Université de Rennes 1

ALGB

ALGÈBRE GÉNÉRALE DE BASE

Auteur
Vincent Guirardel

Notes de cours
Victor Lecerf

2021–2022

Table des matières

Chapitre 1

Nombres premiers et critères de primalité

1.1 Critère de Fermat

Théorème 1.1.1. *Un entier $n \geq 2$ est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Remarques.

— Que n soit premier ou non, un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible *si et seulement si* $a \wedge n = 1$. On a donc

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \,|\, a \wedge n = 1\}.$$

On définit l'indicatrice d'Euler en n comme le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

— $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe pour la multiplication.

Théorème 1.1.2. *Si n est un nombre premier, alors pour tout $a \in [\![1, n-1]\!]$,*

$$a^{n-1} \equiv 1 \mod n.$$

Démonstration. Puisque n est premier, $\varphi(n) = n - 1$. Puisque l'ordre d'un élément divise l'ordre du groupe, on a nécessairement $\overline{a}^n = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.

□

Remarques.

— L'hypothèse de la primalité de n n'est pas tout à fait nécessaire. Lorsque $n \geq 2$ est quelconque, on a toujours $a^{\varphi(n)} \equiv 1 \mod n$.

— On peut s'intéresser à la contraposée : si $a \in [\![1, n-1]\!]$ est tel que $a^{n-1} \not\equiv 1 \mod n$, alors n n'est pas premier. Un tel élément a est dit être un témoin de Fermat de la non primalité de n.

Définition 1.1.1. *Un entier $n \geq 2$ est dit être un nombre de* Carmichael *s'il n'est pas premier qu'il n'a pas de témoin de* Fermat.

Remarque. Les éléments de $\mathbb{Z}/n\mathbb{Z} \setminus ((\mathbb{Z}/n\mathbb{Z})^\times \cup \{0\})$ sont toujours des témoins.

Exemple. 561 est le plus petit nombre de Carmichael.

Théorème 1.1.3. *Soit $n \geq 2$ un entier qui n'est pas de* Carmichael. *Alors, parmi les éléments de $[\![1, n-1]\!]$, au moins la moitié sont des témoins de* Fermat.

Démonstration. Un élément $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas un témoin *si et seulement si* $\overline{a}^{n-1} = \overline{1}$. Ainsi, l'ensemble G_n des entiers non témoins est un sous-groupe multiplicatif de $(\mathbb{Z}/n\mathbb{Z})^\times$. Cependant, $G_n \neq (\mathbb{Z}/n\mathbb{Z})^\times$ car n n'est pas de Carmichael. C'est donc un sous-groupe stricte de $(\mathbb{Z}/n\mathbb{Z})^\times$. Or, $|G_n|$ divise $|(\mathbb{Z}/n\mathbb{Z})^\times|$. On en conclut que $|G_n| \leq n/2$.

□

Cette observation est à l'origine d'un algorithme probabiliste de test de primalité. L'idée est la suivante. Lorsque l'on cherche à déterminer si un entier $n \geq 2$ est premier ou non, on choisit au hasard k nombres $a_1, \ldots, a_k$ dans $[\![1, n-1]\!]$ et l'on vérifie si oui ou non, $a_i^{n-1} \equiv 1 \mod n$ pour tout $i \in [\![1, k]\!]$. Si l'une de ces égalités modulo n est en défaut, alors n n'est *pas premier*. Sinon, n est… probablement premier… ou est un nombre de Carmichael. Si toutes les égalités modulo n tiennent, alors la probabilité que n ne soit pas premier (donc de Carmichael) est moindre que $1/2^k$.

1.2 Critère de Miller-Rabin

Lemme 1.2.1. *Soit k un corps, et $P \in k[X]$ un polynôme de degré d. Alors, P a au plus d racine dans k.*

Corollaire 1.2.1. *Si $n \geq 3$ est premier, $X^2 - 1$ a exactement 2 racines dans $\mathbb{Z}/n\mathbb{Z}$: -1 et 1.*

Principe de primalité de Miller-Rabin. Soit $a \in [\![1, n-1]\!]$ un nombre impair. On calcule d'abord a^{n-1} modulo n. Si ce n'est pas 1, n évidemment n'est pas premier. Si $a^{n-1} \equiv 1 \mod n$ et si $n-1$ est pair, on calcule alors $a^{\frac{n-1}{2}}$. Si $a^{\frac{n-1}{2}} \not\equiv 1 \mod n$, on sait que n n'est pas premier. Si $a^{\frac{n-1}{2}} \equiv -1 \mod n$, on arrête et si $a^{\frac{n-1}{2}} \equiv 1 \mod n$, on recommence.

Définition 1.2.1. *Soit n un entier impair. Un entier $a \in [\![1, n]\!]$ est dit être un témoin de* Miller-Robin *pour la non primalité de n si $a^{n-1} \equiv 1 \mod n$, ou s'il existe $k \in \mathbb{N}$ tel que 2^{k+1} divise $n-1$, et $a^{\frac{n-1}{2^k}} \equiv 1 \mod n$ mais $a^{\frac{n-1}{2^{k+1}}} \not\equiv \pm 1 \mod n$.*

Théorème 1.2.1. *Soit n un entier impair. Si n n'est pas premier, alors au moins la moitié des éléments de $[\![2, n-1]\!]$ sont des témoins de* Miller-Robin.

Remarque. En fait, les trois quarts le sont.

Algorithme probabiliste de Rober-Miller. On prend en entrée un entier n impair, et un paramètre k (entier non nul).

(i) On tire au hasard k entiers $a_1, \dots, a_k \in [\![2, n-1]\!]$.

(ii) On détermine si n est un témoin.

(iii) S'il y a au moins un témoin, alors n n'est pas premier. Sinon, on en déduit que n est *probablement premier*, et la probabilité d'erreur inférieure à $1/2^k$.

1.3 Trouver de grands nombres premiers

Algorithme probabiliste. On prend en entrée un réel positif B et un entier k non nul. En sortie, on obtient un nombre *probablement* premier dans $]B, 2B]$.

(i) On choisit un $n \in]B, 2B] \cap \mathbb{N}$ au hasard.

(ii) On vérifie si n est premier avec le critère de Robin-Miller (faux avec une probabilité $1/2^k$).

(iii) Si la réponse est que n est *probablement* premier, on renvoie n.

(iv) Si la réponse est contraire, on recommence l'algorithme.

Attention. S'il y a très peu de nombres premiers[1] dans $]B, 2B] \cap \mathbb{N}$, la probabilité que le nombre d'entiers renvoyés par l'algorithme qui sont en fait non premiers, pourrait être grande.

Théorème 1.3.1. *Soit $B \geq 59$.*

- *L'algorithme ci-dessus se termine en bouclant au plus $(2 \ln B)$ fois en moyenne.*
- *Le nombre renvoyé par l'algorithme est premier avec probabilité supérieure ou égale à $(2 \ln B)(1 - 2^{-k})$*

Exemple. Si $B = 10^{1000}$, alors $2 \ln B = 4600$. Si en plus $k = 42$, alors la probabilité de se tromper est inférieure à $1/10^9$.

Théorème 1.3.2 (des nombres premiers)**.** *Soit $\mathcal{P}$ l'ensemble des nombres premiers, et soit $x \in \mathbb{R}_+$. On note*

$$\pi(x) = \operatorname{card}\{p \in \mathcal{P} \mid p \leq x\}.$$

Alors,

$$\pi(x) \sim_{n \to \infty} \frac{x}{\ln x}.$$

Plus précisément, dès lors que $x \geq 59$,

$$\frac{x}{\ln x}\left(1 + \frac{1}{2 \ln x}\right) \leq \pi(x) \leq \frac{x}{\ln x}\left(1 + \frac{3}{2 \ln x}\right).$$

Démonstration. C'est long et difficile. □

1. Le théorème de Tchebychev (ou postulat de Bertrand) assure que pour tout entier $n > 1$, il existe un nombre premier p tel que $n < p < 2n$.

On peut avec ce résultat démontrer le théorème 1.3.1. Pour tout $B \geq 59$, et suffisamment grand,

$$\pi(2B) - \pi(B) \geq \frac{B}{2\ln B}.$$

Ainsi, la proportion p de nombres premiers dans $]B, 2B] \cap \mathbb{N}$ vérifie $p \geq \frac{1}{2\ln B}$. Si l'algorithme tire un nombre premier dans $]B, 2B] \cap \mathbb{N}$, le test de Miller-Rabin va s'arrêter, et affirmer que n est probablement premier. À chaque fois qu'on tire un nouveau potentiel témoin, on a la probabilité p de s'arrêter. En moyenne, le temps d'attente pour obtenir un nombre premier est inférieur ou égal à $1/p \leq 2\ln B$ (on boucle au plus $2\ln B$ fois en moyenne).

1.4 Cyclicité du groupe multiplicatif d'un corps fini

On rappelle que si $(K, +, \times)$ est un corps, alors $(K^*, \times)$ est un groupe.

Lemme 1.4.1. *Soit G un groupe. Si $x, y \in G$ sont respectivement d'ordres p et q, avec p et q premiers entre eux, et si x et y commutent, alors xy est d'ordre pq.*

Démonstration. Soit d l'ordre de xy. On remarque que d divise pq car $(xy)^{pq} = x^{p}qy^{pq} = 1$. Montrons donc que pq divise d. On a $\langle x\rangle \cap \langle y\rangle = \{e_G\}$ car cette intersection est un sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$, son cardinal doit diviser p et q. Ce sous-groupe est donc d'ordre 1. L'application

$$\begin{array}{rccc} \varphi : & \langle x\rangle \times \langle y\rangle & \longrightarrow & G \\ & (u, v) & \longmapsto & uv \end{array}$$

est un morphisme de groupe car x et y commutent. On remarque que le noyau de φ est trivial. Or, $(x^d, y^d) \in \ker\varphi$ car $x^d y^d = (xy)^d = 1$. Ainsi, $x^d = y^d = 1$, donc p et q divisent tout deux d.

□

Lemme 1.4.2. *Soit G un groupe abélien fini, et d le plus petit commun multiple des ordres des éléments de G. Alors, G contient un élément d'ordre d.*

Démonstration. Par récurrence, il suffit de montrer que si x est d'ordre p et y d'ordre q dans un groupe G commutatif, alors il existe un élément z d'ordre $p \vee q$. On associe au lemme précédent le fait qu'il est vrai pour tout $p, q \in \mathbb{N}$ qu'il existe $p', q' \in \mathbb{N}$ tels que p' divise p, q' divise q, $p' \wedge q' = 1$, et $p'q' = p \vee q$. On ajoute aussi le fait que si x est d'ordre p et que p' divise p, alorsr il y a un élément d'ordre p' : x' $x^{p/p'}$. On en déduit que même avec $y' = y^{q/q'}$ et alors $z = x'y'$ convient par le lemme auxiliaire.

□

Théorème 1.4.1. *Soit K un corps fini de cardinal q. Alors, K^* est un groupe cyclique de cardinal $q-1$. Autrement dit, K^* est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$. Plus généralement, si K est un corps quelconque, et que $G \subset K^*$ est un sous-groupe multiplicatif fini, alors G est cyclique.*

Exemples.

— Pour tout entier p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, et alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.

— Si $\mathbb{K} = \mathbb{C}$, et si $G = \mathbb{U}_n$ le groupe des racines n-ièmes de l'unité, alors le théorème affirme (et confirme) que G est cyclique.

Démonstration. Rappelons qu'un polynôme $P \in K[X]$ de degré d a au plus d racines dans K. On démontre la seconde formulation (plus générale) du théorème. Soit $G \subset K^*$ un sous-groupe fini. Soit d le plus petit commun multiple des ordres des éléments de G. Pour tout $x \in G$, $x^d = 1$. car d est multiple de l'ordre de x. Or, $X^d - 1 \in K[X]$ a au plus d racines, donc $|G| \leq d$. Selon le lemme précédent, il existe un $x_0 \in G$ d'ordre d. On a donc $\langle x_0 \rangle = d$, donc $|G| \geq d$. On en conclut que $|G| = d$, et que x_0 est un générateur de G.

□

Corollaire 1.4.1. *Pour tout entier p premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Remarque. Il n'est pas facile d'en trouver un générateur.

1.5 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

1.5.1 Lemme chinois et conséquences

Théorème 1.5.1 (lemme chinois)**.** *Soient $a, b \in \mathbb{N}$ des entiers premiers entre eux. Alors, l'application naturelle*

$$\begin{array}{rccc} \Phi_{a,b} : & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & [x]_{ab} & \longmapsto & ([x]_a, [x]_b) \end{array}$$

est un isomorphisme d'anneaux.

Exemple. $\Phi_{5,7}([23]_{35}) = ([3]_5, [2]_7)$.

Démonstration. Il est clair que c'est un morphisme d'anneau. Soit maintenant $\Phi = \Phi_{a,b}$ et $[x]_{ab} \in \ker \Phi$. On a donc $([x]_a, [x]_b) = (0, 0)$. Alors, a et b divise x. Or, puisque a et b sont premiers entre eux, on a nécessairement $[x]_{ab} = 0$. Ainsi, Φ est injectif. On conclut en remarque que $|\mathbb{Z}/ab\mathbb{Z}| = ab = |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}|$.

□

Remarque. On peut calculer des antécédents par $\Phi = \Phi_{a,b}$ grâce au théorème de Bézout. Soit u et $v \in \mathbb{Z}$ tel que $au + bv = 1$. On a

$$\Phi([au]_{ab}) = (0, 1) \quad \text{et} \quad \Phi([bv]_{ab}) = (1, 0).$$

Ainsi, l'antécédent de $([x]_a, [x]_b) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ par Φ est $[xbv]_{ab} + [yau]_{ab}$.

Corollaire 1.5.1. *Si $a_1, \dots, a_k$ sont des entiers premiers entre eux deux à deux, alors si $n = a_1 \cdots a_k$.*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}.$$

En particulier, si $n \in \mathbb{N}$ se décompose en facteurs premiers sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

Corollaire 1.5.2. *Si $n \in \mathbb{N}$ se décompose en facteurs premiers sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors*

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

Ainsi,

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}).$$

1.5.2 Étude de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

Lemme 1.5.1. *Soit p un nombre premier, et $\alpha \in \mathbb{N}^*$. On a*

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

Démonstration. Il suffit de trouver le cardinal de $\{k \in [\![0, p^\alpha - 1]\!] \mid k \wedge p^\alpha = 1\}$, *i.e* le nombre de multiplie de p dans $[\![0, p^\alpha - 1]\!]$: il y en a $p^\alpha - p^{\alpha-1}$.

□

Théorème 1.5.2. *Soit p premier, et $\alpha \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est*

- *cyclique si $p \geq 3$. Il est alors isomorphe à $(\mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}, +)$.*
- *trivial si $p = 2$ et $\alpha = 1$.*
- *isomorphe à $\mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si $p = 2$ et $\alpha \geq 2$.*

1.6 Faits de base sur les groupes cycliques, applications aux racines de l'unité et à $(\mathbb{Z}/p\mathbb{Z})^\times$

Lemme 1.6.1. *Soit U_n un groupe cyclique d'ordre n engendré par a_0.*

(i) Pour tout diviseur d de n, il existe un unique sous groupe U_d de cardinal d, tel que $U_d = \langle a_0^{n/d} \rangle$.

(ii) On a $U_d = \{x \mid x^d = 1\} = \ker \varepsilon_d$ où l'on a posé $\varepsilon_d : U_n \to U_n$, $x \mapsto x^d$.

(iii) On a $U_d = \operatorname{Im} \varepsilon_{n/d}$.

Démonstration. Soit U_d un sous-groupe de cardinal d. Alors, $U_d \subset \ker \varepsilon_d$. Mais $\mathrm{Im}(\varepsilon_d) = \langle a_0^d \rangle$, qui est de cardinal n/d. Ainsi, $|\ker \varepsilon_d = |U_n|/|\operatorname{Im} \varepsilon_d| = n/(n/d) = d$. Ainsi, $U_d = \ker(\varepsilon_d)$. On a donc démontré l'unicité dans (i) ainsi que le point (ii). Pour le point (iii), remarque que $a_0^{n/d}$ est d'ordre d, donc $U_d = \langle a_0^{n/d} \rangle = \operatorname{Im} \varepsilon_{n/d}$.

□

Théorème 1.6.1. *Dans ce groupe cyclique U_n, il y a exactement $\varphi(n)$ éléments d'ordre n.*

Démonstration. On identifie U_n à $(\mathbb{Z}/n\mathbb{Z}, +)$. Soit $x \in U_n$. Alors,

$$\begin{aligned} x \text{ est d'ordre } n &\iff \langle x \rangle = \langle 1 \rangle \\ &\iff \exists k \in \mathbb{N},\ kx \equiv 1 \mod n \\ &\iff x \in (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

□

Corollaire 1.6.1. *Si K est un corps et possède une racine primitive n-ième de l'unité (i.e un élément d'ordre n dans le groupe multiplicatif), il y a alors exactement $\varphi(n)$.*

Démonstration. Si K a une racine primitive n-ième de l'unité, alors il engendre le groupe des racines n-ièmes de l'unité est un groupe cyclique d'ordre n (noté U_n, au hasard). On a montré que U_n a exactement $\varphi(n)$ éléments d'ordre n.

□

Corollaire 1.6.2. *Soit $n \in \mathbb{N}^*$. On a*

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

Démonstration. Soit U_n un groupe cyclique d'ordre n. Pour tout d diviseur de n, on note U'_d l'ensemble des éléments d'ordre d. Alors, les U'_d partitionnent U_n, *i.e*,

$$U_n = \bigsqcup_{d|n} U'_d$$

et donc

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

□

Lemme 1.6.2. *Soit $k \in [\![1, n]\!]$. On a*

$$\ker \varepsilon_k = \ker \varepsilon_{k \wedge n} = U_{k \wedge n}$$

et

$$\operatorname{Im} \varepsilon_k = \operatorname{Im} \varepsilon_{k \wedge n} = U_{n/(k \wedge n)}.$$

Corollaire 1.6.3 (fondement du symbole de Legendre)**.** *Soit K un corps de cardinal q, $\alpha \in K^*$ et $k \in \mathbb{N}^*$. On pose $d = k \wedge (q-1)$.*

(i) L'élément a possède une racine k-ième dans K si et seulement si $a^{\frac{q-1}{d}} = 1$.

(ii) Si q est impair, a est un carré si et seulement si $a^{\frac{q-1}{2}} = 1$.

