bar{x}, \quad x \in G\} := \{x + H, \quad x \in G\} := \{x + h, \quad h \in H.\}$$

Exemple 8. *L'exemple simple est celui de $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ où l'on retrouve la congruence modulo n, les classes $\bar{a} = a + n\mathbb{Z}$ et l'ensemble des classes d'équivalences est noté $\mathbb{Z}/_{n\mathbb{Z}}$. Le cas le plus simple est celui de $n = 2$, où on obtient*

$$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$$

et que l'on interprète une classe d'équivalence comme le reste de la division euclidienne par deux.

Maintenant il est question de munir l'ensemble quotient $\mathbb{G}/H$ d'une structure de groupe.

Proposition 5. *L'ensemble quotient $\mathbb{G}/H$ muni de l'addition des classes d'équivalences, c'est-à-dire, le couple $(\mathbb{G}/H, \tilde{+})$ est un groupe appelé groupe quotient.*

Démonstration. On définit sur $\mathbb{G}/H$ une loi $\tilde{+}$ comme suit

$$\bar{x}\tilde{+}\bar{y} = \overline{x + y}.$$

Les deux lois sont notées différemment parce que elles ne s'appliquent pas sur les mêmes objets. Il faut observer que l'associativité dans $\mathbb{G}/H$ découle de celle de G et que le neutre ainsi que l'inverse dans $\mathbb{G}/H$ sont donnés par

$$0_{\mathbb{G}/H} = \overline{0_G} \quad \text{et} \quad \overline{x'} = \overline{-x}.$$

Il suffit de vérifier qu'il existe une classe $\bar{x'}$ telle que

$$\bar{x}\tilde{+}\bar{x'} = \bar{x} = \bar{x'}\tilde{+}\bar{x}.$$

Ce qui donne d'un côté, $\overline{x + x'} = \bar{x}$, ou bien $x + x' + H = x + H$. Ce qui montre bien que $x' = 0$, donc le neutre de l'addition " $+$ " dans G. Ainsi, $\overline{x'}$ étant le neutre dans $\mathbb{G}/H$, alors c'est exactement $\overline{0_G}$. Il en est de même pour l'inverse. □

D'une façon générale, si $*$ est une loi sur un ensemble E non vide muni d'une relation d'équivalence "R", on dit que la relation "R" est compatible avec la loi $*$ si l'écriture suivante

$$\begin{cases} xRx' \\ yRy' \end{cases}$$

entraîne que $(x*y)R(x'*y')$. On peut alors définir une loi $\tilde{*}$ sur le quotient E/R par

$$\bar{x}\tilde{*}\bar{y} = \overline{x*y}$$

et on voit que toutes les propriétés de la loi $*$ (associativité, commutativité,...) sont transportées dans le quotient et sont vérifiées par la nouvelle loi $\tilde{*}$.

5.2 Quotient d'un groupe multiplicatif par un sous-groupe

On considère un groupe multiplicatif $(G,.)$ non nécessairement abélien et H un sous-groupe de G. Par analogie avec le cas abélien, on définit une relation $\equiv$ sur G par

$$x \equiv y \Longleftrightarrow x^{-1}y \in H.$$

De même que le cas abélien, on peut vérifier qu'il s'agit d'une relation d'équivalence.

Ainsi pour la réflexivité, on a pour tout $x \in G, x \equiv x$, car $x^{-1}x = e \in H$ car H est un sous-groupe de G, i.e. il doit contenir l'élément neutre.
Pour la symétrie, pour tous $x \equiv y$, on a $x^{-1}y \in H$ et H est stable par passage à l'inverse, i.e.

$$(x^{-1}y)^{-1} \in H \Longleftrightarrow y^{-1}x \in H \Longleftrightarrow y \equiv x.$$

Enfin, pour la transitivité, pour tous $x \equiv y$ et $y \equiv z$, et grâce à la stabilité de H sous le produit, on a

$$(x^{-1}y)(y^{-1}z) \in H \Longleftrightarrow x^{-1}ez \in H \Longleftrightarrow x^{-1}z \in H \Longleftrightarrow x \equiv z.$$

La classe d'équivalence d'un élément x de G se note $\bar{x}$. Nous remarquons directement que

$$y \in \bar{x} \Longleftrightarrow \bar{y} = \bar{x} \Longleftrightarrow x \equiv y \Longleftrightarrow x^{-1}y \in H \Longleftrightarrow y \in xH.$$

Ainsi, on remarque que

$$\bar{x} = xH := \{xh, \quad h \in H\}.$$

Ainsi on note $\mathbb{G}/H := \{xH, x \in G\}$.

Les éléments xH s'appellent aussi les classes à gauche de H ou les translatés à gauche de H par x. On peut également définir une relation $x \equiv y$ par $xy^{-1} \in H$, auquel cas les classes d'équivalences sont données par $\bar{x} = Hx$ et sont appelées les classes à droite de H ou les translatées à droite de Hpar x. Dans ce cas, on notera

$$H \setminus G := \{Hx, \quad x \in G.\}$$

Nous pouvons munir l'ensemble quotient $\mathbb{G}/H$ d'une structure de groupe.

Proposition 6. *Le couple* $(\mathbb{G}/H, \tilde{.})$ *est un groupe.*

Démonstration. Si on définit sur $\mathbb{G}/H$ un produit donné par

$$\bar{x}\tilde{.}\bar{y} := \overline{x.y},$$

alors il est clair que cette loi est bien définie(i.e.interne et partout définie). Cette loi est associative. En effet, pour tous $\bar{x}, \bar{y}, \bar{z}$ dans $\mathbb{G}/H$, on a

$$\begin{aligned} \bar{x}\tilde{.}(\bar{y}\tilde{.}\bar{z}) &= \bar{x}\tilde{.}\overline{(y.z)} \\ &= \overline{x.(y.z)} \\ &= \overline{(x.y).z} = \overline{(x.y)}\tilde{.}\bar{z} \\ &= (\bar{x}\tilde{.}\bar{y})\tilde{.}\bar{z} \end{aligned}$$

Cette loi admet un élément neutre. En effet, pour tout $\bar{x} \in \mathbb{G}/H$, il existe un élément $\bar{e}$ dans $\mathbb{G}/H$ tel que

$$\bar{x}\tilde{.}\bar{e} = \bar{x} = \bar{e}\tilde{.}\bar{x}.$$

Ainsi, d'une part, on a

$$(xH).(eH) = xH \Longleftrightarrow (xeh) = xh \Longleftrightarrow e = 1_G,$$

et d'autre part, on obtient la même chose. Donc l'élément neutre $1_{\mathbb{G}/H}$ dans $\mathbb{G}/H$ devient alors $1_{\mathbb{G}/H} = \overline{1_G}$.
Pour le symétrique de $\bar{x}$ dans $\mathbb{G}/H$ c'est pareil, on obtient $\overline{x}^{-1} = \overline{x^{-1}}$. En effet, il suffit de résoudre l'équation

$$\bar{x}\tilde{.}\bar{x'} = \overline{1_G} = \bar{x'}\tilde{.}\bar{x}$$

et en utilisant la définition de la loi $\tilde{.}$.

□

5.3 Quotient d'un espace vectoriel par un sous-espace vectoriel

Soient $(E,+,.)$ un espace vectoriel et F un sous-espace vectoriel de E. On définit sur E une relation telle que pour tous $x,y\in E$ on a $x\sim y\Longleftrightarrow x-y\in F$.

Proposition 7. *La relation $\sim$ ainsi définie est une relation d'équivalence sur E.*

Démonstration. La relation " $\sim$ " est reflexive. En effet, pour tout $x\in E$, on a toujours $x\sim x\Longleftrightarrow x-x=0\in F$ car F est un sous-espace vectoriel(il doit contenir 0).
Ensuite, la relation " $\sim$ " est symétrique. Pour tous $x,y\in E$, si $x\sim y$ alors $y\sim x$. En effet, on écrit que $x\sim y\Longleftrightarrow x-y\in F$ par définition. On sait en plus que F est stable par passage à l'opposé, c'est-à-dire, si $x-y\in F$ alors $-(x-y)\in F\Longleftrightarrow y-x\in F$. Or ceci signifie que $y\sim x$.
Enfin, la loi " $\sim$ " est transitive. En effet, pour tous $x,y,z\in E$ si $x\sim y$ et $y\sim z$ alors $x\sim z$. Ainsi, on écrit que $x\sim y\Longleftrightarrow x-y\in F$ et $y\sim z\Longleftrightarrow y-z\in F$. Le sous-espace vectoriel F est stable sous l'addition, c'est-à-dire, on a

$$x-y+y-z\in F\Longleftrightarrow x-z\in F,$$

donc $x\sim z$. □

On définit donc l'ensemble des classes d'équivalences

$$E/\sim:=E/F:=\{\bar{x}=x+F,x\in E\}.$$

On voudrait ensuite vérifier que cet ensemble est muni d'une structure d'espace vectoriel sur $\mathbb{K}$.

Proposition 8. *Si on définit sur E/F l'addition et la multiplication scalaire respectivement comme suit*

$$\bar{x}\tilde{+}\bar{y}:=\overline{x+y}\quad et\quad \lambda\tilde{.}\bar{x}:=\overline{\lambda.x},\forall x,y\in E,\lambda\in\mathbb{K},$$

alors le triplet $(E/F,\tilde{+},\tilde{.})$ devient un espace vectoriel.

Démonstration. L'addition est stable dans E/F, c'est-à-dire, $\bar{x}\tilde{+}\bar{y}=\overline{x+y}$. Puisque $x+y\in E$, il est clair que $\overline{x+y}$ est une classe d'équivalence, donc un élément de E/F. L'addition "$\tilde{+}$" est associative. En effet, il suffit de voir qu'on doit avoir

$$(\bar{x}\tilde{+}\bar{y})\tilde{+}\bar{z}=\bar{x}\tilde{+}(\bar{y}\tilde{+}\bar{z}).$$

La loi $\tilde{+}$ admet un élément neutre dans E/F. En effet, il existe un élément $\bar{e}$ dans E/F tel que $\bar{x}\tilde{+}\bar{e} = \bar{x} = \bar{e}\tilde{+}\bar{x} = \bar{x}$. Ainsi, on écrit en utilisant la définition de l'addition que

$$\overline{x+e} = \bar{x} \Longleftrightarrow x + e = x \Longleftrightarrow e = 0.$$

On voit que e est le neutre dans E. Donc le neutre dans E/F est exactement $\overline{0_E}$. On fait de même pour la recherche d'un élément symétrique pour toute classe d'équivalence $\bar{x}$. Ainsi pour que l'on ait $\bar{x}\tilde{+}\bar{x'} = \overline{0_E} = \bar{x'}\tilde{+}\bar{x}$, on doit voir que $\bar{x'} = \overline{-x}$. De ce qui précède, on en conclut que $(E/F, \tilde{+})$ est un groupe.

Il reste à vérifier les axiomes de distributivité de la multiplication scalaire par rapport à l'addition dans E/F (et vice-versa) et l'associativité mixte. On vérifie ensuite que

1. on doit avoir $\lambda\tilde{.}(\bar{x}\tilde{+}\bar{y}) = \lambda\tilde{.}\bar{x}\tilde{+}\lambda\tilde{.}\bar{y}, \quad \forall \lambda \in \mathbb{K}$.
2. on a également $(\lambda + \beta)\tilde{.}\bar{x} = \lambda\tilde{.}\bar{x}\tilde{+}\beta\tilde{.}\bar{x}, \quad \forall \lambda, \beta \in \mathbb{K}$.
3. et enfin $(\lambda.\beta)\tilde{.}\bar{x} = \lambda(\beta\tilde{.}\bar{x})$.

pour conclure que $(E/F, \tilde{+}, \tilde{.})$ est un espace vectoriel sur $\mathbb{K}$. □

5.4 Quotient d'un anneau par un idéal

Nous rappelons la définition d'un idéal.

Définition 21. *Soit $(A, +, \times)$ un anneau commutatif et I un sous-ensemble de A. I est appelé idéal de A si:*

- *I est un sous-groupe de $(A, +)$.*
- *pour tout $a \in A$, et pour tout $x \in I$, on a $a.x \in I$ et $xa \in I$.*

Nous avons alors trois types d'idéal:

- idéal à droite:si pour tout $x \in I$ et tout $a \in A$ on a $xa \in I$
- idéal à gauche: si pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$
- idéal bilatère: s'il est à la fois idéal à droite et à gauche.

Pour avoir un quotient on doit d'abord définir une relation sur un anneau A comme suit: pour tous $x, y \in A$, $x \sim y \Longleftrightarrow x - y \in I$. Il est facile de voir que cette relation est une relation d'équivalence sur A.

Définition 22. *L'ensemble quotient d'un anneau A par son idéal I suivant la relation d'équivalence " $\sim$ " et noté A/I ou $A/\sim$ est l'ensemble*

$$A/I := \{\bar{x} : x \in A\} := \{x + I, \quad x \in A\}$$

avec $\bar{x}$ la classe d'équivalence de x suivant la relation d'équivalence " $\sim$ ".

Nous pouvons facilement munir l'ensemble A/I d'une structure d'anneau. Ainsi, il suffit de définir sur A/I une addition $\tilde{+}$ par

$$\bar{x}\tilde{+}\bar{y} = \overline{x + y}, \quad \forall x, y \in A$$

et la multiplication $\tilde{\times}$ définie pour tous $x, y \in A$ par

$$\bar{x}\tilde{\times}\bar{y} = \overline{x \times y}.$$

On vérifie ensuite que $(A/I, \tilde{+}, \tilde{\times})$ est un anneau. En effet, il faut montrer que

1. le couple $(A/I, \tilde{+})$ est un groupe abélien,
2. et vérifier les axiomes de la multiplication $\tilde{\times}$, c'est-à-dire,
   - l'associativité de la loi $\tilde{\times}$,
   - l'existence de l'élément neutre pour la loi $\tilde{\times}$,
   - la distributivité de la loi $\tilde{\times}$ par rapport à l'addition $\tilde{+}$.
3. On devra aussi montrer les éléments neutres pour les deux lois sont

$$0_{A/I} = 0_A + I \quad \text{et } 1_{A/I} = 1_A + I.$$

Ainsi, de (1), (2) et (3), on aura montré que $(A/I, \tilde{+}, \tilde{\times})$ est un anneau quotient.

Exercice 1. *Soit $M_n(\mathbb{R})$ l'anneau non commutatif des matrices carrées de taille n à coefficients dans $\mathbb{R}$. On note*

$$I = \{A \in M_n(\mathbb{R}) \text{ à première colonne nulle.}\}$$

Montrer que I est un idéal à droite et non un idéal à gauche.

5.5 Quotient d'une algèbre unitaire par un idéal

Définition 23. *Une algèbre $\mathcal{A}$ est un espace vectoriel sur un corps $\mathbb{K}$ muni d'une loi appelée "multiplication" et notée " $\times$ " qui est bilinéaire. En d'autres termes, de ce qui vient d'être fait sur un anneau, si on rajoute la multiplication scalaire $\lambda.x = \lambda.x$, alors on obtient la structure d'algèbre $(A, +, ., \times)$. On dit que $\mathcal{A}$ est une algèbre sur le corps $\mathbb{K}$.*

Soit $\mathcal{A}$ une algèbre sur un corps $\mathbb{K}$. On peut voir directement que l'on a

- $\mathcal{A}$ est un anneau
- $\mathcal{A}$ est un espace vectoriel sur $\mathbb{K}$ ou tout simplement un $\mathbb{K}$-espace vectoriel.

On dit que ces 2 structures sont compatibles. Cela signifie qu'on a la propriété suivante:

$$\forall \lambda \in \mathbb{K},\ \forall (x, y) \in \mathcal{A}, \lambda(xy) = (\lambda x)y = x(\lambda y).$$

En considérant que l'idéal I de A est bilatère, puisque l'algèbre $\mathcal{A}$ est unitaire (càd, la loi $\times$ admet un élément neutre), alors tout idéal est stable par multiplication scalaire en vertu de l'identité:

$$\lambda.a = (\lambda.1) \times a, \quad \forall a \in I.$$

En utilisant les résultats des paragraphes précédents, on peut conclure, les propriétés d'une algèbre s'obtenant en passant tout sous la barre. Explicitement, le quadruplet $(\mathcal{A}/I, \tilde{+}, \tilde{.}, \tilde{\times})$ est une algèbre.

Pour terminer cette section, on démontre la proposition suivante.

Proposition 9. *Soit I un sous-groupe de $(\mathcal{A}, +)$. Les lois quotients*

$$\begin{cases} \lambda \tilde{.} \bar{x} = \overline{\lambda.\bar{x}} \\ \bar{x} \tilde{\times} \bar{y} = \overline{x \times y} \end{cases}$$

sur $\mathcal{A}/I$ sont bien définies si et seulement si I est un idéal de $\mathcal{A}$ et alors la projection canonique

$$\pi : (\mathcal{A}, +, ., \times) \to (\mathcal{A}/I, \tilde{+}, \tilde{.}, \tilde{\times}) : x \mapsto \bar{x} = x + I$$

est un morphisme d'algèbres.

Démonstration. Il suffit de montrer que les formules suivantes sont satisfaites.

1. $\pi(x + y) = \pi(x) \tilde{+} \pi(y)$,

2. $\pi(\lambda.x) = \lambda\tilde{.}\pi(x)$,
3. $\pi(x \times y) = \pi(x)\tilde{\times}\pi(y)$.

□

On peut alors démontrer le théorème suivant.

Théorème 8. *Soit $n \in \mathbb{N} \setminus \{0, 1\}$. L'ensemble $Z/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Démonstration. ($\Rightarrow$) On suppose que n n'est pas premier alors n s'écrit $n = ab$ avec $a > 1$ et $b > 1$. On a $\bar{a}.\bar{b} = \bar{0}$. On montre que $\bar{a}$ n'est pas inversible. Supposons qu'il existe $\bar{a}^{-1} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a}.\bar{a}^{-1} = 1$, alors:

$$\bar{a}^{-1}.\bar{a}.\bar{b} = \bar{a}^{-1}.\bar{0} = \bar{0} \Rightarrow \bar{b} = \bar{0}.$$

Ce qui est absurde puisque $1 < b < n$. Puisque $\bar{a}$ n'est pas inversible, ceci contredit le fait que $(\mathbb{Z}/n\mathbb{Z})^{\times} = (\mathbb{Z}/n\mathbb{Z}) \setminus \{\bar{0}\}$.
($\Leftarrow$) Soit $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \in (\mathbb{Z}/n\mathbb{Z}) : PGCD(a, n) = 1\}$ Si n est premier, alors pour $a = 1, 2, \ldots, n-1, PGCD(a, n) = 1$. Donc on a

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = (\mathbb{Z}/n\mathbb{Z}) \setminus \{\bar{0}\}.$$

□

5.6 Exercices non corrigées

1. Pour $a, b, c \in \mathbb{R}$, on note

$$M(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

et $E = \{M(a, b, c), a, b, c \in \mathbb{R}\}$. Démontrer que E est une algèbre et en donner une base en tant qu'espace vectoriel. En déduire sa dimension.

2. Soit E l'ensemble des entiers naturels non nuls inférieurs ou égaux à 10. Déterminer l'inverse modulo 11 de tous les éléments de E.

Chapitre 6

Idéaux

Nous savons déjà la définition d'un idéal (voir Définition 21). Notre objectif dans ce chapitre est la description de quelques types d'idéaux. Avant cela, nous démontrons la proposition suivante.

Proposition 10. *Soit A un anneau et I un idéal de A. Alors les assertions suivantes sont équivalentes:*

(*i*) *On a* $I = A$

(*ii*) $1 \in I$

(*iii*) *Il existe* $u \in A^\times, u \in I$

Démonstration. $(i) \Rightarrow (ii)$ évident
$(ii) \Rightarrow (iii)$ évident
$(iii) \Rightarrow (i)$. On doit montrer s'il existe $u \in A^\times$ tel que $u \in I$, alors $I = A$. Soit $a \in A$, montrer que $a \in I$. On a $a = (au^{-1})u \in A$ et I absorbe les éléments de A, $(au^{-1})u \in I$. □

On a une conséquence à cette proposition.

Soit K un corps et I un idéal. On suppose que $I \neq \{0\}$, donc il existe $u \in I$ avec $u \neq 0$. Comme $u \in K \setminus \{0\}$ et K est un corps, alors $u \in K^\times$. Donc I contient un élément inversible et donc $I = K$. Par conséquent, les idéaux d'un corps K sont $\{0\}$ et$K$. Réciproquement, soit A un anneau non nul. On suppose que les seuls idéaux de A sont$\{0\}$ et A. Alors A est un corps. En effet, soit $a \in A \setminus \{0\}$; on montre que $a \in A^\times$.

On considère l'ensemble $I = aA = \{ab, b \in A\}$. On vérifie que I est un idéal de A.

(*i*) $0_A = a0_A$, donc $0_A \in I$.

(*ii*) Soit $x, y \in I$, on pose $x = ab$ avec $b \in A$ et $y = ac$ avec $c \in A$. Alors $x + y = ab + ac = a(b + c) \in I$ car $b + c \in A$.

(*iii*) Soit$x \in I$ et $\alpha \in A$, on montre que $\alpha x \in I$. On pose $x = ab, b \in A$. Alors $\alpha x = \alpha(ab) = a(\alpha b) \in I$, car $\alpha b \in A$.

(*iv*) $a \in I$ puisque $a = a1_A$ et $a \neq 0$ donc $I \neq \{0\}$. Comme I est un idéal non nul de A et les idéaux de A sont $\{0\}$ et A, on déduit que $I = A$. En particulier, $1 \in I$ donc il existe $b \in A$ tel que $1 = ab$ et donc $a \in A^\times$.

