MAT2611 : algèbre 2
Introduction aux anneaux et aux modules

Dimitris Koukoulopoulos

Université de Montréal

Dernière mise-à-jour : 28 mars 2020

Table des matières

Notes

Les symboles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ dénotent les ensembles des nombres naturels, entiers, rationnels, réels et complexes, respectivement. De plus, on écrit $\mathbb{Z}_{\geq a}$ pour dénoter l'ensemble des entiers $\geq a$, $\mathbb{Q}_{<a}$ pour dénoter l'ensemble des rationnels $< a$, etc. On n'inclut pas le nombre 0 à l'ensemble de nombres naturels, c'est-à-dire $\mathbb{N} = \mathbb{Z}_{\geq 1}$.

La plupart d'exercices de ces notes sont pris par le livre de D. S. Dummit et R. M. Foote "Abstract Algebra", 3ème édition, John Willey and Sons, Inc., Hoboken, NJ, 2004. Quand c'est le cas, le numéro de l'exercice et la page où elle se trouve au livre de Dummit et Foote sont indiqués.

Première partie

Anneaux

Chapitre 1

Sommes de deux carrés

On commence en étudiant une question trompeusement simple : quels entiers peuvent s'écrire comme la somme de deux carrés. La réponse à cette question nous amènera de façon naturelle à plusieurs notions importantes de la théorie d'anneaux qu'on développera de façon systématique aux prochains chapitres.

En langage mathématique, on veut classifier les entiers n qui peuvent être exprimés comme $n = x^2 + y^2$ pour quelques $x, y \in \mathbb{Z}$. Si une telle representation existe, on écrira $n = \square + \square$. Evidemment, il faut que $n \geq 0$. Cependant, il existe d'entiers positifs qui ne sont pas de la forme $\square + \square$. Par exemple, $3 \neq \square + \square$. Voici les premiers membres de la suite de nombres représentables comme la somme de deux carrés :

$$\begin{aligned} &0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, \\ &53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106, 109, \\ &113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153, 157, 160, \ldots \end{aligned} \tag{1.1}$$

La suite ne semble pas d'avoir de régularité.

Par contre, si on forme la suite des entiers non-negatifs qui sont la *différence* de deux carrés, on voit tout de suite une structure rigide :

$$0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, \ldots$$

Il semble que $n = \square - \square$ s-si $n \not\equiv 2 \pmod 4$. En effet, si $n = x^2 - y^2$, alors $n \equiv 0, \pm 1 \pmod 4$, car $x^2 \equiv 0, 1 \pmod 4$ et $y^2 \equiv 0, 1 \pmod 4$. Vice-versa, si $n \not\equiv 2 \pmod 4$, alors $n = ab$, où $a \equiv b \pmod 2$. Donc, $n = x^2 - y^2$, où x et y sont définis par les équations

$$a = x + y \quad \text{et} \quad b = x - y,$$

qui possèdent de solutions entières car $a \equiv b \pmod 2$.

La clé derrière la démonstration ci-dessus est la factorisation $x^2 - y^2 = (x - y)(x + y)$. On peut employer une idée semblable pour étudier la suite (1.1). On ne peut pas factoriser l'expression $x^2 + y^2$ sur les entiers, mais on peut le faire si on passe aux **entiers gaussiens**

$$\mathbb{Z}[i] := \{x + iy \,|\, x, y \in \mathbb{Z}\},$$

qui sont un sous-ensemble des nombres complexes. Sur $\mathbb{Z}[i]$, on a que

$$x^2 + y^2 = (x + iy)(x - iy) = |x + iy|^2,$$

où $|x + iy|$ dénote la valeur absolue du nombre complexe $x + iy$. À partir de cette relation, on voit que

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) = |a + ib|^2|c + id|^2 = |(a + ib)(c + id)|^2 = |ac - bd + i(ad + bc)|^2 \\ = (ac - bd)^2 + (ad + bc)^2.\end{aligned}$$

On a montré alors que si $m = \square + \square$ et $n = \square + \square$, alors $mn = \square + \square$, c'est-à-dire la suite de nombres qui sont la somme de deux carrés est **multiplicative**. Vu que les nombres premiers sont les « atoms » de la multiplication, il est naturel d'étudier quels nombres premiers sont la somme de deux carrés. Les nombres premiers de la suite (1.1) sont

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, \ldots$$

Après une brève examination de la suite ci-dessus, on ose à constater :

Conjecture 1.1. *Si p est un nombre premier, alors $p = \square + \square$ s-si $p = 2$ ou $p \equiv 1 \pmod 4$.*

Une partie de notre conjecture est facile à établir : on a que $2 = 1^2 + 1^2$. De plus, si $p \equiv 3 \pmod 4$, alors p ne peut pas s'écrire comme la somme de deux carrés. En effet, $x^2 \equiv 0, 1 \pmod 4$ pour tout $x \in \mathbb{Z}$, donc $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ pour tous $x, y \in \mathbb{Z}$. On trouve, alors que $p \neq \square + \square$ quand $p \equiv 3 \pmod 4$.

La partie difficile de notre conjecture est de montrer que les nombres premiers $p \equiv 1 \pmod 4$ peuvent s'écrire comme la somme de deux carrés. Pour montrer ce fait, on étudiera la structure algébrique des entiers gaussiens. On voit tout d'abord que l'ensemble $\mathbb{Z}[i]$ est fermé sous les opérations usuelles d'addition, de soustraction et de multiplication de nombres complexes. Cependant, $\mathbb{Z}[i]$ n'est pas fermé sous la division. On voit alors que $\mathbb{Z}[i]$ a une structure algébrique similaire avec $\mathbb{Z}$. (Comme on le verra au prochain chapitre, les deux ensembles sont d'*anneaux entiers*.)

Étant données les similarités entre $\mathbb{Z}$ et $\mathbb{Z}[i]$, on peut définir la notion de divisibilité dans $\mathbb{Z}[i]$: si $\alpha, \beta \in \mathbb{Z}[i]$ avec $\beta \neq 0$, on écrit $\beta|\alpha$ s'il existe $\gamma \in \mathbb{Z}[i]$ tel que $\alpha = \beta\gamma$. Par conséquent, on peut aussi parler d'entiers gaussiens premiers : on veut définir $\alpha = x + iy$ d'être premier dans $\mathbb{Z}[i]$ s'il n'a pas une factorisation 'non-triviale' dans $\mathbb{Z}[i]$. Sur $\mathbb{Z}$, chaque entier n possède les factorisations triviales $n = 1 \cdot n$ et $n = (-1)(-n)$. La raison est que les réciproques des entiers 1 et -1 sont aussi entiers ! De manière analogue, les entiers gaussiens dont l'inverse est aussi dans $\mathbb{Z}[i]$ sont de facteurs triviaux de chaque entier gaussien. À part de 1 et -1, les nombres $\pm i$ ont aussi cette propriété : $1/i = -i$ et $1/(-i) = i$. Donc, chaque gaussien α a les factorisations triviales

$$\alpha = 1 \cdot \alpha = (-1)(-\alpha) = i \cdot (-i\alpha) = (-i)(i\alpha).$$

Il est facile de voir que les nombres $\pm 1, \pm i$ sont les seuls gaussiens dont le réciproque est aussi gaussien. En effet, si $x + iy \in \mathbb{Z}[i] \setminus \{0\}$ est tel que $1/(x + iy) \in \mathbb{Z}[i]$, alors $1/(x + iy) = a + ib$

pour quelques $a, b \in \mathbb{Z}$ avec $a + ib \neq 0$. En particulier, $|1/(x + iy)|^2 = a^2 + b^2 \geq 1$, d'où $x^2 + y^2 \leq 1$. Puisque $x + iy \neq 0$, on trouve que $x^2 + y^2 = 1$. On a alors montré que

$$\{x + iy \in \mathbb{Z}[i] : 1/(x + iy) \in \mathbb{Z}[i]\} = \{\pm 1, \pm i\}.$$

Maintenant qu'on a classifié les facteurs triviaux dans $\mathbb{Z}[i]$, on peut définir la notion de primalité dans $\mathbb{Z}[i]$: si $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$ a une factorisation de la forme $\alpha = \beta\gamma$, où $\beta, \gamma \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$, on dit que α est **composé gaussien** ; sinon, on dit qu'il est **premier gaussien**.

Observez que chaque nombre entier $n > 1$ qui est la somme de deux carrés est un composé gaussien : on a que $n = x^2 + y^2 = (x + iy)(x - iy)$ et, puisque $n > 1$, les facteurs $x \pm iy$ sont non-triviaux. En particulier, $2 = 1^2 + 1^2 = (1 + i)(1 - i)$ et $5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i)$ sont de composés gaussiens. Un réciproque partiel existe aussi :

Lemme 1.2. *Si p est un premier dans $\mathbb{Z}$ qui est composé dans $\mathbb{Z}[i]$, alors p est la somme de deux carrés.*

Démonstration. Par hypothèse, on a que $p = (a + ib)(c + id)$ pour quelques $a + ib, c + id \notin \{\pm 1, \pm i\}$. Donc

$$p^2 = |(a + ib)(c + id)|^2 = |a + ib|^2|c + id|^2 = (a^2 + b^2)(c^2 + d^2).$$

Puisque $a + ib, c + id \notin \{\pm 1, \pm i\}$, on a que $a^2 + b^2, c^2 + d^2 > 1$. La primalité de p alors implique que $p = a^2 + b^2 = c^2 + d^2$. □

D'après le lemme 1.2, la preuve de la conjecture 1.1 est réduite à montrer que chaque premier $p \equiv 1 \pmod 4$ est un composé gaussien. Le resultat-clé est le lemme suivant de la théorie des nombres, venant de la théorie des résidus quadratiques :

Lemme 1.3. *Soit p un premier impair. L'équation $x^2 \equiv -1 \pmod p$ a de solutions sur $\mathbb{Z}$ s-si $p \equiv 1 \pmod 4$.*

Démonstration. Soit $k = (p - 1)/2$ et soit

$$G := (\mathbb{Z}/p\mathbb{Z})^* = \{n \pmod p : (n, p) = 1\} = \{1 \pmod p, 2 \pmod p, \ldots, (p - 1) \pmod p\},$$

le groupe multiplicatif mod p. S'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 \pmod p$, alors $x^{2k} \equiv (-1)^k \pmod p$. Nécesairement, $p \nmid x$. Vu que $2k = p - 1 = \#G$, le théorème de Lagrange implique que $x^{2k} \equiv 1 \pmod p$, d'où on déduit que $(-1)^k \equiv 1 \pmod p$. Puisque $1 \not\equiv -1 \pmod p$ de notre hypothèse que p est impair, on trouve que k est pair, c'est-à-dire $p \equiv 1 \pmod 4$.

Vice versa, supposons que $p \equiv 1 \pmod 4$, pour que k soit pair. Les nombres $\pm 1, \pm 2, \ldots, \pm k$ forment un système complet de représentants des résidus réduits mod p, c'est-à-dire $G = \{\pm j \pmod p : 1 \leq j \leq k\}$. Donc

$$\prod_{g \in G} g \equiv 1 \cdot 2 \cdots k \cdot (-1) \cdot (-2) \cdots (-k) \equiv (-1)^k k!^2 \equiv k!^2 \pmod p.$$

D'autre côté, puisque G est un groupe multiplicatif, chaque $g \in G$ possède un inverse. De plus, $g = g^{-1}$ s-si $g^2 \equiv 1 \pmod p$, s-si $p|(g^2 - 1) = (g - 1)(g + 1)$, s-si $p|g - 1$ ou $p|g + 1$, s-si

$g \equiv \pm 1 \pmod p$. Donc, les membres de $G \setminus \{1, -1\}$ peuvent être divisés en paires distincts de la forme $\{g, g^{-1}\}$. Par la suite

$$\prod_{g \in G} g \equiv -1 \cdot 1 \equiv -1 \pmod p,$$

ce qui montre la solubilité de l'équation $x^2 \equiv -1 \pmod p$ en prenant $x = k!$. □

On peut maintenant démontrer qu'un premier $p \equiv 1 \pmod 4$ est la somme de deux carrés. D'après le lemme 1.2, il suffit de montrer qu'il est un gaussien composé. Supposons, au contraire, que p est un premier gaussien. D'après le lemme 1.3, il existe $x \in \mathbb{Z}$ tel que $p|x^2 + 1 = (x - i)(x + i)$ (où la division ici est sur $\mathbb{Z}$). Puisque p est un premier gaussien, il faut que $p|x + i$ ou $p|x - i$ (où la division ici est faite sur $\mathbb{Z}[i]$). Pour simplicité, supposons que $p|x + i$, c'est-à-dire il existe $m, n \in \mathbb{Z}$ tels que $x + i = (m + ni)p$. En particulier, $1 = pn$, ce qui est absurde. Le cas où $p|x - i$ est traité de manière similaire. On a alors montré la conjecture 1.1. Ou, peut-être, non ?

On re-examine l'argument de la paragraphe précédente : on a constaté que si p est un gaussien premier et $p|(x+i)(x-i)$, alors soit $p|x+i$ ou $p|x-i$. Est-ce que cette déduction est évidente ? Le résultat analogue est vrai sur $\mathbb{Z}$, mais sa vérité est fondamentalement liée avec le théorème fondamental de l'arithmétique. La factorisation unique n'est pas évidemment vraie dans $\mathbb{Z}[i]$; il faut la montrer !

Pour expliquer l'importance de ce point subtile, on construit un ensemble similaire à $\mathbb{Z}[i]$ où le théorème fondamental de l'arithmétique est violé. C'est l'ensemble

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Comme les entiers gaussiens, l'ensemble $\mathbb{Z}[i]$ est fermé sous la multiplication, l'addition et la soustraction d'éléments. De plus, dans $\mathbb{Z}[\sqrt{-5}]$ on a les factorisations

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Ces deux factorisations sont différentes de façon essentielle, comme on l'explique ci-dessous.

Fait 1 : les facteurs triviaux de $\mathbb{Z}[\sqrt{-5}]$ sont les nombres ± 1. Pour montrer ce fait, on utilise l'argument qu'on a vu pour $\mathbb{Z}[i]$: si $a+b\sqrt{-5}$ est un élément non-zéro de $\mathbb{Z}[\sqrt{-5}]$ dont le réciproque $1/(a+b\sqrt{-5})$ est aussi dans $\mathbb{Z}[\sqrt{-5}]$, il faut que $a^2 + 5b^2 \leq 1$. Par conséquent, $b = 0$ et $a = \pm 1$.

Fait 2 : les nombres $2, 3, 1 \pm \sqrt{-5}$ ne se factorisent pas de façon non-triviale dans $\mathbb{Z}[\sqrt{-5}]$. En effet, si $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ avec $a + b\sqrt{-5}, c + d\sqrt{-5} \neq \pm 1$, on aurait que

$$4 = |a + b\sqrt{-5}|^2 |c + d\sqrt{-5}|^2 = (a^2 + 5b^2)(c^2 + 5d^2) \quad \Longrightarrow \quad a^2 + 5b^2 = c^2 + 5d^2 = 2,$$

ce qui est impossible. De manière analogue, on peut montrer que les nombres $3, 1 \pm \sqrt{-5}$ n'ont pas de factorisation non-triviale.

Le fait 2 ne suffit pas pour contredit la factorisation unique dans $\mathbb{Z}[\sqrt{-5}]$. Par exemple, dans $\mathbb{Z}$ on a que $4 = 2 \cdot 2 = (-2) \cdot (-2)$ et les facteurs 2 et -2 ne se factorisent pas de façon

non-triviale. Pour conclure la preuve que la factorisation unique est violé dans $\mathbb{Z}[\sqrt{-5}]$, il faut montrer un dernier fait.

Fait 3 : il n'existe pas un facteur trivial $u \in \mathbb{Z}[\sqrt{-5}]$ tel que $2 = u \cdot (1 + \sqrt{-5})$ et $3 = u^{-1} \cdot (1 - \sqrt{-5})$. En effet, les seuls facteurs triviaux sont les nombres ± 1, mais les nombres $2, 3, \pm 1 \pm \sqrt{-5}$ sont tous distincts.

On a alors montré que le théorème fondamental de l'arithmétique est violé dans $\mathbb{Z}[\sqrt{-5}]$. Afin de compléter la preuve de la conjecture 1.1, il faut donc trouver une façon de montrer que le théorème fondamental de l'arithmétique reste vraie dans $\mathbb{Z}[i]$. Pour le faire, on va imiter la démonstration de ce théorème dans $\mathbb{Z}$. La clé dans sa démonstration est le lemme d'Euclide :

Lemme 1.4 (lemme d'Euclide)**.** *Si p est premier et $p|ab$ pour quelques entiers a et b, alors $p|a$ ou $p|b$.*

Démonstration. Supposons que $p \nmid a$. Soit $d = \text{pgcd}(a, p)$. Par définition, d est un facteur positif de p. Mais p est premier et ses seuls facteurs positifs sont less nombres 1 et p. Puisque $p \nmid a$, il faut que $d = 1$. On sait que le plus grand commun diviseur de deux entiers est une combinaison linéaire de ces entiers. En particulier, $1 = ax + py$ pour quelques $x, y \in \mathbb{Z}$, d'où $b = abx + pby$. Puisque $p|ab$ et $p|p$, on a que $p|abx + pby = b$. □

On voit que la clé de la démonstration du lemme d'Euclid est l'algorithme euclidien qui nous a permis d'écrire $\text{pgcd}(a, p)$ comme une combinaison linéaire de a et de p. Finalement, le point de départ pour la démonstration de l'algorithme euclidien est la division euclidienne. Le résultat analogue dans $\mathbb{Z}[i]$ est donné par le le théorème suivant :

Théorème 1.5. *Si $z, w \in \mathbb{Z}[i]$ avec $w \neq 0$, alors il existe $q, r \in \mathbb{Z}[i]$ tels que $|r| < |w|$ et $z = qw + r$.*

Démonstration. On considère le quotient $z/w = x + iy$ pour quelques $x, y \in \mathbb{Q}$. Il existe des entiers a, b tels que $|x - a|, |y - b| \leq 1/2$. On pose $q = a + ib$, pour que $|z/w - q|^2 = |x - a|^2 + |y - b|^2 \leq 1/4 + 1/4 = 1/2$. Donc $r := z - qw$ a magnitude $|r| \leq |w|/\sqrt{2} < |w|$. □

En utilisant le théorème 1.5, on peut montrer que le pgcd de deux nombres gaussiens z, w est une combinaison linéaire de z et w. On peut alors démontrer l'analogue du lemme d'Euclid sur $\mathbb{Z}[i]$. On verra les détails au chapitre 3.

La preuve de la conjecture 1.1 est enfin complète. On peut utiliser ce résultat pour répondre à notre question de classification des entiers qui sont la somme de deux carrés :

Théorème 1.6. *Considérons $n \in \mathbb{N}$ et sa factorisation première $n = p_1^{v_1} \cdots p_r^{v_r}$. Le nombre n peut être écrit comme la somme de deux carrés s-si $2|v_i$ quand $p_i \equiv 3 \pmod 4$.*

Démonstration. Si $n = p_1^{v_1} \cdots p_r^{v_r}$ possède la propriété que $2|v_i$ quand $p_i \equiv 3 \pmod 4$, alors on peut l'écrire $n = d^2 m$, où

$$m = \prod_{\substack{1 \leq i \leq r \\ p_i = 2 \text{ ou } p_i \equiv 1 \pmod 4}} p_i.$$

Du théorème 1.1, on trouve que $p_i = x_i^2 + y_i^2$ quand $p_i \equiv 1 \pmod 4$. Aussi, on a trivialement que $2 = 1^2 + 1^2$. Comme on l'a vu, le produit de sommes de deux carrés est aussi une somme de deux carrés. Donc, $m = x^2 + y^2$ pour quelques $x, y \in \mathbb{Z}$. Par la suite, $n = (dx) + (dy)^2$, ce qui est ce qu'il fallait démontrer.

Réciproquement, supposons que $n = x^2 + y^2$. On pose $d = \text{pgcd}(x, y)$ et on écrit $x = da$ et $y = db$, où $\text{pgcd}(a, b) = 1$, pour que $n = d^2(a^2 + b^2)$. Il suffit de montrer que $a^2 + b^2$ n'est pas divisible par de nombres premiers $p \equiv 3 \pmod 4$. En effet, soit $p|a^2 + b^2$, $p > 2$. On affirme que $p \nmid b$. Sinon, le fait que $p|a^2 + b^2$ impliquerait que $p|a$. Ceci contredit le fait que $\text{pgcd}(a, b) = 1$. Donc, on a montré que $p \nmid b$. En particulier, b est inversible mod p. Puisque $a^2 + b^2 \equiv 0 \pmod p$, on trouve que $(ab^{-1})^2 \equiv -1 \pmod p$. La deuxième partie du lemme 1.3 alors implique que $p \equiv 1 \pmod 4$, ce qui termine la démonstration. □

Le dernier théorème de Fermat

La théorie d'anneaux est née due à un effort de généraliser les résultats de l'arithmétique de $\mathbb{Z}$ à des ensembles plus généraux, comme l'ensemble $\mathbb{Z}[i]$. En fait, historiquement, un ensemble dont l'étude a joué un rôle important dans le développement de la théorie d'anneaux est

$$\mathbb{Z}[\zeta_n] := \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}\},$$

où $\zeta_n = e^{2\pi i/n}$ est une n-ième racine de l'unité. Quand $n = 4$, on revient à $\mathbb{Z}[i]$. L'ensemble $\mathbb{Z}[\zeta_n]$ est important dans l'étude d'un problème fameux, le **dernier théorème de Fermat**. Posé par Fermat comme une affirmation en 1637, ce problème demande de montrer que l'équation

$$x^n + y^n = z^n$$

n'a pas de solutions sur les entiers avec $xyz \neq 0$. La pertinence de $\mathbb{Z}[\zeta_n]$ est facile à voir : si (x, y, z) est une solution, alors

$$x^n = z^n - y^n.$$

Les racines du polynôme $t^n - 1$ sont les nombres $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, donc $t^n - 1 = (t-1)(t-\zeta)\cdots(t-\zeta^{n-1})$. Par la suite,

$$x^n = (z-y)(z-\zeta y)\cdots(z-\zeta^{n-1}y).$$

On voit alors que le produit des nombres $z - \zeta^j y \in \mathbb{Z}[\zeta_n]$ pour $j \in \{0, 1, \ldots, n-1\}$ est une n-ième puissance. Si on savait, par exemple, que les nombres $z - \zeta^j y$ sont deux à deux copremiers dans $\mathbb{Z}[\zeta_n]$, ainsi que le théorème fondamental de l'arithmétique est vrai dans $\mathbb{Z}[\zeta_n]$, on pourrait en déduire que $z - \zeta^j y$ est une n-ième puissance dans $\mathbb{Z}[\zeta_n]$. En 1847, Lamé a publié une fausse démonstration du dernier théorème de Fermat basée sur l'hypothèse que le théorème fondamental de l'arithmétique est vrai dans les ensembles $\mathbb{Z}[\zeta_n]$. Cependant, ceci n'est pas toujours vrai, comme Kummer l'a montré en 1844 (son article original a été publié dans journal obscur et il a été re-publié en 1847 [Jour. de Math. 12 (1847) 185–212]).

La « réparation » de la factorisation unique dans $\mathbb{Z}[\zeta_n]$ et des ensembles similaires a amené à l'introduction de la notion fondamentale des idéaux qu'on va étudier au chapitre 4.

1.1 Exercices

EXERCICE 1.1. Étant donné un entier d, définissons

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

ainsi que la fonction-norme $N(a + b\sqrt{d}) := a^2 - db^2$.

(a) Montrez que $\mathbb{Z}[\sqrt{d}]$ est fermé sous l'addition, la soustraction et la multiplication de nombres complexes.

(b) Montrez que $N(\alpha\beta) = N(\alpha)N(\beta)$ pour tous $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$.

(c) Déterminer si le théorème fondamental d'arithmétique est vrai quand $d = \pm 2, \pm 3, 5, \pm 11$.

EXERCICE 1.2. On sait que l'équation $x^2 \equiv -2 \pmod{p}$ a de solutions s-si $p = 2$ ou $p \equiv 1, 3 \pmod 8$. Montrez qu'un nombre naturel n peut s'écrire comme $n = x^2 + 2y^2$ pour quelques entiers x, y s-si la puissance exacte de chaque premier $p \equiv 5, 7 \pmod 8$ divisant n est paire.

EXERCICE 1.3. Soit

$$\mathcal{O}(\sqrt{5}) = \left\{ \frac{a + b\sqrt{5}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}.$$

(a) Montrez que $\mathcal{O}(\sqrt{5})$ est fermé sous l'addition, la soustraction et la multiplication de nombres réels.

(b) Déterminer si le théorème fondamental d'arithmétique est vrai dans $\mathcal{O}(\sqrt{5})$.

Chapitre 2

Lexique d'anneaux

2.1 Notions de base

Un ensemble A muni de deux lois de composition internes qu'on dénote par $+$ et par $\cdot$, et qu'on appelle « addition » et « multiplication », respectivement, est appelée un **anneau** si :

(i) $(A, +)$ est un groupe abelien, c'est-à-dire :
   - $a + b = b + a$ pour tous $a, b \in A$.
   - il existe un **élément neutre** $0 \in A$ tel que $a + 0 = a$ pour tout $a \in A$.
   - chaque élément $a \in A$ possède un **opposé**, c'est-à-dire il existe un élément $b \in A$ tel que $a + b = 0$. Cet élément est unique (montrer cette affirmation comme exercice) et on le symbolise par $-a$.

(ii) la multiplication est associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pour tous $a, b, c \in A$.

(iii) la multiplication est distributive par rapport à l'addition : $a \cdot (b + c) = a \cdot b + a \cdot c$ et $(a + b) \cdot c = a \cdot c + b \cdot c$, pour tous $a, b, c \in A$.

Souvent, on utilise la notation $(A, +, \cdot)$ pour dénoter l'anneau A et ses opération de l'addition et de la multiplication. De plus, on adopte la convention usuelle que la multiplication est exécutée avant l'addition et la soustraction. Par exemple, au lieu d'écrire $-(a \cdot b)$, on écrit $-a \cdot b$. Finalement, on omet fréquemment le symbole $\cdot$ et on écrit ab au lieu de $a \cdot b$.

Les anneaux possèdent souvent des autres propriétés utiles :

(iv) Si la multiplication est commutative, alors on appelle A **commutatif**.

(v) S'il existe un élément $1 \in A$ tel que $a \cdot 1 = 1 \cdot a = a$ pour tout $a \in A$ (c'est-à-dire, si la multiplication possède un élément neutre), alors on appelle A **unitaire**. L'élément 1 est défini de façon unique (montrer cette affirmation comme exercice) et est appelé l'**unité** de A. Si on veut souligner que 1 est l'unité de A, on le dénote par 1_A.

Si $(A, +, \cdot)$ est un anneau et $B \subset A$, on dit que B est un **sous-anneau** de A si B est un anneau par rapport aux mêmes opérations d'addition et de multiplication. Pour vérifier que B est un sous-anneau de A, il suffit de montrer que :

- $B \neq \emptyset$;
- $a - b \in B$ pour tous $a, b \in B$;

- $ab \in B$ pour tous $a, b \in B$.

Exemple 2.1. L'exemple de base est l'ensemble des entiers $\mathbb{Z}$, muni des opérations usuelles de l'addition et de la multiplication. D'autres exemples sont les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, ainsi que les ensembles $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$ et $\mathbb{Z}[\zeta_n]$ qu'on a vu au chapitre précédent. Tous ces ensembles sont des anneaux commutatifs unitaires.

Exemple 2.2. Pour chaque $n \in \mathbb{Z}_{\geq 1}$, le quotient $\mathbb{Z}/n\mathbb{Z}$, muni des opérations usuelles de l'addition et de la multiplication, est un anneau commutatif unitaire.

Exemple 2.3. Pour chaque $n \in \mathbb{Z}_{\geq 1}$, l'ensemble $M_n(\mathbb{C})$ de matrices carrés $n \times n$ aux coefficients complexes, muni des opérations usuelles de l'addition et de la multiplication de matrices, est un anneau unitaire. Cependant, cet anneau n'est pas commutatif.

Exemple 2.4. Étant donné un anneau $(A, +, \cdot)$, on définit l'ensemble de **polynômes sur** A par

$$A[x] := \{a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{Z}_{\geq 0},\ a_0, a_1, \ldots, a_n \in A\}.$$

On muni cet ensemble de deux opérations, définies comme suivant. Soient $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ et $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ deux polynômes sur A. On met $a_j = 0$ pour $j > m$, $b_j = 0$ pour $j > n$, $k = \max\{m, n\}$ et $\ell = m + n$. On définit alors

$$f(x) + g(x) := (a_0 + b_0) + (a_1 + b_1)x + \cdots (a_k + b_k)x^k,$$

et

$$f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_\ell x^\ell, \quad \text{où} \quad c_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0.$$

C'est facile de vérifier que $A[x]$ devient un anneau avec ces deux opérations. De plus, il hérite des propriétés de A : l'anneau $A[x]$ est unitaire si et seulement A l'est ; de même pour la commutativité.

Une notion importante dans les anneaux polynomiales est le **degré d'un polynôme** : étant donné $f(x) \in A[x] \setminus \{0\}$, on définit son degré $\deg(f)$ comme le plus grand entier $n \geq 0$ tel que le coefficient a_n de la puissance x^n est non-zéro. On appelle a_n le **coefficient en tête** de $f(x)$. Un polynôme sur un anneau unitaire non-trivial dont le coefficient en tête est égal à 1 est appelé **unitaire**. Finalement, on pose $\deg(0) = -\infty$ par convention. Le degré obéit les inégalités importantes suivantes :

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\} \quad \text{et} \quad \deg(fg) \leq \deg(f) + \deg(g).$$

La deuxième inégalité est une égalité pour les polynômes sur $\mathbb{C}$, mais ceci n'est pas le cas en général : par exemple, sur $\mathbb{Z}/4Z$ on a que $\deg(2x) = 1$, mais $\deg((2x)^2) = -\infty$. Ce problème est lié à l'existence de diviseurs de zéro qu'on discute plus bas.

Remarque 2.5. L'anneau polynomial $A[x]$ ne doit être confondu avec l'anneau de *fonctions polynomiales*, c'est-à-dire l'anneau

$$B = \{f : A \to A \,|\, \exists a_0, \ldots, a_n \in A \text{ tels que } f(x) = a_0 + a_1 x + \cdots + a_n x^n \ \forall x \in A\}.$$

En effet, même si dans plusieurs cas importants on a $B = A[x]$ (par exemple, quand $A = \mathbb{C}$), ceci n'est pas le cas en général. Par exemple, si $A = \mathbb{Z}/p\mathbb{Z}$, alors l'expression $x^p - x$ est non-zéro comme polynôme, même si $x^p - x \equiv 0 \pmod p$ pour chaque $x \in \mathbb{Z}/p\mathbb{Z}$ d'après le petit théorème de Fermat (ou le théorème de Lagrange appliqué sur le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$).

Exemple 2.6. Plus généralement, on définit l'anneau polynomial aux n variables $x_1, \ldots, x_n$ par

$$A[x_1, \ldots, x_n] := \left\{ \sum_{j_1=0}^{J_1} \cdots \sum_{j_n=0}^{J_n} a_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n} : J_1, \ldots, J_n \in \mathbb{Z}_{\geq 0},\ a_{j_1,\ldots,j_n} \in A \right\}.$$

On laisse comme exercice la définition de deux opérations qui rend cet ensemble un anneau. Dans cet anneau, le degré de $f(x_1, \ldots, x_n) \neq 0$ est défini par $\deg(f) = \max\{j_1 + \cdots + j_n : a_{j_1,\ldots,j_n} \neq 0\}$. Par exemple, le degré de $x^2y^2 + x^3 \in \mathbb{Z}[x, y]$ est égal à 4. Finalement, on adopte la convention que $\deg(0) = -\infty$.

Exemple 2.7. L'ensemble $2\mathbb{Z} = \{n \in \mathbb{Z} : n \text{ pair}\}$ est un sous-anneau de $\mathbb{Z}$. Notons que, même si $\mathbb{Z}$ est unitaire, $2\mathbb{Z}$ ne l'est pas.

Lemme 2.8. *Soit A un anneaux et a, b deux éléments de A.*

(a) $0 \cdot a = a \cdot 0 = 0$ *;*
(b) $(-a) \cdot b = a \cdot (-b) = -ab$ *;*
(c) $(-a)(-b) = ab$ *;*
(d) si A est unitaire, alors $(-1) \cdot a = -a$.

Démonstration. (a) On a que $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, d'où on déduit que $0 \cdot a = 0$. La preuve du fait que $a \cdot 0 = 0$ est similaire.

(b) On a que $(-a) \cdot b + ab = (-a + a) \cdot b = 0 \cdot b = 0$ par la partie (a). Donc $(-a) \cdot b = -ab$, comme affirmé. La preuve du fait que $a \cdot (-b) = -ab$ est similaire.

(c) Par la partie (b), on a que $(-a)(-b) = a \cdot (-(-b)) = a \cdot b$, comme affirmé.

(d) On a que $(-1) \cdot a = 1 \cdot (-a) = -a$ par la partie (b) et la définition de l'unité 1. □

Corollaire 2.9. *Si A est unitaire et $1 = 0$, alors $A = \{0\}$.*

Démonstration. Si $1 = 0$, on a que $a = a \cdot 1 = a \cdot 0 = 0$ pour tout $a \in A$. □

2.2 Morphismes d'anneaux

Soient A et B deux anneaux. Une application $f : A \to B$ est appelée un **morphisme d'anneaux** si

$$f(a + a') = f(a) + f(a') \quad \text{et} \quad f(aa') = f(a)f(a'), \quad \text{pour tous } a, a' \in A.$$

Si f est injective, on l'appelle un **monomorphisme d'anneaux** ; si elle surjective, on l'appelle un **épimorphisme d'anneaux** ; si elle bijective, on l'appelle un **isomorphisme d'anneaux**.

L'ensemble de tous les éléments de A envoyés à 0 par f est appelé le **noyau** de f et il est dénoté par

$$\ker(f) := \{a \in A : f(a) = 0\}.$$

Il est un sous-anneau de A. De plus, comme on le sait de la théorie des groupes, f est injectif s-si son noyau est trivial, c'est-à-dire $\ker(f) = \{0\}$.

Quand il existe un isomorphisme d'anneaux entre A et B, on les appelle **isomorphes** [1] et on écrit que

$$A \cong B.$$

En langage simple, A et B sont isomorphes comme anneaux quand ils ont les mêmes tables d'addition et de multiplication (après une re-indexation de leurs éléments).

C'est facile de voir que la relation $\cong$ est une relation d'équivalence. Un isomorphisme $f : A \to A$ est appelé un **automorphisme** de A. On dénote l'ensemble de tous les automorphismes de l'anneau A par $\mathrm{Aut}(A)$. Muni de la composition d'application, l'ensemble $\mathrm{Aut}(A)$ devient un groupe.

On étudiera les morphismes d'anneaux de façon plus systématique au chapitre 4.5. On conclut cette section brève avec deux exemples.

Exemple 2.10. Tous les anneaux contenant juste l'élément neutre d'addition sont isomorphes. On peut les identifier et parler de **l'anneau trivial**. Chaque autre anneau est appelé **non-trivial**. D'après le corollaire 2.9, si A est unitaire, alors il est non-trivial s-si $1 \neq 0$.

Exemple 2.11. Soit $A = \mathbb{Z}$ et $B = 2\mathbb{Z}$. Ces deux anneaux ne sont pas isomorphes : A est unitaire, mais B ne l'est pas. Cependant, ils sont isomorphes comme groupes additifs : la fonction $A \ni n \to 2n \in B$ est un isomorphisme de groupes.

2.3 Anneaux intègres et corps

Deux classes spéciales et très importantes d'anneaux sont les anneaux intègres et les corps. On les étudie dans cette section.

Définition 2.12. Soit A un anneau *unitaire et non-trivial*.

(a) Un élément $a \in A$ est appelé **inversible** s'il existe $b \in A$ tel que $ab = ba = 1$. Le nombre b est défini de façon unique (montrer cette affirmation comme exercice) ; on l'appelle l'**inverse** de a et le dénote par a^{-1}.

(b) L'ensemble de tous les éléments inversibles de A est dénoté par $A^\times$ ou par A^*.

(c) Si tous les éléments non-zéros de A sont inversibles, alors on appelle A un **corps gauche**. Si, de plus, A est commutatif, on l'appelle un **corps**.

1. Littéralement, deux objets x et y sont appelés isomorphes quand leurs formes, dans le sens de leurs apparences, sont égales.

(d) Si $K \subset A$ est un sous-anneau de A qui est aussi un corps (c'est-à-dire, $1 \in K$, la multiplication est commutative lorsque restreinte sur K, et chaque élément de K possède un inverse dans K), alors on appelle K un **sous-corps** de A.

Exemple 2.13. (a) Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont tous de corps, contrairement aux anneaux $\mathbb{Z}$ et $\mathbb{Z}[i]$.

(b) Si p est premier, alors l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Souvent, on le dénote par $\mathbb{F}_p$. La lettre F vient du terme anglais pour un corps, qui est *field*.

Une grande différence entre les anneaux généraux et les anneaux plus familiers, comme $\mathbb{Z}$ et $\mathbb{C}$, est la possibilité d'existence de diviseurs de zéro :

Définition 2.14. Soit A un anneau.

(a) Un élément $a \in A \setminus \{0\}$ est appelé un **diviseur de zéro** s'il existe $b \in A \setminus \{0\}$ tel que soit $ab = 0$ ou $ba = 0$.

(b) Si A est commutatif, unitaire, non-trivial, et il n'a pas de diviseurs de zéro, on l'appelle un anneau **intègre**.

Exemple 2.15. (a) Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont intègres.

(b) Si $n > 1$ est composé, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. En effet, il existe $a, b \in \mathbb{Z}_{>1}$ tels que $n = ab$. Donc $ab \equiv 0 \pmod{n}$, mais $n \nmid a, b$ car $1 < a, b < n$. On voit alors que les résidus $a \pmod{n}$ et $b \pmod{n}$ sont de diviseurs de zéro.

Lemme 2.16. *Soit A un anneau intègre. Si $f(x), g(x) \in A[x]$, alors* $\deg(fg) = \deg(f) + \deg(g)$.

Démonstration. Exercice. □

Lemme 2.17. *Soit A un anneau et soit $a \in A \setminus \{0\}$.*

(a) Supposons que a n'est pas un diviseur de zéro. Si $ab = ac$ pour quelques $b, c \in A$, alors $b = c$.

(b) Si a est inversible, alors il n'est pas un diviseur de zéro.

Démonstration. (a) Si $ab = ac$, alors

$$0 = ab - ac = ab + a \cdot (-c) = a \cdot (b - c),$$

d'après le lemme 2.8. Puisque a n'est pas de diviseur de zéro, il faut que $b - c = 0$, c'est-à-dire $b = c$.

(b) Exercice. □

Théorème 2.18.

(a) Si A est un corps, alors il est un anneau intègre.

(b) Si A est un anneau intègre **fini**, *alors il est un corps.*

Démonstration. (a) Un corps est par définition un anneau commutatif, unitaire et non-trivial. De plus, on a que $A^\times = A \setminus \{0\}$. Puisque les inversibles ne sont pas de diviseurs de zéro selon le lemme 2.17(a), l'anneau A n'a pas de diviseurs de zéro. Il est, par conséquent, intègre.

(b) Supposons que A est un anneau intègre fini. Par définition, il est alors commutatif, unitaire et non-trivial. Il reste à montrer que si $a \in A \setminus \{0\}$, alors a est inversible. On considère l'application $f : A \to A$, définie par $f(b) := ab$. Puisque a n'est pas un diviseur de zéro par l'hypothèse que A est intègre, alors le lemme 2.17(b) implique que f est injective. Mais A est fini, donc f doit être aussi surjective. Il existe alors $b \in A$ tel que $ab = 1$. Ceci conclut la démonstration. □

2.4 Corps des fractions

Même si un anneau intègre A n'est pas toujours un corps, on peut de façon naturelle construire un corps qui le contient. Cette construction, appelée le **corps des fractions** de A, est une généralisation de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Comme le nom le dit, les éléments de ce nouveau corps seront de fractions formelles a/b, où a et b sont d'éléments de A. Il faut que le dénominateur b soit non-zéro ; sinon, on va arriver à de conclusions absurdes (justifiez cette affirmation). Pour chaque fraction a/b, alors le pair (a, b) vive dans l'ensemble

$$X := \{(a, b) \in A^2 : b \neq 0\}.$$

On veut que les fractions a/b et c/d soient égales quand $ad = bc$. Pour formaliser cette construction, on impose une relation à l'ensemble X, dénotée par $\approx$:

$$(a, b) \approx (c, d) \quad \Leftrightarrow \quad ad = bc.$$

C'est facile de vérifier que c'est une relation d'équivalence :

- on a que $(a, b) \approx (a, b)$, car A est commutatif comme un anneau intègre ;
- si $(a, b) \approx (c, d)$, alors $(c, d) \approx (a, b)$, encore par la commutativité de A ;
- si $(a, b) \approx (c, d)$ et $(c, d) \approx (e, f)$, alors $ad = bc$ et $cf = de$. Donc $adf = bcf = bde$. Puisque A est commutatif, on en déduit que $daf = dbe$. On peut maintenant utiliser le lemme 2.17(a) pour déduire que $af = be$; en effet, $d \neq 0$, donc d n'est pas un diviseur de zéro car A est intègre. On a alors montré que $(a, b) \approx (e, f)$, comme voulu.

Puisque $\approx$ est une relation d'équivalence, elle partage X dans quelques classes d'équivalence. On dénote la classe d'équivalence de (a, b) par a/b ou par $\frac{a}{b}$, et on dénote l'ensemble de toutes les classes d'équivalence par F, c'est-à-dire

$$F = X/\approx .$$

On muni F de deux opérations :

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Notons que si $b, d \neq 0$, alors $bd \neq 0$ car A est intègre, donc les fractions $(ab + bc)/(bd)$ et $(ac)/(bd)$ sont bien définies. Il faut aussi vérifier que les deux opérations ci-dessus sont bien

définies, c'est-à-dire si on choisit d'autres représentants des classes a/b et c/d, le résultat des opérations sera le même. Supposons, alors, que $(a,b) \approx (a',b')$ et $(c,d) \approx (c',d')$, pour que $ab' = a'b$ et $cd' = c'd$. On veut montrer que $(a'd' + b'c')/(b'd') = (ad+bc)/(bd)$ et que $(a'c')/(b'd') = (ac)/(bd)$. De façon équivalente, il faut vérifier que

$$(a'd' + b'c')bd = b'd'(ad+bc) \quad \text{et} \quad a'c'bd = b'd'ac,$$

ce qui est en effet vrai.