Démonstration. On remarque que (i) implique clairement le point (ii). On montre donc uniquement le premier point. On note $U_n = K^*$ avec $n = q-1$. L'élément a a une racine $k-ime$ *si et seulement si*

$$a \in \operatorname{Im} \varepsilon_k = \operatorname{Im} \varepsilon_d = U_{n/d} \iff a^{n/d} = 1 \iff a^{\frac{q-1}{d}} = 1.$$

□

Chapitre 2

Généralités sur les anneaux, idéaux, et corps

2.1 Définitions

Définition 2.1.1. *Un anneau (commutatif) est la donnée d'un triplet $(A, +, \times)$ tel que $(A, +)$ est abélien, $\times$ est une loi de composition interne commutative, associative, distributive, et possède un élément neutre.*

Remarques.

- On note 0_A le neutre additif et 1_A le neutre multiplicatif. Ils peuvent potentiellement être égaux (et alors $A = \{0_A\}$).
- Un anneau n'est pas nécessairement commutatif. On supposera cependant dans ce cours que les anneaux le sont tous.
- Il n'est pas non plus toujours demander qu'il existe un neutre multiplicatif. Un anneau possédant un tel neutre est parfois appelé *anneau unifère* (ou *unitère*). Les anneaux le seront tous dans ce cours.

Exemple. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}/n\mathbb{Z}[X]$, $A[X]$ et $A[X_1, \ldots, X_n]$ pour tout anneau A, $A\times$ pour tout anneaux A et B.

Définition 2.1.2. *Un anneau A est dit intègre s'il est n'est pas réduit à $\{0_A\}$ et que pour tout $a, b \in A$, $ab = 0$ impose que $a = 0$ ou $b = 0$.*

Remarque. Un anneau produit n'est en général pas intègre. Par exemple dans $A \times B$ où A et B sont des anneaux quelconques,

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

2.2 Groupe multiplicatif

Définition 2.2.1 (inversibilité)**.** *Un élément $x \in A$ est dit inversible s'il existe $y \in A$ tel que $xy = 1_A$. On note $A^\times$ l'ensemble des éléments inversible de A.*

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

Définition 2.2.2. *Un corps $\mathbb{K}$ est un anneau tel que 0_A est le seul élément non inversible.*

Remarques. Tout corps est intègre, et tout sous-anneau d'un corps est intègre.

Théorème 2.2.1. *À partir d'un anneau intègre, on peut construire son corps de fraction* $\mathrm{Frac}(A)$. *C'est un corps qui contient A comme sous-anneau et tel que tout élément de* $\mathrm{Frac}(A)$ *s'écrit sous la forme $\frac{a}{b}$ avec $a, b \in A$ et $b \neq 0$.*

Démonstration. Soit $\sim$ la relation d'équivalence sur $A \times (A \backslash \{0_A\})$ définie pour tout $(a, b), (c, d) \in A \times (A \backslash \{0_A\})$ par

$$(a, b) \sim (c, d) \iff ad = bc.$$

On pose alors $\mathrm{Frac}(A) = (A \times (A \backslash \{0_A\}))/\sim$. On note $\frac{a}{b}$ (ou a/b) la classe d'équivalence de $(a, b) \in A \times (A \backslash \{0_A\})$ dans $\mathrm{Frac}(A)$. On définit

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

On vérifie que $\mathrm{Frac}(A)$ est bien un corps. Enfin, on plonge A dans $\mathrm{Frac}(A)$ *via* l'injection $A \to \mathrm{Frac}(A)$, $a \mapsto a/1_A$ (on notera $a = a/1_A$ dans $\mathrm{Frac}(A)$).

□

Proposition 2.2.1 (propriété universelle de $\mathrm{Frac}(A)$)**.** *Si $f : A \longrightarrow K$ est un morphisme d'anneaux injectif où K est un corps, alors f s'étend de manière unique sur* $\mathrm{Frac}(A)$ *en un morphisme d'anneau F en posant $F(a/b) = f(a)/f(b)$.*

2.3 Morphismes

Définition 2.3.1. *Soient A et B des anneaux. Un morphisme d'anneaux $f : A \longrightarrow B$ est une application telle que*

(i) pour tout $x, y \in A$, $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$;

(ii) $f(1_A) = 1_B$.

Remarques.

— On demande à un morphisme d'anneau que $f(1_A) = 1_B$ car ce n'est pas automatique, et qu'on s'évite ainsi des cas pathologiques.

— $\mathrm{Im}\, f$ est un sous-anneau de B. En revanche, $\ker f$ n'est (en général) pas un sous-anneau de A. C'est ce fait qui justifiera la définition des idéaux.

Proposition 2.3.1 (morphisme d'évaluation (ou de substitution))**.** *Soit $f : A \longrightarrow B$ un morphisme d'anneaux et $x_0 \in B$. Alors, il existe un unique morphisme d'anneaux $\Phi : A[X] \longrightarrow B$ qui coïncide avec f sur A, et telle que $\Phi(X) = x_0$.*

Remarque. Pour tout $P = \sum_{k=0}^{d} a_k X^k \in A[X]$,

$$\Phi(P) = \sum_{k=0}^{d} f(a_k) {x_0}^k.$$

Proposition 2.3.2 (morphisme d'évaluation (ou de substitution), version en n variables)**.** *Soit $n \in \mathbb{N}^*$ et $f : A \longrightarrow B$ un morphisme d'anneaux et $x_1, \ldots, x_n \in B^n$. Alors, il existe un unique morphisme d'anneaux $\Phi : A[X_1, \ldots, X_n] \longrightarrow B$ qui coïncide avec f sur A, et telle que $\Phi(X_k) = x_k$ pour tout $k \in [\![1, n]\!]$.*

Remarque. Pour tout $P(X_1, \ldots, X_n) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n} \in A[X_1, \ldots, X_n]$,

$$\Phi(P) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} f(a_{k_1,\ldots,k_n}) x_1^{k_1} \cdots x_n^{k_n}.$$

Proposition 2.3.3. *Pour tout anneau A, il existe un unique morphisme d'anneaux de $\mathbb{Z}$ vers A.*

Remarque. Ce morphisme φ_A est défini pour tout $n \in \mathbb{N}$ par $\varphi_A(n) = n \cdot 1_A = \sum_{i=1}^{n} 1_A$.

Définition 2.3.2. *Soit φ_A l'unique morphisme de $\mathbb{Z}$ vers A. On appelle **caractéristique** de A l'unique entier $n \in \mathbb{N}$ tel que $\ker \varphi_A = n\mathbb{Z}$.*

Remarques.

- A est de caractéristique nulle *si et seulement si* φ est injectif. Si A est de caractéristique nulle, alors $\mathbb{Z}$ se plonge dans A et donc A est nécessairement infini.
- Si A est intègre, alors sa caractéristique est 0 ou un nombre premier.

Proposition 2.3.4. *Soit $\varphi : A \longrightarrow B$ un morphisme de groupe. Alors, $\varphi(A^\times) = \varphi(B^\times)$. Ainsi, $\varphi_{|A^\times} : A^\times \longrightarrow B^\times$ est un morphisme de groupes.*

Observation. Soit K est un corps et A un anneau non nul. Alors, tout morphisme de K vers A est injectif. En effet, si $x \in K^*$. Ainsi x est inversible, donc $\varphi(x)$ aussi, et nécessairement $\varphi(x) \neq 0_A$ (car A est non nul). On en déduit que $\ker \varphi = \{0_K\}$.

2.4 Noyaux et idéaux

Nous avons déjà remarqué pour tout morphisme d'anneau $\varphi : A \longrightarrow B$ que $\operatorname{Im} \varphi$ est un anneau, mais par $\ker \varphi$ l'est rarement. Cela justifie la définition d'une nouvelle sous-structure dans les anneaux.

Définition 2.4.1. *Soit A un anneau, et $\mathcal{I} \subset A$. $\mathcal{I}$ est dit être un **idéal** de A, si I est un sous-groupe additif, et s'il est absorbant, i.e que $AI \subset I$.*

Formulation équivalente. On peut aussi définir un idéal comme un sous-ensemble de $\mathcal{I}$, tel que $\mathcal{I}$ est un sous-groupe additif de A stable par combinaison linéaire à coefficients dans A, *i.e* que pour tout $(x_1, \dots, x_n) \in \mathcal{I}^n$ et $(a_1, \dots, a_n) \in A^n$, on a

$$\sum_{i=1}^{n} a_i x_i \in \mathcal{I}.$$

Remarques.

— Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, alors pour tout idéal J de B, $\varphi^{-1}(J)$ est un idéal de A.

— En particulier, $\ker \varphi$ est un idéal de A.

— Si φ est surjectif, alors pour tout idéal I de A, $\varphi(I)$ est un idéal de B.

Idéal engendré. Soit A un anneau. Soit P une partie de A. On appelle *idéal engendré par* A le plus petit idéal $\langle P \rangle$ de A contenant P. C'est l'intersection de tous les idéaux de A contenant P.

— La somme de deux idéaux est un idéal : si $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux de A, alors $\mathcal{I}+\mathcal{J} = \langle \mathcal{I} \cup \mathcal{J} \rangle$.

— Soit $x \in A$. Alors, $\langle \{x\} \rangle = xA$. On note cet idéal $\langle x \rangle$ ou encore (x).

— Si $x_1, \dots, x_n \in A$, alors $\langle a_1, \dots, a_n \rangle = x_1 A + \cdots + x_n A$.

Proposition 2.4.1. *Soit A un anneau et $\mathcal{I}$ un idéal de A. Alors,*

$$\mathcal{I} = A \iff 1_A \in \mathcal{I} \iff \mathcal{I} \cap A^\times \neq \varnothing.$$

2.5 Anneaux quotients

Comme avec les groupes, on veut s'intéresser à la possibilité de créer des anneaux de quotients. Cependant, on ne peut pas quotienter un anneau par n'importe quoi pour espérer obtenir un autre anneau. Les idéaux vont justement être la réponse à ce problème.

Soit A un anneau, et $\mathcal{I}$ un idéal de A. Soit $\sim_{\mathcal{I}}$ la relation d'équivalence définie pour tout $(x, y) \in A^2$ par

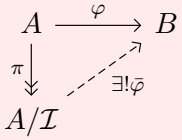
$$x \sim_{\mathcal{I}} y \iff x - y \in \mathcal{I}.$$

On notera $[x] = x + \mathcal{I}$ la classe d'équivalence d'un élément $x \in A$, et $\pi : A \longrightarrow A/\mathcal{I}$ la surjection canonique.

Théorème 2.5.1. *Soit A un anneau et I un idéal de A. Il existe une unique structure d'anneaux sur $A/\mathcal{I}$ telle que π soit un morphisme d'anneau de noyau $\mathcal{I}$.*

Remarque. Avec cette structure, $[x] + [y] = [x + y]$ et $[x][y] = [xy]$ pour tout $x, y \in A$.

Théorème 2.5.2 (propriété universelle du quotient)**.** *Soit A et B des anneaux, $\varphi : A \longrightarrow B$ un morphisme d'anneaux, et $\mathcal{I}$ un idéal de A tel que $\mathcal{I} \subset \ker\varphi$. Alors, il existe un unique morphisme d'anneaux $\bar{\varphi} : A/\mathcal{I} \longrightarrow B$ tel que $\varphi = \bar{\varphi} \circ \pi$. Autrement dit, le diagramme suivant commute.*



Si $\mathcal{I} = \ker\varphi$, alors $\bar{\varphi}$ est injectif.

Théorème 2.5.3 (d'isomorphisme)**.** *Il existe un isomorphisme de $A/\mathcal{I}$ vers $\varphi(A)$:*

$$A/\mathcal{I} \cong \varphi(A).$$

Lemme 2.5.1 (correspondance)**.** *Soit A un anneau, $\mathcal{I}_0$ un idéal de A, et $\pi : A \longrightarrow A/\mathcal{I}_0$. Il existe une correspondance bijective entre les idéaux de A contenant $\mathcal{I}_0$ vers les idéaux de $A/\mathcal{I}_0$, de mécanisme $\mathcal{I} \longmapsto \pi(\mathcal{I})$, et de mécanisme inverse $\mathcal{J} \longmapsto \pi^{-1}(\mathcal{J})$.*

Remarque. Si $\mathcal{I}$ et $\mathcal{J}$ sont deux idéaux (respectivement de A et $A/\mathcal{I}_0$), alors

$$A/\mathcal{I} \cong (A/\mathcal{I}_0)/\mathcal{J}.$$

2.6 Interprétation du quotient comme "ajout de relation", adjonction d'élément

2.6.1 Idée

Soit A un anneau et $x, y \in A$ des éléments. On veut construire un autre anneau dans lequel on aurait $2y^2 - 3x^2 + 57 = 0$. En fait, l'anneau $A/\langle 2y^2 - 3x^2 + 57\rangle$ est un anneau dans lequel les images $\bar{x} = \pi(x)$ et $\bar{y} = \pi(y)$ vérifient $2\bar{y}^2 - 3\bar{x}^2 + 57 = 0$.

Exercice. On choisit $A = \mathbb{Z}$, et $(x, y) = (5, 7)$. On veut pouvoir écrire $x^2 = 2y$. On a

$$\mathbb{Z}/\langle x^2 - 2y\rangle = \mathbb{Z}/11\mathbb{Z}.$$

Effectivement, on observe que dans $\mathbb{Z}/11\mathbb{Z}$, $5^2 = 2 \times 7\,(= 3)$.

Exercice. Montrer que pour tout anneau A et $(x, y) \in A$,

$$(A/\langle x\rangle)/\bar{y} \cong A/\langle x, y\rangle.$$

2.6.2 Adjonction d'éléments

Soit A un anneau. On veut ajouter à A un élément α tel que $\alpha^2 = 1$, ou plus généralement tel que $P(\alpha) = 0$ pour un $P = \sum_{k=0}^{d} a_k \alpha^k \in A[X]$ donné. Pour cela, on construit un nouvel anneau. On pose

$$\mathbb{A} = A[X]/\langle P(X)\rangle.$$

On pose $\alpha = \bar{X}$ l'image de X dans le quotient $\mathbb{A}$. Cet élément est bien tel que $Q(\bar{\alpha}) = 0$ où Q est le polynôme dont les coefficients sont ceux de P projetés dans $\mathbb{A}$, car

$$Q(\alpha) = \sum_{k=0}^{d} \bar{a}_k \alpha^k = \sum_{k=0}^{d} \bar{a}_k \bar{X}^k = \overline{P(X)} = \bar{0}.$$

On note $A[\alpha]$ ce nouvel anneau. La notation $A[\alpha]$ suggère que $A[\alpha]$ contient A (ou du moins que A se plonge dans $A[\alpha]$). C'est vrai si lorsque A est intègre et $\deg P \geq 1$. Le lemme suivant nous permet de déterminer ceci en étudiant le morphisme composé (où i est l'inclusion par injection)

$$A \overset{i}{\hookrightarrow} A[X] \overset{\pi}{\twoheadrightarrow} A[\alpha].$$

Lemme 2.6.1. *Si A est intègre et $\deg P \geq 1$, alors $\pi \circ i$ est injective.*

Démonstration. Le noyau de π est $\langle\pi\rangle = A[X]P$, *i.e* les multiples de π. Or, un multiple de P est de degré supérieur ou égal à $\deg P$ (sauf lorsque le multiplicateur est nul). Soit $QP \in A[X]P$. Puisque A est intègre, on sait que $\deg P + \deg Q = \deg QP$. Ainsi, le seul polynôme constant dans $\ker\pi$ est le polynôme, ce qui signifie que $\ker\pi$ est nul.

□

Exercice. Montrer que $Z[X]/\langle X^2+1\rangle \cong \mathbb{Z}[i]$.

Proposition 2.6.1 (division euclidienne dans un anneau de polynômes)**.** *Soit A un anneau, et $F, G \in A[X]$ avec $G \neq 0$ de coefficient dominant inversible dans A. Alors, il existe un unique couple $(Q, R) \in A[X]^2$ tel que*

$$\begin{cases} F = GQ + R \\ \deg R < \deg G \end{cases}$$

Remarques.

— Cela ne signifie pas que $A[X]$ est euclidien. Il l'est cependant si c'est un corps.

— On peut adjoindre plusieurs éléments satisfaisant des relations, par exemple en calculant l'anneau

$$A[X,Y,Z]/\langle X^2+1, X^2+Y^2+Z^2, 17XYZ-23\rangle.$$

Plus généralement, si $\alpha_1, \ldots, \alpha_n \in A$ sont des éléments tels que

$$P_1(\alpha_1, \ldots, \alpha_n) = \cdots = P_k(\alpha_1, \ldots, \alpha_n) = 0$$

(avec $P_1, \ldots, P_k \in A[X_1, \ldots, X_n]$), alors on peut construire l'anneau

$$A[X_1, \ldots, X_n]/\langle P_1, \ldots, P_k\rangle.$$

2.7 Idéaux maximaux, idéaux premiers

On rappelle qu'un idéal $\mathcal{I}$ de A est dit *propre* si $\mathcal{I} \neq A$ (*i.e* que $1_A \notin \mathcal{I}$).

Définition 2.7.1. *Soit $\mathcal{I}$ un idéal de A, un anneau commutatif. On dit que $\mathcal{I}$ est **maximal** s'il est propre et que pour tout idéal $\mathcal{J}$ de A tel que $\mathcal{I} \subset \mathcal{J}$, alors $\mathcal{J} \in \{\mathcal{I}, A\}$. En d'autres termes, $\mathcal{I}$ est maximal pour l'inclusion parmi les idéaux propres.*

Proposition 2.7.1. *Soit $\mathcal{I} \subset A$ un idéal. Alors, $\mathcal{I}$ est un idéal maximal si et seulement si $A/\mathcal{I}$ est un corps.*

Démonstration. $A/\mathcal{I}$ est un corps, *si et seulement si* $A/\mathcal{I}$ a exactement deux idéaux : $\{0\}$ et $A/\mathcal{I}$. Par le principe de correspondance, cela est équivalent à dire que parmi les idéaux de A contenant $\mathcal{I}$, il y en a exactement deux : $\pi^{-1}(\{0\}) = \mathcal{I}$ et $\pi^{-1}(A/\mathcal{I}) = A$. C'est équivalent à dire que $\mathcal{I}$ est un idéal maximal.

□

Définition 2.7.2. *Soit $\mathcal{I}$ un idéal de A, un anneau commutatif. On dit que $\mathcal{I}$ est **premier** s'il est propre et que pour tout $a, b \in A$, alors*

$$(ab \in \mathcal{I}) \implies (a \in \mathcal{I}) \vee (b \in \mathcal{I}).$$

Proposition 2.7.2. *Un idéal $\mathcal{I}$ est premier si et seulement si $A/\mathcal{I}$ est intègre.*

Démonstration. $A/\mathcal{I}$ est intègre *si et seulement si* pour tout $\bar{a}, \bar{b} \in A/\mathcal{I}$, $\bar{a}\bar{b} = 0$ implique que $\bar{a}$ ou $\bar{b}$ est nul. C'est équivalent à dire que pour tout $a, b \in A$, $ab \in \mathcal{I}$ implique $a \in \mathcal{I}$ ou $b \in \mathcal{I}$.

