Cours, licence 3 ième année, 1er semestre.

Anneaux.

Jean-Robert Belliard année 2011–12.

Table des matières

Chapitre 1

Arithmétique de base dans les entiers

L'anneaux $\mathbb{Z}$ est le premier exemple d'anneaux que chacun rencontre. Il est aussi fondamental en plus d'un sens : Tout anneaux contient un sous-anneaux quotient de $\mathbb{Z}$ par le morphisme caractéristique, l'étude des groupes commutatifs aussi est indissociable de celle de $\mathbb{Z}$: ce point sera développé en partie dans ce cours mais aussi dans le cours « Groupes » de cette année de licence et le « Modules sur les anneaux principaux » du master première année. Pour construire sur des bases saines ce chapitre préliminaire revient sur l'arithmétique élémentaire dans $\mathbb{Z}$.

1.1 L'anneau des entiers

1.1.1 Premières propriétés

Dans ce cours on choisit de considérer comme donnés les ensembles

$$\mathbb{N} = \{0, 1, 2, \cdots\} \quad \text{et} \quad \mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2 \cdots\}$$

munis des opérations d'arithmétique élémentaires $(x, y) \mapsto x + y$ et $(x, y) \mapsto x \times y$, pour $\mathbb{N}$ et pour $\mathbb{Z}$ de l'opération opposée $x \mapsto -x$. Ces deux ensembles sont aussi munis de la relation d'ordre totale usuelle $x \leq y \iff y - x \in \mathbb{N}$. On rappelle simplement les propriétés basiques (forcément admise en l'absence de définitions fixées) de ces opérations. La relation d'ordre $\leq$ vérifie deux propriétés fréquemment utilisées en algèbre :

1. $\leq$ est archimédienne :

$$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}, \ n > 0, \exists k \in \mathbb{N}, k \times n \geq x.$$

2. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément pour $\leq$:

$$\forall F \subset \mathbb{N}, \exists f \in F, \forall x \in F, f \leq x.$$

Les propriétés qui suivent font de $\mathbb{Z}$ un anneaux commutatif unitaire.

Proposition 1.1 (l'anneau $\mathbb{Z}$) *L'ensemble $\mathbb{Z}$ est muni de deux lois de composition interne, l'addition notée $+$ et la multiplication notée $\times$ qui vérifient les propriétés suivantes :*

1. *l'addition est associative :* $\forall x, y, z \in \mathbb{Z},\ (x + y) + z = x + (y + z)$.
2. *le nombre* 0 *est élément neutre pour l'addition :* $\forall x \in \mathbb{Z},\ x + 0 = 0 + x = x$.
3. *tout entier admet un opposé additif :* $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ x + y = y + x = 0$.
4. *l'addition est commutative :* $\forall x, y \in \mathbb{Z},\ x + y = y + x$.
5. *la multiplication est associative :* $\forall x, y, z \in \mathbb{Z},\ (x \times y) \times z = x \times (y \times z)$.
6. *le nombre* 1 *est élément neutre pour la multiplication :* $\forall x \in \mathbb{Z},\ x \times 1 = 1 \times x = x$.
7. *la multiplication est distributive à droite et à gauche par rapport à l'addition :* $\forall x, y, z \in \mathbb{Z},\ (x + y) \times z = x \times z + y \times z$ *et* $z \times (x + y) = z \times x + z \times y$.
8. *la multiplication est commutative :* $\forall x, y \in \mathbb{Z},\ x \times y = y \times x$.

Remarques

1. Étant donné $x \in \mathbb{Z}$ l'usage est de noter $-x$ son unique opposé additif c'est-à-dire l'entier tel que $x + (-x) = (-x) + x = 0$. L'existence de $-x$ est affirmée par l'axiome 3 de la proposition 1.1, son unicité est immédiate parce que si $x + y = y + x = 0$ et $x + z = z + x = 0$ alors $z = z + 0 = z + (x + y) = (z + x) + y = 0 + y = y$.
2. Les axiomes 1 à 8 ci-dessous permettent d'abréger certaines formules en omettant le symbole $\times$ pour la multiplication, et utilisant les règles de priorités usuelles que tout lecteur de ce cours connaît. Ainsi par exemple $((x \times y) + (x \times z)) + (t \times u)$ s'écrit plus lisiblement $xy + xz + tu$. Dans la suite de ce chapitre consacré à l'anneau $\mathbb{Z}$, connu de tout un chacun, on reprend immédiatement les abréviations usuelles.

1.1.2 Algorithme d'Euclide

Toute l'arithmétique élémentaire dans $\mathbb{Z}$ est basée sur l'existence d'une division euclidienne.

Lemme 1.2 *Soit* $a \in \mathbb{Z}$ *et* $b \in \mathbb{Z}$ *avec* $b \neq 0$. *Alors il existe un unique couple* $(q, r) \in \mathbb{Z}^2$ *tel que les entiers* q *et* r *vérifient :*

1. $a = bq + r$
2. $0 \leq r < |b|$

Démonstration Si a et b sont dans $\mathbb{N}$ c'est une conséquence directe de l'existence de la relation d'ordre archimédienne. En effet l'ensemble F dont les éléments sont les entiers $q' \in \mathbb{N}$ tel que $q'b > a$ est non vide et admet un unique plus petit élément, notons p ce plus petit élément. Alors $q = (p - 1)$ n'appartient pas à F et est le plus grand entiers tel que $qb \leq a$. Nécessairement on a alors $0 \leq a - qb < b$, d'où l'existence et l'unicité du couple $(q, a - bq)$ recherché.

Si $a < 0$ et $b > 0$ alors par le cas précédent on a l'existence et l'unicité d'entiers x et y tels que $-a = xb + y$ avec $0 \leq y < b$. Si $y = 0$ alors l'unique couple recherché est $(-x, 0)$, si $1 \leq y \leq b - 1$ alors l'unique couple recherché est $(-x - 1, b - y)$.

Si maintenant $b < 0$ alors une division euclidienne par $-b$ donne aussi une division euclidienne par b avec $a = -q \times (-b) + r$.

Définition 1.3 *Soient $a, b \in \mathbb{Z}$. On dit que b divise a et on note $b \mid a$ lorsqu'il existe un co-diviseur $c \in \mathbb{Z}$ tel que $a = bc$. On appelle diviseur commun à a et b un entier d tel que $d \mid a$ et $d \mid b$. Lorsque $a \mid m$ on dit que m est un multiple de m, et on dit que m est un multiple commun à a et b lorsque $a \mid m$ et $b \mid m$.*

L'ensemble des diviseurs communs à a et b donné est fini car compris entre $-c$ et c pour $c = \min\{|a|, |b|\}$. L'existence d'un plus grand diviseur commun (forcément positif) au sens de l'ordre archimédien est donc immédiate mais dénué d'intérêt arithmétique. Un fait plus significatif est que ce plus grand diviseurs commun est aussi un majorant pour la relation d'ordre de divisibilité parmi les diviseurs communs positifs. Cette propriété ne se démontre pas dans $\mathbb{Z}$ sans utiliser de division euclidienne. Cela conduit aussi à une notion de PGCD plus utile et généralisable à des anneaux dépourvu de la relation d'ordre archimédienne.

Théorème 1.4 (Algorithme d'Euclide) *Soient $a, b \in \mathbb{Z}$ deux entiers ordonnés de telle sorte que $|a| \geq |b|$, et soit d le plus grand des diviseurs communs à a et b.*

1. *Algorithme d'Euclide : Tout diviseur commun à a et b divise d.*
2. *Algorithme d'Euclide étendu : Il existe un matrice $M \in M_2(\mathbb{Z})$ avec $\det(M) = \pm 1$ et telle que*
$$M \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$
En particulier il existe un couple d'entier (u, v) dans $\mathbb{Z}^2$ tel que $ua + vb = d$.
3. *Soit $m = |ab|/d$. Alors a et b divisent m et tout multiple commun à a et b est un multiple de m et cela justifie la terminologie « m est le Plus Petit Multiple Commun à a et b ».*

Démonstration

1. Lorsque $b = 0$ alors on a $d = |a|$ et comme tout entier divise 0 avec 0 comme codiviseur l'ensemble des diviseurs communs à a et b est exactement l'ensemble des diviseurs de d. La démonstration consiste, par des divisions euclidiennes successives, à se ramèner à ce cas particulier simple. Soit $b \neq 0$ et soit a tel que $|a| \geq |b|$. On écrit par division euclidienne $a = bq + r$ avec $0 \leq r < |b|$. Alors l'ensemble des diviseurs communs à a et b est exactement celui des diviseurs commun à b et r, parce que si un entier divise a et b il divise $r = a - bq$ et si un entier divise r et b il divise aussi $a = bq + r$. Ainsi sans changer l'ensemble des diviseurs communs on peut remplacer le couple (a, b) par (b, r) et on a $|r| < |b|$, donc au bout d'un nombre fini de telles substitutions on arrivera à un couple de la forme $(\pm d, 0)$.
2. Dans la démonstration qui précède, on passe du couple (a, b) au couple $(b, r = a - bq)$ en multipliant à sa gauche le vecteur colonne $\begin{bmatrix} a \\ b \end{bmatrix}$ par la matrice $N = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix}$, dont le déterminant est -1. Grâce à l'associativité du produit matriciel on obtient la matrice M de l'énoncé en multipliant toute ces matrices N intermédiaires (et dans l'éventualité où l'algorithme termine avec $(-d, 0)$ on

multiplie encore à gauche par $-I_2$). Lorsqu'on a $M \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$ la première ligne de M fournit les entiers u, v.

3. Clairement $m = \pm a(b/d) = \pm b(a/d)$ est un multiple commun à a et b. Soit ensuite $n = aa' = bb'$ un multiple commun à a et b. Alors avec $d = au + bv$ on obtient $1 = u(a/d) + v(b/d)$ puis $n = nu(a/d) + nv(b/d) = ub'(ba/d) + va'(ab/d) = (ab/d)(ub' + va')$; en utilisant chacune des deux expressions de $n = bb' = aa'$ dans chacun des deux termes de la somme. Donc $m = (ab)/d$ divise bien n.

Notations

1. Le plus grand commun diviseur de a et b se note, suivant les auteurs, $d = pgcd(a, b)$ ou $d = (a, b)$ ou $d = a \wedge b$.
2. Le plus petit multiple commun de a et b se note, suivant les auteurs, $m = ppcm(a, b)$ ou $m = a \vee b$.

Terminologie

1. On appelle relation de Bézout l'équation $au + bv = d$ obtenue à l'issue de l'algorithme d'Euclide étendu.
2. Deux entiers a et b tels que $a \wedge b = 1$ sont dits premiers entre eux ou comaximaux ou encore étrangers. Ces trois notions coïncident dans $\mathbb{Z}$ mais seront redéfinies et bien distinctes dans des anneaux plus généraux.

1.2 Théorème fondamental de l'arithmétique

1.2.1 Nombres premiers

Définition 1.5 *On appelle* ***nombre premier*** *un entier $p > 1$ dont les seuls diviseurs sont les diviseurs triviaux ± 1 et $\pm p$.*

L'énoncé et sa preuve qui suivent était déjà dans les écrits d'Euclide :

Proposition 1.6 *Il existe une infinité de nombres premiers.*

Démonstration On procède par l'absurde. On suppose, en vue d'une contradiction, qu'il n'y a que n nombres premiers disons $p_1 = 2, p_2 = 3, \cdots p_n$. Alors le nombre entier positif $1 + p_1 p_2 \cdots p_n$ n'est divisible par aucun des p_j donc est un $(n+1)^{\text{ime}}$ nombre premier.

Le crible d'Eratosthène C'est une méthode pour avoir la liste des nombres premiers entre 1 et N. On commence par écrire tous les nombres entre 1 et N. Puis on raye les nombres divisibles par 2, puis ceux divisibles par 3, puis ceux divisibles par 5 le plus petit nombre supérieur à 3 et non encore rayé ... Et ainsi de suite. À chaque nouvelle étape on raye les multiples stricts du plus petit nombre non rayé qui est supérieur aux nombres premiers déjà exploités ; évidemment ce nombre est

premier. On s'arrête dès que la partie entière de $\sqrt{N}$ est atteinte. Les nombres non rayés sont alors premiers car divisible par aucun nombre premier plus petit que leur racine carré. Cette méthode teste aussi la primalité de N.

1.2.2 Lemme de Gauß

C'est ainsi qu'on désigne l'énoncé suivant :

Lemme 1.7 *Soient a et b deux entiers tels que $pgcd(a,b) = 1$ et a divise bc. Alors a divise c.*

Démonstration On part d'une relation de Bézout $1 = au + bv$ et on en tire en multipliant par c l'égalité $c = auc + bcv$. Mais a divise bc, donc a divise bcv et aussi $c = auc + bcv$.

Lemme 1.8 *Soit p un nombre premier et b et c deux entiers. Si p divise le produit bc alors p divise b ou p divise c.*

Démonstration On suppose p premier. Le $pgcd(p,b)$ qui est un diviseur positif de p vaut p si $p \mid b$ et 1 si $p \nmid b$. On suppose que p divise bc et pas b. Alors par le lemme de Gauß p divise c.

Le lemme 1.8 qui est un cas particulier utile du lemme de Gauß, est aussi connu sous le nom de lemme d'Euclide.

Proposition 1.9 *Soient a, b et c des entiers positifs. On a les égalités :*

1. $a(b \wedge c) = ab \wedge ac$.
2. $a(b \vee c) = ab \vee ac$.

Démonstration

1. On procède par double divisibilité. Il y a une divisibilité évidente, c'est $a(b \wedge c) \mid ab \wedge ac$. En effet $(b \wedge c) \mid b$ donc $a(b \wedge c) \mid ab$, et de façon symétrique $a(b \wedge c) \mid ac$. Donc $a(b \wedge c)$ est un diviseur commun à ab et ac et divise $ab \wedge ac$. Réciproquement on part d'une relation de Bézout $b \wedge c = ub + vc$ et on multiplie par a pour avoir $a(b \wedge c) = uab + vac$. Ainsi on voit que $ab \wedge ac$ qui divise ab et ac divise aussi $a(b \wedge c) = uab + vac$.
2. On utilise le 1., pour calculer :

$$a(b \vee c) = a\frac{bc}{b \wedge c} = \frac{ab\ ac}{a(b \wedge c)} = \frac{ab\ ac}{ab \wedge ac} = ab \vee ac\ .$$

1.2.3 L'anneau des entiers est factoriel

Le théorème fondamental de l'arithmétique est l'existence et l'unicité de la factorisation en un signe et un produit de puissance de nombre premier de tout entier non nul $a \in \mathbb{Z}$. L'existence est évidente à démontrer et facile à comprendre. Toute la subtilité de ce théorème réside dans l'unicité qu'il faut commencer par définir, et qui ne se démontre pas sans le lemme d'Euclide.

Théorème 1.10 *Soient $a \in \mathbb{Z}$ un entier non nul fixé. Il existe un unique entier N, une unique famille strictement croissante de N nombres premiers $p_1 < p_2 < \cdots < p_N$, une unique famille de N entiers strictement positifs $n_1, \cdots, n_N$ avec $n_i > 0$, et un unique signe $\varepsilon \in \{\pm 1\}$ tels que*

$$a = \varepsilon \prod_{i=1}^{N} p_i^{n_i}.$$

Démonstration Le signe ε est évidemment le signe de a. Il existe et il est unique. Donc quite à multiplier par ε on peut supposer $a > 0$ et $\varepsilon = 1$. Pour l'existence de N, des p_i et des n_i il suffit de montrer que tout entier est produit d'un nombre fini de nombre(s) premier(s) (non nécessairement distincts deux à deux) ; puis de regrouper correctement les premiers p_i en utilisant l'associativité de la multiplication. On établit cette existence par récurrence sur a. L'initialisation s'obtient avec $1 = 1$. Supposons que l'on sache factoriser les entiers inférieur ou égaux à $a - 1$ en produit fini de nombres premiers. Si a est premier il est factorisé en $a = a$. Sinon il admet une factorisation non triviale $a = bc$ avec $1 < b < a$ et $1 < c < a$. Par récurrence on sait factoriser b et factoriser c et on en tire une factorisation de $a = bc$.

Passons à l'unicité. Pour ce, on se donne deux écritures :

$$a = \prod_{i=1}^{N} p_i^{n_i} = \prod_{j=1}^{M} q_j^{m_j},$$

pour deux entiers $N, M \in \mathbb{N}$, deux familles finies strictement croissantes de N premiers p_i et M premiers q_j et deux familles finies d'exposants n_i et m_j. Soit $\mathbb{P}$ l'ensemble des nombres premiers divisant a. On commence par constater l'égalité ensembliste $\mathbb{P} = \{p_1, p_2, \cdots, p_N\}$. En effet si p divise a alors il divise le produit $\prod_{i=1}^{N} p_i^{n_i}$ et donc par le lemme d'Euclide 1.8 il divise l'un des p_i, par exemple p_t. S'agissant de deux nombres premiers la divisibilité $p \mid p_t$ donne l'égalité $p = p_t$; d'où l'inclusion de $\mathbb{P}$ dans $\{p_1, p_2, \cdots, p_N\}$. Comme l'inclusion réciproque revient à dire que chaque p_i divise a on a bien l'égalité $\mathbb{P} = \{p_1, p_2, \cdots, p_N\}$. Par symétrie on a aussi $\{p_1, \cdots, p_N\} = \mathbb{P} = \{q_1, \cdots, q_M\}$. On obtient alors directement $N = M$ et aussi avec nos conventions d'ordre strict sur les p_i et q_i les égalités $\forall i,\ p_i = q_i$ car p_i et q_i sont tous les deux le i^{ime} élément de $\mathbb{P}$ pour l'ordre archimédien. Il reste à démontrer pour tout i l'égalité $n_i = m_i$. Mais par le lemme d'Euclide 1.8 p_i ne divise pas le produit $\prod_{j \neq i} p_j^{n_j}$ et donc $p_i^{n_i+1} \nmid a$. On a donc une définition intrinsèque de n_i avec $n_i = \max\{k \in \mathbb{N}, p_i^k \mid a\}$. Forcément on a aussi $m_i = \max\{k \in \mathbb{N}, p_i^k \mid a\} = n_i$; ce qui conclut la démonstration du théorème 1.10.

Les entiers $n_i = \max\{k \in \mathbb{N}, p_i^k \mid a\} = v_{p_i}(a)$ qui interviennent dans cette démonstration s'appellent les valuations p_i-adique de a.

Définition 1.11 *Soit p un nombre premier et $a \in \mathbb{Z}$ un entier non nul. On appelle valuation p-adique de a et on note $v_p(a)$ l'entier $v_p(a) = \max\{k \in \mathbb{N}, p^k \mid a\}$ (on a toujours $p^0 = 1 \mid a$). Cela définit une application $v_p \colon \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$.*

Remarque Dans la formulation usuelle du théorème 1.10, on ne précise pas l'ordre d'écriture des facteurs premiers p_i divisant a et on parle « d'unicité à l'ordre des facteurs premiers près ». Clairement les deux énoncés sont équivalents. L'énoncé choisi ici tire avantage de l'ordre archimédien canonique qui en plus simplifie agréablement la démonstration. La notion d'unicité à permutation près demande aussi un effort de compréhension supplémentaire et est lourde à formaliser. On devra néanmoins faire cet effort dans le cadre plus général des anneaux factoriels qui, a priori, sont dénué d'ordre naturel (par exemple pour la définition 6.4).

En corollaire du théorème 1.10, ou si l'on préfère du lemme d'Euclide 1.8, les valuations p-adiques vérifient les propriétés :

Corollaire 1.12 *Soient a, b deux entiers non nuls et p un nombre premier.*

1. $v_p(ab) = v_p(a) + v_p(b)$.
2. $a \mid b \iff \forall p \text{ premier } v_p(a) \leq v_p(b)$.
3. $v_p(a \wedge b) = \min\{v_p(a), v_p(b)\}$.
4. $v_p(a \vee b) = \max\{v_p(a), v_p(b)\}$.

Démonstration

1. Par définition de v_p on peut écrire $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$ avec $p \nmid a'$ et $p \nmid b'$. On a donc $ab = p^{v_p(a)+v_p(b)}a'b'$. Par le lemme d'Euclide $p \nmid a'b'$ et donc $p^{v_p(a)+v_p(b)+1}$ ne divise pas ab. Cela donne bien $v_p(ab) = v_p(a) + v_p(b)$.
2. Si $a \mid b$ alors pour tout premier p on a $p^{v_p(a)} \mid a \mid b$ et donc $v_p(a) \leq v_p(b)$. Réciproquement si pour tout p on a $v_p(a) \leq v_p(b)$ on obtient par le théorème 1.10 $b = \pm a \prod_{p|b} p^{v_p(b)-v_p(a)}$, d'où l'équivalence.
3. Soit $i_p = \min\{v_p(a), v_p(b)\}$. Il s'agit de montrer que $v_p(a \wedge b) = i_p$. Par le point 2 ci-dessus on a $\prod_p p^{i_p} \mid a$ et $\prod_p p^{i_p} \mid b$ donc $\prod_p p^{i_p} \mid a \wedge b$ et donc $i_p \leq v_p(a \wedge b)$. Réciproquement comme $a \wedge b$ divise a et b on a $v_p(a \wedge b) \leq i_p$.
4. Par définition on a $a \vee b = (ab)/(a \wedge b)$. Par le point 1 ci dessus on en déduit $v_p(a \vee b) = v_p(a) + v_p(b) - \min\{v_p(a), v_p(b)\} = \max\{v_p(a), v_p(b)\}$.

1.3 Congruences modulo un entier

1.3.1 Relation d'équivalence

Définition 1.13 *Soit E un ensemble. On appelle* ***relation d'équivalence*** *sur E la donnée d'un sous-ensemble $\mathcal{R} \subset E \times E$ vérifiant :*

1. *Réflexivité :* $\forall x \in E \ (x, x) \in \mathcal{R}$
2. *Symétrie :* $\forall x, y \in E \ (x, y) \in \mathcal{R} \Rightarrow (y, x) \in \mathcal{R}$
3. *Transitivité :* $\forall x, y, z \in E \ ((x, y) \in \mathcal{R} \text{ et } (y, z) \in \mathcal{R}) \Rightarrow (x, z) \in \mathcal{R}$

Terminologie-Notations

1. L'usage est de noter $x \sim y$ pour $(x, y) \in \mathcal{R}$ et de dire que x et y sont équivalent pour la relation $\mathcal{R}$ ou $\sim$.
2. L'ensemble des éléments $y \in E$ tels que $x \sim y$ s'appelle la **classe** de x, et se note parfois $\overline{x} \subset E$.
3. L'ensemble dont les éléments sont les classes d'équivalence sous une relation $\sim$ est un sous-ensemble de l'ensemble $\mathcal{P}(E)$ de toutes les parties de E s'appelle **l'ensemble quotient** de E pour $\sim$ et se note parfois $E/\sim$.
4. L'application $x \mapsto \bar{x}$ est une surjection de E sur $E/\sim$ et s'appelle la **projection canonique** de E sur $E/\sim$.
5. Le choix d'un, et d'un seul, élément $x_i \in \overline{x_i}$ dans chacune des classes produit ce qu'on appelle un **système de représentants** dans E de $E/\sim$. Soit $S \subset E$ une partie de E. Alors S est un système de représentant dans E de $E/\sim$ si et seulement si la restriction à S de la projection canonique réalise une bijection entre S et $E/\sim$.

Exemples

1. Sur tout ensemble l'égalité est une relation d'équivalence.
2. La relation de congruence modulo 10 dans $\mathbb{Z}$, par définition :

$$x \equiv y[10] \iff 10 \mid (x - y).$$

3. La colinéarité des vecteurs dans tout $\mathbb{K}$-espace vectoriel, par définition

$$u \sim v \iff \exists \lambda \in \mathbb{K}, \lambda \neq 0 \quad \lambda u = v.$$

1.3.2 Calcul modulaire dans les entiers

L'exemple de relation d'équivalence qui nous intéresse dans cette section est la relation de congruence modulo un entier n dans $\mathbb{Z}$.

Définition 1.14 *Soit $n \in \mathbb{N}$ un entier on dit que deux entiers a et b sont **congrus** modulo n et on écrit $a \equiv b[n]$ lorsque $n \mid (a - b)$.*

Proposition 1.15 *Soit $n > 0$ un entier non nul.*

1. *La congruence modulo n est une relation d'équivalence.*
2. *Soit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la congruence modulo n. Alors l'ensemble $\{0, 1, \cdots, n-1\}$ est un système de représentants dans $\mathbb{Z}$ de $\mathbb{Z}/n\mathbb{Z}$ qui contient donc n éléments.*
3. *Tout intervalle d'entiers de longueur n forme un système de représentant dans $\mathbb{Z}$ de $\mathbb{Z}/n\mathbb{Z}$.*
4. *Les formules $\bar{a} + \bar{b} := \overline{a+b}$ et $\bar{a} \times \bar{b} := \overline{a \times b}$ définissent deux loi de composition interne sur l'ensemble des classes $\mathbb{Z}/n\mathbb{Z}$.*
5. *Ces opérations $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ héritent des propriétés 1 à 8 de la proposition 1.1, avec $\bar{0}$ comme neutre additif, $\bar{1}$ comme neutre multiplicatif et $\overline{-x}$ comme opposé additif de x.*

Démonstration

1. Soit n fixé dans $\mathbb{N}$ et soient a, b et c dans $\mathbb{Z}$. Alors n divise $a-a$; si n divise $a-b$ il divise $b-a$; et si n divise simultanément $a-b$ et $b-c$ alors n divise $a-c$. Ainsi la congruence modulo n est une relation d'équivalence.
2. Tout entier est congru modulo n au reste de sa division euclidienne par n donc $\{0, 1, \cdots, n-1\}$ représente au moins une fois chaque classe de $\mathbb{Z}/n\mathbb{Z}$. Si $x > y$ sont dans $\{0, 1, \cdots, n-1\}$ alors $0 < x - y < x < n$ et donc $n \nmid (x-y)$ de sorte que $\{0, 1, \cdots, n-1\}$ représente une et une seule fois toutes les classes de $\mathbb{Z}/n\mathbb{Z}$.
3. Soit $I = \{a, a+1, \cdots, a+n-1\}$ un tel intervalle. Alors l'application $x \mapsto \bar{x}$ est une injection de I dans $\mathbb{Z}/n\mathbb{Z}$ pour la même raison que dans le point 2. Comme ces deux ensembles finis ont le même nombre d'éléments cette injection est surjective.
4. Il faut s'assurer que ces formules définissent bien des lois de composition internes sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ c'est-à-dire des applications $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. En effet la formule $(a, b) \mapsto \overline{a+b}$ définit correctement une application $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ mais a priori pas une application $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. Prenons $a \equiv a'[n]$ et $b \equiv b'[n]$. Alors $a' = a + kn$ et $b' = b + ln$ pour deux entiers k et l. Et donc $a' + b' = a + b + n(k+l) \equiv a + b[n]$. Donc la classe $\overline{a+b}$ dépend seulement des classes $\bar{a}$ et $\bar{b}$ dans $\mathbb{Z}/n\mathbb{Z}$ et pas du choix de leur représentants a et b dans $\mathbb{Z}$. Cela démontre que $(\bar{a}, \bar{b}) \mapsto \overline{a+b}$ est bien une loi de composition sur $\mathbb{Z}/n\mathbb{Z}$. De même si $a' = a + kn$ et $b' = b + ln$ alors $a'b' = ab + n(al + bk + kln) \equiv ab[n]$ et la multiplication aussi est loi de composition sur $\mathbb{Z}/n\mathbb{Z}$.
5. Il suffit d'utiliser la propriété analogue dans $\mathbb{Z}$ et de la réduire modulo n. Comme le résultats des opérations modulo n ne dépend pas du choix des représentants, chaque formule dans $\mathbb{Z}$ donne la formule analogue dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque Ces propriétés font de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ un anneau commutatif unitaires. On dit que c'est l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$. On reviendra sur ces notions dans un cadre plus général.

1.3.3 Théorème des restes chinois

L'énoncé élémentaire de ce théorème dans $\mathbb{Z}$ est le suivant :

Théorème 1.16 *Soient $a_1, a_2, \cdots, a_n \in \mathbb{N}$ des entiers deux à deux premiers entre eux, soit $a = \prod_{i=1}^{n} a_i$ et soient $x_1, x_2, \cdots, x_n \in \mathbb{Z}$ des entiers arbitraires. Il existe un x dans $\mathbb{Z}$ tel que $\forall i$, $x \equiv x_i[a_i]$. De plus la classe de congruence de x modulo a est unique.*

Démonstration Par le lemme d'Euclide 1.8 les facteurs premiers de a_1 ne divisent pas $b_1 = \prod_{i=2}^{n} a_i$ et donc $pgcd(a_1, b_1) = 1$. En partant d'une relation de Bezout $1 = ua_1 + vb_1$ on obtient un entier $e_1 = 1 - ua_1$ qui vérifie $e_1 \equiv 0[a_i]$ pour tout $i > 1$ et $e_1 \equiv 1[a_1]$. On procédant de la même façon on définit des $e_i \in \mathbb{Z}$ tels que $e_i \equiv 1[a_i]$

et $\forall j \neq i$, $e_i \equiv 0[a_j]$. Alors l'entier $x = \sum_{i=1}^{n} x_i e_i$ vérifie le système de congruence de l'énoncé. Soit y une autre solution de ce système de congruence. Alors pour tout i l'entier a_i divise $y - x$. Donc $y - x$ est multiple du ppcm des a_i qui est a puisque les a_i sont premiers entre eux.

De façon plus conceptuelle ce théorème donne un isomorphisme d'anneaux entre l'anneau $\mathbb{Z}/a\mathbb{Z}$ et l'anneau produit $\prod_i \mathbb{Z}/a_i\mathbb{Z}$. On reviendra sur ces notions lorsqu'on disposera des définitions générales d'anneaux produits et d'anneaux quotient.

FIN DU CHAPITRE PRÉLIMINAIRE

Chapitre 2

Anneaux commutatifs

La structure d'anneau est celle qui évoque les notions de « calcul algébrique » au sens commun et d'arithmétique. En outre, elle débouche directement sur des applications pratiques intéressantes, comme l'interpolation polynomiale et le calcul modulaire, que nous développerons au chapitre 4, des méthodes de factorisation des polynômes, qui seront vues au chapitre 6, et encore les transformées de Fourier discrètes, dont les applications actuelles sont innombrables, mais que nous n'avons pas incluses dans ce cours. Elle contient enfin, comme cas particulier, la structure de corps qui fait l'objet du cours de « Corps » du Master.

2.1 Anneaux

2.1.1 Définitions et premières propriétés

Définition 2.1 (Anneau) *Un **anneau** est un ensemble A sur lequel se trouvent définies deux lois de composition, (la première notée additivement $+$, la seconde multiplicativement $\times$) vérifiant les conditions suivantes :*

1. *l'addition est associative :* $\forall x, y, z \in A,\ (x + y) + z = x + (y + z)$.
2. *il existe un neutre noté* 0 *pour l'addition et tel que :* $\forall x \in A,\ x+0 = 0+x = x$.
3. *tout élément de A admet un opposé additif :* $\forall x \in A,\ \exists y \in A,\ x+y = y+x = 0$.
4. *l'addition est commutative :* $\forall x, y \in A,\ x + y = y + x$.
5. *la multiplication est associative :* $\forall x, y, z \in A,\ (x \times y) \times z = x \times (y \times z)$.
6. *Il existe un neutre multiplicatif (l'élément unité de l'anneau) noté* 1 *et tel que :* $\forall x \in \mathbb{Z},\ x \times 1 = 1 \times x = x$.
7. *la multiplication est distributive à droite et à gauche par rapport à l'addition :* $\forall x, y, z \in A,\ (x + y) \times z = x \times z + y \times z$ *et* $z \times (x + y) = z \times x + z \times y$.

Si le produit est commutatif, on dit que l'anneau est commutatif.

Remarques

1. Le fait que A possède un élément unité est un point essentiel de la notion d'anneau (certains anciens manuels parlent alors « d'anneaux unitaires ») ; actuellement un anneau « non unitaire » s'appelle un pseudo-anneau ; nous n'en considérerons pas.

2. Un ensemble G muni d'une seule loi de composition interne vérifiant les propriétés 1 à 4 de la définition 2.1 s'appelle un groupe commutatif (additif si la loi est notée additivement). Les groupes généraux font l'objet du cours « Groupes ». Dans ce cours nous rencontrerons essentiellement des groupes commutatifs qui du point de vue strict de la théorie des groupes sont moins subtils.
3. Bien que les définitions 2.1 soient générales, nous supposerons dès le 2.2 que les anneaux considérés sont commutatifs (c'est-à-dire que leur seconde loi elle aussi est commutative). On devra cependant observer les précautions élémentaires de calcul dans un anneau non commutatif (comme celui des matrices de type (n, n) à coefficients dans $\mathbb{C}$).

Notations

Somme de x et $y \in A$: $x + y$

Neutre de l'addition : 0 ou 0_A

Opposé de x : $-x$

Produit de x et y : xy

Élément unité : 1 ou 1_A. On n'impose pas d'avoir $1 \neq 0$; si $1 = 0$, alors $A = \{0\}$ (cf. proposition 2.2).