On a alors montré qu'on peut munir F de deux opérations. Il faut montrer que ces deux opérations le rend un corps. Tout d'abord, il faut vérifier qu'il est un anneau. On laisse cette vérification comme exercice aux axioms d'anneaux - on remarque juste que l'élément neutre de F est donné par la fraction $0/1$. Le fait que K est commutatif découle facilement de la commutativité de A. De plus, F est unitaire avec unité la fraction $1/1$. Finalement, F est un corps : soit $a/b \neq 0/1$. On a alors que $a \cdot 1 \neq b \cdot 0$, c'est-à-dire que $a \neq 0$. On peut donc considérer la fraction b/a et vérifier facilement que $(a/b) \cdot (b/a) = 1/1$.

La discussion ci-dessus conclut notre affirmation que l'ensemble F est un corps. On a aussi affirmé que F contient A. Plus précisément, F contient une *copie isomorphe* de A, qui l'ensemble $A' := \{a/1 : a \in A\}$. C'est facile de voir que $A \cong A'$ comme anneaux. Un isomorphisme est donnée par l'application $a \to a/1$. Puisque A et A' sont isomorphes, on peut les identifier, c'est-à-dire, on adopte la convention que $a/1 = a$. Avec cette convention, $A \subset F$.

Exemple 2.19. Si $A = \mathbb{Z}[x]$, alors son corps des fractions est

$$\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Q}[x],\ g(x) \neq 0 \right\}.$$

Quand l'anneau A est contenu dans un corps ambient K (par exemple, quand $A \subset \mathbb{C}$), on peut décrire son corps des fractions en terms des opérations du corps ambient K.

Théorème 2.20. *Soit A un anneau intègre contenu dans un corps K. Alors le corps des fractions de A est isomorphe à $\{ab^{-1} : a \in A,\ b \in A \setminus \{0\}\}$, où l'inversion de b est faite dans K.*

Démonstration. Soit $F = X/\sim$ le corps des fractions de A, comme on l'a défini plus haut, et soit $E = \{ab^{-1} : a \in A,\ b \in A \setminus \{0\}\}$. C'est facile de vérifier que l'application $F \ni a/b \to ab^{-1} \in E$ est bien définie et elle est un isomorphisme d'anneaux. Donc, $F \cong E$, ce qui montre le théorème. □

Exemple 2.21. Si $A = \mathbb{Z}[i]$, alors son corps des fractions est isomorphe à

$$\mathbb{Q}[i] = \{a + bi \,|\, a, b \in \mathbb{Q}\}.$$

En effet, en appliquant le théorème 2.20, on a que le corps des fractions de A est isomorphe à $F := \{(a+bi)(c+di)^{-1} : a,b,c,d \in \mathbb{C}, (c,d) \neq (0,0)\}$. Évidemment, on a que $\mathbb{Q}[i] \subset F$. De plus, dans $\mathbb{C}$ on a que

$$(a+bi)(c+di)^{-1} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + i\frac{-ad+bc}{c^2+d^2} \in \mathbb{Q}[i].$$

Donc, on a aussi que $F \subset \mathbb{Q}[i]$, ce qui montre que $F = \mathbb{Q}[i]$.

On fini cette section en montrant une caractérisation *catégorique* (i.e. référant à la *théorie des catégories*) du corps des fractions comme *le plus petit corps* contenant A :

Théorème 2.22. *Soit A un anneau intègre et soit F son corps des fractions.*

(a) Si K est un corps contenant A, alors il existe un corps $F' \cong F$ tel que $A \subset F' \subset K$.

(b) Supposons que E est un corps tel que :

- *E contient A ;*
- *Si K est un corps contenant A, alors il existe un corps $E' \cong E$ tel que $A \subset E' \subset K$.*

Donc, $E \cong F$.

Démonstration. (a) Supposons que K est un corps contenant A. Si $F' := \{ab^{-1} : a \in A,\ b \in A \setminus \{0\}\}$, alors $F' \cong F$ d'après le théorème 2.20. Ceci montre la première partie du théorème.

(b) Sans perte de généralité, on peut supposer que $A \subset E$. Par la partie (a), il faut que E contient une copie isomorphe de F, soit $F' \subset E$. En fait, on a que $F' = \{ab^{-1} : a \in A,\ b \in A \setminus \{0\}\}$, où l'inversion de b est faite dans E. Puisque F' est un corps contenant A, les hypothèses sur E impliquent qu'il existe un corps $E' \cong E$ tel que $A \subset E' \subset F'$. Mais si $A \subset E'$, alors $ab^{-1} \in E'$ pour tous $a \in A$, $b \in A \setminus \{0\}$. On en déduit que $E' = F'$. Puisque $E' \cong E$ et $F' \cong F$, on conclut que $E \cong F$, comme voulu. □

2.5 Exercices

Exercice 2.1 (ex. 25, p. 232). Soit A un anneau unitaire. Montrez que

$$(1+1)(a+b) = a+b+a+b,$$

ainsi que

$$(1+1)(a+b) = a+a+b+b.$$

Concluez qu'on peut enlever des axioms l'hypothèse que l'addition est commutative.

Exercice 2.2. Soit A un anneau intègre. Montrez que les éléments inversibles de $A[x]$ sont les polynômes constants $f(x) = a$, où $a \in A^\times$.

Exercice 2.3. On définit l'ensemble des quaternions de Hamilton

$$\mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

Cet ensemble devient un anneau unitaire et non-commutatif si on définit l'addition par

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) := (a + a') + (b + b')i + (c + c')j + (d + d')k$$

et la multiplication selon les règles

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Par exemple, $(1+i)(j+k) = 1+k+ij+ik = 1+k-k-j = 1-j$. On défini la norme $N : \mathbb{H} \to [0, +\infty)$ par

$$N(a+bi+cj+dk) = a^2+b^2+c^2+d^2.$$

(a) Prouvez que $N(\alpha) = \alpha\overline{\alpha}$ pour tout $\alpha \in I$, où $\overline{a+bi+cj+dk} := a-bi-cj-dk$. Déduisez que $\mathbb{H}$ est un corps gauche.

(b) Prouvez que $N(\alpha\beta) = N(\alpha)N(\beta)$ pour tout $\alpha, \beta \in I$.

(c) Si

$$I = \{a+bi+cj+dk : a, b, c, d \in \mathbb{Z}\},$$

est l'anneau des quaternions de Hamilton intégraux, alors montrez qu'un élément de I est inversible dans I s-si sa norme est égale à 1. Déduisez que $I^\times$ est un groupe de 8 éléments.

EXERCICE 2.4 (ex. 7, 8, p. 231).

(a) Soit A un anneau. Son **centre** est défini d'être

$$C = \{z \in A : za = az \text{ pour tout } a \in A\},$$

c'est-à-dire, l'ensemble des éléments qui commutent avec tous les éléments de A. Prouvez que :

(i) C est un sous-anneau de A ;

(ii) si A a une unité 1, alors $1 \in C$;

(iii) le centre d'un corps gauche est un corps.

(b) Décrivez le centre des quaternions réelles de Hamilton $\mathbb{H}$. Montrez que $\{a+bi : a, b \in \mathbb{R}\}$ est un sous-anneau de $\mathbb{H}$ qui est un corps mais qu'il n'est pas contenu au centre de $\mathbb{H}$.

EXERCICE 2.5 (ex. 15, 16, 22, p. 231-2). Un anneau A est appelé un **anneau de Boole** si $a^2 = a$ pour tout $a \in A$.

(a) Montrez que chaque anneau de Boole est commutatif.

(b) Montrez que le seul anneau de Boole qui est également intègre est $\mathbb{Z}/2\mathbb{Z}$.

(c) Donnez un exemple d'un anneau de Boole infini.

EXERCICE 2.6 (ex. 17, 19, p. 231). (a) Soit A et B anneaux. Prouvez que le produit direct $A \times B$, muni des opérations de l'addition $(a, b) + (a', b') := (a + a', b + b')$ et de la multiplication $(a, b) \cdot (a', b') := (aa', bb')$, est un anneau.

(i) Montrez que $A \times B$ est commutatif s-si A et B sont commutatifs.

(ii) Montrez que $A \times B$ possède d'une unité s-si A et B possèdent d'une unité.

(iii) Est-que c'est possible que $A \times B$ est un anneau intègre ?

(b) Soit A un anneau. Prouvez que l'ensemble $\{(a, a) : a \in A\}$ est un sous-anneau de $A \times A$.

EXERCICE 2.7 (ex. 26, 27, p. 232-3).

(a) Soit K un corps. Une valuation discrète sur K est une fonction $\nu : K^\times \to \mathbb{Z}$ qui satisfait :
- $\nu(xy) = \nu(x) + \nu(y)$,
- ν est surjective,
- $\nu(x+y) \geq \min(\nu(x), \nu(y))$ pour tout $x, y \in K^\times$ avec $x + y \neq 0$.

L'ensemble
$$A = \{x \in K^\times : \nu(x) \geq 0\} \cup \{0\}$$
est appelé l'anneau de valuation de ν. Prouvez que :
(i) A est un sous-anneau de K qui contient l'unité de K.
(ii) pour tout $x \in K^\times$ on a que soit $x \in A$ ou $x^{-1} \in A$.
(iii) un élément x de A set inversible s-si $\nu(x) = 0$.

(b) Soit $K = \mathbb{Q}$ and p un nombre premier. Montrez que la fonction $\nu_p(a/b) = \ell$, où
$$\frac{a}{b} = p^\ell \cdot \frac{c}{d} \quad \text{avec} \quad p \nmid cd,$$
est une valuation discrète. Aussi, prouvez que l'anneau de valuation discrète qui correspond à ν_p est l'anneau de tous les nombres rationnels dont dénominateur est co-premier à p. Décrivez les éléments inversibles de cet anneau.

EXERCICE 2.8. Soit $D \in \mathbb{Z}$. Montrez que le corps de fractions de $\mathbb{Z}[\sqrt{D}]$ est isomorphe à
$$\mathbb{Q}[\sqrt{D}] := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}.$$

EXERCICE 2.9. Soit $A = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Z}\}$.

(a) Montrez que A est un sous-anneau de $\mathbb{C}$.

(b) (difficile) Montrez que le corps des fractions de A est isomorphe à
$$F = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Q}\}.$$
(C'est donné que si $a, b, c \in \mathbb{Q}$, alors $a + b2^{1/3} + c2^{2/3} = 0$ s-si $a = b = c = 0$.)

EXERCICE 2.10. Soit A et B anneaux intègres et E et F leurs corps des fractions, respectivement. Considérons les morphismes $\iota : A \to F$ et $j : B \to E$, définis par $\iota(a) = a/1_A$ et $j(b) = b/1_B$. Si $\phi : A \to B$ est un morphisme injectif d'anneaux, il y a un morphisme injectif $\hat{\phi} : F \to E$ tel que le diagramme
$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle j} \\ F & \xrightarrow{\hat{\phi}} & E \end{array}$$
commute, c'est-à-dire $\hat{\phi} \circ \iota = j \circ \phi$.

EXERCICE 2.11.

(a) Soit A un anneaux. Si $\{A_i : i \in I\}$ est un ensemble de sous-anneaux de A (respectivement, de sous-corps de A), alors montrez que leur intersection $\bigcap_{i\in I} A_i$ est un sous-anneau de A (resp. un sous-corps de A).

(b) Soient A un anneau commutatif et unitaire, $\alpha_1, \ldots, \alpha_n \in A$ et B un sous-anneaux de A contentant l'unité 1_A. Définissons $B[\alpha_1, \ldots, \alpha_n]$ d'être le plus petit sous-anneau de A contenant B et les éléments $\alpha_1, \ldots, \alpha_n$. Montrez que [2]

$$\begin{aligned} B[\alpha_1, \ldots, \alpha_n] &= \{f(\alpha_1, \ldots, \alpha_n) : f(x_1, \ldots, x_n) \in B[x_1, \ldots, x_n]\} \\ &= \left\{ \sum_{j_1=0}^{J_1} \cdots \sum_{j_n=0}^{J_n} b_{j_1,\ldots,j_n} \alpha_1^{j_1} \cdots \alpha_n^{j_n} : J_1, \ldots, J_n \in \mathbb{N} \cup \{0\},\ b_{j_1,\ldots,j_n} \in B \right\}. \end{aligned}$$

(c) Quand $B = \mathbb{Z}$, $A = \mathbb{C}$ et $d \in \mathbb{N}$, montrez que la définition de $\mathbb{Z}[\sqrt{d}]$ donnée ci-dessus est consistante avec sa définition comme l'ensemble $\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

(d) Soient L un corps, $\alpha_1, \ldots, \alpha_n \in L$ et K un sous-corps de L. Définissons $K(\alpha_1, \ldots, \alpha_n)$ d'être le plus petit sous-corps de L contenant K et les éléments $\alpha_1, \ldots, \alpha_n$.

(i) Prouvez que $K(\alpha_1, \ldots, \alpha_n)$ est le corps des fractions de $K[\alpha_1, \ldots, \alpha_n]$.

(ii) Montrez que [3]

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : \begin{array}{l} f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \end{array} \right\}.$$

(e) (i) Quand $K = \mathbb{Q}$, $L = \mathbb{C}$, et $d \in \mathbb{N}$, montrez que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$. (Donc, la définition de $\mathbb{Q}[i]$ donnée à l'exercice 2.8 est consistante avec la définition de cet exercice.)

(ii) Plus généralement, montrez que si α est un nombre irrationnel quadratique (c'est-à-dire, $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ et $f(\alpha) = 0$ pour un polynôme quadratique $f(x) \in \mathbb{Q}[x]$), alors $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

EXERCICE 2.12. Soit un nombre sans-carré $D \in \mathbb{Z} \setminus \{0, 1\}$. Posons

$$\omega = \begin{cases} (1 + \sqrt{D})/2 & \text{si } D \equiv 1 \pmod 4, \\ \sqrt{D} & \text{si } D \equiv 2, 3 \pmod 4, \end{cases}$$

et $\mathcal{O} = \mathbb{Z}[\omega]$ selon la définition donnée dans l'exercice 2.11.

(a) Montrez que $\mathcal{O} = \{a + b\omega : a, b \in \mathbb{Z}\}$.

(b) Montrez que $\mathcal{O}$ est l'ensemble de tous les éléments de $\mathbb{Q}(\sqrt{D})$ qui sont de racines d'un polynôme quadratique unitaire sur $\mathbb{Z}$. (Pour cette raison, on appel $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.)

2. Ici $f(\alpha_1, \ldots, \alpha_n)$ est la valeur de $f(x_1, \ldots, x_n)$ quand $x_j = \alpha_j$ pour tout $j \in \{1, \ldots, n\}$, qui est un élément de l'anneau A.

3. Puisque on travaille dans un corps L, $\frac{a}{b}$ est la même chose que $a \cdot b^{-1}$.

EXERCICE 2.13 (ex. 12, p. 248). Soit D un nombre entier qui n'est pas un carré parfait dans $\mathbb{Z}$. Considerons

$$S = \left\{ \begin{pmatrix} a & b \\ Db & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Montrez les propositions suivantes.

(a) S est un sous-anneau de $M_2(\mathbb{Z})$,

(b) L'application $\phi : \mathbb{Z}[\sqrt{D}] \to S$, définie par

$$\phi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix},$$

est un isomorphisme d'anneaux.

(c) Si $D \equiv 1 \pmod 4$, l'ensemble

$$T = \left\{ \begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

est un sous-anneaux de $M_2(\mathbb{Z})$ qui est isomorphe avec l'anneau

$$\mathcal{O} = \left\{ a + b \cdot \frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z} \right\}.$$

EXERCICE 2.14. (a) Soit $\phi : K \to A$ un morphisme d'anneaux, où K est un corps. Montrez que si $\phi \neq 0$, alors ϕ est un monomorphisme.

(b) Soit $\phi : \mathbb{C} \to \mathbb{C}$ un morphisme d'anneaux non-trivial. Montrez que $\phi(x) = x$ pour tout $x \in \mathbb{Q}$.

(c) Soit $\phi : \mathbb{R} \to \mathbb{R}$ un isomorphisme d'anneaux. Montrez que ϕ est l'identité. [*Indice :* Montrez que $\phi(x) > 0$ pour $x > 0$.]

Chapitre 3

Divisibilité

Dans ce chapitre, on généralise les notions de la divisibilité et de la primalité dans d'anneaux plus généraux que les entiers.

3.1 Le plus grand commun diviseur

Définition 3.1. Soit A un anneau commutatif, et soient $a, b \in A$ avec $b \neq 0$.

(a) On dit que b **divise** a et on écrit $b|a$ s'il existe $c \in A$ tel que $a = bc$.

(b) Soit $d \in A \setminus \{0\}$. On dit que d est un **plus grand commun diviseur** de a et de b (souvent abrégé comme pgcd) si :

(i) $d|a$ et $d|b$;

(ii) si $d'|a$ et $d'|b$, alors $d'|d$.

On dénote l'ensemble de tous les pgcd de a et de b par $\text{pgcd}(a, b)$.

Remarque 3.2. Une propriété importante de $\mathbb{Z}$ est qu'il existe toujours un pgcd de deux entiers non-zéros. Ceci n'est pas le cas en général : c'est possible que $\text{pgcd}(a, b) = \emptyset$ (voir exercice 3.1).

En examinant la définition du pgcd, on voit tout de suite que si $d \in \text{pgcd}(a, b)$ et $u \in A^\times$, alors $ud \in \text{pgcd}(a, b)$. Ceci nous amène à la définition suivante :

Définition 3.3. Soit A un anneau commutatif, unitaire et non-trivial. Soient, aussi, $a, b \in A$. On dit que a et b sont **associés** et on écrit $a \sim b$ s'il existe un élément inversible $u \in A$ tel que $b = ua$.

C'est facile de montrer que la relation d'association est une relation d'équivalence. La classe d'équivalence de 1 est l'ensemble $A^\times$, et la classe d'équivalence de 0 et le singleton $\{0\}$. La proposition suivante montre que l'ensemble $\text{pgcd}(a, b)$ est aussi une classe d'équivalence.

Proposition 3.4. *Soit A un anneau intègre, $a \in A$ et $b \in A \setminus \{0\}$. Si $d, d' \in \text{pgcd}(a, b)$, alors $d \sim d'$. Vice versa, si $d \in \text{pgcd}(a, b)$ et $d' \sim d$, alors $d' \in \text{pgcd}(a, b)$.*

Démonstration. Puisque $d, d' \in \text{pgcd}(a, b)$, par l'axiom (ii) de la définition du pgcd, on a que $d'|d$, ainsi que $d|d'$. Donc, il existe $u, v \in A$ tels que $d' = ud$ et $d = vd'$. On a alors que $d = vud$. Puisque $d \neq 0$ et A est intègre, le lemme 2.17(a) implique que $vu = 1$, ce qui veut dire que u est inversible, comme voulu.

La deuxième partie de la proposition est déjà prouvée. □

La démonstration précédente prouve, entre autres, un critère pour déterminer si deux éléments sont associés.

Lemme 3.5. *Soit A un anneau intègre et $a, b \in A \setminus \{0\}$. On a que $a \sim b$ s-si $a|b$ et $b|a$.*

On conclut cette section avec une dernière définition.

Définition 3.6. Soit A un anneau commutatif et unitaire, et soient $a, b \in A$ avec $b \neq 0$. On dit que a et b sont **copremiers** is $1 \in \text{pgcd}(a, b)$.

Lemme 3.7. *Soit A un anneau commutatif et unitaire, et soient $a, b \in A$ avec $b \neq 0$. Alors a et b sont copremiers s-si tous leurs communs diviseurs sont d'éléments inversibles de A.*

Démonstration. Supposons, d'abord, que $1 \in \text{pgcd}(a, b)$. Si $d \neq 0$ est un commun diviseur de a et de b, alors $d|1$ par définition, ce qui veut dire que $1 = de$ pour un $e \in A$. Ceci implique que $d \in A^\times$.

Vice versa, supposons que tous les communs diviseurs de a et de b sont d'éléments inversibles de A. On affirme que $1 \in \text{pgcd}(a, b)$. En effet, c'est évident que $1|a$ et que $1|b$. De plus, si $d|a$ et $d|b$, alors $d \in A^\times$ par hypothèse. Donc il existe $e \in A$ tel que $1 = de$, d'où on trouve que $d|1$, ce qui est ce qu'il fallait démontrer. □

3.2 Anneaux euclidiens

Dans $\mathbb{Z}$, le pgcd de deux entiers est exprimable comme une combinaison linéaire de ces entiers. On donne un nom spécial aux anneaux possédant cette propriété :

Définition 3.8. On dit qu'un anneau A est un **anneau de Bezout** si :

(i) A est intègre ;
(ii) pour tout $a \in A$ et tout $b \in A \setminus \{0\}$, on a que $\text{pgcd}(a, b) \neq \emptyset$;
(iii) si $d \in \text{pgcd}(a, b)$, alors il existe $x, y \in A$ tels que $d = ax + by$.

L'exemple prototype d'un anneau de Bezout est $\mathbb{Z}$. Dans cet anneau, les coefficients x et y peuvent être calculé en utilisant l'algorithme euclidien. Il existe une grande généralisation de ce fait, sur une famille importante d'anneaux qui possèdent un analogue de la division euclidienne :

Définition 3.9. Soit A un anneau intègre. Supposons qu'il existe une fonction $N : A \to \mathbb{Z}_{\geq 0}$ telle que $N(0) = 0$ et $N(a) > 0$ pour $a \neq 0$. Supposons, aussi, que pour chaque $a \in A$ et

chaque $b \in A \setminus \{0\}$, il existe q, r satisfaisant les relations

$$a = bq + r \quad \text{et} \quad N(r) < N(b).$$

On dit alors que A est un **anneau euclidien** et on appelle N un **préstathme euclidien** [1] [2].

Si N a la propriété additionnelle que $N(a) \leq N(b)$ quand $a|b$ avec $a, b \neq 0$, alors l'appelle un **stathme euclidien**.

Exemple 3.10. L'anneau $\mathbb{Z}$ est euclidien par rapport au stathme $N(a) = |a|$.

Exemple 3.11. L'anneau $\mathbb{Z}[i]$ est euclidien par rapport au stathme $N(a + bi) = a^2 + b^2$, comme on l'a montré au théorème 1.5.

Exemple 3.12. Un corps K est toujours euclidien, avec stathme $N(a) = 0$ si $a = 0$, et $N(a) = 1$ si $a \neq 0$.

Exemple 3.13. Si K est un corps, alors l'anneau polynomial $K[x]$ est euclidien par rapport au stathme $N(f) = 2^{\deg(f)}$. En effet, soient $f(x) \in K[x]$ et $g(x) \in K[x] \setminus \{0\}$. On utilise induction sur $\deg(f)$ pour montrer qu'il existe $q(x), r(x) \in K[x]$ tels que

$$f(x) = q(x)g(x) + r(x) \quad \text{et} \quad N(r) < N(g). \tag{3.1}$$

Si $f(x) = 0$, on a que $f(x) = 0 \cdot g(x) + 0$, où $N(0) = 0 < N(g)$. Supposons maintenant que $f(x) \neq 0$. On écrit $f(x) = a_0 + a_1x + \cdots + a_mx^m$ et $g(x) = b_0 + b_1x + \cdots + b_nx^n$, où $m = \deg(f)$ et $n = \deg(g)$. En particulier, $b_n \neq 0$. Si $m < n$, on peut mettre $q(x) = 0$ et $r(x) = g(x)$; sinon, on observe que le polynôme

$$f_1(x) = f(x) - \frac{a_m}{b_n}x^{m-n}g(x)$$

a degré $< m$. Par l'hypothèse d'induction, il existe alors $q_1(x), r_1(x) \in K[x]$ tels que $f_1(x) = q_1(x)g(x)+r_1(x)$ et $N(r_1) < N(g)$. La relation (3.1) découle en posant $q(x) = q_1(x)+\frac{a_m}{b_n}x^{m-n}$ et $r(x) = r_1(x)$.

L'argument de l'exemple précédent se généralise facilement pour montrer le résultat suivant :

Théorème 3.14. *Soit A un anneau intègre. Considérons deux polynômes $f(x) \in A[x]$ et $g(x) \in A[x]\setminus\{0\}$. Si le coefficient en tête de $g(x)$ est inversible, alors il existe $q(x), r(x) \in A[x]$ tels que $f(x) = q(x)g(x) + r(x)$ et $\deg(r) < \deg(g)$.*

1. D'autres auteurs utilisent de petites variations de la définition d'un stathme euclidien. Par exemple, souvent le stathme est défini seulement sur les éléments non-zéro. D'autres fois, le préstathme n'est pas supposé d'avoir la propriété que $N(a) > 0$ pour $a \neq 0$. Dans ces variations, il faut supposer dans la définition d'un anneau euclidient que soit $r = 0$ soit $N(r) < N(b)$.

2. Parfois, on appelle une telle fonction une *norme euclidienne*. Le mot stathme vient du grec et veut dire littéralement 'niveau', référant habituellement au niveau d'un liquide, comme l'eau de mer. Cette définition nous permet de visualiser le concept d'un stathme : si $N(a) = N(b)$, on imagine que a et b sont au même 'niveau'. Par contre, si $N(a) < N(b)$, alors on imagine que a est 'plus bas' que b.

À la section prochaine, on montrera que le théorème fondamental d'arithmétique est vrai dans les anneaux euclidiens. Une étape cruciale dans cette démonstration est donné au théorème suivant :

Théorème 3.15. *Chaque anneau euclidien est un anneau de Bezout.*

Démonstration. Soit $q \in A$. Si $d|a$ et $d|b$, alors $d|a-qb$ et $d|b$. Vice versa, si $d|a-qb$ et $d|b$, alors $d|(a-qb)+qb = a$ et $d|b$. Donc, on a la relation cruciale que $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a-qb,b)$. De plus, puisque A est euclidien, on sait qu'il existe $q_1 \in A$ tels que $N(a-q_1b) < N(b)$. On met $a_0 = a$, $a_1 = a$ et $a_2 = a - q_1b$, pour que

$$\operatorname{pgcd}(a_0,a_1) = \operatorname{pgcd}(a_1,a_2) \quad \text{et} \quad N(a_2) < N(a_1).$$

Si $a_2 \neq 0$, on divise a_1 par a_2 pour trouver un $q_2 \in A$ tel que $N(a_1 - q_2a_2) < N(a_2)$. Si $a_3 = a_1 - q_2a_2$, alors

$$\operatorname{pgcd}(a_0,a_1) = \operatorname{pgcd}(a_1,a_2) = \operatorname{pgcd}(a_2,a_3) \quad \text{et} \quad N(a_3) < N(a_2) < N(a_1).$$

Si $a_3 \neq 0$, on répète l'argument précédent pour trouver un $q_3 \in A$ tel que $\operatorname{pgcd}(a_2,a_3) = \operatorname{pgcd}(a_3,a_4)$, où $a_4 = a_2 - q_3a_3$ et $N(a_4) < N(a_3)$. Cette procedure doit terminer après un nombre d'étapes fini, car les nombres $N(a_1), N(a_2), N(a_3), \ldots$ sont tous des entiers distincts dans l'intervalle $[0, N(a_1)]$. À la dernière étape, soit la n-ième, on aura que $a_{n+1} = a_{n-1} - q_na_n = 0$. Donc

$$\operatorname{pgcd}(a_0,a_1) = \operatorname{pgcd}(a_n,0).$$

Evidemment, a_n est un pgcd des nombres a_n et 0, donc $\operatorname{pgcd}(a,b) \neq \emptyset$. De plus, par construction, on a que $a_j = a_{j-2} - q_{j-1}a_{j-1}$ pour chaque $j \in \{2,\ldots,n\}$. En particulier, a_j est une combinaison linéaire de a_{j-1} et de a_{j-2}. On voit alors que a_n est une combinaison linéaire de a_0 et de a_1. Les coefficients peuvent être calculés :

$$a_n = a_{n-2} - q_{n-1}a_{n-1} = a_{n-2} - q_{n-1}(a_{n-3} - q_{n-2}a_{n-2}) = -q_{n-1}a_{n-3} + (1+q_{n-1}q_{n-2})a_{n-2} = \cdots.$$

Ceci termine la démonstration. □

On conclut cette section avec une étude des stathmes et des préstathmes euclidiens.

Proposition 3.16. *Soit A un anneau euclidien*

(a) Si N est un préstathme euclidien de A, alors la fonction

$$\tilde{N}(a) := \min_{k \in A\setminus\{0\}} N(ka)$$

est un stathme euclidien.

(b) Soit N un stathme de A.

(i) Si $a \sim b$, alors $N(a) = N(b)$.

(ii) Si $a, b \neq 0$ et $a|b$, alors $N(a) = N(b)$ s-si $a \sim b$.

Démonstration. (a) Évidemment, si $a|b$ et $a, b \neq 0$, alors $\tilde{N}(a) \leq \tilde{N}(b)$.

Or, soient $a \in A$ et $b \in A \setminus \{0\}$. On veut montrer qu'il existe $q, r \in A$ tels que $a = qb + r$ et $\tilde{N}(r) < \tilde{N}(b)$. Soit $k \neq 0$ tel que $N(kb) = \tilde{N}(b)$. Il existe $q_0, r_0 \in A$ tels que $ka = q_0 \cdot (kb) + r_0$ et $N(r_0) < N(kb) = \tilde{N}(b)$. Posons $q = q_0$ et $r = a - qb$. On a que $r_0 = kr$, donc $\tilde{N}(r) \leq N(r_0) < N(kb) = \tilde{N}(b)$. Ceci prouve que N est un stathme euclidien.

(b-i) Si $a = b = 0$, on a que $N(a) = N(b) = 0$ par définition. Si $a \sim b \neq 0$, alors $a|b$ et $b|a$. Donc, $N(a) \leq N(b) \leq N(a)$, par hypothèse.

(b-ii) Soit $b = ka$, pour que $N(ka) = N(a)$. On veut montrer que k est inversible. Il suffit de montrer que $ka|a$. Il existe $q, r \in A$ tels que $a = qka + r$ et $N(r) < N(ka) = N(a)$. Évidemment, $a|r$. Si $r \neq 0$, alors $N(a) \leq N(r)$ par l'hypothèse que N est un stathme euclidien. Mais ceci est impossible, donc il faut que $r = 0$, comme voulu. □

3.3 Primalité

Afin d'étudier l'arithmétique des anneaux intègres, on introduit de nouvelle terminologie :

Définition 3.17. Soit A un anneau intègre.

(a) Un élément $a \in A \setminus \{0\}$ est appelé **réductible** s'il existe $b, c \in A \setminus A^\times$ tels que $a = bc$.

(b) Un élément $a \in A \setminus (A^\times \cup \{0\})$ est appelé **irréductible** s'il n'est pas réductible. C'est-à-dire, $a \in A \setminus (A^\times \cup \{0\})$ est irréductible si pour chaque $d|a$, on a que soit $d \sim 1$ ou $d \sim a$.

(c) Un élément $p \in A \setminus (A^\times \cup \{0\})$ est appelé **premier** si chaque fois que $p|ab$ pour quelques $a, b \in A$, on a nécessairement que soit $p|a$ ou $p|b$.

On voit que dans $\mathbb{Z}$ et dans $\mathbb{Z}[i]$ les notions de la primalité et de l'irréductibilité coincident. Cependant, ce n'est pas toujours le cas : selon la discussion au chapitre précédent, les nombres $2, 3, 1 \pm \sqrt{5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$. Mais ils ne sont pas premiers. Par exemple, $2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, mais $2 \nmid 1 \pm \sqrt{-5}$.

En général, la primalité est une propriété plus forte que l'irréductibilité. Elles sont, quand même, équivalentes dans les anneaux de Bezout :

Théorème 3.18. *Soit A un anneau intègre.*

(a) Si p est un élément premier de A, alors il est aussi irréductible.

(b) (lemme d'Euclide) Si A est un anneaux de Bezout, alors un élément $p \in A$ est premier si et seulement s'il est irréductible.

Démonstration. (a) Supposons que $p = ab$. En particulier, $p|ab$ et, puisque p est premier, il faut que soit $p|a$ ou $p|b$. Sans perte de généralité, on suppose que $p|a$ - l'autre cas est traité de manière similaire. On a alors que $a = pc$ pour un $c \in A$. En remplaçant cette relation à l'équation $p = ab$, on trouve que $p = pbc$. Puisque p n'est pas zéro (donc, il n'est pas un diviseur de zéro), le lemme 2.17(a) implique que $bc = 1$, ce qui veut dire que b est inversible. On a donc montré que p n'a pas une factorisation non-triviale. Ceci termine la démonstration de la partie (a).

(b) Supposons, maintenant, que A est un anneau de Bezout. Soit p un élément irréductible de A. Supposons que $p|ab$. On veut montrer que soit $p|a$ ou $p|b$. Supposons que $p \nmid a$. Soit d un pgcd de a et de p. En particulier, $d|p$ et, puisque p est irréductible, il faut que soit $d \sim 1$ ou $d \sim p$. Mais on sait que $d|a$, ainsi que $p \nmid a$. Donc, on ne peut pas avoir que $d \sim p$. Il faut alors que $d \sim 1$, c'est-à-dire 1 est un pgcd de a et de p. L'hypothèse que A est un anneau de Bezout veut dire qu'on peut écrire 1 comme une combinaison linéaire de a et de p, soit $1 = ax + py$. Donc $b = abx + pby$. Puisque $p|ab$ et $p|p$, il faut que $p|b$ également. Ceci termine la démonstration. □

3.4 Anneaux factoriels

En utilisant le concept d'irréductibilité, on peut définir de façon précise qu'est-ce qu'on veut dire quand on dit que 'le théorème fondamental d'arithmétique reste vrai dans un anneau A' :

Définition 3.19. Soit A un anneau intègre. Supposons que pour chaque $a \in A \setminus (A^\times \cup \{0\})$ il existe une factorisation $a = p_1 \cdots p_m$ dans quelques éléments irréductibles de A. Supposons, aussi, que cette factorisation est unique, dans le sens que si $a = q_1 \cdots q_n$ est une autre telle factorisation de a, alors $m = n$ et il existe une permutation $\sigma \in S_m$ telle que $q_j \sim p_{\sigma(j)}$ pour chaque $j \in \{1, \ldots, m\}$. On dit alors que A est un anneau **factoriel**.

On commence en montrant que le théorème fondamental d'arithmétique est vrai dans chaque anneau euclidien.

Théorème 3.20. *Chaque anneau euclidien est aussi factoriel.*

Démonstration. Soit A un anneau euclidien. D'après la proposition 3.16(a), il existe un stathme euclidien N. On montre d'abord que $a \in A \setminus (A^\times \cup \{0\})$ possède une factorisation dans quelques irréductibles. Sinon, il existe un tel a de stathme minimal. Évidemment, un tel a ne peut pas être irréductible. Alors, il existe une factorisation $a = bc$, où b et c sont non-inversibles. Puisque a n'a pas une factorisation dans quelques irréductibles, alors soit b ou c n'en pas une non plus. Supposons que b n'est pas le produit de quelques irréductibles. Par la définition de a, on a que $N(b) \geq N(a)$. D'autre côté, $b|a$, donc $N(b) \leq N(a)$. Par conséquent, $N(a) = N(b)$. La proposition 3.16(b) implique alors que $b \sim a$. Ceci est impossible car on a supposé que c n'est pas inversible. On est arrivé à une contradiction. Donc, il faut que chaque $a \in A \setminus (A^\times \cup \{0\})$ soit le produit de quelques irréductibles.

Finalement, on montre que la factorisation dans irréductibles est unique. En effet, soit $a = p_1 \cdots p_m = q_1 \cdots q_n$ deux factorisations d'un $a \in A \setminus (A^\times \cup \{0\})$. Sans perte de généralité, on suppose que $m \geq n$. On a que $q_1 | p_1 \cdots p_m$. Chaque anneau euclidien est de Bezout, donc q_1 est premier. Il existe donc $j_1 \in \{1, \ldots, m\}$ tel que $q_1 | p_{j_1}$. En permutant les p_i, on peut supposer que $j_1 = 1$. On sait que p_1 est irréductible, donc ses seuls facteurs sont inversibles ou associés à p_1. Puisque q_1 n'est pas inversible par définition, il faut que $q_1 \sim p_1$, c'est-à-dire $p_1 = u_1 q_1$ pour un $u_1 \in A^\times$. On trouve alors que $q_2 \cdots q_n = u_1 p_2 \cdots p_m$. En particulier, $q_2 | p_2 \cdots p_m$ et, en répétant l'argument précédent, on trouve qu'il existe $j_2 \in \{2, \ldots, m\}$ et $u_2 \in A^\times$ tels que $p_{j_2} = u_2 q_2$. En permutant les p_i, on peut supposer que $j_2 = 2$. On déduit

que $q_3 \cdots q_n = u_1 u_2 p_3 \cdots p_m$.

En itérant l'argument ci-dessus, on trouve qu'on peut permuter les p_i de sorte qu'il existe $u_1, \ldots, u_n \in A^\times$ tels que $p_j = u_j q_j$ pour $j \in \{1, \ldots, n\}$. En particulier, $1 = u_1 \cdots u_n p_{n+1} \cdots p_m$. Si $m > n$, cette relation impliquerait que p_m est inversible, ce qui est absurde. On conclut alors que $m = n$. Ceci termine la démonstration. □

L'arithmétique des anneaux factoriels est similaire à celle des entiers. D'abord, on a besoin d'une définition :

Définition 3.21. Soit A un anneau factoriel. Si p est irréductible et $a \in A \setminus \{0\}$, on définit

$$\nu_p(a) := \max\{j \in \mathbb{Z}_{\geq 0} : p^j | a\}.$$

On appelle $\nu_p(a)$ la **valuation p-adique** de a.

On ramasse les propriétés les plus important d'un anneau factoriel au résultat suivant :

Théorème 3.22. *Soit A un anneau factoriel.*

(a) (lemme d'Euclid) Chaque élément irréductible de A est aussi premier.

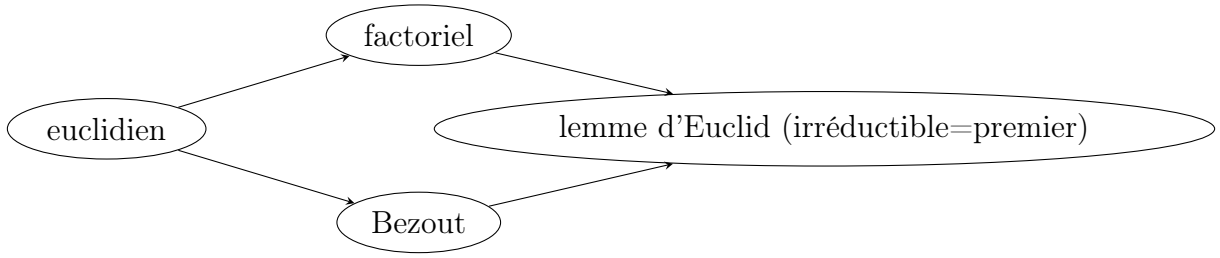
(b) Si $a, b \in A \setminus \{0\}$, alors $a|b$ s-si $\nu_p(a) \leq \nu_p(b)$ pour chaque irréductible p.

(c) La relation d'association partagent les irréductibles de A dans quelques classes d'équivalences. Soit $\mathcal{P}$ un système complet de représentants de ces classes d'équivalence. Un pgcd de a et de b est le produit $\prod_{p \in \mathcal{P}} p^{\min\{\nu_p(a), \nu_p(b)\}}$.

Démonstration. (a) Soit p un élément irréductible de A. Supposons que $p|ab$, pour que $ab = kp$ pour un $k \in A$. Si $a = q_1 \cdots q_m$ et $b = q_{m+1} \cdots q_{m+n}$ sont les factorisation de a et de b en irréductibles, alors $q_1 \cdots q_{m+n} = kp$. Il faut alors que p soit associés avec un q_i. Si $i \leq m$, alors $p|a$; sinon, alors $p|b$. Ceci montre la primalité de p.

On laisse la preuve des parties (b) et (c) comme un exercice. □

Une aide-mémoire de ce qu'on a discuté à ce chapitre est donné dans le diagramme ci-dessous :



3.5 Exercices

EXERCICE 3.1. Montrez que dans l'anneau $\mathbb{Z}[\sqrt{-5}]$, on a que $\text{pgcd}(3+3\sqrt{-5}, 3-3\sqrt{-5}) = \emptyset$.

EXERCICE 3.2. Soient L un corps et K un sous-corps de L.

Soit aussi $\alpha \in L$ un **nombre algébrique sur** K, c'est-à-dire un nombre qui est la racine d'un polynôme non-zéro sur K. Il existe alors $f(x) \in K[x] \setminus \{0\}$ de degré minimal tel que $f(\alpha) = 0$. On peut aussi normaliser $f(x)$ pour que son coefficient en tête soit 1 (i.e. $f(x)$ est unitaire). On appelle ce polynôme $f(x)$ le polynôme **minimal** de α.

Rappelez les définitions de $K[\alpha]$ et de $K(\alpha)$ dans l'exercice 2.11.

(a) Montrez que $f(x)$ est un élément irréductible de $K[x]$. [*Indice :* voir l'exercice 2.2.]

(b) Si $g(x) \in K[x]$, alors montrez que $g(\alpha) = 0$ s-si $f(x)|g(x)$. En particulier, $f(x)$ est défini uniquement. [*Indice :* division euclidienne.]

(c) Si $g(x) \in K[x]$ est tel que $g(\alpha) \neq 0$, alors montrez que $f(x)$ et $g(x)$ sont co-premiers. Déduisez qu'il existe $a(x), b(x) \in K[x]$ tels que $a(x)f(x) + b(x)g(x) = 1$.

(d) Montrez que $K(\alpha) = K[\alpha]$.

EXERCICE 3.3. Soit K, L, α comme ci-dessus. Montrez que si $P(x)$ est un polynôme irréductible et unitaire de $K[x]$ ayant α comme racine, alors $P(x)$ est **le** polynôme minimal de α.

EXERCICE 3.4. Soient L un corps et K un sous-corps de L.

(a) Soit M est un sous-corps de L contenant K.

  (i) Montrez que M est un espace vectoriel[3] sur K.

  (ii) Si la dimension de M est finie, alors montrez que chaque élément m de M est algébrique sur K. [*Indice :* si d est la dimension, alors les éléments/vecteurs $1, m, m^2, \ldots, m^d$ sont linéairement dépendants sur K.]

(b) Soit $\alpha \in K$ un élément algébrique et $f(x) \in K[x]$ son polynôme minimal. Si $n = \deg(f)$, alors montrez que

$$K[\alpha] = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_0, c_1, \ldots, c_{n-1} \in K\},$$

et que chaque $\beta \in K[\alpha]$ a une représentation unique comme $\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$. Déduisez que $K[\alpha]$ est un espace vectoriel de dimension n sur K.

(c) Soient $\alpha, \beta \in L$ deux nombres algébriques sur K. Montrez que $K[\alpha, \beta] = (K[\alpha])[\beta]$ et déduisez que $K[\alpha, \beta]$ est un espace vectoriel de dimension finie sur K.

(d) Montrez que l'ensemble $\{\alpha \in L : \alpha \text{ algébrique sur } K\}$ est un sous-corps de L. [*Indice :* voir exercice 3.2(d).]