□

Exemples.

- Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.
- Les idéaux premier de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier, et $\{0\}$.

Théorème 2.7.1 (Krull)**.** *Soit A un anneau, et $\mathcal{I} \subset A$ un idéal propre. Alors, il existe un idéal maximal $\mathcal{J}$ de A tel que $\mathcal{I} \subset \mathcal{J}$.*

Remarques.

- Il est équivalent de dire que tout anneau possède un idéal maximal.
- En 1978, Wilfrid Hodges démontre que le théorème de Krull est équivalent à l'axiome du choix dans la théorie ZF.

Démonstration. Soit U l'ensemble des idéaux propres de A contenant $\mathcal{I}$. Cet ensemble est ordonné par l'inclusion. Soit $V \subset U$ un sous-ensemble totalement ordonné. On peut supposer V non vide (sinon, $\mathcal{I}$ est un idéal maximal et c'est fini) et soit

$$\mathcal{K} = \bigcup_{\mathcal{J} \in V} \mathcal{J}.$$

Alors, pour tout $\mathcal{J} \in V$, $\mathcal{J} \subset \mathcal{K}$. De plus, $\mathcal{I} \subset \mathcal{K}$. Soient $x_1, x_2 \in \mathcal{K}$. Il existe $\mathcal{J}_1, \mathcal{J}_2 \in V$ tels que $x_1 \in J_1$ et $x_2 \in J_2$. Puisque V est totalement ordonné, on peut supposer sans perte de généralité que $\mathcal{J}_1 \subset \mathcal{J}_2$. Alors, $x_1, x_2 \in \mathcal{J}_2$, et donc $x_1 + x_2 \in \mathcal{J}_2 \subset \mathcal{K}$. Soit maintenant $a \in A$ et $x \in \mathcal{K}$. Il existe un certain $\mathcal{J} \in V$ tel que $x \in \mathcal{J}$, alors $ax \in \mathcal{J} \subset \mathcal{K}$. On conclut que $\mathcal{K}$ est un idéal propre de A (aucun $\mathcal{J} \in V$ ne contient 1_A), donc $K \in U$. Toute chaîne d'inclusion d'éléments de U est majorée. Par le lemme de Zorn, U possède un élément maximal.

□

Corollaire 2.7.1. *Tout anneau non nul a un quotient qui est un corps.*

Chapitre 3

Modules

3.1 Généralités

On se donne dans cette section un anneau A.

Définition 3.1.1 (module)**.** *Un A-module est un ensemble V muni d'une loi de composition interne $+ : V^2 \longrightarrow V$ et d'une loi de composition externe $\cdot : A \times V \longrightarrow V$ telles que*

(i) $(V, +)$ *est un groupe abélien ;*

(ii) pour tout $v \in V$, $1_A \cdot v = v$ *;*

(iii) (distributivité en les vecteurs) pour tout $\lambda \in A$ *et* $u, v \in V$, $\lambda(u + v) = \lambda u + \lambda v$ *;*

(iv) (distributivité en les scalaires) pour tout $\lambda, \mu \in A$, $v \in V$, $(\lambda + \mu)v = \lambda v + \mu v$ *;*

(v) pour tout $\lambda, \mu \in A$, $v \in V$, $(\lambda\mu)v = \lambda(\mu v)$.

Exemples.

— Si A est un corps, alors V est un A-espace vectoriel.

— A^n est un anneau, lorsqu'on le munit des lois habituelles définies par

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

et

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

— *(Exemple fondamental).* Se donner un $\mathbb{Z}$-module $(V, +, \cdot)$ est équivalent à se donner un groupe abélien additif $(V, +)$.

Définition 3.1.2. *Soient V et V' des A-modules. On appelle morphisme de A-module toute application $f : V \longrightarrow V'$ telle que pour tout $u, v \in V$, et $\lambda, \mu \in V$,*

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v).$$

On dit aussi que f est une application A-linéaire.

Définition 3.1.3. *Soient V un A-module. On appelle sous-module tout sous-ensemble de A stable par addition et multiplication scalaire.*

Définition 3.1.4. *Soient V, V' des A-modules, et $f : V \longrightarrow V'$ un morphisme de modules. On note*

$$\ker f = f^{-1}(0_{V'}) \quad et \quad \mathrm{Im}(f) = f(V)$$

*les ensembles respectivement appelés **noyau** et **image** de f.*

Proposition 3.1.1. *Le noyau et l'image d'un morphisme de A-modules sont des sous-modules.*

Définition 3.1.5. *Soit V un A-module. On appelle combinaison linéaire tout élément de V sous la forme*

$$\sum_{i=1}^{n} \lambda_i v_i$$

où $(\lambda_1, \ldots, \lambda_n) \in A^n$ et $(v_1, \ldots, v_n) \in V^n$.

Définition 3.1.6. *Soit V un A-module, et soit $\mathcal{F} = (v_i)_{i \in I}$ une famille d'éléments de V.*

- *La famille $\mathcal{F}$ est dite **libre** si pour toute famille $(\lambda_i)_{i \in I}$ à support fini,*

$$\left(\sum_{i \in I} \lambda_i v_i = 0 \right) \implies (\forall i \in I,\ \lambda_i = 0).$$

- *La famille $\mathcal{F}$ est dite **génératrice** si tout élément de V s'écrit comme combinaison linéaire d'éléments de $\mathcal{F}$.*
- *La famille $\mathcal{F}$ est dite être une **base** si elle est libre et génératrice.*

Exemples.

- Le A-module A^n a pour base (appelée *base canonique*) la famille d'éléments $(e_i)_{1 \leq i \leq n}$ où $e_i = (\delta_{i,j})_{1 \leq j \leq n}$.
- Si V est un A-module, et $\mathcal{F} = (v_i)_{i \in I}$ une famille d'éléments de V, alors on note $\langle \mathcal{F} \rangle$ le plus petit A-module (pour l'inclusion) contenant $\mathcal{F}$. Cet espace est l'ensemble des combinaisons linéaires d'éléments de $\mathcal{F}$. On le notera aussi $\mathrm{Mdl}(\mathcal{F})$ pour éviter les ambiguïtés.

Proposition 3.1.2. *Soit V un A-module et $W \subset V$ un sous-module, et soit $\pi : V \longrightarrow V/W$ la projection canonique.*

(i) Il existe une unique structure de A-module sur V/W telle que π soit un morphisme de A-modules (on munira toujours V/W de cette structure).

(ii) L'application $\pi : V \longrightarrow V/W$ est A-linéaire, surjective, de noyau W.

(iii) Soit $f : V \longrightarrow V'$ une application A-linéaire telle que $W \subset \ker f$. Alors, il existe une unique application A-linéaire $\bar{f} : V/W \longrightarrow V'$ telle que $f = \bar{f} \circ \pi$. Autrement dit, le diagramme suivant commute

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\bar{f}} & \\ V/W & & \end{array}$$

(iv) (théorème d'isomorphisme). Si $W = \ker f$, alors $\bar{f}$ est un isomorphisme de V/W vers $\mathrm{Im}(f)$.

(v) (théorème de correspondance). Il existe une correspondance bijective depuis les sous-modules de V contenant W vers les sous-modules de V/W, de mécanisme $T \longmapsto \pi(T)$ et de mécanisme inverse $S \longmapsto \pi^{-1}(S)$.

Différences entre espaces vectoriels et modules. La différence majeure (et le prix que l'on paye à ne plus considérer des corps) est qu'il n'y a plus nécessairement existence d'une base dans un module. Par exemple, $V = (\mathbb{Z}/7\mathbb{Z})^2$ est un $\mathbb{Z}$-module. En effet, si $(e_i)_{i\in I}$ est une base de V, alors cette famille est nécessairement infini. En effet, pour tout $i_0 \in I$, les ne_{i_0} sont tous différents (pour $n \in \mathbb{Z}$) car si $ne_{i_0} = pe_{i_0}$, $n = p$ car $(e_i)_i$ est une base donc est libre. Il n'y a pas non plus de notion de dimension de module, car certains ont des bases finis de cardinaux différents. Bilan : pas de dimension chez les modules.

Une autre différence majeur est basée sur l'observation suivante. Soit $\mathbb{K}$ un corps et $V = \mathbb{K}$ vu comme $\mathbb{K}$-espace vectoriel. Alors, les sous-$\mathbb{K}$-espaces vectoriels de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$. Mais si $V = A$ est vu comme un A-module, alors les sous-A-modules de A sont *exactement* les idéaux de A (par définition d'un idéal). Or, nous savons que seuls les corps n'ont pas d'idéaux triviaux. Par exemple, les sous-modules de $\mathbb{Z}$ en tant que $\mathbb{Z}$-module sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

3.2 Anneaux noethériens

Définition 3.2.1. *Un A-module V est de type **fini** s'il admet une famille génératrice finie.*

Remarque. En particulier, un idéal $I \subset A$ est de type fini (comme sous-A-module) s'il existe $x_1, \dots x_n \in I$ tel que $I = \langle x_1, \dots, x_n \rangle$.

Définition 3.2.2. *Un anneau est dit noethérien si tous ses idéaux sont de type fini.*

Exemple. Un anneau principal [1] (*i.e* un anneau intègre dont tous les idéaux sont engendrés par un seul élément chacun) est noethérien.

1. En anglais, *principal ideal domain*.

Lemme 3.2.1. *Soit $f : V_1 \longrightarrow V_2$ une application A-linéaire. Si* $\ker f$ *et* $\operatorname{Im} f$ *sont de type fini, alors V_1 est de type fini.*

Remarque. Ce théorème est au module ce que le théorème du rang est aux espaces vectoriels.

Théorème 3.2.1. *Soit A un anneau. Les assertions suivantes sont équivalentes.*

(i) A est noethérien.

(ii) Pour toute suite croissante d'idéaux $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ est stationnaire (il existe $N \in \mathbb{N}^*$ tel que $I_n = I_N$ pour tout $n \geq N$).

(iii) Pour tout A-module V de type fini, tout sous-module $W \subset V$ est de type fini.

(iv) Pour tout A-module V de type fini, toute suite croissante de sous-modules $W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$ est stationnaire.

Remarques.

— Le point (i) est un cas particulier de (iii).

— Le plus remarquable (du moins pour la suite du cours) est que (i) implique (iii) et (iv).

Démonstration. — $(iii) \implies (iv)$. Soit $W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$ une suite croissante de sous-modules. Soit $W = \bigcup_{n\geq 1} W_n$. W est un sous-module de V, il est donc de type fini. Il existe $v_1, \ldots, v_n \in V$ tels que $W = \langle v_1, \ldots, v_n \rangle$. Il existe $i_1, \ldots, i_n \in \mathbb{N}^*$ des indices tels que $v_1 \in W_{i_1}, \ldots, v_n \in W_{i_n}$. Soit $i = \max(i_1, \ldots, i_n)$. Alors, $v_1, \ldots, v_n \in W_i$. Donc, $\langle v_1, \ldots, v_n \rangle \subset W_i$, *i.e* que $W \subset W_i$. On conclut que $W_i = W$ et que la suite est stationnaire.

— $(iv) \implies (iii)$. Par l'absurde, supposons qu'il existe $W \subset V$ un module qui n'est pas de type fini. On veut construire une chaîne $W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$ strictement croissante. Soit $v_1 \in W$. Puisque W n'est pas de type fini, $\langle v_1 \rangle \subsetneq W$. Soit $v_2 \in W \backslash \langle v_1 \rangle$. Encore une fois, $\langle v_1, v_2 \rangle \subsetneq W$. On construit par récurrence de cette façon une suite $(v_i)_{i\in\mathbb{N}^*}$. On pose pour tout $i \geq 1$, $W_i = \langle v_1, \ldots, v_i \rangle$. Alors,

$$W_1 \subsetneq W_2 \subsetneq \cdots .$$

C'est une suite croissante non-stationnaire de sous-modules. Remarquons qu'on a alors aussi montré que (i) et (ii) sont équivalents.

— $(i) \implies (iii)$. On montre le résultat dans le cas particulier où $V = A^n$ (je fais cette partie de la démonstration quand j'ai le temps).

On en déduit le cas général. Soit V un module de type fini, et $W \subset V$ un sous-module. Il existe $\mathcal{F} = (v_1, \ldots, v_n) \in V^n$ tels que $V = \langle v_1, \ldots, v_n \rangle$. On en déduit que l'application $\mathrm{CL}_{\mathcal{F}} : A^n \to V$, $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^n x_i v_i$ est surjective. Soit $\widetilde{W} = \mathrm{CL}_{\mathcal{F}}^{-1}(W)$. Alors, $\widetilde{W}$ est un sous-module de A^n, il est donc de type fini d'après le cas particulier. On écrit $\widetilde{W} = \langle \tilde{w}_1, \ldots, \tilde{w}_n \rangle$. Puisque $\mathrm{CL}_{\mathcal{F}}$ est surjective, $\mathrm{CL}_{\mathcal{F}}(\widetilde{W}) = W$, et

$$\langle \mathrm{CL}_{\mathcal{F}}(\tilde{w}_1), \ldots, \mathrm{CL}_{\mathcal{F}}(\tilde{w}_n) \rangle = W.$$

Ainsi, W est de type fini.

□

Conséquence. Puisque $\mathbb{Z}$ est noethérien, un sous-$\mathbb{Z}$-module d'un $\mathbb{Z}$-module de type fini est encore de type fini. Autrement dit, un sous-groupe d'un abélien de type fini est de type fini.

Lemme 3.2.2. *Soit A un anneau noethérien et $\mathcal{I}$ un idéal de A. Alors, $A/\mathcal{I}$ est aussi noethérien.*

Démonstration. Soit $\mathcal{J} \subset A/\mathcal{I}$ un idéal. Alors, $\pi^{-1}(\mathcal{J}) \subset A$ est un idéal de type fini par hypothèse. Il existe donc $x_1, \dots, x_n \in A$ tels que $\pi^{-1}(\mathcal{J}) = \langle x_1, \dots, x_n \rangle$. Ainsi, $\mathcal{J} = \pi(\pi^{-1}(\mathcal{J})) = \langle \pi(x_1), \dots, \pi(x_n) \rangle$.

□

Théorème 3.2.2 (de la base de Hilbert)**.** *Si A est un anneau noethérien, alors $A[X]$ l'est aussi.*

Démonstration. Soit $\mathcal{I}$ un idéal de $A[X]$, qu'on suppose ne pas être de type fini. Alors, on peut construire par récurrence avec l'axiome du choix dépendant une suite $(f_n)_{n\in\mathbb{N}}$ de polynômes dans $\mathcal{I}$ tels que pour tout $n \in \mathbb{N}$, $f_{n+1} \notin \langle f_0, \dots, f_n \rangle$ et f_n est de degré minimal. Il est clair que $(\deg f_n)_n$ n'est pas décroissante. Notons a_n le coefficient dominant de a_n et soit $\mathcal{J}$ l'idéal engendré par les a_n. Puisque A est noethérien, la suite croissante d'idéaux

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots$$

est stationnaire. Ainsi, il existe $N \in \mathbb{N}^*$ tel que $\mathcal{J} = \langle a_0, \dots, a_{N-1} \rangle$. En particulier, il existe $u_0, \dots, u_{N-1} \in A$ tels que

$$a_N = \sum_{k=0}^{N-1} u_k a_k.$$

On considère alors le polynôme

$$g(X) = \sum_{k=0}^{N-1} u_i X^{\deg(f_N)-\deg(f_k)} f_k.$$

Or, g et f_N ont même degré et coefficient dominant. Cependant, g est élément de $\langle f_0, \dots, f_{N-1} \rangle$ mais pas f_N. Nécessairement, $f_N - g \in \mathcal{I} \backslash \langle f_0, \dots, f_{N-1} \rangle$ est de degré strictement plus petit que f_N, ce qui contredit la minimalité de f_N. □

Corollaire 3.2.1. *Si A est un anneau noethérien, alors $A[X_1, \dots, X_n]$ l'est aussi.*

Remarque. Si k est un corps, l'anneau en une infinité d'indéterminées $k[X_1, X_2, \dots, X_n, \dots]$ n'est pas noethérien. En effet la suite (strictement) croissante

$$\langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \cdots$$

n'est pas stationnaire.

Corollaire 3.2.2. *Si A est un anneau noethérien, alors pour tout idéal $\mathcal{I}$ de $A[X_1, \dots, X_n]$, $A[X_1, \dots, X_n]/\mathcal{I}$ est aussi noethérien.*

3.3 Modules libres, rang, matrices

3.3.1 Modules libres et rang

Définition 3.3.1. *On appelle module* ***libre*** *tout module admettant une base.*

Exemple. Un espace vectoriel est un module libre.

Lemme 3.3.1. *Un module V admet une base de cardinal n si et seulement si V est isomorphe à A^n.*

Démonstration. Si $(v_1, \dots, v_n)$ est une base, alors l'application $\varphi : V \longrightarrow A^n$ définie par $\varphi(v_i) = e_i$ pour tout $i \in [\![1, n]\!]$, est bien définie et est un isomorphisme. Réciproquement, si V et A^n sont isomorphes, alors si $\psi : A^n \longrightarrow V$ est un isomorphisme, la famille $(\psi(e_1), \dots, \psi(e_n))$ est une base de V.

□

Remarques.

— On verra que n est indépendant du choix de la base. Cet entier n est appelé *rang de V*.

— Dans le cas infini, si I est une famille d'éléments de V, alors I est une base de V *si et seulement si* V est isomorphe à $A^{(I)}$.

3.3.2 Matrice d'une application linéaire entre modules libres.

Si $f : V \longrightarrow V'$ est une application A-linéaire, que V possède une base $\mathcal{B} = (v_1, \dots, v_n)$ et V' une base $\mathcal{B}' = (v'_1, \dots, v'_p)$. Alors f est uniquement déterminée par la décomposition des vecteurs $f(v_1), \dots, f(v_n)$ dans la base $\mathcal{B}'$. Si $f(v_i) = \sum_{j=1}^{p} m_{i,j} v'_j$, alors on note $\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(f)$ la matrice $(m_{i,j})_{i,j}$ de taille $p \times n$. Réciproquement, toute matrice $M \in \mathcal{M}_{p,n}(A)$ induit une application A-linéaire

$$\begin{array}{ccc} A^n & \longrightarrow & A^p \\ X & \longmapsto & MX \end{array}$$

est une application A-linéaire, et toute application de $A^n \longrightarrow A^p$ est de cette forme. Entre autre, on a un isomorphisme de A-modules entre $\mathrm{Hom}_A(V, V')$ et $\mathcal{M}_{p,n}(A)$ (et même un isomorphismes de A-algèbres).