Proposition 2.2 *Soit A un anneau quelconque ; on a les propriétés suivantes :*

1. $0x = x0 = 0$, *pour tout* $x \in A$
2. $(-x)(-y) = xy$ *et* $(-x)y = x(-y) = -(xy)$, *pour tout* $x, y \in A$ *(règles des signes)*
3. *un élément* $x \in A$ *est dit inversible dans* A *s'il existe* $x' \in A$, *tel que* $xx' = x'x = 1$. *L'ensemble des éléments inversibles forme un groupe pour la multiplication (ce groupe est noté* $A^\times$*)*[1].

Démonstration

1. On a $(0+0)x = 0x = 0x+0x$, d'où $0x = 0$; de même, $x(0+0) = x0 = x0+x0$, d'où $x0 = 0$.
2. On a $xy + (-x)y = \Big(x + (-x)\Big)y = 0y = 0$, d'où $(-x)y = -(xy)$;
   de même, $xy + x(-y) = x\Big(y + (-y)\Big) = x0 = 0$; il en résulte que l'on a $(-x)(-y) = -\Big(x(-y)\Big) = -\Big(-(xy)\Big) = xy$.
3. Si x et y sont inversibles, il existe $x', y' \in A$ tels que $xx' = x'x = yy' = y'y = 1$. On a $xyy'x' = 1$ et $y'x'xy = 1$, donc xy est inversible (le produit sur A, restreint à $A^\times \times A^\times$, est une loi de composition sur $A^\times$) ; si x est inversible on vérifie que son inverse est unique (on le notera désormais x^{-1}) et est inversible (d'inverse x) ; enfin 1 est inversible et est l'élément neutre pour la loi ; $A^\times$ est donc bien un groupe multiplicatif (abélien si A est commutatif).

1. Ne pas confondre $A^\times$ avec $A - \{0\}$. En particulier $\mathbb{Z}^\times$ désigne $\{-1\ ;\ 1\}$!

Corollaire 2.3 (Ce qui se passe si $1 = 0$) *Si $1 = 0$ alors $A = \{0\}$ $(= \{1\})$ et $A^\times = A$.*

Définition 2.4 (Anneau intègre) *On dit que l'anneau A est intègre si $1 \neq 0$ et si chaque fois que $xy = 0$ alors $x = 0$ ou $y = 0$.*

Définition 2.5 (Corps) *Si un anneau commutatif A est tel que $1 \neq 0$ et tel que tout élément non nul est inversible, on dit que c'est un corps (dans le cas d'un corps, on a donc $1 \neq 0$ et $A^\times = A - \{0\}$).*

Définition 2.6 (Sous-anneau) *Soit A un anneau ; un sous-ensemble B de A est dit un sous-anneau de A si pour tout $x, y \in B$, $xy \in B$, si pour tout $x, y \in B$, $x - y \in B$, et enfin si $1 \in B$.*

Remarque On vérifie que B est un anneau pour la restriction des deux lois de composition aux éléments de B.

2.1.2 Un exemple fondamental : $A[X]$

Soit A un anneau commutatif. La construction de $A[X]$ étant supposée connue, elle ne sera pas rappelée ici. De même pour l'anneau des polynômes à plusieurs indéterminées : $A[X, Y]$, $A[X, Y, Z]$, ..., $A[X_1, \ldots, X_n]$. On rappelle que l'on peut faire cette construction de telle sorte que A soit un sous-anneau de $A[X]$.

Rappel des propriétés élémentaires des polynômes Soit A un anneau commutatif ; considérons $A[X]$. Tout $P \in A[X]$ s'écrit de façon unique $P = \sum_{i=0}^{N} a_i X^i$, $a_i \in A$, $N \geq 0$; pour simplifier, on écrit parfois $P = \sum_{i \geq 0} a_i X^i$, avec la convention $a_i = 0$ pour $i > N$ (ou, si l'on préfère, $a_i = 0$ pour tout i assez grand, ou encore : les a_i sont presque tous nuls).

On appelle degré de $P = \sum_{i \geq 0} a_i X^i \in A[X]$, l'indice $n \geq 0$, s'il existe, tel que $a_n \neq 0$ et $a_i = 0$ pour tout $i > n$. On a par exemple :

$$\text{degré}(P) = 0 \iff P = a, \qquad a \in A - \{0\}.$$

Si n n'existe pas, c'est que $P = 0$; dans ce cas on affecte au degré la valeur symbolique $-\infty$. On note $\mathrm{d}(P) \in \mathbb{N} \cup \{-\infty\}$ le degré de P. Si $n = \mathrm{d}(P) \neq -\infty$, on peut écrire $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$, avec $a_n \neq 0$; dans ce cas (i.e. $P \neq 0$), on dit que le coefficient **dominant** de P est a_n ; si $a_n = 1$, on dit que P est **unitaire.**

Proposition 2.7 (Propriétés du degré d'un polynôme)
On a les propriétés suivantes (pour tout P, $Q \in A[X]$) :

1. $\mathrm{d}(P + Q) \leq \max\Big\{\mathrm{d}(P), \mathrm{d}(Q)\Big\}$

   $\mathrm{d}(P + Q) = \max\Big\{\mathrm{d}(P), \mathrm{d}(Q)\Big\}$, *si* $\mathrm{d}(P) \neq \mathrm{d}(Q)$;

2. $\mathrm{d}(PQ) \leq \mathrm{d}(P) + \mathrm{d}(Q)$
pour P et Q non nuls, $\mathrm{d}(PQ) = \mathrm{d}(P) + \mathrm{d}(Q)$ *si le produit des coefficients dominants de P et Q est non nul*

(par définition, on a les règles suivantes d'opérations sur $\mathbb{N} \cup \{-\infty\}$ *:*
$-\infty + (-\infty) = -\infty$ *; pour tout* $n \in \mathbb{N}$, $n > -\infty$, $n + (-\infty) = -\infty$*).*

Division euclidienne généralisée dans $A[X]$

Proposition 2.8 (Division euclidienne dans $A[X]$) *Soient U, $V \in A[X]$; on suppose V non nul et de coefficient dominant* ***inversible*** *dans A. Alors il existe des polynômes Q et R de $A[X]$, uniques, tels que l'on ait : $U = VQ + R$, avec* $\mathrm{d}(R) < \mathrm{d}(V)$ *dans* $\mathbb{N} \cup \{-\infty\}$.

Démonstration On pose $V = b_m X^m + \cdots + b_1 X + b_0$, $m \geq 0$, $b_m \in A^\times$. On fait la démonstration par récurrence sur le degré n de U, avec m fixé :

Pour les $n \in \mathbb{N} \cup \{-\infty\}$, tels que $n < m$, il suffit de prendre $Q = 0$ et $R = U$. On peut donc considérer que le premier pas de la récurrence est montré pour au moins une valeur de $n \in \mathbb{N} \cup \{-\infty\}$, puisque $m \neq -\infty$ par hypothèse.

On admet la propriété pour tous les polynômes U de degré majoré strictement par n, avec ici $n \geq m$, et on pose $U = a_n X^n + \cdots + a_1 X + a_0$; on considère alors :

$$\begin{aligned} U' &= U - a_n b_m^{-1} X^{n-m} V \\ &= a_n X^n + \cdots + a_1 X + a_0 - a_n b_m^{-1} X^{n-m}(b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0) \\ &= a_n X^n + \cdots + a_1 X + a_0 - a_n X^n - a_n b_m^{-1} b_{m-1} X^{n-1} - \cdots - a_n b_m^{-1} b_0 \end{aligned}$$

Le polynôme U' est de degré $< n$: il existe donc Q' et R' tels que $U' = VQ' + R'$, $\mathrm{d}(R') < \mathrm{d}(V)$ (hypothèse de récurrence) et

$$U = U' + a_n b_m^{-1} X^{n-m} V = V(Q' + a_n b_m^{-1} X^{n-m}) + R' \ .$$

On a bien le résultat en prenant $Q = Q' + a_n b_m^{-1} X^{n-m}$ et $R = R'$.

L'unicité est immédiate :
si l'on suppose $U = VQ + R = VQ' + R'$, avec $\mathrm{d}(R) < \mathrm{d}(V)$ et $\mathrm{d}(R') < \mathrm{d}(V)$, alors $V(Q - Q') = R' - R$, et on a $\mathrm{d}(R' - R) \leq \max(\mathrm{d}(R), \mathrm{d}(R')) < \mathrm{d}(V)$ par hypothèse ; mais par ailleurs, on a $\mathrm{d}(R' - R) = \mathrm{d}(V(Q - Q'))$ et ici le coefficient dominant de V est inversible.

Si l'on suppose $Q - Q' \neq 0$, le produit des coefficients dominants de V et de $Q - Q'$ n'est pas nul (le vérifier), et on a $\mathrm{d}(V(Q - Q')) = \mathrm{d}(V) + \mathrm{d}(Q - Q')$ (proposition 2.7 page 17), soit, avec ce qui précède :

$$\mathrm{d}(V) + \mathrm{d}(Q - Q') < \mathrm{d}(V)$$

ceci est absurde car, comme on a $V \neq 0$, et que $Q - Q'$ a été supposé non nul, cette inégalité est dans $\mathbb{N}$. D'où $Q = Q'$ et $R = R'$.

Remarque En général, on ne peut pas en déduire un algorithme d'Euclide si A n'est pas un corps.

Exemple $U = X^3 + 3X^2 + 5X + 1$ et $V = X^2 + 2$ dans $\mathbb{Z}[X]$; on trouve alors $U = (X+3)(X^2+2) + 3X - 5$, mais il n'y a plus de division euclidienne de X^2+2 par $3X - 5$ car 3 n'est pas inversible dans $\mathbb{Z}$.

2.2 Idéal d'un anneau commutatif

Définition 2.9 (Idéal) *Soit A un anneau commutatif. On appelle idéal de A toute partie $\mathfrak{a}$ de A qui a les propriétés suivantes :*

1. *$\mathfrak{a}$ est un sous-groupe additif de A ; c'est-à-dire $\mathfrak{a} \neq \emptyset$ et pour tout $x, y \in \mathfrak{a}$ on a $x - y \in \mathfrak{a}$.*
2. *Pour tout $a \in A$ et tout $x \in \mathfrak{a}$ alors $ax \in \mathfrak{a}$*

Remarques

1. Pour qu'un idéal $\mathfrak{a}$ soit un sous-anneau de A, il faut que $1 \in \mathfrak{a}$; or si $1 \in \mathfrak{a}$, alors $a1 = a \in \mathfrak{a}$ pour tout $a \in A$, donc $\mathfrak{a} = A$ (et c'est le seul cas).
2. L'ensemble $\{0\}$ est un idéal de A appelé l'idéal nul.

Définition 2.10 (Idéal engendré par une partie P de A) *Si $\mathcal{A} \neq \emptyset$ est un ensemble non vide d'idéaux de A, alors on vérifie que l'intersection de ces idéaux, $\bigcap_{\mathfrak{a} \in \mathcal{A}} \mathfrak{a}$, est un idéal de A (le vérifier). On a donc une notion d'idéal engendré par une partie P : on appelle idéal de A engendré par $P \subseteq A$, l'idéal $\bigcap_{\mathfrak{a} \supseteq P,\, \mathfrak{a} \text{ idéal de } A} \mathfrak{a}$ qui est noté (P) (autrement dit, on prend ici pour $\mathcal{A}$ l'ensemble des idéaux $\mathfrak{a}$ de A qui contiennent P ; cet ensemble $\mathcal{A}$ est bien non vide puisque $A \in \mathcal{A}$).*

Proposition 2.11 (Caractérisation d'un idéal engendré par une partie)

$$(P) = \left\{ \sum_{i=1}^{n} a_i x_i,\ n \geq 0,\ x_i \in P,\ a_i \in A \right\}$$

(sommes finies quelconques de n termes ($n \geq 0$) de la forme $a_i x_i$, $x_i \in P$, $a_i \in A$).

Démonstration Soit $\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i x_i,\ n \geq 0,\ x_i \in P,\ a_i \in A \right\}$. Si $x \in P$, $x = 1x \in \mathfrak{b}$, donc $P \subseteq \mathfrak{b}$. Montrons alors que $\mathfrak{b}$ est un idéal de A :

si $x,\ y \in \mathfrak{b}$, on peut écrire $x = \sum_{i=1}^{n} a_i x_i$ et $y = \sum_{j=1}^{m} a'_j x'_j$, $n,\ m \geq 0$, $x_i,\ x'_j \in P$, $a_i,\ a'_j \in A$; il est clair que $x + y$ est de la forme voulue et est donc dans $\mathfrak{b}$; on a $-x = -\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (-a_i) x_i$ (règle des signes) $\in \mathfrak{b}$; enfin 0 s'écrit comme somme de zéro termes. Si $x \in \mathfrak{b}$ et si $a \in A$ alors $ax = a \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (aa_i) x_i \in \mathfrak{b}$. On

a donc montré l'inclusion $(P) \subseteq \mathfrak{b}$, car $\mathfrak{b}$ est un idéal contenant P $\Big($autrement dit, $\mathfrak{b} \in \mathcal{A}$, soit $\bigcap_{\mathfrak{a}\in\mathcal{A}} \mathfrak{a} \subseteq \mathfrak{b}\Big)$.

L'inclusion opposée est immédiate par définition d'un idéal (expliciter les détails).

Remarques

1. Si P est finie, $P = \{\alpha_1, \ldots, \alpha_r\}$; on déduit du résultat précédent que (P) est égal à $\{a_1\alpha_1 + \cdots + a_r\alpha_r, a_i \in A\}$, ce que l'on peut écrire sous la forme $(P) = A\alpha_1 + \cdots + A\alpha_r$; en pratique on écrit aussi $(P) = \alpha_1 A + \cdots + \alpha_r A$, mais ceci est moins correct bien que consacré par l'usage [2] (dans $\mathbb{Z}$ notamment, ainsi que dans les anneaux « numériques »).
2. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A, on note $\mathfrak{a}+\mathfrak{b}$ l'idéal engendré par $\mathfrak{a}$ et $\mathfrak{b}$. On a $\mathfrak{a}+\mathfrak{b} = \{a+b, a \in \mathfrak{a},\ b \in \mathfrak{b}\}$ (se déduit immédiatement de la proposition 2.11). La notation $\mathfrak{a} + \mathfrak{b}$ désigne aussi (en notation additive) le sous-groupe de A engendré $\mathfrak{a}$ et $\mathfrak{b}$: il se trouve que si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux de A, le sous-groupe de A engendré par $\mathfrak{a}$ et $\mathfrak{b}$ est aussi un idéal de A.

Définition 2.12 (Idéal principal) *On dit qu'un idéal $\mathfrak{a}$ est principal s'il est engendré par $P = \{\alpha\}$, $\alpha \in A$ (on écrit alors $\mathfrak{a} = (\alpha) = A\alpha = \alpha A$).*

Exemples

1. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau où tout idéal est principal : en effet, soit $\mathfrak{a}$ un idéal de $\mathbb{K}[X]$; on peut supposer $\mathfrak{a} \neq (0)$ car l'idéal nul est engendré par 0. Étant non nul, $\mathfrak{a}$ possède au moins un élément $Q \neq 0$ de degré minimum d (dans $\mathbb{N}$) parmi tous les éléments non nuls de $\mathfrak{a}$. Montrons qu'on a $\mathfrak{a} = (Q)$; l'inclusion $(Q) \subseteq \mathfrak{a}$ étant évidente, prenons $P \in \mathfrak{a}$ et considérons la division euclidienne de P par Q dans $\mathbb{K}[X]$: $P = QS + R$, $\mathrm{d}(R) < d$; comme $R = P - QS$ et que $P, Q \in \mathfrak{a}$, on a $R \in \mathfrak{a}$; si l'on avait $R \neq 0$, R serait un élément non nul de $\mathfrak{a}$ de degré $< d$, ce qui est contraire à la définition de d. Donc $R = 0$, et $P = QS \in (Q)$ (i.e. $\mathfrak{a} \subseteq (Q)$).
2. Idéaux de $\mathbb{Z}$. La même démonstration que ci-dessus en remplaçant la division euclidienne des polynômes par la division euclidienne de $\mathbb{Z}$ montre que les idéaux de $\mathbb{Z}$ sont principaux. Comme pour tout entier n on a l'égalité $n\mathbb{Z} = -n\mathbb{Z}$ les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Plus généralement un anneaux dans lequel on peut faire une division euclidienne est dit **euclidien**. Cette preuve démontre que les idéaux des anneaux euclidiens sont principaux.

2.2.1 Inversibles et idéaux

Proposition 2.13 (Idéal égal à l'anneau) *Un idéal $\mathfrak{a}$ de A est égal à A tout entier si et seulement si $\mathfrak{a}$ contient un élément inversible de l'anneau.*

2. C'est correct à cause de la commutativité de A ; dans le cas contraire aA et Aa peuvent être distincts (notions d'idéaux à droite, d'idéaux à gauche et d'idéaux bilatères, non évoquées ici)

Démonstration Si $\mathfrak{a} = A$, $\mathfrak{a}$ contient 1 qui est inversible.

Si $\mathfrak{a}$ contient $u \in A^\times$, alors, en considérant $u^{-1} \in A$, $u^{-1}u \in \mathfrak{a}$ par définition d'un idéal ; donc $1 \in \mathfrak{a}$ et on sait que cela entraîne $\mathfrak{a} = A$.

Corollaire 2.14 (Idéaux d'un corps) *Si A est un corps, alors l'ensemble des idéaux de A est constitué des deux idéaux distincts* (0) *et A.*

En effet, si $\mathfrak{a}$ est un idéal non nul de A, $\mathfrak{a}$ contient un élément $a \neq 0$; or cet élément est inversible par définition d'un corps.

2.2.2 Idéaux premiers et maximaux

Définition 2.15 (Idéal premier. Idéal maximal.) *Soit A un anneau commutatif ; on appelle :*

1. *idéal **premier**, tout idéal $\mathfrak{p}$ de A tel que $\mathfrak{p} \neq A$ et tel que pour tout $x, y \in A$ vérifiant $xy \in \mathfrak{p}$, alors x ou y est dans $\mathfrak{p}$;*
2. *idéal **maximal**, tout idéal $\mathfrak{m}$ de A tel que $\mathfrak{m} \neq A$ et tel que tout idéal $\mathfrak{a}$ intermédiaire entre $\mathfrak{m}$ et A (i.e. $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$) est nécessairement égal à $\mathfrak{m}$ ou à A.*

Théorème 2.16 (Théorème de Krull) *Soit A un anneau commutatif, alors tout idéal $\mathfrak{a}$ distinct de A est contenu dans un idéal maximal de A.*

Démonstration C'est une conséquence immédiate du lemme de Zorn qui lui-même est équivalent à l'axiome du choix. Ces notions de théorie des ensembles ne sont pas développées dans ce cours. On propose donc au lecteur d'admettre ce résultat qui est l'application de l'axiome du choix la plus utile dans la théorie des anneaux. Les étudiants qui sont intéressés par ces questions ensemblistes peuvent consulter avec profit le premier chapitre du livre de G. et M.-N. Gras « Algèbre fondamentale Arithmétique » de la bibliographie.

Remarques

1. Si $\mathbb{K}$ est un corps, son seul idéal maximal est (0).
2. L'anneau $\{0\}$ est le seul anneau à ne pas avoir d'idéaux maximaux.

Corollaire 2.17 (Une caractérisation de $A^\times$) *Soit A un anneau commutatif et soit U le complémentaire dans A de la réunion de tous les idéaux maximaux de A. Alors $U = A^\times$.*

En effet, soit $x \in A^\times$, il est clair que x n'est contenu dans aucun idéal maximal. Inversement, soit $x \in U$, x supposé non inversible ; alors $Ax \neq A$ (car $1 \notin Ax$) et Ax est contenu dans un idéal maximal, d'après le théorème de Krull, ce qui est absurde ($x \in U$). Donc $x \in A^\times$.

2.3 Homomorphismes et quotients d'anneaux (cas commutatif)

2.3.1 Homomorphismes

Définition 2.18 (Homomorphisme d'anneaux) *Soient A et B deux anneaux. Une application h de A dans B est un* ***homomorphisme*** *d'anneaux si les trois conditions suivantes sont réalisées :*

1. *h est un homomorphisme de groupes additifs (i.e. $h(a+b) = h(a)+h(b)$, pour tout $a, b \in A$),*
2. *$h(ab) = h(a)h(b)$, pour tout $a, b \in A$,*
3. *$h(1_A) = 1_B$ (1_A et 1_B désignent les éléments unités respectifs de A et B).*

Un ***isomorphisme*** *d'anneaux est un homomorphisme d'anneaux bijectif.*

Définition 2.19 (Noyau d'un homomorphisme) *Soit $h\colon A \longrightarrow B$ un homomorphisme d'anneaux. On appelle* ***Noyau*** *de h et on note $\mathrm{Ker}(h)$ le sous-ensemble de A image réciproque de $\{0\}$ par h, autrement dit*

$$\mathrm{Ker}(h) = \{a \in A, h(a) = 0\}.$$

Théorème 2.20 *Le noyau d'un homomorphisme $h : A \longrightarrow B$ est un idéal de A.*

Démonstration Pour commencer $0_A \in \mathrm{Ker}(h) = \{a \in A,\ h(a) = 0_B\}$, donc $\mathrm{Ker}(h) \neq \emptyset$. Puis si $x, y \in \mathrm{Ker}(h)$ alors $h(x-y) = h(x) - h(y) = 0_B$, donc $(x-y) \in \mathrm{Ker}(h)$ ce qui démontre que $\mathrm{Ker}(h)$ est un sous-groupe de A. Soit alors $b \in A$, et soit $a \in \mathrm{Ker}(h)$; alors $h(ab) = h(a)h(b) = 0_B h(b) = 0_B$, donc $ab \in \mathrm{Ker}(h)$ qui est donc un idéal.

Corollaire 2.21 *Si h est un homomorphisme d'un corps $\mathbb{K}$ dans un anneau B tel que $1_B \neq 0_B$, alors h est injectif et $\mathrm{Im}(h)$ est un sous-corps de B (i.e. un sous-anneau qui est un corps).*

En effet, $\mathrm{Ker}(h) = (0_{\mathbb{K}})$ ou $\mathbb{K}$ (les seuls idéaux d'un corps) ; comme $h(1_{\mathbb{K}}) = 1_B$ et que l'on a $1_B \neq 0_B$, $1_{\mathbb{K}} \notin \mathrm{Ker}(h)$, et de ce fait la seule possibilité est $\mathrm{Ker}(h) = (0_{\mathbb{K}})$, donc h est injectif.

Remarques

- L'image d'un homomorphisme d'anneaux $h : A \longrightarrow B$ est un sous-anneau de B (le démontrer).
- h est injectif si et seulement si $\mathrm{Ker}(h) = (0)$: ceci est déjà impliqué par la structure de groupe. En effet si h est injectif le seul antécédent pour h de 0_B est 0_A donc $\mathrm{Ker}(h) = (0_A)$. Réciproquement si $\mathrm{Ker}(h) = (0)$ et si $x, y \in A$ vérifient $h(x) = h(y)$ alors $h(x-y) = 0$ et donc $(x-y) \in \mathrm{Ker}(h)$, puis $x = y$.

Proposition 2.22 *Soit $h : A \longrightarrow B$ un homomorphisme d'anneaux ; alors la restriction de h à $A^\times$ est un homomorphisme de groupes de $A^\times$ dans $B^\times$.*

Démonstration Si $a \in A^\times$, on peut écrire $aa^{-1} = 1_A$ donc $h(aa^{-1}) = h(1_A) = 1_B$, soit $h(a)h(a^{-1}) = 1_B$, ce qui fait que $h(a) \in B^\times$ (son inverse, que l'on doit donc noter $h(a)^{-1}$, est $h(a^{-1})$) ; on vérifie que la restriction de h à $A^\times$ est un homomorphisme de groupes multiplicatifs.

Proposition 2.23 *Soit $h : A \longrightarrow B$ un isomorphisme d'anneaux de A sur B ; alors l'application réciproque $h^{-1} : B \longrightarrow A$ est un isomorphisme d'anneaux.*

Démonstration Soit $b, b' \in B$. Comme h est surjective il existe $a, a' \in A$ tels que $h(a) = a$ et $h(a') = b'$. Il suit $h^{-1}(b + b') = h^{-1}(h(a) + h(a')) = h^{-1}(h(a + a')) = a + a'$; car h est un morphisme de groupe. Mais comme h et h^{-1} sont des bijections réciproques on a $a = h^{-1}(b)$ et $a' = h^{-1}(b')$ et cela démontre que h^{-1} est un morphisme de groupe. On vérifie exactement de la même façon que $h^{-1}(bb') = aa'$. Comme $h(1_A) = 1_B$ on a $h^{-1}(1_B) = 1_A$. Donc h^{-1} est un morphisme d'anneaux.

2.3.2 Quotients

La notion de quotient est essentielle à l'algèbre et intervient pour toutes les structures usuelles. Étant donné un anneau A on peut décrire, à isomorphismes près, tous les anneaux images de A par un homomorphisme d'anneaux à partir des seuls idéaux de A. En effet un tel anneau image est isomorphe à l'anneau quotient de A par le noyau de l'homomorphisme considéré. On va définir et étudier ces notions.

Théorème 2.24 *Soit A un anneau commutatif, et soit $\mathfrak{a}$ un idéal de A. Alors il existe un anneau A' et un homomorphisme d'anneaux h de A dans A' tels que* $\mathrm{Ker}(h) = \mathfrak{a}$.

Démonstration L'idéal $\mathfrak{a}$ permet de définir la relation de congruence modulo $\mathfrak{a}$ sur l'ensemble A par la formule $x \equiv y\ \mathfrak{a} \iff x - y \in \mathfrak{a}$. C'est clairement une relation d'équivalence. Considérons l'ensemble quotient des classes d'équivalence pour cette relation de congruence, notons-le $A/\mathfrak{a}$, et soit q la projection canonique de A sur $A/\mathfrak{a}$. Montrons que l'on peut définir sur $A/\mathfrak{a}$ l'addition et la multiplication des classes X et Y par $X + Y = q(x + y)$ et $XY = q(xy)$, pour $x \in X$, $y \in Y$; pour cela, il faut vérifier que chacune de ces définitions sont indépendantes du choix des représentants x et y :

si $x' \equiv x\ \mathfrak{a}$ et $y' \equiv y\ \mathfrak{a}$, on a $x' - x \in \mathfrak{a}$ et $y' - y \in \mathfrak{a}$, soit $x' = x + a$, $y' = y + b$, $a, b \in \mathfrak{a}$. On a alors pour l'addition $x' + y' = x + a + y + b = x + y + a + b$ et pour la multiplication $x'y' = (x + a)(y + b) = xy + xb + ya + ab$; or les derniers termes $a + b$ et $xb + ya + ab$ sont dans $\mathfrak{a}$, donc $x' + y' \equiv x + y\ \mathfrak{a}$ et $x'y' \equiv xy\ \mathfrak{a}$.

On vérifie que $\bar{0} = \mathfrak{a}$ est neutre pour cette addition, l'associativité et la commutativité de cette addition, le fait que $q(-a)$ est l'opposée de $q(a)$ pour cette addition, l'associativité de ce produit, le fait que $q(1)$ est l'élément unité dans $A/\mathfrak{a}$, et enfin la distributivité du produit par rapport à l'addition dans $A/\mathfrak{a}$.

Par construction q est bien un homomorphisme d'anneaux, $\mathrm{Ker}(q) = \mathfrak{a}$, et en outre q est surjectif.

Corollaire 2.25 (Image de $A^\times$) *L'image par $q : A \longrightarrow A/\mathfrak{a}$, de $A^\times$, est un sous-groupe de $(A/\mathfrak{a})^\times$.*

Remarque Il existe une unique structure d'anneau sur l'ensemble quotient $A/\mathfrak{a}$, telle que $q : A \longrightarrow A/\mathfrak{a}$ soit un homomorphisme d'anneaux. On appelle $A/\mathfrak{a}$ l'anneau quotient de A par $\mathfrak{a}$ et q s'appelle encore l'homomorphisme canonique. Enfin, si $\sim$ est une relation d'équivalence sur A, il existe sur $A/\sim$ une structure d'anneau telle que q soit un homomorphisme d'anneaux, si et seulement si $\sim$ est la relation d'équivalence associée à l'idéal de A noyau de q (le vérifier). Cette remarque justifie *a posteriori* le point de départ de la démonstration du théorème.

Définition 2.26 (Écriture congruentielle.) *Soit $\mathfrak{a}$ un idéal de A ; pour a, $b \in A$), on écrit souvent $a \equiv b \bmod \mathfrak{a}$ (qui signifie donc $a - b \in \mathfrak{a}$). On a alors les règles suivantes qui traduisent les propriétés de l'homomorphisme d'anneaux q : si $a \equiv b \bmod \mathfrak{a}$ et $a' \equiv b' \bmod \mathfrak{a}$, alors $a \pm a' \equiv b \pm b' \bmod \mathfrak{a}$ et $aa' \equiv bb' \bmod \mathfrak{a}$*

Écrire les détails afin de s'habituer au calcul congruentiel qui sera indispensable ultérieurement.

2.3.3 Théorème de factorisation des homomorphismes

Théorème 2.27 (Diagramme commutatif) *Soit $h : A \longrightarrow B$ un homomorphisme d'anneaux commutatifs et soit $\mathfrak{a}$ un idéal de A* ***contenu dans*** $\mathbf{Ker}(h)$*. Alors, il existe un unique homomorphisme d'anneaux h^* de $A/\mathfrak{a}$ dans B tel que le diagramme suivant soit commutatif (i.e. $h = h^* \circ q$) :*

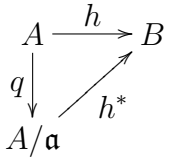

Figure 2.1 : Diagramme commutatif

Démonstration L'hypothèse $\mathfrak{a} \subset \mathrm{Ker}(h)$ permet de définir l'homomorphisme h^*. En effet soit $x \in A$ et soit $x+\mathfrak{a}$ sa classe de congruence. Alors l'ensemble image directe $h(x + \mathfrak{a})$ est réduit au singleton $\{h(x)\}$ parce que h est compatible avec l'addition et que $h(\mathfrak{a}) \subset h(\mathrm{Ker}(h)) = (0)$. Ainsi la formule $X \mapsto h(x)$ pour tout $x \in X$ donne une application bien définie $h^* : A/\mathfrak{a} \longrightarrow B$. D'autre part la commutativité du diagramme qui revient à $h = q \circ h^*$ force à définir h^* par cette formule : on doit avoir $h^*(q(x)) = h(x)$. Cela donne l'existence et l'unicité de l'application h^* faisant commuter le diagramme. Il reste à s'assurer que h^* est un homomorphisme d'anneaux. On a

$$\begin{aligned}
h^*\Big(q(x) + q(y)\Big) &= h^*\Big(q(x+y)\Big) \qquad \text{(définition de l'addition dans } A/\mathfrak{a}) \\
h^*\Big(q(x+y)\Big) &= h(x+y) \qquad (\text{car } h^* \circ q = h) \\
h(x+y) &= h(x) + h(y) \qquad (h \text{ homomorphisme d'anneaux}) \\
h(x) + h(y) &= h^*\Big(q(x)\Big) + h^*\Big(q(y)\Big)
\end{aligned}$$

donc $h^*\Big(q(x)+q(y)\Big) = h^*\Big(q(x)\Big) + h^*\Big(q(y)\Big)$ et h^* est compatible avec l'addition. On a

$$\begin{aligned} h^*\Big(q(x)q(y)\Big) &= h^*\Big(q(xy)\Big) \qquad \text{(définition du produit dans } A/\mathfrak{a}) \\ h^*\Big(q(xy)\Big) &= h(xy) \qquad (\text{car } h^* \circ q = h) \\ h(xy) &= h(x)h(y) \qquad (h \text{ homomorphisme d'anneaux}) \\ h(x)h(y) &= h^*\Big(q(x)\Big)h^*\Big(q(y)\Big) \end{aligned}$$

donc $h^*\Big(q(x)q(y)\Big) = h^*\Big(q(x)\Big)h^*\Big(q(y)\Big)$; enfin, $h^*\Big(q(1_A)\Big) = h(1_A) = 1_B$.

Corollaire 2.28 (Isomorphisme canonique d'anneaux) *Si* $\mathfrak{a} = \mathrm{Ker}(h)$, *alors on a l'isomorphisme canonique d'anneaux*

$$A/\operatorname{Ker}(h) \simeq \operatorname{Im}(h).$$

Démonstration Soit $x \in A$ tel que $q(x) \in \operatorname{Ker} h^*$. Alors par construction $x \in \operatorname{Ker}(h)$ et donc $x \in \mathfrak{a}$ d'où $q(x) = 0$. Il suit h^* injectif. Par construction aussi l'image de h^* est égale à l'image de h.

Exemple Les anneaux $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{Z}$: comme $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau (anneau des « entiers modulo n ») ; si $n = 0$, $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$, si $n = 1$, $\mathbb{Z}/\mathbb{Z} \simeq \{0\}$. Dans les autres cas, on obtient l'anneau fini ayant $|n| \geq 2$ éléments étudié en section 1.3.

Théorème 2.29 ($\mathbb{Z}/p\mathbb{Z}$ si p premier) *Si* p *est premier, alors* $\mathbb{Z}/p\mathbb{Z}$ *est un corps.*

Démonstration On considère, pour $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ fixé, $\overline{a} \neq \overline{0}$, l'application $\overline{x} \longmapsto \overline{a}\,\overline{x}$ de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même ; si $\overline{a}\,\overline{x} = \overline{a}\,\overline{y}$, ceci implique $a(x-y) \equiv 0 \bmod p$; comme $\overline{a} \neq \overline{0}$, $p \nmid a$, donc $p|(x-y)$ (lemme d'Euclide 1.8) et $\overline{x} = \overline{y}$: cette application est injective, donc surjective puisque $\mathbb{Z}/p\mathbb{Z}$ est fini, et il existe $\overline{x_0}$ tel que $\overline{a}\,\overline{x_0} = \overline{1}$. Ainsi tout $\overline{a} \neq \overline{0}$ est inversible, et $\mathbb{Z}/p\mathbb{Z}$ est un corps (noté $\mathbb{F}_p$).