6.1 Intersection et réunion d'idéaux

Proposition 11. *Soit $(I_i)_{i\in F}$ une famille d'idéaux d'un anneau A. Alors $\bigcap_{i\in F} I_i$ est un idéal de A.*

Démonstration. Soit $a_i \in \cap_{i\in F} I_i$ et $b \in A$. On sait que $a_i \in I_i$ pour tout $i \in F$. Donc pour tout $i \in F$, on a $a_i \in A$. Ainsi $\cap_{i\in F} I_i \subset A$ est un sous-groupe de A. De plus, on a que $a_i.b \in I_i$ car I_i est un idéal de A pour tout $i \in F$. Puisque $a_i \in \cap_{i\in F} I_i$ alors on voit que $a_i.b \in \cap_{i\in F} I_i$. Donc pour tout $i \in F$, l'ensemble $\cap_{i\in F} I_i$ est un idéal de A. □

Proposition 12. *Soient I et J des idéaux de A. Alors $I \cup J$ est un idéal de A si et seulement si $I \subset J$ ou $J \subset I$.*

Démonstration. ($\Leftarrow$) évident
($\Rightarrow$) $I \cup J$ est un idéal de A, ce qui implique que $I \cup J$ est un sous-groupe de $(A, +)$. Or la réunion des deux sous-groupes n'est un sous-groupe que si l'un des sous-groupes est contenu dans l'autre. □

On peut montrer en exercice que si on a $n, m \in \mathbb{N}$, alors

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(n, m)\mathbb{Z}.$$

Penons les cas de $3\mathbb{Z}$ et $4\mathbb{Z}$: on a donc $3\mathbb{Z} \cap 4\mathbb{Z} = \text{ppcm}(3, 4)\mathbb{Z} = 12\mathbb{Z}$.

6.2 Idéal engendré par une partie

Définition 24. *Soit A un anneau et B une partie non vide de A. L'idéal engendré par B, qu'on note (B) est le plus petit idéal de A qui contient B.*

Explicitement,dans un anneau A, on a

$$(x) := Ax := \langle x \rangle := \{ax | x \in A\},$$

c'est le plus petit idéal qui contient x, on dit qu'il est engendré par x.

Proposition 13. *On a que l'idéal (B) est donné par*

$$(B) = \bigcap_{I \text{ idéal de } A, B \subset I} I.$$

Démonstration. On pose

$$J = \bigcap_{I \text{ idéal de } A, B \subset I} I.$$

On voit que J est un idéal de A qui contient B. Donc $(B) \subset J$. Maintenant, on montre que $J \subset (B)$. Comme J est l'intersection de tous les idéaux qui contiennent B et (B) est un idéal qui contient B, alors $J \subset (B)$. □

Proposition 14. *On a* $(B) = \{a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in B, k \geq 1\}$

Démonstration. On pose $I = \{a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in B, k \geq 1\}$. On montre que I est un idéal qui contient B.

(*i*) $B \neq \emptyset \Rightarrow \exists b \in B$, on a $0_A = 0_A b \in I$.

(*ii*) Soit $x, y \in I$, on montre que $x + y \in I$. On pose:

$$x = a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in B$$

$$y = a'_1b'_1 + \ldots + a'_kb'_k, a'_i \in A, b'_i \in B$$

Alors, on a

$$x + y = a_1b_1 + \ldots + a_kb_k + a'_1b'_1 + \ldots + a'_kb'_k \in I.$$

(*iii*) Soit $x \in I$ et $a \in A$. On montre que $ax \in I$.
On pose $x = a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in B, k \geq 1$: on note

$$ax = a(a_1b_1 + \ldots + a_kb_k) = (aa_1)b_1 + \ldots + (aa_k)b_k \in I$$

car les facteurs aa_1 et aa_k sont des éléments de A.

(*iv*) Soit $b \in B$ alors $b = 1_Ab \in I$. Donc $B \subset I$. Comme I est un idéal de A qui contient B et (B) est le plus petit idéal de A qui contient B, $(B) \subset I$. On montre que $I \subset (B)$. Soit alors $x \in I$, il s'écrit

$$x = a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in B, k \geq 1.$$

Soit $1 \leq i \leq k, b_i \in B$. Comme (B) contient B, $b_i \in (B)$. Or (B) est un idéal donc

$$a_1b_1 + \ldots + a_kb_k \in (B).$$

□

Cas particulier

Soit A un anneau et $x_1, \ldots, x_m \in A$. L'idéal engendré par $x_1, \ldots, x_m$ qu'on note $(x_1, \ldots, x_m)$ est l'idéal engendré par $\{x_1, \ldots, x_m\}$. On a une conséquence:

$$(x_1, \ldots .x_m) = \{a_1x_1 + \ldots + a_nx_n, a_i \in A\} = x_1A + \ldots + x_nA.$$

Exemple 9. *On se place dans* $\mathbb{Z}$.

1. *Soit* $n \in \mathbb{Z}, (n) = n\mathbb{Z}$.

2. *Soit* $n, m \in \mathbb{Z}, (n, m) = \{na + mb, a, b \in \mathbb{Z}\} = PGCD(m, n)\mathbb{Z}$.

6.3 Somme de deux idéaux

Définition 25. *Soit A un anneau, I et J des idéaux de A. La somme des idéaux I et J qu'on note $I + J$ est l'idéal engendré par l'ensemble $I \cup J$ et $I + J = (I, J)$.*

Proposition 15. $I + J = \{i + j, i \in I, j \in J\}$

Démonstration. On a

$$I + J = \{a_1b_1 + \ldots + a_kb_k, a_i \in A, b_i \in I \cup J, k \geq 1\}$$

ou encore

$$I + J = \{a_1i_1 + \ldots + a_ni_n + c_1j_1 + \ldots + c_mj_m, a_l, c_l \in A, i_l \in I, j_l \in J, n, m \geq 1\}$$

Comme I et J sont des idéaux de A, les sommes
$a_1b_1 + \ldots + a_ni_n \in I$ et $c_1j_1 + \ldots + c_mj_m \in J$. Donc $I + J = \{i + j, i \in I, j \in J\}$. □

6.4 Produit d'idéaux

Définition 26. *Soit A un anneau, I et J des idéaux de A. Le produit des idéaux I et J qu'on note IJ est l'idéal engendré par l'ensemble $\{ij, i \in I, j \in J\}$. On note*

$$I.J = \{ij, i \in I, j \in J\}.$$

Prenons dans un anneau $\mathbb{Z}$ les cas suivants:

$$(n) = n\mathbb{Z} \quad \text{et } (m) = m\mathbb{Z}.$$

On sait par définition que le produit de ces deux idéaux devient l'idéal $(nm) = nm\mathbb{Z}$. Par exemple, prenons $n = 3$ et $m = 4$. Déterminer l'idéal produit $(12) = 12\mathbb{Z}$.

On peut donc démontrer la propriété suivante.

Proposition 16. *Si I et J sont des idéaux d'un anneau A, alors on a*

$$IJ = \{i_1j_1 + i_2j_2 + \ldots + i_kj_k, i_l \in I, j_l \in J, k \geq 1.\}$$

Démonstration. On pose $K = IJ = \{i_1j_1 + i_2j_2 + \ldots + i_kj_k, i_l \in I, j_l \in J, k \geq 1.\}$ On peut montrer que K est un idéal de A qui contient $\{ij, i \in I, j \in J\}$. Donc K contient l'ensemble $\{ij, i \in I, j \in J\}$ et IJ est le plus petit idéal qui contient $\{ij, i \in I, j \in J\}$, donc $IJ \in K$.
On montre que $K \subset IJ$. Soit $x \in K$, x s'écrit comme suit

$$x = \{i_1j_1 + i_2j_2 + \ldots + i_kj_k, i_l \in I, j_l \in J.$$

Soit $1 \leq l \leq k, i_lj_l \in \{ij, i \in I, j \in J.\}$ Comme IJ contient $\{ij, i \in I, j \in J\}$ alors on a $i_lj_l \in IJ, \forall l, 1 \leq l \leq k$. Or IJ est un idéal, donc

$$x = \sum_{l=1}^{k} i_lj_l \in IJ.$$

□

Soit A un anneau, I un idéal de A et A/I l'anneau quotient. On donne, dans le paragraphe qui suit les conditions nécessaires et suffisantes sur I pour que l'anneau A/I soit intègre (respectivement un corps).

6.5 Idéal premier

Définition 27. *Soit A un anneau non nul et I un idéal de A. I est un idéal premier de A si les propriétés suivantes sont satisfaites:*

(*i*) $I \subsetneqq A$

(*ii*) *pour tous $a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.*

Proposition 17. *Les idéaux premiers de $\mathbb{Z}$ sont (0) et $p\mathbb{Z}$ où p est un nombre premier de $\mathbb{Z}$.*

Démonstration. (*i*) (0) est un idéal premier car d'une part $(0) = \{0\} \subsetneqq \mathbb{Z}$ et d'autre part, en considérant $a, b \in \mathbb{Z}$ tel que $ab \in (0)$ et comme $\mathbb{Z}$ est un anneau intègre, alors $ab = 0$ implique que $a = 0$ ou $b = 0$, donc $a \in (0)$ ou $b \in (0)$.

(*ii*) Soit p un nombre premier de $\mathbb{Z}$. On montre que (p) est un idéal premier. En effet, on a $(p) \subsetneqq \mathbb{Z}$ d'une part et d'autre part, soit $a, b \in \mathbb{Z}$ tel que $ab \in (p)$. Comme p est premier , $a \in (p)$ ou $b \in (p)$.

(*iii*) Montrons qu'ils sont les seuls idéaux. Soit I un idéal de $\mathbb{Z}$, alors il existe $n \in \mathbb{N}$ tel que $I = (n)$. D'une part, si $n = 0$ alors $I = (0)$ est un idéal premier. D'autre part, supposons que $n \in \mathbb{N}^*$:

$$I = (n), \quad \text{idéal premier } \Rightarrow I \subsetneqq A \Rightarrow n \geq 2.$$

Supposons que n n'est pas premier alors $n = n_1 n_2$ avec $n_1 > 1$ et $n_2 > 1$. Donc on a: $n_1 n_2 \in (n)$ mais $n_1 \in (n)$ et $n_2 \in (n)$. Donc (n) n'est pas un idéal premier.

□

Exemple 10. *Soit $4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ et $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ les idéaux de $\mathbb{Z}$. Pour l'idéal $4\mathbb{Z}$ si on prend les éléments $2, -2 \in \mathbb{Z}$ alors $(2)(-2) = -4 \in 4\mathbb{Z}$ n'implique pas que en aucun cas que $2 \in 4\mathbb{Z}$ ou $-2 \in 4\mathbb{Z}$. Donc $4\mathbb{Z}$ n'est pas premier. Par contre pour $2\mathbb{Z}$ est premier de même pour tous les idéaux $p\mathbb{Z}$ avec p premier.*

On peut alors montrer la proposition suivante.

Proposition 18. *Soit A un anneau non nul et I un idéal de A. Alors A/I est un anneau intègre si et seulement si I est un idéal premier.*

Démonstration. ($\Rightarrow$) A/I est un anneau intègre. Cela implique que A/I est un anneau non nul, ce qui implique que $I \subsetneqq A$. Soit $a, b \in A$ tel que $ab \in I$:

$$ab \in I \Rightarrow ab + I = 0_A + I \Rightarrow (a+I)(b+I) = 0_A + I = 0_{A/I}$$

car $a+I$ et $b+I$ sont tous des éléments de A/I. Comme A/I est intègre, $a+I = 0_A+I$ ou $b+I = 0_A+I$. Donc $a \in I$ ou $b \in I$.
($\Leftarrow$) Le fait que $I \subsetneqq A$ implique que A/I est un anneau non nul. Soit $x, y \in A/I$ tels que $xy = 0_{A/I}$. Si $x, y \in A/I$ alors x et y s'écrivent

$$x = a + I, y = b + I, a, b \in A.$$

Donc

$$xy = (a+I)(b+I) = ab + I = 0_{A/I} = 0_A + I.$$

Donc $ab \in I$. Comme I est premier, $a \in I$ ou $b \in I$. Donc $x = a + I = 0_A + I = 0_{A/I}$ ou $y = b + I = 0_A + I = 0_{A/I}$. □

6.6 Idéal maximal

Définition 28. *Soit A un anneau non nul et I un idéal de A. I est un idéal maximal si les propriétés suivantes sont satisfaites:*

(*i*) $I \subsetneqq A$

(*ii*) *Dès qu'un idéal J contient I, alors $J = I$ ou $J = A$, c'est-à-dire pour tout autre idéal J de A, l'écriture $I \subset J \subset A$ implique que $J = I$ ou $J = A$.*

Comme exemple, on peut montrer que les idéaux maximaux de $\mathbb{Z}$ sont (p) où p est un élément premier de $\mathbb{Z}$.

Exemple 11. *Soit $4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ et $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ les idéaux de $\mathbb{Z}$. L'idéal $4\mathbb{Z}$ est contenu dans l'idéal $2\mathbb{Z}$. Donc il peut pas être maximal. Par contre les idéaux $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, 7, bref les idéaux $p\mathbb{Z}$ avec p premier ne sont contenus que dans l'idéal $\mathbb{Z}$. Donc ces derniers sont des idéaux maximaux.*

On peut démontrer la condition nécessaire et suffisante pour que A/I soit un corps.

Proposition 19. *Soit A un anneau non nul et I un idéal de A. Alors A/I est un corps si et seulement si I est un idéal maximal.*

Démonstration. ($\Rightarrow$). A/I est un corps implique que A/I est un anneau non nul, ce qui implique que $I \subsetneqq A$.
Soit J un idéal de A tel que $I \subset J$. On montre que $J = I$ ou $J = A$. Supposons que $J \neq I$. On montre que $J = A$. L'écriture $I \subsetneqq J$ implique qu'il existe $j \in J$ tel que $j \in J$ et $j \notin I$. L'écriture $j \notin I$ implique que $j + I \neq 0_A + I = 0_{A/I}$. Comme A/I est un corps, il existe $a \in A$ tel que

$$(j + J)(a + I) = 1_A + I.$$

Donc il existe $a \in A$ tel que $ja + I = 1_A + I$. Donc il existe $a \in A$, il existe $i \in I$ tel que $ja = 1 + i$. Comme $j \in J, i \in I \subset J$ et J est un idéal, $1 \in J$, donc $J = A$.
($\Leftarrow$). $I \subsetneqq A$ implique que A/I est un anneau non nul.
Soit $x \in A/I \setminus \{0_{A/I}\}$, on montre qu'il existe $y \in A/I$ tel que $xy = 1_{A/I}$. Comme $x \in A/I \setminus \{0_{A/I}\}$ alors x s'écrit $x = a + I, a \in A$ et $a \notin I$. Comme $a \notin I, I \subsetneqq (a, I) =: J$

$$J = (a, I) = aA + I = (aA \cup I)$$

Comme I est maximal, $aA + I = A$. Donc il existe $b \in A, i \in I$ tel que $1 = ab + i$. Donc $ab + I = 1_A + I$, c'est-à-dire:

$$(a + I)(b + I) = 1_A + I = 1_{A/I} \quad \text{avec } x = a + I, y = b + I.$$

On prend $y = b + I$. On a aussi $xy = 1_{A/I}$. □

Corollaire 1. *Soit A un anneau non nul. Si I est un idéal maximal de A alors I est un idéal premier.*

Démonstration. I maximal implique que A/I est un corps. A/I est un corps implique que A/I est un anneau intègre. A/I est un anneau intègre implique que I est un idéal premier. □

Chapitre 7

Anneaux et Morphismes d'anneaux

On va analyser les applications qui transforment les éléments d'un anneau A en d'autres éléments d'un anneau B.

7.1 Morphismes d'anneaux

Définition 29. *Soit A et B des anneaux et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux si:*

(*i*) *Pour tous $x, y \in A$, $f(x +_A y) = f(x) +_B f(y)$. ($f$ est un morphisme du groupe $(A, +_A)$ dans $(B, +_B)$)*

(*ii*) *Pour tous $x, y \in A, f(x \times_A y) = f(x) \times_B f(y)$*

(*iii*) $f(1_A) = 1_B$

On précise que la notation " $*_M$ " signifie que l'opération " $*$ " s'effectue dans M.

Exemple 12. *Soit A un anneau et I un idéal de A. Soit*

$$s : A \to A/I : a \mapsto a + I.$$

s est un morphisme d'anneaux surjectif. Soit $a, b \in A$, on a

$$s(a + b) = a + b + I = (a + I) + (b + I) = s(a) + s(b).$$

$$s(ab) = ab + I = (a + I).(b + I) = s(a)s(b)$$

$$s(1_A) = 1_A + I = 1_{A/I}$$

On appelle s la surjection canonique (On retrouve la même appellation dans le théorème9 mais notée différemment).

Proposition 20. *Soit $f : A \to B$ un morphisme d'anneaux. Alors:*

(*i*) $f(0_A) = 0_B$ *et pour tout* $x \in A, f(-x) = -f(x)$

(*ii*) $\mathrm{Ker}(f) = \{x \in A, f(x) = 0_B\}$ *est un idéal de* A

(*iii*) $\mathrm{Im}(f) = f(A) = \{f(x), x \in A\}$ *est un sous-anneau de* B.

(*iv*) f *est injective si et seulement si* $\mathrm{Ker}(f) = \{0_A\}$ *et* f *est surjective si et seulement si* $f(A) = B$.

Démonstration. (*i*) Evident

(*ii*) $f(0_A) = 0_B \Rightarrow 0_A \in \mathrm{Ker}(f)$. Soit $x, y \in \mathrm{Ker}(f)$, montrons que $x + y \in \mathrm{Ker}(f)$. On écrit que

$$x \in \mathrm{Ker}(f) \Rightarrow f(x) = 0_B, y \in \mathrm{Ker}(f) \Rightarrow f(y) = 0_B.$$

Comme f est un morphisme, $f(x + y) = f(x) + f(y) = 0_B$. Soit $a \in A, x \in \mathrm{Ker}(f)$, on montre que $ax \in \mathrm{Ker}(f)$:

$$f(ax) = f(a)f(x) = f(x)0_B = 0_B.$$

(*iii*) On écrit que

$$0_B = f(0_A) \Rightarrow 0_B \in f(A), 1_B = f(1_A) \Rightarrow 1_B \in f(A).$$

Soit $x, y \in f(A)$, on montre que $x + y \in f(A)$ et $xy \in f(A)$. On pose $x = f(a)$ et $y = f(b)$ avec $a, b \in A$. On a

$$x + y = f(a) + f(b) = f(a + b) \in f(A) \quad \text{et } xy = f(a)f(b) = f(ab) \in f(A).$$

(*iv*) C'est évident □

7.2 Transfert d'un idéal par un morphisme

Proposition 21. *Soit $f : A \to B$ un morphisme. Alors*

1. *Si J est un idéal de B, alors $f^{-1}(J) = \{x \in A, f(x) \in J\}$ est un idéal de A qui contient* $\mathrm{Ker}(f)$
2. *Si I est un idéal de A, $f(I)$ n'est pas nécessairement un idéal de B. Par contre, si f est surjectif, $f(I)$ est un idéal de B.*
3. *On suppose que f est surjectif. On a une bijection entre les idéaux de A qui contient* $\mathrm{Ker}(f)$ *et les idéaux de B. On pose: $\mathcal{I}_A^*$ =\{les idéaux de A qui contient* $\mathrm{Ker}(f)$\}, $\mathcal{I}_B$ =\{les idéaux de B\} *et une bijection*

$$\varphi : \mathcal{I}_A^* \to \mathcal{I}_B : I \mapsto f(I)$$

Démonstration. 1) soit J un idéal de B. On a $x \in f^{-1}(J)$ ssi $f(x) \in J$.
(i) On a $f(0_A) = 0_B$ et $0_B \in J$, puisque J est un idéal de B. Donc $0_A \in f^{-1}(J)$.
(ii) Soit $x, y \in f^{-1}(J)$, est-il que $x + y \in f^{-1}(J)$?
$x, y \in f^{-1}(J)$ ssi $f(x), f(y) \in J$. Comme f est un morphisme, $f(x + y) = f(x) + f(y)$ et comme $f(x), f(y) \in J$ et J est un idéal alors $f(x + y) \in J$ et donc $x + y \in f^{-1}(J)$.

(iii) Soit $a \in A, x \in f^{-1}(J)$. On montre que $ax \in f^{-1}(J)$. Ainsi $x \in f^{-1}(J)$ implique que $f(x) \in J$. Comme f est un morphisme, cela implique que $f(ax) = f(a)f(x)$. Comme J est un idéal de B, alors $f(a)f(b) \in J$. Donc $ax \in f^{-1}(J)$.
(iv) Montrons que $\mathrm{Ker}(f) \subset f^{-1}(J)$. Soit $x \in \mathrm{Ker}(f)$ alors $f(x) = 0_B \in J$, donc $x \in f^{-1}(J)$.

2) On se sert d'un exemple pour montrer le point deux. Soit $f : \mathbb{Z} \to \mathbb{Q} : k \mapsto k$. Soit $I = 2\mathbb{Z}$ un idéal de $\mathbb{Z}$, $f(I) = I = 2\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$ (tous les idéaux de $\mathbb{Q}$ dont $\{0_\mathbb{Q}\}$ et $\mathbb{Q}$. On suppose que f est surjective. Soit I un idéal de A. On suppose que $f(I)$ est un idéal de B.
(i) On a $0_B = f(0_A)$ et $0_B \in f(I)$.
(ii) Soit $x, y \in f(I)$. On montre que $x + y \in f(I)$:

$$x + y \in f(I) \Rightarrow \exists x', y' \in I, x = f(x') \quad \text{et } y = f(y').$$

Comme f est un morphisme, alors $x + y = f(x' + y')$. Comme I est un idéal, $x' + y' \in I$. Donc $x + y \in f(I)$.

(*iii*) Soient $b \in B$ et $x \in f(I)$. On montre que $bx \in f(I)$. En effet, on a

$$x \in f(I) \Rightarrow \exists x' \in I, x = f(x').$$

Comme f est surjective, il existe $a \in A$ tel que $b = f(a)$. Comme f est un morphisme , $bx = f(ax)$. Comme I est un idéal, $a \in A$ et $x' \in I, ax' \in I$. Donc $bx \in (I)$.
3) On suppose que f est surjective. Soit $\varphi : \mathcal{I}_A^* \to \mathcal{I}_B : I \mapsto f(I)$. On montre que φ est bijective.
(a) Soit $J \in \mathcal{I}_B$ alors $f^{-1}(J) \in \mathcal{I}_A^*$. Comme f est surjective, alors $f(f^{-1}(J) = J$.Donc $J = \varphi(f^{-1}(J))$.
(b) Soient $I, I' \in \mathcal{I}_A^*$ tels que $\varphi(I) = \varphi(I')$.(cela veut dire que $f(I) = f(I')$). On montre que $I = I'$. Soit $i \in I$. Comme $f(I) = f(I')$, il existe $i' \in I$ tel que $f(i) = f(i') \Rightarrow i - i' \in \mathrm{Ker}(f) \subset I'$. Comme $\mathrm{Ker}(f) \subset I'$ et I' est un idéal, alors $i \in I'$. Comme I et I' jouent un même rôle, on a aussi $I' \subset I$. Donc $I = I'$.