Conséquence. $\mathrm{Hom}_A(V, V')$ est un module libre de rang np.

3.3.3 Déterminant.

Définition 3.3.2. *Soit $M = (m_{i,j})_{i,j} \in \mathcal{M}_n(A)$. On appelle* ***déterminant de*** *M la quantité*

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \in A.$$

Remarque. On admettra sur le déterminant les propriétés suivantes.

— Pour tout $M, N \in \mathcal{M}_n(A)$, $\det(MN) = \det M \det N$.

— Pour tout $M \in \mathcal{M}_n(A)$, ${}^t\mathrm{com}(M)M = M\,{}^t\mathrm{com}(M) = \det(M)I_n$.

Lemme 3.3.2. *Une matrice carrée $M \in \mathcal{M}_n(A)$ est inversible dans $\mathcal{M}_n(A)$ si et seulement si* $\det A$ *est inversible dans $A^\times$.*

Exemple. $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}) \mid \det(M) \in \{-1, 1\}\}$.

Proposition 3.3.1. *Si V est un module libre, les bases de V ont toutes le même cardinal.*

Démonstration. (Cas des bases finis). Supposons que V possède une base $\mathcal{B}$ de cardinal n et $\mathcal{B}'$ de cardinal p avec $n > p$. Alors, on a $A^n \cong A^p$. Il existe donc deux matrice $M \in \mathcal{M}_{n,p}(A)$ et $N \in \mathcal{M}_{p,n}(A)$ telles que $MN = I_n$ et $NM = I_p$. Soient

$$\tilde{M} = \left(\begin{array}{c|c} M & 0 \end{array}\right) \in \mathcal{M}_n(A) \quad \text{et} \quad \tilde{N} = \begin{pmatrix} N \\ \hline 0 \end{pmatrix} \in \mathcal{M}_n(A).$$

Alors, $\tilde{M}\tilde{N} = I_n$. Ainsi, $\det(\tilde{M})\det(\tilde{N}) = 1_A$ mais pourtant $\det(\tilde{M}) = 0_A$. □

3.4 Permanence des identités

On cherche à démontrer que pour tout $M, N \in \mathcal{M}_n(A)$, $\det(MN) = \det M \det N$. Cette égalité est vraie sur les espaces vectoriels, donc lorsque A est un corps. Dans l'anneau $B = \mathbb{Z}[X_{i,j}, Y_{i,j} : 1 \leq i, j \leq n]$ (des polynômes à coefficients en $2n^2$ inconnues), soit $\mathbb{X} = (X_{i,j})_{i,j}$ et $\mathbb{Y} = (Y_{i,j})_{i,j}$ des éléments de $\mathcal{M}_n(B)$. Alors, $\det \mathbb{X}$ et $\det \mathbb{Y}$ sont des éléments de B. A-t-on nécessairement $\det(\mathbb{X}\mathbb{Y}) = \det \mathbb{X} \det \mathbb{Y}$? On sait que si l'on remplace les $X_{i,j}$ et $Y_{i,j}$ par des réels $x_{i,j}$ et $y_{i,j}$, alors l'égalité tient. Nous allons combiner cette observation avec la proposition suivante.

Proposition 3.4.1. *Soient $P, Q \in \mathbb{R}[X_1, \ldots, X_r]$. Si P et Q sont analytiquement égaux, ils sont formellement égaux. En d'autres termes, si P et Q sont égaux en tant que fonctions, alors $P = Q$.*

Démonstration. Notons $\tilde{P}$ la fonction polynomiale associée à P. Par linéarité, on peut supposer sans perte de généralité que $Q = 0$. Ainsi, il nous suffit de montrer que si $\tilde{P}$ est constante à zéro, alors $P = 0$. Si $\tilde{P}$ est constante à zéro, alors ses dérivées partielles sont toutes nulles. Mais si P n'est pas le polynôme nul,

$$\frac{\partial^{i_1+\cdots+i_r}\tilde{P}}{\partial x_1^{i_1}\cdots\partial x_r^{i_r}}(0) \neq 0.$$

□

Ainsi, on peut appliquer ce résultat à notre question, et affirmer (avec $r = 2n^2$) que

$$\det(\mathbb{X}\mathbb{Y}) = \det \mathbb{X} \det \mathbb{Y}.$$

On peut maintenant démontrer l'égalité pour n'importe quelle anneau A dans $\mathcal{M}_n(A)$. Soit $M = (a_{i,j})_{i,j}$ et $N = (b_{i,j})_{i,j}$ des éléments de $\mathcal{M}_n(A)$, et soit $\varphi : \mathbb{Z} \longrightarrow A$ le morphisme canonique. Soit

de plus $\Phi : B \longrightarrow A$ l'unique morphisme d'anneaux tel que $\Phi_{|\mathbb{Z}}$, $\Phi(X_{i_j}) = a_{i,j}$ et $\Phi(Y_{i,j}) = b_{i,j}$ pour tout $i, j \in [\![1, n]\!]$. Alors, on remarque $\Phi(\det \mathbb{X}) = \det M$ et que $\Phi(\det \mathbb{Y}) = \det N$. On a enfin

$$\det(MN) = \Phi(\det(\mathbb{X}\mathbb{Y})) = \Phi(\det \mathbb{X}\ \det \mathbb{Y}) = \det M \det N.$$

3.5 Rappels sur les anneaux euclidiens et principaux

Définition 3.5.1. *Un anneau A est dit euclidien s'il est intègre et s'il est muni d'une fonction $\delta : A\backslash\{0\} \longrightarrow \mathbb{N}$ appelée **stathme euclidien** (ou jauge euclidienne) telle que pour tout $a \in A$ et $b \in B\backslash\{0_A\}$, il existe un couple $(q, r) \in A$ tel que $a = bq + r$ avec $r = 0$ ou $\delta(r) < \delta(b)$.*

Exemples. Plusieurs anneaux classiques sont euclidiens. Par exemple,

- $\mathbb{Z}$ muni du stathme défini par $\delta(n) = |n|$,
- $\mathbb{K}[X]$ lorsque $\mathbb{K}$ est un corps avec $\delta(P) = \deg P$,
- ou encore $\mathbb{Z}[i]$ avec $\delta(z) = |z|^2$.

sont euclidiens.

Remarque. On ne demande pas l'unicité du couple (q, r). Certains auteurs demandent des conditions supplémentaires sur le stathme δ. D'ailleurs, on étend son domaine de définition à A en posant par exemple $\delta(0) = 0$ sur $\mathbb{Z}$, ou $\delta(0) = -\infty$ sur $\mathbb{K}[X]$.

Proposition 3.5.1. *Tout anneau euclidien est principal.*

Démonstration. Soit $\mathcal{I} \subset A$ un idéal, et $a \in \mathcal{I}$ un élément non nul tel que $\delta(a)$ est minimal. Soit $x \in \mathcal{I}$, il existe $(q, r) \in A^2$ tel que $x = aq + r$, et $r = 0$ ou $\delta(r) < \delta(a)$. De par la structure d'idéal de $\mathcal{I}$, $r = x - aq$ est élément de $\mathcal{I}$. Or, a étant tel que $\delta(a)$ est minimal, on a nécessairement $r = 0$.

□

Remarque. Dans un anneau principal (donc aussi dans un anneau euclidien),

- tout couple $(a, b) \in (A\backslash\{0_A\})^2$ possède un pgcd ;
- le théorème de Bézout est vrai : pour tout couple $(a, b) \in A\backslash\{0_A\})^2$, il existe $(u, v) \in A^2$ un couple tel que $au + bv = \text{pgcd}(a, b)$.

Rappelons qu'un pgcd de a et b est un élément tel d tel que pour tout $x \in A$ divisant a et b, alors x divise d, c'est-à-dire que d est maximal pour la relation de division. Un pgcd est unique à association près.

Définition 3.5.2. *Soit A un anneau intègre. On dit que deux éléments d et d' de A sont **associés** si l'une des conditions (équivalentes) suivantes est vérifiée.*

(i) $d|d'$ *et* $d'|d$.

(ii) Il existe $u \in A^\times$ *tel que* $d' = du$.

(iii) $\langle d\rangle = \langle d'\rangle$ *(idéaux engendrés).*

On note $d \sim d'$.

3.6 Forme de Smith

Théorème 3.6.1. *Soit R un anneau euclidien, et soit $A \in \mathcal{M}_{n,p}(\mathbb{R})$. Alors, il existe $P \in \mathrm{GL}_n(R)$, $Q \in \mathrm{GL}_p(R)$, $r \in \mathbb{N}^*$, et $D = \mathrm{diag}(d_1, \dots d_r)$ avec $d_i \neq 0_R$ pour tout $i \in [\![1, n]\!]$ et $d_1 | d_2 | \cdots | d_r$, tels que*

$$PAQ = \left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right).$$

De plus, on peut exiger que P et Q soient produits de matrices élémentaires, ainsi $\det(P) = \det(Q) = 1_R$. Enfin, les d_i sont uniques à association près.

Démonstration. — *Existence.*

— *Unicité.* Supposons qu'on ait deux décompositions

$$PAQ = \left(\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right) \quad \text{et} \quad P'AQ' = \left(\begin{array}{c|c} D' & 0 \\ \hline 0 & 0 \end{array}\right)$$

où $D = \mathrm{diag}(d_1, \dots d_r)$ et $D' = \mathrm{diag}(d'_1, \dots d'_{r'})$. avec $d_i d'_j \neq 0_R$, $d_1 | d_2 | \cdots | d_r$ et $d'_1 | d'_2 | \cdots | d'_{r'}$. D'abord, d_1 est le PGCD de tous les coefficients de A. En effet, si $d \in \mathbb{R}$ divise tous les coefficients de A *si et seulement si* d divise tous les coefficients de

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right),$$

ce qui est équivalent à dire que d divise d_1. Ainsi, le pgcd étant unique à association près, on a $d_1 \sim d'_1$. Pour les autres coefficients, on observe la chose suivante : pour tout $i \in [\![2, r]\!]$, si Δ_i désigne le pgcd de tous les mineurs de taille i extraits de A, alors $\Delta_i \sim d_1 \cdots d_i$. En effet, lorsque qu'on effectue une opération sur les lignes et les colonnes, le pgcd des mineurs de taille i ne change pas. De plus, dans la matrice

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

le pgcd des mineurs de taille i est $d_1 \cdots d_i$. On en déduit ainsi l'unicité.

□

Remarque. Sur un corps, toute matrice est équivalente à une matrice

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

où $r = \mathrm{rg}(A)$.

Exemple.

$$\begin{pmatrix} 3 & 5 \\ 8 & 5 \end{pmatrix} \xrightarrow[L_2 \leftarrow L_2 - 2L_1]{} \begin{pmatrix} 3 & 5 \\ -2 & -5 \end{pmatrix} \xrightarrow[L_1 \leftarrow L_1 - L_2]{} \begin{pmatrix} 1 & 2 \\ 10 & -5 \end{pmatrix} \xrightarrow[L_2 \leftarrow L_2 - 2L_1]{} \begin{pmatrix} 1 & 10 \\ 0 & -25 \end{pmatrix}$$

Enfin, l'opération "$C_2 \leftarrow C_2 + 10C_1$" donne la matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & -25 \end{pmatrix}.$$

Soient u et v des entiers tels que $3u + 8v = 1$. On a $(u,) = (3, -1)$. Soit

$$P = \begin{pmatrix} u & v \\ -8 & 3 \end{pmatrix}.$$

Alors $\det P = 1$. De plus ,

$$P \times \begin{pmatrix} 3 & 5 \\ 8 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 5u + 5v \\ 0 & -25 \end{pmatrix} = \begin{pmatrix} 1 & 10 \\ 0 & -25 \end{pmatrix}.$$

Corollaire 3.6.1. *Soit R un anneau euclidien. Alors, $\mathrm{GL}_n(R)$ est engendré par les matrices élémentaires.*

Démonstration. Soit $A \in \mathrm{GL}_n(R)$. Alors, $\det A \in \mathbb{R}^\times$ et $A' = PAQ$ est aussi inversible où $A' = \mathrm{diag}(d_1, \dots d_n)$. Puisque $\det A = d_1 \cdots d_n$, alors les d_i sont tous inversibles. Pour tout $i \in [\![1, n]\!]$, on effectue l'opération $L_i \leftarrow \lambda L_i$ avec $\lambda \in \mathbb{R}^\times$. On a donc une décomposition $I_n = \tilde{P}A\tilde{Q}$, et donc $A = \tilde{P}^{-1}\tilde{Q}^{-1}$ est un produit de matrices élémentaires.

□

3.7 Interprétations et applications

3.7.1 Lien avec le pgcd et les coefficients de Bézout

Si l'on part de $A = \begin{pmatrix} a \\ b \end{pmatrix}$, l'algorithme revient à faire l'algorithme d'Euclide sur a et b. On obtient alors une matrice $\begin{pmatrix} d \\ 0 \end{pmatrix}$ où $d = a \wedge b$. Ici, il n'y a pas de matrice Q dans la décomposition de Smith. On a

$$P = \begin{pmatrix} u & v \\ w & z \end{pmatrix}.$$

On observe en fait que u et v sont des coefficients de Bézout dans le sens où $au + bv = d$. Plus généralement, si

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

alors sa forme de Smith est

$$\begin{pmatrix} d \\ \vdots \\ 0 \end{pmatrix}$$

où $d = a_1 \wedge \cdots \wedge a_n$, et la première ligne de P contient des coefficients de Bézout pour la famille $(a_1, \dots, a_n)$.

3.7.2 Applications linéaires entre $\mathbb{Z}$-modules

Corollaire 3.7.1. *Soient U et W deux $\mathbb{Z}$-modules libres de type fini, et $\varphi : V \longrightarrow W$ une application $\mathbb{Z}$-linéaire. Alors, il existe une base $\mathcal{B} = (v_1, \dots, v_n)$ de V et $\mathcal{B}' = (w_1, \dots, w_p)$ de W telles que $\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(\varphi)$ soient diagonale au sens qu'il existe $d_1, \dots, d_r$ des coefficients tels que*

$$\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(\varphi) = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

avec $d_1 | d_2 | \cdots | d_r$.

Démonstration. Conséquence directe du théorème de décomposition de Smith.

□

3.7.3 Noyau et image

Corollaire 3.7.2. *Soit R un anneau euclidien et R et W des R-modules libres de type fini, et si $\varphi : V \longrightarrow W$ une application R-linéaire, alors il existe une base de V, $(e_1, \dots, e_n)$ telle que $\ker \varphi = \langle e_1, \dots, e_s \rangle$ où $s \leq n$.*

Démonstration. Il existe une base$\mathcal{B}$ de V et $\mathcal{B}'$ de W telles que

$$\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(\varphi) = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right).$$

Ainsi, si $x \in V$,

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \ker \varphi \iff \begin{pmatrix} d_1 x_1 \\ \vdots \\ d_r x_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0.$$

Ainsi, $x \in \ker \varphi$ *si et seulement si* $x_1 = \cdots = x_r = 0$. On en déduit que $\ker \varphi = \langle e_{r+1}, \dots, e_n \rangle$.

□

Corollaire 3.7.3. *Sous les mêmes hypothèses, il existe une base $(w_1, \dots, w_p)$ de W et un $r \leq p$ tel que $\mathrm{Im}\, \varphi = \langle d_1 w_1, \dots, d_r w_r \rangle$, où $d_1, \dots d_r$ sont les coefficients apparaissant dans la forme de Smith de φ.*

Théorème 3.7.1 (de la base adaptée)**.** *Soit R un anneau euclidien, et W un sous-module d'un module libre de type fini $V \cong R^n$. Alors il existe une base $(e_1, \dots, e_n)$ de V, et $d_1, \dots, d_r$ des coefficients vérifiant $d_1|d_2|\cdots|d_r$ et $r \leq n$, tels que $(d_1e_1, \dots, d_re_r)$ soit une base de W.*

Démonstration. Puisque R est euclidien, il est principal et donc noethérien. Alors, W est de type fini. Soit donc $w_1, \dots w_k$ des générateurs de W. Alors, l'application

$$\begin{array}{rcl} R^k & \longrightarrow & V \\ (x_1, \dots, x_k) & \longmapsto & x_1w_1 + \cdots + w_kw_k \end{array}$$

est R-linéaire, d'image W. On conclut en appliquant le corollaire précédent.

□

Corollaire 3.7.4. *Tout sous-groupe de $\mathbb{Z}^n$ est un sous-groupe abélien libre de rang inférieur ou égal à n (en tant que $\mathbb{Z}$-module).*

3.8 Générateurs et relations pour un module

Soit un R-module V de type fini, et $\mathcal{F} = (v_1, \dots, v_n)$ une famille génératrice de V. On veut expliciter les relations entre $v_1, \dots, v_n$. Soit l'application

$$\begin{array}{rccl} \mathrm{CL}_{\mathcal{F}} : & R^n & \longrightarrow & V \\ & (x_1, \dots, x_n) & \longmapsto & x_1v_1 + \cdots + x_nv_n. \end{array}$$

Alors, $\ker \mathrm{CL}_{\mathcal{F}}$ est "l'ensemble des relations" satisfaites par $v_1, \dots, v_n$.

Définition 3.8.1. *On appelle présentation de V toute isomorphisme*

$$\varphi : R^n / \operatorname{Mdl}(w_1, \dots, w_p) \longrightarrow V$$

où $w_1, \dots, w_p \in R^n$. La matrice

$$(w_1| \dots |w_p) \in \mathcal{M}_{n,p}(R)$$

est appelée la matrice de la représentation.

Exemple. Si $V \cong \mathbb{Z}^3/\langle (1,2,3), (4,5,6), (7,8,9), (10,11,12)\rangle$, cela signifie que V est engendré par trois vecteurs v_1, v_2, v_3 qui satisfont les relations

$$\begin{cases} v_1 + 2v_2 + 3v_3 = 0 \\ 4v_1 + 5v_2 + 6v_3 = 0 \\ 7v_1 + 8v_2 + 9v_3 = 0 \\ 10v_1 + 11v_2 + 12v_3 = 0 \end{cases}$$

Proposition 3.8.1. *Si R est un anneau noethérien, et si V est un R-module de type fini, alors V admet un présentation.*

Démonstration. Soit $\mathcal{F} = (v_1, \dots, v_n)$ une famille génératrice de V. L'application $\mathrm{CL}_\mathcal{F}$ est surjective, et $\ker \mathrm{CL}_\mathcal{F} \subset \mathbb{R}^n$ est de type fini car R est noethérien. Soit $w_1, \dots, w_p \in \mathbb{R}^n$ un système de générateurs de $\ker \mathrm{CL}_\mathcal{F}$. Selon le théorème d'isomorphisme, on a le diagramme

$$\begin{array}{ccc} R^n & \xrightarrow{\mathrm{CL}_\mathcal{F}} & V \\ \downarrow & \nearrow_{\sim} & \\ R^n/\ker \mathrm{CL}_\mathcal{F} & & \end{array}$$

□

3.9 Théorème de structure des groupes abéliens de type fini

Soit R un anneau euclidien.