Remarque S'interdire la notation $\mathbb{Z}_n$ pour l'anneau $\mathbb{Z}/n\mathbb{Z}$; elle est malheureusement utilisée dans certains ouvrages ; or pour $n = p$ premier, $\mathbb{Z}_p$ désigne « l'anneau des entiers p-adiques », et $\mathbb{Z}_{(p)}$ désigne « le localisé en p » de l'anneau $\mathbb{Z}$.

2.3.4 Caractérisation des idéaux premiers, maximaux

Passons maintenant à une caractérisation de premier et maximal, en termes de quotients :

Théorème 2.30 *Soit* A *un anneau commutatif, et soit* $\mathfrak{a}$ *un idéal de* A *:*

1. $\mathfrak{a}$ *est premier si et seulement si* $A/\mathfrak{a}$ *est intègre ;*
2. $\mathfrak{a}$ *est maximal si et seulement si* $A/\mathfrak{a}$ *est un corps.*

Démonstration

1. Supposons $\mathfrak{a}$ premier. On a $\mathfrak{a} \neq A$, donc $A/\mathfrak{a} \neq \{q(0)\}$; soient $q(x), q(y) \in A/\mathfrak{a}$ tels que $q(x)q(y) = q(0)$; alors $q(xy) = q(0)$ et $xy \in \mathfrak{a}$; par définition x ou y est dans $\mathfrak{a}$, autrement dit $q(x) = q(0)$ ou $q(y) = q(0)$, et ceci démontre que $A/\mathfrak{a}$ est intègre. Inversement, si $A/\mathfrak{a}$ est intègre, on a $\mathfrak{a} \neq A$ et si l'on suppose que $xy \in \mathfrak{a}$ $(x, y \in A)$, alors $q(xy) = q(0)$ soit $q(x)q(y) = q(0)$, qui implique $q(x) = q(0)$ ou $q(y) = q(0)$, soit $x \in \mathfrak{a}$ ou $y \in \mathfrak{a}$, et $\mathfrak{a}$ est premier.
2. Supposons $\mathfrak{a}$ maximal. On a $\mathfrak{a} \neq A$, donc $A/\mathfrak{a} \neq \{q(0)\}$. Soit $q(x) \neq q(0)$ dans $A/\mathfrak{a}$; on a $x \notin \mathfrak{a}$ et l'idéal $\mathfrak{a}+Ax$ est donc égal à A, et on peut écrire $1 = y+ax$, $y \in \mathfrak{a}$, $a \in A$, d'où $q(1) = q(ax) = q(a)q(x)$ et $q(x)$ est inversible ; donc $A/\mathfrak{a}$ est un corps. Inversement, si $A/\mathfrak{a}$ est un corps, on a aussi $\mathfrak{a} \neq A$; soit $\mathfrak{b}$ un idéal de A tel que $\mathfrak{a} \subsetneqq \mathfrak{b} \subseteq A$; montrons que $\mathfrak{b} = A$. Soit $b \in \mathfrak{b} - \mathfrak{a}$; on a $q(b) \neq q(0)$, donc $q(b)$ est inversible et il existe $a \in A$ tel que $q(a)q(b) = q(1)$, soit $ab = 1 + c$, $c \in \mathfrak{a}$, puis $1 = ab - c \in \mathfrak{b}$, d'où $\mathfrak{b} = A$.

Corollaire 2.31 (Idéal (0)) *Dans un anneau A, l'idéal (0) est premier si et seulement si l'anneau est intègre, et maximal si et seulement si l'anneau est un corps.*

En effet, on a $A/(0) \simeq A$.

Corollaire 2.32 *Un idéal maximal est un idéal premier.*

En effet, un corps est intègre.

2.4 Anneaux de polynômes

On va établir une propriété « universelle » des anneaux $A[X]$, à savoir que tous les homomorphismes d'anneaux $A[X] \longrightarrow B$ peuvent se décrire très simplement :

Théorème 2.33 (Prolongement des homomorphismes à $A[X]$)
Soit $A[X]$ l'anneau des polynômes à coefficients dans l'anneau commutatif A. Soit B un anneau quelconque. On suppose donnés :

1. *un élément $\beta \in B$ quelconque,*
2. *un homomorphisme d'anneaux f de A dans B quelconque.*

Alors il existe un homomorphisme h et un seul de $A[X]$ dans B, tel que h prolonge f et tel que $h(X) = \beta$. [3]

Tout homomorphisme d'anneaux h de $A[X]$ dans B est obtenu de cette manière.

3. Si B n'était pas commutatif, il faudrait rajouter la condition supplémentaire que β commute aux éléments de $f(A)$.

Démonstration

1. Construction de h. Soit $P = \sum_{i\geq 0} a_i X^i$, $a_i \in A$; on associe à P l'expression $\sum_{i\geq 0} f(a_i)\beta^i$ (c'est un élément de B : d'une part cette somme a un sens car $f(a_i) = 0$ pour tout i assez grand et, d'autre part, $f(a_i)\beta^i \in B$ pour tout i) ; les coefficients a_i d'un polynôme étant uniques, on a bien **défini** une application, que l'on appelle h.

   Vérifions que h est un homomorphisme : soient $P = \sum_{i\geq 0} a_i X^i$ et $Q = \sum_{i\geq 0} b_i X^i$; alors :

$$\begin{aligned} h(P+Q) &= h\left(\sum_{i\geq 0}(a_i+b_i)X^i\right) && \text{(définition de + dans } A[X]) \\ &= \sum_{i\geq 0} f(a_i+b_i)\beta^i && \text{(définition de } h) \\ &= \sum_{i\geq 0}(f(a_i)+f(b_i))\beta^i && (f \text{ est un homomorphisme}) \\ &= \sum_{i\geq 0} f(a_i)\beta^i + \sum_{i\geq 0} f(b_i)\beta^i \\ &= h(P)+h(Q). \end{aligned}$$

   Calculons $h(PQ)$:

$$\begin{aligned} h(PQ) &= h\left[\left(\sum_{i\geq 0} a_i X^i\right)\left(\sum_{j\geq 0} b_j X^j\right)\right] \\ &= h\left(\sum_{i,j\geq 0} a_i b_j X^{i+j}\right), \end{aligned}$$

   par définition du produit dans $A[X]$ et propriétés des sommations : attention, les indices de sommation étant « muets », ils doivent être pris distincts dans les sommations multiples ; on en déduit en calculant le coefficient de chaque monôme X^k (ce calcul est nécessaire car h n'est défini que pour un polynôme

« bien écrit ») :

$$\begin{aligned}
h(PQ) &= h\left[\sum_{k\geq 0}\left(\sum_{i,j,i+j=k} a_i b_j\right) X^k\right] \\
&= \sum_{k\geq 0} f\left(\sum_{i,j,i+j=k} a_i b_j\right)\beta^k \\
&= \sum_{k\geq 0}\left(\sum_{i,j,i+j=k} f(a_i)f(b_j)\right)\beta^k \quad (f \text{ est un homomorphisme}) \\
&= \sum_{k\geq 0}\sum_{i,j,i+j=k} f(a_i)f(b_j)\beta^{i+j} \qquad (\text{distributivité dans } B) \\
&= \sum_{k\geq 0}\sum_{i,j,i+j=k} f(a_i)\beta^i f(b_j)\beta^j \qquad (\text{commutativité dans } B)^{\,4} \\
&= \sum_{i,j\geq 0} f(a_i)\beta^i f(b_j)\beta^j \ .
\end{aligned}$$

Cette somme sur i, j est le produit développé dans B de $\sum_{i\geq 0} f(a_i)\beta^i$ par $\sum_{j\geq 0} f(b_j)\beta^j$. Cela démontre

$$h(PQ) = h(P)h(Q) \ .$$

Enfin on a $h(1_A) = f(1_A) = 1_B$.

On a donc bien un homomorphisme d'anneaux tel que la restriction à A vérifie $h(a) = f(a)$ pour tout $a \in A$ (en effet a est le polynôme constant $a + 0X + 0X^2 + \cdots$), et tel que $h(X) = \beta$ (X est le polynôme $0 + 1X + 0X^2 + \cdots$). Ceci assure l'unicité de h lorsque f et β sont donnés.

2. Soit maintenant h un homomorphisme d'anneaux quelconque de $A[X]$ dans B. Pour montrer que h est de la forme précédente, il suffit de trouver f et β. Il est clair qu'il suffit, d'une part, de poser $h(X) = \beta$, et, d'autre part, de remarquer que la restriction f de h à $A \subset A[X]$ est un homomorphisme d'anneaux de A dans B. En pratique, on représente un tel homomorphisme $h : A[X] \longrightarrow B$ par les quantités f et β qui le définissent, sous la forme symbolique :

$$\begin{array}{ccc}
A[X] & \longrightarrow & B \\
a \in A & \longmapsto & f(a) \\
X & \longmapsto & \beta \quad (\text{en explicitant } f(a) \text{ et } \beta).
\end{array}$$

Cas particuliers

1. Évaluation. C'est le cas où A est un sous-anneau de B et où f est l'identité sur A :

$$\begin{array}{ccc}
A[X] & \longrightarrow & B \\
a \in A & \longmapsto & a \\
X & \longmapsto & \beta
\end{array}$$

dans ce cas, $h(P)$ se note $P(\beta)$ et s'appelle l'homomorphisme d'évaluation en $\beta \in B$.

2. Réduction modulo un idéal $\mathfrak{a}$ de A. Dans ce cas, $B = A/\mathfrak{a}[X]$ et $f = q : A \longrightarrow A/\mathfrak{a}$:

$$\begin{array}{ccc} A[X] & \longrightarrow & A/\mathfrak{a}[X] \\ a \in A & \longmapsto & q(a) \\ X & \longmapsto & X \end{array}$$

autrement dit à X on associe encore X et à $a \in A$ sa classe $q(a)$ modulo $\mathfrak{a}$.

Exemple On prend $A = \mathbb{Z}$ et $\mathfrak{a} = n\mathbb{Z}$, $n \in \mathbb{N}$; dans certaines questions, on est amené à prendre n premier, car $\mathbb{Z}/n\mathbb{Z}$ est alors un corps.

Application à la notion de racine On suppose ici que l'anneau A est un sous-anneau de l'anneau B, et on considère l'homomorphisme d'évaluation en $\beta \in B$ (cas 1) :

$$\begin{array}{ccc} A[X] & \longrightarrow & B \\ a \in A & \longmapsto & a \\ X & \longmapsto & \beta \end{array}$$

pour lequel l'image de $P \in A[X]$ a été notée $P(\beta)$.

Définition 2.34 (Racine d'un polynôme) *Soit $P \in A[X]$; on dit que $\beta \in B$ est racine de P **dans** B si $P(\beta) = 0$ (i.e. l'évaluation en β est nulle).*

Proposition 2.35 (Factorisation d'un polynôme par $X - \beta$) *Si $\beta \in B$ est racine de $P \in A[X]$ dans B, alors il existe $Q \in B[X]$ tel que $P = (X - \beta)Q$.*

Démonstration Comme $X - \beta$ est unitaire, on peut effectuer la division euclidienne généralisée dans $B[X]$ de P (considéré comme élément de $B[X]$)par $X - \beta$; on obtient $P = (X - \beta)Q + R$, Q, $R \in B[X]$ et $\mathrm{d}(R) < 1$; donc $R \in B$ et l'homomorphisme d'évaluation h en β donne $0 \Big(= P(\beta)\Big) = (\beta - \beta)Q(\beta) + R(\beta) = R$ (car $R(\beta) = R$ ici), d'où $R = 0$ et $P = (X - \beta)Q$.

Corollaire 2.36 (Racines d'un polynôme dans un anneau intègre) *Si B est intègre, si β_1, ..., β_n sont n racines distinctes de $P \in A[X]$, dans B, alors on a $P = (X - \beta_1) \dots (X - \beta_n)Q$, $Q \in B[X]$. Par conséquent, si $P \neq 0$, le nombre de racines distinctes de P dans B est majoré par le degré de P.*

En effet, par récurrence sur n (le cas $n = 1$ étant déjà prouvé) :
si $P = (X - \beta_1) \dots (X - \beta_k)Q'$, $Q' \in B[X]$,
alors : $P(\beta_{k+1}) = (\beta_{k+1} - \beta_1) \dots (\beta_{k+1} - \beta_k) \times Q'(\beta_{k+1}) = 0$;
comme $\beta_{k+1} - \beta_1 \neq 0$, ..., $\beta_{k+1} - \beta_k \neq 0$, l'intégrité de B entraîne $Q'(\beta_{k+1}) = 0$, d'où $Q' = (X - \beta_{k+1})Q$ dans $B[X]$, d'où le résultat.

Remarque Dans $B = \mathbb{Z}/8\mathbb{Z}, P = X^2 - \overline{1}$ a pour racines $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$ (4 racines distinctes pour P de degré 2 ; mais $\mathbb{Z}/8\mathbb{Z}$ n'est pas intègre !).

Remarque Le corollaire 2.36 sert en théorie des groupes pour décrire la structure (en tant que groupe) de tous sous-groupes finis des groupes multiplicatifs $k^\times$ des corps k (commutatifs). Cette structure est la plus simple possible pour un groupe fini : on dit que ces groupes sont cycliques. Par définition un groupe cyclique est un groupe engendré par un seul élément et on démontre que de tels groupes sont isomorphes au groupe additif de l'anneau $\mathbb{Z}/n\mathbb{Z}$ où n est le nombre d'élément du groupe de départ. La preuve de la cyclicité des sous-groupes finis de $k^\times$ demande d'être familiarisé avec la notion d'ordre des éléments d'un groupe et utilise aussi un peu d'astuce combinatoire. Hormis le corollaire 2.36 cette preuve relève purement de la théorie des groupes et n'a pas sa place dans ce cours ; mais puisque l'on a démontré dans le théorème 2.29 page 25 que, pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps (noté $\mathbb{F}_p$), on peut énoncer :

Proposition 2.37 ($(\mathbb{Z}/p\mathbb{Z})^\times$ pour p premier)
Soit p un nombre premier ; le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique à $p-1$ éléments.

Fin du deuxième chapitre

Chapitre 3

Produits d'anneaux. Théorèmes chinois

3.1 Produits d'anneaux

Définition 3.1 (Produit direct) *Soient $A_1, \ldots, A_n$, n groupes commutatifs (resp .anneaux commutatifs) non nécessairement distincts de neutres additifs O_{A_i} (resp. et d'unités 1_{A_i}, $i = 1, \ldots, n$). On considère le produit cartésien $A = A_1 \times \cdots \times A_n$ noté aussi $\prod_{i=1}^{n} A_i$. On peut le munir des lois produits muni des deux lois de composition suivantes :*

somme : $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$, *pour tout x_i, $y_i \in A_i$, et tout $i = 1, \ldots, n$;*

produit : $(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$, *pour tout x_i, $y_i \in A_i$, et tout $i = 1, \ldots, n$ (si les A_i sont des anneaux).*

*A est appelé le **produit direct** de $A_1, \ldots, A_n$ (en tant que groupe ou anneaux suivant la structure donnée aux A_i).*

Vérifier à titre d'exercice, que l'on obtient bien ainsi un groupe commutatif (resp. anneau commutatif) dont le neutre additif est $0_A = (0_{A_1}, \ldots, 0_{A_n})$ (resp. et l'élément unité est $1_A = (1_{A_1}, \ldots, 1_{A_n})$).

Proposition 3.2 ($(A_1 \times \cdots \times A_n)^\times$) *Si $A = A_1 \times \cdots \times A_n$, alors $A^\times = A_1^\times \times \cdots \times A_n^\times$ considéré comme sous-ensemble de $A_1 \times \cdots \times A_n$ (et donc l'identité est un isomorphisme de groupes commutatifs).*

Démonstration Soit $a \in A^\times$; posons $a = (a_1, \ldots, a_n)$, $a_i \in A_i$ pour $i = 1, \ldots, n$; par hypothèse, il existe $b = (b_1, \ldots, b_n)$, $b_i \in A_i$ pour $i = 1, \ldots, n$, tel que $ab = 1_A$, soit $(a_1 b_1, \ldots, a_n b_n) = (1_{A_1}, \ldots, 1_{A_n})$, d'où $a_i b_i = 1_{A_i}$ pour $i = 1, \ldots, n$, ce qui traduit l'inversibilité des a_i dans A_i pour chaque i (i.e. $a_i \in A_i^\times$, soit $a \in A_1^\times \times \cdots \times A_n^\times$).

Inversement si $a = (a_1, \ldots, a_n)$ avec $a_i \in A_i^\times$ pour tout i, il est immédiat de voir que $b = (a_1^{-1}, \ldots, a_n^{-1})$ est inverse de a dans A (a_i^{-1} étant l'inverse de a_i dans A_i pour chaque i).

On s'intéresse à la situation inverse ; autrement dit, on cherche à reconnaître dans quels cas un anneau commutatif A donné est isomorphe à un produit direct d'anneaux.

Proposition 3.3 (Idéaux principaux d'un produit d'anneaux) *Si $A = A_1 \times \cdots \times A_n$, alors, pour chaque $i = 1, \ldots, n$,*

$$\mathfrak{a}_i = \{0_{A_1}\} \times \cdots \times A_i \times \cdots \times \{0_{A_n}\},$$

considéré comme sous-ensemble de A, est un idéal de A qui est l'idéal principal engendré par $e_i = (0_{A_1}, \ldots, 1_{A_i}, \ldots, 0_{A_n}) \in A$. En outre les e_i, $i = 1, \ldots, n$, ont les propriétés suivantes :

1. *$e_i \neq 0_A$, pour tout i,*
2. *$e_i e_j = 0_A$, quels que soient $i, j, i \neq j$ (orthogonalité),*
3. *$\sum_{i=1}^{n} e_i = 1_A$,*
4. *$e_i^2 = e_i$, quel que soit i (idempotence).*

Les vérifications sont élémentaires et sont laissées au lecteur à titre d'exercice (à faire impérativement).

Remarques

1. La propriété 4 est impliquée (logiquement) par 2 et 3, car :

$$e_i \sum_{k=1}^{n} e_k = e_i \qquad \text{(d'après 3)},$$

d'où :

$$e_i = \sum_{k=1}^{n} e_i e_k = e_i^2 \qquad \text{(d'après 2)}.$$

2. On a $e_i = 1$, pour au moins un $i \in \{1, \ldots, n\}$, si et seulement si $n = 1$.

On peut donc partir d'une définition qui repose sur les considérations ci-dessus :

Définition 3.4 (Système fondamental d'idempotents orthogonaux) *Soit A un anneau commutatif. On dit qu'une famille $\{e_1, \ldots, e_n\}$ d'éléments de A constitue un* ***système fondamental d'idempotents orthogonaux*** *lorsque les propriétés suivantes sont vérifiées :*

1. *$e_i \neq 0_A$, pour tout $i = 1, \ldots, n$,*
2. *$e_i e_j = 0_A$, quels que soient $i, j = 1, \ldots, n$, $i \neq j$,*
3. *$\sum_{i=1}^{n} e_i = 1_A$,*

(ceci implique donc la propriété d'idempotence des e_i).

Théorème 3.5 *Soit A un anneau commutatif dans lequel il existe un système fondamental d'idempotents orthogonaux $\{e_1, \ldots, e_n\}$. Alors il existe n anneaux A_1, …, A_n tels que $A \simeq A_1 \times \cdots \times A_n$.*

0. On suppose $A_i \neq \{0\}$ pour tout i ; ceci n'est pas restrictif car $B \times \{0\} \simeq B$ pour tout anneau B.

Démonstration Dans A considérons les idéaux $\mathfrak{a}_i = Ae_i$, $i = 1, \ldots, n$; on peut munir $\mathfrak{a}_i$ d'une structure d'anneau de la manière suivante [1] : la loi de groupe est celle qui existe sur $\mathfrak{a}_i$ (comme sous-groupe de $(A, +)$), la multiplication est la **restriction** du produit sur A à $\mathfrak{a}_i \times \mathfrak{a}_i$ qui définit bien une loi de composition sur $\mathfrak{a}_i$ car $(ae_i)(be_i) = abe_i^2 = abe_i$ pour tout $a, b \in A$ (vérifier que l'on obtient un anneau d'élément unité e_i) ; les anneaux $\mathfrak{a}_i$ ne sont pas des sous-anneaux de A (sauf si $n = 1$, car alors $e_1 = 1_A$ par 3) : si on avait $1_A \in \mathfrak{a}_i$, on aurait $1_A = ue_i$, $u \in A$, soit, avec $j \neq i$ (si $n \geq 2$), $1_A e_j = ue_i e_j = 0$, soit $e_j = 0$, ce qui n'est pas. On note désormais A_i, $i = 1, \ldots, n$, ces nouveaux anneaux.

Pour montrer l'isomorphisme $A \simeq \prod_{i=1}^{n} A_i$, on a le choix entre définir

$$h \ : \ \prod_{i=1}^{n} A_i \longrightarrow A \text{ ou } h' \ : \ A \longrightarrow \prod_{i=1}^{n} A_i$$

Nous allons suivre la règle générale qui consiste à définir plutôt les applications en partant du produit cartésien (c'est plus canonique), mais ici il se trouve que la définition de l'application inverse est aussi canonique et a un intérêt pratique ; il s'agit des applications suivantes :

$$\begin{array}{rrcll} h \ : & \displaystyle\prod_{i=1}^{n} A_i & \longrightarrow & A & \\ & (a_1 e_1, \ldots, a_n e_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} a_i e_i, & \text{pour tout } a_1, \ldots, a_n \in A \ ; \\ h' \ : & A & \longrightarrow & \displaystyle\prod_{i=1}^{n} A_i & \\ & a & \longmapsto & (ae_1, \ldots, ae_n), & \text{pour tout } a \in A. \end{array}$$

Faisons donc la démonstration à l'aide de h (en exercice refaire intégralement la démonstration à partir de l'application h', puis démontrer que $h' = h^{-1}$) :

Si $x = (a_1 e_1, \ldots, a_n e_n)$, $y = (b_1 e_1, \ldots, b_n e_n)$,

$$\begin{aligned} h(x + y) &= \sum_{i=1}^{n} (a_i + b_i) e_i \\ &= h(x) + h(y) \\ h(xy) &= h\Big((a_1 b_1 e_1, \ldots, a_n b_n e_n)\Big) \\ &= \sum_{i=1}^{n} a_i b_i e_i \end{aligned}$$

1. Situation entièrement nouvelle, où l'on définit un anneau dont l'ensemble sous-jacent est une partie (remarquable) de l'anneau A, sans obtenir pour autant un sous-anneau de A ; à étudier avec soin.

$$\begin{aligned}
\text{or } h(x)h(y) &= \sum_{i=1}^{n} a_i e_i \sum_{j=1}^{n} b_j e_j \\
&= \sum_{i,j} a_i b_j e_i e_j \\
&= \sum_{k=1}^{n} a_k b_k e_k \qquad \text{(en utilisant l'orthogonalité, puis l'idempotence)} \\
\text{enfin } h\Big((e_1,\ldots,e_n)\Big) &= \sum_{i=1}^{n} e_i \\
&= 1_A \qquad \text{(propriété 3)} \quad \text{(noter que } (e_1,\ldots,e_n) \text{ est bien l'élément unité de } A_1 \times \cdots \times A_n)
\end{aligned}$$

On a donc un homomorphisme d'anneaux. Si $a \in A$, on écrit $a = a1_A = a\sum_{i=1}^{n} e_i = \sum_{i=1}^{n} ae_i$, et $a = h\Big((ae_1,\ldots,ae_n)\Big)$; alors, si $h\Big((a_1e_1,\ldots,a_ne_n)\Big) = 0_A$, on a $\sum_{i=1}^{n} a_ie_i = 0_A$, d'où $0_A = \left(\sum_{i=1}^{n} a_ie_i\right) e_k = a_ke_k$, ceci pour tout $k = 1,\ldots,n$. On a donc montré que h était un isomorphisme d'anneaux.

Remarque Dès qu'un anneau A contient un système fondamental d'idempotents orthogonaux $\{e_1,\ldots,e_n\}$, avec $n \geq 2$, alors A n'est pas intègre.

Abordons maintenant le résultat essentiel, dit des restes chinois, et qui repose sur la définition suivante :

Définition 3.6 (Co-maximalité) *Soit A un anneau commutatif et soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A ; on dit que $\mathfrak{a}$ et $\mathfrak{b}$ sont co-maximaux si $\mathfrak{a} + \mathfrak{b} = A$ (autrement dit $\mathfrak{a}$ et $\mathfrak{b}$ engendrent A).*

Théorème 3.7 (Théorème des restes chinois) *Soit A un anneau commutatif et soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux co-maximaux de A. Soient a et b deux éléments de A donnés arbitrairement. Alors il existe $x \in A$ tel que l'on ait :*

$$x \equiv a \bmod \mathfrak{a} \textit{ et } x \equiv b \bmod \mathfrak{b}.$$

Démonstration (revoir les notations congruentielles, très utiles ici, car on manipule les deux quotients $A/\mathfrak{a}$ et $A/\mathfrak{b}$ simultanément). On a $\mathfrak{a} + \mathfrak{b} = A$, donc il existe $\alpha \in \mathfrak{a}$ et $\beta \in \mathfrak{b}$ tels que $1 = \alpha + \beta$; soit alors $x = a\beta + b\alpha$ et montrons que x a les propriétés requises : on a $x \equiv a\beta \bmod \mathfrak{a}$ (car α, donc $b\alpha$, est dans $\mathfrak{a}$) ; or $\beta = 1 - \alpha$, d'où $x \equiv a(1-\alpha) \bmod \mathfrak{a}$, soit $x \equiv a - a\alpha \equiv a \bmod \mathfrak{a}$ (car $a\alpha \in \mathfrak{a}$). De même, $x \equiv b\alpha \bmod \mathfrak{b}$, soit, de façon analogue, $x \equiv b(1-\beta) \equiv b - b\beta \equiv b \bmod \mathfrak{b}$.

Corollaire 3.8 *Soient $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$, $n \geq 2$, des idéaux de A, co-maximaux deux à deux (i.e. $\mathfrak{a}_i + \mathfrak{a}_j = A$, pour tout $i,j = 1,\ldots,n$, $i \neq j$). Soient $a_1,\ldots,a_n$ des éléments*

quelconques de A. Alors il existe $x \in A$ tel que l'on ait $x \equiv a_i \bmod \mathfrak{a}_i$, pour tout $i = 1, \ldots, n$.

Il s'agit d'une simple induction à partir du cas $n = 2$ (qui donne en même temps une méthode pratique[2]). Supposons avoir trouvé $y \in A$ vérifiant les congruences $y \equiv a_i \bmod \mathfrak{a}_i$ pour tout $i = 2, \ldots, n$; il est clair que si l'on peut trouver $x \in A$ vérifiant les congruences $x \equiv a_1 \bmod \mathfrak{a}_1$ et $x \equiv y \bmod \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n$, x sera bien une solution au problème posé. Il suffit donc de prouver que $\mathfrak{a}_1$ et $\mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n$ sont co-maximaux : par hypothèse on a $A = \mathfrak{a}_1 + \mathfrak{a}_i$ pour $i = 2, \ldots, n$; donc $1 = b'_i + b_i$, $b'_i \in \mathfrak{a}_1$, $b_i \in \mathfrak{a}_i$, $i = 2, \ldots, n$; donc on a $1 = \prod_{i=2}^{n}(b'_i + b_i) \equiv \prod_{i=2}^{n} b_i \bmod \mathfrak{a}_1$, mais $\prod_{i=2}^{n} b_i \in \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n$, d'où le résultat. Ces résultats (dits aussi « d'approximations simultanées ») permettent d'énoncer le théorème suivant :

Théorème 3.9 (Isomorphisme des restes Chinois) *Soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $n \geq 2$, des idéaux de A, co-maximaux deux à deux.*

Alors l'homomorphisme canonique $h : A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$, défini pour tout $a \in A$ par $h(a) = \Big(q_{\mathfrak{a}_1}(a), \ldots, q_{\mathfrak{a}_n}(a)\Big)$ (où, pour un idéal $\mathfrak{a}$ de A, $q_{\mathfrak{a}}$ désigne l'homomorphisme canonique $A \to A/\mathfrak{a}$), est surjectif et a pour noyau $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$. Il en résulte que les anneaux $A/\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$ et $A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$ sont canoniquement isomorphes.

Démonstration On vérifie que h est un homomorphisme d'anneaux ; il s'agit de le factoriser. On a $h(a) = 0 = (\ldots, q_{\mathfrak{a}_i}(0), \ldots)$ si et seulement si $q_{\mathfrak{a}_i}(a) = q_{\mathfrak{a}_i}(0)$ pour $i = 1, \ldots, n$, soit si et seulement si $a \in \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$. Le point essentiel est alors la surjectivité : soit $\Big(q_{\mathfrak{a}_1}(a_1), \ldots, q_{\mathfrak{a}_n}(a_n)\Big)$, $a_i \in A$, $i = 1, \ldots, n$, un élément quelconque du produit direct ; d'après le théorème des restes chinois général, il existe $x \in A$ tel que $q_{\mathfrak{a}_i}(x) = q_{\mathfrak{a}_i}(a_i)$, pour tout $i = 1, \ldots, n$; x est bien un antécédent de l'élément donné.

Nous allons appliquer ce procédé de décomposition en produit direct, aux anneaux $\mathbb{Z}/m\mathbb{Z}$.

3.2 Étude des anneaux $\mathbb{Z}/m\mathbb{Z}$

3.2.1 Étude générale

Le théorème 1.16 des restes Chinois dans $\mathbb{Z}$ est en fait un cas particulier du théorème 3.7 comme on va le voir dans l'énoncé et la démonstration qui suit[3] :

2. Nous en verrons d'autres au chapitre 4.

3. Voir aussi page 39 pour une autre démonstration directe n'utilisant pas le théorème 3.7 page 34.

Théorème 3.10 *Soient $m_1, \ldots, m_n$, $n \geq 1$, n entiers non nuls étrangers deux à deux*[4]*. Alors on a l'isomorphisme canonique d'anneaux :*

$$\mathbb{Z}/m_1 \ldots m_n\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

Démonstration Dans l'anneau $\mathbb{Z}$, pour i, j fixés, $i \neq j$, les idéaux $\mathfrak{a}_i = m_i\mathbb{Z}$ et $\mathfrak{a}_j = m_j\mathbb{Z}$ sont co-maximaux : en effet, puisque m_i et m_j sont étrangers, il existe une relation de Bézout de la forme $\lambda_i m_i + \lambda_j m_j = 1$, λ_i, $\lambda_j \in \mathbb{Z}$; ainsi 1 est bien dans $\mathfrak{a}_i + \mathfrak{a}_j$ ($\lambda_i m_i \in \mathfrak{a}_i$, $\lambda_j m_j \in \mathfrak{a}_j$) donc l'idéal $\mathfrak{a}_i + \mathfrak{a}_j$ est l'anneau tout entier. Le théorème précédent donne l'isomorphisme :

$$\mathbb{Z}/\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n \simeq \mathbb{Z}/\mathfrak{a}_1 \times \cdots \times \mathbb{Z}/\mathfrak{a}_n = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z};$$

il ne reste plus qu'à voir que $m_1\mathbb{Z} \cap \ldots \cap m_n\mathbb{Z} = m_1 \ldots m_n\mathbb{Z}$:

L'inclusion « $\supseteq$ » étant triviale, démontrons l'autre par induction sur $n \geq 1$; pour $n = 1$, l'assertion est évidente ; supposons la vraie au rang k, $1 \leq k < n$, et montrons-la pour le rang $k+1$: on a déjà $m_1\mathbb{Z} \cap \ldots \cap m_k\mathbb{Z} = m_1 \ldots m_k\mathbb{Z}$ (par hypothèse, les $m_i\mathbb{Z}$ sont co-maximaux deux à deux pour $i = 1, \ldots, k$) ; soit alors $x \in m_1 \ldots m_k\mathbb{Z} \cap m_{k+1}\mathbb{Z}$; on a $x = m_1 \ldots m_k\lambda = m_{k+1}\mu$, λ, $\mu \in \mathbb{Z}$, et comme m_{k+1} est étranger à chaque m_i, $i = 1, \ldots, k$, m_{k+1} est étranger à $m_1 \ldots m_k$ et d'après le théorème de Gauss, m_{k+1} divise λ, d'où $\lambda = m_{k+1}\lambda'$, $\lambda' \in \mathbb{Z}$, soit $x = m_1 \ldots m_k m_{k+1}\lambda'$. D'où le résultat.

Remarque On utilise le fait que m_{k+1} étranger à $m_1, \ldots, m_k$ implique m_{k+1} étranger à $m_1 \ldots m_k$; ceci se retrouve au moyen (analogue à une partie de la preuve du corollaire 3.8 page 34) des relations de Bézout correspondantes : si $1 = u_i m_{k+1} + v_i m_i$, $u_i, v_i \in \mathbb{Z}$, $i = 1, \ldots k$, il vient $1 = \prod_{i=1}^{k}(u_i m_{k+1} + v_i m_i)$ qui se développe sous la forme $um_{k+1} + vm_1 \ldots m_k$ (et ceci **n'utilise pas** le fait que les m_i, $i = 1, \ldots, k$ sont étrangers deux à deux).