□

Corollaire 2. *Soient A un anneau et I un idéal de A. Alors les idéaux de A/I sont J/I où J est un idéal de A qui contient I.*

Démonstration. Soit $s : A \to A/I : a \mapsto a + I$ la surjection canonique. On a $\mathrm{Ker}(s) = \{a \in A, a + I = 0_A + I\} = I$. D'après la proposition 21, un idéal de A/I est $s(I')$ où I' est un idéal de A qui contient I. On a

$$s(I') = \{s(i'), i' \in I\} = \{i' + I, i' \in I'\} = I'/I.$$

□

Exemple 13. *Soit $n \in \mathbb{N}^*$. On cherche les idéaux de $\mathbb{Z}/n\mathbb{Z}$. Soit la surjection canonique*

$$s : \mathbb{Z} \to \mathbb{Z}/(n\mathbb{Z}) : k \mapsto k + n\mathbb{Z}.$$

Soit $I/n\mathbb{Z}$ où I est un idéal de $\mathbb{Z}$ qui contient $n\mathbb{Z}$. On suppose $I = m\mathbb{Z}$ où $m\mathbb{Z} \supset n\mathbb{Z}$ ssi $m|n$. Donc les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont $m\mathbb{Z}/n\mathbb{Z}$ où $m \in \mathbb{Z}$. On prend par exemple $n = 5$. Les idéaux de $\mathbb{Z}/5\mathbb{Z}$ sont $m\mathbb{Z}/5\mathbb{Z}$ tel que $m \in \mathbb{N}, m|5$. Les seuls idéaux de $\mathbb{Z}/5\mathbb{Z}$ sont:

$$\mathbb{Z}/5\mathbb{Z}, 5\mathbb{Z}/5\mathbb{Z} = \{0_{\mathbb{Z}/5\mathbb{Z}}\}.$$

On prend maintenant $n = 6$. Les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont:

$$\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z}, 6\mathbb{Z}/6\mathbb{Z} = \{0_{\mathbb{Z}/6\mathbb{Z}}.\}$$

On montre que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux. Soit $I = m\mathbb{Z}/n\mathbb{Z}$ avec $m, n \in \mathbb{N}$ et $m|n$, un idéal de $\mathbb{Z}/n\mathbb{Z}$.

$m\mathbb{Z}/n\mathbb{Z} = \{mk+n\mathbb{Z}, k \in \mathbb{Z}\} = \{(m+n\mathbb{Z})(k+n\mathbb{Z}), k \in \mathbb{Z}\} = (m+n\mathbb{Z})(\mathbb{Z}/n\mathbb{Z}) = (m+n)\mathbb{Z}$.

7.3 Factorisation d'un morphisme

Rappelons qu'une relation $\mathcal{R}$ sur un ensemble X est une relation d'équivalence si elle est réfléxive (pour tout $x, x\mathcal{R}x$), symétrique (si $x\mathcal{R}y$, alors $y\mathcal{R}x$) et transitive (si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$). L'ensemble des classes d'équivalences de X pour la relation $\mathcal{R}$ est noté $X/\mathcal{R}$.
Soit maintenant A un anneau. On peut alors chercher les relations d'équivalences sur A qui sont compatibles avec la structure d'anneau. On veut ainsi que soit satisfaite la propriété:

$$\text{si} \quad x\mathcal{R}y, x'\mathcal{R}y', \text{alors} \quad (x+x')\mathcal{R}(y+y) \quad \text{et} \quad (xx')\mathcal{R}(yy').$$

Notons alors I la classe d'équivalence de 0. Si $x\mathcal{R}y$, comme $y\mathcal{R}y$, on a donc $(x-y)\mathcal{R}0$, soit $(x-y) \in I$, et réciproquement. Ainsi, $\mathcal{R}$ est définie par $x\mathcal{R}y$ si et seulement si $(x-y) \in I$.
Montrons d'autre part que I est un idéal de A. On a déjà $0 \in I$. De plus, si $x \in I$ et $y \in I$, $x\mathcal{R}0, y\mathcal{R}0$, donc $(x+y)\mathcal{R}0$, ce qui prouve que $(x+y) \in I$. Enfin, si $x \in I$ et $a \in I$, $x\mathcal{R}0$, d'où $ax\mathcal{R}a0$; comme $a0 = 0$, on a bien $ax \in I$.
Réciproquement, les calculs ci-dessus montrent que l'on a le théorème suivant:

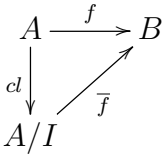
Théorème 9. *Soit A un anneau et soit I un idéal de A. La relation $\mathcal{R}$ sur A définie par $x\mathcal{R}y$ si et seulement si $(x-y) \in I$ est une relation d'équivalence compatible avec la structure d'anneau. L'ensemble quotient $A/\mathcal{R}$ possède une unique structure d'anneau telle que la surjection canonique $cl : A \to A/\mathcal{R}$ est un morphisme d'anneaux. Ce morphisme est surjectif de noyau I.*
L'anneau quotient $A/\mathcal{R}$ est noté A/I. Le morphisme $A \to A/I$ est aussi appelé surjection canonique.

Remarquons aussi que si $\mathbb{K}$ est anneau et $i : \mathbb{K} \to A$ un morphisme d'anneaux, de sorte que (A, i) est une $\mathbb{K}$-algèbre, la composition $cl \circ i : \mathbb{K} \to A/I$ munit A/I d'une (mieux, de l'unique) structure de $\mathbb{K}$-algèbre pour laquelle la surjection canonique est un morphisme de $\mathbb{K}$-algèbres. L'importance de la structure d'anneau quotient vient notamment du théorème de factorisation que nous démontrons maintenant.

Théorème 10. *Soit A et B deux anneaux et soit $f : A \to B$ un homomorphisme d'anneaux. Si I est un idéal de A contenu dans* Ker$f$*, il existe un unique homomorphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ cl$.*

Une façon visuelle et commode d'écrire cette dernière égalité est de dire que le

diagramme



est commutatif. Ici, il faut voir que les éléments de A/I sont notés $cl(a)$ ou tout simplement $a+I$ pour tout élément a de A. Dans la démonstration, nous utilisons la première notation.

Démonstration. Nécessairement,$\overline{f}$ doit être tel que $\overline{f}(cl(a)) = f(a)$ pour tout $a \in A$. Comme tout élément de A/I est de la forme $cl(a)$ pour un certain $a \in A$, cela montre qu'il existe au plus un homomorphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ cl$.
Montrons maintenant l'existence de $\overline{f}$. Soit x un élément de A/I. On sait qu'il existe $a \in A$ tel que $x = cl(a)$. Si a' est un autre représentant de x, donc tel qu'il existe $a \in A$, donc tel que $x = cl(a')$, on a $a - a' \in I$, donc puisque $I \subset \mathrm{Ker}f$, $f(a-a') = 0$ et par conséquent , $f(a) = f(a')$. On peut ainsi poser $\overline{f}(x) = f(a)$. Le résultat est indépendant du représentant a choisi. Il reste à montrer que $\overline{f}$ est un homomorphisme d'anneaux. Comme $cl(0_A) = 0_{A/I}$ et $cl(1_A) = 1_{A/I}$, on a bien $\overline{f}(0_{A/I}) = 0_B$ et $\overline{f}(1_{A/I}) = 1_B$. De plus, si $x = cl(a)$ et $y = cl(b)$ sont deux éléments de A/I, on a $x + y = cl(a+b)$ et

$$\begin{aligned} \overline{f}(x+y) &= \overline{f}(cl(a+b)) = f(a+b) = f(a) + f(b) \\ &= \overline{f}(cl(a)) + \overline{f}(cl(b)) \\ &= \overline{f}(x) + \overline{f}(y) \end{aligned}$$

et, de même,

$$\begin{aligned} \overline{f}(xy) &= f(ab) = f(a)f(b) \\ &= \overline{f}(cl(a))\overline{f}(cl(b)) \\ &= \overline{f}(x)\overline{f}(y). \end{aligned}$$

Il en résulte que $\overline{f}$ est un homomorphisme d'anneaux. Le théorème est ainsi démontré. □

Corollaire 3. *Soit $f : A \to B$ un morphisme d'anneaux. Alors on a*

$$\tilde{f} : A/\mathrm{Ker}(f) \to B : a + \mathrm{Ker}(f) \mapsto f(a)$$

est un morphisme d'anneaux injectif.

Démonstration. Reste à prouver que $\tilde{f}$ est injectif.

$$\begin{aligned}\mathrm{Ker}(\tilde{f}) &= \{a+\mathrm{Ker}(f), \tilde{f}(a+\mathrm{Ker}(f))=0_B\}\\ &= \{a+\mathrm{Ker}(f), f(a)=0_B\}\\ &= \{a+\mathrm{Ker}(f), a\in\mathrm{Ker}(f)\}\\ &= \{0_A+\mathrm{Ker}(f)\}=0_{A/\mathrm{Ker}(\tilde{f})}\end{aligned}$$

□

Remarque 3. *Soit $f : A \to B$ un morphisme d'anneaux. Alors*

$$\tilde{f} : A/\mathrm{Ker}(f) \to f(A) : a+\mathrm{Ker}(f) \mapsto f(a)$$

est un isomorphisme d'anneaux.

Ainsi, on a la définition suivante:

Définition 30. *La factorisation d'un morphisme $f : A \to B$ consiste en la décomposition de f en*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ \downarrow{\scriptstyle cl} & & \uparrow{\scriptstyle i} \\ A/Ker(f) & \xrightarrow{\ \tilde{f}\ } & f(A) \end{array}$$

C'est-à-dire en la composition d'un homomorphisme surjectif cl, d'un isomorphisme $\tilde{f}$ et d'un homomorphisme injectif i.

Soit A un anneau et soit I un idéal de A. On s'intéresse maintenant aux idéaux de l'anneau A/I. Soit $\mathfrak{I}$ un idéal de A/I. Alors, on sait que $cl^{-1}(\mathfrak{I})$ est un idéal de A. Par construction, il contient I puisque pour tout $a \in I$, $cl(a) = 0$ est un élément de $\mathfrak{I}$.

Proposition 22. *Soit $f : A \to B$ un morphisme d'anneaux et soit I un idéal de A contenu dans* $\mathrm{Ker}(f)$. *Soit $\overline{f} : A/I \to B$ l'homomorphisme fourni par le théorème de factorisation. Alors, le noyau de $\overline{f}$ est égal à* $\mathrm{Ker}(f)/I$.

Démonstration. En effet, si $\overline{f}(x) = 0$, soit $a \in A$ tel que $x = cl(a)$. On a alors $f(a) = 0$, d'où $a \in \mathrm{Ker}(f)$ et $x = cl(a) \in cl(\mathrm{Ker}f) = (\mathrm{Ker}f)/I$. Réciproquement, si $x \in (\mathrm{Ker}f)/I$, il existe $a \in \mathrm{Ker}(f)$ tel que $x = cl(a)$. On a alors $\overline{f}(x) = f(a) = 0$ et $x \in \mathrm{Ker}\overline{f}$. □

7.4 Caractéristique d'un anneau

Définition 31. *Soit A un anneau non nul et f le morphisme d'anneaux*

$$f : \mathbb{Z} \to A : k \mapsto k1_A$$

où on a

$$k1_A = \begin{cases} 1_A + \ldots + 1_A, k \text{ fois si } k > 0 \\ 0 \text{ si } k = 0 \\ (-1_A) + \ldots + (-1_A), -k \text{ fois si } k < 0 \end{cases}$$

On a

$$\mathrm{Ker}(f) = \{k \in \mathbb{Z}, k1_A = 0_A\} \in \mathcal{I}_{\mathbb{Z}}.$$

Comme $\mathrm{Ker}(f)$ est un idéal de $\mathbb{Z}$, il existe $n \geq 0$ tel que $\mathrm{Ker}(f) = n\mathbb{Z}$. On appelle n la caractéristique de l'anneau.

- Si $n = 0, \forall k \in \mathbb{Z}, k1_A = 0_A \Rightarrow k = 0$.
- Si $n = 1$ ssi $A = \{0\}$.
- Si $n \geq 2$, n est le plus petit entier supérieur à 1 qui vérifie $n1_A = 0_A$. En effet, soit n_0 le plus petit entier tel que $n_0 1_A = 0_A$. Donc $n_0 \in \mathrm{Ker}(f) = n\mathbb{Z}$ donc $n|n_0 \Rightarrow n_0 = nk, k \in \mathbb{N}$. Or pour que n_0 soit le plus petit entier supérieur à 1, $n_0 = n(n1_A = 0_A)$.

Exemple 14. *1. On cherche*[1] *$Car(\mathbb{Z})$. Soit $k \in \mathbb{Z}$. L'égalité $k.1 = 0 \Rightarrow k = 0$.*

2. On cherche $Car(\mathbb{Z}/5\mathbb{Z})$. Soit $k \in \mathbb{Z}$. On a l'égalité $k.1_{\mathbb{Z}/5\mathbb{Z}} = 0_{\mathbb{Z}/5\mathbb{Z}}$ ssi $k(1+5\mathbb{Z}) = 5\mathbb{Z}$ ssi $k \in 5\mathbb{Z}$ ssi $Car(\mathbb{Z}/5\mathbb{Z}) = 5$.

3. On peut montrer que pour $n \in \mathbb{N}$ alors $Car(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 23. *Soit A un anneau non nul. Alors:*

1. Si $Car(A) = 0$ alors A contient un sous-anneau isomorphe à $\mathbb{Z}$.

2. Si $Car(A) = n > 1$ alors A contient un sous-anneau isomorphe à $\mathbb{Z}/(n\mathbb{Z})$.

[1] Ici $Car(A)$ signifie la caractéristique de A: qui est l'ordre de 1_A dans le groupe additif $(A, +)$

Démonstration. On a le morphisme suivant

$$f : \mathbb{Z} \to A : k \mapsto k1_A.$$

D'après la factorisation canonique de f, on a :

$$\mathbb{Z}/\mathrm{Ker}(f) \simeq f(\mathbb{Z}).$$

1. Si $Car(A) = 0$ alors $\mathbb{Z}/\{0\} \simeq \mathbb{Z} \simeq f(\mathbb{Z})$, comme $f(\mathbb{Z})$ est un sous-anneau de A, A contient un sous-anneau isomorphe à $\mathbb{Z}$.
2. Si $Car(A) = n > 1$ alors $\mathbb{Z}/n\mathbb{Z} \simeq f(\mathbb{Z})$. Donc A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

□

Proposition 24. *Soit A un anneau intègre.*

$$Car(A) = \begin{cases} 0 \\ ou \\ p \text{ nombre premier} \end{cases}$$

En particulier, si A est un corps: on peut donner un exemple ici. Les corps $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0 tandis que le corps $\mathbb{Z}/(3\mathbb{Z})$ est de caractéristique 3.

Démonstration. On suppose que $Car(A) = n > 1$. On a

$$\mathbb{Z}/n\mathbb{Z} \simeq f(\mathbb{Z})$$

où f est donné par

$$f : \mathbb{Z} \to A : k \mapsto k1_A.$$

Comme A est intègre et $f(\mathbb{Z})$ est un sous-anneau de A, $f(\mathbb{Z})$ est intègre, donc $\mathbb{Z}/n\mathbb{Z}$ est intègre et donc n est forcément premier. □

7.5 Exercices corrigés

1. On considère les anneaux quotients suivants $\mathbb{Z}/(6\mathbb{Z})$ et $\mathbb{Z}/(2\mathbb{Z})$. On notera $\bar{l}$ la classe de l'entier l dans $\mathbb{Z}/(6\mathbb{Z})$ et $\hat{l}$ la classe de l'entier l dans $\mathbb{Z}/(2\mathbb{Z})$.

   i) Montrer que l'application $f : \mathbb{Z}/(6\mathbb{Z}) \to \mathbb{Z}/(2\mathbb{Z})$ définie par $f(\bar{l}) = \hat{l}$ est bien définie et que c'est un morphisme surjectif de groupes.

ii) Déterminer le noyau $\ker(f)$ et déterminer sa table de composition

iii) Construire un isomorphisme entre $\ker(f)$ et $\mathbb{Z}/(3\mathbb{Z})$

2. On note A l'ensemble de réels suivant:

$$A = \{m + n\sqrt{6},\ m, n \in \mathbb{Z}\}.$$

i) Montrer que $(A, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

ii) On considère l'application φ de A dans lui-même, qui a $m + n\sqrt{6}$ associe

$$\varphi(m + n\sqrt{6}) = m - n\sqrt{6}.$$

Montrer que φ est un automorphisme de l'anneau $(A, +, \times)$(c'est à dire, une bijection et un morphisme pour chacune des deux lois).

iii) Pour tout $x \in A$, on pose $N(x) = x\varphi(x)$. Montrer que N est une application de A dans $\mathbb{Z}$, qui est un morphisme pour la multiplication.

iv) Démontrer que x est un élément inversible dans A si et seulement si $N(x) = \pm 1$.

v) Vérifier que $5 + 2\sqrt{6}$ est inversible dans A et calculer son inverse.

Démonstration. 1. *i*) Soit $l' \in \bar{l}$, il existe $k \in \mathbb{Z}$ tel que $l' = l + 6k$, donc $l' = l + 2 \times (3k) \equiv l (\text{mod } 2)$. Par conséquent on a $f(\overline{l'}) = \hat{l}$.

Si on change de représentant dans la classe de l dans $\mathbb{Z}/6\mathbb{Z}$, on ne change pas la valeur de $f(\bar{l})$ donc f est bien définie. On notera $+$ l'addition dans $\mathbb{Z}/6\mathbb{Z}$ et dans $\mathbb{Z}/2\mathbb{Z}$ (mais il faut savoir que c'est un abus de notation).

$$f(\overline{l_1} + \overline{l_2}) = \widehat{\overline{l_1 + l_2}} = \hat{l_1} + \hat{l_2} = f(\overline{l_1}) + f(\overline{l_2}).$$

Donc f est bien un morphisme de groupes.
Il reste à montrer que f est surjectif. Dans $\mathbb{Z}/2\mathbb{Z}$, il n'y a que deux classes $\hat{0}$ et $\hat{1}$. Comme $f(\overline{0}) = \hat{0}$ et $f(\overline{1}) = \hat{1}$, ces deux classes ont au moins un antécédent. Il faut en plus constater que

$$f(\overline{2}) = \hat{2} = \hat{0}; f(\overline{3}) = \hat{3} = \hat{1}; f(\overline{4}) = \hat{4} = \hat{0}; f(\overline{5}) = \hat{5} = \hat{1}$$

ii) De la question précédente, on voit que $\ker(f) = \{\overline{0}, \overline{2}, \overline{4}.\}$ Sinon, pour le faire plus généralement, on cherche $\bar{l} \in \mathbb{Z}/6\mathbb{Z}$ tels que

$$f(\bar{l}) = \hat{0} \Longleftrightarrow \hat{l} = \hat{0} \Longleftrightarrow \exists k \in \mathbb{Z}, l = 0 + 2k = 2k \Longleftrightarrow \exists k \in \mathbb{Z}, \bar{l} = \overline{2k}.$$

Dans $\mathbb{Z}/6\mathbb{Z}$ il y a trois classes paires, $\overline{0}, \overline{2}, \overline{4}$. On rappelle que le noyau d'un morphisme est un sous-groupe de l'ensemble de départ.

$+$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

iii) on notera $\dot{l}$ les classes de $\mathbb{Z}/(3\mathbb{Z})$. On définit $\varphi : \ker(f) \to \mathbb{Z}/(3\mathbb{Z})$ par:

$$\varphi(\overline{0}) = \dot{0}; \varphi(\overline{2}) = \dot{1} \quad \text{et } \varphi(\overline{4}) = \dot{2}.$$

Soit d'une manière plus générale $\varphi(\overline{2k}) = \dot{k}$. Comme pour f on doit se demander ce qui se passe si on change de représentant dans $\overline{2k}$, est-ce que l'on retombe bien sur la même classe modulo 3?
Soit $2k' \in \overline{2k}$, il existe $n \in \mathbb{Z}$ tel que $2k' = 2k + 6n$, ce qui entraîne que $k' = k + 3n$ et que par conséquent $\dot{k'} = \dot{k}$. Manifestement φ est une bijection, est-ce un morphisme?

$$\varphi(\overline{2k_1} + \overline{2k_2}) = \varphi(\overline{2k_1 + 2k_2}) = \overline{2k_1 + 2k_2} = \dot{\overline{2k_1}} + \dot{\overline{2k_2}} = \varphi(\overline{2k_1}) + \varphi(\overline{2k_2}).$$

φ est un morphisme.

Une autre méthode simple:
On pouvait dresser une table de composition de $\mathbb{Z}/(3\mathbb{Z})$ et constater qu'elle est identique à celle de $\ker(f)$.

2. *i*) L'ensemble A est non vide. Il suffit donc de vérifier que A est un sous-groupe pour l'addition et que la multiplication est stable. Soient donc $m, n, m', n' \in \mathbb{Z}$. Il suffit de voir que

$$(m + n\sqrt{6}) + (m' + n'\sqrt{6}) = (m + m') + (n + n')\sqrt{6}) \in\in A$$

et

$$(m + n\sqrt{6}) \times (m' + n'\sqrt{6}) = (mm' + 6nn') + (mn' + m'n)\sqrt{6} \in A.$$

ii) Observons d'abord que pour tout élément a de A, $\varphi(\varphi(a)) = a$. Donc φ est une bijection, puisque tout élément de A a pour antécédent $\varphi(a)$. Montrons que φ est un morphisme pour l'addition.

$$\varphi\left((m + n\sqrt{6}) + (m' + n'\sqrt{6})\right) = \varphi\left((m + m') + (n + n')\sqrt{6})\right) = (m+m')-(n+n')\sqrt{6}$$

Ce qui donne encore après un simple arrangement des termes,

$$\varphi\Big((m+n\sqrt{6})+(m'+n'\sqrt{6})\Big)=\varphi(m+n\sqrt{6})+\varphi(m'+n'\sqrt{6}).$$

Montrons enfin que φ est un morphisme pour la multiplication.

$$\begin{aligned}\varphi\Big((m+n\sqrt{6})\times(m'+n'\sqrt{6})\Big) &= \varphi\Big((mm'+6nn')+(mn'+m'n)\sqrt{6}\Big)\\ &= (mm'+6nn')-(mn'+m'n)\sqrt{6}\\ &= (m-n\sqrt{6})\times(m'-n'\sqrt{6})\\ &= \varphi(m+n\sqrt{6})\times\varphi(m'+n'\sqrt{6})\end{aligned}$$

iii) Soit $a=m+n\sqrt{6}$ un élément quelconque de A.

$$N(a)=a\varphi(a)=(m+n\sqrt{6})\times(m-n\sqrt{6})=m^2-6n^2.$$

Donc N est bien une application de A dans $\mathbb{Z}$. Montrons que c'est un morphisme pour la multiplication. Soient a et a' deux éléments de A.

$$N(aa')=aa'\varphi(aa')=aa'\varphi(a)\varphi(a')=(a\varphi(a)(a'\varphi(a')))=N(a)N(a').$$

En utilisant le fait que φ est un morphisme pour la multiplication, on voit bien que N est un morphisme pour la multiplication.

iv) Si $N(x)=xN(x)=1$, alors $\varphi(x)$ est un inverse de x, et si $N(x)=x\varphi(x)=1$ alors $-\varphi(x)$ est un inverse de x: la condition est suffisante. Montrons qu'elle est nécessaire. Soit x un élément inversible de A: il existe y tel que $sy=1$. Mais comme N est un morphisme pour la multiplication, on a $N(x)N(y)=1$. Or $N(x)$ et $N(y)$ sont des entiers. Les seuls éléments de $\mathbb{Z}$ inversibles pour la multiplication sont 1 et -1. D'où le résultat.

v) Il suffit de calculer l'image par N, et d'appliquer le résultat de la question précédente

$$N(5+2\sqrt{6})=25-24=1$$

Donc l'inverse de $5+2\sqrt{6}$ est bien $5-2\sqrt{6}$.