Lemme 3.9.1. *Soit $A, A' \in \mathcal{M}_{n,p}(R)$ des matrices de présentations. On suppose qu'il existe $P \in \mathrm{GL}_n(R)$ et $Q \in \mathrm{GL}_p(R)$ des matrices telles que $A' = PAQ$. Alors, les modules présentés par A et A' sont isomorphes. En d'autres termes, il existe un isomorphisme*

$$R^n/\operatorname{Im} A \xrightarrow{\sim} R^n/\operatorname{Im} A'$$

induit par le morphisme

$$\begin{array}{ccc} R^n & \longrightarrow & R^n \\ X & \longmapsto & PX. \end{array}$$

Exemple. Si l'on reprend l'exemple précédent, on remarque que

$$A = \begin{pmatrix} 1 & 4 & 7 & 10 \\ 2 & 5 & 8 & 11 \\ 3 & 6 & 9 & 12 \end{pmatrix} = P \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} Q$$

pour des certaines matrices P et Q. Ainsi, selon le lemme,

$$\mathbb{Z}^3/\langle (1,2,3), (4,5,6), (7,8,9), (10,11,12) \rangle = \mathbb{Z}^3/\langle (1,0,0), (0,3,0) \rangle$$

qui est isomorphe à $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/0\mathbb{Z} \cong \{0\} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$.

Démonstration. Puisque Q est une matrice inversible, $\operatorname{Im}(AQ) = \operatorname{Im} A$. On a donc $\operatorname{Im}(PAQ) = P \operatorname{Im}(AQ) = P \operatorname{Im} A$. On conclue avec le diagramme suivant.

$$\begin{array}{ccc} R^n & \xrightarrow{P} & R^n \\ & & \\ \operatorname{Im} A & \longrightarrow & \operatorname{Im} A' \\ \downarrow & & \downarrow \\ R^n/\operatorname{Im} A & \xrightarrow{\sim} & R^n/\operatorname{Im} A' \end{array}$$

□

Théorème 3.9.1 (structure des groupes abéliens de type fini)**.** *Soit V un groupe abélien de type fini. Alors, il existe $s \in \mathbb{N}$, et $d_1|d_2|\cdots|d_k \in \mathbb{N}$ des entiers tels que $d_i \geq 2$ pour tout $i \in [\![1,k]\!]$, et tels que*

$$V \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^s.$$

Démonstration. Soit A une matrice de présentation de V, de sorte que $V \cong \mathbb{Z}^n/\operatorname{Im} A$. Soit

$$A' = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_l & \\ \hline & 0 & & 0 \end{array}\right)$$

la forme de Smith de A. Selon le lemme précédent, V est isomorphe à

$$\mathbb{Z}^n/\langle d_1 e_1, \ldots, d_l e_l\rangle$$

où $(e_1, \ldots, e_n)$ est la base canonique de $\mathbb{Z}^n$. On conclue avec l'exercice suivant, et en supprimant les $\mathbb{Z}/d_i\mathbb{Z}$ où $d_i = 1$.

□

Exercice. Montrer que

$$Z^n/\langle d_1 e_1, \ldots, d_l e_l\rangle \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_l\mathbb{Z} \times \mathbb{Z}^{n-l}.$$

Corollaire 3.9.1 (théorème de structure, seconde version)**.** *Tout groupe abélien de type fini est isomorphe à un produit de la forme*

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \times \mathbb{Z}^s$$

où les p_i sont des nombres premiers (pas nécessairement différents), et les α_i des entiers non nuls.

Théorème 3.9.2 (unicité dans les théorèmes de structures)**.** *Les décompositions dans les théorèmes de structure sont uniques au sens suivant.*

(i) Si

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^s \cong \mathbb{Z}/d'_1\mathbb{Z} \times \mathbb{Z}/d'_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_{k'}\mathbb{Z} \times \mathbb{Z}^{s'}$$

avec $d_i, d'_j \geq 2$, $d_1|d_2|\cdots|d_k$ et $d'_1|d'_2|\cdots|d'_k$. Alors, $s = s'$, $k = k'$ et $d_i = d'_i$ pour tout $i \in [\![1,k]\!]$.

(ii) Si

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z} \times \mathbb{Z}^s \cong \mathbb{Z}/q_1^{\beta_1}\mathbb{Z} \times \mathbb{Z}/q_2^{\beta_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{\beta_l}\mathbb{Z} \times \mathbb{Z}^{s'}$$

avec p_i, q_j des nombres premiers et α_1, β_j des entiers non nuls. Alors, $s = s'$, $k = l$ et quitte à réordonner, $p_i^{\alpha_i} = q_i^{\beta_i}$.

3.10 Application en algèbre linéaires

On a déjà vu que la donnée d'un $\mathbb{Z}$-module est équivalente à la donnée d'un groupe abélien. De même, si $\mathbb{K}$ est un corps, la donnée d'un $\mathbb{K}[X]$-module équivaut à la donnée d'un couple (V, u), où V est un $\mathbb{K}$-espace vectoriel et $u \in \mathscr{L}(V)$ est un endomorphisme de $\mathbb{K}$-espaces vectoriels. Si l'on se donne (V, u) un tel couple, alors V a une structure de $\mathbb{K}[X]$-module définie de la manière suivante : pour tout $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ et $v \in V$,

$$P \times v = \sum_{k=0}^{n} a_k u^k(v).$$

Réciproquement, si V est un $\mathbb{K}[X]$-module, alors c'est un $\mathbb{K}$-espace vectoriel en restreignant la loi de composition externe à $\mathbb{K}$ (ou plutôt à $\mathbb{K}^2$). On définit alors $u : V \to V$, $v \mapsto X \cdot v$. On montre aussi que la donnée d'un sous-$\mathbb{K}[X]$-module équivaut à la donnée d'un sous-$\mathbb{K}$-espace vectoriel stable par u.

$\mathbb{K}[X]$ est un anneau euclidien, donc le théorème de forme normale de Smith s'applique ainsi que le théorème de structure des $\mathbb{K}[X]$-modules de type fini.

Présentation d'un $\mathbb{K}[X]$-module. On suppose ici $V = \mathbb{K}^n$, que l'on munit toujours de son endomorphisme $u \in \mathscr{L}(\mathbb{K}^n)$. Si $u : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ a pour matrice $A \in \mathcal{M}_n(\mathbb{K})$ dans la base canonique de $\mathbb{K}^n$, alors pour tout $i \in [\![1, n]\!]$, $u(e_i) = Ae_i$, et donc $Xe_i = Ae_i$. Ainsi, $(A - XI_n)e_i = 0$. Si l'on note $A = (a_{i,j})_{i,j}$, on trouve que

$$\sum_{j=1}^{n} a_{i,j} e_j - Xe_i = 0.$$

C'est une relation dans $V = \mathbb{K}^n$ entre les e_k. En fait, ces relations forment une présentation du $\mathbb{K}[X]$-module V. De plus, sa matrice de présentation est $A - XI_n$, et alors V est isomorphe en tant que $\mathbb{K}[X]$-module à

$$\mathbb{K}[X]^n / \operatorname{Im}(A - XI_n).$$

Exemple. Si

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},$$

alors on a

$$\begin{array}{rccc} u : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x, y) & \longmapsto & (x + 2y, 3x + 4y). \end{array}$$

Le $\mathbb{R}[X]$-module associé a pour matrice de présentation

$$\begin{pmatrix} 1 - X & 2 \\ 3 & 4 - X \end{pmatrix}.$$

On peut lui appliquer le théorème de Smith, et il existe alors $P_1, \ldots, P_r \in \mathbb{R}[X]$ des polynômes telles que la matrice précédente soit semblable à

$$\left(\begin{array}{ccc|c} P_1 & & & \\ & \ddots & & 0 \\ & & P_r & \\ \hline & 0 & & 0 \end{array}\right)$$

et $P_1|\cdots|P_r$. Puisque V est de dimension finie sur $\mathbb{K}$. Alors,

$$V \cong \mathbb{K}[X]^n/\operatorname{Im}(A - XI_n) \cong \mathbb{K}[X]^{n-r} \prod_{i=1}^{r} \mathbb{K}[X]/\langle P_i\rangle.$$

Puisque V est de dimension finie sur $\mathbb{K}$, $n = r$. De plus, certains P_i peuvent être constants non nulles, et alors $\mathbb{K}[X]/\langle P_i\rangle = \{0\}$. On peut décider d'enlever ses polynômes pour simplifier la décomposition.

Nos interrogations se résument en fait à la suivante : à quoi correspondent les $\mathbb{K}[X]$-modules de la forme $\mathbb{K}[X]/\langle P\rangle$.

Lemme 3.10.1. *Supposons V un $\mathbb{K}$-espace vectoriel de dimension finie, et $u \in \mathscr{L}(V)$. Sont équivalents.*

(i) Le $\mathbb{K}[X]$-module associé à (V, u) est est isomorphe à

$$\mathbb{K}[X]/\langle P\rangle.$$

(ii) P est le polynôme minimal de u et V est cyclique, i.e qu'il existe $v_0 \in V$ et $d \in \mathbb{N}$ tel que

$$V = \operatorname{Vect}(v_0, u(v_0), \ldots, u^{d-1}(v_0)).$$

(iii) Il existe une base $\mathcal{B}$ de V en tant que $\mathbb{K}$-espace vectoriel dans laquelle la matrice de u s'écrit sous la forme

$$\operatorname{mat}_{\mathcal{B}}(u) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

appelée matrice compagnon du polynôme $X^d + a_{d-1}X^{d-1} + \cdot + a_0$.

Théorème 3.10.1 (théorème des invariants de similitude)**.** *Soit $\mathbb{K}$ un corps, V un $\mathbb{K}$-espace vectoriel de dimension finie, et $u : V \longrightarrow V$ un endomorphisme de $\mathbb{K}$-espaces vectoriels. Alors, il existe une décomposition en somme directe en sous-espaces stables par u,*

$$V = V_1 \oplus \cdots \oplus V_k$$

telle que

(i) pour tout $i \in [\![1, k]\!]$, $u_{|V_i}$ est cyclique ;

(ii) le polynôme minimal de $u_{|V_i}$ est le polynôme unitaire non constant P_i.

(iii) $P_1|P_2|\cdots|P_k$.

*Les P_i sont appelés **invariants de similitude** de u. De plus, deux endomorphismes $u \in \mathscr{L}(V)$ et $u' \in \mathscr{L}(V')$ sont conjugués si et seulement s'ils ont les mêmes invariants de similitude, au sens où il existe $\varphi : V \longrightarrow V'$ un isomorphisme tel que $u' = \varphi u \varphi^{-1}$.*

Soit P_i le polynôme minimal de $u_{|V_i}$. Il existe une base $\mathcal{B}$ de V tel que

$$\mathrm{mat}_{\mathcal{B}}(u) = \begin{pmatrix} \mathcal{C}(P_1) & & (0) \\ & \ddots & \\ (0) & & \mathcal{C}(P_k) \end{pmatrix}$$

où $\mathcal{C}(P_i)$ est la matrice compagnon de $u_{|V_i}$, et $P_1 | \cdots | P_r$.

Corollaire 3.10.1. *Il existe un algorithme qui prend en entrée deux matrices dans $\mathcal{M}_n(\mathbb{Q})$, vérifiant si elles sont conjugués ou non dans $\mathcal{M}_n(\mathbb{Q})$.*

Chapitre 4

Extensions de corps, éléments algébriques, degré, règle et compas

4.1 Extensions de corps, éléments algébriques, degré

4.1.1 Extensions de corps

Définition 4.1.1. *Une extension de corps $\mathbb{K}$ est un corps $\mathbb{L}$ muni d'un morphisme (injectif) $i : \mathbb{K} \longrightarrow \mathbb{L}$.*

Remarque. Le morphisme i nous indique comment plonger $\mathbb{K}$ dans le plus grand corps $\mathbb{L}$. On identifiera donc souvent $\mathbb{K}$ à son image $i(\mathbb{K})$, ce qui nous permettra de considérer $\mathbb{K}$ comme un sous-corps de $\mathbb{L}$. Notons aussi qu'un morphisme de corps est toujours non nul et est injectif.

Définition 4.1.2. *Une $\mathbb{K}$-algèbre commutative unitaire $\mathbb{L}$ est la donnée d'un couple $(\mathbb{L}, i)$ où $i : \mathbb{K} \longrightarrow \mathbb{L}$ est un morphisme de corps (injectif).*

Fait. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ (ou plus généralement une $\mathbb{K}$-algèbre), alors c'est un $\mathbb{K}$-espace vectoriel, où la loi de composition externe est la multiplication $\mathbb{L}^2 \longrightarrow \mathbb{L}$.

Définition 4.1.3. *Une extension $\mathbb{L}$ de $\mathbb{K}$ est dite être un extension **finie** si $\dim_{\mathbb{K}}(\mathbb{L}) < \infty$. On note cette dimension $[\mathbb{L} : \mathbb{K}]$, appelée **degré** de l'extension.*

Exemple. $\mathbb{C}$ est un extension finie de $\mathbb{R}$ de degré 2.

Lemme 4.1.1. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et V un $\mathbb{L}$-espace vectoriel. Alors, V est un $\mathbb{K}$-espace vectoriel, et*

$$\dim_{\mathbb{K}}(V) = [\mathbb{L} : \mathbb{K}] \dim_{\mathbb{L}}(V).$$

Démonstration. On suppose V de $\mathbb{L}$-dimension finie. Soit $v_1, \ldots, v_n$ une $\mathbb{L}$-base de V, et soit $l_1, \ldots, l_d$ un $\mathbb{K}$-base de $\mathbb{L}$. Alors, les $(l_i v_k)_{i,j}$ forment une base de V comme $\mathbb{K}$-espace vectoriel. En effet, si $v \in V$, on peut écrire

$$v = \sum_{i=1}^{n} a_i v_i$$

avec $a_i \in \mathbb{L}$ pour tout $i \in [\![1, n]\!]$. Mais pour tout $i \in [\![1, n]\!]$, il existe $(b_{i,1}, \dots, b_{i,d}) \in \mathbb{K}^d$ tel que

$$a_i = \sum_{j=1} b_{i,j} l_j.$$

Ainsi,

$$v = \sum_{i=1}^{n} \sum_{j=1}^{d} b_{i,j} l_j v_i.$$

De même, si

$$\sum_{i,j} \lambda_{i,j} l_i v_j = 0$$

avec $\lambda_{i,j} \in \mathbb{K}$, alors

$$\sum_{j=1}^{d} \left(\sum_{i=1}^{d} \lambda_{i,j} \right) v_j = 0$$

donc pour tout $j \in [\![1, d]\!]$,

$$\sum_{i=1}^{d} \lambda_{i,j} = 0$$

par liberté de $(v_1, \dots, v_n)$ sur $\mathbb{L}$. De même, on en déduit que $\lambda_{i,j} = 0$ par liberté de $(l_1, \dots, l_d)$ sur $\mathbb{K}$.

□

Définition 4.1.4. *Si $\mathbb{K} \subset \mathbb{M}$ est une extension de corps, on appelle extension de corps* ***intermédiaire*** *toute extension de corps de $\mathbb{K} \subset \mathbb{L}$ telle que $\mathbb{L} \subset \mathbb{M}$.*

Corollaire 4.1.1 (théorème de la base télescopique)**.** *Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ est une extension de corps intermédiaire, alors*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] \times [\mathbb{L} : \mathbb{K}].$$

4.1.2 Définitions des anneaux et corps $\mathbb{K}[x]$ et $\mathbb{K}(x)$

Définition 4.1.5. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps (ou une $\mathbb{K}$-algèbre), et si $x \in \mathbb{L}$, on note $\mathbb{K}[x]$ le plus petit sous-anneau de $\mathbb{L}$ contenant $\mathbb{K}$ et x.*

Remarques. On a $\mathbb{K}[x] = \{P(x) \mid P \in \mathbb{K}[X]\}$. C'est l'image du morphisme d'évaluatation

$$\Phi : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{L} \\ P & \longmapsto & P(x). \end{array} \right.$$

Plus généralement, si A est une partie de $\mathbb{L}$, on note $\mathbb{K}[A]$ le plus petit anneau contenant $\mathbb{K}$ et A. Si $A = \{x_1, \ldots, x_n\}$, on le note $\mathbb{K}[x_1, \ldots, x_n]$. S'il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[x]$, $\mathbb{L}$ est dit être une extension *monogène*.

Définition 4.1.6. *Si $\mathbb{K} \subset \mathbb{L}$ est un extension de corps, et $x \in \mathbb{L}$, on note $\mathbb{K}(x)$ le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et x.*

Remarque. On a $\mathbb{K}(x) = \{P(x)/Q(x) \mid P, Q \in \mathbb{K}[X],\ Q(x) \neq 0\}$.

Lemme 4.1.2. *Soit $\mathbb{K}$ un corps, et $\mathbb{L}$ un $\mathbb{K}$-algèbre de dimension finie sur $\mathbb{K}$. Alors, si $\mathbb{L}$ est intègre, c'est un corps.*

Démonstration. Rappelons avant tout qu'un endomorphisme injectif φ d'un espace vectoriel de dimension fini est nécessairement surjectif. Soit $x \in \mathbb{L}$ un élément non nul, et soit $\mu_x : \mathbb{L} \to \mathbb{L}$, $z \mapsto xz$. Cette application est injective car $\mathbb{L}$ est intègre, et est $\mathbb{K}$-linéaire. Cette application est donc surjective, donc $1 \in \mathrm{Im}(\mu_x)$. Il existe donc $z \in \mathbb{L}$ tel que $xz = 1$.

□

Corollaire 4.1.2. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. Alors, pour tout $x \in \mathbb{L}$, $\mathbb{K}[x]$ est automatiquement un corps. Ainsi,*

$$\mathbb{K}[x] = \mathbb{K}(x).$$

De même, pour tout $x_1, \ldots, x_n \in \mathbb{L}$,

$$\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}(x_1, \ldots, x_n).$$

4.1.3 Éléments algébriques et transcendants

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps, soit $x \in \mathbb{L}$, et soit

$$\Phi_x : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{L} \\ P & \longmapsto & P(x). \end{array} \right.$$

le morphisme d'évaluation.

Définition 4.1.7 (élément algébrique, transcendant)**.** *Si φ_x est injectif, et l'on dit que x est **transcendant** sur $\mathbb{K}$. Sinon, on dit que x est **algébrique** sur $\mathbb{K}$.*

Remarques.