Corollaire 3.11 *Écrivons l'entier $m > 1$ sous la forme $m = p_1^{n_1} \times \cdots \times p_r^{n_r}$, $r \geq 1$, où les p_i sont des nombres premiers distincts, $i = 1, \ldots, r$, et les entiers $n_i \geq 1$. Alors on a l'isomorphisme d'anneaux :*

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}.$$

Corollaire 3.12 *On a l'isomorphisme de groupes (voir la proposition 3.2 page 31) :*

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{n_r}\mathbb{Z})^\times.$$

Étudions maintenant les groupes multiplicatifs $(\mathbb{Z}/m\mathbb{Z})^\times$, points de départ de propriétés arithmétiques intéressantes. Commençons par une description sommaire des classes inversibles des anneaux finis $\mathbb{Z}/m\mathbb{Z}$, $m \geq 1$. Notons pour simplifier, $\overline{a}$ la classe de $a \in \mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ ($m \geq 1$) et $[0, m[$ l'ensemble $\{a \in \mathbb{Z}, 0 \leq a < m\}$; on a alors le résultat suivant :

4. En pratique $n \geq 2$, mais pour $n = 1$ l'énoncé reste correct, car alors la condition « étrangers deux à deux » est vide puisqu'il y a zéro paires d'entiers distincts, et l'énoncé se réduit bien à $\mathbb{Z}/m_1\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z}$.

Lemme 3.13 (Classes inversibles de $\mathbb{Z}/m\mathbb{Z}$) *L'ensemble $(\mathbb{Z}/m\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/m\mathbb{Z}$ est en bijection avec l'ensemble $\Big\{a \in \mathbb{Z},\ a \in [0,m[$ et $(a,m)=1\Big\}$. Ainsi*

$$(\mathbb{Z}/m\mathbb{Z})^\times = \Big\{\overline{a} \in \mathbb{Z}/m\mathbb{Z},\ a \in [0,m[\text{ et } (a,m)=1\Big\}.$$

Comme $\mathbb{Z}/m\mathbb{Z}$ est en bijection avec $[0,m[$ (système exact de représentants des classes), il suffit de montrer que pour $a \in [0,m[$, $\overline{a}$ est inversible si et seulement si $(a,m)=1$:

1. Supposons $\overline{a}$ inversible ($a \in [0,m[$) ; alors il existe $\overline{b}$ tel que $\overline{a}\,\overline{b} = 1$, soit $ab \equiv 1 \bmod m\mathbb{Z}$, donc il existe $\lambda \in \mathbb{Z}$ tel que $ab = 1 + \lambda m$; ceci entraîne bien a et m étrangers.
2. Si $(a,m)=1$ ($a \in [0,m[$), il existe $u,v \in \mathbb{Z}$ tels que $ua+vm=1$, d'où $\overline{a}\,\overline{u} = \overline{1}$ dans $\mathbb{Z}/m\mathbb{Z}$.

Noter que pour $m=1$, 0 et 1 sont étrangers.

3.2.2 La fonction d'Euler

Définition 3.14 (Indicateur d'Euler) *Pour tout $m \in \mathbb{N}-\{0\}$, on pose $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$; la fonction φ s'appelle la* ***fonction (ou indicateur) d'Euler****.*

Par le lemme 3.13 page 37 on a :

$$\varphi(m) = |\{a \in [0,m[, (a,m)=1\}|.$$

Pour $m=1$, $\mathbb{Z}/\mathbb{Z}$ est l'anneau réduit à $\{0\}$ pour lequel $0=1$; 0 est ici inversible car $0\times 0 = 1$ (bien entendu dans tout anneau où $1 \neq 0$, ceci ne peut être). Donc $\varphi(1)=1$.

Proposition 3.15 (Expression de $\varphi(m)$) *Si $m = p_1^{n_1}\dots p_r^{n_r}$, $r \geq 1$, p_i premiers distincts, $n_i \geq 1$, $i=1,\dots,r$, alors on a :*

$$\varphi(m) = p_1^{n_1-1}(p_1-1)p_2^{n_2-1}(p_2-1)\dots p_r^{n_r-1}(p_r-1).$$

Démonstration On utilise le corollaire 3.12 page 36 qui conduit immédiatement à l'égalité $\varphi(m) = \varphi(p_1^{n_1})\varphi(p_2^{n_2})\dots\varphi(p_r^{n_r})$, comme on le voit par dénombrement d'un produit cartésien d'ensembles finis. Il reste donc à calculer $\varphi(p^n)$, pour tout nombre premier p et tout $n \geq 1$, ce qui est immédiat si l'on tient compte du lemme précédent qui donne ici

$$\begin{aligned}(\mathbb{Z}/p^n\mathbb{Z})^\times &= \Big\{\overline{1},\overline{2},\dots,\overline{p-1},\overline{p+1},\dots,\overline{a},\dots,\overline{p^n-1}\Big\}\\ &= \Big\{\overline{a},\ a \in [0,p^n[,\ a \text{ non divisible par } p\Big\}.\end{aligned}$$

Comme l'ensemble des multiples de p (compris entre 0 et p^n-1) est l'ensemble $\{0,\ p,\ 2p,\ 3p,\ \dots,\ (p^{n-1}-1)p\}$, il a donc p^{n-1} éléments, et son complémentaire en a donc $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Exemples

1. On a $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2(2-1) = 2$, $\varphi(5) = 4$, $\varphi(6) = \varphi(2)\varphi(3) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, ...
2. $\varphi(\ell n) = \varphi(\ell)\varphi(n)$, dès que ℓ et n sont étrangers.
3. Si n est impair, $\varphi(2n) = \varphi(n)$.

3.2.3 Structure des groupes $(\mathbb{Z}/m\mathbb{Z})^\times$, $m \geq 2$

Par le corollaire 3.11 l'étude de la structure de $(\mathbb{Z}/m\mathbb{Z})^\times$ se ramène à celle des groupes $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (p premier, $n \geq 1$). On va énoncer le théorème suivant ; mais une preuve complète, malgré son intérêt arithmétique, nous entraînerait trop loin en théorie des groupes.

Théorème 3.16 (Structure de $(\mathbb{Z}/p^n\mathbb{Z})^\times$) *La structure de $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est la suivante :*

1. *Si $p = 2$ et $n = 1$ (resp. 2), $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est un groupe cyclique à 1 (resp. 2) éléments ;*
2. *si $p = 2$ et $n \geq 3$, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est produit direct interne du sous-groupe cyclique à 2 éléments engendré par $-\overline{1}$ et du sous-groupe cyclique à 2^{n-2} éléments engendré par $\overline{5}$;*
3. *si $p \neq 2$, $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est un groupe cyclique à $(p-1)p^{n-1}$ éléments.*

3.2.4 Relèvement des classes inversibles

Définition 3.17 (Diviseur saturé) *Soit $m \in \mathbb{N} - \{0\}$, et soit n un diviseur de m ; nous dirons que n est un **diviseur saturé** de m si n et $\dfrac{m}{n}$ sont étrangers.*

Le mot saturé vient du fait que si p est un diviseur premier de n, alors n est divisible par la puissance de p maximum divisant m ; par exemple, les diviseurs saturés de $72 = 8 \times 9$ sont ± 1, ± 8, ± 9, ± 72, et les diviseurs non saturés sont ± 2, ± 3, ± 4, ± 6, ± 12, ± 18, ± 24, ± 36.

Si $d \mid m$, il existe un plus petit multiple D de d qui soit un diviseur saturé de m : en effet, si $d = \pm p_1^{\nu_1} \dots p_r^{\nu_r}$, p_i nombres premiers distincts, $\nu_i \geq 1$, $i = 1, \dots, r$, il suffit de prendre $D = \pm p_1^{n_1} \dots p_r^{n_r}$, où $n_i \geq \nu_i$, est l'exposant de p_i dans la décomposition de m en facteurs premiers, $i = 1, \dots, r$ (et on vérifie qu'il n'y a pas d'autres solutions). Nous dirons que D (choisi positif) est **le** diviseur saturé de m associé à d.

Théorème 3.18 (Cas de deux entiers étrangers) *Soit $m \in \mathbb{N} - \{0\}$, et soit d un diviseur de m. Si $a \in \mathbb{Z}$ est étranger à d, alors il existe dans la classe $a + d\mathbb{Z}$ un entier étranger à m.*

Démonstration Soit D le diviseur saturé de m associé à d ; on a donc, dans $\mathbb{N}$, $m = D\Delta$, avec $d \mid D$, D et Δ étant étrangers ; on peut donc appliquer le théorème des restes chinois avec D et Δ : il existe $x \in \mathbb{Z}$ tel que l'on ait $x \equiv a \bmod D$ et $x \equiv 1 \bmod \Delta$; on a bien $x \in a + d\mathbb{Z}$, puisque $d \mid D$, et x est étranger à m pour

les raisons suivantes : si p premier divise x et m, on a $p \mid D$ ou $p \mid \Delta$, or si $p \mid D$, la congruence $x \equiv a \bmod D$ implique $p \mid a$, ce qui n'est pas, donc $p \mid \Delta$, ce qui est absurde car $x \equiv 1 \bmod \Delta$ conduit à $p \mid 1$.

Corollaire 3.19 *L'application partant de $(\mathbb{Z}/m\mathbb{Z})^\times$ et à valeur dans $(\mathbb{Z}/d\mathbb{Z})^\times$, qui à la classe $u+m\mathbb{Z}$ (u étranger à m) associe la classe $u+d\mathbb{Z}$, est un homomorphisme de groupes* ***surjectif*** [5].

Remarque Un homomorphisme de groupe (commutatif) est une application

$$f : G \longrightarrow H,$$

compatible avec les lois de groupes de G et H c'est-à-dire, en notation multiplicative, telle que $f(gg') = f(g)f(g')$ pour tout $g, g' \in G$. Si on note 1_G et 1_H les éléments neutre respectifs des groupes G et H on définit $\mathrm{Ker}(f) = \{g \in G, f(g) = 1\}$. On démontre alors que f est injective si et seulement si $\mathrm{Ker}(f) = \{1_G\}$. S'agissant de groupe finis on peut même dire mieux, en effet dans ce cas on a l'égalité entre cardinaux

$$\#f(G) = \frac{\#G}{\#\,\mathrm{Ker}(f)},$$

où $f(G) \subset H$ désigne l'image (finie) de f. Pour voir cette égalité on utilise l'équivalence (évidente) $f(g) = f(g') \iff g^{-1}g' \in \mathrm{Ker}(f)$ qui en particulier montre que tout élément de l'image de f a exactement $\#ker(f)$ antécédents distincts par f.

3.2.5 Complément

Démonstration directe du théorème 3.10 page 35. On considère donc n entiers $m_1, \ldots, m_n > 0$, étrangers deux à deux. L'application canonique :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \displaystyle\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z} \\ x & \longmapsto & (\ldots, q_{m_i}(x), \ldots) \end{array}$$

a pour noyau $\left\{x \in \mathbb{Z},\ x \equiv 0 \bmod m_i \text{ pour } i = 1, \ldots, n\right\} = \displaystyle\bigcap_{i=1}^{n} m_i\mathbb{Z} = m\mathbb{Z}$, où $m = m_1 \ldots m_n$. On a donc, par factorisation, l'injection canonique :

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}.$$

Mais ici $|\mathbb{Z}/m\mathbb{Z}| = m$ et $\left|\displaystyle\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}\right| = \displaystyle\prod_{i=1}^{n} |\mathbb{Z}/m_i\mathbb{Z}| = m$; or toute injection d'un ensemble fini dans un ensemble de même cardinal est aussi surjective. D'où le résultat.

5. Résultat non démontrable « élémentairement ».

Mais ceci n'est pas généralisable si les quotients considérés ne sont pas finis, ce qui sera le cas des quotients de la forme $\mathbb{C}[X]/(X-a)$ (isomorphes à $\mathbb{C}$) qui seront considérés dans le chapitre 4, et cette démonstration directe n'est donc pas significative de la situation modulaire.

Fin du troisième chapitre

Chapitre 4

Méthodes modulaires dans les anneaux principaux

Ce chapitre présente essentiellement des applications de la décomposition des anneaux en produits d'anneaux ; ces applications ont effectivement une utilité pratique dans le domaine de l'ingénierie mathématique. Il n'y a pas de notions théoriques nouvelles mais il faut savoir pratiquer (numériquement parlant) les méthodes et algorithmes proposés, qui ne reposent que sur le calcul congruentiel.

Dans tout ce chapitre, on suppose que A est un anneau **principal** (c'est-à-dire que A est intègre et que ses idéaux sont principaux ; en pratique, il s'agit de $\mathbb{Z}$, ou de $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps (cf. chapitre 2, définition 2.12 page 20). Dans le chapitre 6, nous montrerons qu'un anneau principal a toutes les propriétés arithmétiques classiques qui sont, plus généralement, celles des « anneaux factoriels » ; mais nous n'avons pas besoin ici de ces aspects arithmétiques, puisqu'en fait les méthodes modulaires sont valables dans un anneau **quelconque**, pourvu que l'on sache caractériser la co-maximalité de deux idéaux ; nous allons donc seulement indiquer comment se traduit la co-maximalité dans le cas principal.

4.1 Co-maximalité dans un anneau principal

Pour simplifier, tout idéal (principal) est noté (a), $a \in A$, au lieu de aA ; par abus d'écriture, une congruence de la forme $y \equiv x \bmod (a)$ s'écrit souvent $y \equiv x \bmod a$, surtout dans les calculs numériques.

Définition 4.1 (Éléments étrangers) *Soient a, $b \in A$, A principal ; on dit que a et b sont **étrangers** si leurs seuls diviseurs communs sont les éléments inversibles de A (i.e. si $a = ds$, $b = dt$, d, s, $t \in A$, alors nécessairement on a $d \in A^*$).*

Le lien entre les notions d'idéaux co-maximaux et d'éléments étrangers, **dans un anneau principal**, est donné par le résultat suivant :

Lemme 4.2 *Dans un anneau principal, deux idéaux (a) et (b) sont co-maximaux si et seulement si a et b sont étrangers.*

Démonstration

$\Longrightarrow$ **:** Supposons que $(a)+(b)=A$ et posons $1=ua+vb$, u, $v\in A$; soit $d\in A$ un diviseur commun à a et b : on a $a=ds$, $b=dt$, s, $t\in A$, d'où $1=uds+vdt=(us+vt)d$ qui implique $d\in A^*$; donc a et b sont étrangers.

$\Longleftarrow$ **:** Supposons a et b étrangers et considérons l'idéal $(a)+(b)$. Comme l'anneau A est principal, il existe $d\in A$ tel que $(a)+(b)=(d)$; mais on a $a\in(a)+(b)$, $b\in(a)+(b)$ (puisque $(a)+(b)$ est aussi l'idéal engendré par a et b), d'où $a=ds$, $b=dt$, s, $t\in A$; par hypothèse on a donc $d\in A^*$, d'où $(a)+(b)=A$ (co-maximalité).

Comme cela a déjà été évoqué pour $A=\mathbb{Z}$, on a aussi la simplification suivante :

Lemme 4.3 *Dans un anneau A (non nécessairement principal), si deux idéaux principaux (a) et (b) sont co-maximaux, alors $(a)\cap(b)=(ab)$.*

Une inclusion étant triviale, considérons $x\in(a)\cap(b)$, et posons $x=as=bt$, s, $t\in A$; écrivons $1=ua+vb$, u, $v\in A$, ce qui conduit à $x=x(ua+vb)=uax+vbx$, d'où (en remplaçant x par bt, puis par as) $x=uabt+vbas=(ut+vs)ab$, d'où $x\in(ab)$.

Proposition 4.4 *Si les idéaux $(a_1),\ldots,(a_n)$ de A sont co-maximaux deux à deux*[1]*, alors*

$$\bigcap_{i=1}^{n}(a_i)=\left(\prod_{i=1}^{n}a_i\right).$$

Immédiat par récurrence : si $(a_1)\cap\ldots\cap(a_k)=(a_1\ldots a_k)$, on utilise (cf. chapitre 3, démonstration du corollaire 3.8 page 34) le fait que $(a_1)\cap\ldots\cap(a_k)=(a_1\ldots a_k)$ et (a_{k+1}) sont co-maximaux, auquel cas :

$$\Big((a_1)\cap\ldots\cap(a_k)\Big)\cap(a_{k+1})=(a_1\ldots a_k)\cap(a_{k+1})=(a_1\ldots a_{k+1}).$$

On peut donc énoncer (cf. chapitre 3, théorème 3.9 page 35) :

Proposition 4.5 (Cas des anneaux principaux) *Soit A un anneau principal et soient $a_1,\ldots,a_n$ des éléments de A étrangers deux à deux ; alors on a l'isomorphisme canonique :*

$$A/(a_1\ldots a_n)\xrightarrow{\simeq}A/(a_1)\times\cdots\times A/(a_n)$$

qui à la classe de $a\in A$ modulo $(a_1\ldots a_n)$ associe le n-uple des classes de a modulo les (a_i), $i=1,\ldots,n$.

Remarque On a obtenu la stricte généralisation du cas $A=\mathbb{Z}$, traité au chapitre 3 (cf. théorème 3.10 page 35), au cas d'un anneau principal A quelconque.

1. ou encore (par le lemme 4.2 page 41), si $a_1,\ldots,a_n$ sont étrangers deux à deux, lorsque A est principal.

Corollaire 4.6 (Système de congruences) *Toujours si $a_1, \ldots, a_n$ sont des éléments de A étrangers deux à deux, tout système de congruences de la forme :*

$$\left\{ \begin{array}{rcll} x & \equiv & x_1 & \mod (a_1) \\ & \vdots & & \\ x & \equiv & x_n & \mod (a_n), \end{array} \right.$$

où $x_1, \ldots, x_n$ sont n éléments arbitraires de A, admet toujours des solutions ; l'ensemble de toutes les solutions est donné par

$$x = x' + \lambda a_1 \ldots a_n, \qquad \lambda \in A,$$

où x' est une solution particulière arbitraire.

En effet, l'existence n'est autre que la surjectivité de l'homomorphisme canonique $A/(a_1 \ldots a_n) \to \prod_{i=1}^{n} A/(a_i)$; quant au fait que deux solutions diffèrent d'un multiple de $a_1 \ldots a_n$, il s'agit de l'injectivité de cet homomorphisme.

Remarque Dans certains cas, la solution particulière x' pourra être « relativement canonique ».

Problèmes modulaires Nous appellerons **problème modulaire**, tout problème qui est équivalent à la résolution d'un système de congruences de la forme précédente (nous allons en voir plusieurs exemples).

L'essentiel étant de calculer une solution x', nous allons développer les deux méthodes qui permettent l'obtention systématique de la solution x', à partir des propriétés de l'anneau A. Ces méthodes sont :

1. la méthode des idempotents ;
2. la méthode des développements « multi-adiques ».

4.2 Méthode des idempotents

Soient $a_1, \ldots, a_n$, des éléments étrangers deux à deux de A, et soit q l'homomorphisme canonique $A \to A/(a_1 \ldots a_n)$; on sait que cet anneau quotient admet un système de n idempotents orthogonaux qui sont de la forme $q(e_1), \ldots, q(e_n)$, $e_1, \ldots, e_n \in A$, et qui sont les images réciproques, dans l'isomorphisme canonique rappelé dans la proposition 4.5 page 42 (voir également dans le chapitre 3 la proposition 3.3 page 32 et le théorème 3.5 page 32), des éléments $\Big(q_1(0), \ldots, q_i(1), \ldots, q_n(0)\Big)$, $i = 1, \ldots, n$, où l'on désigne comme d'habitude par q_i les homomorphismes canoniques $A \to A/(a_i)$, $i = 1, \ldots, n$.

Utilisons la notation congruentielle : des représentants $e_1, \ldots, e_n \in A$ des idempotents de $A/(a_1 \ldots a_n)$ (les $q(e_i)$, $i = 1, \ldots n$) sont donc caractérisés par les congruences suivantes dans A :

$$\left. \begin{array}{rcll} e_i & \equiv & 0 & \mod (a_j) \quad \text{pour tout } j \neq i \\ e_i & \equiv & 1 & \mod (a_i) \end{array} \right\} \qquad i = 1, \ldots, n. \tag{4.1}$$

Il s'agit donc d'un problème modulaire particulier.

Fixons i ; les premières congruences équivalent à :

$$e_i \in \bigcap_{j,j\neq i} (a_j),$$

et la proposition 4.4 page 42 implique que e_i est de la forme

$$e_i = \alpha_i \prod_{j,j\neq i} a_j = \alpha_i a_1 \dots \widehat{a_i} \dots a_n, \qquad \alpha_i \in A, \tag{4.2}$$

où le symbole $\widehat{\ }$ signifie l'omission du facteur correspondant. Les secondes congruences conduisent alors à :

$$\alpha_i a_1 \dots \widehat{a_i} \dots a_n \equiv 1 \bmod (a_i). \tag{4.3}$$

Or, dans $A/(a_i)$, les $q_i(a_j)$, $j \neq i$, sont inversibles : en effet, pour $i \neq j$, a_i et a_j sont étrangers par hypothèse, donc $(a_i) + (a_j) = A$, et il existe λ_i, $\lambda_j \in A$ tels que $1 = \lambda_i a_i + \lambda_j a_j$, d'où $q_i(\lambda_j) q_i(a_j) = q_i(1)$.

La classe $q_i(a_1 \dots \widehat{a_i} \dots a_n)$ est donc inversible dans $A/(a_i)$ (i.e. $a_1 \dots \widehat{a_i} \dots a_n$ est « inversible mod a_i »), et il existe $\alpha_i \in A$ tel que l'on ait la congruence écrite (c'est n'importe quel représentant de l'inverse de $a_1 \dots \widehat{a_i} \dots a_n$ modulo a_i).

Remarques

1. Comme on calcule $q_i(\alpha_i)$, il en résulte que le représentant $\alpha_i \in A$ est défini modulo (a_i) seulement, ce qui implique que $e_i = \alpha_i a_1 \dots \widehat{a_i} \dots a_n$ est bien défini modulo $a_1 \dots a_n$.
2. La détermination effective de α_i dépend fortement de la nature de A ; on reviendra sur cette question.

Si l'on dispose de $e_1, \dots, e_n$, les problèmes modulaires dans A sont immédiats et systématiques, comme on l'a déjà vu (cf. chapitre 3, démonstration du théorème 3.5 page 32) :

Corollaire 4.7 (Solution d'un système de congruences) *Soient $a_1, \dots, a_n \in A$ étrangers deux à deux. Tout $x \in A$ vérifiant les congruences simultanées suivantes (où $x_1, \dots, x_n$ sont arbitraires dans A) :*

$$\Big\{ x \equiv x_i \bmod (a_i), \quad i = 1, \dots, n,$$

est donné par la formule suivante :

$$x = \sum_{i=1}^{n} x_i \alpha_i a_1 \dots \widehat{a_i} \dots a_n + \lambda a_1 \dots a_n, \qquad \lambda \in A, \tag{4.4}$$

où, pour $i = 1, \dots, n$, α_i est inverse de $a_1 \dots \widehat{a_i} \dots a_n$ modulo (a_i).

En effet, puisque $q(1) = \sum_{i=1}^{n} q(e_i)$, on a $q(x) = \sum_{i=1}^{n} q(x)q(e_i) = \sum_{i=1}^{n} q(xe_i)$; mais comme $x \equiv x_i \bmod (a_i)$, on a $xe_i \equiv x_i e_i \bmod (a_i e_i)$, soit $xe_i \equiv x_i e_i \bmod (a_1 \dots a_n)$ d'après l'expression (cf. (4.2) page 44) des e_i ; d'où $q(x) = \sum_{i=1}^{n} q(x_i e_i)$, ou encore :

$$x \equiv \sum_{i=1}^{n} x_i \alpha_i a_1 \dots \widehat{a_i} \dots a_n \bmod (a_1 \dots a_n).$$

4.3 Applications classiques

Elles vont se situer au niveau des quotients des anneaux (principaux) $\mathbb{Z}$ et $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps). Commençons par une situation numérique :

4.3.1 Exemple dans $\mathbb{Z}/m\mathbb{Z}$

Déterminons les idempotents de $\mathbb{Z}/180\mathbb{Z}$ correspondant à la décomposition :

$$\mathbb{Z}/180\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

On résout les congruences suivantes :

$$\left\{ \begin{array}{rcrcl} e_1 & = & \alpha_1 \times 9 \times 5 & \equiv & 1 \mod 4 \\ e_2 & = & \alpha_2 \times 4 \times 5 & \equiv & 1 \mod 9 \\ e_3 & = & \alpha_3 \times 4 \times 9 & \equiv & 1 \mod 5 \end{array} \right.$$

soit

$$\left\{ \begin{array}{rcrl} 45\alpha_1 & \equiv & 1 & \mod 4 \\ 20\alpha_2 & \equiv & 1 & \mod 9 \\ 36\alpha_3 & \equiv & 1 & \mod 5 \end{array} \right. \iff \left\{ \begin{array}{rcrl} \alpha_1 & \equiv & 1 & \mod 4 \\ 2\alpha_2 & \equiv & 1 & \mod 9 \\ \alpha_3 & \equiv & 1 & \mod 5 \end{array} \right.$$

$$\iff \left\{ \begin{array}{rcrl} \alpha_1 & \equiv & 1 & \mod 4 \\ \alpha_2 & \equiv & 5 & \mod 9 \\ \alpha_3 & \equiv & 1 & \mod 5 \end{array} \right.$$

d'où $e_1 \equiv 45 \bmod 180$, $e_2 \equiv 100 \bmod 180$, $e_3 \equiv 36 \bmod 180$.

Remarques

1. Lorsque l'inverse de b modulo a (dans $\mathbb{Z}$, a et b étrangers) n'est pas évident numériquement, on devra rechercher (par l'algorithme d'Euclide dans $\mathbb{Z}$) la « relation de Bézout » $1 = ua + vb$ qui donne un représentant de cet inverse par le coefficient v.
2. Le nombre d'idempotents à trouver dans $\mathbb{Z}/m\mathbb{Z}$ dépend de la décomposition choisie pour m en facteurs étrangers. Par exemple, ici, on peut également dire $\mathbb{Z}/180\mathbb{Z} \simeq \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (36 et 5 sont étrangers) et le système d'idempotents ne comporte alors que 2 éléments $q(e'_1)$, $q(e'_2)$. La décomposition la plus « fine » correspond au cas où les a_i $(i = 1, \dots, n)$ sont les puissances des nombres

premiers qui factorisent m (ici 2^2, 3^2, 5). On démontrera, à titre d'exercice, que si $q(e_1), \ldots, q(e_n)$ sont les idempotents correspondant à la décomposition la plus fine $\left(\mathbb{Z}/m\mathbb{Z} = \prod_{i=1}^{n} \mathbb{Z}/p_i^{r_i}\mathbb{Z},\ r_i \geq 1,\ p_i \text{ premiers distincts}\right)$, alors les autres systèmes d'idempotents s'obtiennent en effectuant les sommes de $q(e_i)$ qui correspondent aux regroupements opérés ; par exemple, ici, $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ correspond au regroupement de $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$, ce qui fait que (le vérifier) :

$$\begin{array}{rcccl} e_1' & \equiv & e_1 + e_2 & \equiv & 145 \bmod 180 \\ e_2' & \equiv & e_3 & \equiv & 36 \bmod 180 \end{array}$$

4.3.2 Les polynômes d'interpolation simple

On considère $A = \mathbb{K}[X]$, où $\mathbb{K}$ est un corps quelconque (commutatif).

Soient $x_1, \ldots, x_n$, n éléments **distincts** de $\mathbb{K}$, fixés, et soient $y_1, \ldots, y_n$, n valeurs arbitraires de $\mathbb{K}$. On cherche les polynômes P de $\mathbb{K}[X]$ tels que $P(x_i) = y_i$ pour tout $i = 1, \ldots, n$ (polynômes dont le graphe de la fonction polynomiale associée contient (ou passe par) les points (x_i, y_i), $i = 1, \ldots, n$).

On remarque que la condition $P(x_i) = y_i$ est équivalente à $P \equiv y_i \bmod (X - x_i)$. En effet, on a, par définition, $X \equiv x_i \bmod (X - x_i)$, d'où :

$$P \quad \Big(= P(X)\Big) \quad \equiv P(x_i) \quad (= y_i) \quad \bmod (X - x_i)$$

En outre, les $X - x_i$ sont étrangers deux à deux (en effet, on a $X - x_i - (X - x_j) = x_j - x_i$ qui est dans $\mathbb{K}^\times$ pour tout $j \neq i$; d'où $\dfrac{1}{x_j - x_i}(X - x_i) - \dfrac{1}{x_j - x_i}(X - x_j) = 1$ (co-maximalité) et le fait que les x_i soient distincts est donc bien une condition nécessaire et suffisante pour que les $X - x_i$ soient étrangers deux à deux). D'où l'isomorphisme canonique :

$$\mathbb{K}[X] \Big/ \Big((X - x_1) \ldots (X - x_n)\Big) \simeq \mathbb{K}[X] \Big/ (X - x_1) \times \cdots \times \mathbb{K}[X] \Big/ (X - x_n) \tag{4.5}$$

qui conduit au résultat suivant :

Théorème 4.8 *Soit $\mathbb{K}$ un corps et soient $x_1, \ldots, x_n$ des éléments **distincts** de $\mathbb{K}$. Soient $y_1, \ldots, y_n$ arbitraires dans $\mathbb{K}$. Alors il existe un unique polynôme $P \in \mathbb{K}[X]$, de degré $d \leq n - 1$, tel que $P(x_i) = y_i$, pour tout $i = 1, \ldots, n$. Ce polynôme est donné par*

$$P = \sum_{i=1}^{n} y_i \prod_{\substack{j \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

Démonstration Ici la formule donnée pour P suffit à prouver l'existence (car on a trivialement $P(x_i) = y_i$ pour tout $i = 1, \ldots, n$) ; cependant il est intéressant de montrer qu'il s'agit encore d'un problème modulaire [2]. En utilisant des notations

2. et qu'on obtient cette formule sans avoir à la deviner.

semblables à celles utilisées en (4.1) page 43, on doit déterminer des $e_i \in \mathbb{K}[X]$, $i = 1, \ldots, n$, tels que :

$$\left.\begin{array}{rcll} e_i & \equiv & 0 \mod (X - x_j) & \text{pour tout } j \neq i \\ e_i & \equiv & 1 \mod (X - x_i) & \end{array}\right\} \quad i = 1, \ldots, n$$

ce qui conduit à (cf. (4.2) page 44) :

$$e_i = \lambda_i (X - x_1) \ldots \widehat{(X - x_i)} \ldots (X - x_n), \quad \lambda_i \in \mathbb{K}[X]$$

puis la congruence $e_i \equiv 1 \mod (X - x_i)$, qui devient ici, avec $X \equiv x_i \mod (X - x_i)$ (cf. (4.3) page 44) :

$$\lambda_i \prod_{\substack{j \\ j \neq i}} (x_i - x_j) \equiv 1 \mod (X - x_i)$$

d'où, par exemple $\lambda_i = \dfrac{1}{\displaystyle\prod_{\substack{j \\ j \neq i}} (x_i - x_j)}$ (solution de degré minimum 0).

D'où $e_i = \displaystyle\prod_{\substack{j \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$ qui est un représentant de degré minimum $(n-1)$ pour tout i (choix canonique ici des e_i). Ces représentants canoniques s'appellent aussi les « multiplicateurs de Lagrange » et sont évidemment bien connus en analyse numérique.

Le reste du théorème est alors immédiat, l'unicité de P (de degré $\leq n-1$) venant de (4.4) page 44 qui dit que toute solution P est de la forme $P = P_0 + \Lambda \displaystyle\prod_{i=1}^{n} (X - x_i)$, $\Lambda \in \mathbb{K}[X]$, où P_0 désigne par exemple le polynôme de degré $\leq n-1$ de l'énoncé $\Big($le module $\displaystyle\prod_{i=1}^{n} (X - x_i)$ étant de degré n, il faut bien prendre $\Lambda = 0$ pour avoir une solution de degré $\leq n-1$ (unicité donc)$\Big)$.

Nous allons voir maintenant que l'on peut généraliser très facilement la situation précédente à une situation modulaire plus précise

4.3.3 Polynômes d'interpolation avec conditions aux dérivées

On est seulement obligé de supposer que dans le corps $\mathbb{K}$, $n1_{\mathbb{K}} = 0$ a lieu si et seulement si $n = 0$ (i.e. $\mathbb{K}$ est de « caractéristique » nulle, voir chapitre 5, définition 5.17 page 64).

Exemple Prenons $\mathbb{K} = \mathbb{F}_2$ (pour lequel $2.\overline{1} = \overline{0}$) et cherchons P tel que l'on ait les conditions suivantes :

$$P(\overline{0}) = \overline{0}, \qquad P(\overline{1}) = \overline{0}, \qquad P'(\overline{0}) = P''(\overline{0}) = \overline{1}$$

on a déjà $P = X(X-\overline{1})Q$, $Q \in \mathbb{F}_2[X]$, d'où $P' = -Q + X(X-\overline{1})Q'$ (car $(X^2)' = 2X = \overline{0}$), $P'' = -Q' + (-Q' + X(X-\overline{1})Q'') = X(X-\overline{1})Q''$; d'où $P''(x) = \overline{0}$ pour tout $x \in \mathbb{F}_2$, et une impossibilité à résoudre le problème posé.