□

7.6 Exercices non corrigés

1. Soit $f : \mathbb{Z} \to \mathbb{Z}/(n\mathbb{Z}) : a \mapsto a(\text{mod } n)$.
   - Montrer que f est un homomorphisme d'anneaux (surjectif en plus).
   - Montrer que le noyau $\ker(f) = n\mathbb{Z}$.
2. Écrire la table de composition d'un groupe à 2 éléments. Vérifier qu'il est isomorphe aux groupes suivants:
   - Le groupe $(\mathbb{Z}/(2\mathbb{Z}), +)$
   - Le groupe $(\{-1, 1\}, \times)$
   - Le groupe $\left(\{x \mapsto x, x \mapsto \frac{1}{x}\}, \circ\right)$
3. Écrire la table de composition d'un groupe à 3 éléments. Vérifier qu'il est isomorphe aux groupes suivants:
   - Le groupe $(\mathbb{Z}/(3\mathbb{Z}), +)$
   - Le groupe $(\{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}, \times)$
   - Le groupe $(\{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}, \circ)$

Chapitre 8

Anneau de polynômes à une indéterminée

Dans ce chapitre, après quelques définitions des concepts de base, nous allons étudier l'arithmétique des polynômes. Il y a une grande analogie entre l'arithmétique des polynômes et celles des entiers. On continue avec un théorème fondamental de l'algèbre:"Tout polynôme de degré n admet n racines complexes". On termine avec les fractions rationnelles: une fraction rationnelle est le quotient de deux polynômes.

8.1 Définitions

Définition 32. *Soit A un anneau, un polynôme à coefficients dans A est une expression de la forme*

$$a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0$$

où $n \in \mathbb{N}, a_i \in A, X$ est une indéterminée.

Un polynôme est nul si tous les coefficients sont nuls. On note $A[X]$ l'ensemble des polynômes à coefficients dans A.

Définition 33. *Soit $P \in A[X]$ non nul. On pose*

$$P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0$$

avec $n \in \mathbb{N}, a_i \in A, a_n \neq 0_A$.

1. *a_n est appelé le coefficient dominant de P*

2. *Le degré de P noté deg(P) est $n \in \mathbb{N}$. Par convention, le degré du polynôme nul est $-\infty$.*

8.2 Opérations sur les polynômes

-Égalité des polynômes: Soient les polynômes suivant

$$P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0, n \in \mathbb{N}, a_i \in \mathbb{K}$$

et

$$Q = b_nX^n + b_{n-1}X^{n-1} + \ldots + b_2X^2 + b_1X + b_0, n \in \mathbb{N}, b_i \in A.$$

On a $P = Q$ ssi $a_i = b_i$ pour tout i.

-Addition: Soient les polynômes suivant

$$P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0, n \in \mathbb{N}, a_i \in \mathbb{K}$$

et

$$Q = b_nX^n + b_{n-1}X^{n-1} + \ldots + b_2X^2 + b_1X + b_0, n \in \mathbb{N}, b_i \in A.$$

La somme de P et Q est donné par

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \ldots + (a_1 + b_1)X + a_0 + b_0.$$

-Multiplication: Si on a

$$P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0, n \in \mathbb{N}, a_i \in A$$

et

$$Q = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_2X^2 + b_1X + b_0, m \in \mathbb{N}, b_i \in A$$

alors le produit PQ est définie par

$$PQ = c_rX^r + c_{r-1}X^{r-1} + \ldots + c_1X + c_0$$

où $r = n + m$ et les coefficients c_r sont donnés par la formule

$$c_k = \sum_{i+j=k} a_ib_j \quad \text{pour } k = \{0, 1, \ldots, r\}.$$

-Multiplication par un scalaire: Si $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0, n \in \mathbb{N}, a_i \in A$ et $\lambda \in A$ alors $\lambda.P$ est le polynôme dont le i-eme coefficient est λa_i.

Proposition 25. *Le triplet $(A[X], +, .)$ est un anneau où les éléments neutres pour l'addition et la multiplication sont respectivement $= 0_{A[X]} = 0X^n + \ldots + 0X + 0$ et $1_{A[X]} = 1_A + 0X^n + \ldots + 0X^1 + 0 \ldots$.*

Proposition 26. *Soit $f : A \to A[X] : a \mapsto 0X^n + \ldots + 0X^2 + 0X + a$. Alors f est un morphisme d'anneaux injectif. Ceci permet d'identifier A comme un sous-anneau de l'anneau $\{aX^0, a \in A\}$.*

8.3 Degré d'un polynôme

Proposition 27. *Soit A un anneau et $P, Q \in A[X]$. Alors:*

(i) $deg(P+Q) \leq max(deg(P), deg(Q))$. De plus, si $deg(P) \neq deg(Q)$ alors:

$$deg(P+Q) = max(deg(P), deg(Q)).$$

(ii) $deg(PQ) \leq deg(P) + deg(Q)$. De plus, si on pose:

$$P = a_n X^n + \ldots + a_1 X + a_0, n \in \mathbb{N}, a_n \neq 0$$

et

$$Q = b_m X^m + \ldots + b_1 X + b_0, m \in \mathbb{N}, b_m \neq 0$$

et si $a_n b_m \neq 0$ alors $deg(PQ) = deg(P) + deg(Q)$. En particulier, si A est intègre:

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

Exemple 15. *On se place dans $\mathbb{Z}/4\mathbb{Z}[X]$. Soit*

$$P = \bar{2}X + \bar{1} = (2 + 4\mathbb{Z})X + (1 + 4\mathbb{Z})$$

et

$$P^2 = \bar{4}X^2 + \bar{4}X + \bar{1} = \bar{1}.$$

Donc $deg(P^2) = 0$.

8.4 Intégrité et éléments inversibles de l'anneau $A[X]$

Proposition 28. *Soit A un anneau intègre. Alors:*

(*i*) $A[X]$ *est intègre*

(*ii*) $(A[X])^\times = A^\times$

Démonstration. (*i*) Soit $P, Q \in A[X]$ tels que $PQ = 0$. On montre que $P = 0$ ou $Q = 0$. On suppose que $P \neq 0$ et $Q \neq 0$. On pose:

$$P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0, a_i \in A, a_n \neq 0$$

$$Q = b_m X^m + a_{m-1}X^{m-1} + \ldots + a_2X^2 + a_1X + a_0, a_i \in A, a_m \neq 0$$

Alors $PQ = a_n b_m X^{n+m} + \ldots + a_0 b_0$. Comme $a_n \neq 0$ et $b_m \neq 0$ et A est intègre, $a_n b_m \neq 0$. Donc $PQ \neq 0$. Ce qui contredit le fait que $PQ = 0$.

(*ii*) On a $A^\times \subset (A[X])^\times$. Soit $P \in (A[X])^\times$ alors il existe $Q \in A[X]$ tel que $PQ = 1_A$. Comme A est intègre, $deg(PQ) = deg(P) + deg(Q)$. Or $PQ = 1$ et $deg(PQ) = 0$. Donc $deg(P) = deg(Q) = 0$. Par conséquent, $P, Q \in A$. Comme $PQ = 1_A, P \in A^\times$.

□

Exemple 16. *Soit $A = \mathbb{Z}/(6\mathbb{Z})$. Alors les polynômes $\overline{3}X - \overline{2}$ et $-\overline{2}X + \overline{3}$ ne sont pas inversibles dans $\mathbb{Z}/(6\mathbb{Z})[X]$ car les termes constants ne sont pas inversibles dans $\mathbb{Z}/(6\mathbb{Z})$.*

Les étudiants sont invités à vérifier comment les coefficients $\overline{3}$ et $-\overline{2}$ de ces polynômes $\overline{3}X - \overline{2}$ et $-\overline{2}X + \overline{3}$ ne sont pas inversibles dans $\mathbb{Z}/(6\mathbb{Z})$.

Exemple 17. *On a que $(\mathbb{Z}[X])^\times = \mathbb{Z}^\times = \{-1, 1\}$*
Si K est un corps, alors $(K[X])^\times = K^\times = K \setminus \{0\}$.

8.5 Arithmétique des polynômes

Il existe de grandes similarités entre l'arithmétique dans $\mathbb{Z}$ et l'arithmétique dans $K[X]$. Cela nous permet d'aller assez vite et d'omettre certaines preuves.

8.5.1 Division euclidienne

Définition 34. *Soient $A, B \in \mathbb{K}[X]$, on dit que B divise A s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B|A$.*

On dit aussi que A est multiple de B ou que A est divisible par B. Outre les propriétés évidentes comme $A|A$ et $A|0$ nous avons:

Proposition 29. *Soient $A, B, C \in \mathbb{K}[X]$.*

1. *Si $A|B$ et $B|A$ alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.*
2. *Si $A|B$ et $B|C$ alors $A|C$.*
3. *Si $C|A$ et $C|B$ alors $A|(AU + BV)$, pour tout $U, V \in \mathbb{K}[X]$.*

Théorème 11. *Soient $A, B \in \mathbb{K}[X]$, avec $B \neq 0$, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que:*

$$A = BQ + R \quad et \deg R < \deg B.$$

Q est appelé le quotient et R est le reste. Cette écriture est la **division euclidienne**.

Notez que la condition $\deg R < \deg B$ signifie $R = 0$ ou bien $0 \leq \deg R < \deg B$. Enfin $R = 0$ si et seulement si $B|A$. On va présenter directement des exemples de division euclidienne.

Exemple 18. *On pose une division de polynômes comme on pose une division euclidienne de deux entiers. Par exemple si $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$. Alors on trouve $Q = 2X^2 + X - 3$ et $R = -X + 2$. On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.*

$$\begin{array}{rrrrr|l}
2X^4 & -X^3 & -2X^2 & +3X & -1 & X^2 -X +1 \\
\cline{6-6}
-2X^4 & +2X^3 & -2X^2 & & & 2X^2 +X -3 \\
\cline{1-3}
 & X^3 & -4X^2 & +3X & -1 & \\
 & -X^3 & +X^2 & -X & & \\
\cline{2-4}
 & & -3X^2 & +2X & -1 & \\
 & & +3X^2 & -3X & +3 & \\
\cline{3-5}
 & & -X & +2 & & \\
\end{array}$$

Exemple 19. *Pour* X^4-3X^3+X+1 *divisé par* X^2+2 *on trouve un quotient égal à* X^2-3X-2 *et un reste égale à* $7X+5$.

$$\begin{array}{rrrr|l}
X^4 & -3X^3 & +X & +1 & X^2 \quad +2 \\
\cline{5-5}
-X^4 & & -2X^2 & & X^2 \ -3X \ -2 \\
\cline{1-3}
 & -3X^3 & -2X^2 & +X+1 & \\
 & -3X^3 & & +6X & \\
\cline{2-4}
 & & -2X^2 & +7X+1 & \\
 & & 2X^2 & \quad +4 & \\
\cline{3-4}
 & & 7X & +5 &
\end{array}$$

8.6 pgcd

Proposition 30. *Soient* $A,B\in K[X]$, *avec* $A\neq 0$ *ou* $B\neq 0$. *Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois* A *et* B.

Cet unique polynôme est appelé le pgcd (plus grand commun diviseur) de A et B que l'on note $\text{pgcd}(A,B)$.

Remarque 4.

- $\text{pgcd}(A,B)$ *est un polynôme unitaire.*
- *Si* $A|B$ *et* $A\neq 0$, *alors* $\text{pgcd}(A,B)=\frac{1}{\lambda}A$, *où* λ *est le coefficient dominant de* A.
- *Pour tout* $\lambda\in\mathbb{K}^*$, $\text{pgcd}(\lambda A,B)=\text{pgcd}(A,B)$.
- *Comme pour les entiers : si* $A=BQ+R$ *alors* $\text{pgcd}(A,B)=\text{pgcd}(B,R)$. *C'est ce qui justifie l'algorithme d'Euclide.*

Algorithme d'Euclide. Soient A et B des polynômes, $B\neq 0$. On calcule les divisions euclidiennes successives,

$$\begin{aligned}
A &= BQ_1+R_1 \quad \deg R_1<\deg B\\
B &= R_1Q_2+R_2 \quad \deg R_2<\deg R_1\\
R_1 &= R_2Q_3+R_3 \quad \deg R_3<\deg R_2\\
&\vdots\\
R_{k-2} &= R_{k-1}Q_k+R_k \quad \deg R_k<\deg R_{k-1}\\
R_{k-1} &= R_kQ_{k+1}
\end{aligned}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd est le dernier reste non nul R_k (rendu unitaire).

Exemple 20. *Calculons le pgcd de* $A = X^4 - 1$ *et* $B = X^3 - 1$. *On applique l'algorithme d'Euclide:*

$$\begin{aligned} X^4 - 1 &= \boxed{(X^3 - 1)} \times X + X - 1 \\ \boxed{X^3 - 1} &= \boxed{(X\text{ -}1)} \times (X^2 + X + 1) + 0 \end{aligned}$$

Le pgcd est le dernier reste non nul, donc $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$.

Exemple 21. *Calculons le pgcd de* $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ *et* $B = X^4 + 2X^3 + X^2 - 4$.

$$\begin{aligned} X^5 + X^4 + 2X^3 + X^2 + X + 2 &= \boxed{(X^4 + 2X^3 + X^2 - 4)} \times (X - 1) + 3X^3 + 2X^2 + 5X - 2 \\ \boxed{X^4 + 2X^3 + X^2 - 4} &= \boxed{(3X^3 + 2X^2 + 5X - 2)} \times \frac{1}{9}(3X + 4) - \frac{14}{9}(X^2 + X + 2) \\ \boxed{3X^3 + 2X^2 + 5X - 2} &= (X^2 + X + 2) \times (3X - 1) + 0 \end{aligned}$$

Ainsi $\text{pgcd}(A, B) = X^2 + X + 2$.

Définition 35. *Soient* $A, B \in \mathbb{K}[X]$. *On dit que* A *et* B *sont premiers entre eux si* $\text{pgcd}(A, B) = 1$.

Pour A, B quelconques on peut se ramener à des polynômes premiers entre eux: si $\text{pgcd}(A, B) = D$ alors A et B s'écrivent: $A = DA'$, $B = DB'$ avec $\text{pgcd}(A', B') = 1$.

8.7 Théorème de Bézout

Le théorème de Bézout fonctionne également sur les polynômes.

Théorème 12. ***Théorème de Bézout.*** *Soient* $A, B \in \mathbb{K}[X]$ *des polynôme avec* $A \neq 0$ *ou* $B \neq 0$. *On note* $D = \text{pgcd}(A, B)$. *Il existe deux polynômes* $U, V \in \mathbb{K}[X]$ *tels que* $AU + BV = D$.

Ce théorème découle de l'algorithme d'Euclide et plus spécialement de sa remontée comme on le voit sur l'exemple suivant.

Exemple 22. *Nous avons calculé* $\text{pgcd}(X^4-1, X^3-1) = X-1$. *Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne :* $X^4-1 = (X^3-1)\times X + X - 1$, *pour en déduire*

$$X - 1 = (X^4-1)\times 1 + (X^3-1)\times(-X).$$

Donc $U = 1$ *et* $V = -X$ *conviennent.*

Exemple 23. *Pour* $A = X^5+X^4+2X^3+X^2+X+2$ *et* $B = X^4+2X^3+X^2-4$ *nous avions trouvé* $D = \text{pgcd}(A,B) = X^2+X+2$. *En partant de l'avant dernière ligne de l'algorithme d'Euclide on a d'abord:* $B = (3X^3+2X^2+5X-2)\times\frac{1}{9}(3X+4) - \frac{14}{9}D$

donc

$$\frac{14}{9}D = B - (3X^3+2X^2+5X-2)\times\frac{1}{9}(3X+4).$$

La ligne au-dessus dans l'algorithme d'Euclide était: $A = B\times(X-1)+3X^3+2X^2+5X-2$. *On substitue le reste pour obtenir :*

$$-\frac{14}{9}D = B - (A - B\times(X-1))\times\frac{1}{9}(3X+4).$$

On en déduit

$$-\frac{14}{9}D = -A\times\frac{1}{9}(3X+4) + B(1+(X-1)\times\frac{1}{9}(3X+4)).$$

Donc en posant $U = \frac{1}{14}(3X+4)$ *et* $V = \frac{9}{14}(1+(X-1)\frac{1}{9}(3X+4)) = -\frac{1}{14}(3X^2+X+5)$, *on a* $AU+BV = D$.

Le corollaire suivant s'appelle aussi le théorème de Bézout.

Corollaire 4. *Soient* A *et* B *deux polynômes.* A *et* B *sont premiers entre eux si et seulement s'il existe deux polynômes* U *et* V *tels que* $AU+BV = 1$.

On a également le corollaire suivant:

Corollaire 5. *Soient* $A, B, C \in \mathbb{K}[X]$ *avec* $A \neq 0$ *ou* $B \neq 0$. *Si* $C|A$ *et* $C|B$ *alors* $C|\text{pgcd}(A,B)$.

Corollaire 6. ***Lemme de Gauss*** *Soient* $A, B, C \in \mathbb{K}[X]$. *Si* $A|BC$ *et* $\text{pgcd}(A,B) = 1$ *alors* $A|C$.

8.8 ppcm

Proposition 31. *Soient $A, B \in K[X]$ des polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $A|M$ et $B|M$.*

Cet unique polynôme est appelé le ppcm (plus petit commun multiple) de A et B qu'on note $\text{ppcm}(A, B)$.

Exemple 24.

$$\text{ppcm}(X(X-2)^2(X^2+1)^4, (X+1)(X-2)^3(X^2+1)^3 = X(X+1)(X-2)^3(X^2+1)^4.$$

De plus le ppcm est aussi le plus petit au sens de la divisibilité:

Proposition 32. *Soient $A, B \in \mathbb{K}[X]$ des polynômes non nuls et $M = \text{ppcm}(A, B)$. Si $C \in \mathbb{K}[X]$ est un polynôme tel que $A|C$ et $B|C$, alors $M|C$.*

8.9 Exercices non corrigés

1. Trouver les diviseurs de $X^4 + 2X^2 + 1$ dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
2. Montrer que $X - 1|X^n - 1$ (pour $n \geq 1$).
3. Calculer les divisions euclidiennes de A par B avec $A = X^4 - 1$, $B = X^3 - 1$. Puis $A = 4X^3 + 2X^2 - X - 5$ et $B = X^2 + X$; $A = X^5 - 2X^4 + 6X^3$ et $B = 2X^3 + 1$.
4. Déterminer le pgcd de $A = X^5+X^3+X^2+1$ et $B = 2X^3+3X^2+2X+3$. Trouver les coefficients de Bézout U, V. Mêmes questions avec $A = X^5 - 1$ et $B = X^4 + X + 1$. Montrer que si $AU + BV = 1$ avec $\deg U < \deg B$ et $\deg V < \deg A$alors les polynômes U, V sont uniques.

8.10 Racine d'un polynôme, factorisation

8.10.1 Racine d'un polynôme

Définition 36. *Soit $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{K}[X]$. Pour un élément $x \in \mathbb{K}$, on note $P(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. On associe ainsi au polynôme P une fonction polynôme (que l'on note encore P)*

$$P : \mathbb{K} \to \mathbb{K}, x \mapsto P(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0.$$

Définition 37. *Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une racine (ou un zero) de P si $P(\alpha) = 0$.*

Proposition 33. *On a*

$$P(\alpha) = 0 \Longleftrightarrow (X - \alpha) \quad \textit{divise } P.$$

Démonstration. Lorsque l'on écrit la division euclidienne de P par $X - \alpha$ on obtient $P = Q.(X - \alpha) + R$ où R est une constante car $\deg R < \deg(X - \alpha) = 1$. Donc

$$P(\alpha) = 0 \Longrightarrow R(\alpha) = 0 \Longleftrightarrow R = 0 \Longleftrightarrow (X - \alpha)|P.$$

□

Définition 38. *Soit $k \in \mathbb{N}^*$. On dit que α est une racine de multiplicité k de P si $(X - \alpha)^k$ divise P alors que $(X - \alpha)^{k+1}$ ne divise pas P. Lorsque $k = 1$ on parle d'une racine simple, lorsque $k = 2$ d'une racine double, etc.*

On dit aussi que α est une racine d'ordre k.

Proposition 34. *Il y a équivalence entre:*

1. *α est une racine de multiplicité k de P.*
2. *Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^k Q$, avec $Q(\alpha) \neq 0$.*
3. *$P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.*

On remarque que:
Par analogie avec la dérivée d'une fonction, si $P(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \in \mathbb{K}[X]$ alors le polynôme $P'(X) = a_1 + 2a_2 X + \ldots + n a_n X^{n-1}$ est le polynôme dérivé de P.

8.10.2 Théorème de d'Alembert-Gauss

Passons à un résultat essentiel de ce chapitre:

Théorème 13. ***(Théorème de d'Alembert-Gauss)*** *Tout polynôme à coefficients complexes de degré $n \geq 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.*

Nous admettons ce théorème.