(e) Si $\mathbb{A} \subset \mathbb{C}$ est l'ensemble des nombres algébriques sur $\mathbb{Q}$, montrez que $\mathbb{C} \setminus \mathbb{A}$ est non-vide.

EXERCICE 3.5. Soit un nombre sans-carré $D \in \mathbb{Z} \setminus \{0, 1\}$. Définissons ω et $\mathcal{O}$ comme on l'a fait à l'exercice 2.12. Soit, aussi, l'application $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Z}$, définie par $N(a + b\sqrt{D}) = a^2 - Db^2$. (Voir l'exercice 1.1 pour quelques propriétés utiles de cette application.)

3. Rappelez qu'un ensemble V est un espace vectoriel sur un corps K si : (a) il existe une loi de composition interne $+$ qui rend V un groupe abeline ; (b) il existe une action à gauche de K à V telle que $1 \cdot v = v$, $\ell \cdot (\ell' \cdot v) = (\ell \cdot \ell') \cdot v$, $(\ell + \ell') \cdot v = \ell \cdot v + \ell' \cdot v$, et $\ell \cdot (v + w) = \ell \cdot v + \ell \cdot w$, pour tous $\ell, \ell' \in K$ et $v, w \in V$.

(a) (ex. 8(a), p. 278) Montrez que si $D \in \{-1, -2, -3, -7, -11\}$, alors $\mathcal{O}$ est un anneau euclidien et un stathme euclidien est donné par la restriction de N sur $\mathcal{O}$. [*Indice* : Quand $D \equiv 1 \pmod 4$, alors montrez que $\mathcal{O} = \{a/2 + b\sqrt{D}/2 : a, b \in \mathbb{Z},\ a \equiv b \pmod 2\}$.]

(b) Trouvez $\alpha \in \mathbb{Z}[i]$ tel que $(3 + 5i, 1 + 3i) = (\alpha)$.

Exercice 3.6.

(a) Vérifiez que les nombres $5 + \sqrt{2}$, $2 - \sqrt{2}$, $11 - 7\sqrt{2}$ et $2 + \sqrt{2}$ sont irréductibles dans $\mathbb{Z}[\sqrt{2}]$.

(b) Vérifiez que
$$(5 + \sqrt{2})(2 - \sqrt{2}) = (11 - 7\sqrt{2})(2 + \sqrt{2})$$
et expliquez pourquoi ce fait ne contredit pas la factorisation unique dans $\mathbb{Z}[\sqrt{2}]$.

(c) (ex. 9, p. 278) Montrez que $\mathbb{Z}[\sqrt{2}]$ est un anneau euclidien par rapport au stathme $M(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Exercice 3.7. Soit $A = \mathbb{Z}[\sqrt{-n}] := \{a + b\sqrt{-n} : a, b \in \mathbb{Z}\}$, où n est un entier sans carré plus grand que 3.

(a) Montrez que les éléments 2, $\sqrt{-n}$ et $1 + \sqrt{-n}$ sont irréductibles dans A.

(b) Prouvez que A nest pas un anneau factoriel. Concluez que l'anneau des entiers quadratique $\mathcal{O}$, définit au Problème 1 au-dessus, n'est pas factoriel quand $D \equiv 2, 3 \pmod 4$, $D < -3$ (alors il n'est pas un anneau euclidien ni un anneau principal) [*Indication :* Montrez que le nombre 2 n'est pas premier dans A.]

(c) Donnez un exemple d'un idéal de A qui n'est pas principal. [*Indication :* Considérez un idéal maximal qui contient (2).]

Exercice 3.8 (ex. 4, p. 301). Soit F un corps fini. Prouvez que $F[x]$ contient un nombre infini d'éléments premiers et non-associés $p_1(x), p_2(x), \ldots$

Exercice 3.9. Soit A un anneau euclidien muni d'un stathme euclidien $N : A \to \mathbb{Z}_{\geq 0}$. Si $n_0 = \min\{N(a) : a \neq 0\}$, alors montrez que $N(a) = n_0$ s-si $a \in A^\times$.

Chapitre 4

Idéaux

4.1 Le problème de la factorisation unique

On a vu que dans quelques anneaux le théorème fondamental de l'arithmétique est violé. Par exemple, dans $\mathbb{Z}[\sqrt{-5}]$ on a les factorisation $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, où $2, 3, 1 \pm \sqrt{-5}$ sont d'irréductibles non-associés. Kummer avait une idée pour réparer ce problème. Supposons qu'il existait quelques *nombres idéaux* $\alpha, \beta, \gamma, \delta$ tels que

$$2 = \alpha\beta, \quad 3 = \gamma\delta, \quad 1 + \sqrt{-5} = \alpha\gamma, \quad 1 - \sqrt{-5} = \beta\delta.$$

Donc

$$2 \cdot 3 = \alpha\beta\gamma\delta = \alpha\gamma\beta\delta = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Bien sûr, ces nombres ne peuvent pas être construits dans $\mathbb{Z}[\sqrt{-5}]$, car 2,3 et $1 \pm \sqrt{-5}$ sont d'irréductibles de cet anneau. On les construits comme suivant : étant donnés $a_1, \ldots, a_n \in \mathbb{Z}[\sqrt{-5}]$, on considère l'ensemble $(a_1, \ldots, a_n)$, défini comme l'ensemble de toutes les combinaisons linéaires sur $\mathbb{Z}[\sqrt{-5}]$ de $a_1, \ldots, a_n$. C'est-à-dire,

$$(a_1, \ldots, a_n) := \{\lambda_1 a_1 + \cdots + \lambda_n a_n : \lambda_j \in \mathbb{Z}[\sqrt{-5}] \ \forall j\}.$$

On appelle $(a_1, \ldots, a_n)$ **l'idéal engendré par** $a_1, \ldots, a_n$, et on identifie a et (a).

La motivation pour cette définition provient du fait que si on remplace $\mathbb{Z}[\sqrt{-5}]$ par un an anneau de Bezout A, alors $(a_1, \ldots, a_n) = (d)$, où d est un pgcd de $a_1, \ldots, a_n$. En effet, d divise tous les combinaisons linéaires de $a_1, \ldots, a_n$, pour que $(a_1, \ldots, a_n) \subset (d)$. Vice verse, d est une combinaison linéaire de $a_1, \ldots, a_n$, alors $d \in (a_1, \ldots, a_n)$ et donc $(d) \subset (a_1, \ldots, a_n)$.

La discussion de la paragraphe précédente implique qu'on peut penser à $(a_1, \ldots, a_n)$ comme 'un facteur commun' de $a_1, \ldots, a_n$. Pour formaliser cette intuition, il faut définir quel est le produit de $(a_1, \ldots, a_m)$ et $(b_1, \ldots, b_n)$. On le définit tout simplement comme étant l'idéal engendré par les produits $a_i b_j$, c'est-à-dire

$$(a_1, \ldots, a_m) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_1 b_n, a_2 b_1, \ldots, a_2 b_n, \ldots, a_m b_1, \ldots, a_m b_n).$$

Avec les définitions ci-dessus, on a que

$$(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (6, 4, 2 - 2\sqrt{-5}, 2 + 2\sqrt{-5}).$$

L'ensemble de combinaisons linéaires de a et de b est le même que celui de combinaisons linéaires de $a-b$ et de b. Donc

$$\begin{aligned}(6,4,2-2\sqrt{-5},2+2\sqrt{-5}) &= (6-4,4,2-2\sqrt{-5},2+2\sqrt{-5})\\ &= (2,4,2-2\sqrt{-5},2+2\sqrt{-5}).\end{aligned}$$

Vu que 4 et $2\pm 2\sqrt{-5}$ sont de multiples de 2 dans $\mathbb{Z}[\sqrt{-5}]$ (donc, "linéairement dependent" de 2), on déduit que $(2,4,2-2\sqrt{-5},2+2\sqrt{-5})=(2)$. On a alors montré que

$$(2,1+\sqrt{-5})(2,1-\sqrt{-5})=(2).$$

De même, on peut montrer que

$$\begin{aligned}(3,1+\sqrt{-5})(3,1-\sqrt{-5}) &= (9,6,3-3\sqrt{-5},3+3\sqrt{-5})\\ &= (3,6,-3\sqrt{-5},3+3\sqrt{-5},6)\\ &= (3).\end{aligned}$$

On a également que

$$\begin{aligned}(2,1+\sqrt{5})(3,1+\sqrt{5}) &= (3+3\sqrt{-5},2+2\sqrt{-5},6,(1+\sqrt{-5})^2)\\ &= (3+3\sqrt{-5}-2+2\sqrt{-5},2+2\sqrt{-5},6,(1+\sqrt{-5})^2)\\ &= (1+\sqrt{-5},2+2\sqrt{-5},6,(1+\sqrt{-5})^2).\end{aligned}$$

Les éléments $2+2\sqrt{-5}=2(1+\sqrt{-5})$, $6=(1+\sqrt{-5})(1-\sqrt{-5})$ et $(1+\sqrt{-5})^2$ sont de multiples de $1+\sqrt{-5}$, donc

$$(2,1+\sqrt{5})(3,1+\sqrt{5})=(1+\sqrt{-5}).$$

En prenant les conjugués, on trouve aussi que

$$(2,1-\sqrt{5})(3,1-\sqrt{5})=(1-\sqrt{-5}).$$

On a trouvé alors les factorisations affirmées de 2,3 et $1\pm\sqrt{-5}$, mais quand on les voit comme idéaux.

4.2 Définition et génération d'idéaux

Définition 4.1. Soit A un anneau et $I\subset A$. On dit que I est un **idéal** de A si :

- I est un sous-groupe additif de A (c'est-à-dire $I\neq\emptyset$ et $i-j\in I$ pour tous $i,j\in I$) ;
- pour tout $a\in A$ et pour tout $i\in I$, on a que $ai, ia\in I$.

Remarque 4.2. Si I est un idéal de l'anneau A, alors I est un sous-anneau de A. L'inverse n'est pas toujours vrai. Par exemple, $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$ mais il n'est pas un idéal de $\mathbb{C}$.

Exemple 4.3. Dans chaque anneaux A, les ensembles $\{0\}$ et A sont toujours d'idéaux.

Définition 4.4. Soit A un anneau et I un idéal de A. On dit que I est **non-trivial** si $I \neq \{0\}$; on dit que I est **propre** si $I \neq A$.

Théorème 4.5.

(a) Soit A un anneau unitaire et I un idéal de A. Alors, $I = A$ s-si $1 \in I$, s-si $I \cap A^\times \neq \emptyset$.

(b) Soit A un anneau commutatif, unitaire et non-trivial. Alors, A est un corps s-si $\{0\}$ et A sont ses seuls idéaux.

Démonstration. (a) Si $I = A$, alors évidemment $1 \in A$. De plus, si $1 \in A$, alors évidemment $I \cap A^\times \neq \emptyset$. Il reste à montrer que s'il existe $u \in I \cap A^\times$, alors $A = I$. En effet, si c'est le cas, alors pour tout $a \in A$ on a que $a = (au^{-1})u \in I$ comme un multiple de u. Ceci termine la démonstration.

(b) Supposons que A est un corps et que I est un idéal de A. Si $I \neq \{0\}$, alors il existe $a \in I \setminus \{0\}$. Mais un tel a est inversible car on est dans un corps, donc $I = A$ par la partie (a).

Vice versa, supposons que les seuls idéaux de A sont les ensembles $\{0\}$ et A. Soit $a \in A \setminus \{0\}$. Puisque $(a) \neq \{0\}$, il faut que $(a) = A$. En particulier, $1 \in (a)$. Mais, ceci implique que $1 = ab$ pour un $b \in A$, c'est-à-dire a est inversible. On a montré alors que A est un corps. □

Exemple 4.6. Si $A = \mathbb{Z}$, alors les ensembles $n\mathbb{Z}$, où n est un entier non-négatif, sont d'idéaux de $\mathbb{Z}$.

Vice versa, soit I un idéal de $\mathbb{Z}$. On affirme que $I = n\mathbb{Z}$ pour un $n \in \mathbb{Z}_{\geq 0}$. Si $I = \{0\}$, alors évidemment on a que $I = 0\mathbb{Z}$. Supposons, maintenant, que $I \neq \{0\}$.

Soit $n = \min(\mathbb{Z}_{\geq 1} \cap I)$. On montrera que $I = n\mathbb{Z}$. Evidemment, $n\mathbb{Z} \subset I$: par définition, I contient nq pour chaque $q \in \mathbb{Z}$. Réciproquement, soit $m \in \mathbb{Z}$. Il existe $q, r \in \mathbb{Z}$ tels que $m = qn + r$ et $0 \leq r < n$. On a que $qn, m \in I$, donc $r = m - qn \in I$. Mais le plus petit entier non-négatif contenu dans I est n. Il faut alors que $r = 0$, c'est-à-dire $m = qn \in n\mathbb{Z}$.

Une façon générale de construire d'idéaux et en utilisant de générateurs :

Lemme 4.7. *Soit A un anneau.*

(a) Si $\mathcal{I}$ est un ensemble non-vide d'idéaux de A, alors leur intersection $\cap_{I \in \mathcal{I}} I$ est aussi un idéal de A.

(b) Si $S \subset A$, alors il existe un idéal I de A qui contient S et qui est minimal, dans le sens que si J est un autre idéal de A contenant S, alors $I \subset J$.

(c) Si A est **unitaire***, alors l'idéal I de la partie (b) est donné par*

$$I = \{a_1 s_1 b_1 + \cdots + a_n s_n b_n : a_j, b_j \in A, s_j \in S \ (1 \leq j \leq n), n \in \mathbb{Z}_{\geq 0}\},$$

avec la convention qu'une somme vide est zéro. Si, de plus, A est **commutatif***, alors*

$$I = \{a_1 s_1 + \cdots + a_n s_n : a_j \in A, s_j \in S \ (1 \leq j \leq n), n \in \mathbb{Z}_{\geq 0}\}.$$

Démonstration. (a) Exercice.

(b) Soit $\mathcal{I}$ l'ensemble de tous les idéaux de A contenant S. Puisque A est un tel idéal, alors $\mathcal{I} \neq \emptyset$. L'idéal cherché est $I := \cap_{J \in \mathcal{I}} J$.

(c) Soit

$$I' := \{a_1 s_1 b_1 + \cdots + a_n s_n b_n : a_j, b_j \in A, s_j \in S \ (1 \leq j \leq n), n \in \mathbb{Z}_{\geq 0}\}.$$

Pour montrer que $I' = I$, alors on montrera que I' est un idéal contenant S et que I' est minimal (dans le même sens que I l'est). Ceci conclut la démonstration, car la minimalité de I implique que $I \subset I'$, et la minimalité de I' implique que $I' \subset I$.

Évidemment, $I' \supset S$: en prenant $n = 1$ et $a_1 = b_1 = 1_A$, on voit que $s_1 = 1 \cdot s_1 \cdot 1 \in I'$ pour n'importe quel $s_1 \in S$.

Or, on montre que I' est un idéal. Par construction, il contient 0 et il est fermé sous la soustraction :

$$\begin{aligned}(a_1 s_1 b_1 + \cdots + a_n s_n b_n) - (a_1' s_1' b_1' + \cdots + a_{n'} s_{n'} b_{n'}) \\ = a_1 s_1 b_1 + \cdots + a_n s_n b_n + (-a_1) s_1 b_1 + \cdots + (-a_{n'}) s_{n'} b_{n'} \in I'.\end{aligned}$$

De plus, c'est evident que si $i = a_1 s_1 b_1 + \cdots + a_n s_n b_n \in I'$ et $a \in A$, alors $ai, ia \in I'$. Ceci montre notre affirmation que I' est un idéal.

Finalement, on montre la minimalité de I'. Soit J un idéal de A contenant S. Alors, pour tous $s_1, \ldots, s_n \in S$, on a que $s_1, \ldots, s_n \in J$. Mais J est un idéal, donc si $a_1, \ldots, a_n \in A$, alors $a_1 s_1, \ldots, a_n s_n \in J$. En utilisant encore une fois le fait que J est un idéal, on trouve qu'on peut multiplier les éléments $a_j s_j$ en droit par n'importe quels $b_j \in A$ et trouver de nouveaux éléments de J. Alors, $a_1 s_1 b_1, \ldots, a_n s_n b_n \in J$ pour tous $b_1, \ldots, b_n \in A$. Finalement, on sait que J est fermé sous l'addition comme un idéal, donc $a_1 s_1 b_1 + \cdots + a_n s_n b_n \in J$. Ceci montre que $I' \subset J$, en complétant la démonstration que $I = I'$.

Il reste à montrer que quand A est commutatif et unitaire, alors I est égal à

$$I'' = \{a_1 s_1 + \cdots + a_n s_n : a_j \in A, s_j \in S \ (1 \leq j \leq n), n \in \mathbb{Z}_{\geq 0}\}.$$

Il suffit de montrer que $I'' = I'$. Vu que $a_1 s_1 b_1 = (a_1 b_1) s_1$ par commutativité, on a que $I' \subset I''$. Finalement, vu que $a_1 s_1 = a_1 \cdot s_1 \cdot 1$, on a également que $I'' \subset I'$. Ceci termine la démonstration du lemme. □

Définition 4.8. Soit A un anneau.

- Si $S \subset A$, alors on définit (S) comme étant le plus petit idéal de A contenant S, dans le sens de la partie (b) du lemme 4.7. On appelle (S) l'idéal **engendré** par S.
- Si $S = \{s_1, \ldots, s_n\}$ est un sous-ensemble fini de A, alors on écrit $(s_1, \ldots, s_n)$ plutôt que $(\{s_1, \ldots, s_n\})$.
- Si I est un idéal de A et $S \subset A$ sont tels que $I = (S)$, alors on dit que S **engendre** I, et on appelle S un ensemble de **générateurs** de I.
- Si I est un idéal de A engendré par un ensemble fini de A, alors on dit que I est **de type fini**. Les anneaux dont tous les idéaux sont de type fini sont appelés **noetheriens**.

- Si I est un idéal de A engendré par un seul élément de A, alors on dit que I est **principal**. Les anneaux *intègres* dont tous les idéaux sont principaux sont appelés **principaux**.

Le lemme suivant justifie pourquoi dans la section 4.1 on a identifie un élément d'un anneau avec l'idéal qu'il engendre.

Lemme 4.9. *Soit A un anneau intègre. Alors $a \sim b$ s-si $(a) = (b)$.*

Démonstration. On a que $(a) \subset (b)$ s-si $a \in (b)$, s-si $b|a$. Par consèquent, le lemme découle du lemme 3.5. □

On conclut cette section en montrant que la notion d'idéaux rend rigoureux le discours au début du chapitre.

Définition 4.10. Soit A un anneau, et soient I, J deux idéaux de A. On définit IJ comme étant l'idéal de A engendré par l'ensemble $\{ij : i \in I, j \in J\}$.

Lemme 4.11. *Soit A un anneau commutatif et unitaire. Pour tous $a_1, \ldots, a_m, b_1, \ldots, b_n \in A$, on a que*

$$(a_1, \ldots, a_m)(b_1, \ldots, b_n) = (a_1b_1, \ldots, a_1b_n, a_2b_1, \ldots, a_2b_n, \ldots, a_mb_1, \ldots, a_mb_n).$$

Démonstration. Soit $I = (a_1, \ldots, a_m)$, $J = (b_1, \ldots, b_n)$ et $K = (\{a_ib_j : 1 \leq i \leq m,\ 1 \leq j \leq n\})$. Puisque $a_i \in I$ pour tout i, et $b_j \in J$ pour tout j, on a que $a_ib_j \in IJ$, donc l'idéal engendré par les produits a_ib_j est contenu dans IJ, c'est-à-dire $K \subset IJ$.

Pour montrer que $IJ \subset K$, on utilise le lemme 4.7 qui dit que

$$I = \{x_1a_1 + \cdots + x_ma_m : x_1, \ldots, x_m \in A\} \quad \text{et} \quad J = \{y_1b_1 + \cdots + y_nb_n : y_1, \ldots, y_m \in A\}.$$

Puisque

$$(x_1a_1 + \cdots + x_ma_m)(y_1b_1 + \cdots + y_nb_n) = \sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} x_iy_ja_ib_j$$

par commutativité, on trouve que $IJ \subset K$, ce qui termine la démonstration. □

4.3 Les anneaux d'Euclide et de Bezout revisités

L'exemple (4.6) montre que $\mathbb{Z}$ est un anneau principal. Ceci est une propriété de tous les anneaux euclidiens :

Théorème 4.12. *Chaque anneau euclidien est principal.*

Démonstration. Soit A un anneau euclidien. En particulier, A est intègre. Soit I un idéal de A. On affirme que $I = (a)$ pour un $a \in A$.

Si $I = \{0\}$, alors évidemment on a que $I = (0)$.

Supposons, maintenant, que $I \neq \{0\}$. Soit $N : A \to \mathbb{Z}_{\geq 0}$ un préstathme euclidien. Il existe alors $a \in I \setminus \{0\}$ tel que $N(a) = \min\{N(i) : i \in I \setminus \{0\}$. On montrera que $I = (a)$. Evidemment, $(a) \subset I$, car $a \in I$. Réciproquement, soit $i \in I$. Il existe alors $q, r \in A$ tels que $i = qa + r$ et $N(r) < N(a)$. Puisque I est un idéal et $i, a \in I$, on a que $r = i - qa \in I$. Mais $N(r) < N(a)$, et la minimalité de $N(a)$ entre les valeurs du préstathe aux éléments non-zéro de A implique que $r = 0$. On a montré alors que $i = qa \in (a)$. Ceci termine la démonstration. □

On peut aussi caractèriser les anneaux de Bezout en utilisant la notion d'idéaux :

Lemme 4.13. *Soit A un anneau commutatif et unitaire, et soient $a, b \in A$ avec $b \neq 0$, et soit $d \in A$.*

On a que $(a, b) = (d)$ s-si $d \in \text{pgcd}(a, b)$ et il existe $x, y \in A$ tels que $d = ax + by$.

Démonstration. Supposons que $(a, b) = (d)$. Le lemme 4.7(c) implique tout de suite que $d = ax + by$ pour quelques $x, y \in A$. Il reste à montrer que $d \in \text{pgcd}(a, b)$.

Puisque $a \in (a, b) = (d)$, il existe $c \in A$ tel que $a = cd$. En particulier, $d|a$. De manière similaire, on trouve que $d|b$ car $d \in (a, b)$. Alors d est un commun diviseur de a et b. Si e est un autre commun diviseur de a et b, alors e divise $ka + \ell b$ pour tous $k, \ell \in A$. Ceci implique que $ka + \ell b \in (e)$ pour tous $k, \ell \in A$, c'est-à-dire que $(a, b) \subset (e)$. Puisque $(d) = (a, b)$, on trouve alors que $d \in (e)$. Ceci montre que $e|d$, comme il fallait démontrer.

Réciproquement, supposons que $d \in \text{pgcd}(a, b)$ et qu'il existe $x, y \in A$ tels que $d = ax + by$. On montre que $(a, b) = (d)$. Tout d'abord, puisque $d|a$ et $d|b$, alors d divise chaque combinaison linéaire de a et de b, ce qui implique que $(a.b) \subset (d)$. Finalement, puisque $d = ax + by$, on a que $d \in (a, b)$. Par conséquent, $(d) \in (a, b)$. Ceci montre que $(a, b) = (d)$ et termine la preuve du lemme. □

Théorème 4.14. *Soit A un intègre. Alors A est un anneau de Bezout s-si chaque idéal de type fini de A est principal.*

En particulier, si A est intègre et noetherien, alors il est un anneau de Bezout s-si il est principal.

Démonstration. Supposons d'abord que chaque idéal de type fini de A est principal. Si $a, b \in A$ avec $b \neq 0$, alors il existe $d \in A \setminus \{0\}$ tel que $(a, b) = (d)$. Le lemme 4.13 implique alors que $d \in \text{pgcd}(a, b)$ et que d est une combinaison linéaire de a et de b. Ceci montrer que A est un anneau de Bezout (on sait déjà que A est intègre, car il est principal).

Supposons maintenant que A est un anneau de Bezout (en particulier, A est intègre). Soit I un idéal de type fini. On montre par induction sur le nombre de générateurs non-zéros de I que I est principal.

Si I est engendré par l'ensemble vide, alors $I = \{0\} = (0)$. De plus, si I est engendré par juste un seul élément $a \neq 0$, alors $I = (a)$ par définition.

Supposons, maintenant, que le résultat est vrai quand I est engendré par $n \geq 1$ éléments non-zéros, et considérons l'idéal $(a_1, \ldots, a_{n+1})$, où $a_j \neq 0$ pour tout j. Puisque A est un anneau de Bezout, le corollaire il existe $d \in \text{pgcd}(a_n, a_{n+1})$. De plus, d peut s'écrire comme une combinaison linéaire de a_n et de a_{n+1}. Donc, le lemme 4.13 implique que $(a_n, a_{n+1}) = (d)$.

On en déduit que $(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_{n-1}, d)$. L'hypothèse d'induction nous dit alors que $(a_1, \ldots, a_{n+1})$ est principal. Ceci conclut l'étape inductive, et donc la démonstration. □

Corollaire 4.15. *Chaque anneau principal est un anneau de Bezout.*

4.4 L'arithmétique modulaire généralisée

Supposons que A est un anneau et $S \subset A$. On veut construire un nouveau anneau en utilisant les éléments de A en imposant entre eux la condition que tous les éléments de S deviennent 0. Soit $B =$ " A/S " ce nouveau anneau hypothétique. On a que $s = 0_B$ dans B. Plus généralement, si $i = 0_B$ pour un $i \in A$, on remarque qu'il faut aussi que $ai = a \cdot 0_B = 0_B$ et $ia = 0_B \cdot a = 0_B$ pour tout $a \in A$. De plus, si $i = 0_B$ et $i' = 0_B$, alors il faut que $i - i' = 0_B$ aussi. On voit alors que l'ensemble $I := \{i \in A : i = 0_A\}$ est un idéal de A contenant S. En fait, si on veut construire B en imposant l'ensemble de relations le plus petit possible, alors $I = (S)$.

On formalise maintenant l'argument de la paragraphe précédente. Soit A un anneau et I un idéal de A. Étant donnés $a, b \in A$, on définit la relation

$$a \equiv b \,(\mathrm{mod}\, I) \quad \iff \quad a - b \in I,$$

et si c'est le cas, on dit que a **et** b **sont équivalents modulo** I. Puisque I est un sous-groupe additif de A, alors on la théorie des groupes implique que cette relation est une relation d'équivalence. Les classes d'équivalences sont les ensembles

$$a + I := \{a + i : i \in I\},$$

qu'on dénote parfois par $a \,(\mathrm{mod}\, I)$ ou même par $\overline{a}$, si I est censé être connu. Finalement, on dénote par A/I l'ensemble de toutes les classes d'équivalences mod I, c'est-à-dire

$$A/I := \{a \,(\mathrm{mod}\, I) : a \in A\},$$

appelé l'**anneau-quotient**. Le théorème suivant justifie le nom :

Théorème 4.16. *Si A est un anneau et I est un idéal de A, alors A/I est un anneau par rapport aux opérations*

$$\overline{a} + \overline{b} := \overline{a + b} \quad \textit{et} \quad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Si A est commutatif, alors A/I l'est. De plus, si A est unitaire, alors A/I l'est et $1_{A/I} = \overline{1_A}$.

Démonstration. Le fait que l'addition est bien définie et qu'elle rende A/I un groupe additif abélien est un théorème de la théorie des groupes.

Or, étudions la multiplication. On montre d'abord qu'elle est bien définie : si $\overline{a_1} = \overline{a_2}$ et $\overline{b_1} = \overline{b_2}$, alors on veut montrer que $\overline{a_1 b_1} = \overline{a_2 b_2}$. En effet, on a que $i := a_1 - a_2 \in I$ et que $j := b_1 - b_2 \in I$. Donc

$$a_2 b_2 - = (a_1 + i)(b_1 + j) - a_1 b_1 = (a_1 b_1 + a_1 j + i b_1 + ij) - a_1 b_1 = a_1 j + i b_1 + ij \in I,$$

car I est un idéal et $i, j \in I$.

L'associativité et l'additivité de deux opérations sur A/I sont un corollaire direct des mêmes propriétés sur A (il faut juste "mettre de barres" sur les éléments).

Les deux dernières affirmations du théorème sont évidentes. □

Evidemment, le notion de l'anneau-quotient généralise les anneaux $\mathbb{Z}/n\mathbb{Z}$, où $A = \mathbb{Z}$ et $I = (n) = n\mathbb{Z}$.

Exemple 4.17. Soit $A = \mathbb{Z}[i]$, $I = (3)$ et $J = (1 + i)$. On veut comprendre A/I et A/J.

On a $a + bi \equiv c + di \,(\mathrm{mod}\,(3))$ s-si $(a + bi) - (c + di) = 3(k + \ell i)$ pour quelques $k, \ell \in \mathbb{Z}$, s-si $a - c = 3k$ et $b - d = 3\ell$ pour quelques $k, \ell \in \mathbb{Z}$, s-si $a \equiv c \,(\mathrm{mod}\, 3)$ et $b \equiv d \,(\mathrm{mod}\, 3)$. Donc, l'ensemble $\{a + bi : 0 \leq a, b \leq 2\}$ est un système complet de représentants de résidus mod I. Cependant, on affirme que

$$Z[i]/(3) \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

comme anneaux. En effet, puisque 3 est premier dans $\mathbb{Z}[i]$, on voit que $\mathbb{Z}[i]/(3)$ est intègre (si $\overline{a}\overline{b} = \overline{0}$, il faut que $3|ab$; donc, soit $3|a$ ou $3|b$). Par contre, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ n'est pas intègre : $(\overline{0}, \overline{1})(\overline{1}, \overline{0}) = (\overline{0}, \overline{0})$.

Le quotient A/J est plus compliqué à analyser. D'abord, on cherche une representation de J. On a que $a+bi \in J$ s-si $a+bi = (m+ni)(1+i) = m \cdot (1+i)+n \cdot (-1+i)$. On voit alors que J consiste de toutes le combinaisons linéaires sur $\mathbb{Z}$ de vecteurs/nombres complexes $1+i$ et $-1+i$. En faisant un dessin, on peut voir que cet ensemble forme un réseau tourné par 45 degrés. En fait, ce réseau peut être obtenu par translations du carré dont les sommets sont $0, 1+i, -1+i, 2i$. On voit alors que l'ensemble $\{0, 1\}$ est un système complet de représentants de résidus mod J. Par conséquent,

$$A/J \cong \mathbb{Z}/2\mathbb{Z}.$$

Exemple 4.18. Soit $A = K[x]$, où K est un corps. Si $f(x) \in K[x] \setminus \{0\}$ a degré n, alors on affirme que l'ensemble $R := \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\}$ de polynômes de degré $< n$ est un ensemble de représentants complet de résidus mod $f(x)$.

En effet, si $g(x) \in K[x]$, alors on sait qu'il existe $q(x), r(x) \in K[x]$ tels que $g(x) = f(x)q(x) + r(x)$ et $\deg(r) < \deg(f) = n$. Donc, $g(x) \equiv r(x) \,(\mathrm{mod}\,(f(x)))$. Observons que $r(x) \in R$.

Pour finir la démonstration de notre affirmation poru R, il faut montrer que si $g(x) \equiv s(x) \,(\mathrm{mod}\,(f(x)))$ pour un autre polynôme $s(x) \in R$, alors $s(x) = r(x)$. En effet, on a que $s(x) \equiv r(x) \,(\mathrm{mod}\,(f(x)))$ et, par conséquent, $r(x) - s(x)$ est un multiple de $f(x)$. Cependant, on a que $\deg(r - s) < \deg(f)$, donc la seule façon dans laquelle $r(x) - s(x)$ peut être un multiple de $f(x)$ est si $r(x) - s(x) = 0$. Ceci conclut la démonstration.

On a aussi une vaste généralisation du théorème des restes chinois.

Définition 4.19. Si I et J sont deux idéaux d'un anneau A, alors on les appelle **comaximaux** si $I + J = A$, où on utilise la notation $I + J =: \{i + j : i \in I, j \in J\}$.

Remarque 4.20. Du théorème 4.5(a), I et J sont comaximaux s-si il existe $i \in I$ et $j \in J$ tels que $i + j = 1$. De façon équivalent, I et J sont comaximaux s-si il existe $i \in I$ tel que $i \equiv 1 \pmod{J}$.

Remarque 4.21. Supposons que A est un anneau de Bezout, et soient $a, b \in A$ avec $b \neq 0$. Les idéaux (a) et (b) sont comaximaux s-si a et b sont copremiers.

En effet, on a que $(a) + (b) = (a, b)$ et que $A = (1)$. De plus, le lemme 4.13 implique que $(a, b) = (1)$ s-si a et b sont copremiers.

Lemme 4.22. *Soit A un anneau commutatif, unitaire et non-trivial, et soient I, J, K trois idéaux de A qui sont deux-à-deux comaximaux. Alors, I et JK sont aussi comaximaux.*

Démonstration. Le remarque 4.20 implique qu'il existe $j \in J$ et $k \in K$ tels que $j, k \equiv 1 \pmod{I}$. Donc $jk \equiv 1 \pmod{I}$, ce qui veut dire que I et JK sont comaximaux, en appliquant encore une fois le remarque 4.20. □

Théorème 4.23 (théorème des restes chinois)**.** *Soit A un anneau commutatif, unitaire et non-trivial, et soient $I_1, \ldots, I_k$ d'idéaux de A. Définissons l'application*

$$\begin{aligned} \pi : A &\longrightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_k \\ a &\longrightarrow (a \pmod{I_1}, a \pmod{I_2}, \ldots, a \pmod{I_k}) \end{aligned}$$

(a) L'application π est un morphisme d'anneau avec $\ker(\pi) = I_1 \cap I_2 \cap \cdots \cap I_k$.

(b) Si les idéaux $I_1, \ldots, I_k$ sont deux-à-deux comaximaux, alors π est surjective, $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$, et

$$A/I_1 I_2 \cdots I_k \cong A/I_1 \times A/I_2 \times \cdots A/I_k.$$

Démonstration. (a) Exercice.

(b) On montre d'abord que maintenant que $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$. Considérons premièrement le cas où $k = 2$. Si $i_1 \in I_1$ et $i_2 \in I_2$, alors $i_1 i_2 \in I_1 \cap I_2$, donc $I_1 I_2 \subset I_1 \cap I_2$. De plus, la comaximalité de I_1 et e I_2 implique l'existence de $i_1 \in I_1$ et de $i_2 \in I_2$ tels que $i_1 + i_2 = 1$. En particulier, $a = ai_1 + ai_2$ pour tout $a \in A$. Si $a \in I_1 \cap I_2$, alors $ai_1, ai_2 \in I_1 I_2$ par commutativité, ce qui conclut la démonstration que $I_1 I_2 = I_1 \cap I_2$.

Pour montrer le cas général, on utilise induction sur k : si la conclusion est vraie pour $k-1$ idéaux, on a que $I_1 \cap \cdots \cap I_{k-1} = I_1 \cdots I_{k-1}$, qui est un idéal comaximal avec I_k d'après le lemme 4.22. Donc

$$I_1 \cap \cdots \cap I_k = (I_1 \cdots I_{k-1}) \cap I_k = (I_1 \cdots I_{k-1}) I_k = I_1 \cdots I_k$$

d'après le cas $k = 2$ qu'on a déjà montré.

Maintenant, on montre la surjectivité de π. On sait $I_1, I_2, \ldots, I_k$ sont deux à deux copremiers, donc le lemme 4.22 (appliqué de façon inductive) implique que I_1 et $I_2 \cdots I_k$ sont comaximaum. Le remarque 4.20 nous dit qu'il existe $i_1 \in I_2 \cdots I_k$ tel que $i_1 \equiv 1 \pmod{I_1}$. Donc, $\pi(i_1) = (\overline{1}, \overline{0}, \ldots, \overline{0})$.

De façon analogue, on peut trouver $i_2, \ldots, i_k$ tels que $\pi(i_j) = (\overline{\delta_{1,j}}, \ldots, \overline{\delta_{1,k}})$, où $\delta_{m,n}$ est le symbole de Kronecker. Donc $\pi(a_1 i_1 + \cdots + a_k i_k) = (\overline{a_1}, \ldots, \overline{a_k})$ pour tous $a_1, \ldots, a_k \in A$, ce qui montre la surjectivité de π.

Il reste à monter que $A/I_1 \cdots I_k = A/\ker(\pi)$ et $A/I_1 \times \cdots A/I_k = \pi(A)$ sont isomorphes. Ceci est un cas particulier du premier théorème d'isomorphisme d'anneaux qu'on étudiera plus généralement dans le chapitre 4.5. Pour maintenant, il suffit d'observer que l'application $f : A/\ker(\pi) \to A/I_1 \times \cdots A/I_k$, définie par $f(\overline{a}) := \pi(a)$, est bien définie (théorème de la théorie des groupes) et nous donne un isomorphisme entre $A/\ker(\pi)$ et $A/I_1 \times \cdots A/I_k$. On laisse les détails de vérification de cette affirmation comme un exercice. □

Exemple 4.24. Soit $p \equiv 1 \pmod 4$ un nombre premier entier. On sait alors que $p = a^2 + b^2$. Donc, on peut factoriser $p = \pi \cdot \overline{\pi}$ dans $\mathbb{Z}[i]$, où $\pi := a + bi$. On affirme que

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi}). \tag{4.1}$$

Il suffit de montrer que les idéaux (π) et $(\overline{\pi})$ sont comaximaux. D'après le remarque (4.20), il faut montrer que π et $\overline{\pi}$ sont copremiers dans $\mathbb{Z}[i]$.

On commence en montrant que π et $\overline{\pi}$ sont d'éléments irréductibles de $\mathbb{Z}[i]$. On a que $N(\pi) = a^2 + b^2 = p$. Donc, si $\pi = \alpha\beta$, alors $N(\alpha)N(\beta) = p$, ce qui implique que soit $N(\alpha) = 1$ ou $N(\beta) = 1$. C'est-à-dire, soit α est inversible, ou β l'est, ce qui montre notre affirmation que π est irréductible. Le résultat pour $\overline{\pi}$ est montré de façon similaire.

Maintenant qu'on sait que π et $\overline{\pi}$ sont irréductibles et on est dans un anneau factoriel, la seule façon possible dans laquelle π et $\overline{\pi}$ ne sont pas copremiers est s'ils sont associés, c'est-à-dire si $\overline{\pi} = u\pi$ pour un $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. On ne peut pas avoir que $\pi = \pm\overline{\pi}$, car ceci impliquerait que $a = 0$ ou que $b = 0$. Par contre, ceci est impossible car p n'est pas un carré. De plus, on ne peut pas avoir que $\pi = \pm i\overline{\pi}$, car ceci impliquerait que $a = \pm b$. Par contre, ceci est impossible car $p \neq 2$.

On a conclut la démonstration de (4.1).

Remarque 4.25. Dans le remarque ci-dessus, pbservez que $m + ni \equiv m' + n'i \pmod{(p)}$ s-si $(m + ni) - (m' + n'i) = p(k + \ell i)$ pour quelques $k, \ell \in \mathbb{Z}$, s-si $m - m' = pk$ et $n - n' = p\ell$ pour quelques $k, \ell \in \mathbb{Z}$, s-si $m \equiv m' \pmod p$ et $n \equiv n' \equiv \pmod p$ dans $\mathbb{Z}$. Donc on trouve que l'ensemble $\{m + ni : 0 \leq m, n \leq p - 1\}$ est un système complet de représentants des résidus mod (p) dans $\mathbb{Z}[i]$. En particulier,

$$\#(\mathbb{Z}[i]/(p)) = p^2. \tag{4.2}$$

En comparant cette identité avec (4.1), on en déduit que

$$\#(\mathbb{Z}[i]/(\pi)) = \#(\mathbb{Z}[i]/(\overline{\pi})) = p. \tag{4.3}$$

4.5 Théorèmes d'isomorphisme d'anneaux

Comme on l'a indiqué à la démonstration du théorème des restes chinois, en analogie avec les morphismes de groupes, les morphismes d'anneaux satisfassent quatre théorèmes d'isomorphismes.

Théorème 4.26 (1er théorème d'isomorphisme d'anneaux)**.** *Soit $\phi : A \to B$ un morphisme d'anneaux. Son noyau* $\ker(\phi)$ *est un idéal de A et son image $\phi(A)$ est un sous-anneau de B. De plus, on a que*

$$A/\ker(\phi) \cong \phi(A).$$

Démonstration. Puisque ϕ est un morphisme entre les groupes additifs de A et de B, $\ker(\phi)$ est un sous-groupe additif de A et $\phi(A)$ est un sous-groupe additif de B.

De plus, si $a \in \ker(\pi)$ et a' est n'importe que élément de A, alors $\phi(aa') = \phi(a)\phi(a') = 0 \cdot \phi(a') = 0$ et, de manière similaire $\phi(a'a) = 0$. On en déduit que $\ker(\phi)$ est un idéal de A.

Puis, si $b, b' \in \phi(A)$, alors $b = \phi(a)$ et $b' = \phi(a')$ pour quelques $a, a' \in A$. Donc $bb' = \phi(a)\phi(a') = \phi(aa') \in \phi(A)$. Ceci montre que $\phi(A)$ est un sous-anneau de B.

Finalement, pour montrer que $A/\ker(\phi) \cong \phi(A)$, on définit $\psi : A/\ker(\phi) \to \phi(A)$ par $\psi(\overline{a}) = \phi(a)$. On sait de la théorie des groupes que ψ est bien défini, ainsi qu'il est un isomorphisme entre les groupes additifs de $A/\ker(\phi)$ et $\phi(A)$. Finalement, on a que $\psi(\overline{a_1} \cdot \overline{a_2}) = \psi(\overline{a_1 a_2}) = \phi(a_1 a_2) = \phi(a_1)\phi(a_2) = \psi(\overline{a_1})\psi(\overline{a_2})$. □

Corollaire 4.27. *Soient L un corps et K un sous-corps de L. Si $P(x) \in K[x]$ est un polynôme irréductible et $\alpha \in L$ est tel que $P(\alpha) = 0$, alors*

$$K[x]/(P(x)) \cong K(\alpha).$$

Démonstration. On a que $K[\alpha] = K(\alpha)$ d'après l'exercice 3.2(c). Définissons $\phi : K[x] \to K[\alpha]$ par $\phi(f) := f(\alpha)$. Clairement, ϕ est un épimorphisme d'anneaux. De plus, d'après l'exercice 3.2(b), on a que $f(\alpha) = 0$ s-si $P(x)|f(x)$. Donc, $\ker(\phi) = (P(x))$ et le corollaire découle du théorème 4.26. □

Exemple 4.28. Comme un cas spécial du corollaire 4.27, on a que $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Exemple 4.29 (la caractéristique d'un anneau)**.** Soit A un anneau unitaire. Pour $n \in \mathbb{Z}$, définissons

$$n \times 1 := \begin{cases} \underbrace{1 + \cdots + 1}_{n \text{ fois}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ \underbrace{-1 - \cdots - 1}_{|n| \text{ fois}} & \text{si } n < 0. \end{cases}$$

Une vérification facile permet nous de montrer les rélations $(m + n) \times 1 = m \times 1 + n \times 1$ et $(mn) \times 1 = m \times (n \times 1)$ pour tous $m, n \in \mathbb{Z}$. Donc, l'application $\phi : \mathbb{Z} \to A$, définie par $\phi(n) := n \times 1$, est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, donc il existe $m \in \mathbb{Z}_{\geq 0}$ tel que $\ker(\phi) = m\mathbb{Z}$. On appelle m la **caractéristique** de A on écrit

$$m = \operatorname{car}(A).$$

En autres mots, on a que

$$m = \begin{cases} 0 & \text{si } n \times 1 \neq 0 \text{ pour tout } n \in \mathbb{Z}_{\geq 1}, \\ \min\{n \in \mathbb{Z}_{\geq 1} : n \times 1 = 0\} & \text{sinon.} \end{cases}$$

De plus, $\mathbb{Z}/m\mathbb{Z} \cong \phi(A)$. En particulier, si A est intègre, alors $\mathbb{Z}/m\mathbb{Z}$ est aussi intègre. On a alors montré le théorème suivant.