Posons maintenant le problème général suivant :

Existe-t-il $P \in \mathbb{K}[X]$ vérifiant les conditions de dérivations suivantes ? (où $P^{(0)} = P$, et où $P^{(i)}$ est la i-ème dérivée formelle de P) :

$$\left.\begin{array}{rcl} P^{(0)}(x_i) & = & y_i^0 \\ P^{(1)}(x_i) & = & y_i^1 \\ & \vdots & \\ P^{(\nu_i)}(x_i) & = & y_i^{\nu_i} \end{array}\right\} \quad i = 1, \ldots, n \tag{4.6}$$

où les $\nu_i \geq 0$ sont fixés, les x_i étant donnés **distincts** dans $\mathbb{K}$, et où les $y_i^{\ell_i}$ sont des éléments **arbitraires** dans $\mathbb{K}$ (ils ont été indexés, pour $i = 1, \ldots, n$, par l'indice supérieur ℓ_i, $\ell_i = 0, 1, \ldots, \nu_i$).

Fixons i et, en supposant que l'on a une solution P, considérons le reste P_i de la division euclidienne de P par $(X - x_i)^{\nu_i+1}$:

$$P = P_i + (X - x_i)^{\nu_i+1} Q_i, \qquad \mathrm{d}(P_i) \leq \nu_i \tag{4.7}$$

on vérifie par le calcul, et en utilisant (4.6) page 48, que

$$P^{(\ell_i)}(x_i) = P_i^{(\ell_i)}(x_i) = y_i^{\ell_i}$$

pour tout ℓ_i tel que $0 \leq \ell_i \leq \nu_i$.

Or, d'après la formule de Taylor pour les polynômes, il existe un unique polynôme P_i de degré $\leq \nu_i$ vérifiant les conditions de dérivations précédentes

$$P_i^{(\ell_i)}(x_i) = y_i^{\ell_i}, \qquad 0 \leq \ell_i \leq \nu_i$$

c'est le polynôme :

$$P_i = y_i^0 + \frac{1}{1\,!} y_i^1 (X - x_i) + \cdots + \frac{1}{\nu_i\,!} y_i^{\nu_i} (X - x_i)^{\nu_i} \tag{4.8}$$

(c'est ici que le choix de la caractéristique 0 s'impose : il faut pouvoir écrire les $\dfrac{1}{\ell_i\,!}$ étant entendu qu'il y a là un abus d'écriture : $\dfrac{1}{\ell}$ signifie, pour tout entier $\ell > 0$, l'inverse de $\ell.1_{\mathbb{K}}$ dans $\mathbb{K}^\times$) [3].

Le polynôme P vérifie donc les congruences simultanées :

$$P \equiv P_i \bmod (X - x_i)^{\nu_i+1} \qquad \text{(cf. (4.7) page 48)}, \; i = 1, \ldots, n \tag{4.9}$$

où les P_i sont maintenant donnés de façon numériquement explicite via (4.8) page 48 ; il s'agit donc bien d'un problème modulaire que l'on sait résoudre si les $(X - x_i)^{\nu_i+1}$ sont étrangers deux à deux, ce qui est le cas ici puisque les x_i sont choisis distincts (le fait que les $X - x_i$ soient étrangers deux à deux entraîne cette propriété pour des puissances arbitraires grâce au lemme suivant).

Lemme 4.9 *Soient P et Q deux éléments étrangers d'un anneau principal A ; alors, pour tout entier $m \geq 1$ et tout entier $n \geq 1$, P^m et Q^n sont étrangers.*

3. La formule (4.8) page 48 montre que l'on peut améliorer l'hypothèse sur la caractéristique de $\mathbb{K}$; lorsque celle-ci est non nulle, c'est un nombre premier p (cf. chapitre 5, proposition 5.18 page 65) et le problème d'interpolation est possible si $\nu_i \leq p - 1$, $i = 1, \ldots, n$.

Démonstration Par hypothèse, il existe u, $v \in A$ tels que $uP + vQ = 1$; on élève à la puissance $m+n-1$ et on obtient une expression de la forme :

$$\sum_{k=0}^{m+n-1} S_k P^k Q^{m+n-1-k} = 1$$

avec $S_k \in A$ pour tout $k = 0, \ldots, m+n-1$; on en déduit :

$$Q^n \sum_{k=0}^{m-1} S_k P^k Q^{m-1-k} + P^m \sum_{k=m}^{m+n-1} S_k P^{k-m} Q^{m+n-1-k} = 1$$

c'est-à-dire $VQ^n + UP^m = 1$, avec U, $V \in A$ (les exposants dans les deux sommes sont tous positifs). Donc P^m et Q^n sont étrangers. CQFD.

Le problème modulaire posé trouve sa solution dans l'isomorphisme canonique correspondant, à savoir :

$$\mathbb{K}[X] \Big/ \prod_{i=1}^{n} (X - x_i)^{\nu_i+1} \simeq \prod_{i=1}^{n} \mathbb{K}[X]/(X - x_i)^{\nu_i+1} \tag{4.10}$$

Théorème 4.10 *Soit $\mathbb{K}$ un corps de caractéristique nulle et soient $x_1, \ldots, x_n \in \mathbb{K}$ donnés distincts. Alors quels que soient les éléments $y_i^{\ell_i}$ de $\mathbb{K}$, $0 \leq \ell_i \leq \nu_i$, $\nu_i \geq 0$, donnés pour $i = 1, \ldots, n$, il existe un unique polynôme $P \in \mathbb{K}[X]$ tel que $\mathrm{d}(P) \leq -1 + \sum_{i=1}^{n} (\nu_i + 1)$ et tel que $P^{(\ell_i)}(x_i) = y_i^{\ell_i}$, pour tout ℓ_i, $0 \leq \ell_i \leq \nu_i$, et tout $i = 1, \ldots, n$.*

4.3.4 Calcul des idempotents

On suit à nouveau (4.1) page 43 : des représentants $e_i \in \mathbb{K}[X]$ sont tels que

$$e_i = \Lambda_i \prod_{\substack{j \\ j \neq i}} (X - x_j)^{\nu_j+1}, \quad \Lambda_i \in \mathbb{K}[X] \qquad \text{(cf. (4.2) page 44)}$$

et

$$\Lambda_i \prod_{\substack{j \\ j \neq i}} (X - x_j)^{\nu_j+1} \equiv 1 \bmod (X - x_i)^{\nu_i+1} \qquad \text{(cf. (4.3) page 44)}$$

On constate que si $\nu_i \neq 0$, on n'a plus $X \equiv x_i \bmod (X - x_i)^{\nu_i+1}$ (en particulier, Λ_i ne sera pas un élément de $\mathbb{K}$). Le calcul de Λ_i reste cependant accessible facilement : on peut déjà trouver une relation de Bézout

$$U(X - x_i)^{\nu_i+1} + V \prod_{\substack{j \\ j \neq i}} (X - x_j)^{\nu_j+1} = 1$$

dans laquelle le polynôme V donne Λ_i ; mais on a d'autres possibilités, compte tenu de la forme particulière des polynômes, qui sont plus agréables :

Fixons i et posons $X - x_i = T$ (évaluation $\mathbb{K}[X] \longrightarrow \mathbb{K}[T]$, qui à X associe $T + x_i$, et qui ici est un isomorphisme). Notons Λ l'image de Λ_i dans $\mathbb{K}[T]$, Q celle de $\prod_{\substack{j \\ j\neq i}} (X - x_j)^{\nu_j+1}$, et posons $\nu_i = \nu$; on a :

$$Q = \prod_{\substack{j \\ j\neq i}} (T + x_i - x_j)^{\nu_j+1}$$

et on doit résoudre la congruence :

$$\Lambda Q \equiv 1 \bmod T^{\nu+1} \qquad \text{dans } \mathbb{K}[T]$$

Première méthode : On peut inverser modulo $T^{\nu+1}$ chaque facteur $T + x_i - x_j$ de la façon suivante : on pose $x_j - x_i = u$ qui est non nul puisque $x_i \neq x_j$ pour $i \neq j$; l'égalité

$$\left(1 - \frac{T}{u}\right)\left(1 + \frac{T}{u} + \cdots + \left(\frac{T}{u}\right)^{\nu}\right) = 1 - \left(\frac{T}{u}\right)^{\nu+1}$$

conduit à

$$q(T-u)^{-1} = q\left(-\frac{1}{u}\left(1 + \frac{T}{u} + \cdots + \left(\frac{T}{u}\right)^{\nu}\right)\right) \qquad \text{dans } \mathbb{K}[T]/T^{\nu+1}$$

soit

$$q(X-x_j)^{-1} = q\left(-\frac{1}{x_j - x_i}\left(1 + \frac{X - x_i}{x_j - x_i} + \cdots + \left(\frac{X - x_i}{x_j - x_i}\right)^{\nu}\right)\right) \quad \text{dans } \mathbb{K}[X]/(X - x_i)^{\nu+1}$$

D'où $q(Q)^{-1}$ en calculant $\prod_{\substack{j \\ j\neq i}} q(X - x_j)^{-(\nu_j+1)}$.

Deuxième méthode : On développe Q sous la forme explicite $u_0 + \cdots + u_r T^r$; on a $u_0 = \prod_{\substack{j \\ j\neq i}} (x_i - x_j)^{\nu_j+1}$ qui est non nul par hypothèse, et on utilise le résultat suivant :

Lemme 4.11 *Soit $P \in \mathbb{K}[T]$ et soit m un entier arbitraire, $m \geq 0$. Pour tout polynôme Q dont le terme constant $u_0 = Q(0)$ est non nul, il existe S, $M \in \mathbb{K}[T]$ tels que :*

$$P = QS + M, \qquad M \equiv 0 \bmod T^{m+1}$$

Ceci s'établit par récurrence. L'égalité étant triviale pour $m = 0$:

$$S = -\frac{P(0)}{Q(0)},\ M = P - \frac{P(0)}{Q(0)}Q$$

supposons la établie au niveau $\ell-1$; écrivons $P = QS' + M'$, $M' \equiv 0 \bmod T^\ell$, et posons $M' = a_\ell T^\ell + \cdots + a_{\ell+t}T^{\ell+t}$, $t \geq 0$. Considérons $S = S' + \dfrac{a_\ell}{u_0}T^\ell$; alors :

$$\begin{aligned} P - QS &= P - QS' - Q\frac{a_\ell}{u_0}T^\ell \\ &= M' - (u_0 + \cdots + u_r T^r)\frac{a_\ell}{u_0}T^\ell \\ &= a_\ell T^\ell + \cdots + a_{\ell+t}T^{\ell+t} - a_\ell T^\ell - (u_1 T + \cdots + u_r T^r)\frac{a_\ell}{u_0}T^\ell \\ &\equiv 0 \bmod T^{\ell+1} \end{aligned}$$

Remarque Cet algorithme classique est souvent appelé la « division selon les puissances croissantes » de P par Q, mais il ne s'agit pas d'une division comme la division euclidienne. Nous dirons aussi que le polynôme S est le développement limité formel (ou développement $T-$adique) à l'ordre m de la fraction rationnelle $\dfrac{P}{Q}$; on peut en effet écrire :

$$\frac{P}{Q} = S + \frac{M}{Q} = S + T^{m+1}\frac{M'}{Q} \qquad (\text{avec } Q \not\equiv 0 \bmod T)$$

(égalité dans $\mathbb{K}(T)$, où S, M' sont dans $\mathbb{K}[T]$). Autrement dit, il s'agit d'un analogue de la « division décimale » [4], si l'on se place dans le cadre de l'anneau des séries formelles, $\mathbb{K}[[T]]$, dont on peut démontrer qu'il contient tous les éléments de $\mathbb{K}(T)$ dont le dénominateur est étranger à T ; ici, pour $\dfrac{P}{Q}$ il existe une unique série formelle $\displaystyle\sum_{i\geq 0} a_i T^i$, $a_i \in \mathbb{K}$, égale à $\dfrac{P}{Q}$ ($= PQ^{-1}$, où Q^{-1} est alors l'inverse du polynôme Q dans ce nouvel anneau $\mathbb{K}[[T]]$) que l'on tronque à partir de T^{m+1} pour obtenir S.

Dans ce cadre de calculs formels, on perçoit assez facilement la similitude avec le cas de l'algorithme d'approximation décimale d'un rationnel < 1 (par exemple, on a $\dfrac{219}{627} = 0,34928\ldots$) qui est lui-même une série de la forme $\displaystyle\sum_{i\geq 0} \delta_i \big(10^{-1}\big)^i$, $\delta_i \in \{0, 1, \ldots, 9\}$ (convergente pour la métrique usuelle), la « convergence » dans le cas de $\mathbb{K}[[T]]$ ayant un sens dans le cadre de la « topologie $T-$adique », facile à définir, et pour laquelle $\mathbb{K}[[T]]$ n'est autre que le complété de $\mathbb{K}[T]$ [5]. Ceci résout notre problème car alors Λ n'est autre que le développement limité formel de $\dfrac{1}{Q}$ à l'ordre ν.

Exemple Résoudre la congruence :

$$\Lambda\Big(T^3 - 2T + 1\Big) \equiv 1 \bmod T^4$$

4. digressions qu'il n'est pas demandé d'approfondir !
5. comme $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la métrique usuelle.

On utilise la disposition habituelle :

$$\begin{array}{rrrrrrr|l}
1 & & & & & & & 1-2T+T^3 \\
\hline
-1 & + & 2T & & & - & T^3 & 1+2T+4T^2+7T^3=\Lambda \\
\hline
 & & 2T & & & - & T^3 & \\
 & - & 2T & + & 4T^2 & & & \\
\hline
 & & & & 4T^2 & - & T^3 & \\
 & & & - & 4T^2 & + & 8T^3 & \\
\hline
 & & & & & & 7T^3 & \\
 & & & & & - & 7T^3 & \\
\hline
 & & & & & & 0 &
\end{array}$$

(on cherche à éliminer à chaque étape, le monôme de plus petit degré ; on omet les termes en T^i, $i \geq 4$, car la valeur exacte de M n'est pas nécessaire).

On aurait pu également écrire (dans $\mathbb{K}[[T]]$) :

$$\begin{aligned}
\frac{1}{1-2T+T^3} &= \frac{1}{1-(2T-T^3)} \\
&= 1+(2T-T^3)+(2T-T^3)^2+(2T-T^3)^3+\cdots \\
&\equiv 1+2T-T^3+4T^2+8T^3 \bmod T^4 \\
&\equiv 1+2T+4T^2+7T^3 \mod T^4,
\end{aligned}$$

puisque le développement formel de $\dfrac{1}{1-X}$ est bien connu.

4.4 Calculs par développements multi-adiques

L'inconvénient majeur de tout calcul modulaire, via le calcul d'un système fondamental d'idempotents, est que si l'on souhaite passer du produit $A/(a_1)\times\cdots\times A/(a_n)$ au produit $A/(a_1)\times\cdots\times A/(a_m)$, $m>n$ (toujours en supposant tous les a_i étrangers deux à deux) on doit recommencer tous les calculs d'idempotents. On peut déjà dire que le calcul modulaire par les idempotents est à envisager lorsque l'on a plusieurs problèmes à résoudre avec le **même système** de a_i, $i=1,\ldots,n$; par exemple si l'on doit résoudre des systèmes de congruences de la forme

$$x \equiv x_i \bmod (a_i), \qquad i=1,\ldots,n$$

pour un grand nombre de données $(x_i)_i$, puisqu'alors on aura seulement à calculer $\displaystyle\sum_{i=1}^{n} x_i e_i \bmod \prod_{i=1}^{n} a_i$.

En revanche, si on a un problème modulaire susceptible d'évoluer quant au nombre d'idéaux (a_i) (par exemple si l'on veut rajouter des points d'interpolation afin d'obtenir un polynôme d'interpolation plus précis), on utilisera la méthode que nous allons décrire maintenant.

4.4.1 Développements multi-adiques

Soit A un anneau principal, et soit à résoudre le système de congruences simultanées :

$$\Big(S_n\Big) \qquad \Big\{ x \equiv x_i \bmod (a_i), \qquad i = 1, \ldots, n$$

où les $a_i \in A$ sont étrangers deux à deux, et les $x_i \in A$ arbitraires.

Considérons, pour $1 \leq k < n$, le système **partiel** :

$$\Big(S_k\Big) \qquad \Big\{ x \equiv x_i \bmod (a_i), i = 1, \ldots, k$$

D'après le corollaire 4.6 page 43, la solution générale de (S_k) est donnée par

$$x = u_k + \lambda_k a_1 \ldots a_k, \qquad \lambda_k \text{ arbitraire dans } A$$

où u_k est une solution particulière de (S_k).

L'idée est alors de montrer, par induction, que l'on peut déduire u_{k+1} (donc la solution générale de (S_{k+1})) de u_k et des données supplémentaires x_{k+1}, a_{k+1}, le cas $k = 1$ étant trivial ($x = u_1 + \lambda_1 a_1$, avec $u_1 = x_1$).

On a alors les équivalences suivantes :

$$\begin{aligned}
\Big\{ x \text{ est solution de } (S_{k+1}) \quad &\Longleftrightarrow \quad \begin{cases} x \text{ est solution de } (S_k) \\ x \equiv x_{k+1} \bmod (a_{k+1}) \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} x = u_k + \lambda_k a_1 \ldots a_k, \quad \lambda_k \in A \\ x \equiv x_{k+1} \bmod (a_{k+1}) \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} x = u_k + \lambda_k a_1 \ldots a_k, \quad \lambda_k \in A \\ \lambda_k a_1 \ldots a_k \equiv x_{k+1} - u_k \bmod (a_{k+1}) \end{cases} \\
&\Longleftrightarrow \quad \begin{cases} x = u_k + \lambda_k a_1 \ldots a_k, \\ \lambda_k = \alpha_k (x_{k+1} - u_k) + \lambda_{k+1} a_{k+1}, \quad \lambda_{k+1} \in A \end{cases}
\end{aligned}$$

(où α_k est un inverse arbitraire de $a_1 \ldots a_k$ modulo a_{k+1}).

On a donc obtenu l'équivalence suivante :

$$\begin{array}{c} x \text{ est solution de } (S_{k+1}) \\ \Updownarrow \\ x = u_k + \alpha_k a_1 \ldots a_k (x_{k+1} - u_k) + \lambda_{k+1} a_1 \ldots a_k a_{k+1} \end{array}$$

λ_{k+1} arbitraire dans A ; il suffit alors de prendre

$$u_{k+1} \equiv u_k + \alpha_k a_1 \ldots a_k (x_{k+1} - u_k) \bmod a_1 \ldots a_k a_{k+1}$$

En pratique, il suffit donc de traiter les congruences au fur et à mesure, à condition, à chaque étape (i.e. à chaque k), de bien écrire la **solution générale** correspondante.

4.4.2 Exemples

1. Résoudre le système de congruences suivant dans $\mathbb{Z}$:

$$\left\{\begin{array}{rcrl} x & \equiv & 1 & \bmod 4 \\ x & \equiv & -1 & \bmod 9 \\ x & \equiv & 3 & \bmod 5 \end{array}\right.$$

On écrit donc $x = 1 + 4\lambda_1$, $\lambda_1 \in \mathbb{Z}$, puis $1 + 4\lambda_1 \equiv -1 \bmod 9$, soit :

$$4\lambda_1 \equiv -2 \bmod 9$$

Un représentant de $q_9(4)^{-1}$ est 7, d'où $\lambda_1 \equiv -2 \times 7 \equiv 4 \bmod 9$, et on écrit $\lambda_1 = 4 + 9\lambda_2$, d'où $x = 1 + 16 + 36\lambda_2 = 17 + 36\lambda_2$. La dernière congruence conduit à $17 + 36\lambda_2 \equiv 3 \bmod 5$, ou encore $2 + \lambda_2 \equiv 3 \bmod 5$, soit :

$$\lambda_2 \equiv 1 \bmod 5$$

En posant $\lambda_2 = 1 + 5\lambda$, on obtient finalement $x = 53 + 180\lambda$, λ arbitraire dans $\mathbb{Z}$.

Remarque Avec les idempotents calculés en 4.3.1 page 45, on aurait à écrire :

$$x \equiv 1 \times e_1 - 1 \times e_2 + 3 \times e_3 \equiv 45 - 100 + 108 \equiv 53 \bmod 180$$

2. Pour les polynômes d'interpolation, la méthode est également très efficace : Trouver le polynôme P de $\mathbb{R}[X]$, de degré minimum, tel que :

$$\left\{\begin{array}{l} P(-1) = 1, \quad P'(-1) = 0, \quad P''(-1) = 2 \\ P(0) = 2, \\ P(1) = -1, \quad P'(1) = 0 \end{array}\right.$$

Ce problème modulaire est relatif aux a_i suivants (qui sont étrangers) (cf. théorème 4.10 page 49) :

$$a_1 = (X+1)^3, \qquad a_2 = X, \qquad a_3 = (X-1)^2$$

et équivalent au système de congruences suivant (cf. (4.8) page 48) :

$$\left\{\begin{array}{rcl} P & \equiv & 1 + 0 \times (X+1) + 2\dfrac{(X+1)^2}{2} \bmod (X+1)^3 \\ P & \equiv & 2 \bmod X \\ P & \equiv & -1 + 0 \times (X-1) \bmod (X-1)^2 \end{array}\right.$$

Posons $P = 1 + (X+1)^2 + \Lambda_1(X+1)^3$, $\Lambda_1 \in \mathbb{R}[X]$; on a à résoudre :

$$\begin{array}{rcll} \Lambda_1(X+1)^3 + 1 + (X+1)^2 \equiv 2 \bmod X & \iff & \Lambda_1 + 2 \equiv 2 \bmod X & \\ & & & (\text{car } X + 1 \equiv 1 \bmod X) \\ & \iff & \Lambda_1 \equiv 0 \bmod X & \\ & \iff & \Lambda_1 = X\Lambda_2 & \end{array}$$

d'où :

$$P = 1 + (X+1)^2 + \Lambda_2 X(X+1)^3, \qquad \Lambda_2 \in \mathbb{R}[X]$$

La congruence $P \equiv -1 \bmod (X-1)^2$ conduit à :

$$\Lambda_2 X(X+1)^3 \equiv -2 - (X+1)^2 \bmod (X-1)^2$$

Posons $T = X - 1$; on obtient :

$$\begin{aligned} \Lambda_2(1+T)(2+T)^3 &\equiv -2-(2+T)^2 \bmod T^2, \qquad \text{soit} \\ \Lambda_2(1+T)(8+12T) &\equiv -2-(4+4T) \equiv -6-4T \bmod T^2 \\ \Lambda_2(8+20T) &\equiv -6-4T \bmod T^2 \end{aligned}$$

(noter les calculs du type « développements limités »). On calcule alors le développement limité formel de $\dfrac{-6-4T}{8+20T}$ modulo T^2 :

$$\begin{array}{rl|l} -6 - 4T & & 8+20T \\ \cline{3-3} 6 + 15T & & -\frac{3}{4}+\frac{11}{8}T \\ \cline{1-2} 11T & & \\ -11T + \cdots & & \\ \cline{1-2} 0 + \cdots & & \end{array}$$

d'où $\Lambda_2 \equiv -\dfrac{3}{4} + \dfrac{11}{8}T \bmod T^2$; en réexprimant Λ_2 dans $\mathbb{R}[X]$, il vient :

$$\begin{aligned} \Lambda_2 &\equiv -\frac{3}{4} + \frac{11}{8}(X-1) \\ &\equiv -\frac{3}{4} - \frac{11}{8} + \frac{11}{8}X \\ &\equiv -\frac{17}{8} + \frac{11}{8}X \bmod (X-1)^2 \end{aligned}$$

d'où

$$P \equiv 1 + (X+1)^2 - \frac{17}{8}X(X+1)^3 + \frac{11}{8}X^2(X+1)^3 \bmod \left((X+1)^3 X(X-1)^2\right)$$

soit finalement :

$$P = \frac{1}{8}(16 - X - 32X^2 - 18X^3 + 16X^4 + 11X^5)$$

Fin du quatrième chapitre

Chapitre 5

Anneaux commutatifs intègres. Caractéristique d'un anneau

Nous revenons à des considérations générales sur les anneaux commutatifs qui s'inscrivent essentiellement dans la suite du chapitre 2, et qui visent les objectifs suivants : montrer qu'un anneau intègre peut être vu comme un sous-anneau d'un corps, classifier les anneaux en fonction de leur « caractéristique ».

5.1 Diviseurs de 0, intégrité (rappels)

Définition 5.1 (Diviseur de 0) *Soit A un anneau commutatif. Soit $x \in A$; on dit que x est un diviseur de 0 s'il est non nul et s'il existe $y \in A$, $y \neq 0$, tel que $xy = 0$.*

Définition 5.2 (Anneau intègre) *On dit que A est un anneau intègre si on a $1 \neq 0$ (i.e. $A \neq \{0\}$) et si A est sans diviseurs de 0 (cf. chapitre 2, définition 2.4 page 17).*

Proposition 5.3 *Soit A un anneau commutatif intègre et soit $\mathfrak{a}$ un idéal principal, $\mathfrak{a} \neq (0)$. Alors $\mathfrak{a} = Aa = Ab$ équivaut à $b = ua$, $u \in A^\times$.*

Démonstration Si $Aa = Ab$, alors $b = ua$, $u \in A$, et de même, $a = vb$, $v \in A$; donc $a = vua$, et $(1 - vu)a = 0$; comme $\mathfrak{a} \neq (0)$, on a $a \neq 0$ donc, comme il ne peut y avoir dans A de diviseurs de 0, il vient $1 - vu = 0$, et $u \in A^\times$.

5.2 Construction du corps des fractions d'un anneau intègre

5.2.1 Construction

Soit A un anneau commutatif intègre ; on pose $S = A - \{0\}$ et on remarque que S a les propriétés suivantes :

1. pour tout $x, y \in S$, $xy \in S$ (en effet, $xy = 0$ entraînerait, par intégrité, $x = 0$ ou $y = 0$, ce qui n'est pas)
2. $1 \in S$ (car $1 \neq 0$ par hypothèse)
3. $0 \notin S$

De telles parties vérifiant 1, 2, 3 sont dites des parties multiplicatives de l'anneau, ou encore multiplicativement stables.

Sur le produit cartésien $A \times S$ on définit la relation suivante ($a, b \in A$, $s, t \in S$) :

$$(a, s) \sim (b, t) \qquad \text{si et seulement si} \qquad at - bs = 0 \qquad \text{dans } A$$

Lemme 5.4 (Relation d'équivalence sur $A \times S$) *Cette relation binaire est une relation d'équivalence sur $A \times S$.*

- On a $(a, s) \sim (a, s)$ car $as - as = 0$.
- Si $(a, s) \sim (b, t)$, on a $at - bs = 0$ soit $bs - at = 0$ qui traduit $(b, t) \sim (a, s)$.
- Si $(a, s) \sim (b, t)$ et si $(b, t) \sim (c, u)$, on a donc $at - bs = 0$ et $bu - ct = 0$ d'où $atu - bus = 0$ et $bsu - cts = 0$, ce qui donne, en ajoutant, $atu - cts = 0$; comme $t \in S$, $t \neq 0$, et A étant intègre, on a $au - cs = 0$, d'où $(a, s) \sim (c, u)$.

On appelle K_A l'ensemble des classes de $A \times S$ modulo cette relation d'équivalence ($K_A = (A \times S)/\mathcal{R}$, si $\mathcal{R}$ désigne cette relation). On note la classe de (a, s) par $\dfrac{a}{s}$ ($a \in A$, $s \in S$).

Remarque On reconnaît la notation fractionnaire : on a donc $\dfrac{a}{s} = \dfrac{b}{t}$ si et seulement si $at - bs = 0$ (pour $a, b \in A$, $s, t \in S$).

On va définir sur K_A une structure d'anneau :

Définition 5.5 (Addition) *On pose* $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{at + bs}{st}$ *pour tout* $\dfrac{a}{s}$ *et* $\dfrac{b}{t} \in K_A$.

Lemme 5.6 (Addition sur K_A) *Cette définition a un sens et définit une loi de composition sur K_A.*

Elle a un sens car $st \in S$ (propriété 1 de S). Montrons alors que la définition ne dépend pas du choix des représentants des classes : si $\dfrac{a'}{s'} = \dfrac{a}{s}$ et $\dfrac{b'}{t'} = \dfrac{b}{t}$ on doit montrer que $\dfrac{a't' + b's'}{s't'}$ est la même classe que $\dfrac{at + bs}{st}$ (sachant que $a's - as' = 0$ et $b't - bt' = 0$).

Calculons :

$$\begin{aligned}(a't' + b's')st - (at + bs)s't' &= a'stt' + b'tss' - as'tt' - bt'ss' \\ &= (a's - as')tt' + (b't - bt')ss' \\ &= 0\end{aligned}$$

ce qui donne l'égalité des deux classes.

Définition 5.7 (Multiplication) *On pose* $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$ *pour tout* $\frac{a}{s}$ *et* $\frac{b}{t} \in K_A$.

Lemme 5.8 (Multiplication sur K_A) *Cette définition a un sens et définit une loi de composition sur* K_A.

Comme précédemment et avec les mêmes notations auxiliaires, on doit calculer :
$$a'b'st - abs't' = b'tas' - abs't' = as'(b't - bt') = 0.$$

Théorème 5.9 (Corps K_A) *Muni de ces deux lois de composition,* K_A *est un corps (commutatif) contenant un sous-anneau canoniquement isomorphe à* A.

1. Étude de l'addition $\left(\frac{a}{s}\frac{b}{t}\frac{c}{u} \in K_A\right)$:

   Associativité :

$$\begin{aligned}\left(\frac{a}{s}+\frac{b}{t}\right)+\frac{c}{u} &= \frac{at+bs}{st}+\frac{c}{u}\\ &= \frac{(at+bs)u+cst}{stu}\\ &= \frac{atu+bsu+cst}{stu}\\ &= \frac{a(tu)+(bu+ct)s}{s(tu)}\\ &= \frac{a}{s}+\left(\frac{b}{t}+\frac{c}{u}\right)\end{aligned}$$

   Commutativité : Évidente.

   Neutre : Le neutre est $\frac{0}{1}$ car $\frac{a}{s}+\frac{0}{1} = \frac{a+0s}{s1} = \frac{a}{s}$ (ici on utilise le fait que $1 \in S$, mais ce n'est pas crucial car $\frac{0}{s} = \frac{0}{1}$ pour tout $s \in S$).

   Opposé : L'opposé de $\frac{a}{s}$ est $\frac{-a}{s}$ car $\frac{a}{s}+\frac{-a}{s} = \frac{as-as}{s^2} = \frac{0}{s^2} = \frac{0}{1}$. On note comme d'habitude l'opposé par $-\frac{a}{s}$.

2. Étude de la multiplication :

   Associativité : Évidente.

   Commutativité : Évidente.

   Unité : L'unité est $\frac{1}{1}$ car $\frac{a}{s}\frac{1}{1} = \frac{a}{s}$.

Distributivité :

$$\begin{aligned}
\frac{a}{s}\left(\frac{b}{t}+\frac{c}{u}\right) &= \frac{a}{s}\left(\frac{bu+ct}{tu}\right)\\
&= \frac{abu+act}{stu}\\
\frac{a}{s}\frac{b}{t}+\frac{a}{s}\frac{c}{u} &= \frac{absu+acst}{s^2tu}\\
&= \frac{s(abu+act)}{sstu}\\
&= \frac{abu+act}{stu} \qquad \text{(par définition)}
\end{aligned}$$

3. Étude des éléments inversibles de K_A :
   Si $\frac{a}{s} \neq \frac{0}{1}$ c'est que $a1-s0 \neq 0$, soit $a \neq 0$; donc $a \in S$, $\frac{s}{a} \in K_A$, et on remarque que $\frac{a}{s}\frac{s}{a} = \frac{1}{1}$; K_A est bien un corps commutatif $\left(\text{remarquer que } \frac{1}{1} \neq \frac{0}{1}\right)$.
4. Existence d'un sous-anneau de K_A isomorphe à A :
   Considérons l'application $h : A \to K_A$ définie par $h(a) = \frac{a}{1}$.
   On a $h(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$ $h(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1}$ et $h(1) = \frac{1}{1}$. Donc h est un homomorphisme d'anneaux ; calculons son noyau : si $h(a) = \frac{0}{1}$ alors $\frac{a}{1} = \frac{0}{1}$, soit $a = 0$. Si on pose $A' = \left\{\frac{a}{1},\ a \in A\right\}$, on vient de prouver l'isomorphisme $A \simeq A'$ (A' étant l'image de h, c'est un sous-anneau de K_A).

5.2.2 Conséquences

On « identifie » en pratique A' et A en notant a les éléments de la forme $\frac{a}{1}$; de cette façon « $A \subseteq K_A$ », et un élément quelconque $\frac{a}{s}$ de K_A s'écrit $\frac{a}{1}\frac{1}{s}$ soit $\frac{a}{1}\left(\frac{s}{1}\right)^{-1}$ que l'on peut écrire as^{-1} en vertu de l'identification faite.

On peut dire que dans le corps K_A, tous les éléments de $A-\{0\}$ y sont inversibles (dans K_A et non dans A !). On appelle K_A le corps des fractions de l'anneau intègre A.