Exemple 25. *Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2 à coefficients réels:$a, b, c \in \mathbb{R}$ et $a \neq 0$.*

- *Si $\triangle = b^2 - 4ac > 0$ alors P admet 2 racines réelles distinctes $\frac{-b+\sqrt{\triangle}}{2a}$ et $\frac{-b-\sqrt{\triangle}}{2a}$*
- *Si $\triangle < 0$ alors P admet 2 racines complexes distinctes $\frac{-b+i\sqrt{|\triangle|}}{2a}$ et $\frac{-b-i\sqrt{|\triangle|}}{2a}$.*
- *Si $\triangle = 0$ alors P admet une racine réelle double $\frac{-b}{2a}$*

En tenant compte des multiplicités on a donc toujours exactement 2 racines

Exemple 26. *$P(X) = X^n - 1$ admet n racines distinctes.*
Sachant que P est de degré n alors par le théorème de d'Alembert-Gauss on sait qu'il admet n racines comptées avec multiplicité. Il s'agit donc maintenant de montrer que ce sont des racines simples. Supposons –par l'absurde– que $\alpha \in \mathbb{C}$ soit une racine de multiplicité ≥ 2. Alors $P(\alpha) = 0$ et $P'(\alpha) = 0$. Donc $\alpha^n - 1 = 0$ et $n\alpha^{n-1} = 0$. De la seconde égalité on déduit $\alpha = 0$, contradictoire avec la première égalité. Donc toutes les racines sont simples. Ainsi les n racines sont distinctes. (Remarque: sur cet exemple particulier on aurait aussi pu calculer les racines qui sont ici les racines n-ième de l'unité.)

Pour les autres corps que les nombres complexes nous avons le résultat plus faible suivant:

Théorème 14. *Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. Alors P admet au plus n racines dans $\mathbb{K}$.*

Exemple 27. *$P(X) = 3X^3 - 2X^2 + 6X - 4$ considéré comme un polynôme à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, P n'a qu'une seule racine (qui est simple) $\alpha = \frac{2}{3}$ et il se décompose en $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$. Si on considère maintenant P comme un polynôme à coefficients dans $\mathbb{C}$ alors $P(X) = 3(X - \frac{2}{3})(X - i\sqrt{2})(X + i\sqrt{2})$ et admet 3 racines simples.*

8.10.3 Polynômes irréductibles

Définition 39. *Soit $P \in \mathbb{K}[X]$ un polynôme de degré ≥ 1. On dit que P* ***est irréductible*** *si pour tout $Q \in \mathbb{K}[X]$ divisant P, alors soit $Q \in \mathbb{K}^*$, soit il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.*

On remarque que:

- Un polynôme irréductible P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près).
- La notion de polynôme irréductible pour l'arithmétique de $\mathbb{K}[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.
- Dans le cas contraire, on dit que P est réductible ; il existe alors des polynômes A, B de $\mathbb{K}[X]$ tels que $P = AB$, avec $\deg A \geq 1$ et $\deg B \geq 1$.

Exemple 28.

Tous les polynômes de degré 1 *sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.*

$X^2 - 1 = (X - 1)(X + 1) \in \mathbb{R}[X]$ *est réductible.*

$X^2 + 1 = (X - i)(X + i)$ *est réductible dans* $\mathbb{C}[X]$ *mais est irréductible dans* $\mathbb{R}[X]$.

$X^2 - 4 = (X - 2)(X + 2)$ *est réductible dans* $\mathbb{R}[X]$ *mais est irréductible dans* $\mathbb{Q}[X]$.

Nous avons l'équivalent du lemme d'Euclide de $\mathbb{Z}$ pour les polynômes:

Proposition 35. ***(Lemme d'Euclide)*** *Soit* $P \in \mathbb{K}[X]$ *un polynôme irréductible et soient* $A, B \in K[X]$. *Si* $P|AB$ *alors* $P|A$ *ou* $P|B$.

Démonstration. Si P ne divise pas A alors $\text{pgcd}(P, A) = 1$ car P est irréductible. Donc, par le lemme de Gauss, P divise B. □

8.10.4 Théorème de factorisation

Théorème 15. *Tout polynôme non constant* $A \in \mathbb{K}[X]$ *s'écrit comme un produit de polynômes irréductibles unitaires:*

$$A = \lambda P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$$

où $\lambda \in \mathbb{K}^*, r \in \mathbb{N}^*, k_i \in \mathbb{N}^*$ *et les* P_i *sont les polynômes irréductibles distincts. De plus cette décomposition est unique à l'ordre près des facteurs.*

Il s'agit bien sûr de l'analogue de la décomposition d'un nombre en facteurs premiers.

8.10.5 Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème 16. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Donc pour $P \in \mathbb{C}[X]$ de degré $n \geq 0$ la factorisation s'écrit*

$$P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\dots(X-\alpha_r)^{k_r},$$

où $\alpha_1, \dots, \alpha_r$ sont les racines distinctes de P et $k_1, \dots, k_r$ sont leurs multiplicités.

Démonstration. Ce théorème résulte du théorème de d'Alembert-Gauss. □

Théorème 17. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant $\triangle < 0$. Soit $P \in \mathbb{R}[X]$ de degré $n \neq 1$. Alors la factorisation s'écrit*

$$P = \lambda(X-\lambda_1)^{k_1}(X-\alpha_2)^{k_2}(X-\alpha_r)^{k_r}Q_1^{l_1}\dots Q_s^{l_s},$$

où les α_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2: $Q_i = X^2 + \beta_i X + \gamma_i$ avec $\triangle = \beta_i^2 - 4\gamma_i < 0$.

Exemple 29. *$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ alors que sa décomposition dans $\mathbb{C}[X]$ est*

$$P(X) = 2X^4(X-1)^3(X-i)^2(X+i)^2(X-j)(X-j^2)$$

où $j = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$.

Exemple 30. *Soit $P(X) = X^4 + 1$.*

- *Sur $\mathbb{C}$: On peut d'abord décomposer $P(X) = (X^2+i)(X^2-i)$. Les racines de P sont donc les racines carrées complexes de i et $-i$. On rappelle que pour trouver les racines carrées complexes de i et $-i$, on cherche un nombre complexe $z = a+bi$ tel que $z^2 = i$ et $z^2 = -i$ respectivement. Le calcul montre que les racines carrées complexes de i sont $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ et $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ tandis que celles de $-i$ sont $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ et $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$.*
  Ainsi P se factorise dans $\mathbb{C}[X]$:

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

- *Sur $\mathbb{R}$: Pour un polynôme à coefficient réels, si α est une racine alors $\bar{\alpha}$ aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel:*

$$\begin{aligned} P(X) &= \left((X-\frac{\sqrt{2}}{2}(1+i))(X-\frac{\sqrt{2}}{2}(1-i))\right)\left((X+\frac{\sqrt{2}}{2}(1+i))(X+\frac{\sqrt{2}}{2}(1-i))\right) \\ &= \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right), \end{aligned}$$

qui est la factorisation dans $\mathbb{R}[X]$.

8.11 Exercices corrigés

Les exercices corrigés vont nous servir d'exemples dans la résolution des exercices non corrigés qui vont suivre.

1. Trouver le polynôme P de degré inférieur ou égal à 3 tel que:

$$P(0)=1 \quad \text{et } P(1)=0; \quad P(-1)=-2 \text{ et } P(2)=4.$$

2. À quelle condition sur $a,b,c\in\mathbb{R}$ le polynôme X^4+aX^2+bX+c est-il divisible par X^2+X+1?

3. Déterminer les pgcd des polynômes suivants:

   (a) X^3-X^2-X-2 et $X^5-2X^4+X^2-X-2$

   b) $nX^{n+1}-(n+1)X^n+1$ et $X^n-nX+n-1$ $(n\in\mathbb{N}^*)$

4. Calculer le pgcd des polynômes A et B ci-dessous. Trouver des polynômes U et V tels que $AU+BV=D$.

   (a) $A=X^5+3X^4+2X^3-X^2-3X-2$ et $B=X^4+2X^3+2X^2+7X+6$

   (b) $A=X^6-2X^5+2X^4-3X^3+3X^2-2X$ et $B=X^4-2X^3+X^2-X+1$

5. Factoriser dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$ les polynômes suivants:

   (a) X^3-3

(b) $X^{12}-1$

(c) X^6+1

(d) $X^9+X^6+X^3+1$

6. Factoriser les polynômes suivants:

(a) $X^2+(3i-1)X-2-i$

(b) $X^3+(4+i)X^2+(5-2i)X+2-3i$

Démonstration. 1. On cherche P sous la forme $P(X)=aX^3+bX^2+cX+d$, ce qui donne le système linéaire suivant à résoudre:

$$\begin{cases} d=1 \\ a+b+c+d=0 \\ -a+b-c+d=-2 \\ 8a+4b+2c+d=4 \end{cases}$$

Après calculs, on trouve une unique solution: $a=3/2, \quad b=-2, \quad c=-1/2, \quad d=1$, c'est-à-dire,

$$P(X)=\frac{3}{2}X^3-2X^2-\frac{1}{2}X+1.$$

2. La division euclidienne de $A=X^4+aX^2+bX+c$ par $B=X^2+X+1$ donne

$$X^4+aX^2+bX+c=(X^2+X+1)(X^2-X+a)+(b-a+1)X+c-a.$$

Or A est divisible par B si et seulement si le reste $R=(b-a+1)X+c-a$ est le polynôme nul, c'est-à-dire si et seulement si $b-a+1=0$ et $c-a=0$.

3. L'algorithme d'Euclide permet de calculer le pgcd par une suite de divisions euclidiennes.

(a) $X^5-2X^4+X^2-X-2=(X^3-X^2-X-2)(X^2-X)+2X^2-3X-2$ puis $X^3-X^2-X-2=(2X^2-3X-2)(1/2X+1/4)+3/4X-3/2$ puis $2X^2-3X-2=(3/4X-2/3)(8/3X+4/3)$. Le pgcd est le dernier reste non nul, divisé par son coefficient dominant:

$$\text{pgcd}(X^3-X^2-X-2, X^5-2X^4+X^2-X-2)=X-2.$$

(*b*) $nX^{n+1}-(n+1)X^n+1=(X^n-nX+n-1)(nX-(n+1))+n^2(X-1)^2$
Si $n=1$ alors $X^n-nX+n-1=0$ et le pgcd vaut $(X-1)^2$. On constate que 1 est racine de $X^n-nX+n-1$, et on trouve $X^n-nX+n-1=(X-1)(X^{n-1}+X^{n-2}+\ldots+X^2+X-(n-1))$.
Si $n\geq 2$: 1 est racine de $X^{n-1}+X^{n-2}+\ldots+X^2+X-(n-1)$ et on trouve

$$X^{n-1}+X^{n-2}+\ldots+X^2+X-(n-1)=(X-1)(X^{n-2}+2X^{n-3}+\ldots+(n-1)X^2+nX+(n+1)),$$

donc finalement $(X-1)^2$ divise $X^n-nX+n-1$ (on pourrait aussi remarquer que 1 est racine de multiplicité au moins deux de $X^n-nX+n-1$, puisqu'il est racine de ce polynôme et de sa dérivée). Ainsi

$$\text{si } n\geq 2, \text{pgcd}(nX^{n+1}-(n+1)X^n+1, X^n-nX+n-1)=(X-1)^2.$$

4. On va utiliser l'algorithme d'Euclide:

a) $A=X^5+3X^4+2X^3-X^2-3X-2$ et $B=X^4+2X^3+2X^2+7X+6$ donc $A=BQ_1+R_1$ avec $Q_1=X+1, R_1=-2X^3-10X^2-16X-8$
puis $B=R_1Q_2+R_2$ avec $Q_2=-1/2X+3/2$ et $R_2=9X^2+27X+18$
et enfin $R_1=R_2Q_3$ avec $Q_3=-29X-4/9$ Donc $D=X^2+3X+2$, et on obtient

$$9D=B-R_1Q_2=B-(A-BQ_1)Q_2=AQ_2+B(1+Q_1Q_2).$$

$$\begin{cases} U=\frac{1}{9}(-Q_2)=\frac{1}{18}X-\frac{1}{6} \\ V=\frac{1}{9}(1+Q_1Q_2)=-\frac{1}{9}(1+Q_1Q_2)=-\frac{1}{18}X^2+\frac{1}{18}X^2+\frac{1}{9}X+\frac{5}{18} \end{cases}$$

b) On a $A=BQ1+R1$ avec $Q_1=X^2+1, R_1=X^2-X-1$ puis $B=R_1Q_2+R_2$ avec $Q_2=X^2-X+1$ et $R_2=-X+2$ et enfin $R_1=R_2Q_3+R_3$ avec $Q_3=-X-1$ et $R_3=1$ Donc $D=1$, et on obtient

$$\begin{aligned} 1 &= R_1-R_2Q_3=R_1-(B-R_1Q_2)Q_3=R_1(1+Q_2Q_3)-BQ_3 \\ &= (A-BQ_1)(1+Q_2Q_3)-BQ_3 \\ &= A(1+Q_2Q_3)-B(Q_1(1+Q_2Q_3)+Q_3) \end{aligned}$$

soit

$$\begin{cases} U=1+Q_1Q_2=-X^3 \\ V=-Q_1(1+Q_2Q_3)-Q_3=1+X+X^3+X^5 \end{cases}$$

5. On va faire le point a) et c), les autres points se font de la même façon.

   a) $X^3-3=(X-3^{1/3})(X^2+3^{1/3}X+3^{2/3})$ où $X^2+3^{1/3}X+3^{2/3}$ est irréductible sur $\mathbb{R}$. On cherche ses racines complexes pour obtenir la factorisation sur $\mathbb{C}$:

   $$X^3-3=(X-3^{1/3})(X+\frac{1}{2}3^{1/3}-\frac{i}{2}3^{1/3}-\frac{i}{2}3^{5/6})(X+\frac{1}{2}3^{1/3}+\frac{i}{2}3^{\frac{5}{6}}).$$

   c) Pour X^6+1, $z=re^i$ vérifie $z^6=-1$ si et seulement si $r=1$ et $6\theta\equiv\pi[2\pi]$, on obtient donc comme racines complexes les $e^{\frac{i(\pi+2k\pi)}{6};(k=0,\ldots,5)}$. D'où la factorisation dans $\mathbb{C}[X]$:

   $$X^6+1=(X-e^{\frac{i\pi}{6}})(X-e^{\frac{3i\pi}{6}})(X-e^{\frac{5i\pi}{6}})(X-e^{\frac{7i\pi}{6}})(X-e^{\frac{9i\pi}{6}})(X-e^{\frac{11i\pi}{6}}).$$

   Pour obtenir la factorisation dans $\mathbb{R}[X]$, on regroupe les paires de racines complexes conjuguées:

   $$X^6+1=(X^2+1)(X^2-\sqrt{3}X+1)(X^2+\sqrt{3}X+1).$$

6. On va faire seulement a).

   a) Pour $X^2+(3i-1)X-2-i$, on calcule le discriminant

   $$\triangle=(3i-1)^2-4(-2-i)=-2i$$

   et on cherche les racines carrées (complexes!) de $\triangle$: $w=a+ib$ vérifie $w^2=\triangle$ si et seulement si $w=1-i$ ou $w=-1+i$. Les racines du polynômes sont donc

   $$\frac{1}{2}(-(3i-1)\pm(1-i)) \quad \text{et } P(X)=(X+i)(X-1+2i).$$

   b) Cet exercice est laissé aux étudiants

□

8.12 Exercices non corrigés

1. Trouver un polynôme $P(X)\in\mathbb{Z}[X]$ de degré minimal tel que: $\frac{1}{2}$ soit une racine simple, $\sqrt{2}$ double et i soit une racine triple.

2. Montrer cette partie de la proposition 35: $P(\alpha)=0$ et $P'(\alpha)=0\Longleftrightarrow\alpha$ est une racine de multiplicité ≥ 2.

3. Montrer que pour $P \in \mathbb{C}[X]$: P admet une racine de multiplicité $\geq 2 \iff P$ et P' ne sont pas premiers entre eux.

4. Factoriser $P(X) = (2X^2 + X - 2)^2(X^4 - 1)^3$ et $Q(X) = 3(X^2 - 1)^2(X^2 - X + \frac{1}{4})$ dans $\mathbb{C}[X]$. En déduire leur pgcd et leur ppcm. Mêmes questions dans $\mathbb{R}[X]$.

5. Si $\text{pgcd}(A, B) = 1$. montrer que $\text{pgcd}(A + B, A \times B) = 1$.

6. Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C} \setminus \mathbb{R}$ tel que $P(\alpha) = 0$. Vérifier que $P(\bar{\alpha}) = 0$. Montrer que $(X - \alpha)(X - \bar{\alpha})$ est un polynôme irréductible de $\mathbb{R}[X]$ et qu'il divise P dans $\mathbb{R}[X]$.

8.13 Fractions rationnelles

On commence par donner la définition d'une fraction rationnelle des polynômes.

Définition 40. *Une fonction rationnelle à coefficients dans $\mathbb{K}$ est une expression de la forme*

$$F = \frac{P}{Q}$$

où $P, Q \in \mathbb{K}[X]$ sont deux polynômes et $Q \neq 0$.

Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des "éléments simples". Mais les éléments simples sont différents sur $\mathbb{C}$ ou sur $\mathbb{R}$.

8.13.1 Décomposition en éléments simples sur $\mathbb{C}$

Théorème 18. ***Décomposition en éléments simples sur*** $\mathbb{C}$***:*** *Soit $\frac{P}{Q}$ une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $\text{pgcd}(P, Q) = 1$ et $Q = (X - \alpha_1)^{k_1} \dots (X - \alpha_r)^{k_r}$. Alors il existe une et une seule écriture:*

$$\begin{aligned} \frac{P}{Q} &= E + \frac{a_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{a_{1,2}}{(X-\alpha_1)^{k_1-1}} + \dots + \frac{a_{1,k_1}}{(X-\alpha_1)} + \frac{a_{2,1}}{(X-\alpha_1)^{k_2}} \\ &+ \dots + \frac{a_{2,1}}{(X-\alpha_2)^{k_2}} \frac{a_{2,k_2}}{(X-\alpha_2)} + \dots \end{aligned}$$

Le polynôme E s'appelle la partie polynomiale (ou partie entière). Les termes $\frac{a}{(X-\alpha)^i}$ éléments simples sur $\mathbb{C}$.

Exemple 31. • *Verifier que* $\frac{1}{X^2+1} = \frac{a}{X+i} + \frac{b}{X-i}$ *avec* $a = \frac{1}{2}i$, $b = -\frac{1}{2}i$.

- *Verifier que*

$$\frac{X^4 - 8X^2 + 9X - 7}{(X-2)^2(X+3)} = X + 1 + \frac{-1}{(x-2)^2} + \frac{2}{X-2} + \frac{-1}{X+3}.$$

Comment se calcule cette décomposition? En général on commence par déterminer la partie polynomiale. Tout d'abord si $\deg Q > \deg P$ alors $E(X) = 0$. Si $\deg P \geq \deg Q$ alors effectuons la division P par Q: $P = QE + R$ donc $P/Q = E + \frac{R}{Q}$ où $\deg R < \deg Q$. La partie polynomiale est donc le quotient de cette division. Et on s'est ramené au cas d'une fraction. Voyons en détails comment continuer sur un exemple.

Exemple 32. *Décomposons la fraction*

$$P = \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2}.$$

- ***Première étape: partie polynomiale****. On calcule la division euclidienne de P par Q:*

$$P(X) = (X^2 + 1)Q(X) + 2X^2 - 5X + 9.$$

Donc la partie polynomiale est $E(X) = X^2 + 1$ et la fraction s'écrit

$$\frac{P(X)}{Q(X)} = X^2 + 1 + \frac{2X^2 - 5X + 9}{Q(X)}.$$

Notons que pour la fraction $\frac{2X^2-5X+9}{Q(X)}$ le degré du numérateur est strictement plus petit que le degré du dénominateur.

- ***Deuxième étape: factorisation du dénominateur****. Q a pour racine évidente $+1$ (racine double) et -2 (racine simple) et se factorise donc ainsi*

$$Q(X) = (X-1)^2(X+2).$$

- ***Troisième étape: décomposition théorique en éléments simples****. Le théorème de décomposition en éléments simples nous dit qu'il existe une unique décomposition:*

$$\frac{P(X)}{Q(X)} = E(X) + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}.$$

Nous savons que $E(X) = X^2 + 1$, il reste à trouver les nombres a, b, c.

- ***Quatrième étape: détermination des coefficients***. *Voici une première façon de déterminer a, b, c. On récrit la fraction $\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{c}{X+2}$ au même dénominateur et on l'identifie avec $\frac{2X^2-5X+9}{Q(X)}$:*

$$\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{c}{X+2}=\frac{(b+c)X^2+(a+b-2c)X+2a-2b+c}{(X-1)^2(X+2)}$$

qui doit être égale à $\frac{2X^2-5X+9}{(X-1)^2(X+2)}$. On en déduit $b+c=2, a+b-2c=-5$ et $2a-2b+c=9$. Cela conduit à l'unique solution $a=2, b=-1, c=3$.. Donc

$$\frac{P}{Q}=\frac{X^5-2X^3+4X^2-8X+11}{X^3-3X+2}=X^2+1+\frac{2}{(X-1)^2}+\frac{-1}{X-1}+\frac{3}{X+2}.$$

Cette méthode est souvent plus longue.

- ***Quatrième étape (bis): détermination des coefficients***. *Voici une autre méthode plus efficace. Notons $\frac{P'(X)}{Q(X)}=\frac{2X^2-5X+9}{(X-1)^2(X+2)}$ dont la décomposition théorique est:$\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{c}{X+2}$. Pour déterminer a on multiplie la fraction $\frac{P'}{Q}$ par $(X-1)^2$ et on évalue en $x=1$. Tout d'abord en partant de la décomposition théorique on a:*

$$F_1(X)=(X-1)^2\frac{P'(X)}{Q(X)}=a+b(X-1)+c\frac{(X-1)^2}{X+2},\quad donc\, F_1(1)=a.$$

D'autre part,

$$F_1(X)=(X-1)^2\frac{P'(X)}{Q(X)}=(X-1)^2\frac{2X^2-5X+9}{(X-1)^2(X+2)}=\frac{2X^2-5X+9}{X+2},\quad donc\, F_1(1)=2.$$

On en déduit que $a=2$.
On fait le même processus pour déterminer c: on multiplie par $(X+2)$ et on évalue en -2. On calcule

$$F_2(X)=(X+2)\frac{P'(X)}{Q(X)}=(X+2)\frac{2X^2-5X+9}{(X-1)^2(X+2)}=a\frac{X+2}{(X-1)^2}+b\frac{X+2}{X-1}+c$$

de deux façons et lorsque l'on évalue $x=-2$ on obtient d'une part $F_2(-2)=c$ et d'autre part $F_2(-2)=3$. Ainsi on a $c=3$.
Comme les coefficients sont uniques tous les moyens sont bons pour les déterminer. Par exemple lorsque l'on évalue la décomposition théorique $\frac{P'(X)}{Q(X)}=\frac{a}{(X-1)^2}+\frac{b}{X-1}+\frac{c}{X+2}$ en $x=0$, on obtient,

$$\frac{P'(0)}{Q(0}=a-b+\frac{c}{2}.$$

Donc $\frac{9}{2}=a-b+\frac{c}{2}$. Donc $b=a+\frac{c}{2}-\frac{9}{2}=-1$.