Théorème 4.30. *Si A est un anneau intègre, alors soit $\mathrm{car}(A) = 0$ ou $\mathrm{car}(A)$ est un nombre premier.*

Théorème 4.31 (2ème théorème d'isomorphisme d'anneaux)**.** *Soit A un anneau, B un sous-anneau de A, et I un idéal de A. Alors, $B + I$ est un sous-anneau de A contenant I, $B \cap I$ est un idéal de B, et*

$$(B + I)/I \cong B/B \cap I.$$

Démonstration. On laisse comme exercise la vérification des affirmations que $B + I$ est un sous-anneau de A contenant I, et que $B \cap I$ est un idéal de B. Définissons $\phi : B+I \to B/B\cap I$ par $\phi(b+i) = \overline{b}$. Elle est bien définie : si $b_1 + i_1 = b_2 + i_2$, alors $b_1 - b_2 = i_2 - i_1 \in B \cap I$ car $b_1 - b_2 \in B$ et $i_2 - i_1 \in I$. On en déduit que $b_1 \equiv b_2 \pmod{B \cap I}$, comme requis.

Puis, on montre que ϕ est un morphisme d'anneaux. L'additivité de ϕ est déjà montré en théorie des groupes. Pour la multiplicativité, on a que

$$(b_1 + i_1)(b_2 + i_2) = b_1b_2 + i,$$

où $i = b_1i_2 + i_1b_2 + i_1i_2 \in I$, d'où

$$\phi((b_1 + i_1)(b_2 + i_2)) = \overline{b_1b_2} = \phi(b_1 + i_1)\phi(b_2 + i_2).$$

Finalement, si $x \in \ker(\phi)$, alors $x = b + i$ et $\phi(x) = \overline{b} = \overline{0}$, ce qui implique que $b \in I$. Donc, $x \in I$. Vice versa, si $x \in I$, alors $x = 0 + i$ et $\phi(x) = \overline{0}$, c'est-à-dire $x \in \ker(\phi)$. On en déduit que $\ker(\phi) = I$. Le théorème découle du théorème 4.26. □

Théorème 4.32 (3ème théorème d'isomorphisme d'anneaux)**.** *Soit A un anneau. Si $I \subset J$, où I et J sont deux idéaux de A, alors J/I est un idéal de A/I et*

$$(A/I)/(J/I) \cong A/J$$

Démonstration. On laisse comme exercice la vérification que J/I est un idéal de A/I. Pour la deuxième partie de l'exercice, considérons $\phi : A/I \to A/J$, définie par $\phi(a + I) = a + J$. Elle est bien définie, car si $a \equiv a' \pmod{I}$, alors $a \equiv a' \pmod{J}$, vu que $a - a' \in I \subset J$. C'est facile aussi de prouver qu'elle un épimorphisme d'anneaux. Finalement, on a que $\phi(a+I) = 0$ s-si $a \in J$, s-si $a + I \in J/I$. Le résultat alors découle du théorème 4.26. □

Théorème 4.33 (4ème théorème d'isomorphisme d'anneaux - théorème de correspondence)**.** *Soit A un anneau et I un idéal de A. Dénotons par $\mathcal{S}$ l'ensemble de sous-anneaux de A contenant I, et par $\mathcal{I}$ l'ensemble d'idéaux de A contenant I, et*

(a) Si $B \in \mathcal{S}$, alors B/I est un sous-anneau de A/I.
(b) Si $J \in \mathcal{I}$, alors J/I est un idéal de A/I.
(c) Si $B, C \in \mathcal{S}$, alors $B \subset C$ s-si $B/I \subset C/I$.
(d) Tous les sous-anneaux de A/I sont de la forme B/I, où $B \in \mathcal{S}$.

(e) Tous les idéaux de A/I sont de la forme J/I, où $J \in \mathcal{I}$.

Démonstration. Les parties (a) et (b) sont évidentes.

(c) Une direction est évidente : si $B \subset C$, alors $B/I \subset C/I$. Vice versa, supposons que $B/I \subset C/I$ et soit $b \in B$. Donc $b + I \in C/I$, c'est-à-dire il existe $c \in C$ et $i \in I$ tels que $b = c + i$. Puisque $C \supset I$ et C est fermé sous l'addition comme un sous-anneau de A, on trouve que $b \in C$. Ceci montre que $B/I \subset C/I$, ce qui est ce qu'il fallait prouver.

(d) Il faut montrer que si R un sous-anneau de A/I, alors il existe $B \in \mathcal{S}$ tel que $R = B/I$. Définissons $B := \{b \in A : b + I \in R\}$.

On affirme que $B \in \mathcal{S}$. Tout d'abord, c'est clair que $B \supset I$, car $I = 0_R \in R$. En particulier, $B \neq \emptyset$. De plus, si $b_1, b_2 \in B$, alors $b_1 + I, b_2 + I \in B$. Donc, $b_1 - b_2 + I = (b_1 + I) - (b_2 + I) \in R$ car R est fermé sous la soustraction, ainsi que $b_1 b_2 + I = (b_1 + I)(b_2 + I) \in R$ car R est fermé sous la multiplication. Ceci montre que $B \in\in \mathcal{S}$.

Or, on montre que $B/I = R$. Par définition, $b + I \in R$ pour tout $b \in B$, donc $B/I \subset R$. Vice versa, si $b + I \in R$, alors $b \in B$ et donc $b + I \in B/I$.

(e) On observe que si R est un idéal de A/I, alors il est un sous-anneau de A/I. On peut alors défini $B = \{b \in A : b + I\}$ comme ci-dessus. On sait déjà que B est un sous-anneau de A contenant I, et que $R = B/I$. Pour montrer que B est un idéal de A, considérons $b \in B$ et $a \in A$. Puisque $b + I \in R$ et R est un idéal, on a que $ab + I = (a + I)(b + I) \in R$, d'où on déduit que $ab \in R$. De même, on montre que $ba \in R$ également. Ceci conclut la démonstration. □

4.6 Idéaux premiers et maximaux

On étudie maintenant les éléments premiers d'un anneau en utilisant la notion d'idéaux. Soit A un anneau intègre et p un élément premier de A. Ceci veut dire que si $p|ab$, alors soit $p|a$ ou $p|b$. De façon équivalente, on a que si $ab \in (p)$, alors soit $a \in (p)$ ou $b \in (p)$. Cette observation nous amène à la notion d'un idéal premier :

Définition 4.34. Soit A un anneau commutatif. Un idéal P de A est appelé **premier** si :

— $P \neq A$;
— si $ab \in P$ pour quelques $a, b \in A$, alors soit $a \in P$ ou $b \in P$.

On voit donc qu'un élément p non-zéro d'un anneau intègre A est premier s-si l'idéal (p) est premier [1].

Théorème 4.35. *Soit A un anneau commutatif et unitaire. Un idéal P de A est premier s-si A/P est un anneau intègre.*

Démonstration. Supposons que P est premier. Puisque $P \neq A$, on trouve que A/P est non-trivial. On sait aussi que A est unitaire et commutatif, donc A/P l'est.

1. Observons que $(p) \neq A$ s-si $p \notin A^\times$.

Il reste à montrer que A/P n'a pas de diviseurs de zéro. En effet, si $\overline{a}\overline{b} = \overline{0}$, alors $\overline{ab} = \overline{0}$, c'est-à-dire $ab \in P$. La primalité de P implique alors que soit $a \in P$ ou $b \in P$. De façon équivalente, on a que soit $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Réciproquement, supposons que A/P est intègre. En particulier, il est non-trivial, donc $P \neq A$. Si $ab \in P$, alors $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0}$. Mais P n'a pas de diviseurs de zéro, donc il faut que soit $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. C'est-à-dire, il faut que soit $a \in P$ ou $b \in P$. □

Corollaire 4.36. *Soit A un anneau unitaire, commutatif et non-trivial. L'idéal $\{0\}$ est premier s-si A est intègre.*

Vu que chaque corps est un anneau intègre, il est naturel de considérer un autre type d'idéaux M, pour lesquels l'anneau-quotient A/M est un corps. Si A est commutatif et unitaire, alors A/M l'est aussi. Donc, le théorème 4.5(b) implique que A/M est un corps s-si $M \neq A$ et les seuls idéaux de A/M sont $\{0_{A/M}\}$ et A/M. En général, le théorème 4.33 dit que les idéaux de A/M sont tous de la forme I/M, où I est un idéal de A contenant M. Donc, A/M est un corps s-si les seuls idéaux I de A contenant M sont M soi-même et A.

Cette discussion nous amène naturellement à la définition suivante :

Définition 4.37. Soit A un anneau. Un idéal M de A est appelé **maximal** si

— $M \neq A$;
— il n'existe pas d'idéaux I de A tels que $M \subsetneqq I \subsetneqq A$.

L'argument précédant la définition 4.37 établit la caractérisation suivante d'idéaux maximaux :

Théorème 4.38. *Soit A un anneau commutatif et unitaire. Un idéal M de A est maximal s-si A/M est un corps. En particulier, si M est maximal, alors il est également premier.*

Les idéaux maximaux jouent un rôle important dans la théorie d'anneaux. Comme on va le montrer, si I est un idéal propre d'un anneau unitaire A, alors on peut rajouter à I quelques éléments de A et le rend maximal. Le problème est que A pourrait avoir une cardinalité gigantesque. Donc, pour trouver les éléments nécessaires à rajouter à I pour le rendre maximal, il faut utiliser l'axiom de choix de la théorie d'ensembles. On l'utilise dans sa forme équivalente, qui est le lemme de Zorn :

Lemme de Zorn. *Soit X un ensemble non-vide et partiellement ordonné*[2] *par rapport à une relation $\leq$.*

Supposons que si Y est une chaîne ascendante et non-vide (c'est-à-dire, Y est totalement ordonné[3] *par rapport à $\leq$ possède une borne supérieure, c'est-à-dire il existe $x \in X$ tel que $y \leq x$ pour tout $y \in Y$.*

Donc, il existe un élément maximal dans X, c'est-à-dire il existe $x \leq X$ tel que il n'existe pas $y \in X$ avec $y > x$.

2. On rappelle que ceci veut dire que : (a) $x \leq x$ pour tout $x \in X$; (b) si $x \leq y$ et $y \leq x$, alors $x = y$; (c) si $x \leq y$ et $y \leq z$, alors $x \leq z$.

3. On rappelle que ceci veut dire que si $y, y' \in Y$, alors soit $y \leq y'$ ou $y' \leq y$.

Théorème 4.39. *Soit A un anneau unitaire et non-trivial. Si I est un idéal propre de A, alors il existe un idéal maximal M de A contenant I.*

En particulier, en prenant $I = \{0\}$, on déduit que A possède au moins un idéal maximal.

Démonstration. Soit $X = \{J \text{ idéal propre de } A : J \supset I\}$. Puisque $I \in X$, alors $X \neq \emptyset$. De plus, X est partiellement ordonné par rapport à la relation $\subset$. On va montrer que le lemme de Zorn est applicable.

Soit Y une chaîne ascendante et non-vide de X. On va montrer qu'elle possède une borne supérieure. Ceci sera l'ensemble

$$K := \bigcup_{J \in Y} J.$$

Évidemment, $K \supset J$ pour tout $J \in Y$. En particulier, $K \supset I$. Pour montrer que K est une borne supérieure de Y, il reste à montrer qu'il appartient à X, c'est-à-dire qu'il est un idéal propre de A.

On a que $J \neq A$ pour tout $J \in Y$. Selon le théorème 4.5, ceci veut dire que $1 \notin J$ pour tout $J \in Y$. En particulier, $1 \notin K$, d'où on déduit que $K \neq A$.

Finalement, on montre que K est un idéal de A. Il est non-vide car il est la réunion de quelques idéaux (en particulier, K contient 0). Supposons, maintenant, que $k \in K$ et $a \in A$. Donc, il existe $J \in Y$ contenant k. Puisque J est un idéal, on a que $ak, ka \in J \subset K$. L'étape dernière est de montrer que si $k, k' \in K$, alors $k - k' \in K$. En effet, on sait qu'il existe $J, J' \in Y$ tels que $k \in J$ et $k' \in J'$. Puisque Y est totalement ordonné, soit $J \subset J'$ ou $J \subset J'$. Par conséquent, soit $k, k' \in J$ ou $k, k' \in J'$. Mais J et J' sont d'idéaux, d'où on déduit que soit $k - k' \in J \subset K$ ou $k - k' \in J' \subset K$. En tout cas, $k - k' \in K$, ce qui montre que K est un idéal.

On a alors montré que les hypothèses du lemme de Zorn sont satisfaites. Par la suite, X possède un élément maximal, soit M. Par définition, M est un idéal propre contenant I. De plus, vu que M est maximal dans X par rapport à l'inclusion d'ensembles, il n'existe pas un idéal propre $J \supsetneq M$. Donc, M est un idéal maximal contenant I. □

4.7 Anneaux noetheriens et principaux

On finit ce chapitre en montrant que les anneaux principaux sont factoriels. On commence avec une étude des anneaux noetheriens, dont un exemple spécial sont les anneaux principaux. Le théorème suivant donne une caractérisation des anneaux noetheriens qui est très utile et qu'on va revoir plus tard dans le contexte de la théorie de modules.

Théorème 4.40. *Soit A un anneau. Alors, A est noetherien s-si chaque chaîne ascendante d'idéaux de A*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

se termine, *dans le sens qu'il existe $n \in \mathbb{Z}_{\geq 1}$ tel que $I_n = I_{n+1} = I_{n+2} = \cdots$.*

Démonstration. Supposons que A est noetherien, et soit $I_1 \subset I_2 \subset \cdots$ une chaîne ascendante d'idéaux de A. Considérons $I := \bigcup_{j=1}^{\infty} I_j$. Comme on l'a montré dans la démonstration du théorème 4.39, I est un idéal de A. Puisque A est noetherien, I est de type fini, c'est-à-dire il

existe $a_1, \ldots, a_k \in A$ tels que $I = (a_1, \ldots, a_k)$. En particulier, $a_\ell \in I = \bigcup_{j=1}^{\infty} I_j$. Il existe alors $j_\ell \in \mathbb{Z}_{\geq 1}$ tel que $a_\ell \in I_{j_\ell}$. Soit $n = \max\{j_1, \ldots, j_k\}$, pour que $a_\ell \in I_n$ pour tout ℓ. Il faut, alors, que $I = (a_1, \ldots, a_k) \subset I_n$. Par conséquent, pour tout $j \geq n$ on a que $I_n \subset I_j \subset I \subset I_n$, ce qui implique que $I_j = I_n$ pour tout $j \geq n$.

Réciproquement, supposons que A est tel que chaque chaîne ascendante d'idéaux de A se termine. Soit I un idéal de A. On cherche de générateurs de I. Supposons que I n'est pas de type fini. On arrivera à une contradiction.

En effet, soit $a_1 \in I$. Puisque I n'est pas de type fini, alors $(a_1) \neq I$. Il existe alors $a_2 \in I \setminus (a_1)$, pour que $(a_1) \subsetneqq (a_1, a_2)$. En utilisant encore l'hypothèse que I n'est pas de type fini, on a que $(a_1, a_2) \neq I$. En particulier, on peut trouver $a_3 \in I \setminus (a_1, a_2)$, pour que $(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3)$. On a aussi que $(a_1, a_2, a_3) \neq I$ car I n'est pas de type fini. En continuant de cette façon, on peut trouver une suite infinie d'éléments $a_1, a_2, \ldots$ tels que $(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3) \subsetneqq \cdots$. Ceci contredit l'hypothèse que chaque chaîne ascendante d'idéaux de A se termine. Il faut alors que I soit de type fini, comme on le voulait démontrer. □

Théorème 4.41. *Chaque anneau principal est factoriel.*

Démonstration. Soit $a \in A' := A \setminus (A^\times \cup \{0\})$. On veut montrer que a peut s'écrire comme un produit d'irréductibles. Supposons que ce n'est pas le cas. En particulier, a est réductible, ce qui implique que $a = a_1 a_1'$ pour quelques $a_1, a_1' \in A'$. Il faut que soit a_1 ou a_1' n'est pas un produit d'irréductibles. Sans perte de généralité, supposons que a_1 n'est pas un produit d'irréductibles. Puisque $a_1 | a$ et $a_1 \not\sim a$, on a que $(a) \subsetneqq (a_1)$. Maintenant, on répète cet argument pour trouver $a_2 | a_1$ qui n'est pas un produit d'irréductibles et tel que $(a_1) \subsetneqq (a_2)$. En continuant de cette manière, on peut construire une chaîne ascendante d'idéaux de A qui ne se termine pas. D'après le théorème 4.40, ceci contredit le fait que A est un anneau noetherien.

On a alors montré que chaque $a \in A'$ possède une factorisation dans quelques irréductibles. L'unicité de cette factorisation est montrée en suivant l'argument du théorème 3.20. La seule chose dont on a besoin pour faire marcher cet argument est que les irréductibles sont premiers dans A. Mais un anneau principal est un anneau de Bezout par le corollaire 4.15. Donc le lemme 3.18(b) implique que les notions de primalité et d'irréductibilité coincident dans un anneau principal. Ceci conclut la démonstration. □

En fait, la démonstration n'utilise pas la force complète de la principalité de l'anneau A, mais juste qu'il est noetherien ainsi que la coincidence des notions de primalité et d'irréductibilité. Donc, on a le théorème suivant plus général :

Théorème 4.42. *Si A est un anneau intègre et noetherien, dont chaque élément irréductible est également premier, alors A est factoriel.*

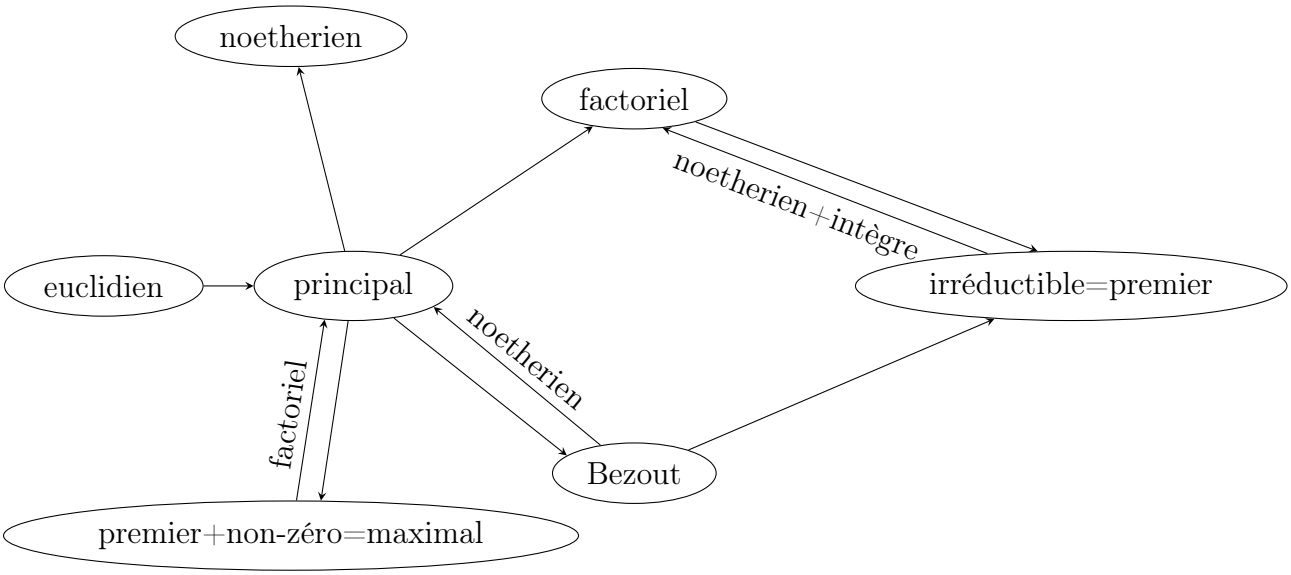
Théorème 4.43. *Dans un anneau principal, chaque idéal premier et non-trivial est maximal.*

Démonstration. Soit P un idéal premier et non-trivial. Donc $P = (p)$ pour un élément p premier de A. Si I est un idéal de A contenant P, alors $I = (a)$ pour un $a \in A$. Vu qu $I \supset P$,

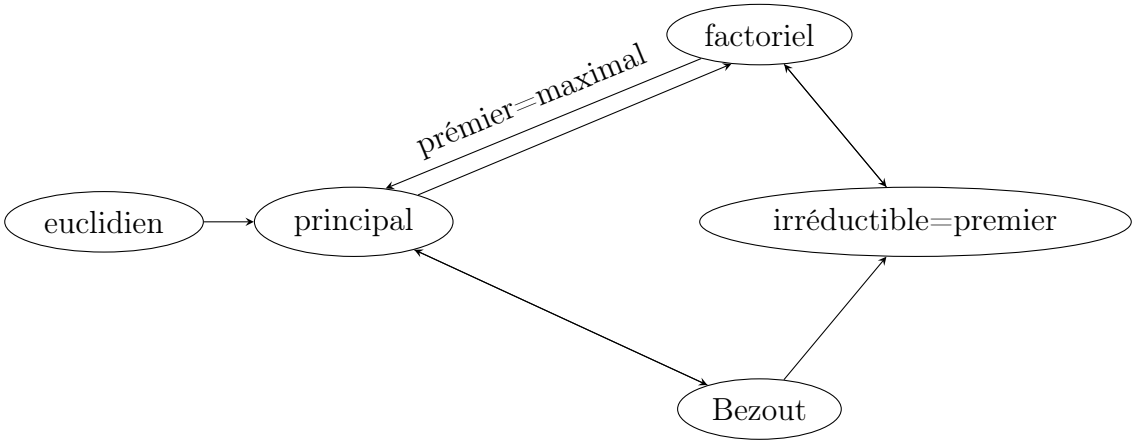
il faut que $a|p$. Mais p est irréductible comme premier, donc soit $a \in A^\times$, au quel cas $I = A$ par le théorème 4.5(a), ou $a \sim p$, au quels cas $I = P$ par le lemme 4.9. Ceci montre que P est maximal. □

Remarque 4.44. L'exercice 4.6 montre un inverse partiel du dernier théorème.

On conclut le chapitre avec une mise à jour du diagramme du chapitre 3 :



En supposant que l'anneau est noetherien et intègre, le diagramma se simplifie :



Remarque 4.45. Rappelez que si I est un idéal propre de A, alors I est premier s-si A/I est intègre, ainsi que I est maximal s-si A/I. Dans plusieurs exemples importants d'anneaux, les quotients A/I avec $I \neq \{0\}$ sont tous finis. Donc, le théorème 2.18 implique que les notions de maximalité de primalité pour les idéaux non-zéros coincident. Si un tel anneau est aussi intègre et noetherien, on a une équivalence complète entre les notions d'être factoriel, d'être de Bezout, d'être principal, et d'avoir la propriété que tous les irréductibles sont de premiers.

La théorie des modules qu'on développera à la prochaine partie des notes nous aidera de construire plusieurs exemples d'anneaux A dont tous les quotients A/I non-triviaux sont finis.

4.8 Exercices

Exercice 4.1 (Ex. 37, 38, 39, p. 259-60).

(a) Soit A un anneau commutatif et unitaire. On dit que A est un anneau **local** s'il possède un idéal maximal unique.

(i) Montrez que si A est un anneau local dont l'idéal maximal est M, alors chaque élément de $A \setminus M$ est inversible.

(ii) Réciproquement, prouvez que si les éléments non-inversibles de A forment un idéal M, alors A est un anneau local dont l'idéal maximal unique est M.

(b) En suivant la notation de l'exercice 2.7, soit K un corps, ν une valuation discrète sur K est A l'anneau de valuation de ν. Pour chaque nombre entier $k \geq 0$, on définit

$$A_k = \{x \in K^\times : \nu(x) \geq k\} \cup \{0\}.$$

Montrez que :

(i) A_k est un idéal principal de $A = A_0$.

(ii) Montrez que si I est un idéal non-zero de A, on a que $I = A_k$ pour un $k \geq 0$. Déduisez que A est un anneau local dont l'idéal maximal unique est A_1.

(c) Soit p un nombre premier. Montrez que l'anneau $A = \{a/b : a, b \in \mathbb{Z},\ \text{pgcd}(a,b) = 1,\ p \nmid b\}$ est un anneau local dont l'idéal maximal unique est $\{a/b : a, b \in \mathbb{Z},\ \text{pgcd}(a,b) = 1,\ p|a,\ p \nmid b\}$.

Exercice 4.2. Montrez que chaque idéal I de $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ est de type fini comme suite :

(a) Soit $I_0 = I \cap \mathbb{Z}$ et $I_1 = \{b \in \mathbb{Z} : a + b\sqrt{d} \in I \text{ pour un } a \in \mathbb{Z}\}$. Montrez que I_0 et I_1 sont d'idéaux de $\mathbb{Z}$. Par la suite, $I_0 = (n_0)$ and $I_1 = (n_1)$ pour deux nombres entiers n_0 et n_1.

(b) Montrez que $I_0 \subseteq I_1$.

(c) D'après la définition de I_1, il y a $a_1 \in \mathbb{Z}$ tel que $a_1 + n_1\sqrt{d}$ apparient à I. Prouvez que I est l'idéal engendré par n_0 et $a_1 + n_1\sqrt{d}$.

Exercice 4.3.

(a) Soit $A = \mathbb{Q}[x]$. Montrez que l'idéal engendré par le polynôme $x^2 - 2$ est maximal. Plus précisément, prouvez que

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}].$$

(b) Est-ce que l'idéal engendré par le polynôme $x^2 - 2$ est maximal dans l'anneau $\mathbb{C}[x]$?

EXERCICE 4.4. Soit A un anneau de Boole, c'est-à-dire, $a^2 = a$ pour tout $a \in A$ (cf. exercice 2.5). Prouvez les propositions suivantes.

(a) (ex. 23, p. 258) Si A est non-zéro et unitaire, alors chaque idéal premier de A est aussi maximal.

(b) (ex. 24, p. 258) Chaque idéal de type fini de A est principal [*Indice* : Montrez que $(a, b) = (a + ab + b)$.]

(c) (ex. 1, p. 267) Si A est unitaire, alors $A \cong (a) \times (1 - a)$ pour tout $a \in A$. De plus, l'élément a est l'unité de (a) et l'élément $1 - a$ est l'unité de $(1 - a)$.

(d) (ex. 2, p. 267) Si A est fini, non-zéro et unitaire, alors il y a un $n \in \mathbb{N}$ tel que

$$A \cong \underbrace{\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ fois}}.$$

EXERCICE 4.5. Soit A un anneau intègre et soit $\mathcal{I}(A)$ l'ensemble de tous les idéaux non-zéros de A.

(a) Si $I \in \mathcal{I}(A)$ et $a \in A \setminus \{0\}$, alors montrez que $aI \in \mathcal{I}(A)$.

(b) Soient $I, J \in \mathcal{I}(A)$. On dit que I est équivalent à J et on écrit $I \sim J$ s'il existe $a, b \in A \setminus \{0\}$ tels que $aI = bJ$. Montrez que c'est une relation d'équivalence sur $\mathcal{I}(A)$.

(c) Montrez que l'ensemble de tous les idéaux principaux est une classe d'équivalence de la relation $\sim$ qu'on peut écrire comme $[A]$ (ici $[I]$ dénote la classe d'équivalence de l'idéal I).

(d) Si $\mathcal{C}_1 = [I_1]$ et $\mathcal{C}_2 = [I_2]$ sont deux classes d'équivalence, alors on définit $\mathcal{C}_1 \cdot \mathcal{C}_2 = [I_1 I_2]$. Montrez que cette opération est bien définie. De plus, montrez que la classe d'équivalence $[A]$ des idéaux principaux est l'élément neutre de cette opération.

EXERCICE 4.6. Soit A un anneau factoriel dont chaque idéal premier non-trivial est maximal.

(a) Montrez que A est un anneau de Bezout.

(b) Montrez que A est principal.
[*Indice* : Si I est un idéal propre et non-zéro de A, alors montrez qu'il est principal par induction sur $\min\{\Omega(a) : a \in I \setminus \{0\}\}$, où $\Omega(a) = n$ si $a = p_1 \cdots p_n$ est une factorisation de a à des éléments irréductibles.]

Remarque. On sait que l'inverse de (b) est aussi vrai : un anneau principal est factoriel et ses idéaux premiers sont tous maximaux.

EXERCICE 4.7.

(a) Soit $\phi : A \to B$ un morphisme d'anneaux surjectif. Montrez que si A a une unité, alors B en a aussi une. Déduisez que $m\mathbb{Z}/dm\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ comme anneaux s-si $(d, m) = 1$.

(b) Soit $n \in \mathbb{Z}$, $n > 1$. Déterminez tous les idéaux de $\mathbb{Z}/n\mathbb{Z}$ qui sont premiers ou maximaux.

EXERCICE 4.8. Soit A et B deux anneaux commutatifs avec unités $1_A \neq 0_A$ et $1_B \neq 0_B$. Considérons $\phi : A \to B$ un morphisme d'anneaux surjectif. Prouvez les propositions suivantes :

(a) $\ker(\phi)$ est un idéal premier de A s-si B est intègre.

(b) $\ker(\phi)$ est un idéal maximal de A s-si B est un corps.

(c) Si I est un idéal de A qui contenant $\ker(\phi)$, alors on a que $A/I \cong B/\phi(I)$.

(d) Si Q est un idéal premier de B, alors son image réciproque $\phi^{-1}(Q)$ est un idéal premier de A contenant $\ker(\phi)$. Réciproquement, si P est un idéal premier de A contenant $\ker(\phi)$, alors son image $\phi(P)$ est un idéal premier de B.

(e) Si N est un idéal maximal de B, alors son image réciproque $\phi^{-1}(N)$ est un idéal maximal de A. Réciproquement, si M est un idéal maximal de A, soit $\phi(M) = B$ soit $\phi(M)$ est un idéal maximal de B. Si, de plus, $\ker(\phi) \subset M$, alors l'ensemble $\phi(M)$ est nécessairement un idéal maximal de B. Finalement, donnez un exemple où M et maximal et $\phi(M) = B$.

Chapitre 5

Anneaux polynomiaux

Le but de ce chapitre est d'étudier la décomposition d'un polynôme en facteurs irréductibles, ainsi que de développer des outils qui va nous permettre de décider quand un polynôme donné est irréductible.

5.1 Polynômes sur un corps

Si K est un corps, on se rappelle que $K[x]$ est un anneau euclidien. Alors, il est un anneau de Bezout, principal, factoriel, et un anneau où chaque idéal premier non-zéro est maximal.

On commence en montrant quelques résultats de bases.

Lemme 5.1. *Soit K un corps, $\alpha \in K$ et $f(x) \in K[x]$. Alors, α est une racine de $f(x)$ s-si $x - \alpha | f(x)$, s-si il existe $g(x) \in K[x]$ tel que $f(x) = (x - \alpha)g(x)$.*

Démonstration. Puisque $\alpha \in K$, alors son polynôme minimal sur K est le polynôme $x - \alpha$ (voir l'exercice 3.2). Donc, $f(\alpha) = 0$ s-si $x - \alpha | f(x)$, d'après l'exercice 3.2(b). □

Définition 5.2. Soit K un corps, $\alpha \in K$ et $f(x) \in K[x]$. Si α est une racine de $f(x)$, alors la **multiplicité** de α est le plus grand nombre entier m tel que $(x - \alpha)^m | f(x)$.

Théorème 5.3. *Soient K un corps et $f(x) \in K[x] \setminus \{0\}$. Si $\alpha_1, \ldots, \alpha_r \in K$ sont de racines distinctes de $f(x)$ de multiplicité $m_1, \ldots, m_r$, respectivement, alors il existe $g(x) \in K[x]$ tel que $f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} g(x)$ et $g(\alpha_j) \neq 0$ pour $j = 1, 2, \ldots, r$.*

En particulier, $m_1 + \cdots + m_r \leq \deg(f)$.

Démonstration. On montre le théorème par induction sur r. Si $r = 0$, alors il découle du lemme 5.1 en prenant $g = f$. Supposons qu'il est vrai pour r racines et soit α_{r+1} une autre racine de multiplicité m_{r+1}.

On sait que $f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} g(x)$, où $g(\alpha_j) \neq 0$ pour $j = 1, 2, \ldots, r$.

Fait 1 : $(x - \alpha_{r+1})^m | f(x)$ s-si $(x - \alpha_{r+1}^m | g(x)$.

Puisque on est dans un anneau factoriel (donc dans un anneau où le lemme d'Euclide est vrai), il suffit de montrer que $x - \alpha_{r+1}$ est copremier avec $x - \alpha_j$ pour tout $j \leq r$. En effet, l'idéal engendré par $x - \alpha_j$ et par $x - \alpha_{r+1}$ contient $\alpha_j - \alpha_{r+1} = (x - \alpha_{r+1}) - (x - \alpha_j)$. Mais

K est un corps, et chaque élément de $K \setminus \{0\}$ est inversible dans K (et donc dans $K[x]$). En particulier, $\alpha_j - \alpha_{r+1}$ est inversible dans $K[x]$, ce qui implique que

$$(x - \alpha_j, x - \alpha_{r+1}) = K[x] = (1).$$

Ceci montre que $x - \alpha_j$ et $x - \alpha_{r+1}$ sont copremiers, comme on l'a affirmé.

D'après le fait 1 et la définition de la multiplicité d'une racine, on a que $(x-\alpha_{r+1})^{m_{r+1}} | g(x)$. Donc, il existe $h(x) \in K[x]$ tel que $g(x) = (x - \alpha_{r+1})^{m_{r+1}} h(x)$. En particulier, $f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_{r+1})^{m_{r+1}} h(x)$. Il reste à montrer que $h(\alpha_{r+1}) \neq 0$. En effet, si on avait que $h(\alpha_{r+1}) = 0$, alors $x-\alpha_{r+1}$ diviserait $h(x)$ selon le lemme 5.1. Par conséquent, $(x-\alpha_{r+1})^{1+m_{r+1}}$ diviserait $f(x)$, ce qui contredit la définition de m_{r+1}. Ceci conclut la démonstration de la première partie du théorème.

Finalement, pour la deuxième partie, on observe que $\deg(f) = m_1 + \cdots + m_r + \deg(g) \geq m_1 + \cdots + m_r$. (On a que $g \neq 0$ car $f \neq 0$.) □

Corollaire 5.4. *Si K est un corps et $f(x) \in K[x] \setminus \{0\}$, alors f a au plus $\deg(f)$ racines sur K (même si on compte ses racines avec leur multiplicité).*

On a montré que si on peut trouver toutes les racines d'un polynôme, alors on peut l'écrire comme un produit de quelques facteurs linéaires. Mais est-ce que chaque polynôme a de racines ? Si $f(x) = x^2 + 1$ et $K = \mathbb{R}$, alors on sait que $f(x)$ n'a pas de racines dans $\mathbb{R}$. Cependant, on sait qu'on peut passer à une **extension** de $\mathbb{R}$ (c'est-à-dire, un corps contenant $\mathbb{R}$ comme un sous-corps) qui contient toutes les racines de $\mathbb{R}$. Cette extension est le corps des nombres complexes $\mathbb{C}$. Plus généralement, Gauss a montré que chaque polynôme aux coefficients réels a toutes ses racines dans $\mathbb{C}$. Ceci est le théorème fondamental de l'algèbre. Ici on montre que pour chaque polynôme $f(x) \in K[x]$ il existe une extension L de K contenant toutes les racines de f (mais sans spécifiant L).

Théorème 5.5. *Soit K un corps et soit $f(x) \in K[x] \setminus \{0\}$. Il existe une extension L de K où $f(x)$ se factorise complètement, dans le sens qu'il existe $c, \alpha_1, \ldots, \alpha_n \in L$ tels que $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ dans $L[x]$.*

Démonstration. On montre le théorème par induction sur $\deg(f)$. Quand $\deg(f) = 0$, alors f est constant et non-zéro, donc le théorème est trivialement vrai.

Supposons, maintenant, qu'il est vrai quand le degré du polynôme est $< n$, et soit f de degré $n \geq 1$.

Cas 1. Si $f(x)$ est réductible, alors $f(x) = g(x)h(x)$ pour quelques $g(x), h(x) \in K[x]$ non-constants de degré $< n$. Selon l'hypothèse d'induction, il existe une extension L où $g(x)$ se factorise complètement. En réalisant $h(x)$ comme un polynôme de $L[x]$, il existe alors une extension L' de L (donc, une extension de K) où $h(x)$ se factorise complètement. Donc, $f(x)$ se factorise complètement dans L'.

Cas 2. Si $f(x)$ est irréductible, alors on sait que l'idéal $(f(x))$ est premier. Puisque $K[x]$ est euclidien (donc principal), on trouve que $(f(x))$ est un idéal maximal. Alors, le quotient

$$L := K[x]/(f(x))$$

est un corps. De plus, le quotient contient une copie isomorphe de K, donnée par l'ensemble $\{\overline{k} : k \in K\}$. Sans perte de généralité, on identifie $\overline{k}$ et k, donc on peut supposer que L contient K comme un sous-corps, c'est-à-dire qu'il est une extension de K.

On montre que $f(x)$ a une racine dans L. Soit $\alpha := \overline{x}$ (i.e. la classe d'équivalence de x modulo $P(x)$). On observe que si $P(x) = a_0 + a_1x + \cdots + a_nx^n$, où $a_j \in K$, alors

$$P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = a_0 + a_1\overline{x} + \cdots + a_n\overline{x}^n = \overline{a_0 + a_1x + \cdots + a_nx^n} = \overline{P(x)} = \overline{0}.$$

C'est-à-dire, α est une racine de $f(x)$, comme on l'affirmé. Le lemme 5.1 implique qu'il existe On a alors construit une extension L de K contenant une racine de f. D'après le lemme 5.1, il existe $g(x) \in L[x]$ tel que $f(x) = (x - \alpha)g(x)$. Puisque $\deg(g) = \deg(f) - 1 < n$, on peut appliquer l'hypothèse d'induction sur g : il existe une extension L' de L où $g(x)$ se factorise complètement. Donc, $f(x)$ se factorise complètement dans L', qui est une extension de L. □

Corps finis

Une application jolie de la théorie des polynômes est sur les corps finis :

Théorème 5.6. *Soit K un corps, et soit G un sous-groupe* **fini** *du groupe multiplicatif $K^\times$. Alors, G est cyclique.*

Corollaire 5.7. *Si F est un corps fini, alors $F^\times$ est un groupe cyclique.*

Corollaire 5.8. *Si p est un premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique.*

Avant montrer le théorème 5.6, on a besoin d'un lemme.

Lemme 5.9. *Soit $(G, \cdot)$ un groupe abelien. Soit $g, h \in G$ d'ordre m et n, respectivement. Si m et n sont copremiers, alors* $\operatorname{ord}(gh) = mn$.

Démonstration. Soit $k = \operatorname{ord}(gh)$. Certainement, $(gh)^{mn} = 1$ vu que $g^m = h^n = 1$ et G est commutatif. Donc $k = \operatorname{ord}(gh) | mn$.

Puis, on a que $(gh)^k = 1$. Donc $1 = (gh)^{km} = h^{km}$ d'après la commutativité de G et de la définition de m. Donc, $n = \operatorname{ord}(h) | km$. Puisque m et n sont copremiers, on en déduit que $n | k$. De même, on peut aussi montrer que $m | k$. En utilisant la coprimalité de m et de n pour une dernière fois, on trouve que $mn | k$. Ceci montre que $k = mn$, comme on l'affirmé. □

Démonstration du théorème 5.6. Soit

$$m := \exp(G) := \max\{\operatorname{ord}(g) : g \in G\}.$$

On sait que $m \leq |G|$, d'après le théorème de Lagrange. On affirme que $g^m = 1$ pour tout $g \in G$. Supposons pour un instant que ceci est le cas. On observe que le polynôme $x^m - 1$ a alors $|G|$ racines sur K (chaque élément g de G est une racine de $x^m - 1$). Donc, il faut que $|G| \leq m = \deg(x^m - 1)$. Puisque on a aussi que $m \leq |G|$, on en déduit que $m = |G|$, ce qui veut dire qu'il existe $g \in G$ d'ordre $|G|$. Un tel g doit engendre G, ce qui montre que G est cyclique.

On montre que $g^m = 1$ pour tout $g \in G$ par contradiction. Supposons qu'il existe $h \in G$ tel que

$$h^m \neq 1.$$

Soit aussi $g \in G$ d'ordre maximal, c'est-à-dire

$$m = \mathrm{ord}(g).$$

Si $n = \mathrm{ord}(h)$, il faut que $n \nmid m$ (sinon, $h^m = 1$). Il existe alors un premier p dont la puissance exacte divisant n est plus grande que celle divisant m. Soit $p^a \| m$ (i.e. a est la puissance exacte de p divisant m) et $p^b \| n$, pour que $b > a$. Si $n = p^b k$, alors on construit deux nouveaux éléments :

$$g_1 = g^{p^a} \quad \text{et} \quad h_1 = h^k.$$

On a que $\mathrm{ord}(g_1) = m/p^a$ et que $\mathrm{ord}(h_1) = p^b$. De plus, p^b et m/p^a sont copremiers. Donc, le lemme 5.9 implique que $\mathrm{ord}(g_1 h_1) = mp^{b-a} > m$, ce qui est impossible. Ceci conclut la démonstration de notre affirmation que $g^m = 1$ pour tout $g \in G$. Le théorème en découle comme on l'a expliqué ci-dessus. □

5.2 Polynômes sur un anneau factoriel

Les anneaux polynomiaux sur un corps sont euclidiens, donc factoriels. Dans cette section, on montre la même chose quand l'anneau de coefficients est factoriel.