— L'extension entre en jeu dans la définition : π et e sont transcendants sur $\mathbb{Q}$, mais pas sur $\mathbb{R}$. Si l'on travaille sur $\mathbb{R}$, il est souvent convenu que $\mathbb{R}$ est vu comme une extension de $\mathbb{Q}$. Ainsi, on dit généralement que π et e sont transcendants (sous-entendu sur $\mathbb{Q}$).

— Si $x \in \mathbb{L}$ est transcendant sur $\mathbb{K}$, alors $\mathbb{K}[x] \cong \mathbb{K}[X]$ et $\mathbb{K}(x) \cong \mathbb{K}(X)$. Ces remarques donnent lieu au lemme suivant.

Lemme 4.1.3. *Si $\mathbb{K} \subset \mathbb{L}$ est une extension **finie**, alors tout élément $x \in \mathbb{L}$ est algébrique sur $\mathbb{K}$.*

Démonstration. S'il existait $x \in \mathbb{L}$ transcendant sur $\mathbb{K}$, alors $\mathbb{K}[x] \cong \mathbb{K}[X]$ donc $\mathbb{K}[x]$ serait de dimension infinie sur $\mathbb{K}$, ce qui contredit l'hypothèse de finitude de l'extension.

□

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Si $x \in \mathbb{L}$ est algébrique, alors puisque $\mathbb{K}[X]$ est principal, il existe M_x un unique polynôme unitaire tel que $\ker \varphi_x = M_x\mathbb{K}[X]$.

Définition 4.1.8 (polynôme minimal)**.** *On appelle polynôme minimal de x le polynôme M_x.*

Proposition 4.1.1. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. On a les résultats suivants.*

(i) *M_x est irréductible sur $\mathbb{K}[X]$.*

(ii) *$\mathbb{K}[x]$ est isomorphe à $\mathbb{K}[X]/\langle M_x \rangle$.*

(iii) *Soit d le degré de M_x, alors $\mathbb{K}[x]$ est de dimension d sur $\mathbb{K}$, et une base de $\mathbb{K}[x]$ sur $\mathbb{K}$ est $(1, x, \dots, x^{d-1})$.*

Remarques. On a $\deg M_x = [\mathbb{K}[x] : \mathbb{K}]$. Cet entier est appelé *degré* de x sur $\mathbb{K}$

Exemple. $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/\langle X^2 + 1 \rangle$.

Démonstration. *(i)* Si M_x n'était pas irréductible, il existerait un polynôme de plus petit degré (strictement) s'annulant en x, ce qui contredirait la minimalité de M_x.

(ii) Appliquer le théorème d'isomorphisme.

(iii) On sait que $(1, \overline{X}, \dots, \overline{X}^{d-1})$ est une base de $\mathbb{K}[X]/\langle M_x \rangle$ (où $\overline{X}$ est le projeté de X dans $\mathbb{K}[X]/\langle M_x \rangle$). On en conclut avec le point précédent.

□

Lemme 4.1.4. *Soit $\mathbb{L}$ une extension finie de $\mathbb{K}$ de degré $d = [\mathbb{L} : \mathbb{K}]$. Alors pour tout $x \in \mathbb{L}$, le degré de x divise d.*

Démonstration. Pour tout $x \in \mathbb{L}$, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}[x]] \times [\mathbb{K}[x] : \mathbb{K}]$.

□

Lemme 4.1.5. *Soit $\mathbb{K} \subset \mathbb{L}$ un extension de corps, l'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un corps.*

Démonstration. Soient $x, y \in \mathbb{L}$ des éléments algébriques sur $\mathbb{K}$. Alors,

$$\mathbb{K}[x] = \mathrm{Vect}_{\mathbb{K}}(1, x, \ldots, x^{d-1})$$

donc $\mathbb{K}[x]$ est de $\mathbb{K}$-dimension finie et est alors un corps (lemme 4.1.2). On pose $\mathbb{M} = \mathbb{K}[X]$. Puisque y est algébrique sur $\mathbb{K}$, il existe un polynôme unitaire $f \in \mathbb{K}[X]$ s'annulant en y. Ainsi, y est algébrique sur $\mathbb{M}$ puisque f est un polynôme unitaire à coefficients dans $\mathbb{M}$ ($\mathbb{K} \subset \mathbb{M}$) qui s'annule en y. Ainsi, $\mathbb{M}[y]$ est dimension finie sur $\mathbb{M}$ et donc sur $\mathbb{K}$ (théorème de la base télescopique) et c'est aussi un corps (corollaire 4.1.2). Ainsi, $\mathcal{M}[y] = \mathbb{K}[x, y]$ contient xy, $x + y$, et x/y. D'après le lemme 4.1.2, ces trois éléments sont donc algébriques sur $\mathbb{K}$.

□

Exemple. $\sqrt{2} + \sqrt{3} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, c'est en tout cas affirmé par le théorème. En revanche, trouver un polynôme de $\mathbb{Q}[X]$ l'annulant n'est pas chose facile. Une façon de construire un tel polynôme consiste à écrire la matrice de $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \to \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $x \mapsto (\sqrt{2} + \sqrt{3})x$ dans la base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$, puis à appliquer le théorème de Cayley-Hamilton.

4.2 Construction à la règle et au compas

4.3 Corps de rupture et corps de décomposition

4.3.1 Corps de rupture d'un polynôme irréductible

Si $f \in \mathbb{K}[X]$ est un polynôme irréductible de degré supérieur ou égal à deux, alors il n'a pas de racine dans $\mathbb{K}$. Nous avons vu précédemment comment adjoindre à $\mathbb{K}$ un élément satisfaisant certaines équations polynomiales. La présente sous-section aura pour objectif d'adjoindre à $\mathbb{K}$ un élément qui soit racine de $\mathbb{K}$, mais de sorte qu'on puisse encore travailler sur un corps.

Lemme 4.3.1. *Soit $f \in \mathbb{K}[X]$ un polynôme irréductible. Alors, $\mathbb{K}[X]/\langle f \rangle$ est un corps. C'est plus particulièrement une extension de corps de $\mathbb{K}$ lorsqu'il est muni de la restriction de la projection canonique à $\mathbb{K}$, $\pi_{|\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{K}[X]/\langle f \rangle$.*

Démonstration. Soit $\overline{g} \in \mathbb{L} := \mathbb{K}[X]/\langle f \rangle$ un élément non nul. Alors $g \in \mathbb{K}[X]$ n'est pas divisible par f. Puisque f est irréductible, f et g sont premiers entre eux, il existe donc $u, v \in \mathbb{K}[X]$ tel que $uf + vg = 1$. Dans $\mathbb{L}$, cette égalité devient $\overline{gv} = 1_{\mathbb{L}}$.

□

Remarque. Si $x = \overline{X}$, alors par construction x est racine de f dans le corps $\mathbb{L}$.

Définition 4.3.1. *Soit $\mathbb{K}$ un corps, et $f \in \mathbb{K}[X]$ un polynôme irréductible. On appelle corps de **rupture** de f (relativement à $\mathbb{K}$) toute extension de corps $\mathbb{L}$ de $\mathbb{K}$ contenant une racine x de f et telle que $\mathbb{L} = \mathbb{K}[x]$.*

On a fait montré que $\mathbb{K}[X]/\langle f \rangle$ est un corps de rupture de f par rapport à $\mathbb{K}$ dans le cas où f est irréductible. Le lemme suivant montre que les corps de rupture sont isomorphes, et unique au sens suivant.

Lemme 4.3.2. *Soit $\mathbb{L}$ un corps de rupture de $f \in \mathbb{K}[X]$, un polynôme irréductible. Soit $(\mathbb{M}, y)$ où $\mathbb{M}$ est une extension de $\mathbb{K}$ et $y \in \mathbb{M}$ racine de f. Il existe un unique morphisme $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ envoyant x sur y tel que $\varphi_{|\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. Si de plus $\mathbb{M}$ est aussi un corps de rupture de f relativement à $\mathbb{K}$, φ est un isomorphisme.*

Démonstration. Le corps $\mathbb{L}_0 = \mathbb{K}[X]/\langle f \rangle$ est un corps de rupture. Le morphisme d'évaluation en x $\Phi_x : \mathbb{K}[X] \longrightarrow \mathbb{L}$ passe au quotient en un isomorphisme $\overline{\Phi}_x : \mathbb{L}_0 \longrightarrow \mathbb{L}$ qui se restreint à l'identité $\mathbb{K}$. Le morphisme d'évaluation $\Phi_y : \mathbb{K}[X] \longrightarrow \mathbb{M}$ passe au quotient en un morphisme $\overline{\Phi}_y : \mathbb{L}_0 \longrightarrow \mathbb{M}$. Le morphisme $\varphi = \overline{\Phi}_y \circ \overline{\Phi}_x$ convient. Puisque que c'est un morphisme de corps, il est nécessairement injectif. Cela démontre son existence. Pour l'unicité : si $\mathbb{M}$ est une corps de rupture de f et si φ_1 et φ_2 sont deux morphismes d'anneaux vérifiant la même propriété que φ, alors ces morphismes coïncident sur $\mathbb{K}$ et sur x donc sur $\mathbb{K}[x] = \mathbb{L}$. Puisque $\mathbb{M} = \mathbb{K}[y]$, φ est nécessairement surjectif.

□

4.3.2 Corps de décomposition d'un polynôme quelconque

Désormais, on ne travaille plus nécessairement avec des polynômes irréductibles.

Proposition 4.3.1. *Soit $\mathbb{K}$ un corps et $f \in \mathbb{K}[X]$ un polynôme unitaire de degré $d \geq 1$. Il existe une extension finie $\mathbb{L}$ de $\mathbb{K}$ tel que f est scindé dans $\mathbb{L}[X]$ (i.e que f s'y écrit comme produit de polynômes de degré 1). De plus, $[\mathbb{L} : \mathbb{K}] \leq d!$.*

Démonstration. On raisonne par récurrence sur $d \in \mathbb{N}^*$. Si $d = 1$, c'est évident. On suppose $d \geq 2$ et soit $f \in \mathbb{K}[X]$ un polynôme unitaire de degré d. Soit de plus Q_1 un facteur irréductible de f de degré au moins 2 (il existe car sinon f serait déjà scindé). Soit $\mathbb{L}_1 = \mathbb{K}[T]/\langle Q \rangle$ (on note ici T l'indéterminée) le corps de rupture associé. $\mathbb{L}_1$ peut être vu comme un corps contenant $\mathbb{K}$, et donc f peut être vu comme un polynôme de $\mathbb{L}_1[X]$. Or, f a une racine dans $\mathbb{L}_1$ donc f s'écrit $(X - x_1)f_1$ dans $\mathbb{L}_1[X]$ avec f_1 un polynôme de degré $d - 1$. On conclut avec l'hypothèse de récurrence appliquée à f_1

□

Définition 4.3.2. *Soit $\mathbb{K}$ un corps, et $f \in \mathbb{K}[X]$. On appelle corps de **décomposition** de f (relativement à $\mathbb{K}$) toute extension de corps $\mathbb{L}$ de $\mathbb{K}$ telle que f soit scindé dans $\mathbb{L}[X]$ et telle qu'il existe $x \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}[x_1, \ldots, x_d]$.*

Une extension de décomposition est la plus petite possible dans laquelle f est scindé. On a en fait montré le lemme suivant.

Lemme 4.3.3. *Soit $f \in \mathbb{K}[X]$ un polynôme. Alors, il existe une extension de décomposition de f.*

L'unicité suit naturellement.

Lemme 4.3.4. *Soit $\mathbb{L}$ une extension de décomposition de $f \in \mathbb{K}[X]$ et $\mathbb{M}$ une extension quelconque de $\mathbb{K}$.*

(i) Si f est scindé dans $\mathbb{M}$, il existe un morphisme $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ tel que $\varphi_{|\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.

(ii) Si de plus $\mathbb{M}$ est une extension de décomposition, φ est un isomorphisme.

En particulier, si $\mathbb{L}$ et $\mathbb{M}$ sont deux extensions de décomposition de f, elles sont isomorphes.

Démonstration. Exercice.

□

4.3.3 Propriété de divisibilité préservées dans une extension

Nous travaillons depuis quelques sections et sous-sections avec des polynômes $P \in \mathbb{K}[X]$ et considérons des extensions $\mathbb{L}$ de $\mathbb{K}$. Alors, P peut être vu comme un polynôme de $\mathbb{L}[X]$. C'est un fait que nous avons utilisé maintes fois, mais il est important de se demander si des propriétés basiques d'arithmétiques polynomiale passe de $\mathbb{K}[X]$ à $\mathbb{L}[X]$.

Lemme 4.3.5. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps, et $A, B \in \mathbb{K}[X]$.*

(i) La division euclidienne dans $\mathbb{K}[X]$ et $\mathbb{L}[X]$ de A par B ont mêmes quotients et restes.

(ii) A divise B dans $\mathbb{L}[X]$ si et seulement si A divise B dans $\mathbb{K}[X]$.

(iii) Le pgcd unitaire de A et B dans $\mathbb{K}[X]$ est le même que dans $\mathbb{L}[X]$.

(iv) Si A et B ont une racine commune dans $\mathbb{L}$, alors A et B ne sont pas premiers entre eux dans $\mathbb{K}[X]$. Réciproquement, si A et B ne sont pas premiers entre eux dans $\mathbb{K}[X]$, il existe une extension $\mathbb{M}$ de $\mathbb{K}$ dans laquelle A et B ont une racine commune.

Démonstration. (*i*) Si $A = BQ + R$ dans $\mathbb{K}[X]$ avec $\deg R < \deg B$, alors c'est une écriture valide de la division euclidienne de A par B dans $\mathbb{L}[X]$. On conclut par unicité.

(*ii*) Découle de (*i*).

(*iii*) C'est une conséquence du point (*i*). En effet, le pgcd est calculé par l'algorithme d'Euclide. Dans les deux corps, le pgcd sera donc le même puisque le résultat de l'algorithme d'Euclide sera déterminé par les mêmes divisions euclidiennes.

(*iv*) Si A et B ont une racine commune $\alpha \in \mathbb{L}$, alors $X - \alpha$ divise $A \wedge B$ qui ne peut donc pas 1 dans $\mathbb{K}[X]$ (car son degré est nécessairement supérieur ou égal à 1). Réciproquement si $D = A \wedge B \in \mathbb{K}[X]$ n'est pas constant, soit $\mathbb{K} \subset \mathbb{L}$ un corps de décomposition de $D(X)$, et $\alpha \in \mathbb{L}$ une racine de $D(X)$ (elle existe car D est scindé et non constant dans $\mathbb{L}$). Puisque D divise A et B, α est racine de A et B.

□

4.3.4 Racines multiples

Soit $\mathbb{K}$ un corps.

Définition 4.3.3. *Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une racine multiple de P si $(X - a)^2$ divise P.*

Lemme 4.3.6. *Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors, α est une racine multiple de P si et seulement si $P(\alpha) = P'(\alpha) = 0$.*

Démonstration. Exercice.

□

Corollaire 4.3.1. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Alors, P n'a de racine multiple dans aucune extension de $\mathbb{K}$, sauf lorsque P' est le polynôme nul.*

Remarque. En caractéristique nulle, P' n'est jamais nul lorsque P est irréductible.

Fait général. P est non constant et P' est est nul *si et seulement si* $\mathbb{K}$ est d'une certaine caractéristique $p > 0$ et il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X^p)$.

Démonstration. Exercice.

□

4.3.5 Clôture algébrique

Rappel. Si $\mathbb{K} \subset \mathbb{L}$ est une extension de corps, un élément $x \in \mathbb{L}$ est *algébrique* sur $\mathbb{K}$ *si et seulement si* $[\mathbb{K}[x] : \mathbb{K}] < \infty$. De manière équivalente, x est algébrique *si et seulement s'il* existe $f \in \mathbb{K}[X]$ un polynôme non nul tel que $f(x) = 0$.

Définition 4.3.4. *Une extension $\mathbb{K} \subset \mathbb{L}$ est **algébrique** si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.*

Exemple. Une extension finie $\mathbb{K} \subset \mathbb{L}$ est toujours algébrique car $[\mathbb{K}[x] : \mathbb{K}] < [\mathbb{L} : \mathbb{K}]$, mais la réciproque est fausse. En effet, si $\overline{\mathbb{Q}}$ désigne l'ensemble des éléments algébriques sur $\mathbb{Q}$, alors $\overline{\mathbb{Q}}$ est un corps mais $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Lemme 4.3.7. *Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des extensions de corps. Si $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et $\mathbb{M}$ est algébrique sur $\mathbb{L}$, alors $\mathbb{M}$ est algébrique sur $\mathbb{K}$.*

Démonstration. Soit $x \in \mathbb{M}$. Puisque x est algébrique sur $\mathbb{L}$, x est racine d'un polynôme $P = \sum_{k=0}^{d} l_i X^i$ de $\mathbb{L}[X]$. Or, les l_i sont algébriques sur $\mathbb{K}$. On a donc une tour d'extensions finies

$$\mathbb{K} \subset \mathbb{K}[l_0] \subset \mathbb{K}[l_0, l_1] \subset \cdots \subset \mathbb{K}[l_0, \ldots, l_d].$$

On a donc que $[\mathbb{K}[l_0, \ldots, l_d] : \mathbb{K}] < \infty$. Or, $[\mathbb{K}[l_0, \ldots, l_d][x] : \mathbb{K}[l_0, \ldots, l_d]] < \infty$ puisque x est racine de P. Ainsi, $[\mathbb{K}[l_0, \ldots, l_d, x] : \mathbb{K}] < \infty$ donc $[\mathbb{K}[x] : \mathbb{K}] < \infty$ car $\mathbb{K}[x] \subset \mathbb{K}[l_0, \ldots, l_d, x]$.

□

Définition 4.3.5. *Un corps $\mathbb{K}$ est dit **algébriquement** clos si tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet une racine dans $\mathbb{K}$.*

Remarque. Il est équivalent dire que tout polynôme est scindé dans $\mathbb{K}$.

Exemple. Les corps finis ne sont *jamais* algébriquement clos.

Théorème 4.3.1. *Le corps $\mathbb{C}$ est algébriquement clos.*

Démonstration. C'est une conséquence du théorème de Liouville qui affirme que toute fonction holomorphe $f : \mathbb{C} \longrightarrow \mathbb{C}$ est bornée est constante. Supposons par l'absurde qu'il existe $P \in \mathbb{C}[X]$ avec $\deg P \geq 1$ sans racine dans $\mathbb{C}$. Alors, la fonction $f : \mathbb{C} \to \mathbb{C}$, $z \mapsto 1/P(z)$ est telle que $f(z) \xrightarrow[|z|\to\infty]{} 0$ car $\deg P \geq 1$. Ainsi, f est bornée donc constante ce qui est contradictoire.