Exemples Le corps des fractions de $\mathbb{Z}$, noté $\mathbb{Q}$, est le corps des rationnels, celui de $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), noté $\mathbb{K}(X)$, est le corps des fractions rationnelles en une indéterminée.

Remarque Tout anneau intègre peut donc être considéré comme inclus dans un corps (en fait comme sous-anneau d'un corps), et de ce fait calculer dans un anneau intègre revient à calculer dans un corps d'une certaine manière.

Théorème 5.10 (Prolongement d'un homomorphisme à K_A) *Soient A et B des anneaux (commutatifs) ; on suppose A intègre. Soit h un homomorphisme de A dans B ; on suppose que $h(S) \subset B^\times$ ($S = A - \{0\}$). Alors il existe un unique homomorphisme $\widetilde{h}$ de K_A dans B qui prolonge h.*

Démonstration On définit $\widetilde{h}$ par $\widetilde{h}\left(\frac{a}{s}\right) = h(a)h(s)^{-1}$; on vérifie que ceci a un sens : si $\frac{a}{s} = \frac{b}{t}$ alors $at - bs = 0$ et $h(a)h(t) = h(b)h(s)$, mais par hypothèse $h(s)$, $h(t) \in B^\times$, donc $h(a)h(s)^{-1} = h(b)h(t)^{-1}$, d'où $\widetilde{h}\left(\frac{a}{s}\right) = \widetilde{h}\left(\frac{b}{t}\right)$. On a :

$$\begin{aligned}
\widetilde{h}\left(\frac{a}{s} + \frac{b}{t}\right) &= \widetilde{h}\left(\frac{at+bs}{st}\right) \\
&= h(at+bs)h(st)^{-1} \\
&= h(at)h(s)^{-1}h(t)^{-1} + h(bs)h(s)^{-1}h(t)^{-1} \\
&= h(a)h(s)^{-1} + h(b)h(t)^{-1} \\
&= \widetilde{h}\left(\frac{a}{s}\right) + \widetilde{h}\left(\frac{b}{t}\right) \\
\widetilde{h}\left(\frac{a}{s}\,\frac{b}{t}\right) &= \widetilde{h}\left(\frac{ab}{st}\right) \\
&= h(ab)h(st)^{-1} \qquad (\text{car } st \in S) \\
&= h(a)h(b)h(s)^{-1}h(t)^{-1} \\
&= \widetilde{h}\left(\frac{a}{s}\right)\widetilde{h}\left(\frac{b}{t}\right)
\end{aligned}$$

Enfin $\widetilde{h}\left(\frac{1}{1}\right) = h(1) = 1_B$.

Donc $\widetilde{h}$ est un homomorphisme : il prolonge bien h, car $\widetilde{h}(a) = \widetilde{h}\left(\frac{a}{1}\right) = h(a)$ pour tout $a \in A$.

L'unicité de $\widetilde{h}$ résulte du fait que $\frac{a}{s} = as^{-1}$ dans K_A et que tout homomorphisme prolongeant h prend la valeur $h(a)h(s)^{-1}$ sur $\frac{a}{s} \in K_A$.

Corollaire 5.11 (Prolongement d'un homomorphisme injectif à K_A) *Si A est intègre, si $\mathbb{L}$ est un corps, alors tout homomorphisme injectif h de A dans $\mathbb{L}$ se prolonge de façon unique en un homomorphisme injectif de K_A dans $\mathbb{L}$.*

5.3 Étude des anneaux principaux

On dit qu'un anneau commutatif est un anneau principal s'il est intègre et si tous ses idéaux sont principaux.

Exemples L'anneau $\mathbb{Z}$ et tous les anneaux $\mathbb{K}[X]$ pour tout corps $\mathbb{K}$.

Le résultat suivant est extrêmement important en pratique :

Théorème 5.12 *Soit A un anneau principal. Alors tout idéal premier* ***non nul*** *de A est maximal.*

Démonstration Remarque préliminaire : Si A est un corps (qui est évidemment un anneau principal) il n'existe pas d'idéaux premiers $\mathfrak{p} \neq (0)$; dans ce cas, (0) est d'ailleurs premier et maximal (et c'est le seul cas car si A n'est pas un corps, (0) est premier, parce que A est intègre, mais non maximal). L'énoncé n'est donc intéressant que si l'anneau principal A n'est pas un corps.

Soit $\mathfrak{p}$ premier, $\mathfrak{p} \neq (0)$; on a donc $\mathfrak{p} \neq A$. Soit alors $\mathfrak{a}$ un idéal tel que $\mathfrak{p} \subsetneqq \mathfrak{a} \subseteq A$; on va prouver que $\mathfrak{a} = A$. Posons $\mathfrak{p} = Ax$, $\mathfrak{a} = Ay$, x, $y \in A$; comme $\mathfrak{p} \subseteq \mathfrak{a}$, on a $x = uy$, $u \in A$; mais $\mathfrak{p}$ étant premier, y ou u est dans $\mathfrak{p}$, et comme, par hypothèse, $\mathfrak{p} \subsetneqq \mathfrak{a}$, $y \notin \mathfrak{p}$ (sinon on aurait $\mathfrak{a} = \mathfrak{p}$) ; on a donc $u \in \mathfrak{p}$, soit $u = vx$, $v \in A$, d'où $x = vxy$ et $x(1 - vy) = 0$; comme A est intègre, on a $x = 0$ ou $vy = 1$; or $x = 0$ entraîne $\mathfrak{p} = (0)$ qui est exclu, d'où $vy = 1$, soit $y \in A^\times$, et $\mathfrak{a} = A$.

Proposition 5.13 (Idéal premier de $\mathbb{Z}$) *Dans $\mathbb{Z}$, un idéal premier non nul est de la forme $p\mathbb{Z}$, p étant un nombre premier ($p \in \{2, 3, 5, 7, 11, 13, 17, \ldots\}$).*

Démonstration Soit $\mathfrak{p}$ un idéal premier $\neq (0)$ de $\mathbb{Z}$; comme $\mathbb{Z}$ est principal, $\mathfrak{p} = n\mathbb{Z}$, $n \in \mathbb{N}$, et $n \neq 0$, 1 (car $\mathfrak{p} \neq (0)$ et $\mathfrak{p} \neq \mathbb{Z}$). Si n n'est pas premier, on peut écrire $n = n'n''$, $n' > 1$, $n'' > 1$, et dans $\mathbb{Z}/n\mathbb{Z}$, on aurait $\overline{n'}\,\overline{n''} = \overline{0}$, soit, par exemple, $\overline{n'} = \overline{0}$ (intégrité), d'où n' multiple de n, ce qui est absurde puisque $n' = \dfrac{n}{n''} < n$. Donc n est un nombre premier. On sait alors que $p\mathbb{Z}$ (p premier) est un idéal premier puisqu'on sait que $\mathbb{Z}/p\mathbb{Z}$ est un corps ($p\mathbb{Z}$ est bien maximal).

Corollaire 5.14 (Caractérisation de $\mathbb{Z}/n\mathbb{Z}$ corps) *Pour que $\mathbb{Z}/n\mathbb{Z}$, $n \geq 0$, soit un corps, il faut et il suffit que n soit un nombre premier.*

Pour que $\mathbb{Z}/n\mathbb{Z}$ soit intègre, il faut et il suffit que n soit ou bien nul ou bien premier (autrement dit, tous les $\mathbb{Z}/n\mathbb{Z}$ intègres sont des corps sauf pour $n = 0$ où $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}$ qui n'est pas un corps).

Les corps $\mathbb{Z}/p\mathbb{Z}$, p premier, sont notés $\mathbb{F}_p$: ce sont des corps finis à p éléments.

Remarque Disons à titre de complément que pour tout $n \geq 1$, et pour tout premier p, il existe un corps fini à p^n éléments (admis) ; deux corps finis à p^n éléments sont isomorphes. Ceci justifie le fait que les corps finis soient notés $\mathbb{F}_{p^n}$, p premier, $n \in \mathbb{N} - \{0\}$. De ce fait, on s'interdira la notation $\mathbb{F}_n$ pour $\mathbb{Z}/n\mathbb{Z}$, n non premier, puisque dans ce cas $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps (et $\mathbb{F}$ est l'initiale de « field »). Ces aspects sont traités dans le cours « Corps » (Master 1).

5.4 Les nombres transcendants et algébriques

Soit $\mathbb{L}$ un corps, et soit $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Soit $\alpha \in \mathbb{L}$ et soit $h_\alpha : \mathbb{K}[X] \to \mathbb{L}$ l'homomorphisme d'évaluation en α. Soit $\mathfrak{a} = \mathrm{Ker}(h_\alpha)$; on a donc, par factorisation, $\mathbb{K}[X]/\mathfrak{a} \simeq \mathrm{Im}(h_\alpha)$ qui est un sous-anneau de $\mathbb{L}$, donc intègre ; il en résulte que $\mathbb{K}[X]/\mathfrak{a}$ est intègre, donc que $\mathfrak{a}$ est un idéal **premier** de $\mathbb{K}[X]$. Soit P_α un polynôme engendrant $\mathfrak{a}$ ($\mathbb{K}[X]$ étant principal) ; comme $\mathbb{K}[X]$ est lui-même intègre, deux cas se présentent :

1. ou bien $(P_\alpha) = (0)$
2. ou bien $(P_\alpha \neq (0)$ (et (P_α) est un idéal maximal de $\mathbb{K}[X]$)

Définition 5.15 *Dans le cas $(P_\alpha) = (0)$, on dit que $\alpha \in \mathbb{L}$ est transcendant sur $\mathbb{K}$.*
Dans le cas $(P_\alpha) \neq (0)$, on dit que $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$.

Exemples Les nombres complexes $\sqrt{2}$, i sont algébriques sur $\mathbb{Q}$. On démontre que les nombres e et π ne sont pas algébriques sur $\mathbb{Q}$ (leur transcendance fut très difficile à prouver : celle de e par Hermite en 1873, celle de π par Lindemann en 1882).

On démontre facilement que l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable et que son complémentaire dans $\mathbb{C}$ (i.e. l'ensemble des nombres transcendants) est non dénombrable (résultat de Cantor). On démontre que l'ensemble des nombres complexes algébriques (sur $\mathbb{Q}$) constitue un sous-corps de $\mathbb{C}$. Tout ceci est largement développé dans le cours « Corps ».

5.5 Caractéristique d'un anneau

5.5.1 Cas général

Proposition 5.16 (Homomorphisme caractéristique) *Soit A un anneau (on peut même se dispenser ici de la commutativité). Il existe un et un seul homomorphisme d'anneaux unitaires de $\mathbb{Z}$ dans A. Cet homomorphisme s'appelle l'homomorphisme caractéristique.*

$$h\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n1_A \end{array} = \begin{cases} 1_A + 1_A + \cdots + 1_A;\ n \text{ fois si } n > 0 \\ 0_A;\ \text{si } n = 0 \\ -1_A + (-1_A) + \cdots + (-1_A);\ -n \text{ fois si } n < 0 \end{cases}$$

Démonstration On définit h par une double récurrence en posant $h(0) = 0_A$, puis $h(n+1) = h(n) + 1_A$ pour $n > 0$; et $h(n) = h(n+1) + (-1_A)$ pour $n < 0$. On obtient bien ainsi $h(1) = 1_A$, $h(2) = 1_A + 1_A$, ... et aussi $h(-1) = -1_A$, $h(-2) = -1_A + (-1_A)$, ... Cela donne l'existence de l'application $h\colon \mathbb{Z} \longrightarrow A$, telle que décrite dans l'énoncé. On doit vérifier que h est un morphisme d'anneaux unitaire et que c'est le seul de $\mathbb{Z}$ dans A.

Par construction $h(1) = 1_A$. Soient $m, n \in \mathbb{Z}$. Pour démontrer $h(m+n) = h(m) + h(n)$, comme les additions dans $\mathbb{Z}$ et dans A sont commutatives, il suffit

de considérer le cas $n \geq 0$ et le cas $m < 0$ et $n < 0$. Pour $n \geq 0$ on procède par récurrence sur n. L'initialisation à $n = 0$ étant immédiate on traite l'hérédité. On suppose démontré pour un certain $k \geq 0$ l'égalité $h(m + k) = h(m) + h(k)$. Alors on a $h(m + k + 1) = h(m + k) + 1_A$ par construction de h, et donc par récurrence $h(m+k+1) = h(m)+h(k)+1_A = h(m)+h(k+1)$ de nouveau par construction de h. Cela démontre l'égalité $h(m+n) = h(m)+h(n)$ pour $n \geq 0$. Le cas $m < 0$ et $n < 0$ se traite de façon similaire, par récurrence sur $-n$. On peut déduire de l'additivité de h, ou bien de sa définition par récurrence, l'égalité $h(-m) = -h(m)$. En effet on $h(-m) + h(m) = h(-m + m) = h(0) = 0_A$ et donc $h(-m) + h(m) + (-h(m)) = h(-m)$. Pour démontrer l'égalité $h(mn) = h(m)h(n)$, on distingue les cas $m \geq 0$ et $m < 0$. Lorsque $m = 0$ on a $h(mn) = h(0) = 0_A = 0_A h(n) = h(m)h(n)$. Pour $m > 0$ on procède par récurrence sur m l'hérédité s'obtenant avec $h((k + 1)n) = h(kn + n) = h(kn) + h(n) = h(k)h(n) + h(n)$ par l'hypothèse de récurrence au rang k ; puis $h((k+1)n) = (h(k) + 1_A)h(n)$ par distributivité dans A et comme par construction $h(k)+1_A = h(k+1)$ on obtient bien l'hypothèse de récurrence au rang $k+1$. Pour $m < 0$ on procède aussi par récurrence sur $-m$. L'initialisation s'obtient avec le cas $m = 0$. Ensuite si on suppose l'hypothèse de récurrence pour un certain $k \leq 0$ alors au rang $k - 1$ on a $h((k - 1)n) = h(kn - n) = h(kn) + (h(-n)) = h(kn) - h(n)$ par additivité de h. Par l'hypothèse au rang k on obtient ensuite $h((k - 1)n) = h(k)h(n) + (-1_A)h(n) = (h(k) + (-1_A))h(n)$ par distributivité dans A. Par construction $h(k - 1) = h(k) + (-1_A)$ et on a bien établi l'hypothèse de récurrence au rang $k - 1$.

Cela démontre que h est bien un homomorphisme d'anneaux unitaires $h\colon \mathbb{Z} \longrightarrow A$.

Pour l'unicité si f est un homomorphisme d'anneaux unitaires $f\colon \mathbb{Z} \longrightarrow A$, alors la définition des homomorphismes impose $f(1) = 1_A = h(1)$. L'additivité de f suffit ensuite à démontrer par récurrence sur n l'égalité $h(n) = f(n)$ pour $n \geq 0$. Ensuite on a vu que si $n < 0$ alors $f(n) = -f(-n) = -h - (-n) = h(n)$ par additivité de f et h. .

Soit $\mathfrak{c} = \mathrm{Ker}(h)$; on a donc $\mathfrak{c} = c\mathbb{Z}$, $c \geq 0$, et l'anneau $\mathbb{Z}/c\mathbb{Z}$ est canoniquement isomorphe à l'image de h qui est aussi le plus petit sous-anneau de A. On remarque que si $A \neq \{0\}$, alors $1 \notin \mathfrak{c}$ et de ce fait $c \neq 1$.

Définition 5.17 (Caractéristique d'un anneau) *Le nombre c ainsi déterminé s'appelle la* ***caractéristique*** *de A. Pour la détermination pratique de c on utilise la caractérisation suivante :*

1. *Si $\{n \in \mathbb{N}, n1_A = 0\} = \{0\}$ alors $c = 0$.*
2. *Si $\{n \in \mathbb{N}, n > 0,\ n1_A = 0\} \neq \emptyset$ alors $c = \min\{n \in \mathbb{N}, n > 0,\ n1_A = 0\}$.*

En théorie des groupe cet entier c, si il est non nul, s'appelle aussi ***l'ordre additif de*** 1_A *; et on dit que 1_A est d'ordre infini si $c = 0$.*

Remarque Pour l'existence et l'unicité de l'homomorphisme caractéristique h, on utilise seulement que h est un morphisme de groupes additifs vérifiant $h(1) = 1_A$. Plus généralement, étant donné un groupe G et $g \in G$, on peut définir en suivant exactement cette démarche la fonction « puissance de g » qui est l'unique

homomorphisme de groupe $f\colon \mathbb{Z} \longrightarrow G$ tel que $f(1) = g$ (le cas particulier étudié ici est $G = A$ et $g = 1_A$). On démontre aussi que tous les homomorphismes de groupes partant de $\mathbb{Z}$ s'obtiennent ainsi. Comme on va le voir l'anneau $\mathbb{Z}$ est universel, au sens où le plus petit sous-anneau de tout anneaux est un quotient de $\mathbb{Z}$. Mais en réalité le groupe additif $\mathbb{Z}$ lui-même est universel et permet de décrire par produits et quotients tous les groupes commutatifs (qui doivent se comprendre comme des $\mathbb{Z}$-modules). Ces points seront sûrement développés dans le cours « Groupes » de la licence et aussi « Modules sur les anneaux principaux » du master.

Considérons les anneaux $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$, $\mathbb{Z}/1\mathbb{Z} = \{0\}$, $\mathbb{Z}/2\mathbb{Z}$, ..., $\mathbb{Z}/n\mathbb{Z}$, ... Dans chacun d'eux, l'unité 1_A est respectivement d'ordre infini, 1, 2, ..., n, ... Il en résulte que pour un anneau A, il existe un **unique** sous-anneau de A isomorphe à l'un des anneaux ci-dessus ; cet unique sous-anneau $A_1 = \mathrm{Im}(h)$ de A s'appelle le sous-anneau premier de A (ici premier est à prendre au sens de relation d'ordre, car c'est le plus petit : vérifier que A_1 est égal à l'intersection des sous-anneaux de A).

5.5.2 Cas des anneaux intègres et des corps

Proposition 5.18 (Caractéristique d'un anneau intègre) *Si A est un anneau intègre, sa caractéristique est soit 0 soit un nombre premier p. En conséquence, A contient un sous-anneau canoniquement isomorphe à $\mathbb{Z}$ (si $c = 0$) ou à $\mathbb{Z}/p\mathbb{Z}$ (si $c = p$ premier).*

Démonstration Si A est intègre, tout sous-anneau de A est aussi intègre, donc le sous-anneau $\mathrm{Im}(h)$ engendré par 1_A, est intègre, et on sait que $\mathrm{Im}(h) \simeq \mathbb{Z}/c\mathbb{Z}$; or les seuls $\mathbb{Z}/c\mathbb{Z}$ intègres sont $\mathbb{Z}$ ($c = 0$) et $\mathbb{Z}/p\mathbb{Z}$ ($c = p$ premier).

Corollaire 5.19 (Corps) *Si $\mathbb{L}$ est un corps, $\mathbb{L}$ contient un sous-corps canoniquement isomorphe soit à $\mathbb{Q}$ soit à $\mathbb{F}_p$ (p premier).*

En effet, si $c = 0$, d'après le corollaire 5.11 page 61, l'injection $\mathbb{Z} \to \mathbb{L}$ se prolonge en un unique homomorphisme injectif de $K_{\mathbb{Z}} = \mathbb{Q}$ dans $\mathbb{L}$.

Définition 5.20 (Sous-corps premier) *L'unique sous-corps d'un corps $\mathbb{L}$, isomorphe à l'un des corps $\mathbb{Q}$ ou $\mathbb{F}_p$ (p premier), s'appelle le* ***sous-corps premier*** *du corps $\mathbb{L}$.*

Remarques Si A est un anneau intègre de caractéristique nulle, alors A contient $\mathbb{Z}$ mais ne contient pas $\mathbb{Q}$ en général (pour le savoir, appliquer le théorème de prolongement 5.10 page 61, autrement dit, voir si $\mathbb{Z} - \{0\}$ est contenu dans $A^\times$). Par exemple $\mathbb{Z}$ lui-même ; en revanche, $\mathbb{Q}[X]$ contient $\mathbb{Q}$ mais n'est pas un corps.

5.5.3 Caractéristique d'un produit d'anneaux

Soient $A_1, \ldots, A_n$ des anneaux de caractéristiques respectives $c_1, \ldots, c_n$. On définit A par $A = A_1 \times \cdots \times A_n$ et on note $1_A = (1_{A_1}, \ldots, 1_{A_n})$ l'unité de l'anneau produit A.

Proposition 5.21 (Caractéristique d'un produit d'anneaux) *Si l'un des anneaux A_i est de caractéristique 0, l'anneau A est de caractéristique 0. Si les c_i sont toutes non nulles, alors la caractéristique de A est égale à $\underset{i=1,\ldots,n}{ppcm}(c_i)$* [1].

Démonstration On calcule $\lambda 1_A = \lambda(1_{A_1}, \ldots, 1_{A_n}) = (\lambda 1_{A_1}, \ldots, \lambda 1_{A_n})$, pour $\lambda \in \mathbb{N}$, qui est égal à $(0, \ldots, 0)$ si et seulement si $\lambda 1_{A_1} = 0$ pour tout $i = 1, \ldots, n$. Si pour au moins un j, $1 \leq j \leq n$, A_j est de caractéristique 0, on a donc $\lambda 1_{A_j} = 0$ si et seulement si $\lambda = 0$, et A est de caractéristique 0 (1_{A_j} est d'ordre infini dans $(A_j, +)$). Si tous les A_i sont de caractéristique non nulle, $\lambda 1_A = 0$ si et seulement si λ est multiple de c_i pour $i = 1, \ldots, n$. D'où le résultat.

Fin du cinquième chapitre

1. En fait, comme on a en réalité $\text{ppcm}(a, 0) = 0$ pour tout $a \in \mathbb{Z}$ (voir chapitre 6, remarque page 70), la formule vaut en général.

Chapitre 6

Divisibilité dans les anneaux intègres. Anneaux factoriels

C'est le chapitre fondamental qui aborde l'arithmétique proprement dite.

Dans tout le chapitre, on suppose que A est un anneau commutatif **intègre** dont l'élément unité est noté 1.

6.1 Définitions et notations

Définition 6.1 (Divisibilité) *Dans A on dit que b divise a (ce que l'on note $b \mid a$), s'il existe $c \in A$ tel que $a = bc$. On remarque que $b \mid a$ si et seulement si $Aa \subseteq Ab$. Par exemple $0 \mid 0$.*

Définition 6.2 (Irréductibilité) *Cette notion concerne les éléments de $A - A^\times$: on dit que $a \in A - A^\times$ est **irréductible** si toute relation de la forme $a = bc$, b, $c \in A$, implique nécessairement $b \in A^\times$ **ou** $c \in A^\times$ (remarquer que l'on peut toujours écrire $a = a \times 1$, ou même $a = (au^{-1})u$, pour tout $u \in A^\times$, mais ces décompositions sont sans intérêt du point de vue de la factorisation de a dans A). On dira qu'un élément $a \in A - A^\times$ est réductible s'il n'est pas irréductible, soit s'il existe b et $c \in A - A^\times$ (i.e. b et c non inversibles) tels que $a = bc$. On remarquera que 0 est réductible.*

Remarques

1. Par définition, tout élément b de A divise 0 ; cependant b n'est pas un « diviseur de zéro » au sens de la section 5.1 du chapitre 5 (simple facétie de vocabulaire).
   Si l'on prend l'inclusion des idéaux $\Big((a) \subseteq (b)\Big)$ comme définition de la divisibilité $(b \mid a)$, on voit que le cas $a = b = 0$ n'a rien de pathologique.
2. En ce qui concerne l'irréductibilité, elle est souvent énoncée sur A (ou sur $A - \{0\}$), ce qui conduit alors à l'énoncé suivant : « un élément $a \in A$ (ou $A - \{0\}$) est dit irréductible s'il est non inversible et si la relation $a = bc$, b, $c \in A$, implique $b \in A^\times$ **ou** $c \in A^\times$ ».
   Ceci ne change pas le résultat (l'ensemble des éléments irréductibles est le même dans les deux cas), cependant cela change la façon de voir la négation

d'irréductible : en effet, dire que $a \in A$ (ou $A - \{0\}$) n'est pas irréductible équivaut à :

$$\begin{array}{ll} a \in A^\times & \textbf{ou} \quad (\text{il existe } b,\, c \in A - A^\times \text{ tels que } a = bc) \\ & \Longleftrightarrow \\ a \in A^\times & \textbf{ou} \quad (a \in A - A^\times \text{ est réductible}) \end{array}$$

Autrement dit, la négation de « irréductible dans A (ou $A - \{0\}$) » n'est pas « réductible » au sens de la définition 6.2. Simple question de logique. On préférera la définition 6.2 qui répartit en fait les éléments de A selon trois sous-ensembles disjoints :
Le sous-ensemble $A^\times$, qui contient au moins 1 ; le sous-ensemble des éléments réductibles, qui contient au moins 0 ; et le sous-ensemble des éléments irréductibles (qui est vide si A est un corps).

3. Les définitions concernant la divisibilité et l'irréductibilité restent valables même si A n'est pas intègre, mais pas celles qui suivront.

Définition 6.3 (Association) *On dit que deux éléments $a, b \in A$ sont **associés** s'il existe $u \in A^\times$ tel que $a = bu$.*

Définition 6.4 (Factorialité) *On dit que A (commutatif intègre) est **factoriel** lorsque la propriété suivante est vérifiée :*

Tout $a \neq 0$ de A s'écrit $a = up_1 \dots p_n$, $n \geq 0$, $u \in A^\times$, p_i irréductible de A pour $i = 1, \dots, n$, et, si l'on a deux décompositions analogues $a = up_1 \dots p_n = vq_1 \dots q_m$, n, $m \geq 0$, u, $v \in A^\times$, p_i, q_j irréductibles de A pour $i = 1, \dots, n$, $j = 1, \dots, m$, alors $m = n$ et il existe une permutation σ de $\{1, \dots, n\}$ telle que q_i et $p_{\sigma(i)}$ soient associés, pour $i = 1, \dots, n$.

Dans l'ensemble des éléments irréductibles de A, soit $\mathcal{P}$ un système exact de représentants des classes pour l'association dans A (ceci a un sens car l'associé d'un irréductible est encore irréductible, donc le sous-ensemble des irréductibles de A est une réunion de classes) ; pour abréger, on appellera $\mathcal{P}$ un « système d'irréductibles » de A. Lorsqu'un tel système $\mathcal{P}$ est fixé, la factorialité de A équivaut à dire que tout élément $a \neq 0$ de A s'écrit de façon unique (à l'ordre près des facteurs) $a = up_1 \dots p_n$, $n \geq 0$, $u \in A^\times$, $p_i \in \mathcal{P}$ pour $i = 1, \dots, n$. Dans tout anneau factoriel, on fera une fois pour toutes le choix d'un tel système $\mathcal{P}$.

Remarque Dans la factorisation $a = up_1 \dots p_n$ de $a \in A - \{0\}$, certains $p_i \in \mathcal{P}$ peuvent se répéter ; il est donc normal d'écrire $a = up_1^{\alpha_1} \dots p_k^{\alpha_k}$, $k \geq 0$, $\alpha_i \geq 1$, les $p_i \in \mathcal{P}$ étant distincts cette fois. Pour avoir une écriture encore plus souple et qui n'introduise pas un ordre particulier dans l'écriture des p_i [1], on écrit $a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$, en convenant du fait que les $\alpha_p \in \mathbb{N}$ sont presque tous nuls (i.e. tous sauf un nombre fini). Par exemple, dans $\mathbb{Z}$, si l'on prend $\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}$, alors $-20 = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$ avec $u = -1$, $\alpha_2 = 2$, $\alpha_3 = 0$, $\alpha_5 = 1$, $\alpha_p = 0$ pour $p = 7, 11, \dots$ Ceci introduit la notion de valuation qui va être développée dans la section 6.2.

1. Ce qui n'a pas de sens dans un anneau général, le cas de $\mathbb{Z}$ induisant en erreur, à cause de son ordre naturel.

6.2 Propriétés des anneaux factoriels

Définition 6.5 (Valuation d'un anneau factoriel) *Soit A un anneau factoriel et soit $p \in \mathcal{P}$ un irréductible de A. Comme tout $a \in A - \{0\}$ s'écrit de façon* ***unique*** $u \prod_{q \in \mathcal{P}} q^{\alpha_q}$ [2], *$u \in A^\times$, $\alpha_q \in \mathbb{N}$, il en résulte que α_p est unique ($\alpha_p \geq 0$) et que, en associant à a la valeur α_p, on définit une application de $A - \{0\}$ dans $\mathbb{N}$, notée v_p, et appelée la* ***valuation p-adique*** *de A.*

Lemme 6.6 (Valuation d'un produit) *On a : $v_p(ab) = v_p(a) + v_p(b)$, pour tout $a, b \in A - \{0\}$.*

En effet, écrivons $a = u \prod_{q \in \mathcal{P}} q^{v_q(a)}$, $b = v \prod_{q \in \mathcal{P}} q^{v_q(b)}$, u, $v \in A^\times$; alors :

$$ab = uv \prod_{q \in \mathcal{P}} q^{v_q(a)+v_q(b)}$$

Par unicité de l'écriture de ab sous la forme analogue $w \prod_{q \in \mathcal{P}} q^{v_q(ab)}$, $w \in A^\times$, on obtient $w = uv$ et, surtout, $v_p(ab) = v_p(a) + v_p(b)$, pour tout $p \in \mathcal{P}$.

Soit maintenant K_A le corps des fractions de A. On étend v_p à $K_A^\times$ de la façon suivante : soit $x \in K_A^\times$, $x = ab^{-1}$, a, $b \in A - \{0\}$; montrons que si l'on pose $v_p(x) = v_p(a) - v_p(b)$ on définit une application : soit $x = a'b'^{-1}$ une autre fraction représentant x ; on a donc $a'b - ba' = 0$, soit $a'b = ba'$ dans A, ce qui donne $v_p(a'b) = v_p(b'a)$, soit $v_p(a') + v_p(b) = v_p(b') + v_p(a)$, soit $v_p(a) - v_p(b) = v_p(a') - v_p(b')$, d'où l'invariance de la définition de v_p sur $K_A^\times$. Bien entendu, ici $v_p(x) \in \mathbb{Z}$.

Remarque Par commodité, on prolonge v_p à K_A en posant $v_p(0) = +\infty$; v_p est alors à valeurs dans l'ensemble $\mathbb{Z} \cup \{\infty\}$ sur lequel on étend les opérations et les relations habituelles en posant : $n + \infty = \infty$, $n < \infty$, pour tout $n \in \mathbb{Z}$.

Théorème 6.7 (Valuation d'une somme) *Dans l'anneau factoriel A, on a, pour tout x, $y \in K_A$, et tout $p \in \mathcal{P}$,*
$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, et $v_p(x + y) = \min\{v_p(x), v_p(y)\}$ lorsque $v_p(x) \neq v_p(y)$.

Démonstration On peut supposer x et y non nuls, sinon le résultat est immédiat. Posons $v_p(x) = \alpha$, $v_p(y) = \beta$, puis $x' = p^{-\alpha}x$, $y' = p^{-\beta}y$; il vient immédiatement $v_p(x') = v_p(y') = 0$. Posons $x' = \dfrac{a}{b}$, $y' = \dfrac{c}{d}$, a, b, c, $d \in A$ (non nuls par hypothèse) ; comme $v_p(x') = 0$, on a $v_p(a) = v_p(b)$, et on peut représenter $\dfrac{a}{b}$ de telle sorte que p ne divise ni a ni b $\left(\text{de même pour } \dfrac{c}{d}\right)$. Supposons par exemple $\alpha \geq \beta$; on a $x + y = p^\alpha \dfrac{a}{b} + p^\beta \dfrac{c}{d} = p^\beta \left(\dfrac{p^{\alpha-\beta}a}{b} + \dfrac{c}{d}\right) = p^\beta \left(\dfrac{p^{\alpha-\beta}ad + bc}{bd}\right)$, et $p^{\alpha-\beta}ad + bc \in A$ (car $\alpha - \beta \geq 0$, donc $p^{\alpha-\beta} \in A$) ;

2. Ici, l'indice q est « muet » (i.e. ne figure pas dans l'expression) ; il ne faut pas utiliser l'indice p, p ayant été fixé au départ.

1. si $\alpha > \beta$, $v_p(x+y) = v_p(p^\beta)+v_p(p^{\alpha-\beta}ad+bc)-v_p(bd) = \beta+v_p(p^{\alpha-\beta}ad+bc)$ car $v_p(b) = v_p(d) = 0$; l'élément $p^{\alpha-\beta}ad + bc$ de A n'est pas multiple de p (sinon bc le serait, par différence ; or $v_p(bc) = v_p(b) + v_p(c) = 0$), d'où le résultat dans ce cas : $v_p(x + y) = \beta$ qui est bien égal à $\min\{v_p(x), v_p(y))\}$;
2. si $\alpha = \beta$, le même calcul que ci-dessus conduit à $v_p(x+y) = \beta+v_p(ad+bc) \geq \beta$ car $ad + bc$ est dans A, donc de valuation positive ou nulle (on ne peut rien dire de plus précis ici car $ad+bc$ pourrait être divisible par une puissance non nulle de p (exemple : $\frac{7}{2}+\frac{2}{3} = \frac{25}{6}$, avec $p = 5$, sans parler de la simple relation $v_p\Big(x + (-x)\Big) = \infty$).