Définition 5.10. Soit A un anneau intègre et soit $f(x) \in A[x] \setminus \{0\}$. On dit que $f(x)$ est **primitif** si ses coefficients sont copremiers, c'est-à-dire, si $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ et $d | a_0, a_1, \ldots, a_n$, alors d est inversible.

Si $f(x)$ n'est pas primitif, on l'appelle **imprimitif**.

Exemple 5.11. Si $A = \mathbb{Z}$, alors le polynôme $2x^2 + 4x + 3$ est primitif, mais le polynôme $2x^2 + 4x + 6$ ne l'est pas.

Exemple 5.12. Chaque polynôme unitaire sur un anneau intègre est primitif.

Remarque 5.13. Soient A un anneau factoriel et K son corps des fractions. Soit, aussi, $f(x) \in K[x]$ de degré $n \geq 0$. Les coefficients de $f(x)$ sont tous des fractions, soient $a_0/b_0, a_1/b_1, \ldots, a_n/b_n$ avec $a_j \in A, b_j \in A \setminus \{0\}$. Donc

$$f(x) = \frac{1}{b} \cdot \tilde{f}(x),$$

où $b = b_0 \cdot b_n$ et tous les coefficients de $\tilde{f}(x)$ sont dans A. Si a est un pgcd de coefficients de $\tilde{f}(x)$, alors on peut écrire $\tilde{f}(x) = a \cdot F(x)$, où $F(x)$ est un polynôme primitif de $A[x]$. Donc, on peut écrire

$$f(x) = \frac{a}{b} \cdot F(x)$$

pour quelques $a, b \in A \setminus \{0\}$. (En éclairant les facteurs communs de a et de b, on peut même supposer que a et b sont copremiers.)

Théorème 5.14. *Si A est un anneau factoriel, alors $A[x]$ est un anneau factoriel. De plus, si K est le corps des fractions de A, alors les polynômes irréductibles sont :*

(a) les polynômes constants $f(x) = p$, où p est un élément irréductible de A ;

(b) les polynômes primitifs non-constants $f(x) \in A[x]$ tels que $f(x)$ est irréductible dans l'anneau $K[x]$.

On a besoin de quelques résultats auxiliaires.

Lemme 5.15. *Soit A un anneau et I un idéal de A. Donc $I[x]$ est un idéal de $A[x]$ et*

$$A[x]/I[x] \cong (A/I)[x].$$

Démonstration. Considérons l'application

$$\begin{aligned} \phi : A[x] &\longrightarrow (A/I)[x] \\ a_0 + a_1 x + \cdots + a_n x^n &\longrightarrow \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n, \end{aligned}$$

où $\overline{a}$ dénote la classe d'équivalence de a mod I. Évidemment, ϕ est un épimorphisme d'anneaux. De plus, son noyau est clairement égal à $I[x]$, les polynômes aux coefficients dans I. En appliquant le premier théorème d'isomorphisme d'anneaux, on trouve que $\ker(\phi) = I[x]$ est un idéal de $A[x]$, ainsi que $A[x]/I[x] \cong (A/I)[x]$, comme on l'a affirmé. □

Le résultat-clé est le **lemme de Gauss** :

Lemme 5.16 (lemme de Gauss)**.** *Si A est un anneau factoriel, alors le produit de deux polynômes primitifs de $A[x]$ est aussi un polynôme primitif de $A[x]$.*

Démonstration. Soit $f(x) = a(x)b(x)$, où $a(x), b(x)$ sont deux polynômes primitifs de $A[x]$. On montre que $f(x)$ est aussi primitif par raisonnement par l'absurde.

Si $f(x)$ n'était pas primitif, alors il existerait un $d \in A \setminus (\{0\} \cup A^\times)$ divisant tous les coefficients de f. Puisque A est factoriel, d a au moins un facteur irréductible, soit p. Ce facteur p doit évidemment diviser tous les coefficients de f. En particulier, on voit que $\overline{f}(x) = \overline{0}$, où $\overline{f}(x)$ dénote l'élément de $(A/(p))[x]$ obtenu en réduisant tous les coefficients de $f(x)$ mod (p). D'après le lemme 5.15 (et de sa démonstration), on trouve donc que

$$\overline{a}(x)\overline{b}(x) = \overline{0}. \tag{5.1}$$

Puisque p est irréductible et A est factoriel, alors p est premier. On trouve, alors, que l'idéal (p) est premier et, par la suite, le quotient $A/(p)$ est un anneau intègre. Comme résultat, la relation (5.1) implique que soit $\overline{a}(x) = \overline{0}$ ou $\overline{b}(x) = \overline{0}$. Mais ceci est impossible, car on en obtiendrait que p divise soit tous les coefficients de $a(x)$ ou ceux de $b(x)$, en contredisant l'hypothèse de primitivité de $a(x)$ ou celle de $b(x)$, respectivement. Ceci montre l'absurdité de l'hypothèse que $f(x)$ est imprimitif, en concluant la démonstration. □

On est prêt de prouver le résultat principal de cette section. On le divise en deux parties, en caractérisant d'abord les éléments irréductibles de $A[x]$ quand A est factoriel :

Lemme 5.17. *Soient A un anneau factoriel et K son corps des fractions. Les polynômes irréductibles de $A[x]$ sont :*

(a) les polynômes constants $f(x) = p$, où p est un élément irréductible de A ;

(b) les polynômes primitifs non-constants $f(x) \in A[x]$ tels que $f(x)$ est irréductible dans l'anneau $K[x]$.

Démonstration. Puisque A est intègre, on se rappelle que, selon l'exercice 2.2, les éléments inversibles de $A[x]$ sont les polynômes constants $f(x) = a$, où $a \in A^\times$. Donc, on polynôme constant $f(x) = c$ est réductible dans $A[x]$ s-si c est réductible dans A. Ceci montre la caractérisation affirmée de polynômes irréductibles constants.

Or, supposons que $f(x)$ est un polynôme irréductible et non-constant de $A[x]$. Montrons que $f(x)$ est primitif et irréductible dans $K[x]$.

Pour la primitivité de $f(x)$, on observe que si les coefficients de $f(x)$ étaient tous divisibles par un $d \in A \setminus (\{0\} \cup A^\times)$, alors on pourrait écrire $f(x) = d \cdot g(x)$, où $g(x) \in A[x]$ est non-constant. Donc, d et $g(x)$ sont d'élément non-inversibles de $A[x]$, ce qui contredit l'hypothèse que $f(x)$ est irréductible.

Puis, on montre que $f(x)$ est irréductible dans $K[x]$. Supposons au contraire que $f(x) = g(x)h(x)$ pour quelques $f(x), g(x) \in K[x]$. Selon le remarque 5.13, il existe deux polynômes primitifs $G(x), H(x) \in A[x]$ et des nombres $a, b, c, d \in A \setminus \{0\}$ tels que

$$g(x) = \frac{a}{b} \cdot G(x) \quad \text{et} \quad h(x) = \frac{c}{d} \cdot H(x).$$

Donc,

$$bd \cdot f(x) = ac \cdot G(x)H(x). \tag{5.2}$$

Puisque $f(x)$ est primitif, le nombre bd est un pcdg des coefficients du polynôme $bd \cdot f(x)$. D'autre côté, puisque G et H sont primitifs, le lemme de Gauss implique que $G(x)H(x)$ l'est aussi. On trouve alors ac est un pgcd des coefficients du polynôme $ac \cdot G(x)H(x)$. Par la suite, $bd \sim ac$, ce qui implique que $ac = u \cdot bd$ pour un $u \in A^\times$. On en déduit que $f(x) = u \cdot G(x)H(x)$. Mais on a supposé que f est irréductible dans $A[x]$. Donc, soit G est constant ou H l'est. Par conséquent, soit g est constant ou h l'est. Ceci montre l'irréductibilité de $f(x)$ dans $K[x]$.

Réciproquement, on montre que si $f(x) \in A[x]$ est non-constant, primitif est irréductible dans $K[x]$, alors il est également irréductible dans $A[x]$. En effet, si $f(x) = g(x)h(x)$ pour quelques $g(x), h(x) \in A[x]$, alors on a une factorisation de $f(x)$ dans $K[x]$. Par l'irréductibilité de $f(x)$ dans $K[x]$, il faut que soit $g(x)$ est constant ou $h(x)$ l'est. Sans perte de généralité, supposons que $g(x)$ est constant, soit $g(x) = a$. On trouve donc que $f(x) = a \cdot h(x)$. Par cette relation, il faut que a divise tous les coefficients de $f(x)$. Mais on a supposé que $f(x)$ est primitif, donc $a \in A^\times$. On a alors montré que $g(x) = a \in A^\times$, ce qui implique que $g(x)$ est inversible dans $A[x]$. Ceci conclut la démonstration de l'irréductibilité de $f(x)$ dans $A[x]$ et, donc, du lemme. □

Démonstration du théorème 5.14. Le lemme 5.17 caractérise les éléments irréductibles de $A[x]$. Il reste à montrer que $A[x]$ est factoriel.

Soit $f(x) \in A[x] \setminus (\{0\} \cup A^\times)$. Puisque $K[x]$ est factoriel, il existe quelques polynômes irréductibles $p_1(x), \ldots, p_m(x) \in K[x]$ tels que $f(x) = p_1(x) \cdots p_m(x)$ dans l'anneau $K[x]$. Selon le remarque 5.13, il existe quelques polynômes primitifs $P_1(x), \ldots, P_m(x) \in A[x]$ et quelques éléments $a_j, b_j \in A \setminus \{0\}$ tels que $p_j(x) = (a_j/b_j)P_j(x)$ pour tout j. En particulier, $p_j(x) \sim P_j(x)$ dans l'anneau $K[x]$, donc les polynômes $P_j(x)$ sont aussi irréductibles dans $K[x]$. Puisque ils sont aussi primitifs dans $A[x]$, ils sont irréductibles dans $A[x]$ selon le lemme 5.17. On trouve donc que

$$(b_1 \cdots b_n) \cdot f(x) = (a_1 \cdots a_n) \cdot P_1(x) \cdots P_m(x). \tag{5.3}$$

On montre que $b_1 \cdots b_n | a_1 \cdots a_n$ en ré-utilisant l'argument après l'équation (5.2) : puisque les polynômes P_j sont tous primitifs, le lemme de Gauss implique implique que $P_1 \cdots P_m$ est aussi primitif. En comparant les pgcds de deux côtés de (5.3), on en déduit que $(b_1 \cdots b_n) \cdot d \sim a_1 \cdots a_n$, où d est un pgcd de coefficients de f. Donc $a_1 \cdots a_n / b_1 \cdots = ud$ pour un $u \in A^\times$, et on a montré que $f(x) = ud \cdot P_1(x) \cdots P_m(x)$. En factorisant le nombre d en éléments irréductibles de A, on a montré que $f(x)$ peut se factoriser comme un produit d'éléments irréductibles de $A[x]$.

Il reste à montrer que la factorisation de $f(x)$ en éléments irréductibles de $A[x]$ est unique. Supposons que

$$f(x) = q_1 \cdots q_k \cdot P_1(x) \cdots P_m(x) = \tilde{q}_1 \cdots \tilde{q}_\ell \cdot \tilde{P}_1(x) \cdots \tilde{P}_n(x), \tag{5.4}$$

où $q_j, \tilde{q}_j$ sont d'éléments irréductibles de A, et $P_j, \tilde{P}_j$ sont de polynômes primitifs et non-constants de $A[x]$ qui sont irréductibles dans l'anneau $K[x]$. En réalisant la relation (5.4) comme une identité dans l'anneau factoriel $K[x]$, on trouve que $m = n$, ainsi que il existe une permutation $\sigma \in S_m$ telle que $\tilde{P}_j$ et $P_{\sigma(j)}$ sont associés dans l'anneau $K[x]$. Donc $\tilde{P}_j = (a_j/b_j)P_{\sigma(j)}$ pour quelques $a_j, b_j \in A \setminus \{0\}$. On en déduit que $b_j \tilde{P}_j = a_j P_j$. En comparant les pgcds de coefficients de deux côtés, et en utilisant l'hypothèse que $P_{\sigma(j)}$ et $\tilde{P}_j$ sont irréductibles, on trouve que $a_j \sim b_j$, c'est-à-dire $a_j = u_j b_j$ pour un $u_j \in A^\times$. Donc

$$\tilde{P}_j = u_j P_{\sigma(j)}, \tag{5.5}$$

ce qui implique que $\tilde{P}_j$ et $P_{\sigma(j)}$ sont associés dans l'anneau $A[x]$. De plus, en insérant (5.5) dans (5.4), on trouve que

$$q_1 \cdots q_k = u_1 \cdots u_m \cdot \tilde{q}_1 \cdots \tilde{q}_\ell.$$

Puisque A est factoriel, il faut que $k = \ell$ et il existe une permutation $\tau \in S_k$ telle que $\tilde{q}_j$ et $q_{\tau(j)}$ sont associés dans A pour tout j. Ceci conclut la démonstration que $A[x]$ est factoriel. □

5.3 Polynômes sur un anneau noetherien

Théorème 5.18 (théorème de la base de Hilbert)**.** *Si A est un anneau noetherien et unitaire, alors les anneaux polynomiaux $A[x_1, \ldots, x_n]$ sont tous noetheriens.*

Démonstration. Puisque $A[x,y] \cong (A[x])[y]$, il suffit de montrer le théorème quand $n = 1$.

Soit I un idéal de $A[x]$. On cherche un nombre fini de polynômes de $A[x]$ qui l'engendre. Pour $d \geq 0$, considérons

$$J_d := \{0\} \cup \{a \in A \setminus \{0\} : \exists f(x) \in A[x] \text{ de degré } d \text{ et de coefficient en tête égal à } a\}.$$

L'ensemble J_d est un idéal de A :

- Par définition, $0 \in J_d$, donc J_d est non-vide.
- Soit $a, b \in J_d$. On montre que $a + b \in J_d$. Si $a = 0$ ou $b = 0$, alors évidemment $a + b \in \{a, b\} \subset J_d$. Si $a, b \neq 0$ et $a + b = 0$, alors évidemment $a + b \in J_d$. Finalement, supposons que $a, b, a+b \neq 0$. Il existe alors $f(x), g(x) \in I$ tels que $f(x) = ax^d + \text{ppp}$ et $g(x) = bx^d + \text{ppp}$, où *ppp* veut dire qu'on ajoute une somme de *plus petites puissances de* x. Puisque I est un idéal, on a que $f(x)+g(x) \in I$. De plus, $f(x)+g(x) = (a+b)x^d + \text{ppp}$. On en déduit que $a + b \in J_d$ dans ce dernier cas aussi.
- Soit $a \in J_d$. On montre que $-a \in J_d$. Si $a = 0$, alors $-a = 0 \in J_d$. Si $a \neq 0$, alors il existe $f(x) = ax^d + \text{ppp} \in I$. Puisque I est un idéal, on a que $-f(x) \in I$. Mais $-f(x) = -ax^d + \text{ppp}$, donc $-a \in J_d$, comme affirmé.
- Soit $a \in J_d$ et $b \in A$. On montre que $ab, ba \in J_d$. On donne l'argument pour ab ; l'argument pour ba est similaire. Si $ab = 0$, alors $ab \in J_d$. Supposons que $ab \neq 0$. Puisque $a \in J_d$, il existe $f(x) \in I$ tel que $f(x) = ax^d + \text{ppp}$. Mais I est un idéal, donc $f(x)b \in I$. Puisque $f(x)b = ab + \text{ppp}$, on trouve que $ab \in J_d$.

Puisque on est dans un anneau noetheriens, il existe quelques $a_{d,1}, \ldots, a_{d,n_d} \in A \setminus \{0\}$ tels que

$$J_d = (a_{d,1}, \ldots, a_{d,n_d}).$$

Par la définition de J_d, il existe aussi quelques polynômes $f_{d,1}, \ldots, f_{d,n_d} \in I$ tels que

$$f_{d,j}(x) = a_{d,j}x^d + \text{ppp}.$$

Puis, considérons les réunions $K_d := \bigcup_{i=0}^{d} J_i$. C'est facile de vérifier qu'elles sont d'idéaux de A. De plus, $K_0 \subset K_1 \subset \cdots$. Puisque A est noetherien, le théorème 4.40 implique l'existence d'un entier $D \geq 0$ tel que $K_D = K_{D+1} = \cdots$. On affirme que les polynômes $f_{d,j}$ avec $0 \leq d \leq D$ et $1 \leq j \leq n_d$ engendrent I. Si

$$\tilde{I} := (\{f_{d,j} : 0 \leq d \leq D,\ 1 \leq j \leq n_d\}) \subset I,$$

il faut montrer que pour tout $f(x) \in I$, on a que $f(x) \in I_0$. On le montre par induction sur $\deg(f)$.

Quand $f = 0$, on a que $f \in I$. Quand $f(x) = a$ est constant, alors

$$a \in J_0 = (a_{0,1}, \ldots, a_{0,n_0}) = (f_{0,1}, \ldots, f_{0,n_0}) \subset \tilde{I}.$$

Supposons, maintenant, que $f(x) \in \tilde{I}$ pour chaque $f(x) \in I$ de degré $< n$, et considérons $f(x) \in I$ de degré $n \geq 1$. Si $f(x) = ax^n + \text{ppp}$, alors $a \in J_n$. Si $n > D$, on a donc que $a \in K_n = K_D$. En tout cas, $a \in K_m$ avec $m = \min\{n, D\}$. Par la suite,

$$a = \sum_{\substack{0 \leq d \leq m \\ 1 \leq j \leq n_d}} \lambda_{d,j} a_{d,j} \mu_{d,j}$$

pour quelques coefficients $\lambda_{d,j}, \mu_{d,j} \in A$. On observe alors que le polynôme

$$g(x) = f(x) - \sum_{\substack{0 \leq d \leq m \\ 1 \leq j \leq n_d}} \lambda_{d,j} f_{d,j}(x) \mu_{d,j} x^{n-d}$$

a degré $< n$. De plus, puisque $f(x), f_{d,j}(x) \in I$ et I est un idéal, on a que $g(x) \in \tilde{I}$ par l'hypothèse d'induction. Mais on a que $f(x) = g(x) + \sum_{\substack{0 \leq d \leq m \\ 1 \leq j \leq n_d}} \lambda_{d,j} f_{d,j}(x) \mu_{d,j} x^{n-d}$, et $g(x), f_{d,j}(x) \in \tilde{I}$ avec $d \leq m \leq D$. Par la suite, $f(x) \in \tilde{I}$. Ceci conclut la démonstration. □

Corollaire 5.19. *Si K est un corps, alors les anneaux polynomiaux $K[x_1, \ldots, x_n]$ sont tous noetheriens.*

Remarque 5.20. On remarque que, quand $n \geq 2$, les anneaux $K[x_1, \ldots, x_n]$ ne sont pas en général principaux. Par exemple, si $K = \mathbb{C}$ et $n = 2$, alors l'idéal (x_1, x_2) n'est pas principal.

5.4 Critères d'irréductibilité

Une question fondamentale à laquelle on va partiellement répondre à cette section est quand un polynôme donné est irréductible dans un anneau.

Soit A un anneau intègre. Si $f(x) = ax + b$ avec $a \in A \setminus \{0\}$ et $b \in A$, alors c'est facile de voir que $f(x)$ est irréductible s-si il est primitif. Alors, sur un corps, tous les polynômes linéaires sont irréductibles. C'est aussi facile de caractériser quels polynômes quadratiques et cubiques sont irréductibles sur un corps :

Proposition 5.21. *Soit K un corps et $f(x) \in K[x]$ de degré 2 ou 3. Alors $f(x)$ est irréductible dans $K[x]$ s-si il n'a pas de racines dans K.*

Démonstration. Si $f(\alpha) = 0$ pour un $\alpha \in K$, alors le lemme 5.1 implique que $f(x) = (x - \alpha)g(x)$ pour un $g(x) \in K[x]$. On a que $\deg(g) = \deg(f) - 1 \geq 1$, donc on trouve que $f(x)$ est réductible.

Réciproquement, si $f(x) = g(x)h(x)$ pour quelques $g(x), h(x) \in K[x]$ qui ne sont pas inversibles, il faut que $\deg(g), \deg(h) \geq 1$. Puisque $\deg(g) + \deg(h) = \deg(f) \in \{2, 3\}$, on trouve que soit $\deg(g) = 1$ ou $\deg(h) = 1$. Sans perte de généralité, supposons que $\deg(g) = 1$. Il existe alors $a \in K \setminus \{0\}$ et $b \in K$ tels que $g(x) = ax + b$. En particulier, $g(-b/a) = 0$, d'où $f(-b/a) = 0$. □

Exemple 5.22. On étudie l'irréductibilité de $f(x) = x^3 + 3x + 1$ dans $\mathbb{Z}[x]$. Puisque $\mathbb{Z}$ est factoriel et $f(x)$ primitif, le théorème 5.14 implique que $f(x)$ est irréductible dans $\mathbb{Z}[x]$ s-si il est irréductible dans $\mathbb{Q}[x]$. Selon la proposition 5.21, ceci est équivalente à l'existence d'un nombre rationnel a/b qui est une racine de $f(x)$, où on peut supposer que a et b sont copremiers. On a que

$$(a/b)^3 + 3(a/b) + 1 = 0 \quad \Longrightarrow \quad a^3 + 3ab^2 + b^3 = 0.$$

On a que $a | a^3 + 3ab^2$, donc il faut que $a | b^3$. Puisque a et b sont copremiers, il faut que $a = \pm 1$. De même, on a que $b | 3ab^2 + b^3$, donc $b | a^3$, et on en déduit que $b = \pm 1$. Par la suite,

les racines possibles de f sont les nombres ± 1. On vérifie directement que $f(\pm 1) \neq 0$, donc f est irréductible dans $\mathbb{Q}[x]$ et dans $\mathbb{Z}[x]$.

Un autre critère d'irréductibilité qui s'applique à de polynômes de tous les degrés est donné ci-dessous :

Proposition 5.23. *Soit A un anneau intègre et I un idéal propre de A. Soit $f(x) \in A[x]$ un polynôme primitif, de degré $n \geq 1$, et de coefficient en tête $c_n \in A \setminus I$.*

Si la réduction de $f(x)$ mod I ne peut pas s'écrire comme le produit de deux polynômes non-constants de degré $< n$ dans $(A/I)[x]$, alors $f(x)$ est irréductible dans $A[x]$.

Corollaire 5.24. *Soit A un anneau intègre et P un idéal premier de A. Soit $f(x) \in A[x]$ un polynôme unitaire non-constant. Si $f(x)$ est irréductible dans l'anneau $(A/P)[x]$, alors il est irréductible dans $A[x]$.*

Démonstration de la proposition 5.23. Supposons, au contraire, qu'il existe une factorisation non-triviale de $f(x)$ dans $A[x]$, soit $f(x) = a(x)b(x)$. Posons $k = \deg(a)$ et $\ell = \deg(b)$. Soient, aussi, a_k et b_ℓ les coefficients en tête de $a(x)$ et de $b(x)$.

Il faut que $k, \ell \geq 1$. En effet, si par exemple, on avait que $k = 0$, il fallait que a_k soit un diviseur commun des coefficients de $f(x)$. Puisque $f(x)$ est primitif, on aurait alors que $a_k \in A^\times$. Ceci est impossible, car on a supposé que $a(x) \notin A[x]^\times$. Le même argument exclut le cas où $\ell = 0$.

Puis, l'hypothèse que A est intègre implique que $k + \ell = n$ et que $c_n = a_k b_\ell$. Puisque $k, \ell \geq 1$, il faut que $k, \ell < n$. De plus, en utilisant le fait que $c_n \notin I$, on déduit que $a_k, b_\ell \notin I$. En particulier, si on réduit les polynômes mod I, on trouve que $\deg(\overline{f}) = \deg(f) = n$, $\deg(\overline{a}) = \deg(a) = k < n$ et $\deg(\overline{b}) = \deg(b) = \ell < n$. Ceci est impossible, car on a supposé que $f(x)$ n'est pas le produit de deux polynômes de degré $< n$ dans $(A/I)[x]$. □

Exemple 5.25. On étudie l'irréductibilité de $f(x) = x^3 + x + 1$ dans $\mathbb{Z}[x]$. On observe si on réduit $f(x)$ mod 2, alors $f(x)$ n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$. Donc, $f(x)$ est irréductible dans l'anneau $(\mathbb{Z}/2\mathbb{Z})[x]$ d'après la proposition 5.21. Le corollaire 5.23 implique que $f(x)$ est aussi irréductible dans $\mathbb{Z}[x]$.

Exemple 5.26. On étudie l'irréductibilité de $f(x, y) = x^2 + xy + 1$ dans $\mathbb{Z}[x, y]$. On a que $\mathbb{Z}[x, y] = (\mathbb{Z}[y])[x]$. On va appliquer le corollaire 5.24 avec $A = \mathbb{Z}[y]$ et $P = (y)$. On a que $f(x, y) \equiv x^2 + 1 \pmod{P}$. De plus, on a affirme que $x^2 + 1$ est irréductible dans $(A/P)[x]$. En effet, on a que

$$(A/P)[x] = (\mathbb{Z}[y]/(y))[x] \cong \mathbb{Z}[x].$$

En particulier, P est un idéal premier. De plus, on observe que $x^2 + 1$ est irréductible dans $\mathbb{Z}[x]$: puisque il est primitif, le théorème 5.14 implique qu'il suffit de montrer l'irréductibilité de $x^2 + 1$ dans $\mathbb{Q}[x]$. On la voit en appliquant la proposition 5.21 (évidemment, $x^2 + 1$ n'a pas de racines rationnelles).

Puisque $x^2 + 1$ est irréductible dans $(A/P)[x]$, $f(x, y)$ est irréductible dans $A[x] = \mathbb{Z}[x, y]$.

Théorème 5.27 (critère d'Eisenstein)**.** *Soient A un anneau intègre et P un idéal premier de A. Si $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ est tel que : $a_1, \ldots, a_{n-1} \in P$ et $a_0 \in P \setminus P^2$,*

alors $f(x)$ est irréductible dans $A[x]$.

Démonstration. Soit $f(x) = g(x)h(x)$, où $g(x) = b_0 + b_1x + \cdots + b_kx^k$ et $h(x) = c_0 + c_1x + \cdots + c_\ell x^\ell$ ne sont pas inversibles dans $A[x]$. On observe que $b_kc_\ell = 1$, donc $b_k, c_\ell \in A^\times$. En particulier, il faut que $k, \ell \geq 1$; sinon, $g(x)$ ou $h(x)$ serait inversible dans $A[x]$.

Puis, on remarque que $b_0c_0 = a_0 \in P \setminus P^2$. Puisque P est premier, il faut que soit $b_0 \in P$ ou $c_0 \in P$. Puisque $a_0 \notin P^2$, on ne peut pas avoir que b_0 et c_0 sont les deux dans P. Sans perte de généralité, supposons que $b_0 \in P$. On montrera que $b_j \in P$ pour tout j, ce qui contredit le fait que $b_k \in A^\times$.

On utilise induction sur j : supposons que $b_i \in P$ pour tous $i \in \{0, 1, \ldots, j-1\}$. Puisque $a_j \in P$ et $a_j = b_jc_0 + b_{j-1}c_1 + \cdots + b_0c_j$, où on a posé $c_i = 0$ pour $i > \ell$, on a que

$$b_jc_0 = a_j - b_{j-1}c_1 - \cdots - b_0c_j \in P$$

par l'hypothèse inductive et le fait que P est un idéal. Donc $b_j = (b_jc_0) \cdot c_0^{-1} \in P$, ce qui conclut la démonstration de l'étape inductive.

Comme on l'a expliqué, on est arrivé à une contradiction : on a que $b_k \in P$, mais $b_k \in A^\times$ et P est un idéal propre car il est premier. Ceci termine la démonstration du théorème. □

Corollaire 5.28. *Si p est premier, alors le polynôme cyclotomique*

$$\Phi_p(x) := 1 + x + \cdots + x^{p-1}$$

est irréductible dans $\mathbb{Q}[x]$.

Démonstration. Puisque $\Phi_p(x)$ est unitaire et $\mathbb{Z}$ est intègre avec corps des fractions $\mathbb{Q}$, le théorème 5.14 implique qu'il suffit de montrer que $\Phi_p(x)$ est irréductible dans $\mathbb{Z}[x]$.

Observons que $(x-1)\Phi_p(x) = x^p - 1$. Cette observation nous motive de faire un changement de variables : on remplace x par $x+1$. Clairement, le polynôme $\Phi_p(x)$ est irréductible dans $\mathbb{Z}[x]$ s-si le polynôme $\Phi_p(x+1)$ l'est. Mais, on a que

$$(x+1)^p - 1 = \sum_{j=0}^{p} \binom{p}{j} x^j - 1 = \sum_{j=1}^{p} \binom{p}{j} x^j.$$

Donc

$$\Phi_p(x+1) = \sum_{j=1}^{p} \binom{p}{j} x^{j-1} = 1 + \sum_{i=0}^{p-2} \binom{p}{i+1} x^i.$$

On applique le théorème 5.27 avec $P = (p)$: on a que $p \big| \binom{p}{i+1}$ pour $0 \leq i \leq p-2$. Effectivement, les nombres $\binom{p}{i+1}$ sont d'entiers. De plus, on a que

$$\binom{p}{i+1} = \frac{p!}{(i+1)!(p-i-1)!}.$$

On a que $p | p!$ et que $p \nmid (i+1)!(p-i-1)!$ car $1 \leq i+1, p-i-1 \leq p-1$. Donc $p \big| \binom{p}{i+1}$ comme affirmé. Finalement, quand $i = 0$, on a que $p^2 \nmid \binom{p}{0+1} = p$. Le théorème 5.27 peut alors être appliqué et conclure la démonstration du corollaire. □

5.5 Exercices

EXERCICE 5.1. Soit K un corps. Pour chaque polynôme $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, définissons sa **dérivée** comme étant le polynôme

$$f'(x) := a_1 + 2a_2x + \cdots + na_nx^{n-1} \in K[x],$$

où ma veut dire $m \times a = \underbrace{a + \cdots + a}_{m \text{ fois}}$, comme on l'a défini dans l'exemple 4.29.

(a) Si $f(x), g(x) \in K[x]$, alors montrez que $(f+g)'(x) = f'(x)+g'(x)$, ainsi que $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

(b) Soit $f(x) \in K[x]$ de degré $n \geq 1$, et soit $c = \text{car}(K)$ (on sait que soit $c = 0$ ou c est premier). Si $c = 0$, ou si c est positive et elle ne divise pas n, alors montrez que $\deg(f') = n - 1$.

(c) Soit $f(x) \in K[x] \setminus \{0\}$ et $\alpha \in K$ une racine de $f(x)$. Montrez que α est une racine **multiple** de $f(x)$ (i.e. de multiplicité ≥ 2) s-si $f'(\alpha) = 0$.

(d) Soit $f(x) \in K[x] \setminus \{0\}$. Si $f(x)$ et $f'(x)$ sont copremiers dans $K[x]$, alors montrez que toutes les racines de $f(x)$ dans K sont **simples** (i.e. de multiplicité 1). Plus généralement, montrez que si L est une extension de K, alors toutes les racines de $f(x)$ dans L sont aussi simples.

(e) Supposons que $\text{car}(K) = 0$. Si L est une extension de K et $f(x)$ est un polynôme irréductible de $K[x]$, alors montrez que toutes les racines de $f(x)$ dans L sont simples.

EXERCICE 5.2. Soit K un corps, et soit $\text{Aut}(K)$ l'ensemble d'isomorphismes $\sigma : K \to K$.

(a) Montrez que si on muni $\text{Aut}(K)$ de l'opération de la composition de fonctions, il devient un groupe.

(b) Si $K \subset \mathbb{C}$ et $\sigma \in \text{Aut}(K)$, alors $\sigma(x) = x$ pour tout $x \in Q$.

(c) Supposons que $K \subset \mathbb{C}$. Si $f(x) \in \mathbb{Q}[x]$ et $\alpha \in K$ est une racine de $f(x)$, alors montrez que $\sigma(\alpha)$ est aussi une racine de $f(x)$.

(d) Supposons que $\text{car}(K) = 0$. Soit $P(x)$ est un polynôme irréductible de $\mathbb{Q}[x]$. L'exercice 5.1(e) implique que toutes les racines de $P(x)$ dans K sont simples. Soit $\mathbb{Z}$ leur ensemble. Si $\sigma \in \text{Aut}(K)$, montrez que $\tilde{\sigma} : Z \to Z$, définie par $\tilde{\sigma}(\alpha) := \sigma(\alpha)$, est une bijection (i.e. une permutation des éléments de Z). Déduisez que $\text{Aut}(K)$ est isomorphe à un sous-ensemble des permutations de l'ensemble Z.

(e) Déterminez $\text{Aut}(K)$ quand $K = \mathbb{Q}(i)$, $K = \mathbb{Q}(\sqrt{2})$ et $K = \mathbb{Q}(2^{1/3})$.

EXERCICE 5.3. Soit K un sous-corps de $\mathbb{C}$, soit α un nombre complexe qui est algébrique sur K et soit $f(x) \in K[x]$ le polynôme minimal de α sur K. (Voir l'exercice 3.2 pour les définitions.)

(a) Montrez que $K \supset \mathbb{Q}$.

(b) Si $\sigma : \mathbb{C} \to \mathbb{C}$ est un morphisme d'anneaux tel que $\sigma\big|_K = \text{id}\big|_K$, alors le polynôme minimal de $\sigma(\alpha)$ sur K est aussi $f(x)$.

(c) Trouvez le polynôme minimal du nombre $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$ et sur $\mathbb{Q}(\sqrt{2})$.

EXERCICE 5.4. Soit p un nombre premier, $\zeta = e^{2\pi i/p}$ et $K = \mathbb{Q}(\zeta)$.

(a) Montrez que le polynôme minimal de ζ sur $\mathbb{Q}$ est le polynôme cyclotomique $\Phi_p(x)$.

(b) Montrez que si $f(\zeta) = g(\zeta)$ pour quelques $f(x), g(x) \in \mathbb{Q}[x]$, alors $f(\zeta^m) = g(\zeta^m)$. [*Indice :* exercice 2.11(b).]

(c) Pour $m \in \mathbb{Z}$, $p \nmid m$, définissons $\sigma_m : K \to K$ par $\sigma_m(f(\zeta)) = f(\zeta^m)$, qui est bien définie par la partie (b). Montrez que $\sigma_m \in \mathrm{Aut}(K)$, ainsi que $\sigma_{m+p} = \sigma_m$.

(d) Observons que si $\alpha \in \mathbb{Q}$, alors $\sigma_m(\alpha) = \alpha$ pour tout $m \in \mathbb{Z}$, $p \nmid m$. Montrez que l'inverse est aussi vrai, comme ci-dessus :

(i) Comme on a vu à l'exercice 3.4(b), il existe une representation unique de α comme $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$. En posant $a_{p-1} = 0$, on a que

$$\sigma_m(\alpha) = \sum_{j=0}^{p-1} a_j e^{2\pi i m j/p}$$

pour chaque $m \in \{0, 1, \ldots, p-1\}$. Montrez la formule de l'inversion de Fourier

$$a_j = \frac{1}{p} \sum_{m=0}^{p-1} \sigma_m(\alpha) e^{-2\pi i m j/p} \quad (0 \le j \le p-1).$$

[*Indice :* on a que $1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{(p-1)j} = 0$ si $p \nmid j$.]

(ii) Déduisez que si $\sigma_m(\alpha) = 0$ pour tout $m \in \{1, \ldots, p-1\}$, alors $a_j = 0$ pour $j = 1, \ldots, p-1$. Donc $\alpha \in \mathbb{Q}$.

(e) Définissons $N : K \to K$ par

$$N(\alpha) := \prod_{j=0}^{p-1} \sigma_j(\alpha).$$

Montrez que :

(i) $N(\alpha\beta) = N(\alpha)N(\beta)$ pour tous $\alpha, \beta \in K$;

(ii) $N(\alpha) = 0$ s-si $\alpha = 0$;

(iii) $N(\alpha) \in \mathbb{Q}$ pour tout $\alpha \in K$. [*Indice :* selon la partie (d), il suffit de montrer que $\sigma_m(N(\alpha)) = N(\alpha)$ pour tout m.]

(f) Montrez que :

(i) si $\alpha \in A := \mathbb{Z}[\zeta]$, alors $N(\alpha) \in \mathbb{Z}$;

(ii) $\alpha \in A^\times$ s-si $N(\alpha) = \pm 1$;

(iii) si $N(\alpha)$ est premier, alors α est irréductible dans A.

(g) Montrez que $\zeta - 1$ est irréductible dans A.

(h) Montrez que les nombres $1 + \zeta + \cdots + \zeta^m$, $0 \le m \le p-2$, sont d'éléments inversibles de l'anneau $\mathbb{Z}[\zeta]$. [*Indice :* observez que $1 + \zeta + \cdots + \zeta^m = (\zeta^{m+1} - 1)/(\zeta - 1)$.]

(i) La partie (f) implique que $\zeta^j - 1 \sim \zeta - 1$ pour $j \in \{1, 2, \ldots, p-1\}$. Déduisez que $p = u \cdot (\zeta - 1)^{p-1}$, où u est un élément inversible de A.

EXERCICE 5.5 (ex. 4, p. 306). Soit $A = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$, c'est-à-dire, A est l'ensemble des polynômes avec coefficients rationnels dont le terme constant est un nombre entier. Montrez que :

(a) A est un anneau intègre dont les éléments inversibles sont ± 1.

(b) les éléments irréductibles de A sont $\pm p$, où p est un nombre premier dans $\mathbb{Z}$, et les polynômes $f(x)$ qui sont irréductibles dans $\mathbb{Q}[x]$ et dont le terme constant est égal à ± 1. Montrez aussi que si $a \in A$ est irréductible, alors (a) est un idéal premier de A.

(c) x ne peut pas être écrit comme un produit d'irréductibles dans A (en particulier, x n'est pas irréductible) et concluez que A n'est pas un anneau factoriel.

(d) l'idéal (x) n'est pas premier et décrivez l'anneau quotient $A/(x)$.

EXERCICE 5.6 (ex. 2, p. 311). Montrez que les polynômes suivants sont irréductibles sur $\mathbb{Z}[x]$:

(a) $x^4 - 4x^3 + 6$

(b) $x^6 + 30x^5 - 15x^3 + 6x - 120$

(c) $x^4 + 4x^3 + 6x^2 + 2x + 1$ [*Indice* : remplacez x avec $x - 1$.]

(d) $((x+2)^p - 2^p)/x$, où p est nombre premier impair.

EXERCICE 5.7 (ex. 14, p. 312). Factorisez les polynômes $x^8 - 1$ et $x^6 - 1$ en produit de polynômes irréductibles dans les anneaux suivants :

(a) $\mathbb{Z}[x]$,

(b) $(\mathbb{Z}/2\mathbb{Z})[x]$,

(c) $(\mathbb{Z}/3\mathbb{Z})[x]$.

EXERCICE 5.8.

(a) (ex. 13, p. 312) Montrez que le polynôme $x^3 + nx + 2$ est irréductible dans $\mathbb{Z}[x]$ pour tous les entiers $n \in \mathbb{Z} \setminus \{1, -3, -5\}$.

(b) (ex. 12, p. 312) Montrez que le polynôme $x^2 + y^2 - 1$ est irréductible dans $\mathbb{Q}[x, y]$.

EXERCICE 5.9.

(a) (ex. 9, p. 311) Montrez que le polynôme $p(x) = x^2 - \sqrt{2}$ est irréductible sur $A = \mathbb{Z}[\sqrt{2}]$ [*Indice* : rappelez que $\mathbb{Z}[\sqrt{2}]$ est un anneau euclidien d'après l'exercice 2(c) du TP du 27 février.]

(b) Montrez que
$$\mathbb{Z}[\sqrt[4]{2}] = \{a + b2^{1/4} + c2^{1/2} + d2^{3/4} : a, b, c, d \in \mathbb{Z}\}$$
et que
$$A[x]/(x^2 - \sqrt{2}) \cong \mathbb{Z}[\sqrt[4]{2}].$$
[*Indice* : observez que $\mathbb{Z}[\sqrt[4]{2}] = A[\sqrt[4]{2}] = \{a + b\sqrt[4]{2} : a, b \in A\}$.]

EXERCICE 5.10.

(a) (ex. 4, p. 311) Montrez que le polynôme $(x-1)(x-2)\cdots(x-n) - 1$ est irréductible sur $\mathbb{Z}[x]$ pour tout $n \geq 1$.

(b) (ex. 5, p. 311) Montrez que le polynôme $(x-1)(x-2)\cdots(x-n)+1$ est irréductible sur $\mathbb{Z}[x]$ pour tout $n \geq 1$, $n \neq 4$, et réductible pour $n = 4$.

Deuxième partie

Modules

Chapitre 6

Lexique de modules

6.1 Définitions et exemples de base

Dans l'algèbre linéaire, on étudie les espaces linéaires. On se rappelle de leur définition :

Définition 6.1. Soit K un corps et V un ensemble. On dit que V est un **espace vectoriel sur** K si :

(a) V est muni d'une opération binaire $+$ qui le rend un groupe abelien ;

(b) K agit à gauche à V d'une façon respectante les structures algébriques de K et de V. Plus précisement, il existe une opération $\cdot : K \times V \to V$ appelée **produit interne** telle que :

(i) $1 \cdot v = v$ pour tout $v \in V$;

(ii) $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$ pour tous $\lambda \in K$ et $v, w \in V$;

(iii) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot w$ pour tous $\lambda, \mu \in K$ et $v \in V$, où $\lambda + \mu$ dénote la somme de λ et de μ dans K ;

(iv) $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$ pour tous $\lambda, \mu \in K$ et $v \in V$, où $\lambda \cdot \mu$ dénote le produit de λ et de μ dans K.

Les modules sont tout simplement une généralisation des espaces vectoriels, où on permet l'ensemble de scalaires K d'être un anneau arbitraire :

Définition 6.2. Soit A un anneau et M un ensemble. On dit que M est un A**-module** si :

(a) M est muni d'une opération binaire $+$ qui le rend un groupe abelien ;

(b) il existe une opération $\cdot : A \times M \to M$ appelée **produit interne** telle que : De plus, cette opération a les propriétés suivantes :

(i) si A est unitaire, alors $1 \cdot m = m$ pour tout $m \in M$;

(ii) $a \cdot (m + n) = a \cdot m + a \cdot n$ pour tous $a \in A$ et $m, n \in M$;

(iii) $(a + b) \cdot m = a \cdot m + b \cdot m$ pour tous $a, b \in A$ et $m \in M$, où $a + b$ dénote la somme de a et de b dans $A.$;

(iv) $(a \cdot b) \cdot m = a \cdot (b \cdot m)$ pour tous $a, b \in A$ et $m \in M$, où $a \cdot b$ dénote le produit de a et de b dans A.