□

Définition 4.3.6. *Soit $\mathbb{K}$ un corps. On appelle clôture algébrique de $\mathbb{K}$ toute extension $\mathbb{L}$ de $\mathbb{K}$ algébriquement close et algébrique sur $\mathbb{K}$.*

Exemple. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Proposition 4.3.2. *Tout corps admet une clôture algébrique. De plus, si $\mathbb{L}$ et $\mathbb{L}'$ sont deux clôtures algébriques de $\mathbb{K}$, il existe un isomorphisme $\varphi : \mathbb{L} \longrightarrow \mathbb{L}'$ tel que $\varphi_{|\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.*

Démonstration. Pour l'existence, on utilise les corps de décomposition et lemme de Zorn.

□

Chapitre 5

Corps finis

Remarquons qu'en anglais, les corps finis sont appelés Galois *fields*. L'intérêt de ce chapitre est de classifier les corps finis : tout corps fini a pour cardinal une puissance d'un nombre premier, et les corps de mêmes cardinaux sont uniques à isomorphismes près. En particulier, si $\mathbb{K}$ est un corps fini de cardinal p premier, alors $\mathbb{K} \cong \mathbb{Z}/p\mathbb{Z}$.

5.1 Propriétés élémentaires des corps finis

5.1.1 Cardinal

Soit $\mathbb{K}$ un corps. On appelle *sous-corps premier* de $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$. C'est le corps engendré par $1_{\mathbb{K}}$. En caractéristique nulle, il est isomorphe à $\mathbb{Q}$. En caractéristique p (avec p premier), il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. En effet, c'est l'image du morphisme canonique $\mathbb{Z} \longrightarrow \mathbb{K}$ d'image isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Lemme 5.1.1. *Soit $\mathbb{K}$ un corps fini et soit p sa caractéristique. Alors, $\mathbb{K}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Ainsi, il existe $r \geq 1$ tel que $|\mathbb{K}| = p^r$.*

Conséquence. Il n'existe pas de corps de cardinal 6. Plus généralement, il n'existe aucun corps de cardinal produit d'au moins deux nombres premiers distincts.

Lemme 5.1.2. *Soit $\mathbb{K}$ un corps fini de cardinal $q = p^r$ (p premier, $r \geq 1$). On a les propriétés suivantes.*

(i) Pour tout $x \in \mathbb{K}$, $x^q = x$.

(ii) Pour tout $x \in \mathbb{K}^*$, $x^{q-1} = 1_{\mathbb{K}}$.

(iii) Le groupe multiplicatif $\mathbb{K}^*$ est un groupe cyclique de cardinal $q - 1$.

5.1.2 Morphisme de Frobenius

Définition 5.1.1. *Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. L'application $\varphi : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$ est appelé **morphisme de Frobenius**.*

Remarque. Le morphisme de Frobenius est... un morphisme[1] de corps.

Proposition 5.1.1. *Si $\mathbb{K}$ est un corps fini et $\varphi : \mathbb{K} \longrightarrow \mathbb{K}$ est un automorphisme, alors l'ensemble* $\operatorname{Fix}\varphi$ *des points fixes de φ est un sous-corps de $\mathbb{K}$.*

Remarque. Si $\mathbb{K}$ est fini de caractéristique $p > 0$ et φ le morphisme de Frobenius, alors $\operatorname{Fix}\varphi \cong \mathbb{Z}/p\mathbb{Z}$.

Corollaire 5.1.1. *Soit $f \in (\mathbb{Z}/p\mathbb{Z})[X]$. Alors, $f(X^p) = f(X)^p$.*

5.2 Existences et unicités des corps finis

5.2.1 Existence et unicité

Théorème 5.2.1. *Pour tout entier p premier et $r \in \mathbb{N}^*$, il existe à isomorphisme près un unique corps de cardinal $q = p^r$ noté $\mathbb{F}_q$.*

Remarque. L'isomorphisme entre deux corps de même cardinal est rarement unique.

Lemme 5.2.1. *Le polynôme $X^{p^r} - X \in \mathbb{F}_p[X]$ est à racines simples dans toute extension de $\mathbb{F}_p$.*

Démonstration. Notons f ce polynôme. On remarque que $f' = 1$, toute racine est nécessairement simple.

□

Démonstration (du théorème).
— *Unicité.* On va montrer que si $\mathbb{K}$ est un tel corps, alors c'est un corps de décomposition $f(X) = X^{p^r} - X$ relativement à $\mathbb{F}_p$ (qui lui est toujours unique). Soit donc $\mathbb{K}$ un tel corps (de cardinal p^r). Chacun de ses éléments est une racine de f, donc f admet p^r racines distinctes dans $\mathbb{K}$ et est donc scindé dans $\mathbb{K}$. C'est bien un corps de décomposition puisque $\mathbb{K}$ est engendré par les racines de f (c'est même exactement l'ensemble des racines de f).

— *Existence.* Soit $\mathbb{K}$ un corps de décomposition de f relativement à $\mathbb{F}_q$. Comme vu dans le point précédent, les racines de f sont toujours simples donc $\mathbb{K}$ a un cardinal d'au moins p^r. Or, l'ensemble des racines de f est exactement l'ensemble des points fixes de $\Phi^r : \mathbb{K} \longrightarrow \mathbb{K}$ (le morphisme de Frobenius itéré k-fois). Notons $\mathbb{L}$ le sous-corps de $\mathbb{K}$ des racines de f. Il est exactement de cardinal p^r. Or, $\mathbb{K}$ étant un corps de décomposition de f relativement à $\mathbb{F}_p$, il est minimal. Ainsi, $\mathbb{K} = \mathbb{L}$.

□

1. Stupéfiant, je sais.

5.2.2 Plongements entre corps finis

Lemme 5.2.2 (divisibilité). *On a les propriétés suivantes.*

- *Soit $\mathbb{K}$ un corps et $n, m \in \mathbb{N}$. Alors, $X^n - 1$ divise $X^m - 1$ si et seulement si n divise m.*
- *Soit $a \geq 2$ un entier, et $n, m \in \mathbb{N}$. Alors, $a \in \mathbb{N}$ $a^n - 1$ divise $a^m - 1$ si et seulement si n divise m.*
- *Si $\mathbb{K}$ est de caractéristique $p > 0$ et $r, s \in \mathbb{N}$, alors $X^{p^r} - X$ divise $X^{p^s} - X$ si et seulement si r divise s.*

Démonstration. Pour les deux premières propositions, écrire la division euclidienne de m par n. Montrons la dernière. On que $X^{p^r} - X$ divise $X^{p^s} - X$ *si et seulement si* $X^{p^r-1} - 1$ divise $X^{p^s-1} - 1$, ce qui est encore équivalent à ce que $p^r - 1$ divise $p^s - 1$, *i.e* que r divise s.

□

Proposition 5.2.1. *$\mathbb{F}_{p^r}$ se plonge dans $\mathbb{F}_{p^s}$ si et seulement si r divise s. Dans ce cas, $\mathbb{F}_{p^s}$ a un unique sous-corps isomorphe à $\mathbb{F}_{p^r}$, et $[\mathbb{F}_{p^s} : \mathbb{F}_{p^r}] = s/r$.*

Démonstration. Si $\mathbb{F}_{p^r}$ se plonge dans $\mathbb{F}_{p^s}$, alors $\mathbb{F}_{p^s}$ est un $\mathbb{F}_{p^r}$-espace vectoriel isomorphe à $\mathbb{F}_{p^r}^n$ où n est sa dimension. On a alors $p^s = (p^r)^n$ donc $s = rn$ et r divise s. Réciproquement si $\mathbb{K}$ est un corps de cardinal p^s, alors si φ est le morphisme de Frobenius sur $\mathbb{K}$, alors les points fixes de φ^r sont les éléments $x \in \mathbb{K}$ tel que $x^{p^r} - x = 0$. C'est un sous-corps k de cardinal p^r puisque c'est l'ensemble des racines d'un polynôme de degré p^r. Puisque $X^{p^r} - X$ divise $X^{p^s} - X$, et que $X^{p^s} - X$ est scindé à racines simples sur L, alors il en est de même pour $X^{p^r} - X$. Ce polynôme a donc exactement p^r racines donc $|k| = p^r$. Enfin, ce sous-corps est unique puisqu'il est toujours l'ensemble des racines de $X^{p^r} - X$.

□

5.3 Polynômes irréductibles sur un corps fini

Pour décrire les corps finis, on va chercher à les écrire sous la forme $\mathbb{F}_p[X]/\langle P \rangle$ (qui est bien un corps lorsque P est irréductible). Le cardinal d'un tel corps est p^d où $d = \deg P$. Par exemple, on peut construire $\mathbb{F}_{7^10}$, il suffit de trouver un polynôme de degré 10 irréductible dans $\mathbb{F}_p[X]$. C'est possible pour tout corps de cardinal p^r de le construire ainsi. En effet, $\mathbb{F}_{p^r}^\times$ est cyclique. Soit donc α un générateur de ce groupe. Alors, $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^r}$ et si $P \in \mathbb{F}_p[X]$ est le polynôme minimal de α, alors c'est un polynôme irréductible de degré r. On peut même trouver algorithmiquement des polynômes irréductibles : au hasard. Il suffit en fait de prendre dans $\mathbb{F}_p[X]$ un polynôme de degré n et de vérifier s'il est irréductible. Si ce n'est pas le cas, on recommence. Pour comprendre l'efficacité de cet algorithme il nous faut savoir deux choses :

(*i*) parmi les polynômes unitaires de degré n, si la proportion de polynômes irréductibles est assez grande ;

(*ii*) s'il existe un bon algorithme de test d'irréductibilité.

Proposition 5.3.1. *Soit $\mathbb{F}_q$ un corps fini de cardinal q, et soit $\mathcal{P}_n$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_q[X]$. Alors, $\mathcal{P}_n$ est non vide et*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P.$$

Démonstration. Soit A l'ensemble des facteurs irréductibles unitaires de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$, B l'ensemble des polynômes minimaux dans $\mathbb{F}_q[X]$ des éléments de $\mathbb{F}_{q^n}$, et C l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ dont le degré divise n. Montrons que $A = B = C$. En effet si $A = C$, puisque $X^{q^n} - X$ est à racines simples, c'est le produit de ses facteurs irréductibles unitaires. On aura donc

$$X^{q^n} - X = \prod_{P \in A} P = \prod_{P \in C} P = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P.$$

Montrons que $A \subset B \subset C \subset A$.

- $A \subset B$. Soit $P \in A$. Puisque $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$, alors P aussi. Il y a donc une racine $\alpha \in \mathbb{F}_{q^n}$. Puisque P est irréductible, P est le polynôme minimal de α.
- $B \subset C$. Soit $\alpha \in \mathbb{F}_{q^n}$ et $P \in \mathbb{F}_q[X]$ son polynôme minimal. Alors, P est irréductible. On a que $\mathbb{F}_q[\alpha] \cong \mathbb{F}_q[X]/\langle P \rangle$, donc $|\mathbb{F}_q[\alpha] = q^{\deg P}$. Or, $\mathbb{F}_q[\alpha]$ est un sous-corps de $\mathbb{F}_{q^n}$ donc $\deg P$ divise n. Ainsi $B \subset C$.
- $C \subset A$. Soit $P \in \mathbb{F}_q[X]$ un polynôme unitaire irréductible de degré d diviseur de n. Alors, $\mathbb{F}_q[X]/\langle P \rangle$ est un corps de cardinal q^d. Soit α l'image de X dans $\mathbb{F}_q[X]/\langle P \rangle$. Alors, $\alpha^{q^d} = \alpha$. Ainsi, P divise $X^{p^d} - X$ (puisque P est le polynôme minimal de α). Par le lemme de divisibilité, $X^{q^d} - X$ divise $X^{q^n} - X$. Ainsi, P est un diviseur irréductible de $X^{p^n} - X$. Ainsi, $P \in A$.

□

En regardant les degrés on obtient le résultat suivant.

Corollaire 5.3.1. *Soit $N_d = \operatorname{card} \mathcal{P}_d$ (le nombre de polynômes unitaires irréductibles de degré d dans $\mathbb{F}_q[X]$), où d divise n. Alors,*

$$p^n = \sum_{d|n} dN_d.$$

Corollaire 5.3.2. *Parmi les q^n polynômes unitaires de degré n, la proportition de polynômes irréductibles vérifie*

$$\frac{1 - q^{1-\frac{n}{2}}}{n} \leq \frac{N_n}{q^n} \leq \frac{1}{n}.$$

Démonstration. Remarquons que $q^n - q^{1-\frac{n}{7}2} \leq nN_n \leq q^n$. En effet, $nN_n \leq q^n$ car

$$q^n = nN_n + \sum_{\substack{d|n \\ d \neq n}} dN_d.$$

On observe plus généralement que pour tout d diviseur de n, $N_d \leq q^d/d$. Ainsi,

$$nN_n = q^n - \sum_{\substack{d|n \\ d\neq n}} dN_d \geq q^n - \sum_{\substack{d|n \\ d\neq n}} d\frac{q^d}{d} \geq \sum_{d\neq n/2} q^d \leq q^n - q^{1+\frac{n}{2}}.$$

□

Corollaire 5.3.3. *Le nombre moyen d'itération dans l'algorithme (q^n/N_n) est tel que*

$$\frac{q^n}{N_n} \leq \frac{n}{1-q^{1-\frac{n}{2}}}.$$

Si $n \geq 3$, alors

$$\frac{n}{1-q^{1-\frac{n}{2}}} \leq \frac{n}{1-\frac{1}{\sqrt{2}}}$$

et donc $q^n/N_n = \mathcal{O}(n)$.

5.4 Test d'irréductibilité de Rabin

Théorème 5.4.1. *Soit $P \in \mathbb{F}_q[X]$ de degré n. Alors, P est irréductible si et seulement si*

(i) P divise $X^{q^n} - X$;

(ii) pour tout facteur premier l de n, $P \wedge (X^{p^{n/l}} - X) = 1$.

Remarque. On ne peut pas travailler avec des polynômes de degré q^n en pratique (7^{1000} par exemple est trop grand). Le test de Rabin permet d'éviter ce problème.

— La première condition de l'équivalence est elle-même équivalente à demander que $X^{q^n} = X \mod P$. On travaille donc dans $\mathbb{F}_q[X]/\langle P\rangle$ et on utilise l'exponentiation rapide pour calculer $X^{q^n} \mod P$.

— On calcule $X^{q^{n/l}} - X \mod P$ et on se ramène à des polynômes de degré inférieur ou égal à n, dont on calcule un pgcd.

Démonstration. On peut supposer que P est unitaire. $\boxed{\Longrightarrow}$ Si $P \in \mathcal{P}_n$, c'est un diviseur de $X^{q^n} - X$ d'après la proposition clé. De plus, si l'on avait $P \wedge (X^{q^{n/l}} - X) \neq 1$, alors puisque P est irréductible, P divise $X^{q^{n/l}} - X$. Ainsi, $P \in \mathcal{P}_d$ donc d divise n/l, et alors $d < n$. Or, $P \in \mathcal{P}_n$ donc $\deg P = n$.

$\boxed{\Longleftarrow}$ Supposons que P satisfait les conditions (i) et (ii). Alors, P se décompose en facteurs irréductibles sous la forme $P = Q_1 \cdots Q_r$. Alors, les Q_i divisent P donc divisent $X^{p^n} - X$. Ainsi, $Q_i \in \mathcal{P}_{d_i}$ avec d_i un diviseur de n. Or, la condition (ii) assure que Q_i n'est pas dans $\mathcal{P}_d$ avec d diviseur de n/l. Puisque c'est vrai pour facteur premier l de n, on en déduit que la seule possibilité est que $Q_i \in \mathcal{P}_n$. Ainsi, $\deg Q_i = n$, et donc P n'a qu'un seul facteur : il est donc irréductible.

□

5.5 Polynômes cyclotomiques

5.5.1 Définition et lien avec les racines de l'unité dans les corps finis

Définition 5.5.1. *Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique le polynôme*

$$\varphi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

Remarques.

— À priori, $\varphi_n \in \mathbb{C}[X]$.

— Pour tout $n \in \mathbb{N}^*$, $\deg \Phi_n = \varphi(n)$, où φ est l'indicatrice d'Euler.

— Les polynômes cyclotomiques sont unitaires.

— Pour tout $n \in \mathbb{N}^*$,

$$\prod_{k=1}^{n} \left(X - e^{\frac{2ik\pi}{n}} \right) = X^n - 1.$$

Exemples.

— $\Phi_1 = X - 1$;

— $\Phi_2 = X + 1$;

— $\Phi_3 = X^2 + X + 1$;

— $\Phi_4 = X^2 + 1$;

— $\Phi_5 = X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}$.

Lemme 5.5.1. *Pour tout $n \in \mathbb{N}^*$,*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Démonstration. On partitionne les racines de l'unité en fonctions de leurs ordres. On a alors que $X^n - 1$ est le produit des $(X - \omega_d)$ où les ω_d sont les racines primitives d-ièmes de l'unité, où d parcourt les diviseurs de n, *i.e* que

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

□

Lemme 5.5.2. *Pour tout $n \in \mathbb{N}$, Φ_n est unitaire à coefficients entiers.*

Démonstration. Par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ est unitaire. Pour la propriété de récurrence, on écrit que

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n} \Phi_d}.$$

On fait donc la division euclidienne de X^n-1 par $P=\prod_{d|n}\Phi_d(X)$ (qui est un polynôme unitaire à coefficients entiers par hypothèse de récurrence). Le quotient est le reste sont donc dans $\mathbb{Z}[X]$. Dans $\mathbb{C}[X]$, la division euclidienne donne le même quotient et le même reste (par unicité de la division euclidienne dans $\mathbb{C}[X]$). Or, dans $\mathbb{C}[X]$, le quotient est Φ_n et le reste est nul. Ainsi, $\Phi_n \in \mathbb{Z}[X]$. □

Proposition 5.5.1. *Soit $n \in \mathbb{N}^*$ et $\mathbb{K}$ un corps de caractéristique 0 ou $p>0$ tel que $p \wedge n = 1$. Alors, les racines de Φ_n dans $\mathbb{K}$ sont exactement les racines primitives n-ièmes de l'unité dans $\mathbb{K}$.*

Démonstration. Toute racine de Φ_n est une racine n-ième de l'unité car Φ_n divise X^n-1. Soit alors α une racine n-ième de l'unité dans $\mathbb{K}$. Alors, $\alpha^n-1=0$ donc

$$\prod_{d|n}\Phi_d(\alpha)=0.$$

Ainsi, α annule un certain Φ_d où d divise n. Si $d<n$, alors α est une racine d-ième de l'unité (ce qui est impossible puisque α est une racine primitive). Ainsi, α est une racine de Φ_n. Supposons désormais α être une racine de Φ_n. C'est donc une racine n-ième de l'unité et il existe d un diviseur de n tel que $\alpha^d=1$. Supposons qu'on puisse trouver un tel d tel que $d<n$. Alors, α est une racine $X^d-1=\prod_{d'|d}\Phi_{d'}$. Ainsi, α est une racine d'un certain $\Phi_{d'}$ où d' est un diviseur de d. Alors, α est une racine double de X^n-1 et donc une racine de Φ_n et $\Phi_{d'}$. Or,

$$X^n-1=\Phi_n\prod_{\substack{d|n\\ d\neq n}}\Phi_d.$$

Mais $f(X):=X^n-1$ est à racine simples dans $\mathbb{K}$ car $f'(X)=nX^{n-1}$ avec $n\neq 0$ dans $\mathbb{K}$ (car si $\mathbb{K}$ est de caractéristique non nulle $p>0$, on a supposé que $n^p=1$). Ainsi, f' ne s'annule qu'en 0, il n'a donc que des racines simples.