8.13.2 Décomposition en éléments simples sur $\mathbb{R}$

Dans cette section, on présentera ce résultat et un exemple pour l'illustrer.

Théorème 19. *Soit $\frac{P}{Q}$ une fraction rationnelle avec $P, Q \in \mathbb{R}[X]$, $\text{pgcd}(P,Q) = 1$. Alors $\frac{P}{Q}$ s'écrit de manière unique comme somme:*

- *d'une partie polynomiale $E(X)$,*
- *d'éléments simples du type $\frac{a}{(X-\alpha)^i}$,*
- *d'éléments simples du type $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$*

Où les $X-\alpha$ et $X^2+\alpha X+\beta$ sont les facteurs irréductibles de $Q(X)$ et les exposants i' sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.

Exemple 33. *Décomposition en éléments simples de*

$$\frac{P(X)}{Q(X)} = \frac{3X^4+5X^3+8X^2+5X+3}{(X^2+X+1)^2(X-1)}.$$

Comme $\deg P < \deg Q$ alors $E(X) = 0$. Le dénominateur est déjà factorisé sur $\mathbb{R}$ car X^2+X+1 est irréductible. La décomposition théorique est donc:

$$\frac{P(X)}{Q(X)} = \frac{aX+b}{(X^2+X+1)^2} + \frac{cX+d}{X^2+X+1} + \frac{e}{X-1}.$$

Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir:

$$\frac{P(X)}{Q(X)} = \frac{2X+1}{(X^2+X+1)^2} + \frac{-1}{X^2+X+1} + \frac{3}{X-1}.$$

8.14 Exercices non corrigés

1. Soit $Q(X) = (X-2)^2(X^2-1)^3(X^2+1)^4$. Pour $P \in \mathbb{R}[X]$ quelle est la forme théorique de la décomposition en éléments simples sur $\mathbb{C}$ de $\frac{P}{Q}$? Et sur $\mathbb{R}$?
2. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$ et $\mathbb{C}$ les fractions

$$\frac{1}{X^2-1}; \quad \frac{X^2+1}{(X^2-1)^2}; \quad \frac{2X^2-X}{(X^2+2)^2}.$$

Chapitre 9

Anneau produit, Anneau et corps des fractions

9.1 Anneau produit

Définition 41. *Soit $A_1, \ldots, A_n$ des anneaux. On définit*

$$A = A_1 \times \ldots \times A_n = \{(x_1, \ldots, x_n), x_i \in A_i\}$$

l'anneau produit.

Dans cet anneau, l'addition est définie par

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 +_{A_1} y_1, \ldots, x_n +_{A_n} y_n)$$

où la notation $x_i +_{A_i} y_i$ signifie que l'addition est effectuée dans l'anneau A_i. La multiplication dans A est définie par

$$(x_1, \ldots, x_n) \times (y_1, \ldots, y_n) = (x_1 \times_{A_1} y_1, \ldots, x_n \times_{A_n} y_n).$$

Proposition 36. *Le triplet $(A, +, .)$ est un anneau (appelé anneau produit) et les éléments neutres de l'addition et de la multiplication sont respectivement $0_A = (0_{A_1}, \ldots, 0_{A_n})$ et $1_A = (1_{A_1}, \ldots, 1_{A_n})$.*

On peut voir aussi que l'anneau produit des éléments inversibles $(A_1 \times \ldots \times A_n)^\times = A_1^\times \times \ldots \times A_n^\times$.

Remarque 5. *L'anneau $A_1 \times \ldots \times A_n$ avec $n > 1$ n'est pas intègre car*

$$(1, 0, \ldots, 0)(0, 1, \ldots, 0) = (0, 0, \ldots, 0).$$

9.2 Anneau des fractions, Corps des fractions

Nous introduisons ensuite, en particulier dans le cas de $n = 2$, deux constructions fondamentales de quotients d'anneaux: Construction de $\mathbb{Q}$ comme espace quotient et sa généralisation: *la localisation.*

9.2.1 Anneau des fractions: Construction de $\mathbb{Q}$

Soit $\mathbb{Z}^* \times \mathbb{Z} = \{(s, a), s \in \mathbb{Z}^*, a \in \mathbb{Z}\}$. Dans $\mathbb{Z}^* \times \mathbb{Z}$, on définit la relation $\mathcal{R}$:

$$(s, a)\mathcal{R}(s', a') \quad \text{si } as' = a's.$$

$\mathcal{R}$ est une relation d'équivalence. On note la classe de (s, a) par a/s ou $\frac{a}{s}$ et on a:

$$\frac{a}{s} = \{(s', a') \in \mathbb{Z}^* \times \mathbb{Z}, as' = a's\}.$$

On note $(\mathbb{Z}^*)^{-1}\mathbb{Z}$ l'ensemble des classes d'équivalence

$$(\mathbb{Z}^*)^{-1}\mathbb{Z} = \{\frac{a}{s}, a \in \mathbb{Z}, s \in \mathbb{Z}^*\}.$$

On définit les opérations suivantes:

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \quad \text{et } \frac{a}{s}.\frac{a'}{s'} = \frac{aa'}{ss'}.$$

On peut vérifier que ces opérations sont bien définies et que le triplet $((\mathbb{Z}^*)^{-1}\mathbb{Z}, +, .)$ est un corps. On a donc $(\mathbb{Z}^*)^{-1}\mathbb{Z} \simeq \mathbb{Q}$.

Généralisation à un anneau quelconque: Localisation

On commence par définir une partie multiplicative d'un anneau.

Définition 42. *Soit A un anneau. Une partie S de A est dite multiplicative si elle vérifie les propriétés:*
$(i) 1 \in S$
(ii) pour tous a et b dans S, on $ab \in S$.

Etant donnés un anneau A et une partie multiplicative S de A, nous allons construire un anneau $S^{-1}A$ et un homomorphisme $i : A \to S^{-1}A$ tel que $i(S)$ est formé d'éléments inversibles dans $S^{-1}A$. Donnons d'abord quelques exemples:

Exemple 34. *a) Si $A = \mathbb{Z}$ et $S = \mathbb{Z} \setminus \{0\}$, alors l'anneau $S^{-1}A$ sera égal à $\mathbb{Q}$ et $i : \mathbb{Z} \to \mathbb{Q}$ est l'injection usuelle.*
b) Si S est formé d'éléments inversibles, alors $S^{-1}A = A$.
c) Si $A = \mathbb{Z}$ et $S = \{1, 10, 100, \cdots\}$, alors $S^{-1}A$ est l'ensemble des nombres décimaux, c'est -à-dire l'ensemble des nombres rationnels qui peuvent s'écrire sous la forme $\frac{a}{10^n}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$.

Ainsi, ce qu'on veut imiter, c'est tout simplement le calcul des fractions que l'on apprend au collège.

Construction

On commence par démontrer l'affirmation suivante.

Proposition 37. *Sur l'ensemble $A \times S$, la relation $\sim$ définie par: $(a, s) \sim (b, t)$ si et seulement s'il existe $u \in S$ tel que $u(at - bs) = 0$ est une relation d'équivalence.*

Démonstration. On peut le voir facilement comme suit:

- pour tout $(a, s) \in A \times S$, puisque $1 \in S$ et $1(as - as) = 0$, $(a, s) \sim (a, s)$. La relation est reflexive;
- si $(a, s) \sim (b, t)$, choisissons $u \in S$ tel que $u(bs - at) = 0$, d'où $(b, t) \sim (a, s)$. La relation est symétrique;
- enfin, si $(a, s) \sim (b, t)$ et $(b, t) \sim (c, u)$, choisissons v et $w \in S$ tels que $v(at - bs) = w(bu - ct) = 0$. Comme

  $$t(au - cs) = u(at - bs) + s(bu - ct), \Rightarrow t(au - cs) = 0$$

  on a $vwt(au - cs) = 0$. Puisque v, w et t appartiennent à S, $vwt \in S$ et $(a, s) \sim (c, u)$. La relation est donc transitive.

Ce qui montre que c'est une relation d'équivalence. □

Définition 43. *On appelle localisation d'un anneau A en S le quotient*

$$S^{-1}A := A \times S/\sim$$

où la relation d'équivalence $\sim$ est définie par la Propsition (37). On désigne par $S^{-1}A$ l'ensemble des classes d'équivalence (on trouve parfois la notation A_S); la classe du couple (a, s) est notée a/s (ou dans certains cas $\frac{a}{s}$). On note $i : A \to S^{-1}A$ l'application qui à $a \in A$ associe la classe $a/1$.

L'ensemble $A\times S$ n'est pas un anneau. En revanche, nous allons montrer que $S^{-1}A$ est bien défini, i.e est muni d'une structure d'anneau de sorte que i soit un homomorphisme d'anneaux. La définition de cette structure d'anneau provient des formules habituelles pour la somme et le produit de fractions. L'élément 1 de $S^{-1}A$ est par définition $1/1$, l'élément 0 est quant à lui $0/1$.

Dans $S^{-1}A$, on définit les opérations d'addition et de multiplication comme suit:

$$(a/s)+(b/t)=(at+bs)/st, \quad (a/s).(b/t)=(ab/st).$$

Vérifions que cette définition a un sens: si $(a,s)\sim(a',s')$, il faut montrer que

$$(at+bs,st)\sim(a't+bs',s't) \quad \text{et } (ab,st)\sim(a'b,s't).$$

On a alors

$$(at+bs)s't-(a't+bs')st=t^2(as'-a's).$$

Choisissons $u\in S$ tel que $u(as'-a's)=0$, il en résulte que

$$u((at+bs)s't-(a't+bs')st)=0$$

et donc $(at+bs,st)\sim(a't+bs',s't)$. De même,

$$u(abs't-a'bst)=ubt(as'-a's)=0$$

et donc $(ab,st)\sim(a'b,st)$. Plus généralement, si $(a,s)\sim(a',s')$ et $(b,t)\sim(b',t')$, on a en répétant ces vérifications (ou en remarquant la commutativité des opérations),

$$(a,s)+(b,t)\sim(a',s')+(b,t)\sim(a',s')+(b',t').$$

La vérification que ces lois confèrent une structure d'anneau à $S^{-1}A$ est un peu longue mais sans surprise et ne sera pas détaillée ici. Par exemple la distributivité de l'addition sur la multiplication se démontre ainsi: si $a/s, b/t$ et c/u sont trois éléments de $S^{-1}A$, alors

$$\frac{a}{s}\left(\frac{b}{t}+\frac{c}{u}\right)=\frac{a(bu+ct)}{stu}=\frac{abu}{stu}+\frac{act}{stu}=\frac{ab}{st}+\frac{ac}{su}=\frac{a}{s}\frac{b}{t}+\frac{a}{s}\frac{c}{u}.$$

Proposition 38. *L'application $i:A\to S^{-1}A$ telle que $i(a)=a/1$ pour tout $a\in A$ est un homomorphisme d'anneaux.*

Démonstration. On sait que $i(0) = 0/1$, $i(1) = 1/1 = 1$, et pour tous a et b, on a

$$i(a+b) = (a+b)/1 = (a+b)/1 = a/1 + b/1 = i(a) + i(b)$$

et

$$i(ab) = ab/1 = (a/1)(b/1) = i(a)i(b).$$

Enfin, si $s \in S$, on a $i(s) = s/1$ et $i(s)(1/s) = s/s = 1$. Donc pour tout $s \in S$, $i(s)$ est inversible dans $S^{-1}A$. □

Exemples de parties multiplicatives

a) Soit A un anneau intègre. La partie $S = A \setminus \{0\}$ est une partie multiplicative de A. L'anneau $S^{-1}A$ est alors un corps, appelé `corps des fractions` A.
En effet, comme A est intègre, $1 \neq 0$ et $1 \in S$. D'autre part, si a et b sont deux éléments non nuls de A, on a par définition $ab \neq 0$. Ainsi, S est une partie multiplicative de A. Un élément de $S^{-1}A$ est de la forme a/s et $s \neq 0$. S'il est nul, il existe un élément $b \in A \setminus \{0\}$ tel que $ab = 0$. Puisque A est intègre, on a alors $a = 0$. En particulier, $1/1 \neq 0$ dans $S^{-1}A$. Si a/s n'est au contraire pas nul, on a $a \neq 0$ et s/a est un élément de $S^{-1}A$ tel que $(a/s)(s/a) = as/as = 1$. Par suite, a/s est inversible. Nous avons donc prouvé que $S^{-1}A$ est un corps.

b) Soit A un anneau et $s \in A$ un élément non nilpotent. Alors, la partie $S = \{1, s, s^2, \cdots\}$ est une partie multiplicative qui ne contient pas zéro et l'anneau localisé $S^{-1}A$ est non nul(voir la remarque 6). On le note en général A_S.

c) Soit $f : A \to B$ un homomorphisme d'anneaux. Si S est une partie multiplicative de A, $f(S)$ est une partie multiplicative de B. Si T est une partie multiplicative de B, alors $f^{-1}(T)$ est une partie multiplicative de A. Lorsque le morphisme est implicite, par exemple lorsque B est explicitement une algèbre, on s'autorisera l'abus d'écriture $S^{-1}B$ pour $T^{-1}B$.

d) Si I est un idéal d'un anneau A, l'ensemble $S = 1 + I$ des éléments $a \in A$ tels que $a - 1 \in I$ est une partie multiplicative. C'est l'image réciproque de la partie multiplicative $\{1\}$ de A/I par la surjection canonique $A \to A/I$.

Remarque 6. *a*) *A quelle condition l'anneau $S^{-1}A$ peut-il être nul? Il résulte de la définition qu'une fraction a/s est nulle dans $S^{-1}A$ si et seulement s'il existe $t \in S$ tel que*

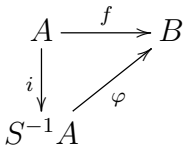
$t(a1-s0) = at = 0$. *Dire que* $S^{-1}A$ *est l'anneau nul signifie alors que* $1/1 = 1 = 0 = 0/1$, *et donc qu'il existe* $s \in S$ *tel que* $s.1 = s = 0$, *autrement dit que* $0 \in S$. *On peut donc affirmer que l'anneau* $S^{-1}A$ *est nul si et seulement si* 0 *appartient à* S. *Cela justifie a posteriori l'interdiction de diviser par zéro: si l'on s'autoriserait cela, les règles du calcul de fractions rendraient toute fraction égale à* 0.

b) La définition de la relation d'équivalence dans la construction de l'anneau localisé peut sembler surprenante puisqu'elle est plus faible que **`l'égalité du produit en croix`** $at = bs$. *Lorsque l'anneau est intègre et* $0 \notin S$, *ou plus généralement lorsque tous les éléments de* S *sont simplifiables, c'est équivalent. En revanche, dans le cas général, l'égalité du produit en croix ne fournirait pas une relation d'équivalence.*

L'importance de cette construction vient de la propriété universelle qu'elle vérifie:

Théorème 20. *Soit* A *un anneau et* S *une partie multiplicative de* A. *Notons* $i : A \to S^{-1}A$ *l'homomorphisme d'anneaux que nous venons de construire. Alors, pour tout anneau* B *et tout homomorphisme* $f : A \to B$ *tel que* $f(S) \subset B^\times$, *il existe un unique homomorphisme* $\varphi : S^{-1}A \to B$ *tel que* $f = \varphi \circ i$.

On peut résumer cette dernière formule en disant que le diagramme



est commutatif.

Démonstration. Si un tel φ existe, il doit vérifier

$$\varphi(a/s)f(s) = \varphi(a/s)\varphi(i(s)) = \varphi(a/s)\varphi(s/1) = \varphi(a/1) = \varphi(i(a)) = f(a)$$

et donc

$$\varphi(a/s) = f(s)^{-1}f(a)$$

où $f(s)^{-1}$ désigne l'inverse de $f(s)$ dans B. Cela prouve qu'il existe en plus un tel homomorphisme φ. Pour montrer son existence, il suffit de vérifier que la formule indiquée définit un homomorphisme $\varphi : S^{-1}A \to B$ tel que $\varphi \circ i = f$. Tout d'abord, si

$(a/s) = (b/t)$, soit $u \in S$ tel que $u(at - bs) = 0$. Alors,

$$\begin{aligned} f(s)^{-1}f(a) &= f(s)^{-1}f(tu)^{-1}f(tu)f(a) \\ &= f(stu)^{-1}f(atu) \\ &= f(stu)^{-1}f(bsu) \\ &= f(t)^{-1}f(b), \end{aligned}$$

ce qui prouve que φ est bien défini. Quant à la vérification des axiomes d'un homomorphisme d'anneaux, on a

$$\varphi(0) = \varphi(0/1) = f(1)^{-1}f(0) = 0 \quad \text{et } \varphi(1) = \varphi(1/1) = f(1)^{-1}f(1) = 1.$$

Puis,

$$\begin{aligned} \varphi(a/s) + \varphi(b/t) &= f(s)^{-1}f(a) + f(t)^{-1}f(b) = f(st)^{-1}(f(at) + f(bs)) \\ &= f(st)^{-1}f(at + bs) = \varphi((at + bs)/st) = \varphi((a/s) + b/t). \end{aligned}$$

Enfin,

$$\begin{aligned} \varphi(a/s)\varphi(b/t) &= f(s)^{-1}f(a)f(t)^{-1}f(b) = f(st)^{-1}f(ab) \\ &= \varphi(ab/st) = \varphi((a/s)(b/t)). \end{aligned}$$

L'application φ est donc un homomorphisme et le théorème est démontré. □

9.2.2 Corps des fractions

Définition 44. *Soit A un anneau intègre et $S = A \setminus \{0\}$. Alors l'anneau $S^{-1}A$ est un corps, appelé le corps des fractions de A et qu'on note* $\mathrm{Fr}(A)$. *Ainsi on a*

$$\mathrm{Fr}(A) = (A \setminus \{0\})^{-1}A.$$

Exemple 35. *1.* $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$

2. On a aussi

$$\mathrm{Fr}(\mathbb{Z}[i]) = \left\{ \frac{a+bi}{c+di}, a, b, c, d \in \mathbb{Z}, (c,d) \neq (0,0) \right\} = \{\alpha + \beta i, \alpha, \beta \in \mathbb{Q}\} := \mathbb{Q}[i].$$

3. L'exemple des polynômes est

$$\mathrm{Fr}(\mathbb{Z}[X]) = \left\{ \frac{P(X)}{Q(X)}, P, Q \in \mathbb{Z}[X], Q \neq 0 \right\} = \left\{ \frac{P(X)}{Q(X)}, P, Q \in \mathbb{Q}[X], Q \neq 0 \right\} := \mathbb{Q}[X].$$

Remarque 7. *Soit A un anneau intègre et* $\mathrm{Fr}(A)$ *le corps des fonctions de A. Soit l'application*

$$i : A \to \mathrm{Fr}(A) : a \mapsto \frac{a}{1}.$$

On a que i est un morphisme d'anneau injectif. A s'identifie donc à un sous-anneau du corps des fractions de A. Tout anneau intègre est un sous-anneau du corps des fractions.

Chapitre 10

Arithmétique dans un anneau

Motivation: L'arithmétique est au cœur du cryptage des communications. Pour crypter un message on commence par le transformer en un - ou plusieurs- nombres. Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

- On choisit deux nombres premiers p et q que l'on garde secrets et on pose $n = p \times q$. Le principe étant que même connaissant n il est très difficile de retrouver p et q (qui sont des nombres ayant des centaines de chiffres).
- La clé secrète et la clé publique se calculent à l'aide de l'algorithme d'Euclide et des coefficients de Bézout.
- Les calculs de cryptage se feront modulo n.
- Le décodage fonctionne grâce à une variante du petit théorème de Fermat.

10.1 Division euclidienne et le pgcd

Définition 45. *Soient $a, b \in \mathbb{Z}$. On dit que b divise a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que*

$$a = bq.$$

Exemple 36.

- $7|21, 6|48$, *a est pair si et seulement si $2|a$.*
- *Pour tout $a \in \mathbb{Z}$, on a $a|0$ et aussi $1|a$.*
- *$a|b$ et $b|a \Longrightarrow b = \pm a$*

- $a|b$ *et* $b|c \Longrightarrow a|c$
- $a|b$ *et* $a|c \Longrightarrow a|b+c$.
- *Si* $a|1$ *alors* $a=+1$ *ou* $a=-1$.

Théorème 21. *Soit* $a \in \mathbb{Z}$ *et* $b \in \mathbb{N} \setminus \{0\}$. *Il existe des entiers* $q, r \in \mathbb{Z}$ *tels que*

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

De plus q *et* r *sont uniques*

Nous avons donc l'équivalence: $r = 0$ si et seulement si b divise a.

Exemple 37. *Pour calculer* q *et* r *on pose la division classique. Prenons le cas d'un polynôme. On obtient* $0 \leq 1 < x - 1$ *(sinon c'est que l'on n'a pas assez loin dans les calculs)*

$$\begin{array}{rrrr|l}
x^3 & +x^2 & & -1 & x \quad -1 \\
\cline{5-5}
-x^3 & +x^2 & & & x^2 +2x +2 \\
\cline{1-2}
 & 2x^2 & & & \\
 & -2x^2 & +2x & & \\
\cline{2-3}
 & & 2x & -1 & \\
 & & -2x & +2 & \\
\cline{3-4}
 & & & +1 &
\end{array}$$

ou tout simplement

$$\begin{array}{r|l}
\textit{dividende} & \textit{diviseur} \\
\hline
 & \\
 & \textit{quotient} \\
\vdots & \\
\hline
\textit{reste} &
\end{array}$$

10.1.1 pgcd de deux entiers

Définition 46. *Soient $a, b \in \mathbb{Z}$ deux entiers, non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle* ***le plus grand commun diviseur de*** *a, b et se note* $\text{pgcd}(a, b)$.

Exemple 38. *1.* $\text{pgcd}(21, 14) = 7, \quad \text{pgcd}(12, 32) = 4, \quad \text{pgcd}(21, 26) = 1$

2. $\text{pgcd}(a, ka) = a$, *pour tout* $k \in \mathbb{Z}$ *et* $a \geq 0$.