Espaces vectoriels	Modules
V espace vectoriel sur K	M un A-module
$\lambda \in K$ est un scalaire	$a \in A$ est un scalaire
W est un sous-espace de V	N est un sous-module de M
V/W est un espace-quotient	M/N est un module-quotient
V a dimension finie	M est de type fini
V possède une base B	M est libre sur S
V a dimension n	M a rang n
$V = \mathrm{Span}_K(S)$	$M = (S)$

Lemme 6.3. *Soit M un A-module.*

(a) Pour tout $m \in M$, on a que

$$0_A \cdot m = 0_M.$$

(b) Pour tout $a \in A$, on a que

$$a \cdot 0_M = 0_M.$$

(c) Pour tout $a \in A$ et tout $m \in M$, on a que

$$(-a) \cdot m = -(a \cdot m) = a \cdot (-m)$$

et que

$$(-a) \cdot (-m) = a \cdot m.$$

(d) Si A est unitaire et $a \in A^\times$, alors

$$a \cdot m = 0_M \quad \Longleftrightarrow \quad m = 0_M.$$

Démonstration. Exercise. □

Corollaire 6.4. *Soit V est un espace vectoriel sur K. Si $\lambda \in K$ et $v \in V$, alors*

$$\lambda \cdot v = 0 \quad \Longrightarrow \quad \lambda = 0 \text{ ou } v = 0.$$

Le corollaire 6.4 n'est vrai en général pour les modules, ce qui est une de raisons principales que la théorie des modules est beaucoup plus compliquée que la théorie des espaces vectoriels.

Exemple 6.5. Si A est un anneau, alors

$$A^n = \underbrace{A \times \cdots \times A}_{n \text{ fois}} = \{(a_1, \ldots, a_n) : a_j \in A \ \forall j\}$$

est un A-module avec produit scalaire défini par

$$a \cdot (a_1, \ldots, a_n) := (aa_1, \ldots, aa_n).$$

Comme on va le voir plus tard, A^n est le module libre sur A de rang n.

De façon plus générale, si $(M_i)_{i\in I}$ est une famille de A-modules, alors leur produit directe

$$\prod_{i\in I} M_i := \{(m_i)_{i\in I} : m_i \in M_i \ \forall i \in I\}$$

est aussi un A-module.

Exemple 6.6. Si A est un anneau et B est un sous-anneau de A, alors A est un B-module dont le produit scalaire est la multiplication de A.

Par exemple, $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module. Comme on va le voir, $\mathbb{Z}[i]$ est *isomorphe* à $\mathbb{Z}^2$ comme un $\mathbb{Z}$-module.

Exemple 6.7. Si $(G,+)$ est un groupe abelien, alors c'est facile de vérifier que l'opération

$$n \cdot g := \begin{cases} \underbrace{g+\cdots+g}_{n \text{ fois}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ -(\underbrace{g+\cdots+g}_{|n| \text{ fois}}) & \text{si } n < 0, \end{cases} \tag{6.1}$$

rend G un $\mathbb{Z}$-module.

Vice versa, si G est un $\mathbb{Z}$-module, alors il est un groupe abelien par définition. De plus, son produit scalaire est nécessairement donné par (6.1). En effet, on a que

$$2 \cdot g = (1+1) \cdot g = 1 \cdot g + 1 \cdot g = g + g.$$

De façon inductive, on peut facilement montrer que

$$n \cdot g = \underbrace{g+\cdots+g}_{n \text{ fois}}.$$

Finalement, si $n < 0$, alors

$$n \cdot g + |n| \cdot g = (n + |n|) \cdot g = 0 \cdot g = 0$$

d'après le lemme 6.3(a). Donc, on a que

$$n \cdot g = -(|n| \cdot g) = -(\underbrace{g+\cdots+g}_{|n| \text{ fois}}).$$

On voit alors que les $\mathbb{Z}$-modules sont en correspondence avec les groupes abeliens.

Exemple 6.8. Soit V un espace vectoriel sur le corps K, et soit $T : V \to V$ une application linéaire. On peut utiliser T pour donner à V la structure d'un $K[x]$-module. Si $T^n : V \to V$ est la n-ième itération de T, c'est-à-dire $T^2(v) = T(T(v))$, $T^3(v) = T(T(T(v)))$, etc, alors définissons

$$x^n \cdot v := T^n(v)$$

et, plus généralement,

$$(a_0 + a_1x + \cdots + a_nx^n) \cdot v := a_0v + a_1T(v) + \cdots + a_nT^n(v). \tag{6.2}$$

C'est facile de vérifier que cette opération rend T un $K[x]$-module.

Vice versa, si V est un $K[x]$-module, alors il est obtenu de la façon précédente. En effet, puisque K est un sous-anneau de $K[x]$, il faut que V soit un K-module aussi, c'est-à-dire un espace vectoriel sur K. De plus, définissons $T : V \to V$ par $T(v) := x \cdot v$. Clairement, T est une application linéaire. De plus, on a que

$$x^2 \cdot v = (x \cdot x) \cdot v = x \cdot (x \cdot v) = x \cdot T(v) = T(T(v)) = T^2(v).$$

En général, on a que $x^n \cdot v = T^n(v)$. Donc, la relation (6.2) décrit l'action de $K[x]$ sur V, comme on l'affirmé.

On voit alors que les $K[x]$-modules sont en correspondence avec les K-espaces vectoriels muni d'une application linéaire $T : V \to V$.

Les exemples 6.7 et 6.8 sont fondamentaux. Ils nous permettent d'étudier les groupes abeliens et l'action d'une application linéaire sur un espace vectoriel du même point de vue, en étudiant les modules. De plus, on observe que les anneaux $\mathbb{Z}$ et $K[x]$, où K est un corps, sont les deux euclidients, donc principaux. Comme on va le voir plus tard, c'est possible de déterminer complètement la structure des modules (de type fini) sur un anneau principal.

6.2 Sous-modules et modules-quotients

Naturellement, il existe la notion d'un sous-module :

Définition 6.9. Soient M un A-module et $N \subset M$. On dit que N est un **sous-module** de M si la restriction du produit scalaire sur N le rend un A-module. Comme habituellement, ceci est équivalente aux propriétés suivantes :

(a) $N \neq \emptyset$;
(b) $n_1 - n_2 \in N$ pour tous $n_1, n_2 \in N$;
(c) $a \cdot n \in N$ pour tout $a \in A$ et tout $n \in N$.

Remarque 6.10. Un anneau A est évidemment un A-module. Ses sous-modules sont les idéaux de A.

Si M est un A-module et N est sous-module, alors $(N, +) < (M, +)$. En particulier, on peut définir leur quotient M/N. De plus, on peut définir un produit scalaire sur M/N par

$$a \cdot \overline{m} := \overline{a \cdot m}.$$

Il est bien défini, car si $m_1 \equiv m_2 \pmod N$, on a que $m_1 - m_2 \in N$, d'où $a(m_1 - m_2) \in N$. Puisque $a(m_1 - m_2) = am_1 - am_2$, on trouve que $am_1 \equiv am_2 \pmod N$.

6.3 Applications linéaires et matrices

Définition 6.11. Si M et N sont de A-modules, alors une application $\phi : M \to N$ est appelée **linéaire** si :

(a) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$ pour tous $m_1, m_2 \in M$;
(b) $\phi(am) = a\phi(m)$ pour tous $a \in A$, $m \in M$.

Si A est unitaire, ces propriétés sont équivalentes à

$$\phi(a_1 m_1 + a_2 m_2) = a_1\phi(m_1) + a_2\phi(m_2)$$

pour tous $a_1, a_2 \in A$ et tous $m_1, m_2 \in M$.

Si ϕ est bijective, on l'appelle un **isomorphisme** de A-modules, on dit que M et N sont **isomorphes** comme A-modules, et on écrit $M \cong N$.

Évidemment, une application linéaire est un morphisme entre les groupes additifs $(M, +)$ et $(N, +)$. Son noyau $\ker(\phi)$ joue, comme habituellement, un rôle important. Il est un sous-module de M. D'autre côté, l'image de ϕ est un sous-module de N.

L'ensemble de toutes les applications linéaires entre M et N est dénoté par

$$\mathcal{L}(M, N) = \{\phi : M \to N,\ \phi \text{ application linéaire}\}.$$

(Attention : dans la literature anglaise, cet ensemble est souvent dénoté par $\mathrm{Hom}_A(M, N)$.)

Si $\phi, \psi \in \mathcal{L}(M, N)$, alors on peut définir leur somme $\phi + \psi : M \to N$ par $(\phi + \psi)(m) := \phi(m) + \psi(m)$. Cette opération rend $\mathcal{L}(M, N)$ un groupe abelien. En fait, $\mathcal{L}(M, N)$ est un A-module : si $a \in A$ et $\phi \in \mathcal{L}(M, N)$, alors définissons $a\phi$ par $(a\phi)(m) := a \cdot \phi(m)$.

Exemple 6.12. Si $M_1, \ldots, M_n$ sont de A-modules, alors les applications

$$\begin{aligned} \pi_j : M_1 \times \cdots \times M_n &\longrightarrow M_j \\ (m_1, \ldots, m_n) &\longrightarrow m_j, \end{aligned}$$

sont d'applications linéaires. La fonction π_j est appelée la **projection au j-ième cordonné**.

Exemple 6.13. Soit A un anneau unitaire et soit $M_{n\times m}(A)$ l'ensemble des matrices $m \times n$ aux coefficients dans A. Quand $m = n$, on écrit simplement $M_n(A)$.

Si $C = (c_{i,j})_{1\le i\le n, 1\le j\le m}$, alors on peut définir l'application linéaire

$$\phi((a_1, \ldots, a_m)) = \left(\sum_{j=1}^{m} c_{1,j}a_j, \ldots, \sum_{j=1}^{m} c_{n,j}a_j \right).$$

En notation matricielle, et en écrivant les éléments de A^m et de A^n comme vecteurs-colonnes, on a que

$$\phi\left(\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}\right) = C \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Vice versa, supposons que $\phi : A^m \to A^n$ est une application linéaire. Considérons la base standard de A^m

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad e_m = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{6.3}$$

Donc

$$\phi\left(\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}\right) = \phi(a_1 e_1 + a_2 e_2 + \cdots + a_m e_m) = a_1\phi(e_1) + \cdots + a_m\phi(e_m).$$

Si on pose

$$\phi(e_j) = \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix},$$

alors on trouve que

$$\phi\left(\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}\right) = \sum_{j=1}^{m} a_j \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{n,j} \end{pmatrix} = C \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix},$$

où on l'a posé $C = (c_{i,j})_{1 \le i \le n,\, 1 \le j \le m}$.

On voit, alors, que les applications linéaires de A^m à A^n sont en correspondence avec les matrices $n \times m$ ayant coefficients dans A. Plus précisement, on a que

$$\mathcal{L}(A^m, A^n) \cong M_{n\times m}(A)$$

comme A-modules.

Dans l'exemple précédent, les éléments de $\mathcal{L}(M, N)$ sont en correspondence avec de matrices. On sait comment multiplier deux matrices (de taille approprié). Cette opération se généralise aux opérations linéaires : si $\phi \in \mathcal{L}(M, N)$ et $\psi \in \mathcal{L}(N, K)$, alors leur composition $\psi \cdot \phi$ est une application linéaire de M à K.

En prenant $K = N = M$, on voit qu'on peut définir une opération multiplicative dans $\mathcal{L}(M, M)$ qui le rend un anneau. Pour cette raison, on appelle $\mathcal{L}(M, M)$ l'**anneau d'endomorphismes** de M et le dénote par

$$\mathrm{End}(M) = \{\phi : M \to M, \phi \text{ application linéaire}\}.$$

Les éléments inversibles de $\mathrm{End}(M)$, c'est-à-dire les applications linéaires biunivoques $\phi : M \to M$, sont appelées les **automorphismes** de M. On dénote leur ensemble par

$$\mathrm{Aut}(M) := \mathrm{End}(M)^\times.$$

C'est un groupe par rapport à l'opération $\circ$.

Exemple 6.14. Si $A = \mathbb{R}$ et $M = \mathbb{R}^n$, alors $\mathrm{End}(M) \cong M_n(\mathbb{R})$ et $\mathrm{Aut}(M) \cong \mathrm{GL}_n(\mathbb{R})$.

Exemple 6.15. Si $A = \mathbb{Z}$ et $M = \mathbb{Z}^n$, alors $\mathrm{End}(M) \cong M_n(\mathbb{Z})$ et

$$\mathrm{Aut}(M) \cong \{B \in M_n(\mathbb{Z}) : \det(B) = \pm 1\} = \mathrm{SL}_n(\mathbb{Z}) \cup (B_0 \cdot \mathrm{SL}_n(\mathbb{Z})),$$

où B_0 est un élément fixé de $M_n(\mathbb{Z})$ avec $\det(B_0) = -1$. Pour voir la deuxième affirmation, on observe que si $AB = I_n$ avec $A, B \in M_n(\mathbb{Z})$, où I_n dénote la matrice-identité $n \times n$, alors $\det(AB) = 1$. Par la suite, $\det(A)\det(B) = 1$, d'où on déduit que $\det(A) = \det(B) = \pm 1$.

Exemple 6.16. Dans le cours de l'algèbre linéaire, on voit la notion de deux matrices **semblables**. On peut généraliser cette notion dans n'importe quel anneau unitaire A : si $C, D \in M_n(A)$, alors on dit que C et D sont semblables quand il existe $P \in M_n(A)^\times \cong \mathrm{Aut}(A^n)$ tel que

$$D = P^{-1} \cdot C \cdot P.$$

On va motiver cette notion en montrant que deux telles matrices proviennent nécessairement de la représentation d'une application linéaire donnée.

Pour simplicité, on travaille sur un corps K. Soit V un espace vectoriel sur K de dimension finie n, et soit $\phi : V \to V$ une application linéaire. Fixons deux bases de V, soient

$$\mathcal{S} = \{v_1, \ldots, v_n\} \quad \text{et} \quad \mathcal{T} = \{w_1, \ldots, w_n\}.$$

Si $v \in V$, alors il a deux représentations : il existe coefficients $\lambda_1, \ldots, \lambda_n$ et $\mu_1, \ldots, \mu_n \in K$ tels que

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 w_1 + \cdots + \mu_n w_n.$$

On dénote ces relations par

$$v = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}_{\mathcal{S}} = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix}_{\mathcal{T}}.$$

Puisque on a deux bases, on peut alors associer deux matrices à l'application ϕ. En travaillant avec la base $\mathcal{S}$, on construit la matrice $C = (c_{i,j})_{1 \le i,j \le n} \in M_n(K)$ par les relations

$$\phi(v_j) = \sum_{k=1}^{n} c_{j,k} v_k = \begin{pmatrix} c_{j,1} \\ c_{j,2} \\ \vdots \\ c_{j,n} \end{pmatrix}_{\mathcal{S}},$$

pour que

$$\phi\left(\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_n\end{pmatrix}_{\mathcal{S}}\right) = C\cdot\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_n\end{pmatrix}_{\mathcal{S}}.$$

D'autre côté, en travaillant avec la base $\mathcal{T}$, on construit la matrice $D=(d_{i,j})_{1\leq i,j\leq n}\in M_n(K)$ par les relations

$$\phi(w_j)=\sum_{k=1}^{n} d_{j,k}w_k=\begin{pmatrix}d_{j,1}\\ d_{j,2}\\ \vdots\\ d_{j,n}\end{pmatrix}_{\mathcal{T}},$$

pour que

$$\phi\left(\begin{pmatrix}\mu_1\\ \mu_2\\ \vdots\\ \mu_n\end{pmatrix}_{\mathcal{S}}\right) = D\cdot\begin{pmatrix}\mu_1\\ \mu_2\\ \vdots\\ \mu_n\end{pmatrix}_{\mathcal{T}}.$$

On veut déterminer D en termes de C. On observe qu'il existe des coefficients $p_{k,\ell}$ tels que

$$v_k=\sum_{\ell=1}^{n} p_{k,\ell}w_\ell.$$

D'autre côté, il existe des coefficients $q_{k,\ell}$ tels que

$$w_k=\sum_{\ell=1}^{n} q_{k,\ell}v_\ell.$$

On a que

$$v_k=\sum_{\ell=1}^{n} p_{k,\ell}w_\ell=\sum_{\ell=1}^{n} p_{k,\ell}\sum_{j=1}^{n} q_{\ell,j}v_j=\sum_{j=1}^{n}\left(\sum_{\ell=1}^{n} p_{k,\ell}q_{\ell,j}\right)v_j.$$

Si on pose $P=(p_{i,j})_{1\leq i,j\leq n}$ et $Q=(q_{i,j})_{1\leq i,j\leq n}$, alors la relation ci-dessus implique que $PQ=I_n$. De même, on peut aussi montrer que $QP=I_n$, c'est-à-dire que $Q=P^{-1}$.

Or, on a que

$$\begin{aligned}\phi(w_j)=\phi\left(\sum_{k=1}^{n} q_{j,k}v_k\right) &= \sum_{k=1}^{n} q_{j,k}\phi(v_k)\\ &= \sum_{k=1}^{n} q_{j,k}\sum_{\ell=1}^{n} c_{k,\ell}v_\ell\\ &= \sum_{k=1}^{n} q_{j,k}\sum_{\ell=1}^{n} c_{k,\ell}\sum_{m=1}^{n} p_{\ell,m}w_m\end{aligned}$$

$$= \sum_{m=1}^{n} \left(\sum_{k=1}^{n} q_{j,k} \sum_{\ell=1}^{n} q_{j,k} c_{k,\ell} p_{\ell,m} \right) w_m.$$

On en déduit que

$$d_{j,m} = \sum_{k=1}^{n} q_{j,k} \sum_{\ell=1}^{n} q_{j,k} c_{k,\ell} p_{\ell,m},$$

d'où on trouve que

$$D = P^{-1}CP,$$

c'est-à-dire C et D sont semblables.

Vice versa, supposons que $D = P^{-1}CP$. Considérons l'espace vectoriel K^n avec la base standard $e_1, \ldots, e_n$, définie par (6.3). Définissons l'application linéaire $\phi : K^n \to K^n$ par

$$\phi\left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}\right) = C \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

On définit, aussi, les vecteurs

$$\varepsilon_k = \sum_{\ell=1}^{n} q_{k,\ell} e_\ell,$$

où $q_{k,\ell}$ sont les coefficients de P^{-1}.

C'est facile de vérifier que les vecteurs $\varepsilon_1, \ldots, \varepsilon_n$ forment une base de K^n, et que la matrice de ϕ par rapport à cette base est $D = P^{-1}CP$. On laisse les détails de cette démonstration aux lecteurs.

On voit alors que deux matrices $C, D \in M_n(K)$ sont semblables s-si elles définissent la même application linéaire par rapport à deux bases différentes (qui sont reliées par la matrice P dans la relation $D = P^{-1}CP$).

6.4 Théorèmes d'isomorphisme de modules

Les applications linéaires satisfont les quatre théorèmes d'isomorphisme usuels qu'on donne sans démonstration, puisque les arguments sont similaires de ceux pour les groupes et les anneaux.

Dans les énoncés suivants, les lettres M, N et K dénotent de A-modules, et le symbole $\cong$ dénote d'isomorphismes entre A-modules.

Théorème 6.17. *Si $\phi : M \to N$ est une application linéaire, alors*

$$M/\ker(\phi) \cong \phi(M).$$

Théorème 6.18. *Si N et K sont deux sous-modules de M, alors $N + K$ et $N \cap K$ le sont aussi et*

$$(N + K)/K \cong N/N \cap K.$$

Théorème 6.19. *Si N et K sont deux sous-modules de M avec $N \subset K$, alors K/N est un sous-module de M/N et*

$$(M/N)/(K/N) \cong M/K.$$

Théorème 6.20 (théorème de correspondence)**.** *Soit N un sous-module de M. Alors, la correspondence*

$$\begin{aligned} \{\textit{sous-modules de } M \textit{ contenant } N\} &\longrightarrow \{\textit{sous-modules de } M/N\} \\ K &\longrightarrow K/N \end{aligned}$$

est une bijection préservant l'ordre, c'est-à-dire si K et K' sont deux sous-modules de M contenant N, alors $K \subset K'$ s-si $K/N \subset K'/N$.

6.5 Génération de modules

Lemme 6.21. *Soit M un A-module. Si $(N_i)_{i\in I}$ est une famille de sous-modules de M, alors leur intersection est aussi un sous-module de M.*

Démonstration. Exercice. □

Définition 6.22. Si M est un A-module et $S \subset M$, alors on dénote par (S) le *plus petit* sous-module de M contenant S, c'est-à-dire

$$(S) := \bigcap_{\substack{N \supset S \\ N \text{ sous-module de } M}} N.$$

Si $S = \{s_1, \ldots, s_k\}$ est fini, alors on utilise la notation $(s_1, \ldots, s_k)$ au lieu de $(\{s_1, \ldots, s_k\})$.

Lemme 6.23. *Si A est un anneau unitaire, M est un A-module et $S \subset M$, alors on a que*

$$(S) = A \cdot S := \{a_1 s_1 + \cdots + a_k s_k : k \in \mathbb{Z}_{\geq 0},\ a_1, \ldots, a_k \in A,\ s_1, \ldots, s_k \in S\}.$$

Démonstration. Exercice. □

Remarque 6.24. Si $A = K$ est un corps, on voit alors que $(S) = \mathrm{Span}_K(S)$.

Définition 6.25. Soit M un A-module. On dit que M est **de type fini** s'il existe $S \subset M$ fini tel que $M = (S)$. Dans ce cas-ci, on appelle S un **ensemble de générateurs** de M.

Si la cardinalité de S est minimale, alors on appelle S un ensemble de générateurs **minimal**.

S'il existe $m \in M$ tel que $M = (m)$, alors on appelle M **cyclique** ou **monogené**.

Comme dans l'algèbre linéaire, on définit la notion d'un ensemble linéairement indépendant :

Définition 6.26. Soit M un A-module et $S \subset M$.

On dit que S est **libre** ou **linéairement indépendant** si

$$\begin{array}{l} a_1 s_1 + \cdots + a_k s_k = 0 \\ s_1, \ldots, s_k \in S \end{array} \qquad \Longrightarrow \qquad a_1 = \cdots = a_k = 0,$$

c'est-à-dire il n'existe pas de relations linéaires non-triviales entre les éléments de S.

Si S est libre et $M = (S)$, alors on dit que M **est libre sur** S et on appelle S une **base** de M.

Remarque 6.27. Notons que $\emptyset$ est toujours linéairement indépendant, donc $\text{rang}(M) \in [0, \infty]$.

Exemple 6.28. Supposons que A est unitaire. Si M est un A-module libre sur l'ensemble fini $\{s_1, \ldots, s_n\}$, alors

$$M \cong A^n.$$

En effet, l'application $\phi : A^n \to M$ définie par $\phi((a_1, \ldots, a_n)) = a_1 s_1 + \cdots + a_n s_n$ est évidemment linéaire et surjective. De plus, son noyau est trivial car S est libre. Donc, $M \cong A^n$, comme on l'a affirmé.

On montre maintenant que chaque espace vectoriel est un module libre :

Théorème 6.29. *Si V est un espace vectoriel sur le corps K, alors V possède une base.*

Démonstration. Soit $X = \{S \subset V : S \text{ linéairement indépendant}\}$. Puisque $\emptyset \in X$, alors $X \neq \emptyset$. On appliquera le lemme de Zorn.

On vérifie d'abord que chaque chaîne de X possède une borne supérieure. En effet, si $Y \subset X$ est une chaîne, alors posons

$$T = \bigcup_{S \in Y} S.$$

On laisse comme exercice de vérifier que T est linéairement indépendant. Donc T est une borne supérieure de Y.

On peut, alors, appliquer le lemme de Zorn. Par la suite, il existe $S \in X$ maximal. On affirment qu'il est une base de V. Il suffit que montrer que $V = (S)$. Soit $v \in V$. Si $v \in S$, alors $v \in (S)$. Supposons que $v \in V \setminus S$. L'ensemble $\{v\} \cup S$ est linéairement dépendant car S est maximal. Donc il existe $s_1, \ldots, s_n \in S$ et $a, a_1, \ldots, a_n \in K$ tels que

$$av + a_1 s_1 + \cdots + a_n s_n = 0$$

et $a, a_1, \ldots, a_n$ ne sont pas tous zéros. Il faut que $a \neq 0$, sinon on aurait que $a_1 s_1 + \cdots + a_n s_n = 0$, c'est-à-dire on aurait une relation linéaire non-triviale entre les éléments de S, ce qui contredit le fait que S est libre. Puisque $a \neq 0$ et K est un corps, on en déduit que

$$v = -a^{-1} a_1 s_1 - \cdots - a^{-1} a_n s_n \in (S).$$

Ceci conclut la démonstration. □

Le théorème précédent peut échouer de façon dramatique dans un module général :

Exemple 6.30. Soit $G = \mathbb{Z}/2\mathbb{Z}$. Puisque G est un groupe abelien, il est un $\mathbb{Z}$-module. Par contre, il ne possède pas de base car $2 \cdot g = 0$ pour tout $g \in G$.

D'autre côté, G est aussi un $\mathbb{Z}/2\mathbb{Z}$-module. Puisque $\mathbb{Z}/2\mathbb{Z}$ est un corps, il faut que G ait une base. En fait, G est un espace vectoriel de dimension 1 sur $\mathbb{Z}/2\mathbb{Z}$.

Cet exemple, nous amène aux définitions suivantes :

Définition 6.31. Soient A un anneau non-trivial et M un A-module.

(a) Un élément $m \in M$ est appelé un **élément de torsion** s'il existe $a \in A \setminus \{0\}$ tel que $a \cdot m = 0$. On dénote par $\mathrm{Tor}(M)$ l'ensemble de tous les éléments de torsion de M.

(b) On dit que M est un **module de torsion** si $M = \mathrm{Tor}(M)$, c'est-à-dire si tous les éléments de M sont d'éléments de torsion.

(c) Si $S \subset M$, alors l'**annulateur** de S est l'ensemble

$$\mathrm{Ann}(S) := \{a \in A : a \cdot s = 0 \ \forall s \in S\}.$$

Quand $S = \{s\}$, on écrit $\mathrm{Ann}(s)$ au lieu de $\mathrm{Ann}(\{s\})$.

Exemple 6.32. Considérons $G = \mathbb{Z}/2\mathbb{Z}$ comme un $\mathbb{Z}$-module. On a que $\mathrm{Tor}(G) = G$. De plus,

$$\mathrm{Ann}(0) = \mathbb{Z}, \quad \mathrm{Ann}(1) = 2\mathbb{Z} \quad \text{et} \quad \mathrm{Ann}(G) = 2\mathbb{Z}.$$

Lemme 6.33. *Chaque groupe abelien fini est un $\mathbb{Z}$-module de torsion.*

Démonstration. Soit G un groupe abelien de cardinalité $n < \infty$. Si $g \in G$, les éléments $0 \cdot g, 1 \cdot g, \ldots, n \cdot g$ ne peuvent pas être tous distincts par le principe des tiroirs. Il existe, alors $0 \leq i < j \leq n$ tels que $i \cdot g = j \cdot g$. Donc,

$$(j - i) \cdot g = j \cdot g - i \cdot g = 0.$$

Puisque $j - i \neq 0$, on a que $g \in \mathrm{Tor}(G)$. On a alors que $\mathrm{Tor}(G) = G$, comme on l'affirmé.

On remarque qu'on peut donner une démonstration algébrique aussi : le théorème de Lagrange nous dit que, pour tout $g \in G$, $\mathrm{ord}(g) | n$ car $\mathrm{ord}(g)$ est la cardinalité du sous-groupe engendré par g et $n = |G|$. Donc, $n \cdot g = 0$. □

Lemme 6.34. *Soit K un corps, et soit V un $K[x]$-module pour lequel $\dim_K(V) < \infty$. Alors, V est un module de torsion.*

Démonstration. Soit $T : V \to V$ l'application $T(v) := x \cdot v$ et soit $n = \dim_K(V)$. Si $f(x) = a_0 + a_1 x + \cdots + a_d x^d$, alors

$$f(x) \cdot v = a_0 v + a_1 T(v) + \cdots + a_d T^d(v).$$

On cherche alors une combinaison linéaire non-triviale de $v, T(v), \ldots, T^d(v)$ qui vaut 0. Si $d = n$, on a $n+1$ vecteurs dans un espace vectoriel de dimension n. Alors, une telle combinaison linéaire existe, ce qui montre que $v \in \mathrm{Tor}_{K[x]}(V)$. Ceci termine la démonstration. □

Remarque 6.35. Comme on va le voir, le théorème de Cayley-Hamilton (cf. théorème 8.16) implique que si $c_T(x)$ est le polynôme caractéristique de T, alors $c_T(x) \cdot v = 0$ pour tout $v \in V$. Ceci est l'analogue du fait que si G est un groupe abelien de n éléments, alors $n \cdot g = 0$ pour tout $g \in G$.

Lemme 6.36. *Soient A un anneau non-trivial et M un A-module.*

(a) Si A est intègre, alors $\mathrm{Tor}(M)$ *est un sous-module de M.*

(b) Pour tout $S \subset M$, l'ensemble $\mathrm{Ann}(S)$ *est un idéal de A.*

Démonstration. Exercice. □

Finalement, on généralise le concept de la dimension d'un espace vectoriel :

Définition 6.37. Soit M un A-module. Le **rang** de M est défini par

$$\mathrm{rang}(M) := \sup\{|S| : S \subset M \text{ linéairement indépendant et fini}\}.$$

Remarque 6.38. Si V est un K espace vectoriel et $n = \mathrm{rang}(V)$, alors V possède une base de n éléments, c'est-à-dire $n = \dim(V)$. En effet, si S est un ensemble libre de V de n éléments, alors S a cardinalité maximale. En suivant la démonstration du théorème 6.29, on en déduit que S doit être une base de V.

On a vu que si M est un A-module qui est libre sur un ensemble de n éléments, alors $M \cong A^n$. On voudrait certainement que $\mathrm{rang}(M) = n$, comme on l'a pour les espaces vectoriels. Ceci n'est pas vrai en général et, en tout cas, c'est difficile de le montrer. On va le montrer dans l'appendice de ce chapitre quand A est commutatif et unitaire.

6.6 Sommes directes

Définition 6.39. Soit M un A-module et soient $N_1, \ldots, N_k$ de sous-modules de M. Leur somme est le module

$$N = N_1 + N_2 + \cdots + N_k := \{n_1 + \cdots + n_k : n_i \in N_i \ \forall i\}.$$

Si l'équation $n_1 + n_2 + \cdots + n_k = 0$ avec $n_i \in N_i$ pour tout i a que la solution triviale $n_1 = n_2 = \cdots = n_k = 0$, alors on écrit

$$N = N_1 \oplus N_2 \oplus \cdots \oplus N_k$$

et on appelle N la **somme directe (interne)** des modules $N_1, \ldots, N_k$.

Plus généralement, si $(N_i)_{i \in I}$ est une famille de sous-modules de M, alors on définit leur somme comme étant l'ensemble $N = \{n_{i_1} + \cdots + n_{i_r} : i_1, \ldots, i_r \in I,\ n_{i_j} \in N_{i_j}\ \forall j\}$. Si l'équation $n_{i_1} + \cdots + n_{i_r} = 0$ avec $i_1, \ldots, i_r$ éléments distincts de I et avec $n_{i_j} \in N_{i_j}$ a que la solution triviale $n_{i_1} = \cdots = n_{i_r} = 0$, alors on dit que N est la **somme directe (interne)** des modules N_i, $i \in I$.

Définition 6.40. Si $(N_i)_{i\in I}$ est une famille de A-modules, on définit leur **somme directe (externe)** par

$$\bigoplus_{i\in I} N_i := \{(n_i)_{i\in I} : n_i = 0 \text{ à part d'un nombre fini } i \in I\}.$$

Cet ensemble est un sous-module du produit directe $\prod_{i\in I} N_i$.

Remarque 6.41. Les sommes directes internes et externes de $N_1, \ldots, N_k$ sont isomorphes. Cependant, pour définir la somme directe externe de $N_1, \ldots, N_k$, on n'a pas besoin de savoir que les N_i sont tous de sous-modules du même module ambient M.

Lemme 6.42. *Soit M un A-module, et soient N_1, N_2, N trois sous-modules de M tels que $N = N_1 + N_2$. On a que $N = N_1 \oplus N_2$ s-si $N_1 \cap N_2 = \{0\}$.*

Démonstration. Supposons que $N_1 \cap N_2 = \{0\}$. Si $n_1 + n_2 = n_1' + n_2'$, alors $n_1 - n_1' = n_2' - n_2$. Puisque $n_1 - n_1' \in N_1$ et $n_2' - n_2 \in N_2$, on trouve que $n_1 - n_1' = n_2' - n_2 \in N_1 \cap N_2 = \{0\}$, d'où $n_1 = n_1'$ et $n_2 = n_2'$.

Vice versa, si $N = N_1 \oplus N_2$ et $n \in N_1 \cap N_2$, alors $0 = 0 + 0 = n + (-n)$ sont deux representations de 0 dans la forme $n_1 + n_2$ avec $n_1 \in N_1$ et $n_2 \in N_2$. Donc $n = 0$, ce qui conclut la démonstration. □

6.7 Modules noetheriens

Définition 6.43. Soit M un module. Si chaque sous-module de M est de type fini, alors on appelle M un module **noetherien**.

Théorème 6.44. *Soit M un module. Les propositions suivantes sont équivalentes :*

(a) M est noetherien.

(b) Chaque chaîne ascendante $N_1 \subset N_2 \subset \cdots$ de sous-modules de M se termine, c'est-à-dire il existe $k \in \mathbb{Z}_{\geq 1}$ tel que $N_k = N_{k+1} = N_{k+2} = \cdots$.

Démonstration. Exercice. □

Théorème 6.45. *Soit M un module et N un sous-module de M. Alors, M est noetherien s-si N et M/N le sont.*

Démonstration. Si M est noetherien, c'est clair que N et M/N le sont aussi : les sous-modules de N sont de sous-modules de M, donc de type fini. De plus, les sous-modules de M/N sont de la forme K/N par le théorème de correspondence (cf. théorème 6.20), où K est un sous-module de M contentant N. Puisque K est de type fini, soit $K = (s_1, \ldots, s_n)$, alors $K/N = (\overline{s}_1, \ldots, \overline{s}_r)$ est aussi de type fine.

Réciproquement, supposons que N et M/N sont noetheriens. Soit K un sous-module de N. On considère les modules $K \cap N$ et $K + N$. Le premier est un sous-module de N, donc il est de type fini. Pour le deuxième, on a $(K + N)/N$ est un sous-module de M/N, donc de

type fini. Puisque $K/K \cap N \cong (K+N)/N$ d'après le deuxième théorème d'isomorphisme de modules (cf. théorème 6.18), alors $K/K \cap N$ est aussi de type fini.

Soient $x_1, \ldots, x_m, y_1, \ldots, y_n \in K$ tels que $K/K \cap N = (\overline{x}_1, \ldots, \overline{x}_m)$ et $K \cap N = (y_1, \ldots, y_n)$. On montrera que $K = (x_1, \ldots, x_m, y_1, \ldots, y_n)$. Soit $x \in K$. Donc $\overline{x} = a_1\overline{x}_1 + \cdots + a_m\overline{x}_m$ pour quelques $a_1, \ldots, a_m \in A$. Par la suite, $x - (a_1x_1 + \cdots + a_mx_m) \in K \cap N$. Donc, il existe $b_1, \ldots, b_n \in A$ tels que $x - (a_1x_1 + \cdots + a_mx_m) = b_1y_1 + \cdots + b_ny_n$. On en déduit que $x = a_1x_1 + \cdots + a_mx_m + b_1y_1 + \cdots + b_ny_n$, ce qui conclut la démonstration. □

Théorème 6.46. *Si $M_1, \ldots, M_k$ sont de A-modules noetheriens, alors leur produit directe $M_1 \times \cdots \times M_k$ l'est aussi.*

Démonstration. Par induction sur k : le cas $k = 1$ est trivial. Puis, si $M_1 \times \cdots \times M_{k-1}$ est noetherien, alos on observe que $N = M_1 \times \cdots \times M_{k-1} \times \{0\}$ est un sous-module noetherien de $M = M_1 \times \cdots \times M_k$. De plus, $M/N \cong M_k$, qui est aussi noetherien. Le théorème 6.45 conclut l'étape inductive. □

Théorème 6.47. *Soit A un anneau noetherien et unitaire. Si M est un A-module de type fini, alors il est noetherien.*

Démonstration. Supposons que $M = (s_1, \ldots, s_k)$ pour quelques $s_1, \ldots, s_k \in M$. Définissons $\phi : A^k \to M$ par $\phi((a_1, \ldots, a_k)) = a_1s_1 + \cdots + a_ks_k$. Clairement, ϕ est un épimorphisme de modules. Donc, le premier théorème d'isomorphismes de modules (cf. théorème 6.17) implique que $M \cong A^k/\ker(\phi)$. Puisque A est un anneau noetherien (donc, un A-module noetherien), le théorème 6.46 nous dit que A^k est un A-module noetherien. Par la suite, le théorème 6.45 implique que $A^k/\ker(\phi)$ est noetherien aussi. Puisque $M \cong A^k/\ker(\phi)$, le théorème est démontré. □

6.8 Exercices

EXERCICE 6.1. Soit V un espace vectoriel non-nul sur un corps K.

(a) Soit S et T deux bases de V. Si $|S| < \infty$, alors montrez que $|T| = |S|$.
[*Indice* : Montrez que si E est une base de V et $X = \{x_1, \ldots, x_n\} \subset V$ est un ensemble linéairement indépendant, alors on peut remplacer n éléments de E par $x_1, \ldots, x_n$ et trouver une nouvelle base de V qui a la même cardinalité avec E. (En particulier, il faut que $\#E \geq n$.)

(b) Si V est de type fini comme un K-module, alors montrez que chaque base de K a la même cardinalité finie. (Cette cardinalité est appelée la dimension de V et elle est dénotée par $\dim(V)$.) s

(c) Montrez que $\dim(K^n) = n$ et concluez que $K^n \cong K^m$ si et seulement si $n = m$.

EXERCICE 6.2. Soit A un anneau avec unité $1 \neq 0$.

(a) (ex. 5, p. 343) Si I est un idéal de A et M un A-module, on pose

$$IM = \left\{ \sum_{j=1}^{n} i_j m_j : n \in \mathbb{N},\ i_1, \ldots, i_n \in I,\ m_1, \ldots, m_n \in M \right\}.$$

Montrez que IM est un sous-module de M.

(b) (ex. 12, p. 350) Montrez que $IA^n = I^n$ et concluez que $A^n/IA^n \cong (A/I)^n$ comme A-modules.

(c) (ex. 2, p. 356) Si A est commutatif, alors $A^n \cong A^m$ si et seulement si $n = m$.
[*Indice* : Si $\phi : A^n \to A^m$ est un isomorphisme de A-modules et I est un idéal de A, alors montrez que $x \in IA^n$ si et seulement si $\phi(x) \in IA^m$.]

(d) En supposant que M est noethérien et qu'il est libre sur un ensemble $S \subset M$, montrez que $|S| < \infty$.

EXERCICE 6.3 (ex. 27, p. 358). Soit $M = \mathbb{Z} \times \mathbb{Z} \times \cdots$, qui est un $\mathbb{Z}$-module. On considère son anneau d'endomorphismes $A = \mathrm{End}_{\mathbb{Z}}(M)$. On définit $\phi_1, \phi_2 \in A$ par

$$\phi_1(a_1, a_2, a_3, \dots) = (a_1, a_3, a_5, \dots) \quad \text{et} \quad \phi_2(a_1, a_2, a_3, \dots) = (a_2, a_4, a_6, \dots).$$

(a) Montrez que $\{\phi_1, \phi_2\}$ est une base du A-module A.
[*Indice* : Définissez les applications ψ_1 et ψ_2 par $\psi_1(a_1, a_2, \dots) = (a_1, 0, a_2, 0, \dots)$ et $\psi_2(a_1, a_2, \dots) = (0, a_1, 0, a_2, \dots)$. Vérifiez que $\phi_1 \circ \psi_1 = 1 = \phi_2 \circ \psi_2$, $\phi_1 \circ \psi_2 = 0 = \phi_2 \circ \psi_1$ et $\psi_1 \circ \phi_1 + \psi_2 \circ \phi_2 = 1$. Utiliser ces relations pour montrer que ϕ_1, ϕ_2 sont indépendants et engendrent A comme un A-module.]

(b) Utiliser la partie (a) pour montrer que $A \cong A^2$ et déduisez que $A \cong A^n$ pour tout $n \in \mathbb{N}$. (Donc, si A n'est pas commutatif, c'est possible que $\mathrm{rang}(A^n) \neq n$.)

EXERCICE 6.4. Soit A un anneau commutatif, unitaire et non-trivial. Un élément $a \in A$ est appelé **régulier** s'il est non-zéro et il n'est pas un diviseur de zéro. C'est-à-dire, a est régulier si l'équation $ab = 0$ toujours implique que $b = 0$.

Définissons

$$\mathrm{Tor}_*(M) := \{m \in M : \exists a \in A \text{ régulier tel que } am = 0\}.$$

(a) Montrez que $\mathrm{Tor}_*(M)$ est un sous-module de M.

(b) Montrez que $\mathrm{rang}(M/\mathrm{Tor}_*(M)) = \mathrm{rang}(M)$.

(c) Montrez que si A est un anneau intègre, alors $\mathrm{Tor}(M) = \mathrm{Tor}_*(M)$. De plus, le module quotient $M/\mathrm{Tor}(M)$ n'a pas d'éléments non-nuls de torsion.

EXERCICE 6.5 (ex. 8, p. 344).

(a) Donnez un exemple d'un anneau A et d'un A-module M pour lesquels l'ensemble $\mathrm{Tor}(M)$ n'est pas un sous-module de M. [*Indice* : Considérez $\mathrm{Tor}(A)$, c'est-à-dire, le sous-module de torsion de l'A-module A.]

(b) Si A a des diviseurs de zéro et M est un A-module non-nul, alors montrez que $\mathrm{Tor}(M) \neq \{0\}$.

(c) (ex. 4, p. 356) M est appelé un module de torsion si $\mathrm{Tor}(M) = M$. Montrez que chaque groupe abélien fini est un $\mathbb{Z}$-module de torsion. Donnez aussi un exemple d'un $\mathbb{Z}$-module de torsion qui est infini.

EXERCICE 6.6. Soit M un A-module.

(a) (ex. 9, p. 344) Montrez que si N est un sous-module de M, alors son annulateur $\mathrm{Ann}(N)$ est un idéal de A. De plus, montrez que l'action $\overline{a} \cdot n := a \cdot n$ rend N un $(A/\mathrm{Ann}(N))$-module dont l'annulateur est nul. [1]

(b) (ex. 10, p. 344) Soit I un idéal de A. Montrez que l'ensemble $M(I) := \{m \in M : im = 0 \text{ pour tout } i \in I\}$ est un sous-module de M.

(c) (ex. 11, p. 344) Supposons que $M = \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$ et que $A = \mathbb{Z}$.

(i) Calculez l'idéal $\mathrm{Ann}(M)$.