Définition 6.8 *Soit A un anneau factoriel, et soient a, $b \in A$* ***non nuls****. On appelle successivement :*

1. ***pgcd*** *de a et b, tout élément de A de la forme $u \prod_{p\in\mathcal{P}} p^{\min\{v_p(a),v_p(b)\}}$, $u \in A^\times$*
2. ***ppcm*** *de a et b, tout élément de A de la forme $v \prod_{p\in\mathcal{P}} p^{\max\{v_p(a),v_p(b)\}}$, $v \in A^\times$*

(tous les produits écrits existent).

Remarque Si par exemple $b = 0$, $a \neq 0$, on voit que la formule définissant les pgcd a un sens et donne $\text{pgcd}(a, 0) = ua$, $u \in A^\times$ (en effet, on a $\min\{v_p(a), \infty\} = v_p(a)$ pour tout $p \in \mathcal{P}$) ; en revanche, comme $\max\{v_p(a), \infty\} = \infty$, celle donnant les ppcm n'est pas définie car et le produit $\prod_{p\in\mathcal{P}} p^\infty$ n'a pas de sens, et ceci pour deux raisons : p^∞ n'a pas de sens et le produit est infini dès que $\mathcal{P}$ l'est ; cependant, de même que l'on a posé $v_p(0) = \infty$, on peut admettre que ceci caractérise 0, et que la factorisation symbolique p^∞ représente 0 quel que soit p. Ceci explique que, de toutes façons, on pose $\text{ppcm}(a, b) = 0$, dès que $a = 0$ **ou** $b = 0$, et de même $\text{pgcd}(a, b) = 0$ dès que $a = 0$ **et** $b = 0$.

Remarquons que les nombres $\text{pgcd}(a, b)$, a, b fixés, constituent exactement une classe d'équivalence pour la relation d'association. On verra, dans certains cas, que les classes pour l'association ont un représentant canonique (par exemple les nombres positifs (ou 0) pour $A = \mathbb{Z}$, les polynômes unitaires (ou le polynôme nul) dans le cas $A = \mathbb{K}[X]$, où $\mathbb{K}$ est un corps). Dans le cas contraire il n'est pas possible de parler **du** pgcd (ou ppcm) de a et b.

Enfin, on définit de façon analogue les pgcd et ppcm de n éléments d'un anneau factoriel A ($n \geq 2$).

Définition 6.9 (Éléments étrangers) *Dans un anneau factoriel A, on dit que a et b sont* ***étrangers*** *(ou* ***premiers entre eux****) si les pgcd de a et b sont inversibles. Par exemple, a et 0 sont étrangers si et seulement si $a \in A^\times$.*

Remarque On définit de façon analogue le fait que n éléments de A sont étrangers dans leur ensemble (peu utilisé si $n \geq 3$, car c'est différent d'être étrangers deux à deux).

Théorème 6.10 *Soit d (resp. m) un pgcd (resp. un ppcm) de a et $b \in A$ (A factoriel) ; alors d et m ont les propriétés suivantes*

1. $\{c \in A,\ c \mid a$ ***et*** $c \mid b\} = \{c \in A,\ c \mid d\}$
2. $\{c \in A,\ a \mid c$ ***et*** $b \mid c\} = \{c \in A,\ m \mid c\}$
3. $(ab) = (dm)$.

Lemme 6.11 (Lien entre divisibilité et valuation) *Si x, $y \in A$, alors $x \mid y$ si et seulement si $v_p(x) \leq v_p(y)$, pour tout $p \in \mathcal{P}$.*

On a $x \mid y$ si et seulement si il existe $z \in A$ tel que $y = zx$; si ceci a lieu, on a $v_p(y) = v_p(z) + v_p(x) \geq v_p(x)$ (dans $\mathbb{N} \cup \{\infty\}$) pour tout $p \in \mathcal{P}$. Inversement, supposons $v_p(y) \geq v_p(x)$ pour tout $p \in \mathcal{P}$; si $y = 0$, on a $x \mid y$, et si $x = 0$, l'hypothèse implique $v_p(y) = \infty$ pour tout $p \in \mathcal{P}$, et $x = y = 0$ (on obtient $0 \mid 0$) ; dans les cas restants, il suffit de poser $z = \prod_{p \in \mathcal{P}} p^{v_p(y) - v_p(x)}$, qui est dans A car $v_p(y) \geq v_p(x)$ (dans $\mathbb{N}$) pour tout p, et $v_p(x) - v_p(y) = 0$ pour presque tout p ; on voit alors que xz et y sont associés, donc que $x \mid y$.

Les deux premières justifient les terminologies de « pgcd » et « ppcm ».

Démonstration du théorème 6.10 page 71 Les points 1 et 2 résultent de l'utilisation systématique de ce lemme (écrire les détails). Quant à 3, pour a et b non nuls, on remarque facilement que pour deux entiers quelconques α, $\beta \in \mathbb{N}$, on a toujours l'égalité : $\min\{\alpha, \beta\} + \max\{\alpha, \beta\} = \alpha + \beta$; donc ici, on a :

$$\begin{aligned} v_p(dm) &= v_p(d) + v_p(m) \\ &= \min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} \quad \text{(par définition de } d \text{ et } m) \\ &= v_p(a) + v_p(b) = v_p(ab) \quad \text{pour tout } p \in \mathcal{P} \end{aligned}$$

d'où les relations $ab \mid dm$ et $dm \mid ab$, soit ab et dm associés. Si $a = 0$ ou $b = 0$, l'égalité est évidente puisque $m = 0$.

Théorème 6.12 *Soient a, b deux éléments arbitraires d'un anneau factoriel A.* ***Si*** *l'idéal engendré par a et b est principal,* ***alors*** *tout générateur de cet idéal est un pgcd de a et b.*

Démonstration En effet, si $(a,b) = (c)$, $c \in A$, il est clair que l'on a $a = ca'$, $b = cb'$, a', $b' \in A$, d'où $c \mid d$; si d est un pgcd de a et b, écrivons $a = da''$, $b = db''$, a'', $b'' \in A$, et $c = as + bt$, s, $t \in A$, alors il vient $c = d(a''s + b''t)$, et $d \mid c$, ce qui conduit au résultat.

Corollaire 6.13 (Si l'idéal engendré est A) *Si $(a, b) = A$, alors a et b sont étrangers.*

Remarque

Si l'idéal engendré par a et b n'est pas principal, cette propriété peut tomber en défaut : par exemple, dans $\mathbb{Z}[X]$, dont on prouvera la factorialité à la section 6.4, les éléments $a = X + 1$ et $b = X - 1$ sont étrangers ; un pgcd est donc égal à 1, mais $(X + 1, X - 1)$ n'est pas égal à A (c'est un idéal maximal de A comme on peut le vérifier facilement). Dans un anneau **factoriel non principal**, il n'y a pas nécessairement de relation de Bézout entre a, b et un pgcd.

Théorème 6.14 *Soit A un anneau factoriel.*

1. *Si un élément irréductible p de A divise ab $(a, b \in A)$, alors p divise a **ou** p divise b.*
2. *Si $c \in A$ divise ab et est étranger à b, alors c divise a.*

Démonstration On remarque d'abord que la relation $p \mid c$ $(c \in A)$ équivaut à $v_p(c) \geq 1$. Comme $v_p(ab) = v_p(a) + v_p(b)$, si $p \mid ab$ on a $v_p(a) + v_p(b) \geq 1$; or a et b étant dans A, on a $v_p(a) \geq 0$, $v_p(b) \geq 0$, donc ou bien on a $v_p(a) \geq 1$, ou bien $v_p(b) \geq 1$, c'est-à-dire $p \mid a$ ou $p \mid b$ (cf. lemme 6.11 page 71).

Pour le second point, il suffit de montrer que $v_p(a) \geq v_p(c)$ pour tout $p \in \mathcal{P}$. Par hypothèse, on a $\min\{v_p(a) + v_p(b), v_p(c)\} = v_p(c)$, d'où $v_p(a) + v_p(b) \geq v_p(c)$ et, par hypothèse, on a aussi $\min\{v_p(b), v_p(c)\} = 0$. Si $v_p(b) = 0$ alors $v_p(a) \geq v_p(c)$; si $v_p(b) > 0$, nécessairement $v_p(c) = 0$, d'où $v_p(a) \geq v_p(c)$ dans tous les cas.

Remarque La seconde propriété s'appelle aussi le théorème de Gauss, en arithmétique.

Corollaire 6.15 *Dans un anneau factoriel A, si $p \in A$, on a l'équivalence suivante : p est irréductible si et seulement si (p) est un idéal premier $\neq (0)$.*

En effet, supposons p irréductible et prenons un produit ab, $a, b \in A$ tel que $ab \in (p)$; on a $ab = pc$, $c \in A$, et alors $p \mid a$ ou $p \mid b$, donc $a \in (p)$ ou $b \in (p)$. On a enfin $(p) \neq A$ car sinon on aurait $p \in A^\times$ ce qui est absurde, et de même, on a $(p) \neq (0)$ car $p \neq 0$.

Si l'on suppose (p) premier $\neq (0)$, on a $p \notin A^\times$, sinon on aurait $(p) = A$, ce qui n'est pas, et si l'on peut écrire $p = rs$, r, $s \in A$, ceci donne $rs \in (p)$, soit $r \in (p)$ ou $s \in (p)$; or, par exemple, $r \in (p)$ signifie $r = ap$, $a \in A$, ce qui donne $p = rs = aps$, soit $as = 1$ puisque A est intègre et que l'on a $(p) \neq (0)$; d'où $s \in A^\times$.

Remarques

1. L'implication : (p) premier non nul entraîne p irréductible, est vraie dans tout anneau intègre (la démonstration ci-dessus n'utilisant que l'intégrité).
2. On remarquera également que le fait que les éléments irréductibles soient des éléments de $A - A^\times$ (par définition) est cohérent avec la notion d'idéal premier.

6.3 Cas des anneaux principaux

On rappelle que « A est un anneau principal » veut dire « A est commutatif intègre et ses idéaux sont principaux ».

Théorème 6.16 (Factorialité d'un anneau principal) *Un anneau principal est factoriel.*

Démonstration Il y a deux parties : il faut d'abord prouver que **tout** élément $a \neq 0$ de A se factorise en un produit de la forme $u \prod_{p \in \mathcal{P}} p^{\alpha_p}$ ($u \in A^\times, \alpha_p \in \mathbb{N}$, presque tous nuls, p parcourant un système d'irréductibles $\mathcal{P}$ de A), puis ensuite montrer l'unicité des décompositions.

1. Supposons qu'il existe des $a \neq 0$ de A non factorisables (sous la forme ci-dessus). On appelle $\mathcal{F}$ l'ensemble des idéaux (a) de A tels que a ne soit pas factorisable ; on vient donc de supposer $\mathcal{F}$ non vide. On ordonne $\mathcal{F}$ par inclusion.

   Soit une chaîne d'éléments de $\mathcal{F}$ de la forme particulière suivante :

   $$(a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_i) \subsetneqq \cdots \quad \text{(finie ou non)},$$

   et soit $\mathfrak{a}$ la réunion de ses éléments. On a déjà vu que, dans une telle situation, $\mathfrak{a} = \bigcup_{i \geq 1} (a_i)$ est un idéal de A (le revoir en exercice). Puisque A est principal, on a $\mathfrak{a} = (a)$, $a \in A$; donc $a \in \bigcup_{i \geq 1} (a_i)$, et il existe $n \geq 1$ tel que $a \in (a_n)$, et on a donc les inclusions $(a) \subseteq (a_n)$ (car $a \in (a_n)$) et $(a_n) \subseteq (a)$ (car $(a_n) \subseteq \mathfrak{a}$ par définition d'une réunion), ce qui donne $(a_n) = (a)$.

   Ceci veut dire que toute chaîne du type précédent est nécessairement limitée à un certain indice n ; donc ces chaînes sont nécessairement **finies**, car on a supposé leurs éléments distincts.

   On a donc prouvé que dans $\mathcal{F}$ il était impossible d'écrire des chaînes **infinies** d'éléments **distincts** de $\mathcal{F}$: elles sont toutes finies.

   On peut affirmer que parmi ces chaînes il en existe une, notée :

   $$(a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_n)$$

   qui n'est pas prolongeable dans $\mathcal{F}$ (i.e. telle que l'on ne puisse pas trouver $(a_{n+1}) \in \mathcal{F}$ telle que $(a_n) \subsetneqq (a_{n+1})$) : en effet, si toute chaîne d'éléments de $\mathcal{F}$ était prolongeable, on pourrait construire une chaîne infinie, ce qui n'est pas. Conservons une telle chaîne non prolongeable, et retenons que si (b) est un idéal de A tel que $(a_n) \subsetneqq (b)$, par définition d'une chaîne non prolongeable, on a $(b) \notin \mathcal{F}$; ceci veut dire, par définition de $\mathcal{F}$, que b est **factorisable**. Utilisons cette remarque à partir de l'élément a_n : l'élément a_n de la chaîne trouvée n'est ni inversible, ni irréductible (car tout irréductible ou tout inversible est factorisable de façon triviale)[3] ; donc, dans A, il existe b, $c \notin A^\times$ tels que

3. Il est donc réductible au sens de la définition 6.2 page 67 (revoir 3 page 68).

$a_n = bc$; ceci entraîne $(a_n) \subsetneqq (b)$ et $(a_n) \subsetneqq (c)$ (les inclusions résultent des relations $b \mid a_n$ et $c \mid a_n$, et le fait qu'elles soient strictes provient du fait que b et c sont non inversibles) ; d'après ce que l'on a dit juste avant, b et c sont factorisables, ce qui entraîne que leur produit est factorisable (i.e. que a_n est factorisable), ce qui est absurde. Donc $\mathcal{F}$ est vide.

2. Démontrons l'unicité des décompositions, par récurrence sur n dans l'égalité

$$up_1 \dots p_n = vq_1 \dots q_m \qquad (m \geq n \geq 0,\ u,\ v \in A^\times,\ p_i,\ q_j \in \mathcal{P}).$$

Remarque on n'a pas le droit d'utiliser le théorème de Gauss, qui suppose A factoriel.

Le cas $n = 0$ entraîne $u = vq_1 \dots q_m \in A^\times$, d'où $1 = u^{-1}vq_1 \dots q_m$, et $m = 0$ (sinon les q_j seraient dans $A^\times$), puis $u = v$.

Supposons $n \geq 1$ et la propriété vraie au rang $n-1$, et considérons l'égalité $up_1 \dots p_n = vq_1 \dots q_m$ $(m \geq n)$; supposons que p_1 soit distinct de tous les q_j, $j = 1, \dots, m$; dans ce cas considérons les idéaux (p_1, q_j) pour tout j : ils sont de la forme (b_j), $b_j \in A$, et on peut écrire $p_1 = b_j c_j$, $c_j \in A$ pour $j = 1, \dots, m$. Comme p_1 est irréductible, b_j ou c_j est dans $A^\times$; si $c_j \in A^\times$, $(p_1) = (b_j)$ et $q_j \in (p_1)$, soit $q_j = p_1 d_j$, $d_j \in A$, et comme q_j est irréductible on a $d_j \in A^\times$ (puisque c'est impossible ici pour p_1), et, pour cet indice j, q_j et p_1 sont associés, donc égaux par définition de $\mathcal{P}$, or ceci n'est pas ; donc c'est toujours b_j qui est dans $A^\times$, pour $j = 1, \dots, m$, et $\boldsymbol{(p_1, q_j) = A}$.

On peut donc écrire pour tout j, $1 = \lambda_j p_1 + \mu_j q_j$, λ_j, $\mu_j \in A$, soit (en utilisant les congruences) $\mu_j q_j \equiv 1 \bmod p_1$, ce qui donne, par multiplication de ces m congruences, $\prod_{j=1}^{m} \mu_j q_j \equiv 1 \bmod p_1$; or $q_1 \dots q_m \equiv 0 \bmod p_1$ (puisque $q_1 \dots q_m = uv^{-1}p_1 \dots p_n$) et ceci est absurde car ceci conduit à $0 \equiv 1 \bmod p_1$ [4]. Donc p_1 est l'un des q_j et, après simplification, on est ramené à l'hypothèse de récurrence ; d'où la conclusion.

Citons un résultat important en pratique :

Corollaire 6.17 *Dans un anneau principal A, tout élément irréductible p engendre un idéal maximal de A, et inversement.*

Ceci résulte du fait que l'idéal (p) est premier non nul (corollaire 6.15 page 72) et l'anneau A principal (théorème 5.12 page 62 du chapitre 5).

Corollaire 6.18 *Si a, b sont deux éléments quelconques d'un anneau principal A, si d est un pgcd de a et b, alors il existe u, $v \in A$ tels que $d = ua + vb$.*

Ceci résulte de la factorialité de A jointe au résultat du théorème 6.12 page 71.

4. On peut aussi utiliser la co-maximalité : (p_1), (q_j) co-maximaux $\Rightarrow (p_1), \prod(q_j)$ co-maximaux, ce qui conduit à $\lambda p_1 + \mu q_1 \dots q_m = 1$, d'où $p_1 | 1$, ce qui est absurde.

Exemples Les anneaux $\mathbb{Z}$, $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps) sont principaux (grâce aux résultats 2 page 20 et 1 page 20 du chapitre 2) ; de même, on a montré que l'anneau des entiers de Gauss, $\{a+bi,\ a,\ b \in \mathbb{Z}\}$, est principal. Ces anneaux sont donc factoriels. Le problème est donc, lorsqu'un anneau est factoriel, de trouver ses éléments irréductibles : leur détermination systématique peut parfois être extrêmement difficile ; analysons un peu différents cas, en laissant à titre d'exercice (que l'on devra rédiger avec soin) les démonstrations qui sont très faciles :

Cas de $\mathbb{Z}$: Dans ce cas on peut prendre pour $\mathcal{P}$ l'ensemble des nombres premiers (positifs) $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\}$; établir leur liste jusqu'à 100 pour se convaincre du fait qu'il n'existe pas de caractérisation « simple » du k-ième nombre premier.

Cas de $\mathbb{K}[X]$ ($\mathbb{K}$ étant un corps) : Dans ce cas, un moyen simple pour avoir des polynômes non associés est de les prendre unitaires (coefficient dominant égal à 1) (en effet, on démontrera pour cela que $A^\times = \mathbb{K}^\times$ ici). Mais $\mathcal{P}$ n'est pas forcément mieux constructible que pour le cas de $\mathbb{Z}$ (par exemple, dans $\mathbb{Q}[X]$, la caractérisation des polynômes irréductibles est très difficile). Citons cependant deux exemples pour lesquels le résultat est bien connu :

1. $A = \mathbb{C}[X]$. Montrer que dans ce cas, on peut prendre pour $\mathcal{P}$, l'ensemble $\{X - z,\ z \in \mathbb{C}\}$.
2. $A = \mathbb{R}[X]$. Montrer que dans ce cas, on peut prendre pour $\mathcal{P}$, l'ensemble $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, où

$$\begin{cases} \mathcal{P}_1 = \{X - a,\ a \in \mathbb{R}\} \\ \mathcal{P}_2 = \{X^2 + bX + c,\ b,\ c \in \mathbb{R},\ b^2 - 4c < 0\} \end{cases}$$

Bien que les résultats soient simples dans ces deux cas, on sera obligé, pour leur démonstration, d'admettre le difficile théorème de d'Alembert, à savoir que dans $\mathbb{C}[X]$ tout polynôme de degré $d \geq 1$ admet au moins une racine dans $\mathbb{C}$.

Le corollaire 6.18 admet l'énoncé réciproque suivant :

Théorème 6.19 *Soit A un anneau factoriel dans lequel tout pgcd est donné par une relation de Bézout (i.e. pour tout a, $b \in A$, il existe u, $v \in A$ tels que $pgcd(a, b) = au + bv$). Alors A est un anneau principal.*

Démonstration Soit $\mathfrak{a}$ un idéal non nul de A $\Big((0)$ étant principal$\Big)$, et soit $a \in \mathfrak{a}$, $a \neq 0$. Considérons les chaînes finies, d'idéaux principaux, de la forme suivante ($n \geq 0$) :

$$(a) \subsetneqq (a_1) \subsetneqq \cdots \subsetneqq (a_n) \subseteq \mathfrak{a}$$

Ceci induit les relations de divisibilité $a_n \mid a_{n-1} \mid \ldots \mid a_1 \mid a$, et les nombres a_1, a_2, …, a_n sont donc des diviseurs de a non associés deux à deux. Comme A est factoriel, on peut écrire

$$a = u \prod_{i=1}^{\ell} p_i^{\alpha_i}, \quad u \in A^\times, \quad p_i \text{ irréductibles distincts de } A, \quad \alpha_i \geq 1$$

le nombre de diviseurs (considérés à association près) de a est fini : en effet, si $b \mid a$, $b = v\prod_{i=1}^{\ell} p_i^{\beta_i}$, $v \in A^\times$, $0 \leq \beta_i \leq \alpha_i$, l'un au moins des β_i étant strictement inférieur à α_i (sinon a et b sont associés) ; ce nombre de diviseurs (à association près) est même majoré par $N = \sum_{i=1}^{\ell} \alpha_i$. Donc n est majoré par N.

Considérons une chaîne de la forme précédente, avec n maximum, et montrons que $\mathfrak{a} = (a_n)$, ce qui achèvera la démonstration : si $(a_n) \subsetneqq \mathfrak{a}$, il existe $b \in \mathfrak{a} - (a_n)$, auquel cas nous avons :

$$(a_n) \subsetneqq (a_n) + (b) \subseteq \mathfrak{a}$$

or par hypothèse, si d est un pgcd de a_n et b, il existe u, $v \in A$ tels que $ua_n + vb = d$, d'où $(a_n) + (b) = (d)$ (comme a_n, $b \in (d)$ une inclusion est triviale, et la relation de Bézout signifie que $d \in (a_n) + (b)$), ce qui contredit le caractère maximal de n. On a donc $(a_n) = \mathfrak{a}$.

Conclusion L'arithmétique, en nombres, dans un anneau factoriel A, est identique à l'arithmétique usuelle (caractéristique des anneaux principaux), **sauf** en ce qui concerne l'existence des relations de Bézout qui suppose A principal.

Remarque Dans $\mathbb{Z}$, les « nombres premiers » sont précisément les irréductibles positifs. La dénomination de « premier » (utilisée pour $\mathbb{Z}$) est dangereuse pour un anneau quelconque ; en effet, si un idéal principal (p) est premier $\neq (0)$, p est irréductible, comme on l'a prouvé, mais la réciproque peut être fausse si l'anneau n'est pas factoriel (par exemple, dans $\{a + b\,\mathrm{i}\sqrt{5},\ a,\ b \in \mathbb{Z}\}$, 3 est irréductible mais (3) n'est pas premier (cf. ci-dessous)). On s'interdira donc de parler de nombre premier dans un anneau quelconque à la place d'élément irréductible. On peut dire, en conclusion, que **la notion d'élément irréductible est sans intérêt si l'anneau n'est pas factoriel** ; s'il n'y a pas factorialité, ce sont les idéaux premiers qui jouent un rôle essentiel (ils ne sont donc plus principaux *a priori*, et l'arithmétique dans un tel anneau est extrêmement délicate). Pour mieux faire comprendre ce qui se passe, considérons l'anneau précédent, noté $\mathbb{Z}[\mathrm{i}\sqrt{5}]$, et établissons quelques propriétés :

1. 3 est irréductible (exercice).
2. (3) n'est pas premier. En effet, supposons (3) premier et considérons $x = 1 + \mathrm{i}\sqrt{5}$ et $\overline{x} = 1 - \mathrm{i}\sqrt{5}$; on a $x\overline{x} = 1+5 = 6 \in (3)$; on doit donc avoir pour un signe ε convenable, $1 + \varepsilon\,\mathrm{i}\sqrt{5} \in 3\mathbb{Z}[\mathrm{i}\sqrt{5}]$, ce qui conduit à $1 + \varepsilon\,\mathrm{i}\sqrt{5} = 3(a + bi\sqrt{5})$, a, $b \in \mathbb{Z}$, ce qui est absurde (on obtient $1 = 3a$).
3. les idéaux $\mathfrak{p} = (3, 1 + \mathrm{i}\sqrt{5})$ et $\overline{\mathfrak{p}} = (3, 1 - \mathrm{i}\sqrt{5})$ sont premiers. On considère pour cela l'homomorphisme composé $\mathbb{Z} \to \mathbb{Z}[\mathrm{i}\sqrt{5}] \to \mathbb{Z}[\mathrm{i}\sqrt{5}]/(3, 1 + \mathrm{i}\sqrt{5})$ dont on montre qu'il est surjectif et de noyau $3\mathbb{Z}$ (écrire les détails) ; on a donc $\mathbb{Z}[\mathrm{i}\sqrt{5}]/\mathfrak{p} \simeq \mathbb{F}_3$, ce qui prouve que $\mathfrak{p}$ est même maximal (idem pour $\overline{\mathfrak{p}}$).
4. on considère la notion de produit d'idéaux dans un anneau A : si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de A, on désigne par $\mathfrak{a}\,\mathfrak{b}$ l'idéal engendré par les produits ab, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$; on vérifie facilement que $\mathfrak{a}\,\mathfrak{b}$ est un idéal de A contenu dans $\mathfrak{a} \cap \mathfrak{b}$, et que si $\mathfrak{a} = (a_1, \ldots, a_k)$, $\mathfrak{b} = (b_1, \ldots, b_k)$, alors $\mathfrak{a}\mathfrak{b} = (\ldots, a_i b_j, \ldots)_{1 \leq i,j \leq k}$.

Considérons ici $\mathfrak{p}\overline{\mathfrak{p}} = (3, 1+\mathrm{i}\sqrt{5})(3, 1-\mathrm{i}\sqrt{5}) = (9, 3(1+\mathrm{i}\sqrt{5}), 3(1-\mathrm{i}\sqrt{5}), 6)$; comme $3 \in \mathfrak{p}\overline{\mathfrak{p}}$ ($3 = 9 - 6$ par exemple) et comme 9 et 6 sont multiples de 3, on a : $\mathfrak{p}\overline{\mathfrak{p}} = (3, 3+3\,\mathrm{i}\sqrt{5}, 3-3\,\mathrm{i}\sqrt{5}) = 3(1, 1+\mathrm{i}\sqrt{5}, 1-\mathrm{i}\sqrt{5}) = 3\mathbb{Z}[\mathrm{i}\sqrt{5}]$. On a donc obtenu l'égalité suivante : $\mathfrak{p}\overline{\mathfrak{p}} = (3)$.

5. les idéaux $\mathfrak{p}$ et $\overline{\mathfrak{p}}$ ne sont pas principaux. En effet, si c'était le cas, on aurait $\mathfrak{p} = (\alpha)$, $\overline{\mathfrak{p}} = (\overline{\alpha})$ [5], soit $\mathfrak{p}\overline{\mathfrak{p}} = (\alpha\overline{\alpha}) = (3)$, d'où $3 = \alpha\overline{\alpha}u$, $u \in \mathbb{Z}[\mathrm{i}\sqrt{5}]^\times$, ce qui précisément voudrait dire que 3 est réductible (en effet, ni α ni $\overline{\alpha}$ ne peuvent être dans $A^\times$ par définition d'idéal premier).

En résumé, dans l'anneau $\mathbb{Z}[\mathrm{i}\sqrt{5}]$, le nombre 3 est irréductible **comme nombre** mais non **au sens** (nouveau) **des idéaux**, ce qui relativise la notion d'irréductible dans un anneau non factoriel (c'est Kummer, notamment pour essayer de démontrer le « Théorème de Fermat », qui a « forcé » des éléments irréductibles non « premiers » à s'écrire comme produits « convenables », créant ainsi (de façon incorrecte) de nouveaux « nombres » (qu'il appelait des nombres idéaux, au sens commun du terme), et c'est Dedekind qui a montré que ceci devenait correct à condition de remplacer les nombres par la notion d'idéal (cette fois au sens mathématique). Ceci conduit à définir une catégorie d'anneaux (les anneaux de Dedekind) pour laquelle tout idéal $\neq (0)$ s'écrit de façon unique comme produit d'idéaux premiers. Malheureusement, dans un anneau de Dedekind, les idéaux n'étant pas principaux en général, l'arithmétique dans un tel anneau est particulièrement délicate. C'est la catégorie la plus naturelle après celle d'anneaux principaux (qu'elle contient) pour aborder les problèmes intéressants de théorie des nombres qui sortent du cadre de ce cours.

6.4 Cas des anneaux $A[X]$, avec A factoriel

On suppose que l'on a fixé une fois pour toutes un système d'irréductibles $\mathcal{P}$ de A.

Définition 6.20 (Valuation et contenu d'un polynôme de $K_A[X]$) *Soit K_A le corps des fractions de l'anneau factoriel A. Si $f \in K_A[X]$, on pose, pour $p \in \mathcal{P}$, $v_p(f) = \min_i\{v_p(a_i)\}$, où $f = \sum_{i\geq 0} a_i X^i$, $a_i \in K_A$; on a $v_p(f) \in \mathbb{Z} \cup \{\infty\}$. On appelle alors **contenu** de $f \neq 0$ tout élément de la forme $C(f) = u\prod_{p\in\mathcal{P}} p^{v_p(f)}$, $u \in A^\times$ (c'est un élément de $K_A^\times$) ; on pose $C(0) = 0$. Au lieu d'écrire $C(f) = u\prod_{p\in\mathcal{P}} p^{v_p(f)}$, on écrira en pratique $C(f) \sim \prod_{p\in\mathcal{P}} p^{v_p(f)}$ (relation d'association).*

Remarque Cette fonction v_p sur $K_A[X]$ prolonge la fonction valuation p-adique que l'on a définie sur K_A (cf. définition 6.5 page 69).

5. Car $\overline{\mathfrak{p}}$, d'après sa définition, est bien $\{\overline{x},\ x \in \mathfrak{p}\}$; donc si $\overline{\mathfrak{p}} = (\beta)$, $\mathfrak{p} = (\overline{\beta})$, d'où $\overline{\beta}$ et α associés (on peut donc prendre $\beta = \overline{\alpha}$).

Exemple Dans $\mathbb{Q}[X]$, si $f = 2X^2 - \frac{4}{3}X + 6$, alors on a $C(f) \sim \frac{2}{3}$.

Remarque Vérifier que pour un autre choix de $\mathcal{P}$, les contenus ne sont pas modifiés.

Proposition 6.21 (Propriétés du contenu) *Le contenu a les propriétés élémentaires suivantes, indépendantes du choix de celui-ci :*

1. *si $f \in K_A$, alors $C(f) \sim f$; si $f = u \in A^\times$, alors $C(u) \sim 1$*
2. *si $f \in K_A[X]$, on a $f \in A[X]$ si et seulement si $C(f) \in A$; si $f \neq 0$, et si $c \in K_A^\times$ est tel que $c \sim C(f)$, alors $C\left(\frac{f}{c}\right) \sim 1$*
3. *si $f \in A[X]$, alors $C(f)$ est un pgcd de l'ensemble des coefficients de f [6] (cf. remarque page 70 lorsque $f = 0$).*

Lemme 6.22 (Lemme de Gauss) *La fonction v_p définie sur $K_A[X]$ est telle que pour tout f, g de $K_A[X]$, on a :*
$v_p(fg) = v_p(f) + v_p(g)$ *(donc de façon équivalente $C(fg) \sim C(f)C(g)$).*

Démonstration Le cas $f = 0$ **ou** $g = 0$ étant immédiat, supposons $fg \neq 0$.

Posons $f' = \left(\prod_{p\in\mathcal{P}} p^{-v_p(f)}\right) f$ et $g' = \left(\prod_{p\in\mathcal{P}} p^{-v_p(g)}\right) g$; il est clair que $v_p(f') = v_p(g') = 0$ pour tout $p \in \mathcal{P}$ (ceci entraîne f', $g' \in A[X]$).

Comme $fg = f'g' \prod_{p\in\mathcal{P}} p^{v_p(f)+v_p(g)}$, le lemme sera prouvé si l'on montre $v_p(f'g') = 0$, pour tout $p \in \mathcal{P}$.

Utilisons l'homomorphisme de réduction modulo p :

$$\begin{array}{ccc} A[X] & \longrightarrow & A/pA[X] \\ f & \longmapsto & \overline{f} \end{array}$$

Si $v_p(f'g') > 0$, c'est que $\overline{f'g'} = \overline{0}$ dans $A/pA[X]$, donc que $\overline{f'}\,\overline{g'} = \overline{0}$; or comme A/pA est intègre (pA étant premier d'après le corollaire 6.15 page 72), $A/pA[X]$ est intègre et on a $\overline{f'} = \overline{0}$ **ou** $\overline{g'} = \overline{0}$, ce qui signifie $v_p(f') \geq 1$ **ou** $v_p(g') \geq 1$, ce qui est absurde.

Corollaire 6.23 (Une propriété du contenu) *Soit $h \in A[X]$, de contenu inversible ; si $h = fg$, avec f, $g \in A[X]$, alors $C(f) \sim C(g) \sim 1$.*

---

6. On remarquera que $C(f) = u \prod_{p\in\mathcal{P}} p^{\min_i\{v_p(a_i)\}}$, $u \in A^\times$, est exactement la définition des $\operatorname{pgcd}_i\{a_i\}$, **étendue** à K_A de façon naturelle, mais avec le phénomène (que l'on analysera) que, par exemple, $\operatorname{pgcd}\left(\frac{1}{2}, \frac{1}{3}\right) = \pm\frac{1}{6}$ dans $\mathbb{Q}$.