3. Cas particuliers. Pour tout $a \geq 0$*:* $\text{pgcd}(a, 0) = a$ *et* $\text{pgcd}(a, 1) = 1$.

10.2 Algorithme d'Euclide

Lemme 1. *Soient $a, b \in \mathbb{N}^*$. Écrivons la division euclidienne $a = bq + r$. Alors on a*

$$\boxed{pgcd(a,b)=pgcd(b,r)}.$$

En fait on a même $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide on applique le lemme avec q le quotient.

Démonstration. Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b donc aussi bq, en plus d divise a donc d divise $bq - a = r$.
- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

Bref, d divise b et r, c'est à dire si $\text{pgcd}(a, b) = d$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r) = d$. □

Algorithme d'Euclide.
On souhaite calculer le pgcd de $a, b \in \mathbb{N}^*$. On peut supposer $a \geq b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul.

- division de a par b, $\quad a = bq_1 + r_1$. Par le lemme 1, $pgcd(a, b) = pgcd(b, r_1)$ et si $r_1 = 0$ alors $\text{pgcd}(a, b) = b$ sinon on continue:
- $b = r_1q_2 + r_2$, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2)$,

- $r_1 = r_2q_3 + r_3, \quad \text{pgcd}(a,b) = \text{pgcd}(r_2, r_3),$
- ...
- $r_{k-2} = r_{k-1}q_k + r_k, \quad \text{pgcd}(a,b) = \text{pgcd}(r_{k-1}, r_k),$
- $r_{k-1} = r_kq_k + 0$. On a $\text{pgcd}(a,b) = \text{pgcd}(r_k, 0) = r_k$.

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leq r_{i+1} < r_i$. Ainsi l'algorithme se termine car nous sommes sûr d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > \ldots \geq 0$.

Exemple 39. *Calculons le* pgcd *de* $a = 600$ *et* $b = 124$.

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

Ainsi le $\text{pgcd}(600, 124) = 4$.

Voici un autre exemple.

Exemple 40. *Calculons* $\text{pgcd}(9945, 3003)$

$$\begin{aligned} 9945 &= 3003 \times 3 + 936 \\ 3003 &= 936 \times 3 + 195 \\ 936 &= 195 \times 4 + 156 \\ 195 &= 156 \times 1 + 39 \\ 156 &= 39 \times 4 + 0 \end{aligned}$$

Ainsi le $\text{pgcd}(9945, 3003) = 39$.

10.2.1 Nombres premiers entre eux

Définition 47. *Deux entiers* a, b *sont dits premiers entre eux si le* $\text{pgcd}(a,b) = 1$.

Exemple 41. *Pour tout $a \in \mathbb{Z}$, a et $a+1$ sont premiers entre eux. En effet soit d un diviseur commun à a et à $a+1$. Alors d divise aussi $a+1-a$. Donc d divise 1 mais alors $d=-1$ ou $d=+1$. Le plus grand diviseur de a et $a+1$ est donc 1. Et donc* $\text{pgcd}(a, a+1) = 1$.

Si deux entiers ne sont pas premiers entre eux, on peut s'y ramener en divisant par leur pgcd:

Exemple 42. *Pour deux entiers quelconques $a, b \in \mathbb{Z}$, notons $d = \text{pgcd}(a, b)$. La décomposition suivante est souvent utile :*

$$\boxed{\begin{cases} a = a'd \\ b = b'd \quad avec\, a', b' \in \mathbb{Z} avec\, \text{pgcd}(a', b') = 1. \end{cases}}$$

Exercice 2.

1. *Écrire la division euclidienne de* 111111 *par* $20xx$*, où* $20xx$ *est l'année en cours.*
2. *Montrer qu'un diviseur positif de* 10008 *et de* 10014 *appartient nécessairement à* $\{1, 2, 3, 6\}$.
3. *Calculer* $\text{pgcd}(560, 133)$, $\text{pgcd}(12121, 789)$, $\text{pgcd}(99999, 1110)$.
4. *Trouver tous les entiers $1 \leq a \leq 50$ tels que a et 50 soient premiers entre eux. Même question avec* 52.

10.3 Théorème de Bézout

Ici, on reprend le théorème de Bézout, vu plus haut sur les polynômes, et on l'applique spécialement pour les entiers.

10.3.1 Théorème de Bézout

Théorème 22. *Soient a, b des entiers. Il existe des entiers $u, v \in \mathbb{Z}$ tels que*

$$au + bv = \text{pgcd}(a, b).$$

Démonstration. La preuve découle de l'algorithme d'Euclide. Les entiers u, v ne sont pas uniques. Les entiers u, v sont **des coefficients de Bézout**. Ils s'obtiennent en "remontant" l'algorithme d'Euclide. □

Exemple 43. *Calculons les coefficients de Bézout pour* $a = 600$ *et* $b = 124$. *Nous reprenons les calculs effectués pour trouver* $\text{pgcd}(600, 124) = 4$. *La première partie est l'algorithme d'Euclide. La seconde partie s'obtient de bas en haut. On exprime le* pgcd *à l'aide de la dernière ligne où le reste est non nul. Puis on remplace le reste de la ligne précédente, et ainsi de suite jusqu'à arriver à la première ligne. Ainsi, on a*

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + \boxed{4} \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

En remontant on obtient

$$\begin{aligned} \boxed{4} &= 104 - 20 \times 5 \\ \boxed{4} &= 104 - (124 - 104 \times 1) \times 5 = 124 \times (-5) + 104 \times 6 \\ \boxed{4} &= 124 \times (-5) + (600 - 124 \times 4) \times 6 = 600 \times 6 + 124 \times (-29) \end{aligned}$$

Ainsi pour $u = 6$ *et* $v = -29$ *alors* $600 \times 6 + 124 \times (-29) = 4$.

On remarque ce qui suit:

- Soignez vos calculs et leur présentation. C'est un algorithme : vous devez aboutir au bon résultat ! Dans la première partie, il faut à chaque ligne bien la reformater. Par exemple $104 - (124 - 104 \times 1) \times 5$ se réécrit en $124 \times (-5) + 104 \times 6$ afin de pouvoir remplacer ensuite 104.
- N'oubliez pas de vérifier vos calculs! C'est rapide et vous serez certain que vos calculs sont exacts. Ici on vérifie à la fin que $600 \times 6 + 124(-29) = 4$.

Exemple 44. *Calculons les coefficients de Bézout correspondant à* $\text{pgcd}(9945, 3003) = 39$.

$$\begin{aligned} 9945 &= 3003 \times 3 + 936 \\ 3003 &= 936 \times 3 + 195 \\ 936 &= 195 \times 4 + 156 \\ 195 &= 156 \times 1 + \boxed{39} \\ 156 &= 39 \times 4 + 0 \end{aligned}$$

Ensuite, on a

$$\begin{aligned} \boxed{39} &= 9945 \times (-16) + 3003 \times 53 \\ \boxed{39} &= \dots \\ \boxed{39} &= \dots \\ \boxed{39} &= 195 - 156 \times 1 \end{aligned}$$

À vous de finir les calculs. On obtient $9945 \times (-16) + 3003 \times 53 = 39$.

10.3.2 Corollaire du théorème de Bézout

Corollaire 7. *Si* $d|a$ *et* $d|b$ *alors* $d|\text{pgcd}(a, b)$.

Un exemple simple: $4|16$ et $4|24$ donc 4 doit diviser $\text{pgcd}(16, 24)$ qui effectivement vaut 8.

Démonstration. Comme $d|au$ et $d|bv$ donc $d|au+bv$. Par le théorème de Bézout $d|\text{pgcd}(a, b)$. □

Corollaire 8. *Soient* a, b *deux entiers. Les nombres* a, b *sont premiers entre eux si et seulement si il existe* $u, v \in \mathbb{Z}$ *tels que*

$$au + bv = 1.$$

On remarque que:
Si on trouve deux entiers u', v' tels que $au' + bv' = d$, cela n'implique pas que $d = \text{pgcd}(a, b)$. On sait seulement alors que $\text{pgcd}(a, b)|d$. Par exemple $a = 12, b = 8; 12 \times 1 + 8 \times 3 = 36$ et $\text{pgcd}(a, b) = 4$.

Corollaire 9. *Soient* $a, b, c \in \mathbb{Z}$.

$$si \quad a|bc \quad et \quad \text{pgcd}(a, b) = 1 \quad alors\ a|c.$$

Exemple: Si $4|7c$ et comme 4 et 7 sont premiers entre eux alors $4|c$.

Démonstration. Comme $\text{pgcd}(a, b) = 1$ alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. On multiplie cette égalité par c pour obtenir $acu + bcv = c$. Mais $a|acu$ et par hypothèse $a|bcv$ donc a divise $acu + bcv = c$. □

10.3.3 Équation $ax + by = c$

Proposition 39. *Soit l'équation* $(E) : ax + by = c$ *où* $a, b, c \in \mathbb{Z}$.

1. *L'équation* (E) *possède des solutions* $(x, y) \in \mathbb{Z}^2$ *si et seulement si* $\text{pgcd}(a, b)|c$.
2. *Si* $\text{pgcd}(a, b)|c$ *alors il existe même une infinité de solutions entières et elles sont exactement les* $(x, y) = (x_0 + \alpha k, y_0 + \beta k)$ *avec* $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ *fixés et* k *parcourant* $\mathbb{Z}$.

Le premier point est une conséquence du théorème de Bézout. Nous allons voir sur un exemple comment prouver le second point et calculer explicitement les solutions. Il est bon de refaire toutes les étapes de la démonstration à chaque fois.

Exemple 45. *Trouver les solutions entières de*

$$161x + 368y = 115.$$

- **Première étape. Y a-t'il de solutions ? L'algorithme d'Euclide.** On effectue l'algorithme d'Euclide pour calculer le pgcd de $a = 161$ et $b = 368$.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

  Donc le $\text{pgcd}(368, 161) = 23$. Comme $115 = 5 \times 23$ alors $\text{pgcd}(368, 161)|115$. Par le théorème de Bézout, l'équation (E) admet des solutions entières.

- **Deuxième étape. Trouver une solution particulière : la remontée de l'algorithme d'Euclide**. On effectue la remontée de l'algorithme d'Euclide pour calculer les coefficients de Bézout.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + \boxed{23} \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

En remontant On obtient alors

$$\begin{aligned}\boxed{23} &= 161 - 46 \times 3\\ \boxed{23} &= 161 - (368 - 161 \times 2) \times 3\\ \boxed{23} &= 161 - (368 \times 3 - 161 \times 6)\\ \boxed{23} &= 161 \times 7 - 3 \times 368\end{aligned}$$

On trouve ainsi $161 \times 7 + 368 \times (-3) = 23$. Comme $115 = 23 \times 5$ en multipliant par 5 on obtient:

$$161 \times 35 + 368 \times (-15) = 115.$$

Ainsi $(x_0, y_0) = (35, -15)$ est une **solution particulière de** (E).

- **Troisième étape. Recherche de toutes les solutions.** Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E). Nous savons que (x_0, y_0) est aussi solution. Ainsi:

$$161x + 368y = 115 \quad \text{et } 161x_0 + 368y_0 = 115$$

(on n'a aucun intérêt à remplacer x_0 et y_0 par leurs valeurs). La différence de ces deux égalités conduit à

$$\begin{aligned}&161 \times (x - x_0) + 368 \times (y - y_0) = 0\\ \Longrightarrow\ &23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0\\ \Longrightarrow\ &7(x - x_0) = -16(y - y_0) \quad (*)\end{aligned}$$

Nous avons simplifier par 23 qui est le pgcd de 161 et 368. (Attention, n'oubliez surtout pas cette simplification, sinon la suite du raisonnement serait fausse.) Ainsi $7|16(y-y_0)$, or $\text{pgcd}(7, 16) = 1$ donc par le lemme de Gauss $7|y-y_0$. Il existe donc $k \in \mathbb{Z}$ tel que $y-y_0 = 7 \times k$. Repartant de l'équation $(*)$: $7(x-x_0) = -16(y-y_0)$. On obtient maintenant $7(x - x_0) = -16 \times 7 \times k$. D'où $x - x_0 = -16k$. (C'est le même k pour x et pour y.) Nous avons donc $(x, y) = (x_0 - 16k, y_0 + 7k)$. Il n'est pas dur de voir que tout couple de cette forme est solution de l'équation (E). Il reste donc juste à substituer (x_0, y_0) par sa valeur et nous obtenons:

Les solutions entières de $161x + 368y = 115$ **sont les**

$$(x, y) = (35 - 16k, -15 + 7k), \quad k \quad \textbf{parcourt } \mathbb{Z}.$$

Pour se rassurer, prenez une valeur de k au hasard et vérifiez que vous obtenez bien une solution de l'équation.

10.3.4 ppcm

Définition 48. *Le ppcm(a,b) (**plus petit commun multiple**) est le plus petit entier ≥ 0 divisible par a et par b à la fois.*

Par exemple $\text{ppcm}(12, 9) = 36$. Le pgcd et le ppcm sont liés par la formule suivante:

Proposition 40. *Si a, b sont des entiers (non tous les deux nuls) alors*

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|.$$

Démonstration. Posons $d = \text{pgcd}(a, b)$ et $m = \frac{|ab|}{\text{pgcd}(a,b)}$. Pour simplifier on suppose $a > 0$ et $b > 0$. On écrit $a = da'$ et $b = db'$. Alors $ab = da'db'$ et donc $m = da'b'$. Ainsi $m = ab' = a'b$ est un multiple de a et de b . Il reste à montrer que c'est le plus petit multiple. Si n est un autre multiple de a et de b alors $n = ka = lb$ donc $kda' = ldb'$ et $ka' = lb'$. Or $\text{pgcd}(a', b') = 1$ et $a'|lb'$ donc $a'b|lb$. Donc $a'b|lb$ et ainsi $m = a'b|lb = n$. □

Voici un autre résultat concernant le ppcm qui se démontre en utilisant la décomposition en facteurs premiers:

Proposition 41. *Si $a|c$ et $b|c$ alors $ppcm(a, b)|c$.*

Il serait faux de penser que $ab|c$. Par exemple $6|36, 9|36$ mais 6×9 ne divise pas 36. Par contre $\text{ppcm}(6, 9) = 18$ divise bien 36.

Exercice 3.

1. *Calculer les coefficients de Bézout correspondant à* $\text{pgcd}(560, 133)$, $\text{pgcd}(12121, 789)$.
2. *Montrer à l'aide d'un corollaire du théorème de Bézout que* $\text{pgcd}(a, a + 1) = 1$.
3. *Résoudre les équations :* $407x + 129y = 1$; $720x + 54y = 6$; $216x + 92y = 8$.
4. *Trouver les couples (a, b) vérifiant* $\text{pgcd}(a, b) = 12$ *et* $\text{ppcm}(a, b) = 360$.

10.4 Nombres premiers

Les nombres premiers sont -en quelque sorte- les briques élémentaires des entiers tout entier s'écrit comme produit de nombres premiers.

10.4.1 Une infinité de nombres premiers

Définition 49. *Un nombre premier p est un entier ≥ 2 dont les seuls diviseurs positifs sont 1 et p.*

Les exemples simples sont les suivants:
$2, 3, 5, 7, 11$ sont premiers, $4 = 22, 6 = 23, 8 = 24$ ne sont pas premiers.

Lemme 2. *Tout entier $n \geq 2$ admet un diviseur qui est un nombre premier.*

Démonstration. Soit $\mathcal{D}$ l'ensemble des diviseurs de n qui sont ≥ 2:

$$\mathcal{D} = \{k \geq 2 : k|n\}.$$

L'ensemble $\mathcal{D}$ est non vide (car $n \in \mathcal{D}$), notons alors $p = min\mathcal{D}$. Supposons, par l'absurde, que p ne soit pas un nombre premier alors p admet un diviseur q tel que $1 < q < p$ mais alors q est aussi un diviseur de n et donc $q \in \mathcal{D}$ avec $q < p$. Ce qui donne une contradiction car p est le minimum. On conclut que p est un nombre premier. Et comme $p \in \mathcal{D}$, p divise n. □

Proposition 42. *Il existe une infinité de nombres premiers.*

Démonstration. Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers que l'on note $p_1 = 2, p_2 = 3, p_3, \ldots, p_n$. Considérons l'entier $N = p_1 \times p_2 \times \ldots \times p_{n+1}$. Soit p un diviseur premier de N (un tel p existe par le lemme précédent), alors d'une part p est l'un des entiers p_i donc $p|p_1 \times \ldots \times p_n$, d'autre part $p|N$ donc p divise la différence $N - p_1 \times \ldots \times p_n = 1$. Cela implique que $p = 1$, ce qui contredit que p soit un nombre premier. Cette contradiction nous permet de conclure qu'il existe une infinité de nombres premiers. □

10.5 Ératosthène et Euclide

Comment trouver les nombres premiers ? **Le crible d'Ératosthène** permet de trouver les premiers nombres premiers. Pour cela on écrit les premiers entiers : pour notre exemple de 2 à 25.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25.$$

Rappelons-nous qu'un diviseur positif d'un entier n est inférieur ou égal à n. Donc 2 ne peut avoir comme diviseurs que 1 et 2 et est donc premier. On entoure 2. Ensuite on raye (ici en gras) tous les multiples suivants de 2 qui ne seront donc pas premiers (car divisible par 2):

$$\boxed{2}, 3, \mathbf{4}, 5, \mathbf{6}, 7, \mathbf{8}, 9, \mathbf{10}, 11, \mathbf{12}, 13, \mathbf{14}, 15, \mathbf{16}, 17, \mathbf{18}, 19, \mathbf{20}, 21, \mathbf{22}, 23, \mathbf{24}, 25.$$

Le premier nombre restant de la liste est 3 et est nécessairement premier : il n'est pas divisible par un diviseur plus petit (sinon il serait rayé). On entoure 3 et on raye tous les multiples de 3 $(6, 9, 12, \ldots.)$.

$$\boxed{2}, \boxed{3}, \mathbf{4}, 5, \mathbf{6}, 7, \mathbf{8}, \mathbf{9}, \mathbf{10}, 11, \mathbf{12}, 13, \mathbf{14}, \mathbf{15}, \mathbf{16}, 17, \mathbf{18}, 19, \mathbf{20}, \mathbf{21}, \mathbf{22}, 23, \mathbf{24}, 25.$$

Le premier nombre restant est 5 et est donc premier. On raye les multiples de 5.

$$\boxed{2}, \boxed{3}, \mathbf{4}, \boxed{5}, \mathbf{6}, 7, \mathbf{8}, \mathbf{9}, \mathbf{10}, 11, \mathbf{12}, 13, \mathbf{14}, \mathbf{15}, \mathbf{16}, 17, \mathbf{18}, 19, \mathbf{20}, \mathbf{21}, \mathbf{22}, 23, \mathbf{24}, \mathbf{25}.$$

7 est donc premier, on raye les multiples de 7 (ici pas de nouveaux nombres à barrer). Ainsi de suite : $11, 13, 17, 19, 23$ sont premiers.

$$\boxed{2}, \boxed{3}, \mathbf{4}, \boxed{5}, \mathbf{6}, \boxed{7}, \mathbf{8}, \mathbf{9}, \mathbf{10}, \boxed{11}, \mathbf{12}, \boxed{13}, \mathbf{14}, \mathbf{15}, \mathbf{16}, \boxed{17}, \mathbf{18}, \boxed{19}, \mathbf{20}, \mathbf{21}, \mathbf{22}, \boxed{23}, \mathbf{24}, \mathbf{25}.$$

Remarque 8. *Si un nombre n n'est pas premier alors un de ses facteurs est $\leq \sqrt{n}$. En effet si $n = a \times b$ avec $a, b \geq 2$ alors $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$ (réfléchissez par l'absurde !). Par exemple pour tester si un nombre ≤ 100 est premier il suffit de tester les diviseurs ≤ 10. Et comme il suffit de tester les diviseurs premiers, il suffit en fait de tester la divisibilité par $2, 3, 5$ et 7. Exemple : 89 n'est pas divisible par $2, 3, 5, 7$ et est donc un nombre premier.*

Proposition 43. ***Lemme d'Euclide*** *Soit p un nombre premier. Si $p|ab$ alors $p|a$ ou $p|b$.*

Démonstration. Si p ne divise pas a alors p et a sont premiers entre eux (en effet les diviseurs de p sont 1 et p , mais seul 1 divise aussi a , donc $\text{pgcd}(a, p) = 1$). Ainsi par le lemme de Gauss $p|b$. □

10.5.1 Décomposition en facteurs premiers

Théorème 23. *Soit $n \geq 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \ldots < \alpha_r \geq 1$ tels que:*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}.$$

De plus les p_i et les α_i $(i = 1, \ldots, r)$ sont uniques.

Exemple: $24 = 2^3 \times 3$ est la décomposition en facteurs premiers. Par contre $36 = 2^2 \times 9$ n'est pas la décomposition en facteurs premiers c'est $2^2 \times 3^2$.

On remarque que la principale raison pour laquelle on choisit de dire que 1 n'est pas un nombre premier, c'est que sinon il n'y aurait plus unicité de la décomposition:

$$24 = 2^3 \times 3 = 1 \times 2^3 \times 3 = 1^2 \times 2^3 \times 3 = \ldots.$$

On ne donne pas ici la démonstration de cette proposition. On se contente de l'exemple suivant.

Exemple 46. *Soient $504 = 2^3 \times 3^2 \times 7$, $300 = 2^2 \times 3 \times 5^2$. Pour calculer le pgcd on réécrit ces décompositions:*

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3 \times 5^2 \times 7^0.$$

Le pgcd est le nombre obtenu en prenant le plus petit exposant de chaque facteur premier:

$$\text{pgcd}(504, 300) = 2^3 \times 3^1 \times 5^0 \times 7^0.$$

Pour le ppcm on prend le plus grand exposant de chaque facteur premier:

$$\text{ppcm}(504, 300) = 2^3 \times 3^2 \times 5^2 \times 7^1.$$

Exercice 4.