(ii) Soit $I = 2\mathbb{Z}$. Décrivez $M(I)$ comme un produit direct de groupes cycliques.

EXERCICE 6.7. Soit A un anneau unitaire.

(a) (ex. 9, p. 356) Un A-module M est appelé irréductible si M n'est pas nul est ses seules sous-modules sont (0) et M. Montrez que M est irréductible si et seulement si $M \neq \{0\}$ et $M = Am$ pour chaque $m \in M \setminus \{0\}$. Déterminez tous les $\mathbb{Z}$-modules irréductibles.

(b) (ex. 10, p. 356) Soit M un A-module. Si A est commutatif, montrez que M est irréductible si et seulement si $M \cong A/I$ comme A-modules, où I est un idéal maximal de A. [*Indice* : Pour chaque $m \in M \setminus \{0\}$, l'application $A \ni a \to am \in M$ est un isomorphisme de A-modules.]

(c) (ex. 11, p. 356) Soit M et N deux A-modules irréductibles. Montrez que chaque application linéaire non-zéro de M à N est un isomorphisme de A-modules. Déduisez que $\mathrm{End}(M)$ est un corps gauche. [*Indice* : Considérez le noyau et l'image de l'application linéaire.]

EXERCICE 6.8. Soient A un commutatif et unitaire et M un A-module libre de rang $n \geq 1$. Soit aussi $S = \{s_1, \ldots, s_n\}$ un sous-ensemble de M qui l'engendre. Montrez que S est linéairement indépendant comme suivant :

(i) Soit $e_1, \ldots, e_n$ une base de M. On peut écrire $s_i = u_{i,1}e_1 + \cdots + u_{i,n}e_n$ pour tout $i \in \{1, \ldots, n\}$, où les coefficients $u_{i,j}$ appartiennent à A. De même, on peut écrire $e_i = v_{i,1}s_1 + \cdots + v_{i,n}s_n$ pour tout $i \in \{1, \ldots, n\}$, où les coefficients $v_{i,j}$ appartiennent à A. Montrez que $VU = I$, où U et V sont les matrices carrés de taille $n \times n$ dont les coefficients sont $u_{i,j}$ et $v_{i,j}$, respectivement, et I est la matrice carré unitaire de taille $n \times n$.

(ii) Étante donnée une matrice $C = (c_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in M_{n \times n}(A)$, on définit son déterminant

$$\det(C) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) c_{1,\sigma(1)} c_{2,\sigma(2)} \cdots c_{n,\sigma(n)},$$

où S_n dénote l'ensemble des permutations de $\{1, \ldots, n\}$ et $\mathrm{sgn}(\sigma)$ le signe de la permutation σ. Montrez que :

— $\det(CD) = \det(C)\det(D)$, où D est aussi dans $M_{n \times n}(A)$;

— si $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ sont les lignes de C et on remplace $\boldsymbol{c}_i$ par $\sum_{j=1}^{n} a_j \boldsymbol{c}_j$, où $a_1, \ldots, a_n \in A$, alors le déterminant de la nouvelle matrice est égal à $a_i \det(C)$.

1. Un A-module M dont l'annulateur $\mathrm{Ann}(M)$ est nul est appelé **fidèle**.

(iii) Si on a que $a_1 s_1 + \cdots + a_n s_n = 0$ pour quelques $a_1 \ldots, a_n \in A$, alors montrez que $a_j \det(U) = 0$ pour chaque $j \in \{1, \ldots, n\}$, où U est la matrice définie à la partie (a). Déduisez que $a_j = 0$ pour chaque $j \in \{1, \ldots, n\}$, c'est-à-dire S est linéairement indépendant.

6.9 Appendice : de rangs de modules

Théorème 6.48. *Soit A un anneau commutatif et unitaire, et soit M un A-module. Si M possède une base de r éléments, alors $r = \mathrm{rang}(M)$.*

Démonstration. Evidemment, $|S| \leq r$. En particulier, S est fini, soit $S = \{s_1, \ldots, s_n\}$. Il reste à montrer que si $m_1, \ldots, m_{n+1} \in M$, alors ils sont linéairement dépendant, c'est-à-dire il existe $a_1, \ldots, a_{n+1} \in A$ n'étant pas tous zéros tels que

$$a_1 m_1 + \cdots + a_{n+1} m_{n+1} = 0. \tag{6.4}$$

Si on écrit $m_j = \sum_{i=1}^{n} b_{i,j} s_i$, où $b_{i,j} \in A$, alors (6.4) devient

$$\sum_{i=1}^{n} \sum_{j=1}^{n+1} b_{i,j} a_j s_i = 0.$$

L'indépendance de $s_1, \ldots, s_n$ nous donne que

$$\sum_{i=1}^{n} \sum_{j=1}^{n+1} b_{i,j} a_j s_i = 0 \quad \Longleftrightarrow \quad \sum_{j=1}^{n+1} b_{i,j} a_j = 0 \quad \forall i \quad \Longleftrightarrow \quad B \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{6.5}$$

où $B = (b_{i,j})_{1 \leq i \leq n,\, 1 \leq j \leq n+1}$.

Soit D_i le déterminant de la matrice B sans son i-ième colonne (voir l'exercice 6.8 pour la définition du déterminant d'une matrice dans un contexte général). Considérons, aussi, la matrice B_i de taille $(n+1) \times (n+1)$ dont les premières n lignes sont celles de B et la $(n+1)$-ième ligne est égale à $(b_{i,1}, \ldots, b_{i,n+1})$. Puisque B_i a deux lignes identiques, on a que $\det(B_i)$. D'autre côté, si on développe le déterminant de B_i par rapport à sa $(n+1)$-ligne, alors on trouve que

$$\det(B_i) = (-1)^{n+2} b_{i,1} D_1 + (-1)^{n+3} b_{i,2} \det(D_2) + \cdots + (-1)^{2n+2} b_{i,n+1} D_{n+1}.$$

On pose alors $a_i = (-1)^i D_i$ pour trouver que

$$b_{i,1} a_1 + b_{i,2} a_2 + \cdots + b_{i,n+1} a_{n+1} = 0 \quad (1 \leq i \leq n+1).$$

Ceci termine la preuve à moins que $D_i = 0$ pour tout $i \in \{1, \ldots, n+1\}$. Soit $B' = (b_{i,j})_{1 \leq i,j \leq n}$ et soit m le *rang déterminantal* de B', c'est-à-dire, le plus grand nombre m pour lequel il existe une sous-matrice C de B' de taille $m \times m$ dont le déterminant n'est pas égal

à zéro. Puisque $\det(B') = D_{n+1} = 0$, alors $m < n$. Sans perte de généralité, on suppose que $C = (b_{i,j})_{1 \leq i,j \leq m}$ (sinon, on permute les m_j et les s_j).

Pour $k \in \{1, \ldots, n+1\}$, considérons la matrice $C'_k \in M_{m+1}(A)$ dont les premières m lignes sont $(b_{i,1}, \ldots, b_{i,m+1})$, $1 \leq i \leq m$, et la $(m+1)$-ième ligne est $(b_{k,1}, \ldots, b_{k,m+1})$.

Si $k > m$, alors la définition de m implique que $\det(C'_k) = 0$. Si $k \leq m$, alors C'_k a deux lignes identiques, d'où on trouve encore que $\det(C'_k) = 0$.

Soit d_j dénote le déterminant de la matrice C'_k sauf sa $(m+1)$-ième ligne et sa j-ième colonne. Notons que d_j ne dépend pas de k. De plus, en développant le déterminant de C'_k par rapport à sa $(m+1)$-ième ligne, on trouve que

$$b_{k,1}d_1 - b_{k,2}d_2 + \cdots + (-1)^m b_{k,m+1}d_{m+1} = 0.$$

Ceci est vrai pour tout $k \in \{1, \ldots, n+1\}$. Par conséquent, si on le pose $a_i = (-1)^i d_i$ pour $i \in \{1, \ldots, m+1\}$ et $a_i = 0$ pour $i \in \{m+2, \ldots, n+1\}$, alors on trouve que $b_{i,1}a_1 + b_{i,2}a_2 + \cdots + b_{i,n+1}a_{n+1} = 0$ pour tout $i \in \{1, \ldots, n+1\}$. Puisque $a_{m+1} = (-1)^{m+1}d_{m+1} = (-1)^{m+1}\det(C) \neq 0$, on conclut que (6.5) (et, par la suite, (6.4)) est vraie pour quelques éléments $a_1, a_2, \ldots, a_{n+1} \in A$ qui ne sont pas tous zéro. Donc on conclut que $m_1, \ldots, m_{n+1}$ sont linéairement dépendants, ce qui termine la preuve. □

Chapitre 7

Théorème des facteurs invariants

Dans ce chapitre on montre un résultat fondamental caractérisant les modules de type fini sur un anneau principal.

On fixe, alors un anneau principal A et M un A-module. On va montrer qu'il existe un entier $r \geq 0$ et quelques $a_1, \ldots, a_k \in A \setminus (A^\times \cup \{0\})$ tels que

$$M \cong A^r \times A/(a_1) \times A/(a_2) \times \cdots A/(a_k).$$

Comme on va le voir, $r = \text{rang}(M)$, donc r est défini de façon unique. Les éléments $a_1, \ldots, a_k$ deviennent aussi uniques si on impose quelques conditions. Les énoncés précises suivent :

Théorème 7.1. *Soient A un anneau principal et M un A-module de type fini. Il existe un entier $r \geq 0$ et quelques éléments $a_1, \ldots, a_k \in A \setminus (\{0\} \cup A^\times)$ tels que*

$$M \cong A^r \times A/(a_1) \times A/(a_2) \times \cdots A/(a_k).$$

De plus :

(a) Le nombre r est défini de façon unique. En fait, on a que $r = \text{rang}(M)$.

(b) Il existe un choix unique d'éléments $a_1, \ldots, a_k$ (modulo multiplication par d'éléments inversibles) tel que

$$(a_1) \subset (a_2) \subset \cdots (a_k) \quad \iff \quad a_k | a_{k-1} | \cdots | a_1.$$

Dans ce cas-ci, on appelle $a_1, \ldots, a_k$ les **facteurs invariants** *de M.*

(c) En factorisant les a_j et en appliquant le théorème des restes chinois, on a que

$$M \cong A^r \times A/(p_1^{v_1}) \times A/(p_2^{v_2}) \times \cdots A/(p_n^{v_n})$$

pour quelques irréductibles $p_1, \ldots, p_m$ et quelques entiers $v_1, \ldots, v_m \geq 1$. Les éléments $p_1^{v_1}, \ldots, p_n^{v_n}$ sont appelés les **diviseurs élémentaires** *de M et ils sont définis de façon unique (modulo leur permutation et leur multiplication par d'éléments inversibles).*

7.1 Le plan de la démonstration

La démonstration du théorème 7.1 est longue et difficile. Pour cette raison, on la divise en plusieurs parties. On commence avec six résultats auxiliaires. On les montrera dans la prochaine section.

Dans tous les énoncés, M dénote un module de type fini sur un anneau principal A. On se rappelle que, selon ces hypothèses, M est un module noetherien. En particulier, son rang est fini.

Proposition 7.2. *Si M est a une base de r éléments et N est un sous-module de M, alors N a une base de $\leq r$ éléments. En particulier, $r = \operatorname{rang}(M)$.*

Proposition 7.3. *Si $\operatorname{Tor}(M) = (0)$, alors il existe $r \in \mathbb{Z}_{\geq 0}$ tel que $M \cong A^r$.*

Proposition 7.4. *Il existe un entier $r \geq 0$ et un sous-module L de M tels que $M = L \oplus \operatorname{Tor}(M)$ et $L \cong A^r$. En particulier, $M \cong A^r \times \operatorname{Tor}(M)$.*

Proposition 7.5. *Si $M \cong A^r \times N$, où N est un A-module de torsion, alors $N \cong \operatorname{Tor}(M)$ et $A^r \cong M/\operatorname{Tor}(M)$.*

Proposition 7.6. *Si M est un A-module de torsion, alors $\operatorname{Ann}(M)$ est un idéal non-trivial de A. En particulier, il existe $a \in A \setminus \{0\}$ tel que $\operatorname{Ann}(M) = (a)$.*

Proposition 7.7. *Si $a \in A$, alors on pose $M(a) = \{m \in M : am = 0\}$.*

(a) $M(a)$ est un sous-module de M.

(b) Si $a, b \in A \setminus \{0\}$ sont copremiers, alors $M(ab) = M(a) \oplus M(b)$.

Proposition 7.8. *Soient $p \in A$ premier et $v \in \mathbb{N}$. Si $p^v M = (0)$, alors il existe un sous-module N de M et un $s \in \mathbb{Z}_{\geq 0}$ tels que $p^{v-1}N = (0)$ et $M \cong (A/(p^v))^s \times N$.*

On montre maintenant comment on peut utiliser les propositions ci-dessus pour en déduire le théorème 7.1.

Démonstration du théorème 7.1. On divise l'argument dans cinq étapes.

Étape 1 : existence des diviseurs élémentaires. Selon la proposition 7.4, on a que

$$M \cong A^r \times \operatorname{Tor}(M).$$

Si $\operatorname{Tor}(M) = (0)$, alors la preuve est terminée (il n'y a pas de diviseurs élémentaires). Supposons alors que $\operatorname{Tor}(M) \neq (0)$.

D'après la proposition 7.6 (appliquée au sous-module $\operatorname{Tor}(M)$ au lieu de M), il existe $a \in A \setminus \{0\}$ tel que $(a) = \operatorname{Ann}(\operatorname{Tor}(M))$. En particulier,

$$\operatorname{Tor}(M) = \{m \in M : am = 0\} = M(a).$$

Si $a = p_1^{v_1} \cdots p_J^{v_J}$ est la factorisation première de a dans A (qui est un anneau factoriel), alors la proposition 7.7 implique que

$$\operatorname{Tor}(M) = \oplus_{j=1}^{J} M(p_j^{v_j}) =: \oplus_{j=1}^{J} M_j. \tag{7.1}$$

On a que $p_j^{v_j} M_j = (0)$. Donc on peut appliquer la proposition 7.8 de façon inductive pour en déduire que

$$M_j \cong (A/(p_j^{v_j}))^{r_{j,1}} \times (A/(p_j^{v_j-1}))^{r_{j,2}} \times \cdots \times (A/(p_j))^{r_{j,v_j}} \tag{7.2}$$

et, par consequent, que

$$M \cong A^r \times \oplus_{j=1}^{J} \left\{ (A/(p_j^{v_j}))^{r_{j,1}} \times (A/(p_j^{v_j-1}))^{r_{j,2}} \times \cdots \times (A/(p_j))^{r_{j,v_j}} \right\}. \tag{7.3}$$

Ceci montre l'existence des diviseurs élémentaires.

Étape 2 : caractérisation de r. Puisque $M \cong A^r \times A/(a_1) \times \cdots \times A/(a_k)$ pour quelques $a_j \in A \setminus (\{0\} \cup A^\times)$ (les diviseurs élémentaires de A), on a que $A^r \cong M/\operatorname{Tor}(M)$. Alors, $M/\operatorname{Tor}(M)$ est un module libre sur r éléments. La proposition 7.2 implique alors que $r = \operatorname{rang}(M/\operatorname{Tor}(M))$. Finalement, en appliquant l'exercice 6.4(b), on trouve que $r = \operatorname{rang}(M/\operatorname{Tor}(M)) = \operatorname{rang}(M)$, ce qui montre la partie (a) du théorème 7.1.

Étape 3 : unicité des diviseurs élémentaires. Supposons que

$$M \cong A^r \times \oplus_{j=1}^{J'} \left\{ (A/(q_j^{w_j}))^{s_{j,1}} \times (A/(p_j^{w_j-1}))^{s_{j,2}} \times \cdots \times (A/(q_j))^{s_{j,w_j}} \right\},$$

où $q_1, \ldots, q_{J'}$ sont d'éléments premiers et non-associés de A. La proposition 7.5 implique que

$$\operatorname{Tor}(M) \cong \oplus_{j=1}^{J'} \left\{ (A/(q_j^{w_j}))^{s_{j,1}} \times (A/(q_j^{w_j-1}))^{s_{j,2}} \times \cdots \times (A/(q_j))^{s_{j,w_j}} \right\}. \tag{7.4}$$

En particulier, on trouve que $\operatorname{Ann}(\operatorname{Tor}(M))$ est l'idéal engendré par $q_1^{w_1} \cdots q_{J'}^{w_{J'}}$. D'autre côté, on a que

$$\operatorname{Ann}(\operatorname{Tor}(M)) = (a) = (p_1^{v_1} \cdots p_J^{v_J}).$$

Donc on trouve que $q_1^{w_1} \cdots q_{J'}^{w_{J'}} = u p_1^{v_1} \cdots p_J^{v_J}$ pour un élément inversible u de A. Puisque A est factoriel (comme principal), alors $J' = J$ et il existe une permutation $\sigma \in S_J$ telle que $(q_i^{w_i}) = (p_{\sigma(i)}^{v_{\sigma(i)}})$ pour tout $i \in \{1, \ldots, J\}$. Sans perde de généralité, on peut supposer que σ est l'identité de S_J. Alors $(q_j) = (p_j)$ et $w_j = v_j$ pour tout $j \in \{1, \ldots, J\}$.

Pour compléter la démonstration, on doit montrer que $r_{j,i} = s_{j,i}$ pour tous i, j. La relation (7.4) implique qu'on peut écrire $\operatorname{Tor}(M) = K_1 \oplus K_2 \oplus \cdots \oplus K_{J'}$, où

$$\begin{aligned} K_j &\cong (A/(q_j^{w_j}))^{s_{j,1}} \times (A/(q_j^{w_j-1}))^{s_{j,2}} \times \cdots \times (A/(q_j))^{s_{j,w_j}} \\ &= (A/(p_j^{v_j}))^{s_{j,1}} \times (A/(p_j^{v_j-1}))^{s_{j,2}} \times \cdots \times (A/(p_j))^{s_{j,v_j}}. \end{aligned}$$

On affirme que $K_j = M_j$. En effet, c'est clair que $K_j \subset M_j = \{m \in M : p_j^{v_j} m = 0\}$. De plus, si $m \in M_j \subset \operatorname{Tor}(M) = K_1 \oplus \cdots \oplus K_J$, alors $m = k_1 + \cdots + k_J$, où $k_i \in K_i$ pour tout $i \in \{1, \ldots, J\}$. On a que

$$0 = p_j^{v_j} m = p_j^{v_j} k_1 + \cdots + p_j^{v_j} k_J \quad \Rightarrow \quad p_j^{v_j} k_i = 0 \quad (1 \le i \le J).$$

Si $i \neq j$, alors $\operatorname{pgcd}(p_i^{v_i}, p_j^{v_j}) = 1$ et, au même temps, $p_i^{v_i} k_i = p_j^{v_j} k_j = 0$. Puisque A est principal, il existe $x, y \in A$ tels que $x p_i^{v_i} + y p_j^{v_j} = 1$. Donc

$$k_i = 1 \cdot k_i = (x p_i^{v_i} + y p_j^{v_j}) k_i = 0 \quad (i \in \{1, \ldots, J\} \setminus \{j\}).$$

On en déduit que $m = k_j \in K_j$. Ceci conclut la preuve que $K_j = M_j$.

On a alors montré que

$$(A/(p_j^{v_j}))^{s_{j,1}} \times \cdots \times (A/(p_j))^{s_{j,v_j}} \cong K_j = M_j \cong (A/(p_j^{v_j}))^{r_{j,1}} \times \cdots \times (A/(p_j))^{r_{j,v_j}}.$$

On va en déduire que $s_{j,i} = r_{j,i}$ pour tout i par induction sur v_j. Si $v_j = 1$, le résultat suit tout de suite, car dans ce cas-ci $(A/(p_j))^{r_{j,1}}$ et $(A/(p_j))^{s_{j,1}}$ sont d'espaces vectoriels sur $A/(p_j)$ qui sont isomorphes (on se rappelle que p_j est premier, donc (p_j) est un idéal premier et, puisque A est principal, il est aussi maximal). Par la suite, leur dimensions, $r_{j,1}$ et $s_{j,1}$ respectivement, sont égales.

Puis, supposons que $s_{j,i} = r_{j,i}$ pour l'exposant $v_j - 1$. On a que

$$(A/(p_j^{v_j-1}))^{s_{j,1}} \times \cdots \times (A/(p_j))^{s_{j,v_j-1}} \cong p_j K_j = p_j M_j \cong (A/(p_j^{v_j-1}))^{r_{j,1}} \times \cdots \times (A/(p_j))^{r_{j,v_j-1}}.$$

Donc l'hypothèse inductive implique que $r_{j,i} = s_{j,i}$ pour $i \in \{1, \ldots, v_j - 1\}$. Finalement, on a que

$$(A/(p_j))^{s_{j,1}+\cdots+s_{j,v_j}} \cong K_j/p_jK_j = M_j/p_jM_j(A/(p_j))^{r_{j,1}+\cdots+r_{j,v_j}}.$$

Alors, le cas quand $v_j = 1$ implique que $s_{j,1} + \cdots + s_{j,v_j} = r_{j,1} + \cdots + r_{j,v_j}$ aussi et, par conséquent, que $r_{j,v_j} = s_{j,v_j}$. Ceci conclut l'étape inductive et, par la suite, la preuve de l'unicité des diviseurs élémentaires.

Étape 4 : existence des facteurs invariables. Tout d'abord, si $\mathrm{Tor}(M) = (0)$, le résultat est évident. Supposons, alors, que $\mathrm{Tor}(M) = (0)$.

D'après (7.3), on a que

$$M \cong A^r \times \oplus_{j=1}^{J} \left\{ \underbrace{A/(p_j^{v_j}) \times \cdots \times A/(p_j^{v_j})}_{r_{j,1} \text{ fois}} \times \cdots \times \underbrace{A/(p_j) \times \cdots \times A/(p_j)}_{r_{j,v_j} \text{ fois}} \right\}, \tag{7.5}$$

où $r_{j,1} \geq 1$ pour tout $j \in \{1, \ldots, J\}$. En utilisant cette représentation de M, on va construire $a_1, a_2, \ldots, a_k$ tels que $a_k | a_{k-1} | \cdots | a_1$.

On pose

$$a_1 = p_1^{v_1} p_2^{v_2} \cdots a_J^{v_J} = p_1^{v_{1,1}} p_2^{v_{1,2}} \cdots p_J^{v_{1,J}}.$$

Puis, on pose

$$a_2 = p_1^{v_{2,1}} p_2^{v_{2,2}} \cdots p_J^{v_{2,J}},$$

où $v_{2,j}$ est le plus grande exposant qui apparait à la relation (7.5) après l'enlèvement de $A/(p_j^{v_j})$ (si il n'existe pas un tel exposant, on pose $v_{2,j} = 0$). Puis, on pose

$$a_3 = p_1^{v_{3,1}} p_2^{v_{3,2}} \cdots p_J^{v_{3,J}},$$

où $v_{3,j}$ est le plus grande exposant qui apparait à la relation (7.5) après l'enlèvement de $A/(p_j^{v_{1,j}})$ et $A/(p_j^{v_{2,j}})$ (si il n'existe pas un tel exposant, on pose $v_{3,j} = 0$).

Si on continue de cette manière, on obtient une suite $a_1, a_2, \ldots$ telle que $a_i | a_{i-1}$ pour tout $i \geq 2$. Naturellement, il existe un indice k tel que $a_{k+1} = 1$ et $a_k \notin A^\times$. Par construction, la suite $a_1, \ldots, a_k$ satisfait les relations $(0) \subsetneq (a_1) \subset (a_2) \subset \cdots \subset (a_k) \subsetneq A$ et $M \cong A^r \cong$

$A/(a_1) \times A/(a_2) \times \cdots \times A/(a_k)$. Cette dernière relation suit par le théorème des restes chinois, qui implique que $A/(ab) \cong A/(a) \times A/(b)$ si a et b sont deux éléments copremiers de $A \setminus \{0\}$. L'isomorphisme obtenu par le théorème des restes chinois est d'anneaux mais il est facile de déduire qu'il est également un isomorphisme de A-modules.

Étape 5 : unicité des facteurs invariables. Supposons que $M \cong A^r \times A/(b_1) \times A/(b_2) \times \cdots \times A/(b_\ell)$, où $(0) \subsetneq (b_1) \subset (b_2) \subset \cdots \subset (b_\ell) \subsetneq A$. En factorisant $b_1, \ldots, b_\ell$ dans leur facteurs premiers et en utilisant le théorème des restes chinois, on trouve une représentation de M similaire à celle donnée dans la relation (7.5). L'unicité des diviseurs élémentaires implique que la liste des puissances de des nombres premiers que apparait est exactement la même avec la liste respective à la relation (7.5). Donc on peut montrer de façon inductive que les nombres $b_1, \ldots, b_\ell$ sont exactement les nombres $a_1, \ldots, a_k$ apparaissant ci-dessus, modulo multiplication par d'éléments inversibles de A (la condition $b_\ell | b_{\ell-1}| \cdots |b_1$ implique qu'ils sont obtenus en suivant la même procédure). □

7.2 Preuve des résultats intermédiaires

Démonstration de la proposition 7.2. Le résultat découle du théorème 6.48. On peut aussi donner un argument alternatif en utilisant le fait que A est principal ici.

Soit $S = \{s_1, \ldots, s_r\}$ une base de M. Posons $M_0 = (0)$ et $M_j = (s_1, \ldots, s_j)$ pour chaque $j \in \{1, \ldots, r\}$. On va montrer le résultat quand $N \subset M_j$ par induction sur j. Si $j = 0$, il est évident. Supposons que il est vrai pour un $j \in \{1, \ldots, k-1\}$ et considérons $N \subset M_{j+1} = M_j \oplus (s_{j+1})$. Soit

$$I = \{a \in A : \exists m \in M_j \text{ tel que } m + as_{j+1} \in N\}.$$

Il est facile de montrer que I est un idéal de A. En particulier, il existe $\alpha \in A$ tel que $I = (\alpha)$. Si $\alpha = 0$, alors $N \subset M_j$ et le résultat suivi par l'hypothèse inductive. Supposons maintenant que $\alpha \neq 0$. Par définition, il existe $m_0 \in M_j$ tel que $w := m_0 + as_{j+1} \in N$. L'ensemble $N \cap M_j$ est un sous-module de M contenu dans M_j. Donc l'hypothèse inductive implique qu'il existe une base $\{t_1, \ldots, t_\ell\}$ de $N \cap M_j$ de $\ell \leq j$ éléments. On affirme que $\{t_1, \ldots, t_\ell, w\}$ est une base de N. D'abord, si $m \in N \subset M_{j+1}$, alors $m = a_1 s_1 + \cdots + a_j s_j + a_{j+1} s_{j+1}$ pour quelques $a_1, \ldots, a_{j+1} \in A$. On a que $a_{j+1} \in I = (\alpha)$ et, par suite, $a_{j+1} = b\alpha$ pour un $b \in A$. On a que $m - bw = a_1 s_1 + \cdots + a_j s_j - bm_0 \in M_j$. Mais on a aussi que $m - bw \in N$ car $m, w \in N$. Donc $m - bw \in N \cap M_j = (t_1, \ldots, t_\ell)$, qui implique que $m \in (t_1, \ldots, t_\ell, w)$. Il reste de montrer que l'ensemble $\{t_1, \ldots, t_\ell, w\}$ est linéairement indépendant. Si $a_1 t_1 + \cdots + a_\ell t_\ell + a_{\ell+1} w = 0$, alors $(a_1 t_1 + \cdots + a_\ell t_\ell + a_{\ell+1} m_0) + (a_{\ell+1})\alpha) s_{j+1}$. Puisque $(a_1 t_1 + \cdots + a_\ell t_\ell + a_{\ell+1} m_0) \in M_j = (s_1, \ldots, s_j)$ et les éléments $s_1, \ldots, s_{j+1}$ sont linéairement indépendants, on trouve que $\alpha a_{\ell+1} = 0$. Mais A est intègre et $\alpha \neq 0$, donc $a_{\ell+1} = 0$. Alors on conclut que $a_1 t_1 + \cdots + a_\ell t_\ell = 0$ et l'indépendance linéaire des $t_1, \ldots, t_\ell$ implique que $a_1 = \cdots = a_\ell = 0$. Ça conclut la preuve que l'ensemble $\{t_1, \ldots, t_\ell, w\}$ est une base de N. Donc N est libre et a rang $\ell + 1 \leq j + 1$, qui complet l'étape inductive. □

Démonstration de la Proposition 7.3. Soit $M = (m_1, \ldots, m_n)$. On considère $S = \{s_1, \ldots, s_r\}$ qui est contenu à $\{m_1, \ldots, m_n\}$, est libre et a cardinalité maximale. (Un tel r fini existe car M est noetherien.) On montrera que, pour tout j, il existe $a_j \in A \setminus \{0\}$ tel que $m_j \in (S)$.

Si $m_j \in S$, ceci est évident : on peut simplement prendre $a_j = 1$, pour que $a_j m_j = m_j \in S \subset (S)$.

Si $m_j \notin S$, alors la maximalité de S implique qu'il existe $a_j, b_1, \ldots, b_k \in A$ n'étant pas tous zéro et tels que

$$a_j m_j + b_1 s_1 + \cdots + b_r s_r = 0.$$

Si $a_j = 0$, alors l'indépendance de S implique que $b_1 = \cdots = b_r = 0$, une contradiction. Alors, $a_j \neq 0$ et $a_j m_j = -(b_1 s_1 + \cdots + b_k s_k) \in (S)$, comme on l'affirmé.

Puisque $a_j \neq 0$ pour tout j, alors $a := a_1 \cdots a_k \neq 0$. De plus, on a que $a m_j \in (S)$ pour tout j et, puisque $M = (m_1, \ldots, m_n)$, on a que $aM \subset (S)$. Le module (S) est libre sur r éléments. D'après la proposition 7.2, le module aM doit être libre. Mais $M \cong aM$ (l'application $m \to am$ est linéaire, surjective et injective car $\mathrm{Tor}(M) = (0)$), donc M est libre. □

Démonstration de la proposition 7.4. Le module quotient $M/\mathrm{Tor}(M)$ n'a pas de torsion. Il est aussi de type fini car M l'est. La proposition 7.3 implique alors que $M/\mathrm{Tor}(M)$ est libre de rang fini. Soit $\{\overline{s}_1, \ldots, \overline{s}_r\}$ une base de $M/\mathrm{Tor}(M)$, où $s_i \in M$ pour chaque i. On pose $L = (s_1, \ldots, s_r)$ et on affirme que L est libre. En effet, si $a_1 s_1 + \cdots + a_r s_r = 0$, alors $a_1 \overline{s}_1 + \cdots + a_r \overline{s}_r = \overline{0}$, donc $a_1 = \cdots = a_r = 0$ par l'indépendance de $\{\overline{s}_1, \ldots, \overline{s}_r\}$.

On a que $M = L + \mathrm{Tor}(M)$: si $m \in M$, il existe $a_1, \ldots, a_r \in A$ tels que $\overline{m} = a_1 \overline{s}_1 + \cdots + a_r \overline{s}_r$. Alors, $t := m - (a_1 s_1 + \cdots + a_r s_r) \in \mathrm{Tor}(M)$, qui montre que $m \in L + \mathrm{Tor}(M)$. Finalement, on a que $M = L \oplus \mathrm{Tor}(M)$ car $L \cap \mathrm{Tor}(M) = \mathrm{Tor}(L) = (0)$ (on a utilise ici que L n'a pas de torsion comme un module libre). Ceci implique que $M = L \oplus \mathrm{Tor}(M)$, comme on l'a affirmé. □

Démonstration de la proposition 7.5. Notre hypothèse implique qu'on peut écrire $M = M_1 \oplus M_2$, où $M_1 \cong A^r$ et $M_2 \cong N$. Evidemment, $M_2 \subset \mathrm{Tor}(M)$. Réciproquement, si $m \in \mathrm{Tor}(M)$, alors $am = 0$ pour un $a \in A \setminus \{0\}$. On écrit $m = m_1 + m_2$, où $m_1 \in M_1$ et $m_2 \in M_2$. Donc $0 = am = am_1 + am_2$, ce qui implique que $am_1 = 0$, c'est-à-dire, $m_1 \in \mathrm{Tor}(M_1)$. Mais M_1 est un module libre, alors il n'a pas de torsion, et on conclut que $m_1 = 0$. Donc $m = m_2 \in M_2$, ce qui démontre que $M_2 = \mathrm{Tor}(M)$.

Finalement, on a que

$$M/\mathrm{Tor}(M) = (M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2) = M_1/(0) \cong M_1,$$

où on a utilisé la relation $M_1 \cap M_2 = (0)$, une conséquence du fait que $M = M_1 \oplus M_2$. □

Démonstration de la proposition 7.6. Observons que $a \in \mathrm{Ann}(M) \Leftrightarrow M = \{m \in M : am = 0\}$. Puis, l'annulateur de M est un idéal de A (Devoir 7). De plus, l'hypothèse que M est de type fini et le fait que A est intègre (comme principal) impliquent que $\mathrm{Ann}(M) \neq (0)$. (Devoir 7). Puisque A est principal, il existe $a \in A \setminus \{0\}$ tel que $\mathrm{Ann}(M) = (a)$. □

Démonstration de la proposition 7.7. Puisque $\mathrm{pgcd}(a, b) = 1$ et A est principal, il existe $x, y \in A$ tels que $ax + by = 1$. Donc si $m \in M$, alors $m = m_1 + m_2$, où $m_1 = (ax)m$ et $m_2 = (by)m$. Si $(ab)m = 0$, on trouve que $bm_1 = 0$ et que $am_2 = 0$. Donc

$$\{m \in M : (ab)m = 0\} \subset \{m \in M : am = 0\} + \{m \in M : bm = 0\}.$$

L'inclusion inverse est evidente. Donc

$$\{m \in M : (ab)m = 0\} = \{m \in M : am = 0\} + \{m \in M : bm = 0\}.$$

Finalement, si $m \in \{m \in M : am = 0\} \cap \{m \in M : bm = 0\}$, alors

$$m = 1 \cdot m = (ax + by)m = (ax)m + (by)m = 0,$$

qui montre que $\{m \in M : am = 0\} \cap \{m \in M : bm = 0\} = (0)$. Ça conclut la preuve que

$$\{m \in M : (ab)m = 0\} = \{m \in M : am = 0\} \oplus \{m \in M : bm = 0\}.$$

□

Lemme 7.9. *Supposons que p est un nombre premier de A et v un nombre naturel tel que $p^v M = (0)$ et $p^{v-1}M \neq (0)$, et soit $m \in M$ tel que $p^{v-1}m \neq 0$.*

(a) Si $M \neq (m)$, alors il existe $m' \in M \setminus \{0\}$ tel que $(m) \cap (m') = (0)$.

(b) Il existe un sous-module N de M tel que $M = (m) \oplus N$.

Démonstration. (a) Soit $m_0 \in M \setminus \{m\}$. On a que $p^v m_0 = 0 \in (m)$ et $1 \cdot m_0 \notin (m)$. Donc il existe $j \in \{1, \ldots, v\}$ tel que $p^j m_0 \in (m)$ et $p^{j-1}m_0 \notin (m_0)$. En particulier, $p^j m_0 = am$ pour un $a \in A$. Donc $0 = p^{v-j}am$. On affirme que $p^v | p^{v-j}a$. Soit $d = \text{pgcd}(p^v, p^{v-j}a)$. Alors $d = xp^v + yp^{v-j}a$ pour quelques $x, y \in A$ et, conséquement, $dm = 0$. Mais d est une puissance de p et on a suppose que $p^{v-1}m \neq 0$. Donc $p^v | d$, qui montre que $p^v | p^{v-j}a$. On déduit que $p^j | a$, c'est-à-dire, $a = p^j b$ pour un $b \in A$. Posons $m' = p^{j-1}m_0 - (p^{j-1}b)m$. On a que $m' \notin (m)$ car $p^{j-1}m_0 \notin (m)$. En particulier, $m' \neq 0$. De plus, $pm' = p^j m_0 - (p^j b)m = p^j m_0 - am = 0$. On affirme que $(m) \cap (m') = (0)$. Sinon, alors il existe $n = \lambda m = \mu m' \in (m) \cap (m') \setminus \{0\}$ pour quelques $\lambda, \mu \in A$. Nécessairement, $p \nmid \lambda$. Sinon, on aurait que $n = 0$, qui est une contradiction. Donc $\text{pgcd}(p, \lambda) =$ et, par suite, $zp + w\lambda = 1$ pour quelques $z, w \in A$. Donc $m' = (zp + w\lambda)m' = w(\lambda m') = wn \in (m)$, qui est une contradiction. On a alors montré que $(m) \cap (m') = (0)$, ce qui termine la preuve.

(b) Soit $\mathscr{S} = \{K \text{ sous-module de } M : K \cap (m) = (0)\}$. On a que $(0) \in \mathscr{S}$. Aussi, il est facile de vérifier que $\mathscr{S}$ satisfait les hypothèses du lemme de Zorn par rapport à la relation d'"inclusion d'ensembles. Donc il existe $N \in \mathscr{S}$ qui est maximal par rapport à l'inclusion. On affirme que $M = N + (m)$. On considère le module quotient M/N. Puisque $N \cap (m) = (0)$, on a que $(N + (m))/N = (\overline{m})$, où $\overline{m}$ est la classe d'équivalence de m modulo N. Donc, pour montrer que $M = N + (m)$, il suffit de montrer que $M/N = (\overline{m})$ (ici on utilise le théorème de correspondance pour les modules). Evidemment, $p^v(M/N) = (\overline{0})$. De plus, $p^{v-1}m \notin N$ car $p^{v-1}m \neq 0$ et $N \cap (m) = (0)$. Donc $p^{v-1}(M/N) \supset (\overline{m}) \neq (\overline{0})$. Alors, si $M/N \neq (\overline{m})$, la partie (a) implique que il existe $m' \in M \setminus N$ tel que $(\overline{m}) \cap (\overline{m'}) = (\overline{0})$. On a que $N + (m') \subset\neq N$. De plus, $(N + (m')) \cap (m) = (0)$: en effet, si $x \in (N + (m')) \cap (m)$, alors $x = n + am' = bm$, où $n \in N$ et $a, b \in A$. Donc $a\overline{m'} = b\overline{m}$ et, puisque $(\overline{m'}) \cap (\overline{m}) = (\overline{0})$, on conclut que $a\overline{m'} = b\overline{m} = \overline{0}$, c'est-à-dire, $am', bm \in N$. Mais c'implique $x \in N$. Puisque $x \in (m)$ aussi et $N \cap (m) = (0)$, on conclut que $x = 0$, qui termine la preuve de notre affirmation que $(N + (m')) \cap (m) = (0)$. Mais c'est impossible car N est un élément maximal de $\mathscr{S}$. La contradiction a été causée par notre hypothèse que $M/N \neq (\overline{m})$. Donc $M/N = (\overline{m})$, ce qui termine la démonstration. □

Démonstration de la proposition 7.8. Si $p^{v-1}M = (0)$, on peut prendre $r = 0$ et $N = M$. Si $p^{v-1}M \neq (0)$, il existe $m_1 \in M$ tel que $p^{v-1}m_1 \neq 0$ et Lemme 7.9(b) implique que $M = (m_1) \oplus M_1$, pour un sous-module M_1 de M. Si $p^{v-1}M_1 = (0)$, alors le résultat suivit avec $r = 1$ et $M = M_1$ (on a que $(m_1) \cong A/(p^v)$ car $p^v m_1 = 0$ et $p^{v-1}m \neq 0$). Si $p^{v-1}M_1 \neq (0)$, alors il existe $m_2 \in M_2$ avec $p^{v-1}m_2 \neq 0$ et Lemme 7.9(b) implique que $M_1 = (m_2) \oplus M_2$ pour un sous-module M_2 de M_1. On continue inductivement comme au-dessus. La procédure va terminer car M est noethérien. Donc il existe $m_1, \ldots, m_r \in M$ et N sous-module de M tels que $p^{v-1}m_1, \ldots, p^{v-1}m_r \neq 0$, $p^{v-1}N = (0)$, et $M = (m_1) \oplus \cdots \oplus (m_r) \oplus N$. Puisque $(m_j) \cong A/(p^v)$ (par les hypothèses que $p^v m = 0$ et $p^{v-1}m \neq 0$), le résultat désiré suit. □

7.3 Exercices

EXERCICE 7.1. Trouvez les diviseurs élémentaires et les facteurs invariables des groupes

$$\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$$

et

$$(\mathbb{Z}/2016\mathbb{Z})^\times.$$

Chapitre 8

Théorie spectrale des matrices

8.1 Valeurs propres et forme de Jordan

Étant donnée une application linéaire $T : V \to V$, où V est un espace vectoriel de dimension $n < \infty$ sur le corps K, on cherche une base de V pour la quelle l'action de T est aussi simple que possible. La situation la plus simple est quand on peut trouver une base $B := \{v_1, \ldots, v_n\}$ telle que

$$T(x_1v_1 + \cdots + x_nv_n) = \lambda_1x_1v_1 + \cdots + \lambda_nx_nv_n$$

pour quelques $\lambda_1, \ldots, \lambda_n \in K$. C'est-à-dire, si $(x_1, \ldots, x_n)$ sont les coordonnés du vecteur v par rapport à la base B, alors $T(v)$ a coordonnés $(\lambda_1x_1, \ldots, \lambda_nx_n)$, obtenues tout simplement en multipliant le j-ième coordonné de v par λ_j.

Remarque 8.1. Géométriquement, quand $K = \mathbb{R}$, il est assez facile de visualiser l'action de T sur V si on identifie B avec la base standard. (Si $n = 2$, $\lambda_1 = 1$ et $\lambda_2 = 2$, quelle est l'image d'un circle sous T ?)

La matrice associée à T par rapport à la base B est la matrice diagonale

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}.$$

Pour cette raison, si V admet une telle base, on appelle T une application **diagonalisable**.

Les éléments λ_j sont de **valeurs propres** de T :

Définition 8.2. Soient V un K-espace vectoriel et $T : V \to V$ une application linéaire. Un vecteur $v \in V \setminus \{0\}$ est appelé un **vecteur propre de** T s'il existe $\lambda \in K$ tel que $T(v) = \lambda v$. Dans ce cas-ci, le multiplicateur λ est appelé une **valeur propre de** T.

Le calcul des valeurs propres est fait au niveau de matrices : évidemment, $\lambda \in K$ est une valeur propre s-si $T - \lambda I$ n'est pas injective, où $I : V \to V$ est l'application-identité de V.