En effet, on a par hypothèse $v_p(h) = 0$ pour tout $p \in \mathcal{P}$, et donc on a :

$$v_p(h) = 0 = v_p(f) + v_p(g)$$

d'autre part, dès que f et g sont dans $A[X]$, on a $v_p(f) \geq 0$, $v_p(g) \geq 0$, auquel cas on a nécessairement $v_p(f) = v_p(g) = 0$; d'où le résultat.

On a le résultat essentiel suivant :

Théorème 6.24 (Factorialité de $A[X]$) *Soit A un anneau factoriel, de corps des fractions K_A. Alors l'anneau $A[X]$ est factoriel, et ses éléments irréductibles sont les irréductibles de A et les polynômes de $A[X]$ qui sont de contenu inversible et qui sont irréductibles dans l'anneau (factoriel) $K_A[X]$.*

Démonstration Caractérisons d'abord les irréductibles de $A[X]$. On utilisera constamment le fait que $A[X]^\times = A^\times$ et que $K_A[X]^\times = K_A^\times$ (le revérifier). Pour les propriétés des contenus, se reporter à la proposition 6.21 page 78.

Lemme 6.25

1. *Les éléments p, irréductibles dans A, sont irréductibles dans $A[X]$*
2. *les polynômes Q de $A[X]$, de contenu inversible, irréductibles dans $K_A[X]$, sont irréductibles dans $A[X]$*

1. Dans ce cas p reste non inversible dans $A[X]$, et si $p = fg$, f, $g \in A[X]$, on a évidemment f, $g \in A$, d'où $f \in A^\times$ ou $g \in A^\times$, donc $f \in A[X]^\times$ ou $g \in A[X]^\times$.
2. Un tel Q est non constant (car irréductible dans $K_A[X]$) ; si $Q = fg$, f, $g \in A[X]$, l'irréductibilité dans $K_A[X]$ implique que f ou g est dans $K_A[X]^\times = K_A^\times$; mais on a $1 \sim C(Q) \sim C(f)C(g)$ et, par hypothèse, $C(f)$, $C(g) \in A$, donc $C(f)$, $C(g) \in A^\times$, et $C(f) \sim C(g) \sim 1$, d'où $f \in A^\times$ ou $g \in A^\times$.

Lemme 6.26 *Un élément h irréductible dans $A[X]$ est, soit un irréductible de A, soit un polynôme de contenu inversible, irréductible dans $K_A[X]$.*

Soit h un élément irréductible de $A[X]$.

1. Si $h \in A$, on a $h \notin A[X]^\times = A^\times$ (irréductibilité dans $A[X]$). Écrivons $h = fg$, f, $g \in A$; par hypothèse f ou g est dans $A[X]^\times = A^\times$.
2. Si $h \notin A$, on écrit $h = C(h)h'$, ce qui implique $C(h') \sim 1$; comme $h \in A[X]$, $C(h) \in A$ et $h' \in A[X]$ est non constant. Par irréductibilité dans $A[X]$, $C(h) \in A[X]^\times = A^\times$ (h' ne pouvant être dans $A^\times$) ; donc $C(h) \sim 1$. Écrivons $h = fg$, f, $g \in K_A[X]$; on a $h \sim f'g'$, où $f' = f/C(f)$, $g' = g/C(g)$ (car $C(f)C(g) \sim C(h) \sim 1$), et f', $g' \in A[X]$; par irréductibilité dans $A[X]$, f' ou g' est dans $A^\times$, donc f ou g est dans $K_A^\times = K_A[X]^\times$.

Remarque Ces deux lemmes conduisent à la propriété suivante : si Q est un polynôme non constant de contenu inversible dans $A[X]$, alors Q est irréductible dans $K_A[X]$ si et seulement s'il est irréductible dans $A[X]$. Démontrons maintenant la factorialité proprement dite de $A[X]$.

Soit $f \in A[X]$ $f \neq 0$; considéré dans $K_A[X]$ qui est factoriel, on a $f = aQ_1 \dots Q_r$, $a \in K_A^\times$, Q_j irréductibles de $K_A[X]$; on peut écrire

$$f = ac_1 \dots c_r Q'_1 \dots Q'_r, \quad Q'_j = Q_j/c_j \in A[X], \quad \text{avec } c_j = C(Q_j)$$

les Q'_j étant de contenus inversibles, et $f = a'Q'_1 \dots Q'_r$, $a' \in K_A^\times$; comme $f \in A[X]$, $C(f) \sim C(a') \sim a'$, donc $a' \in A$. On décompose a' dans A (factoriel) sous la forme $a' = up_1 \dots p_n$, $u \in A^\times$, p_i irréductibles de A. D'après le lemme 6.25 page 79, les p_i et les Q'_j sont des irréductibles de $A[X]$, et f est bien le produit d'un inversible et d'irréductibles de $A[X]$.

Supposons avoir $up_1 \dots p_n Q_1 \dots Q_r = vq_1 \dots q_m R_1 \dots R_s$, u, $v \in A^\times$, p_i, q_k irréductibles dans A, Q_j, R_ℓ polynômes non constants irréductibles dans $A[X]$. D'après le lemme 6.26 page 79, les Q_j et R_ℓ sont de contenu inversible et irréductibles dans $K_A[X]$; donc en utilisant la factorialité dans $K_A[X]$, on obtient (puisque $up_1 \dots p_n$, $vq_1 \dots q_m \in K_A^\times$) : $r = s$ et $R_{\sigma(k)} = u_k Q_k$ (ou σ est une permutation de $\{1, \dots, r\}$) ; mais :

$$\Big(C(R_{\sigma(k)}) \sim C(u_k)C(Q_k)\Big) \quad \text{implique} \quad \Big(C(u_k) \sim 1\Big)$$

soit $u_k \in A^\times$, et $R_{\sigma(k)}$ et Q_k sont associés dans $A[X]$. Donc il vient :

$$up_1 \dots p_n Q_1 \dots Q_r = vq_1 \dots q_m u_1 \dots u_r Q_1 \dots Q_r$$

soit $up_1 \dots p_n = (vu_1 \dots u_r)q_1 \dots q_m$ dans A, avec $vu_1 \dots u_r \in A^\times$, et on conclut avec la factorialité de A.

Corollaire 6.27 *Si A est factoriel, alors $A[X_1, \dots, X_n]$ est factoriel.*

Application pratique[7] Soit $Q \in K_A[X]$ non constant. Supposons que l'on veuille démontrer que Q est irréductible dans $K_A[X]$. Quitte à diviser Q par $C(Q) \in K_A^\times$, on peut supposer Q de contenu inversible (donc $Q \in A[X]$) (on remplace donc Q par un associé dans $K_A[X]$, **ce qui ne change pas le problème posé**). D'après la remarque précédente de la page 80, l'irréductibilité de Q dans $K_A[X]$ est équivalente à celle (plus facile) de Q dans $A[X]$ (uniquement si $Q \in A[X]$ et est de contenu inversible, ce qu'on a supposé). On essaye alors d'écrire $Q = fg$, $f, g \in A[X]$, f, g non constants (de contenus inversibles nécessairement) et de trouver une contradiction. On a bien simplifié le problème (grâce au lemme de Gauss) car on a pu remplacer l'ensemble des coefficients pour f et g (le corps K_A) par un ensemble plus petit (l'anneau A) dans lequel on dispose de méthodes efficaces qui n'existent pas dans le corps K_A ; donnons les plus classiques (on suppose donc $Q \in A[X]$ non constant, de contenu inversible) :

7. À étudier avec un soin tout particulier.

(1) Par identification : On écrit $Q = fg$, f, $g \in A[X]$, non constants,

$$f = \sum_{i=0}^{m} a_i X^i, g = \sum_{j=0}^{n} b_j X^j,\ a_i,\ b_j \in A,\ m,\ n \geq 1,$$

$$m = \mathrm{d}(f), \quad n = \mathrm{d}(g)$$

puis on écrit les relations entre les coefficients a_i et b_j qui résultent de l'égalité $Q = fg$, et on essaye de trouver une contradiction. On doit faire ceci autant de fois qu'il y a de couples (m, n), $m \geq 1$, $n \geq 1$, $m \geq n$ (par raison de symétrie), tels que $m + n = \mathrm{d}(Q)$. La méthode peut donc devenir très lourde si $\mathrm{d}(Q)$ est « trop grand » ; en outre la contradiction peut être très difficile à obtenir car les systèmes obtenus ne sont pas linéaires mais diophantiens. En revanche, si l'on ne sait rien *a priori* sur Q, la méthode peut permettre de trouver une factorisation de Q en polynômes irréductibles de $A[X]$. À ce sujet, le cas $m = 1$ est particulier, car on a alors $f = uX - v$, u, $v \in A$, $u \neq 0$, et un tel cas se produit si et seulement si $\dfrac{v}{u}$ est racine de Q dans K_A ; on recherche donc d'abord si Q a des racines dans K_A, en notant la propriété suivante :

Proposition 6.28 (Racine dans K_A) *Si* $\dfrac{v}{u}$, u, v *étrangers dans* A, $u \neq 0$, *est racine, dans* K_A, *de :*

$$Q = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$$

$$\boldsymbol{\text{alors } u \mid a_n \text{ et } v \mid a_0}$$

En effet, si $Q\left(\dfrac{v}{u}\right) = 0$, il vient immédiatement :

$$a_n v^n + a_{n-1} v^{n-1} u + \cdots + a_1 v u^{n-1} + a_0 u^n = 0$$

soit $a_n v^n = -u(a_{n-1} v^{n-1} + \cdots + a_1 v u^{n-2} + a_0 u^{n-1})$ et, comme u est étranger à v (donc à v^n), $u \mid a_n$; de même, on a $a_0 u^n = -v(a_n v^{n-1} + a_{n-1} v^{n-2} u + \cdots + a_1 u^{n-1})$ qui conduit à $v \mid a_0$.

(2) Par réduction modulo $\mathfrak{a}$: On utilise un homomorphisme de la forme :

$$A[X] \longrightarrow A/\mathfrak{a}[X]$$

où, par définition, l'image de tout $a \in A$ est la classe de a modulo l'idéal $\mathfrak{a}$; on note $\overline{h}$ l'image d'un polynôme $h \in A[X]$ dans $A[X] \to A/\mathfrak{a}[X]$.

On fait les hypothèses suivantes sur Q (de contenu inversible) :

1. l'image du coefficient dominant de Q est non nulle et non diviseur de zéro dans $A/\mathfrak{a}$;
2. le polynôme $\overline{Q}$ est irréductible dans $A/\mathfrak{a}[X]$ (cf. 3 page 68 [8]).

8. Dans cette situation très générale, $A/\mathfrak{a}$ n'est pas nécessairement intègre, et s'il l'est, il n'est pas nécessairement factoriel.

Alors le polynôme Q est irréductible dans $A[X]$.

Supposons en effet que $Q = fg$, f, $g \in A[X]$, f, $g \notin A[X]^\times = A^\times$; comme Q est de contenu inversible, f et g sont nécessairement de degré ≥ 1 (sinon $Q = ag$, $a \in A$, implique $a \in A^\times$ d'après le corollaire 6.23 page 78). Écrivons :

$$Q = a_Q X^{\mathrm{d}(Q)} + \cdots \; ; \quad f = a_f X^{\mathrm{d}(f)} + \cdots \; ; \quad g = a_g X^{\mathrm{d}(g)} + \cdots \tag{6.1}$$

en termes de coefficients dominants et de degrés de polynômes (par définition, a_Q, a_f, a_g sont dans $A - \{0\}$) ; on aura alors :

$$\overline{Q} = \overline{a_Q} X^{\mathrm{d}(Q)} + \cdots \; ; \quad \overline{f} = \overline{a_f} X^{\mathrm{d}(f)} + \cdots \; ; \quad \overline{g} = \overline{a_g} X^{\mathrm{d}(g)} + \cdots \tag{6.2}$$

D'après (6.1) et le fait que $Q = fg$, on a $a_Q = a_f a_g$, ce qui donne $\overline{a_Q} = \overline{a_f}\,\overline{a_g}$; mais, par hypothèse, $\overline{a_Q}$ est $\neq \overline{0}$ et non diviseur de zéro dans $A/\mathfrak{a}$, ce qui implique que $\overline{a_f}$ et $\overline{a_g}$ sont $\neq \overline{0}$ et non diviseurs de zéro ; on a en particulier $\overline{a_Q}$, $\overline{a_f}$, $\overline{a_g} \in A/\mathfrak{a} - \{\overline{0}\}$, ce qui prouve que l'écriture (6.2) est bien en termes de coefficients dominants, et donc que $\mathrm{d}(\overline{Q}) = \mathrm{d}(Q)$, $\mathrm{d}(\overline{f}) = \mathrm{d}(f)$, $\mathrm{d}(\overline{g}) = \mathrm{d}(g)$ dans $A/\mathfrak{a}[X]$.

Il faut maintenant démontrer que $\overline{Q} = \overline{f}\,\overline{g}$ est bien une vraie décomposition de $\overline{Q}$, autrement dit que ni $\overline{f}$ ni $\overline{g}$ ne sont inversibles (le gros piège étant que si $A/\mathfrak{a}$ n'est pas intègre, certains polynômes de $A/\mathfrak{a}[X]$ de degré ≥ 1 sont inversibles : par exemple $\overline{2}X + \overline{1}$ dans $\mathbb{Z}/4\mathbb{Z}[X]$, puisque $(\overline{2}X + \overline{1})^2 = \overline{4}X^2 + \overline{4}X + \overline{1} = \overline{1}$). Supposons par exemple qu'il existe $\overline{h} \in A/\mathfrak{a}[X]$ tel que $\overline{f}\,\overline{h} = \overline{1}$; comme $\mathrm{d}(\overline{f}) = \mathrm{d}(f) \geq 1$, c'est que, nécessairement, le produit des coefficients dominants de $\overline{f}$ et $\overline{h}$ donne $\overline{0}$, et $\overline{a_f}$ (celui de $\overline{f}$) serait diviseur de zéro, ce qui est absurde d'après ce qu'on a montré.

Remarque Dans le cas (fréquent) où $\mathfrak{a}$ est un idéal premier $\mathfrak{p}$ de A, $\overline{a_Q}$ est non diviseur de zéro si et seulement si $\overline{a_Q} \neq \overline{0}$ (i.e. $a_Q \notin \mathfrak{p}$), donc :

$$1 \iff 1' \quad : \quad \mathrm{d}(\overline{Q}) = \mathrm{d}(Q)$$

(3) Critère d'Eisenstein : On a le résultat suivant très utile en pratique :

Théorème 6.29 (Critère d'Eisenstein) *Soit A un anneau factoriel, soit p un élément irréductible de A et soit $Q = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ un polynôme de $A[X]$ de degré $n \geq 1$; on suppose que Q vérifie les hypothèses suivantes (Q étant toujours de contenu inversible) :*

1. *le coefficient dominant a_n est étranger à p (i.e. $v_p(a_n) = 0$)*
2. *pour tout i, $0 \leq i \leq n-1$, a_i est divisible par p (i.e. $v_p(a_i) \geq 1$)*
3. *le coefficient a_0 n'est pas divisible par p^2 (i.e. $v_p(a_0) = 1$)*

alors Q est irréductible dans $A[X]$.

Démonstration Supposons qu'il existe f, $g \in A[X]$ (non constants, nécessairement) tels que $Q = fg$. On considère la réduction modulo $\mathfrak{p} = pA$: $A[X] \longrightarrow A/\mathfrak{p}[X]$ (ici $\mathfrak{p}$ est un idéal premier d'après le corollaire 6.15 page 72) ; on a donc $\overline{Q} = \overline{f}\,\overline{g} = \overline{a_n}X^n$ (on a $\overline{a_n} \neq \overline{0}$ par hypothèse), et on vérifie facilement que $\overline{f}$ et $\overline{g}$ ne sont pas constants car $\mathrm{d}(\overline{f}) + \mathrm{d}(\overline{g}) = n$ ($A/\mathfrak{p}$ est intègre) d'où $\mathrm{d}(\overline{f}) = \mathrm{d}(f)$, $\mathrm{d}(\overline{g}) = \mathrm{d}(g)$. Comme $\mathfrak{p}$ est premier, on peut utiliser le corps des fractions $\mathbb{K}$ de $A/\mathfrak{p}$, et la relation $\overline{f}\,\overline{g} = \overline{a_n}X^n$ est alors une égalité dans $\mathbb{K}[X]$ qui est factoriel ; $\overline{a_n}$ étant dans $\mathbb{K}^\times$, on en déduit $\overline{f} = \lambda X^\alpha$, $\overline{g} = \mu X^\beta$, λ, $\mu \in \mathbb{K}^\times$, $\alpha \geq 1$, $\beta \geq 1$, $\alpha + \beta = n$.

On a $\lambda = \dfrac{\overline{a}}{\overline{s}}$, a, $s \in A$, a, $s \notin pA$, et de même, $\mu = \dfrac{\overline{b}}{\overline{t}}$, b, $t \in A$, b, $t \notin pA$; il vient alors $\overline{s}\,\overline{f} = \overline{a}X^\alpha$ et $\overline{t}\,\overline{g} = \overline{b}X^\beta$. Notons u_0, $v_0 \in A$ les termes constants de f et g ; ceux de $\overline{f}$ et $\overline{g}$ sont donc $\overline{u_0}$ et $\overline{v_0}$, et les relations précédentes donnent $\overline{s}\,\overline{u_0} = \overline{0}$ et $\overline{t}\,\overline{v_0} = \overline{0}$ (car on a $\alpha \geq 1$, $\beta \geq 1$). Comme $A/\mathfrak{p}$ est intègre, et comme on a $\overline{s} \neq \overline{0}$, $\overline{t} \neq \overline{0}$, il vient u_0, $v_0 \in pA$; le terme constant de Q est $a_0 = u_0 v_0$ qui serait divisible par p^2, ce qui est contraire à l'hypothèse. D'où l'irréductibilité de Q.

(4) Méthode numérique dans certains anneaux : La méthode que nous allons décrire ne peut s'utiliser que si $A^\times$ est fini. Donc en pratique ce sera $\mathbb{Z}$, ce que nous supposons pour simplifier.

Soit $Q \in \mathbb{Z}[X]$ de contenu inversible et de degré $n > 1$; supposons qu'il existe un diviseur f de Q dans $\mathbb{Z}[X]$ de degré $\mathrm{d}(f) = d$, $d \leq \dfrac{n}{2}$ (ceci n'est pas une restriction car si $Q = fg$, f ou g a cette propriété).

Soient n_0, n_1, …, n_d, $d+1$ entiers arbitraires distincts ; posons

$$Q(n_i) = r_i \in \mathbb{Z}, \quad \text{et} \quad r = (r_0, \ldots, r_d) \in \mathbb{Z}^{d+1}$$

On dira que $s = (s_0, \ldots, s_d) \in \mathbb{Z}^{d+1}$ divise r si $s_i \mid r_i$ pour chaque $i = 0, \ldots, d$. On forme tous les vecteurs s divisant r (comme $\mathbb{Z}^\times = \{\pm 1\}$, ce nombre de diviseurs est fini). On a alors la possibilité de former les polynômes f_s, polynômes d'interpolation des $\boldsymbol{d+1}$ **points :** $\boldsymbol{(n_i, s_i)}$, $\boldsymbol{i = 0, \ldots, d}$. On a $\mathrm{d}(f_s) \leq d$, pour tout s ; on a alors le résultat suivant :

Proposition 6.30 (Polynôme divisant Q) *Le polynôme f divisant Q et de degré $d \leq \dfrac{n}{2}$ est nécessairement l'un des f_s.*

En effet, on a $f(n_i) = t_i \in \mathbb{Z}$, $i = 0, \ldots, d$, et la décomposition $Q = fg$ conduit à $Q(n_i) = f(n_i)g(n_i)$, d'où $t_i \mid r_i$ pour $i = 0, \ldots, d$; autrement dit :

$$t = (t_0, \ldots, t_d) \text{ divise } r = (r_0, \ldots, r_d)$$

donc f_t a été construit tel que $f_t(n_i) = t_i$, pour tout $i = 0, \ldots, d$; on a donc : $f(n_i) = f_t(n_i)$ pour $d+1$ valeurs distinctes n_i ; on a nécessairement $f = f_t$ (unicité du polynôme d'interpolation de degré $\leq d$ pour $d+1$ points (cf. chapitre 4, théorème 4.8 page 46).

Par exemple, si $Q = X^4 + X + 1$ dans $\mathbb{Z}[X]$, on peut prendre $n_0 = -1$, $n_1 = 0$, $n_2 = 1$, auquel cas $r = \Big(Q(-1), Q(0), Q(1)\Big) = (1, 1, 3)$, ce qui donne 16

diviseurs s de r ; cependant s et $-s$ conduisent à f_s et $f_{-s} = -f_s$, et on peut se limiter aux s suivants :

$$\begin{array}{cccc} (1,1,3) & (1,1,1) & (-1,1,3) & (-1,1,1) \\ (1,1,-3) & (1,1,-1) & (-1,1,-3) & (-1,1,-1) \end{array}$$

Ayant vérifié que Q n'a pas de racine rationnelle (i.e. ± 1), on peut ne retenir que les polynômes f_s de degré 2 exactement :
$X^2 + X + 1$, $-2X^2 - 2X + 1$, $-X^2 - X + 1$, ...
On vérifie alors que Q est irréductible.

Cette méthode, qui exige un très grand nombre de calculs élémentaires, prend toute sa valeur si on la programme (auquel cas on factorise facilement les polynômes de degré ≤ 5).

.

6.5 Anneaux euclidiens

On a vu dans le chapitre 1 que les propriétés arithmétiques de $\mathbb{Z}$ provenaient directement de l'existence de l'algorithme d'Euclide reposant sur une division euclidienne. Dans cette section on va étudier les anneaux sur lesquels on peut définir une division analogue et qui vont être susceptibles de la même démarche ; cependant ils ne représentent pas une nouvelle catégorie d'anneaux (ils seront forcément principaux), le seul intérêt est que les différents attributs arithmétiques les concernant (pgcd, relations de Bézout, ...) s'obtiennent **algorithmiquement** de façon effective, donc précieuse en pratique.

Définition 6.31 (Anneau euclidien) *Soit A un anneau commutatif intègre ; on dit que A est **euclidien** s'il existe une fonction $\varphi : A - \{0\} \to \mathbb{N}$ vérifiant les conditions suivantes :*

1. *si $b \mid a$, $a \neq 0$, alors $\varphi(b) \leq \varphi(a)$*
2. *si $b \in A - \{0\}$, alors pour tout $a \in A$, il existe $q \in A$, $r \in A$, tels que*

$$a = bq + r \quad \textit{avec} \quad r = 0 \quad \textbf{\textit{ou}} \quad \varphi(r) < \varphi(b).$$

Exemples Pour $A = \mathbb{Z}$, on a $\varphi(a) = |a|$ (cf. remarque 3 page 87) ; pour $A = \mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), on a $\varphi(Q) = \mathrm{d}(Q)$ (cf. remarque 2 page 87) ; si $A = \mathbb{Z}[\mathrm{i}]$, alors $\varphi(u + iv) = u^2 + v^2$.

Lemme 6.32 ($\varphi(a)$ pour $a \in A^\times$) *On a $a \in A^\times$ si et seulement si $\varphi(a) = \varphi(1)$.*

$\Rightarrow$: Si $a \in A^\times$, on a $a \mid 1$, et d'après 1, $\varphi(a) \leq \varphi(1)$; comme $1 \mid a$, on a aussi $\varphi(1) \leq \varphi(a)$.

$\Leftarrow$: Si $\varphi(a) = \varphi(1)$, en utilisant 2, on a $1 = aq + r$, avec $r = 0$ **ou** ($r \neq 0$ **et** $\varphi(r) < \varphi(a) = \varphi(1)$) ; mais si $r \neq 0$, la relation $r = 1 - aq = 1(1 - aq)$ conduit à $\varphi(1) \leq \varphi(r)$, ce qui est absurde. On a donc $r = 0$, soit $aq = 1$, et $a \in A^\times$.

Théorème 6.33 *Tout anneau euclidien est principal.*

Démonstration Logiquement, elle est identique à celle utilisée pour $\mathbb{Z}$ ou $\mathbb{K}[X]$ (cf. chapitre 2, définition 2.12 exemple 1 page 20 de ce cours) :

Soit $\mathfrak{a}$ un idéal non nul de A ; alors $\varphi(\mathfrak{a}-\{0\})$ est une partie non vide de $\mathbb{N}$ dont le minimum est atteint pour au moins un $a \in \mathfrak{a}-\{0\}$. Soit alors $x \in \mathfrak{a}$; on a $x = aq+r$, q, $r \in A$, avec $r = 0$ **ou** ($r \neq 0$ **et** $\varphi(r) < \varphi(a)$) ; si $r \neq 0$, $r = x - aq \in \mathfrak{a} - \{0\}$ de façon évidente, et on a donc $\varphi(r) \geq \varphi(a)$ par définition de a, ce qui est absurde. Donc nécessairement $r = 0$ et $x \in (a)$, ce qui prouve l'inclusion $\mathfrak{a} \subseteq (a)$, d'où l'égalité puisque $a \in \mathfrak{a}$.

La division euclidienne conduit à l'**algorithme d'Euclide** que nous rappelons brièvement (mais avec un degré de généralité optimal) :

Théorème 6.34 (Algorithme d'Euclide dans un anneau euclidien) *Si A est un anneau euclidien, il existe un algorithme d'Euclide pour tout couple (a,b), a, $b \in A$, conduisant (via le dernier reste r_n) à un pgcd de a et b, et à une relation de Bézout.*

Démonstration Posons, pour $a \in A$, $b \in A$ donnés :

$$\begin{aligned} r_{-1} &= a \\ r_0 &= b \end{aligned}$$

et considérons les divisions euclidiennes successives (par décalage vers la gauche des couples de « restes » (r_{i-1}, r_i)) tant que c'est possible :

$$\left\{\begin{array}{rcccll} r_{-1} & = & q_0 r_0 & + & r_1, & q_0 \in A, \quad \varphi(r_1) < \varphi(r_0) \\ r_0 & = & q_1 r_1 & + & r_2, & q_1 \in A, \quad \varphi(r_2) < \varphi(r_1) \\ & \vdots & & & & \\ r_{i-1} & = & q_i r_i & + & r_{i+1}, & q_i \in A, \quad \varphi(r_{i+1}) < \varphi(r_i) \\ & \vdots & & & & \\ r_{n-2} & = & q_{n-1} r_{n-1} & + & r_n, & q_{n-1} \in A, \quad \varphi(r_n) < \varphi(r_{n-1}) \\ r_{n-1} & = & q_n r_n & + & 0, & q_n \in A \end{array}\right. \tag{6.3}$$

Si $r_0 = 0$, le tableau ci-dessus est donc vide [9] ; sinon, vu la stricte décroissance des $\varphi(r_i)$, à partir de $\varphi(r_0) > 0$, il existe un reste (non nul) r_n, d'indice maximum $n \geq 0$ (i.e. $r_{n+1} = 0$). Appelons d cet entier r_n

Si le tableau (6.3) est vide, c'est que $n+1 = 0$ (nombre de lignes) et $d = r_{-1} = a$.

On a le résultat suivant :

Lemme 6.35 (Lien entre a, b et r_i) *Pour tout i, $-1 \leq i \leq n+1$, on a : il existe u_i, $v_i \in A$ tels que $r_i = u_i a + v_i b$.*

Pour $i = -1$, $r_{-1} = u_{-1}a + v_{-1}b$, avec $u_{-1} = 1$, $v_{-1} = 0$.

Pour $i = 0$, $r_0 = u_0 a + v_0 b$, avec $u_0 = 0$, $v_0 = 1$.

9. Et le « dernier » couple de restes (r_n, r_{n+1}) obtenu est donc (pour $n = -1$) (r_{-1}, r_0) (i.e. les « initialisations »).

À partir des relations ($i \geq 0$) :

$$\begin{aligned} r_{i-1} &= u_{i-1}a + v_{i-1}b \\ r_i &= u_i a + v_i b \end{aligned}$$

supposées comme hypothèse de récurrence, prouvons le stade suivant (i.e. pour r_i et r_{i+1}, donc pour r_{i+1}) ; on a (milieu du tableau (6.3)) :

$$r_{i-1} = q_i r_i + r_{i+1}$$

d'où, pour trouver u_{i+1}, $v_{i+1} \in A$ tels que :

$$u_{i-1}a + v_{i-1}b = q_i(u_i a + v_i b) + u_{i+1}a + v_{i+1}b$$

il **suffit** de prendre les valeurs suivantes :

$$\begin{aligned} u_{i+1} &= -q_i u_i + u_{i-1} \\ v_{i+1} &= -q_i v_i + v_{i-1} \end{aligned}$$

D'où, pour $i = n$, l'existence[10] de $u = u_n$, $v = v_n$ tels que

$$r_n = d = ua + vb$$

Pour ceux qui font des programmes, ceci conduit à l'algorithme suivant, valable **quels que soient** a, $b \in A$ (résultats dans D, U, V) :

$D := a$; $DD := b$;
$U := 1$; $UU := 0$;
$V := 0$; $VV := 1$;
tant que $DD \neq 0$ **faire**
début
  $Q := D \div DD$;
  $X := U - Q * UU$; $U := UU$; $UU := X$;
  $Y := V - Q * VV$; $V := VV$; $VV := Y$;
  $Z := D - Q * DD$; $D := DD$; $DD := Z$;
fin

Lemme 6.36 (Lien entre a, b et d) *Le nombre d divise a et b.*

On montre, par récurrence descendante sur i, $n+1 \geq i \geq 0$, que $d = r_n$ divise r_i et r_{i-1} :

- Pour $i = n+1$, comme $r_{n+1} = 0$, $d = r_n$ divise trivialement r_{n+1} et r_n ($= d$).
- Si l'on suppose que d divise r_i et r_{i+1}, $n \geq i \geq 0$, la relation $r_{i-1} = q_i r_i + r_{i+1}$ montre que d divise r_{i-1} et r_i.

10. Noter que pour $i = n+1$, on obtient $r_{n+1} = 0 = u_{n+1}a + v_{n+1}b$ (voir sur des exemples numériques, ce que sont u_{n+1} et v_{n+1}).

D'où le résultat pour $i = 0$.

On a donc obtenu le résultat très fort suivant, avec en plus un algorithme de calcul pour tout objet mathématique dont l'existence est affirmée :

Théorème 6.37 (Résultat-clef) *Soit A un anneau euclidien, pour tout a, $b \in A$, il existe d, u, $v \in \mathbb{Z}$ vérifiant les propriétés suivantes (y compris si $a = 0$ **ou** $b = 0$) :*

1. $d \mid a$ ***et*** $d \mid b$
2. $d = ua + vb$.

Remarques

1. Prouver qu'un anneau principal donné A n'est pas euclidien est en général extrêmement difficile : en effet, ceci n'est plus à proprement parler un problème algébrique, mais un problème d'arithmétique non trivial (la non existence de φ supposant un degré de complexité de A difficile à maîtriser).
2. Pour les anneaux $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$, la fonction φ est définie sur A par $\varphi(0_A) = 0$ et est multiplicative ($\varphi(ab) = \varphi(a)\varphi(b)$ pour tout a, $b \in A$) et $\varphi(1) = 1$ (autrement dit, c'est un homomorphisme de monoïdes multiplicatifs, de $(A, \times)$ dans $(\mathbb{N}, \times)$) ; le cas de $\mathbb{K}[X]$ rentre dans le cas précédent si l'on pose $\varphi(Q) = 2^{\mathrm{d}(Q)}$ (par exemple), auquel cas « $\varphi(0) = 2^{-\infty} = 0$ », $\varphi(1) = 2^0 = 1$.
   Lorsque φ est multiplicative et lorsque $\varphi(a) = 0 \iff a = 0$, le point 1 de la définition 6.31 page 84 est automatiquement vérifié, et le point 2 s'énonce ainsi : si $b \in A - \{0\}$, pour tout $a \in A$, il existe q, $r \in A$ tels que $a = bq + r$, avec $\varphi(r) < \varphi(b)$.
3. Dans la définition 6.31 page 84, point 2, les éléments q et r de A ne sont pas nécessairement uniques ; par exemple, on pourra écrire, dans $\mathbb{Z}$, pour $a = 8$, $b = 3$: $8 = 3 \times 2 + 2$ ($r = 2$) ou $8 = 3 \times 3 - 1$ ($r = -1$), et dans tous les cas on a $\varphi(r) < \varphi(b)$. Donc la définition générale ne donne pas directement la division euclidienne telle que nous l'avons définie dans $\mathbb{Z}$, cette dernière résultant d'un choix plus précis de r assurant notamment son unicité.
   On peut utiliser cette division euclidienne plus générale pour atteindre plus vite (peut-être) un pgcd dans $\mathbb{Z}$:
   Par exemple, pour $a = 21$, $b = 13$, on a :

$$\begin{array}{rcrcrl} 21 & = & 13 \times 2 & - & 5 & \\ 13 & = & -5 \times (-3) & - & 2 & \\ -5 & = & -2 \times 2 & - & 1 & \quad (\text{ou } -2 \times 3 + 1) \end{array}$$

   au lieu de :

$$\begin{array}{rcrcr} 21 & = & 13 \times 1 & + & 8 \\ 13 & = & 8 \times 1 & + & 5 \\ 8 & = & 5 \times 1 & + & 3 \\ 5 & = & 3 \times 1 & + & 2 \\ 3 & = & 2 \times 1 & + & 1 \end{array}$$

   d'où un calcul plus rapide des « coefficients de Bézout » dans le premier algorithme.

FIN DU SIXIÈME CHAPITRE