1. *Montrer que $n! + 1$ n'est divisible par aucun des entiers $2, 3, \ldots, n$. Est-ce toujours un nombre premier ?*
2. *Trouver tous les nombres premiers ≤ 103.*
3. *Décomposer $a = 2340$ et $b = 15288$ en facteurs premiers. Calculer leur pgcd et leur ppcm.*
4. *Décomposer 48400 en produit de facteurs premiers. Combien 48400 admet-il de diviseurs ?*
5. *Soient $a, b \geq 0$. À l'aide de la décomposition en facteurs premiers, reprouver la formule $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = a \times b$.*

10.6 Congruences

Définition 50. *Soit $n \geq 2$ un entier. On dit que a est congru à b modulo n si n divise $b-a$. On note alors*

$$a \equiv b(\text{mod } n).$$

On note aussi parfois $a \equiv b(\text{mod } n)$ ou $a \equiv b[n]$. Une autre formulation est

$$a \equiv b(\text{mod } n) \Longleftrightarrow \exists k \in \mathbb{Z} \quad a = b + kn. \tag{10.1}$$

Remarquez que n divise a si et seulement si $a \equiv 0(\text{mod } n)$. Ici b dans (10.1) prend le rôle du reste dans la notation utilisée plus haut $a = bq + r$ et n celui du quotient.

Proposition 44. *On a les affirmations suivantes:*

1. *La relation "congru modulo n" est une relation d'équivalence:*
   - *On a $a \equiv a(\text{mod } n)$*
   - *Si $a \equiv b(\text{mod } n)$ alors $b \equiv a(\text{mod } n)$*
   - *Si $a \equiv b(\text{mod } n)$ et $b \equiv c(\text{mod } n)$ alors $a \equiv c(\text{mod } n)$*
2. *Si $a \equiv b(\text{mod } n)$ et $c \equiv d(\text{mod } n)$ alors $a + c \equiv b + d(\text{mod } n)$*
3. *Si $a \equiv b(\text{mod } n)$ alors pour tout $k \geq 0, a^k \equiv b^k(\text{mod } n)$.*

Exemple 47.
- *on a $15 \equiv 1(\text{mod } 7)$, $72 \equiv 2(\text{mod } 7)$, $3 \equiv -11(\text{mod } 7)$*
- *On a $5x + 8 \equiv 3(\text{mod } 5)$ pour tout $x \in \mathbb{Z}$.*
- *On a $11^{20xx} \equiv 1^{20xx}(\text{mod } 10) \equiv 1(\text{mod } 10)$ où $20xx$ est l'année en cours.*

Exemple 48. ***Critère de divisibilité par*** 9. *N est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.*

Pour prouver cela nous utilisons les congruences. Remarquons d'abord que $9|N$ équivaut à $N \equiv 0(\text{mod } 9)$ et notons aussi $10 \equiv 1(\text{mod } 9)$, $10^2 \equiv 1(\text{mod } 9)$, $10^3 \equiv 1(\text{mod } 9) \ldots$

Nous allons donc calculer N modulo 9. Écrivons N en base 10: $N = a_k \dots a_2 a_1 a_0$ (a_0 est le chiffre des unités, a_1 celui des dizaines, ...) alors $N = 10^k a_k + \dots + 10^2 a_2 + 10^1 a_1 + a_0$. Donc

$$\begin{aligned} N &= 10^k a_k + \dots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &= 1(\text{mod } 9)a_k + 1(\text{mod } 9)a_{k-1} + \dots + 1(\text{mod } 9)a_1 + 1(\text{mod } 9)a_0 \\ &\equiv (a_k + \dots + a_2 + a_1 + a_0)(\text{mod } 9) \end{aligned}$$

Donc N est congru à la somme de ses chiffres modulo 9. Ainsi $N \equiv 0(\text{mod } 9)$ si et seulement si la somme des chiffres vaut 0 modulo 9. En d'autres termes si la somme de ses chiffres est divisible par 9.

Voyons cela sur un exemple :$N = 488889$. Ici $a_0 = 9$ est le chiffre des unités, $a_1 = 8$ celui des dizaines,... Cette écriture décimale signifie

$$N = 4.10^5 + 8.10^4 + 8.10^3 + 8.10^2 + 8.10 + 9.$$

$$\begin{aligned} N &= 4.10^5 + 8.10^4 + 8.10^3 + 8.10^2 + 8.10 + 9 \\ &\equiv 4 + 8 + 8 + 8 + 8 + 9(\text{mod } 9) \\ &\equiv 45(\text{mod } 9) \text{ et on refait la somme des chiffres de } 45 \\ &\equiv 9(\text{mod } 9) \\ &\equiv 0(\text{mod } 9) \end{aligned}$$

Ainsi nous savons que 488889 est divisible par 9 sans avoir effectué de division euclidienne.

On remarque que:

Pour trouver un «bon» représentant de $a(\text{mod } 9)$ on peut aussi faire la division euclidienne de a par n : $a = bn + r$ alors $(a \equiv r \bmod n)$ et $0 \leq r \leq n$.

Exemple 49. *Les calculs bien menés avec les congruences sont souvent très rapides. Par exemple on souhaite calculer* $2^{21}\text{mod } 37)$ *(plus exactement on souhaite trouver* $0 \leq r < 37$ *tel que* $2^{21} \equiv r \bmod 37$*).*

Plusieurs méthodes sont possibles:

1. *On calcule* 2^{21}*, puis on fait la division euclidienne de* 2^{21} *par* 37*, le reste est notre résultat. C'est un calcul qui demande beaucoup de peine.*

2. *On calcule successivement les* 2^k *modulo* 37 *:* $2^1 \equiv 2(\text{mod } 37), 2^2 \equiv 4(\text{mod } 37), 2^3 \equiv 8(\text{mod } 37), 2^4 \equiv 16(\text{mod } 37), 2^5 \equiv 32(\text{mod } 37)$. *Ensuite on n'oublie pas d'utiliser les congruences:* $2^6 \equiv 64 \equiv 27(\text{mod } 37)$. $2^7 \equiv 2.2^6 \equiv 2.27 \equiv 54 \equiv 17(\text{mod } 37)$ *et ainsi de suite en utilisant le calcul précédent à chaque étape. C'est assez efficace et on peut raffiner: par exemple on trouve* $2^8 \equiv 34(\text{mod } 37)$ *mais donc aussi* $2^8 \equiv -3(\text{mod } 37)$ *et donc* $2^9 \equiv 2.2^8 \equiv 2.(-3)(\text{mod } 37) \equiv -6(\text{mod } 37) \equiv 31(\text{mod } 37), \ldots$.

3. *Il existe une méthode encore plus efficace: on écrit l'exposant 21 en base 2 :* $21 = 2^4 + 2^2 + 2^0 = 16 + 4 + 1$. *Alors* $2^{21} = 2^{16}.2^4.2^1$. *Et il est facile de calculer successivement chacun de ces termes car les exposants sont des puissances de* 2. *Ainsi* $2^8 \equiv (2^4)^2(\text{mod } 37) \equiv 16^2(\text{mod } 37) \equiv 256(\text{mod } 37) \equiv 34(\text{mod } 37) \equiv -3(\text{mod } 37)$ *et* $2^{16} \equiv 2^8(\text{mod } 37) \equiv (-3)^2(\text{mod } 37) \equiv 9(\text{mod } 37)$. *Nous obtenons* $2^{21} \equiv 2^{16}.2^4.2^1(\text{mod } 37) \equiv 9 \times 16 \times 2(\text{mod } 37) \equiv 288(\text{mod } 37) \equiv 29(\text{mod } 37)$.

10.6.1 Équation de congruence $ax \equiv b(\text{mod } n)$

Proposition 45. *Soit* $a \in \mathbb{Z}^*, b \in \mathbb{Z}$ *fixés et* $n \geq 2$. *Considérons l'équation*

$$ax \equiv b(\text{mod } n)$$

d'inconnue $x \in \mathbb{Z}$*:*

1. *Il existe des solutions si et seulement si* $\text{pgcd}(a, n)|b$.

2. *Les solutions sont de la forme* $x = x_0 + l\frac{n}{\text{pgcd}(a,n)}$, $l \in \mathbb{Z}$ *où* x_0 *est une solution particulière. Il existe donc* $\text{pgcd}(a, n)$ *classes de solutions.*

Exemple 50. *Résolvons l'équation* $9x \equiv 6(\text{mod } 24)$. *Comme* $\text{pgcd}(9, 24) = 3$ *divise* 6 *la proposition ci-dessus nous affirme qu'il existe des solutions. Nous allons les calculer. (Il est toujours préférable de refaire rapidement les calculs que d'apprendre la formule). Trouver* x *tel que* $9x \equiv 6(\text{mod } 24)$ *est équivalent à trouver* x *et* k *tels que* $9x = 6 + 24k$. *Mis sous la forme* $9x - 24k = 6$ *il s'agit alors d'une équation que nous avons étudiée en détails (voir section 10.3.3). Il y a bien des solutions car* $\text{pgcd}(9, 24) = 3$ *divise* 6. *En divisant par le* pgcd *on obtient l'équation équivalente :*

$$3x - 8k = 2.$$

Pour le calcul du pgcd *et d'une solution particulière nous utilisons normalement l'algorithme d'Euclide et sa remontée. Ici il est facile de trouver une solution particulière à la main*

$$(x_0 = 6, k_0 = 2).$$

On termine comme pour les équations de la section 10.3.3. Si (x, k) *est une solution, on écrit* $3x - 8k = 2$ *et pour* (x_0, k_0) *on a l'équation* $3x_0 - 8k_0 = 2$. *Alors par soustraction membre a membre entre* $3x-8k = 2$ *et* $3x_0-8k_0 = 2$, *on obtient* $3(x-x_0)-8(k-k_0) = 0$. *On a donc* $3(x-x_0) = 8(k-k_0)$. *Cela veut dire que* $3 \mid 8(k-k_0)$. *Puisque* $\text{pgcd}(3, 8) = 1$, *donc* $3 \mid (k - k_0)$. *Ainsi il existe* $l \in \mathbb{Z}$ *tel que* $k - k_0 = 3l$. *Donc, on écrit que*

$$3(x - x_0) = 8 \times 3l$$

ou encore

$$x - x_0 = 8l$$

et on trouve $x = x_0 + 8l$, *avec* $l \in \mathbb{Z}$ *(le terme* k *ne nous intéresse pas). Nous avons donc trouvé les* x *qui sont solutions de* $3x - 8k = 2$, *ce qui équivaut à* $9x - 24k = 6$, *ce qui équivaut encore à* $9x \equiv 6(\text{mod } 24)$. *Les solutions sont de la forme* $x = 6 + 8l$. *On préfère les regrouper en* 3 *classes modulo* 24*:*

$$x_1 = 6 + 24m, \quad x_2 = 14 + 24m, \quad x_3 = 22 + 24m, \quad \text{avec } m \in \mathbb{Z}.$$

Remarque 9. *Expliquons le terme de "classe" utilisé ici. Nous avons considéré ici que l'équation* $9x \equiv 6(\text{mod } 24)$ *est une équation d'entiers. On peut aussi considérer que* $9, x, 6$ *sont des classes d'équivalence modulo* 24, *et l'on noterait alors* $\overline{9}\overline{x} = \overline{6}$. *Pour résoudre cela, on cherche l'inverse de* $\overline{9}$ *dans* $\mathbb{Z}/(24\mathbb{Z})$ *en calculant* $9u + 24v = 1$. *On trouverait comme solutions trois classes d'équivalence:*

$$\overline{x_1} = \overline{6}, \quad \overline{x_2} = \overline{14}, \quad \overline{x_3} = \overline{22}.$$

Démonstration. 1. $x \in \mathbb{Z}$ est solution de l'équation $ax \equiv b(mod\ n)$ si et seulement si $\exists k \in \mathbb{Z} : ax = b + kn$.
$\iff \exists k \in \mathbb{Z} : ax - kn = b \iff \text{pgcd}(a, n)|b$ par la proposition39. Nous avons juste transformé notre équation $ax \equiv b(\text{mod } n)$ en une équation $ax - kn = b$ étudiée auparavant (voir section 10.3.3), seules les notations changent: $au+bv = c$ devient $ax - kn = b$.

2. Supposons qu'il existe des solutions. Nous allons noter $d = \text{pgcd}(a, n)$ et écrire $a = da', n = dn'$ et $b = db'$ (car par le premier point $d|b$). L'équation $ax - kn = b$

d'inconnues $x, k \in \mathbb{Z}$ est alors équivalente à l'équation $a'x - kn' = b'$ notée $(*)$. Nous savons résoudre cette équation (voir de nouveau la proposition 39), si (x_0, k_0) est une solution particulière de $(*)$ alors on connaît tous les (x, k) solutions. En particulier $x = x_0 + ln'$ avec $l \in \mathbb{Z}$ (les k ne nous intéressent pas ici). Ainsi les solutions $x \in \mathbb{Z}$ sont de la forme $x = x_0 + l\frac{n}{\text{pgcd}(a,n)}, l \in \mathbb{Z}$ où x_0 est une solution particulière de $ax \equiv b(\text{mod } n)$. Et modulo n cela donne bien $\text{pgcd}(a, n)$ classes distinctes.

□

10.7 Petit théorème de Fermat

Théorème 24. ***Petit théorème de Fermat.*** *Si p est un nombre premier et $a \in \mathbb{Z}$ alors*

$$a^p \equiv a(\text{mod } p).$$

Corollaire 10. *Si p ne divise pas a alors $a^{p-1} \equiv 1(\text{mod } p)$*

Lemme 3. *Si p divise $\binom{p}{k}$ pour $1 \leq k \leq p-1$, c'est-à-dire $\binom{p}{k} \equiv 0(\text{mod } p)$.*

Démonstration. On sait que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, donc $p! = k!(p-k)!\binom{p}{k}$. Or comme $1 \leq k \leq p-1$ alors p ne divise pas $k!$(sinon p divise l'un des facteurs de $k!$ mais il sont tous $< p$).
De même p ne divise pas $(p-k)!$, donc par le lemme d'Euclide p divise $\binom{p}{k}$. □

Démonstration. **Preuve du théorème**
Nous le montrons par récurrence pour les $a \geq 0$.

- Si $a = 0$ alors $0 \equiv 0(\text{mod } p)$.
- Fixons $a \geq 0$ et supposons que $a^p \equiv a(\text{mod } p)$. Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton:

$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \ldots + \binom{p}{1} + 1.$$

Réduisons maintenant modulo p:

$$\begin{aligned}(a+1)^p &\equiv a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \ldots + \binom{p}{1} + 1 \pmod p \\ &\equiv a^p + 1 \pmod p \quad \text{grâce au lemme précédent lemme 3} \\ &\equiv a + 1 \pmod p \quad \text{a cause de l'hypothèse de récurrence}\end{aligned}$$

- Par le principe de récurrence nous avons démontré le petit théorème de Fermat pour tout $a \geq 0$.
  On peut en déduire le cas des $a \leq 0$(**c'est un travail de l'étudiant en révision**).

□

Exemple 51. *Calculons* $14^{3141} \pmod{17}$. *Le nombre* 17 *étant premier on sait par le petit théorème de Fermat que* $14^{16} \equiv 1 \pmod{17}$. *Écrivons la division euclidienne de* 3141 *par* 16*:*

$$3141 = 16 \times 196 + 5.$$

Alors

$$14^{3141} \equiv 14^{16\times 196+5} \equiv 14^{16\times 196} \times 14^5 \equiv (14^{16})^{196} \equiv 1^{196} \times 14^5 \equiv 14^5 \pmod{17}.$$

Il ne reste plus qu'à calculer $14^5 \pmod{17}$. *Cela peut se faire rapidement:* $14 \equiv -3 \pmod{17}$ *donc* $14^2 \equiv (-3)^2 \pmod{17} \equiv 9 \pmod{17}, 14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \pmod{17} \equiv -27 \pmod{17} \equiv 7 \pmod{17}, 14^5 \equiv 14^2 \times 14^3 \equiv 9 \times 7 \pmod{17} \equiv 63 \pmod{17} \equiv 12 \pmod{17}$.

Conclusion : $14^{3141} \equiv 14^5 \pmod{17} \equiv 12 \pmod{17}$.

10.7.1 Exercices corrigés

1. On sait que si n est un entier premier, $H_n = \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ est un groupe pour la multiplication des classes.

   (*i*) Trouver deux entiers relatifs u et v tels que $8u + 29v = 1$.

   (*ii*) En déduire le symétrique de $\overline{8}$ dans le groupe H_{29}.

   (*iii*) Déterminer les $x \in \mathbb{Z}$ solutions de $8x \equiv 9 \pmod{29}$.

2. Existe-t-il un inverse de $\overline{18}$ pour la multiplication dans $\mathbb{Z}/(49\mathbb{Z})$?

3. Existe-t-il un inverse de $\overline{42}$ pour la multiplication dans $\mathbb{Z}/(135\mathbb{Z})$?

4. Trouver tous les éléments de $(\mathbb{Z}/20\mathbb{Z})^\times$ (c'est à dire les éléments qui admettent un inverse dans $(\mathbb{Z}/20\mathbb{Z})$).

5. Résoudre dans $\mathbb{Z}/(37\mathbb{Z})$ les equations suivantes

   i) $\overline{7}y = \overline{2}$

   ii) $\begin{cases} \overline{3}x + \overline{7}y = \overline{3} \\ \overline{6}x - \overline{7}y = \overline{0} \end{cases}$

Démonstration. 1. (*i*) Par l'algorithme d'Euclide, on obtient $u = 11$ et $v = -3$ qui est le couple de solution.
(*ii*) D'après la question précédente, on a $-3 \times 29 + 11 \times 8 = 1$, donc on a

$$\overline{-3 \times 29 + 11 \times 8} = \overline{1} \Longleftrightarrow \overline{-3} \times \overline{29} + \overline{11} \times \overline{8} = \overline{1} \Longleftrightarrow \overline{11} \times \overline{8} = \overline{1}.$$

Car $\overline{29} = \overline{0}$, le symétrique de $\overline{8}$ est $\overline{11}$.
(*iii*) Sachant que $8x \equiv 9 (\text{mod } 29)$ s'écrit aussi $\overline{8}x \equiv \overline{9}$ et que $\overline{11}$ est l'inverse de $\overline{8}$, on a donc

$$\overline{11} \times \overline{8} \times x = \overline{11} \times \overline{9} \Longleftrightarrow \overline{1} \times x = \overline{99}.$$

$$x = \overline{3 \times 29 + 12} \Longleftrightarrow x = \overline{3 \times 29} + \overline{12} \Longleftrightarrow x = \overline{12}.$$

Les solutions sont donc les entiers x congrus à 12 modulo 29. On peut encore écrire ces solutions comme suit:

$$x = 12 + 29k, \quad k \in \mathbb{Z}.$$

2. On peut voir que 18 et 49 sont premiers entre eux, càd $\text{pgcd}(18, 49) = 1$. Avec l'algorithme d'Euclide, on doit trouver les solutions de l'équation de Bézout $18u + 49v = 1$. Il est facile de trouver que l'on a

$$-19 \times 18 + 7 \times 49 = 1.$$

Ainsi l'inverse de $\overline{18}$ dans $\mathbb{Z}/(49\mathbb{Z})$ est

$$\overline{-19 \times 18 + 7 \times 49} = \overline{1} \Longrightarrow -19 \times 18 = 1 (\text{mod } 49) = \overline{-19 \times 18} = \overline{1}.$$

Donc, on a $\overline{-19} \times \overline{18} = \overline{1}$.
Donc l'inverse de $\overline{18}$ dans $\mathbb{Z}/(49\mathbb{Z})$ est $\overline{-19} = \overline{30} \Longleftrightarrow \overline{-19 + 49} = \overline{30}$.

3. On peut voir facilement que 3 divise a la fois 42 et 135. Ainsi $\overline{42}$ n'est pas inversible dans $\mathbb{Z}/(135\mathbb{Z})$, c'est a dire que $\text{pgcd}(42, 135) \neq 1$

4. Rappelons que par le théorème de Bézout, n est inversible dans $\mathbb{Z}/(20\mathbb{Z})$ si et seulement si n est premier avec 20. On a donc
$$(\mathbb{Z}/(20\mathbb{Z}))^{\times} = \left\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\right\}.$$

5. *i*) Chercher l'inverse de $\overline{7}$ dans $\mathbb{Z}/(37\mathbb{Z})$ s'obtient en résolvant par l'algorithme d'Euclide $7u + 37v = 1$. Ainsi on obtient que $\overline{16}$ est l'inverse de $\overline{7}$ dans $\mathbb{Z}/(37\mathbb{Z})$. Il vient donc
$$\overline{7}y = \overline{2} \Longleftrightarrow \overline{16} \times \overline{7}y = \overline{16} \times \overline{2} \Longleftrightarrow y = \overline{32}.$$
ii)En additionnant membre à membre les deux equations du système, on obtient $\overline{9}x = \overline{3}$, or par l'algorithme d'Euclide, on obtient $1 \times 37 - 4 \times 9 = 1$. Ainsi, on voit que $\overline{-4}$ est l'inverse de $\overline{9}$ dans $\mathbb{Z}/(37\mathbb{Z})$. Le calcul simple montre que l'on a
$$x = \overline{-12} \Longleftrightarrow x = \overline{25}.$$
En remplaçant la valeur de x dans l'autre equation on obtient alors l'équation $\overline{7}y = \overline{2}$ qu'on connaît la solution, i.e, $y = \overline{32}$. Ainsi la solution du système devient alors $S = (\overline{25}, \overline{32})$.

□

10.7.2 Exercices non corrigés

On donne également des exercices d'entraînement pour retenir la théorie.

1. Calculer les restes modulo 10 de $122 + 455$, 122×455, 122^{455} . Mêmes calculs modulo 11,puis modulo 12.

2. Prouver qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

3. Calculer $3^{10}(\text{mod } 23)$.

4. Calculer $3^{100}(\text{mod } 23)$.

5. Résoudre les équations:
   - $3x \equiv 4(\text{mod } 7)$,
   - $4x \equiv 14(\text{mod } 30)$

Bibliographie

[1] F. Ulmer. *Anneaux, Corps, Résultant-Algèbre pour L3/M1/agrégation,* Ellipses, 192 pages, 2018.

[2] J.J. Colin and J.M. Morvan. *Groupes, Anneaux et Corps,* Bien Maîtriser les mathématiques, Collection dirigée par Jean-Marie Morvan, Cépaduès, 2014.

[3] C. Calais. *Elements de théorie des anneaux, Anneaux commutatifs L3,* Mathématiques à l'Université, ellipses, Paris, 2006

[4] R. y=Goblot. *Algèbre commutative, Dunod, Paris, 2001*

[5] Georges et M-Nicole Gras. *Algèbre fondamentale. Arithémetique. Ellipses, 2004.*

[6] J. Marie Monier. *Algèbre MPSI, Cours, méthodes et exercices corrigés, 4ème édition,J'intègre.* Dunod, Paris, 2006.

[7] Xavier Gourdon. *Algèbre. Les maths en tête.* Ellipses, Paris, 1994.