Si on fixe une base $\{v_1, \ldots, v_n\}$ dont la matrice associée par rapport à T est $A \in M_n(K)$, alors λ est une valeur propre de T s-si la matrice $A - \lambda I$ a un vecteur non-trivial dans son noyau, où I ici dénote la matrice-identité de $M_n(K)$. De façon équivalente, λ est une racine du **polynôme caractéristique** de A, défini par

$$c_A(x) := \det(xI - A).$$

Le polynôme c_A ne dépend pas de la base qu'on a choisi : si $\{w_1, \ldots, w_n\}$ est une autre base dont la matrice associée par rapport à T est $A \in M_n(K)$, alors on sait que B et A sont semblables (voir l'exemple 6.16), c'est-à-dire il existe $P \in \mathrm{GL}_n(K)$ telle que $B = P \cdot A \cdot P^{-1}$. Par la suite,

$$xI - B = P \cdot (xI - A) \cdot P^{-1},$$

d'où

$$c_B(x) = \det(P) c_A(x) \det(P^{-1}).$$

Puisque $\det(P)\det(P^{-1}) = \det(I) = 1$ (voir l'exercice 6.8(ii)), on trouve que $c_B = c_A$. Cette observation nous permet de définir le **polynôme caractéristique** de T par

$$c_T(x) := \det(xI - A).$$

Il ne dépend pas du choix de la base $\{v_1, \ldots, v_n\}$.

On résume la discussion ci-dessus dans le théorème suivant :

Théorème 8.3. *Soient V un K-espace vectoriel de dimension finie, $T : V \to V$ une application linéaire, et $\lambda \in K$. Les propositions suivantes sont équivalentes :*

(a) λ est une valeur propre de T ;
(b) l'application $T - \lambda I$ n'est pas injective, où $I : V \to V$ est l'application-identité de V ;
(c) λ est une racine du polynôme caractéristique de T.

Supposons, maintenant, qu'on fixé une base $\{v_1, \ldots, v_n\}$ et sa matrice associée A. On dit que A est **diagonalisable** s'il est semblable à une matrice diagonale.

Il existe de matrices qui ne sont pas diagonalisables, donc ce n'est pas toujours possible de trouver une base de V consistant que de vecteurs propres de T. Comme on va le voir, un exemple simple est donné par la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Jordan a montré quand même que chaque matrice est 'proche' d'être diagonalisable :

Théorème 8.4. *Soient K un corps et $A \in M_n(K)$. Supposons que contient toutes les racines du polynôme caractéristique de A. Donc, A est semblable à une matrice de la forme*

$$\begin{pmatrix} J_{m_1}(\lambda_1) & & & \\ & J_{m_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{m_s}(\lambda_s) \end{pmatrix},$$

où $m_1+\cdots+m_j = n$, la liste $\lambda_1, \ldots, \lambda_s$ comprend toutes les valeurs propres de A, possiblement avec répétitions, et

$$J_m(\lambda) := \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \in M_m(K).$$

Cette representation est appelée la **forme de Jordan** *de A et elle unique modulo une permutation des matrices $J_{m_1}(\lambda_1), \ldots, J_{m_j}(\lambda_j)$, qui sont appelées les* **bloques de Jordan** *de A.*

Remarque 8.5. Il est possible que $\lambda_j = \lambda_{j'}$ pour $j \neq j'$. En fait, si λ est une valeur propre de A dont la multiplicité comme racine du polynôme $c_A(x)$ est μ (i.e. $(x-\lambda)^\mu | c_A(x)$ mais $(x-\lambda)^{\mu+1)} \nmid c_A(x)$, alors λ apparaît exactement μ fois parmi les membres de la liste

$$\underbrace{\lambda_1, \ldots, \lambda_1}_{m_1 \text{ fois}}, \underbrace{\lambda_2, \ldots, \lambda_2}_{m_2 \text{ fois}}, \ldots, \underbrace{\lambda_s, \ldots, \lambda_s}_{m_s \text{ fois}}.$$

Effectivement, si $J = J_m(\lambda)$, alors on peut calculer directement que $c_J(x) = (x-\lambda)^m$. Donc, le polynôme caractéristique de A est égal à

$$c_A(x) = \prod_{j=1}^{s} c_{J_{m_j}(\lambda_j)}(x) = \prod_{j=1}^{s} (x-\lambda_j)^{m_j},$$

d'où on déduit notre affirmation.

Le but de ce chapitre est de montrer le théorème 8.4.

Exemple 8.6. La matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

est déjà en forme de Jordan. De plus, cette forme n'est pas une matrice diagonale. Donc, A n'est pas diagonalisable.

On a que $c_A(x) = (x-1)^2$. Donc, la seule valeur propre de A est $\lambda = 1$. L'espace de vecteurs $v \in \mathbb{R}^2$ tels que $(A-I)v = 0$ a dimension 1. Donc, il n'existe pas une base de vecteurs propres.

Un critère simple pour décider si une matrice est diagonalisable est donné au corollaire suivant :

Corollaire 8.7. *Soient K un corps et $A \in M_n(K)$. Supposons que contient toutes les racines du polynôme caractéristique de A, et que toutes ces racines sont simples. Donc, A est diagonalisable.*

Remarque 8.8. Si une matrice A est diagonalisable, c'est-à-dire semblables à une matrice diagonale

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix},$$

alors ceci est la forme de Jordan de A. De plus, les nombres $\lambda_1, \ldots, \lambda_n$ sont toutes les valeurs propres de A, listées avec leur multiplicités comme racines du polynôme caractéristique de A.

8.2 Sous-espaces stables

L'idée-clé pour diagonaliser une matrice ou une application linéaire est d'étudier leur espaces stables :

Définition 8.9. Soient V un K-espace vectoriel et $T : V \to V$ une application linéaire. Un sous-espace U de V est appelé un **sous-espace stable par** T si $T(U) \subset U$.

Exemple 8.10. Soit $v \in V \setminus \{0\}$ et $U = \langle v \rangle$, l'espace engendré par v. Alors U est stable par T s-si $T(U) \subset U$, s-si $T(v) \in U$, s-si $T(v) = \lambda v$ pour un $\lambda \in K$, s-si v est un vecteur propre de T.

Lemme 8.11. *Soient V un K-espace vectoriel, $T : V \to V$ une application linéaire, et $U \subset V$. Alors, U est sous-espace stable par T s-si il est un $K[x]$-sous-module de V.*

Démonstration. Si $T(U) \subset U$, alors $T^n(U) \subset U$ par induction. Par linéarité, on en déduit que $f(x) \cdot u \in U$ pour tout $u \in U$ et tout $f(x) \in K[x]$. De plus, U est un sous-groupe additif de V. Donc, il est un $K[x]$-sous-module de V.

Réciproquement, supposons que U est un $K[x]$-sous-module de V. En particulier, il est un sous-espace de V. De plus, $T(u) = x \cdot u \in U$ pour chaque $u \in U$. Donc, U est un sous-espace stable par T. □

Lemme 8.12. *Soit V un $K[x]$-module, où K est un corps et $\dim_K(V) < \infty$.*

Supposons qu'il existe deux sous-modules W et U de V tels que $V = W \oplus U$. Si $T : V \to V$ est l'application définie par $T(v) = x \cdot v$, alors il existe une base de V pour la quelle la matrice associée à T est de la forme

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \tag{8.1}$$

où $A \in M_r(K)$ et $B \in M_s(K)$ avec $r = \dim_K(W)$ et $s = \dim_K(U)$.

Vice versa, s'il existe une base pour laquelle la matrice associée à T est de la forme (8.1), alors il existe deux sous-modules de V, soient W et U, tels que $r = \dim_K(W)$, $r' = \dim_K(U)$ et $V = W \oplus U$.

Démonstration. Si $\{w_1, \dots, w_r\}$ est une base de W et $\{u_1, \dots, u_s\}$ est une base de U, alors leur reunion est une base de V. (Montrer cette affirmation comme un exercice.) Si $n = r+s = \dim_K(V)$, alors il existe $a_{i,j} \in K$ tels que

$$T(w_1) = a_{1,1}w_1 + \cdots + a_{r,1}w_r + a_{r+1,1}u_1 + \cdots + a_{n,1}u_s.$$

Puisque W est un sou-module de V, il est stable par T. Donc, $T(w_1) \in W$, ce qui implique que $a_{r+1,1} = \cdots = a_{n,1} = 0$.

De même, on trouve que

$$T(w_j) = a_{1,j}w_1 + \cdots + a_{r,j}w_r \tag{8.2}$$

pour quelques $a_{1,j} \in K$, ainsi que

$$T(u_j) = b_{1,j}u_1 + \cdots + b_{s,j}u_s \tag{8.3}$$

pour quelques $b_{i,j} \in K$. Donc, la matrice de T correspondante à la base $\{w_1, \dots, w_r, u_1, \dots, u_s\}$ est égale à

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

où $A = (a_{i,j})_{i,j=1}^r$ et $B = (b_{i,j})_{i,j=1}^s$.

Réciproquement, s'il existe une base $\{w_1, \dots, w_r, u_1, \dots, u_s\}$ pour laquelle la matrice de T est

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

où $A = (a_{i,j})_{i,j=1}^r$ et $B = (b_{i,j})_{i,j=1}^s$, alors on a les relations (8.2) et (8.3). Alors, si $W = \mathrm{Span}_K(w_1, \dots, w_r)$ et $U = \mathrm{Span}_K(u_1, \dots, u_s)$, on a que W et U sont stables par T, c'est-à-dire ils sont de sous-modules de V selon le lemme 8.11. Finalement, c'est facile de voir que $V = W \oplus U$. □

8.3 Preuve de l'existence de la forme de Jordan

Soit $V = K^n$ qu'on réalise comme vecteurs-colonnes, et considérons l'action de A sur cet espace par multiplication :

$$T(v) := A \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad \text{où} \quad v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

L'observation clé est que V est un $K[x]$-module de torsion par rapport au produit interne

$$(a_0 + a_1x + \cdots + a_dx^d) \cdot v := a_0v + a_1T(v) + \cdots + a_dT^d(v)$$

(voir l'exemple 6.8 et le lemme 6.34). De plus, il est de type fini car V est un espace vectoriel de dimension finie sur K. Puisque $K[x]$ est un anneau principal, le théorème des facteurs

invariants implique qu'il existe de polynômes irréductibles $p_1(x), \ldots, p_\ell(x)$ et d'entiers positifs $m_1, \ldots, m_\ell$ tels que

$$V \cong K/(p_1(x)^{m_1}) \times \cdots \times K/(p_s(x)^{m_s}).$$

(On observe que le rang $r = 0$ car V est un $K[x]$-module de torsion.)

Lemme 8.13. *Soit $T : V \to V$ une application linéaire sur le K-espace vectoriel V. On sait que T rend V un $K[x]$-module. Supposons que $V \cong K/(f(x))$ comme un $K[x]$-module, où $f(x) = a_0 + a_1 + \cdots + a_{d-1}x^{d-1} + x^d$. Alors, $d = \dim_K(V)$ et on peut choisir une base de V dont la matrice associé par rapport à T est*

$$\mathcal{C}_{f(x)} := \begin{pmatrix} & & & -a_0 \\ 1 & & & -a_1 \\ & 1 & & -a_2 \\ & & \ddots & \vdots \\ & & 1 & -a_{d-1} \end{pmatrix} \in M_n(K).$$

Le polynôme caractéristique de cette matrice est égale à $f(x)$, donc $c_T(x) = f(x)$.

Démonstration. D'après la division euclidienne, chaque polynôme $g(x) \in K[x]$ peut s'écrire de façon unique comme $g(x) = f(x)q(x) + c_0 + c_1 + \cdots + c_{d-1}x^{d-1}$. Donc, $g(x) \equiv c_0 \cdot 1 + c_1 \cdot x + \cdots + c_{d-1}x^{d-1} \pmod{f(x)}$, et les coefficients $c_0, c_1, \ldots, c_{d-1}$ sont uniques. Ceci implique que le quotient $K[x]/(f(x))$ est un K-espace vectoriel de dimension d, ainsi que les classes d'équivalences $\overline{1}, \overline{x}, \ldots, \overline{x}^{d-1}$ forme une base de cet espace. L'action de T à V alors peut être déterminée par l'action de la multiplication par x à cette base :

$$\begin{aligned} x \cdot \overline{1} &= \overline{x} = 0 \cdot \overline{1} + 1 \cdot \overline{x} + 0 \cdot \overline{x}^2 + 0 \cdot \overline{x}^3 + \cdots + 0\overline{x}^{d-1} \\ x \cdot \overline{x} &= \overline{x}^2 = 0 \cdot \overline{1} + 0 \cdot \overline{x} + 1 \cdot \overline{x}^2 + 0 \cdot \overline{x}^3 + \cdots + 0\overline{x}^{d-1} \\ &\vdots \\ x \cdot \overline{x}^{d-2} &= \overline{x}^{d-1} = 0 \cdot \overline{1} + 0 \cdot \overline{x} + 0 \cdot \overline{x}^2 + \cdots + 0 \cdot \overline{x}^{d-2} + 1\overline{x}^{d-1} \\ x \cdot \overline{x}^{d-1} &= \overline{x}^d = -c_0 \cdot \overline{1} - c_1 \cdot \overline{x} - c_2 \cdot \overline{x}^2 - \cdots - c_{d-1}\overline{x}^{d-1}. \end{aligned}$$

Donc la matrice associée à cette base est $\mathcal{C}_{f(x)}$.

Finalement, on calcule le polynôme caractéristique de $\mathcal{C}_{f(x)}$: on a que

$$\det(xI - \mathcal{C}_{f(x)}) = \det \begin{pmatrix} x & & & a_0 \\ -1 & x & & a_1 \\ & -1 & & a_2 \\ & & \ddots & \vdots \\ & & -1 & x + a_{d-1} \end{pmatrix}.$$

En développant le déterminant par rapport à la première ligne, on trouve que

$$\det(xI - \mathcal{C}_{f(x)}) = x \cdot \det \begin{pmatrix} x & & & a_1 \\ -1 & x & & a_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{d-1} \end{pmatrix} + (-1)^{d+1}a_0 \cdot \det \begin{pmatrix} -1 & x & & \\ & -1 & x & \\ & & \ddots & x \\ & & & -1 \end{pmatrix}$$

$$= x \det \begin{pmatrix} x & & & a_1 \\ -1 & x & & a_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{d-1} \end{pmatrix} + a_0.$$

En continuant de façon inductive, on trouve que

$$\det(xI - \mathcal{C}_{f(x)}) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d = f(x),$$

ce qui conclut la démonstration. □

Lemme 8.14. *Supposons que V, V_1, V_2 sont de $K[x]$-modules tels que $V \cong V_1 \times V_2$. Si $T : V \to V$, $T_1 : V_1 \to V_1$ et $T_2 : V_2 \to V_2$ sont les applications linéaires associées, alors*

$$c_T = c_{T_1} c_{T_2}.$$

Démonstration. En identifiant V avec $V_1 \times V_2$, V_1 avec $V_1 \times \{0\}$, et V_2 avec $\{0\} \times V_2$, on peut supposer que $V = V_1 \oplus V_2$. De plus, dans ce cas-ci, on a que $T_i = T|_{V_i}$. En appliquant (la démonstration de) le lemme 8.12, on peut trouver une base de V dont la matrice associée à T est de la forme

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

où A_i est une matrice représentant T_i. On a que

$$\begin{aligned} c_T(x) = c_A(x) &= \det \begin{pmatrix} xI - A_1 & 0 \\ 0 & xI - A_2 \end{pmatrix} \\ &= \det(xI - A_1) \det(xI - A_2) \\ &= c_{A_1}(x) c_{A_2}(x) \\ &= c_{T_1}(x) c_{T_2}(x). \end{aligned}$$

□

On est prêt de montrer le théorème principal de ce chapitre :

Démonstration du théorème 8.4. Comme on l'a vu au debut de cette section, il existe de polynômes irréductibles $p_1(x), \ldots, p_\ell(x)$ (qu'on peut supposer qu'ils sont unitaires) et d'entiers positifs $m_1, \ldots, m_\ell$ tels que

$$V \cong K/(p_1(x)^{m_1}) \times \cdots \times K/(p_\ell(x)^{m_\ell}).$$

En particulier, les lemmes 8.13 et 8.14 implique que

$$c_A(x) = p_1(x)^{m_1} \cdots p_\ell(x)^{m_\ell}. \tag{8.4}$$

D'autre côté, on a supposé que K contient toutes les valeurs propres de c_A. Ceci veut dire que $c_A(x)$ se décompose complètement dans un produit de facteurs linéaires, soit

$$c_A(x) = \prod_{j=1}^{J} (x - \lambda_j)^{\mu_j}, \tag{8.5}$$

où $\lambda_1, \dots, \lambda_J$ sont les valeurs propres distinctes de A et $\mu_1, \dots, \mu_J \in \mathbb{Z}_{\geq 1}$.

En comparant les factorisations (8.4) et (8.5), on trouve que $p_j(x) = x - \lambda$ pour une valeur propre λ de A.[1] Afin de conclure la conclure la démonstration, il faut trouver une base pour la quelle la matrice correspondante au $K[x]$-module $K[x]/((x-\lambda)^m)$ est le bloque de Jordan

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \in M_m(K).$$

Par la preuve du lemme 8.13, les classes d'équivalences $\overline{1}, \overline{x}, \dots, \overline{x}^{m-1}$ offre une base des polynômes $g(x) \pmod{x^m}$. Donc, les classes d'équivalences $\overline{1}, \overline{x-\lambda}, \dots, \overline{(x-\lambda)^{m-1}}$ offre une base des polynômes $g(x-\lambda) \pmod{(x-\lambda)^m}$, donc une base de $K[x]/((x-\lambda)^m)$ vu comme un K-espace vectoriel. L'action de A à cette base est donnée par l'action de la multiplication par x des membres de la base. En inversant leur ordre, et en écrivant $x = (x-\lambda) + \lambda$, on a que

$$\begin{aligned} x \cdot \overline{(x-\lambda)^{m-1}} &= \lambda \cdot \overline{(x-\lambda)^{m-1}} \\ x \cdot \overline{(x-\lambda)^{m-2}} &= 1 \cdot \overline{(x-\lambda)^{m-1}} + \lambda \cdot \overline{(x-\lambda)^{m-2}} \\ &= 1 \cdot \overline{(x-\lambda)^{m-2}} + \lambda \overline{(x-\lambda)^{m-3}} \\ &\vdots \\ x \cdot \overline{1} &= 1 \cdot \overline{(x-\lambda)} + \lambda \overline{1}. \end{aligned}$$

Ceci conclut la démonstration du théorème 8.4. □

8.4 La forme rationnelle canonique

On se rappelle de la définition des matrices $\mathcal{C}_{f(x)}$, où $f(x) \in K[x]$.

Théorème 8.15. *Soient K un corps et $A \in M_n(K)$. Alors, A est semblable à une matrice de la forme*

$$\begin{pmatrix} \mathcal{C}_{f_1(x)} & & & \\ & \mathcal{C}_{f_2(x)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{f_\ell(x)} \end{pmatrix},$$

où $f_1(x), \dots, f_\ell(x)$ sont de polynômes unitaires sur K tels que

$$f_1(x) | f_2(x) | \cdots | f_\ell(x) \quad \textit{et} \quad f_1(x) f_2(x) \cdots f_\ell(x) = c_A(x).$$

Cette représentation de A est unique ; elle est appelée sa **forme rationnelle canonique**.

1. On remarque ici que c'est possible que $p_j(x) = p_{j'}(x)$ pour $j \neq j'$, c'est-à-dire que la même valeur propre λ apparaît deux fois. Par exemple, c'est possible que $V \cong K[x]/(x-1) \times K[x]/(x-1)$, comme c'est le cas pour la matrice-identité $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Démonstration. L'action de A à l'espace $V = K^n$ de vecteurs-colonnes rend V un $K[x]$-module de type fini et de torsion. Puisque $K[x]$ est un anneau principal, le théorème des facteurs invariants implique qu'il existe de polynômes $f_1(x)|f_2(x)|\cdots|f_\ell(x)$ tels que

$$K^n \cong K/(f_1(x)) \times \cdots K/(f_\ell(x)) \tag{8.6}$$

et avec $f_1(x)|f_2(x)|\cdots|f_\ell(x)$. Certainement, on peut supposer que les polynômes $f_j(x)$ sont unitaires ; sous cette hypothèse, le théorème 7.1 implique que les polynômes $f_1(x), \ldots, f_\ell(x)$ sont uniques. En appliquant les lemmes 8.13 et 8.14, la démonstration est complète. □

Corollaire 8.16 (Cayley-Hamilton)**.** *Soient K un corps et $A \in M_n(K)$. Alors, $c_A(A) = 0$.*

Démonstration. D'après la relation (8.6), on trouve que $f_1(x)\cdots f_\ell(x) \cdot v = 0$ pour tout $v \in K^n$. Puisque $c_A(x) = f_1(x)\cdots f_\ell(x)$, le résultat affirmé en suit. □

Définition 8.17. Soit $T : V \to V$ une application sur le K-espace vectoriel V de dimension finie. Le **polynôme minimal** de T est le polynôme unitaire $m_T(x) \in K[x]$ de degré minimal ayant la propriété que $m_T(T) = 0$.

On identifie T avec une matrice $A \in M_n(K)$. On se rappelle que

$$\mathrm{Ann}_{K[x]}(V) = \{f(x) \in K[x] : f(x) \cdot v = 0 \ \forall v \in V\} = \{f(x) \in K[x] : f(T) = 0\}.$$

Le théorème de Cayley-Hamilton implique que $c_T(x) \in \mathrm{Ann}_{K[x]}(V)$, et la définition de $m_T(x)$ implique que

$$\mathrm{Ann}_{K[x]}(V) = (m_T(x)).$$

D'autre côté, en utilisant la relation 8.6 et le fait que $f_1(x)|f_2(x)|\cdots|f_\ell(x)$, on trouve que

$$\mathrm{Ann}_{K[x]}(V) = (f_\ell(x)).$$

Donc

$$m_T(x) = f_\ell(x).$$

Théorème 8.18. *Soit $T : V \to V$ une application sur le K-espace vectoriel V de dimension finie.*

(a) $m_T(x)|c_T(x)$.
(b) Il existe $\ell \in \mathbb{Z}_{\geq 1}$ tel que $c_T(x)|m_T(x)^\ell$.
(c) Les polynômes $c_T(x)$ et $m_T(x)$ ont la même liste de facteurs irréductibles distincts. En particulier, ils partagent les mêmes racines.

Démonstration. (a) Puisque $\mathrm{Ann}_{K[x]}(V) = (m_T(x))$ et $c_T(x) \in \mathrm{Ann}_{K[x]}(V)$,. il faut que $m_T(x)|c_T(x)$.

(b) On a que $c_T(x) = f_1(x)\cdots f_\ell(x)$, où $f_1(x)|f_2(x)|\cdots|f_\ell(x) = m_T(x)$. Donc $f_j(x)|m_T(x)$ pour chaque j, d'où $c_T(x)|m_T(x)^\ell$.

(c) Si $p(x)$ est un polynôme irréductible de $K[x]$ divisant $m_T(\lambda)$, alors il divise aussi $c_T(x)$ d'après la partie (a). Vice versa, si $p(x)|c_T(x)$, alors $p(x)|m_T(x)^\ell$ d'après la partie (b). Puisque $p(x)$ est irréductible et on est dans un anneau factoriel, il faut que $p(x)|m_T(x)$. □

Théorème 8.19. *Soit K un corps et $A \in M_n(K)$. Alors, A est diagonalisable s-si les deux conditions suivantes sont vraies :*

(a) K contient toutes les racines de $c_A(x)$;

(b) toutes les racines du polynôme $m_A(x)$ sont simples.

Démonstration. Comme avant, soit $V = K^n$ le $K[x]$-module défini par l'action de A sur les vecteurs-colonnes de K^n.

Si A est diagonalisable, il est semblable à une matrice diagonale de $M_n(K)$, soit

$$B = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}.$$

On peut directement calculer que $c_A(x) = c_B(x) = (x - \lambda_1) \cdots (x - \lambda_n)$. C'est-à-dire, $c_A(x)$ se factorise en polynômes linéaires dans $K[x]$. De façon équivalente, K contient toutes les racines de $c_A(x)$.

Pour montrer (b), on observe que le lemme 8.12 implique qu'il existent de sous-modules $V_1, \ldots, V_n$ tels que

$$V = V_1 \oplus \cdots \oplus V_n \quad \text{et} \quad \dim_K(V_i) = 1 \ \forall i.$$

Le même lemme implique aussi qu'il existe de vecteurs non-zéros $v_1, \ldots, v_n$ tels que $V_j = \mathrm{Span}_K(v_j)$ et $Av_j = \lambda_j v_j$. On affirme que $V_j \cong K[x]/(x - \lambda_j)$ comme $K[x]$-modules.

En effet, on a l'application $\phi_j : V_j \to K[x]/(x-\lambda_j)$, définie par $\phi_j(av_j) := a \,(\mathrm{mod}\, x - \lambda_j)$. Clairement, elle est K-linéaire et bijective. Il reste de montrer qu'elle est un morphisme de $K[x]$-modules.

Si $v = av_j \in V_j$, alors on a que $x \cdot v = Aav_j = aAv_j = a\lambda_j v_j = \lambda_j a v_j$, donc

$$\begin{aligned} \phi_j(x \cdot v) = \phi_j(\lambda_j a v_j) &= \lambda_j a \,(\mathrm{mod}\, x - \lambda_j) \\ &\equiv x \cdot a \,(\mathrm{mod}\, x - \lambda_j) \\ &= x \cdot \phi_j(v). \end{aligned}$$

En itérant cette relation, on trouve que $\phi_j(x^m \cdot v) = x^m \phi_j(v)$ pour tout m. Finalement, la K-linéarité de ϕ_j implique que $\phi_j(f(x) \cdot v) = f(x) \cdot \phi_j(v)$ pour tout $f(x) \in K[x]$ et tout $v \in V$. Alors, ϕ_j est un morphisme de $K[x]$-modules.

On a alors montré que $V_j \cong K[x]/(x - \lambda_j)$. Donc

$$V \cong K[x]/(x - \lambda_1) \times \cdots K[x]/(x - \lambda_n).$$

Puis, si $\rho_1, \ldots, \rho_d$ sont les éléments distincts de la liste $\lambda_1, \ldots, \lambda_n$, c'est-à-dire

$$\{\rho_1, \ldots, \rho_d\} = \{\lambda_j : 1 \leq j \leq n\},$$

alors c'est-facile de voir que

$$\mathrm{Ann}_{K[x]}(V) = ((x - \rho_1) \cdots (x - \rho_d)).$$

En particulier, $m_T(x) = (x - \rho_1) \cdots (x - \rho_d)$ a que de racines simples.

Réciproquement, supposons que K contient toutes les racines de $c_T(x)$ et que $m_T(x)$ a que de racines doubles. Si $f_1(x)|f_2(x)| \cdots |f_\ell(x)$ sont les polynômes de la forme rationnelle canonique de T, alors $f_\ell(x) = m_T(x)$ a que de racines simples. De plus, puisque $m_T(x)|c_T(x)$ et $c_T(x)$ se factorise complètement dans $K[x]$, le polynôme $m_T(x)$ a la même propriété. Puisque $f_j(x)|f_\ell(x) = m_T(x)$, alors $f_j(x)$ a aussi que de racines simples et il se factorise complètement dans $K[x]$. Selon le théorème des restes chinois, on sait que les diviseurs élémentaires de V sont obtenus en décomposant les facteurs invariants $f_1(x), \ldots, f_\ell(x)$ dans leurs facteurs irréductibles. La discussion précédente implique que, pour chaque j, le polynôme $f_j(x)$ a $\deg(f_j)$ facteurs linéaires distincts, qui sont forcement ses facteurs irréductibles. Donc, les diviseurs élémentaires de V sont tous de polynômes linéaires. En particulier, il existe $\lambda_1, \ldots, \lambda_n \in K$ tels que

$$V \cong K[x]/(x - \lambda_1) \times \cdots K[x]/(x - \lambda_n).$$

Ceci implique que A est diagonalisable. □

8.5 Un algorithme pour la détermination de la forme rationnelle canonique

Soient K un corps et $A = (a_{i,j})_{i,j=1}^n \in M_n(K)$. Considérons la matrice

$$xI - A = \begin{pmatrix} x - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & x - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & \vdots & & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & x - a_{1,n} \end{pmatrix},$$

qu'on voit comme une matrice sur l'anneau euclidien $K[x]$. On va transformer $xI - A$ à une matrice diagonale

$$\begin{pmatrix} g_1(x) & & & \\ & g_2(x) & & \\ & & \ddots & \\ & & & g_n(x) \end{pmatrix}$$

en utilisant d'opérations élémentaires sur les lignes et les colonnes de $xI - A$. Les polynômes $g_1(x), \ldots, g_n(x)$ vont déterminer les polynômes $f_1(x), \ldots, f_\ell(x)$ de la forme canonique rationnelle et les opérations élémentaires utilisées vont déterminer une matrice $P \in \mathrm{GL}_n(K)$ telle que $P^{-1}AP$ est la forme rationnelle canonique de A.

On se rappelle que les opérations élémentaires sont les suivantes, où L_i dénote la i-ième ligne et C_i la i-ième colonne :

symbole	opération
$L_i \leftrightarrow L_j$	échanger la i-ième et la j-ième ligne
$C_i \leftrightarrow C_j$	échanger la i-ième et la j-ième colonne
$L_i + aL_j \to L_i$	remplacer la i-ième ligne par $L_i + aL_j$
$C_i + aC_j \to C_i$	remplacer la i-ième colonne par $C_i + aC_j$
$uL_i \to L_i$	remplacer la i-ième ligne par uL_i, où u est inversible
$uC_i \to C_i$	remplacer la i-ième colonne par uC_i, où u est inversible

Ici $a \in K[x]$ et $u \in K[x]^\times$.

Théorème 8.20. *Soient K un corps et $A \in M_n(K)$. Il existe une suite d'opérations élémentaires sur l'anneau $K[x]$ transformant $xI - A$ à la matrice diagonale*

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1(x) & & \\ & & & & \ddots & \\ & & & & & f_\ell(x) \end{pmatrix},$$

où $f_1(x), \ldots, f_\ell(x)$ sont les polynômes de la forme canonique rationnelle de A. Cette matrice est appelée la **forme normale de Smith**.

De plus, l'algorithme suivant détermine une matrice $P \in GL_n(K)$ telle que $P^{-1}AP$: considérons le tableau

opération sur $xI - A$	*opération sur I*
$L_i \leftrightarrow L_j$	$C_i \leftrightarrow C_j$
$C_i \leftrightarrow C_j$	*rien*
$L_i + g(x)L_j \to L_i$	$C_j - g(A)C_i \to C_j$
$C_i + g(x) \to C_i$	*rien*
$uL_i \to L_i$	$u^{-1}C_i \to C_i$
$uC_i \to C_i$	*rien*

En suivant la suite des opérations transformant $xI - A$ à sa forme normale de Smith, les opérations de la deuxième colonne du tableau ci-dessus transforme I à une matrice de la forme

$$\begin{pmatrix} 0 & \cdots & 0 & q_{1,1} & \cdots & q_{1,\ell} \\ \vdots & & & & & \vdots \\ 0 & \cdots & 0 & q_{n,1} & \cdots & q_{n,\ell} \end{pmatrix}.$$

Si

$$q_j = \begin{pmatrix} q_{1,j} \\ \vdots \\ q_{n,j} \end{pmatrix}$$

et $d_j = \deg(f_j(x))$, alors les premières d_1 colonnes de la matrice P sont données par $q_1, Aq_1, \ldots, A^{d_1-1}q_1$, les prochaines d_2 sont $q_2, Aq_2, \ldots, A^{d_2-1}q_2$, etc.

L'algorithme de transformation de $xI - A$ à sa forme normale de Smith. On va montrer la première partie du théorème 8.20 dans une forme plus générale : soit $B = (b_{i,j})_{i,j=1}^{n}$ sur un anneau euclidien R de préstathme $N : R \to \mathbb{Z}_{\geq 0}$. Notre but est de transformer B à une matrice

$$\begin{pmatrix} b'_{1,1} & 0 \\ 0 & B' \end{pmatrix}, \tag{8.7}$$

où $B' = (b'_{i,j})_{i,j=1}^{n-1} \in M_{n-1}(R)$.

Posons

$$N(B) = \begin{cases} 0 & \text{si } B = 0 \\ \min\{N(b_{i,j}) : b_{i,j} \neq 0\} & \text{sinon.} \end{cases}$$

On montrera par induction sur $N(B)$ que c'est possible de transformer B à une matrice de la forme (8.7).

Si $N(B) = 0$, alors B est déjà dans la forme (8.7). Supposons, alors, que $N(B) > 0$. Soit b_{i_0,j_0} tel que $N(B) = N(b_{i_0,j_0})$. En faisant les opérations $L_{i_0} \leftrightarrow L_1$ et $C_{j_0} \leftrightarrow C_1$, on peut supposer que $i_0 = j_0 = 1$.

Cas 1 : $b_{1,1}$ divise tous les éléments de la première ligne et de la première colonne.

Dans ce cas, on peut clairement transformer B à la forme (8.7) en utilisant les opérations élémentaires suivantes :

$$\begin{aligned} B = \begin{pmatrix} b_{1,1} & \lambda_2 b_{1,1} & \cdots & \lambda_n b_{1,1} \\ \mu_2 b_{1,1} & b_{2,2} & \cdots & b_{2,n} \\ & \vdots & & \vdots \\ \mu_n b_{1,1} & b_{n,2} & \cdots & b_{n,n} \end{pmatrix} &\xrightarrow{C_2 - \lambda_2 C_1 \to C_2} \begin{pmatrix} b_{1,1} & 0 & \cdots & \lambda_n b_{1,1} \\ \mu_2 b_{1,1} & b_{2,2} - \lambda_2\mu_2 b_{1,1} & \cdots & b_{2,n} \\ & \vdots & & \vdots \\ \mu_n b_{1,1} & b_{n,2} - \lambda_2\mu_n b_{1,1} & \cdots & b_{n,n} \end{pmatrix} \\ &\to \cdots \to \begin{pmatrix} b_{1,1} & 0 & \cdots & 0 \\ \mu_2 b_{1,1} & b'_{2,2} & \cdots & b'_{2,n} \\ & \vdots & & \vdots \\ \mu_n b_{1,1} & b'_{n,2} & \cdots & b'_{n,n} \end{pmatrix} \\ &\xrightarrow{L_2 - \mu_2 L_1 \to L_2} \cdots \xrightarrow{L_n - \mu_n L_1 \to L_n} \begin{pmatrix} b_{1,1} & 0 & \cdots & 0 \\ 0 & b'_{2,2} & \cdots & b'_{2,n} \\ & \vdots & & \vdots \\ 0 & \tilde{b}_{n,2} & \cdots & \tilde{b}_{n,n} \end{pmatrix}. \end{aligned}$$

Cas 2 : il existe un élément de la première ligne ou de la première colonne qu'il n'est pas divisible par $b_{1,1}$.

Sans perde de généralité, supposons que $b_{1,1} \nmid b_{1,2}$; les autres cas sont similaires. On pérforme la division euclidienne de $b_{1,2}$ par $b_{1,1}$: il existe $q, r \in R$ tels que $b_{1,2} = qb_{1,1} + r$, où $N(r) < N(b_{1,1}) = N(B)$. De plus, $r \neq 0$ car $b_{1,1} \nmid b_{1,2}$. En considérant l'opération $C_2 - qC_1 \to C_2$, on transforme B à une nouvelle matrice, soit $\tilde{B}$ dont la $(1,2)$-coefficient est égal à r. Puisque $N(r) < N(B)$, on trouve que $N(\tilde{B}) < N(B)$.

En itérant cet argument, c'est sûr qu'on va éventuellement entre le cas 1 et donc transformer B à une matrice de la forme (8.7). □

Exemple 8.21. On va appliquer l'algorithme à la matrice

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & -1 & 4 \\ -2 & 2 & 0 \end{pmatrix}$$

Dans les étapes d'algorithme, on colore en rouge les entrés non-zéros de $xI - A$ de degré minimal qu'on utilise et en blé les opérations de lignes car elles sont les opérations déterminant la matrice P plus tard : on a que

$$\begin{aligned}
xI - A = \begin{pmatrix} x-3 & -1 & 1 \\ 0 & x+1 & 4 \\ 2 & -2 & x \end{pmatrix} &\xrightarrow{C_1-(x-3)C_3\to C_1} \begin{pmatrix} 0 & -1 & 1 \\ 4(x-3) & x+1 & 4 \\ 2-x(x-3) & -2 & x \end{pmatrix} \\
&\xrightarrow{C_2+C_3\to C_2} \begin{pmatrix} 0 & 0 & 1 \\ 4x-12 & x-3 & 4 \\ -x^2+3x+2 & x-2 & x \end{pmatrix} \\
&\xrightarrow[L_3-xL_1\to L_3]{L_2+4L_1\to L_2} \begin{pmatrix} 0 & 0 & 1 \\ 4x-12 & x-3 & 0 \\ -x^2+3x+2 & x-2 & 0 \end{pmatrix} \\
&\xrightarrow{C_1\leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 4x-12 \\ 0 & x-2 & -x^2+3x+2 \end{pmatrix} \\
&\xrightarrow{C_3-4C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 0 \\ 0 & x-2 & -x^2+3x+2 \end{pmatrix} \\
&\xrightarrow{L_3-L_2\to L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 0 \\ 0 & 1 & -x^2-x+10 \end{pmatrix} \\
&\xrightarrow{L_2\leftrightarrow L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -x^2-x+10 \\ 0 & x-3 & 0 \end{pmatrix} \\
&\xrightarrow{L_3-(x-3)L_2\to L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -x^2-x+10 \\ 0 & 0 & (x-3)(x^2+x-10) \end{pmatrix} \\
&\xrightarrow{C_3+(x^2+x-10)C_2\to C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-3)(x^2+x-10) \end{pmatrix}.
\end{aligned}$$

Donc, $\ell = 1$ et $c_A(x) = m_A(x) = f_1(x) = (x-3)(x^2+x-10)$.

Finalement, on détermine la matrice P :

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{C_1-4C_2\to C_1} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_1+AC_3\to C_1} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\xrightarrow{C_2+C_3\to C_2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$
$$\xrightarrow{C_2\leftrightarrow C_3} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$
$$\xrightarrow{C_2+(A-3I)C_3\to C_2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

puisque

$$A \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 4 \\ 0 \end{pmatrix},$$

$$A - 3I = \begin{pmatrix} 0 & 1 & -1 \\ 0 & -4 & 4 \\ -2 & 2 & \\ -3 & & \end{pmatrix} \quad \text{et} \quad (A-3I) \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}.$$

Finalement, on observe que

$$A \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} \quad \text{et} \quad A^2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = A \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix}.$$

Donc,

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 3 & 5 \\ 1 & 2 & 6 \end{pmatrix}.$$

On peut vérifier que

$$P^{-1} = \begin{pmatrix} -8 & -2 & 3 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix}$$

et

$$\begin{aligned} P^{-1}AP &= \begin{pmatrix} -8 & -2 & 3 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 & -1 \\ 0 & -1 & 4 \\ -2 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 3 & 5 \\ 1 & 2 & 6 \end{pmatrix} \\ &= \begin{pmatrix} -30 & 0 & 0 \\ 5 & -2 & 3 \\ 3 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 3 & 5 \\ 1 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -30 \\ 1 & 0 & 13 \\ 0 & 1 & 2 \end{pmatrix}. \end{aligned}$$

Finalement, on observe que

$$f_1(x) = (x-3)(x^2+x-10) = x^3 - 2x^2 - 13x + 30,$$

donc on a en effet que $P^{-1}AP = \mathcal{C}_{f_1(x)}$.

8.6 Exercices

EXERCICE 8.1. Soit

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 4 & 3 & 2 \\ 2 & 1 & 1 \end{pmatrix}.$$

Calculez le polynôme caractéristique de A. Trouvez le polynôme minimal de A. Trouvez la forme de Jordan de A et la forme canonique rationnelle de A. Si B est la forme canonique rationnelle de A, trouvez une matrice inversible P telle que $B = P^{-1}AP$.

EXERCICE 8.2 (ex. 9, p. 500). Montrez que les matrices

$$A = \begin{pmatrix} -8 & -10 & -1 \\ 7 & 9 & 1 \\ 3 & 2 & 0 \end{pmatrix} \quad B = \begin{pmatrix} -3 & 2 & -4 \\ 4 & -1 & 4 \\ 4 & -2 & 5 \end{pmatrix}$$

ont les deux $(x-1)^2(x+1)$ comme polynôme caractéristique mais l'un est diagonalisable et l'autre ne l'est pas. Déterminez la forme de Jordan de ces deux matrices.

EXERCICE 8.3. Soit A une matrice $n \times n$ sur un corps F.

(a) (ex. 21, p. 501) Soit A une matrice $n \times n$ sur un corps F. Si $A^2 = A$, alors montrez que A est semblable à une matrice diagonale ayant seulement des 1 et des 0 sur sa diagonale.

(b) (ex. 22, p. 501) Si $F = \mathbb{C}$ et $A^3 = A$, alors montrez que A est diagonalisable. Est-ce que c'est vrai sur n'importe quel corps F ?

(c) (ex. 24, p. 501) Supposons que $n = 3$ et que $F = \mathbb{Q}$. Si $A^8 = I$, alors montrez que $A^4 = I$ également.

EXERCICE 8.4 (ex. 16, p. 489). Montrez que $x^5 - 1 = (x-1)(x^2-4x+1)(x^2+5x+1)$ dans $\mathbb{F}_{19}[x]$. Utilisez ce fait pour déterminez modulo similitude toutes les 2×2 matrices sur $\mathbb{F}_{19}$ d'ordre multiplicative 5

EXERCICE 8.5 (ex. 20, p. 489). Soient ℓ et p deux nombres premiers et soit $\Phi_\ell(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1$ le ℓ-ième polynôme cyclotomique. Le but de cet exercice est d'étudier la factorisation de Φ_ℓ modulo p et, plus précisément, le degré de son plus petite facteur irréductible modulo p.

(a) Si $p = \ell$, alors montrez que $x - 1$ divise $\Phi_\ell(x)$ dans $\mathbb{F}_p[x]$, où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(b) Supposons que $p \nmid \ell$ et soit m le plus petit nombre naturel pour lequel le groupe $\mathrm{GL}_m(\mathbb{F}_p)$ contient un élément d'ordre ℓ. (On a que $|\mathrm{GL}_m(\mathbb{F}_p)| = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$. En particulier, ℓ divise $|\mathrm{GL}_{\ell-1}(\mathbb{F}_p)|$, donc m est bien défini par le théorème de Cauchy.) Si A est un tel élément, alors montrez que $c_A(x)$ est un facteur de $\Phi_\ell(x)$ de degré m qui est irréductible dans $\mathbb{F}_p[x]$. Réciproquement, montrez que si $g(x)$ divise $\Phi_\ell(x)$ dans $\mathbb{F}_p[x]$, alors $\deg(g) \geq m$.

(c) Si $p \nmid \ell$, alors posons $f = \mathrm{ord}_\ell(p)$, c'est-à-dire f est le plus petit nombre naturel pour lequel $p^f \equiv 1 \pmod{\ell}$. Montrez que $f = m$. Déduisez que $\Phi_\ell(x)$ est irréductible dans $\mathbb{F}_p[x]$ s-si p est une racine primitive modulo ℓ.