□

Remarque. On a que

5.5.2 Irréductibilité des polynômes cyclotomiques dans $\mathbb{Q}[X]$

Théorème 5.5.1. *Pour tout $n\geq 1$, Φ_n est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.*

Définition 5.5.2. *On appelle contenu d'un polynôme de $\mathbb{Z}[X]$ le pgcd de ses coefficients.*

Notation. Si $P\in\mathbb{Z}[X]$, on note son contenu $c(P)$.

Remarque. Cette notion est généralisable aux anneaux factoriels, mais le définir sur $\mathbb{Z}$ suffira ici.

Lemme 5.5.3. *Soient P et $Q\in\mathbb{Z}[X]$. Alors $c(PQ)=c(P)c(Q)$.*

Démonstration. Posons $P_1 = \dfrac{1}{c(P)}P$ et $Q_1 = \dfrac{1}{c(Q)}Q$. Supposons par l'absurde que $c(P_1Q_1) \neq 1$. Il existe alors p premier divisant $c(P_1Q_1)$, donc tous les coefficients. On a alors dans $(\mathbb{Z}/p\mathbb{Z})[X]$ que

$$\overline{P_1Q_1} = \bar{P}_1\,\bar{Q}_1 = \bar{0}.$$

Par intégrité, p divise tous les coefficients de P_1 ou de Q_1. Alors p diviserait le contenu d'un des deux polynômes. p divise 1, ce qui est absurde. Ainsi, $c(P_1Q_1) = 1$. D'où

$$c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q).$$

□

Lemme 5.5.4. *Si $f \in \mathbb{Z}[X]$ est un produit de deux polynômes unitaires $P, Q \in \mathbb{Q}[X]$, alors P et Q sont à coefficients entiers.*

Démonstration. On écrit $P(X) = \sum_{i=0}^{n} \frac{\alpha_i}{\beta_i}X^i$ et $Q(X) = \sum_{j=0}^{m} \frac{\gamma_j}{\delta_j}X^j$ en supposant les fractions irréductibles. On note $\beta = \operatorname{ppcm}(\beta_1, \ldots, \beta_n)$ et $\delta = \operatorname{ppcm}(\delta_1, \ldots, \delta_m)$. Par le lemme de Gauss,

$$c(\beta P \delta Q) = c(\beta P)c(\delta Q)$$

Montrons que $c(\beta P) = 1$. On a que $\beta P = \displaystyle\sum_{i=0}^{n} \alpha_i \frac{\beta}{\beta_i}$ et

$$c(\beta P) = \bigwedge_{i=0}^{n} \left(\frac{\alpha_i}{\beta_i} \bigvee_{j=0}^{n} \beta_j \right).$$

Supposons par l'absurde qu'il existe p premier divisant $c(\beta P)$. Ainsi,

$$\forall i \in [\![0, n]\!],\ p \mid \alpha_i \frac{\beta}{\beta_i}$$

Ainsi, $p \mid \alpha_n \frac{\beta}{\beta_n}$ donc $p \mid \beta$. Posons $A = \{v_p(\beta_k) \mid k \in [\![0, n]\!]\}$. C'est une partie non vide de $\mathbb{N}$ majorée, elle admet donc un maximum noté $v_p(\beta_k)$ (puisqu'un tel k existe). Par définition de β et de k, on sait que $v_p(\beta_k) = v_p(\beta)$ donc

$$v_p\left(\frac{\beta}{\beta_k}\right) = 0.$$

Il en découle que p ne divise pas $\dfrac{\beta}{\beta_k}$, p divise donc a_k. Enfin, p divise a_k et β_k avec $a_k \wedge \beta_k = 1$. Nécessairement, $p = 1$.

□

Démonstration (du théorème). On montre uniquement l'irréductibilité dans $\mathbb{Q}[X]$, l'irréductibilité dans $\mathbb{Z}[X]$ en sera une conséquence. Soit P un facteur irréductible unitaire de Φ_n dans $\mathbb{Q}[X]$. Selon le lemme précédent, il est à coefficients entier. Soit désormais $\zeta \in \mathbb{C}$ une racine de P et p un nombre premier ne divisant pas n. Montrons que ζ^p est aussi racine de P. Écrivons $\Phi_n = PQ$. Supposons que P ne s'annule pas ζ^p, c'est donc que Q s'y annule puisque Φ_n s'y annule. Ainsi, $Q(\zeta^p) = 0$ et ζ est une racine de $Q(X^p)$. Puisque P est irréductible et s'annule en ζ, c'est le polynôme minimal de ζ donc P divise $Q(X^p)$ dans $\mathbb{Q}[X]$. Selon le lemme précédent, il existe $R \in \mathbb{Z}[X]$ tel que $PR = Q(X^p)$. On trouve alors dans $\mathbb{F}_p[X]$ que $\bar{P}\bar{R} = \bar{Q}(X^p) = \bar{Q}^p$, et $\bar{\Phi}_n = \bar{P}\bar{Q}$. Mais puisque Φ_n est à racines simples dans toutes extension de $\mathbb{Z}/p\mathbb{Z}$ (c'est un diviseur de $X^n - 1$ et $n \wedge p = 1$), $\bar{P}$ et $\bar{Q}$ sont premiers entre eux, ce qui est contradictoire puisque $\bar{P}\bar{R} = \bar{Q}^p$.

On a donc montré que si $\zeta \in \mathbb{C}$ est une racine de P, alors ζ^p aussi pour tout p premier ne divisant pas n. Soit donc $\zeta \in \mathbb{C}$ une racine de P et ζ' une racine primitive n-ième de l'unité. Nous savons qu'il existe $\bar{m} \in \mathbb{Z}/n\mathbb{Z}^\times$ tel que $\zeta' = \zeta^m$. On décompose m en facteurs premiers avec $m = p_1 \cdots p_k$ (pas forcément distinces). Les p_i ne divisent pas n, car si c'était le cas alors ζ^{p_i} est une racine n/p_i-ième de l'unité, ce qui contredit sa primalité. Soit alors $\zeta_1 = \zeta^{p_1}$. On applique le résultat que l'on a montré pour affirmer que $\zeta_1^{p_2}$ est encore une racine de P. En itérant ce processus, on observe que ζ' est racine de P. Ainsi, toutes les racines primitives n-ièmes de l'unité sont racines de P donc P divise Φ_n, et alors $P = \Phi_n$.

□

Remarque. Le programme du premier contrôle continu s'arrête ici.

On termine cette sous-section avec un résultat admis.

Proposition 5.5.2. *Soit $q = p^s$ avec p un entier premier et $s \geq 1$. Soit n un entier premier avec p. Alors, Φ_n est irréductible dans $\mathbb{F}_q[X]$ si et seulement si la classe de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ engendre ce groupe.*

5.5.3 Construction des corps finis *via* la factorisation des polynômes cyclotomiques

Les polynômes cyclotomiques permettent de construire les corps finis et de produire un générateur pour chaque groupe des inversibles d'un corps. En effet si $q = p^r$, il nous suffit de construire une extension de $\mathbb{F}_p$ contenant une racine primitive $(p^r - 1)$-ième de l'unité. On choisit donc pour cela P un facteur irréductible de Φ_{p^r-1} de degré r et alors $\mathbb{F}_q \cong \mathbb{F}_p[X]/\langle P \rangle$. Évidemment, cela demande de savoir factoriser Φ_{p^r-1} en facteurs irréductibles dans $\mathbb{Z}[X]$. Pour cela, on peut utiliser l'algorithme de Berkelamp ou celui de Cantor-Zassenhaus pour factoriser des polynômes à coefficients dans un corps fini.

5.6 Algorithme de Berkelamp

Nous donnons ici la description d'un algorithme qui, étant donné un polynôme de $\mathbb{F}_p[X]$ le factorise [2]. Tout d'abord, on peut supposer P sans facteur multiple. Si ce n'est pas le cas alors soit $P' = 0$ et P est de la forme $P = Q(X^p)$ et l'on étudie la factorisation de Q, soit $P \wedge P'$ est non constant de degré strictement plus petit que $\deg P$ et suffit de factoriser $P \wedge P'$ et $P/(P \wedge P')$ (qui sont tous de degré strictement inférieur à $\deg P$).

5.6.1 Version déterministe

Soit $P \in \mathbb{F}_p[X]$ un polynôme sans facteur multiple, et on note $P = P_1 \cdots P_r$ sa décomposition. Par le lemme chinois,

$$\mathbb{F}_p[X]/\langle P \rangle \cong \prod_{i=1}^{r} \mathbb{F}_p[X]/\langle P_i \rangle.$$

L'application $\varphi : x \longmapsto x^p$ est $\mathbb{F}_p$-linéaire et a exactement p points fixes formant une droite dans des facteurs. Ainsi, $N := \ker(\varphi - \mathrm{id})$ est de dimension r. On détermine *via* un pivot de Gauss une base du noyau N. S'il est de dimension 1, c'est que P est irréductible. Plus généralement, N contient l'image des constantes dans $\mathbb{F}_p[X]/\langle P \rangle$. Soit $Q \in \mathbb{F}_[X]$ un polynôme non constant de tel que $\bar{Q} \in N$, *i.e* que l'image de P dans chacun des $\mathbb{F}_p[X]/\langle P_i \rangle$ est constante (ce sont les points

2. On peut même généraliser un tel processus à $\mathbb{F}_q[X]$

fixes du morphisme de Frobenius). Ainsi, il existe $\alpha_i \in \mathbb{F}_p$ tel que P_i divise $Q - \alpha_i$. Or, Q étant non constant, la constante α_i n'est pas indépendante de $i \in [\![1, r]\!]$. Ainsi, certains P_j divisent $Q - \alpha_i$ mais pas tous. Ainsi, $P \wedge (Q - \alpha)$ donne un facteur strict de P lorsque α est un α_i.

On arrive au défaut de l'algorithme, qui est qu'on ne connait pas les P_i et donc encore moins les α_i. On calcule donc $P \wedge (Q - \alpha)$ pour tout $\alpha \in \mathbb{F}_p$, jusqu'à trouver un facteur strict de P.

5.6.2 Version randomisée

La méthode déterministe est efficace uniquement lorsque p est petit, puisqu'on doit effectuer des calculs en parcourant le corps $\mathbb{F}_p$. Si p est grand, on doit trouver un moyen pour ne pas avoir à tester tous les α. Afin d'optimiser le nombre de calculs, on utilise le fait que $\alpha_i^{\frac{p-1}{2}} \in \{-1, 0, 1\}$, puisque α_i est dans le sous-corps premier de $\mathbb{F}_p[X]/\langle P_i \rangle$. Soit alors $Q \in \mathbb{F}_p[X]$ tel que $\bar{Q} \in N$. Alors, l'image de $Q^{\frac{p-1}{2}}$ est égale à 0 ou ± 1. On a donc que P_i divise soit $Q^{\frac{p-1}{2}} - 1$, ou $Q^{\frac{p-1}{2}}$, ou alors $Q^{\frac{p-1}{2}} + 1$ (selon que $\alpha_i = 0$, ou que $\alpha_i \neq 0$ est un carré ou non). On en déduit que $P \wedge (Q^{\frac{p-1}{2}} - 1)$ vaut P (*resp.* 1) *si et seulement si* tous les (*resp.*aucun des) α_i ne vérifient $\alpha_i^{\frac{p-1}{2}} = 1$. On a donc découpé les possibilités sur $[\![1, r]\!]$ en trois tiers (de tailles respectives $\frac{p-1}{2}$, $\frac{p-1}{2}$, et 1 (tous inférieurs ou égaux à $p/2$)). On choisit alors Q au hasard, et la probabilité qu'une situation arrive est au plus la probabilité de tirer $r-1$ nombres dans le même tiers, *i.e* inférieure à $1/2^{r-1} \leq 1/2$ (lorsque $r > 1$).

5.6.3 Algorithme de Cantor-Zassenhaus

On termine cette section sur les algorithmes de décomposition en facteurs premiers avec une version simplifiée de la méthode randomisée dans laquelle nous n'avions pas besoin de connaître le noyau N. On suppose ici p impair et que tous les facteurs irréductibles de P ont le même degré d que l'on suppose connu. C'est un cas auquel on peut facilement se ramener puisque l'on sait que $X^{p^k} - X$ a comme facteurs irréductibles les polynômes de degré diviseur de k. On calcule les pgcd de P et $X^{p^i} - X$ pour i croissant, mais on retire à chaque étape à P les facteurs communs trouvés, et on recommence avec le i suivant. Une fois donc ramené au cas décrit, on a que

$$\mathbb{F}_p[X]/\langle P \rangle \cong \prod_{i=1}^{r} \mathbb{F}_p[X]/\langle P_i \rangle$$

est un produit de corps de même cardinaux (p^d). L'argument que nous avons donné plus haut dans $\mathbb{F}_p$ s'adapte : tout élément $\bar{Q} \in \mathbb{F}_p[X]/P_i$ élevé à la puissance $(p^d - 1)/2$ devient 0 ou ± 1. On en déduit donc que P_i divise soit $Q^{\frac{p^d-1}{2}} - 1$, soit $Q^{\frac{p^d-1}{2}}$, soit $Q^{\frac{p^d-1}{2}} + 1$. On choisit alors Q au hasard (de degré inférieur ou égal à $2d$ suffit même), et la probabilité que tous les P_i divisent le même polynôme (parmi les trois) est la probabilité que l'image de Q soit dans même tiers pour tout i, ce qui est au plus une chance sur 2 si $r \geq 2$ (*i.e* s'il y a plusieurs facteurs).

Chapitre 6

Réciprocité quadratique

Étant donné a un entier et p un nombre premier impair, peut-on donner une condition nécessaire et suffisante pour a soit un carré modulo p. Une réponse a déjà été démontré dans ce cours : a est un carré modulo p *si et seulement si* $a^{\frac{p-1}{2}} \equiv 0$ ou $1 \mod p$ (conséquence de la cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$). Si l'on se donne maintenant $a \in \mathbb{Z}$, peut-on déterminer les entiers premiers p impairs tel que a est un carré modulo p. Malheureusement, le critère précédent ne suffit pas.

6.1 Symbole de Legendre

Définition 6.1.1. *Soit p un nombre premier impair, et $a \in \mathbb{Z}$. On définit le symbole de* Legendre *par*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \mod p\,; \\ 1 & \text{si } a \text{ est un carré modulo } p\,; \\ -1 & \text{sinon.} \end{cases}$$

Remarque. Cette quantité ne dépend que de la classe de a modulo p. On peut donc définir $\left(\frac{a}{p}\right)$ pour $a \in \mathbb{Z}/p\mathbb{Z}$.

Lemme 6.1.1. *Soit p un nombre premier impair et $a \in \mathbb{Z}/p\mathbb{Z}$. Alors dans $\mathbb{Z}/p\mathbb{Z}$,*

$$\left(\frac{a}{b}\right) \equiv a^{\frac{p-1}{2}}.$$

Ce lemme a déjà été démontré.

Corollaire 6.1.1. *Soit p un nombre premier impair. Les assertions suivantes sont équivalentes.*

(i) -1 *est un carré modulo p ;*
(ii) $\frac{p-1}{2}$ *est un pair ;*
(iii) $p \equiv 1 \mod 4$.

Exemple. -1 est nu carré modulo 13 mais pas modulo 11.

On présente maintenant le résultat majeur de ce chapitre.

Théorème 6.1.1 (lois de réciprocité quadratique pour le symbole de LEGENDRE)**.** *Soit p un nombre premier impair. On a les résultats suivants.*

(i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *(le symbole de* LEGENDRE *vaut* 1 *si et seulement si* $p \equiv 1 \mod 4$*).*

(ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *(le symbole de* LEGENDRE *vaut* 1 *si et seulement si* $p \equiv \pm 1 \mod 8$*).*

(iii) Soient p et q deux nombres premiers impairs distincts. Alors,

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

Remarque. Les deux premières sont des lois complémentaires. Le point *(iii)* est ce qu'on appelle généralement la *loi de réciprocité quadratique*. Nous démontrerons ces résultats plus tard.

6.2 Application de la réciprocité quadratique, symbole de JACOBI

Définition 6.2.1. *Soit $n \geq 3$ un entier impair qu'on décompose en facteurs premiers avec $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On définit le symbole de* JACOBI *par*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Remarque. Dans le membre de droite, le symbole est celui de LEGENDRE que nous avons déjà défini.

Attention. Si n n'est pas premier, $\left(\frac{a}{n}\right) = \pm 1$ ne signifie pas nécessairement que a est un carré modulo n ou non. Ce symbole va en revanche nous servir dans des calculs intermédiaires à déterminer si a est un carré modulo p.

Proposition 6.2.1 (propriétés du symbole de JACOBI)**.** *Soit $n \geq 3$ un entier impair.*

(i) Si $a \equiv b \mod n$, alors

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

(ii) Si $a \in \mathbb{Z}$,

$$\left(\frac{a}{n}\right) = 0 \iff a \wedge n \neq 1.$$

(iii) Pour tout $a, b \in \mathbb{Z}$,

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

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

(*i*) Si $a \equiv b \mod n$, alors $a \equiv b \mod p_i$ pour tout $i \in [\![1, r]\!]$. Ainsi,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{r} \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{n}\right).$$

(*ii*) On a que

$$\left(\frac{a}{n}\right) = 0 \iff \exists i \in [\![1, r]\!], \left(\frac{a}{p_i}\right) = 0 \iff a \wedge n = 1.$$

(*iii*) Découle du fait que pour tout $i \in [\![1, r]\!]$

$$\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right),$$

et

$$\left(\frac{ab}{p_i}\right) = (ab)^{\frac{p_i-1}{2}} = a^{\frac{p_i-1}{2}} b^{\frac{p_i-1}{2}}.$$

□

Théorème 6.2.1 (lois de réciprocité quadratique pour le symbole de Jacobi)**.** *Soit $m, n \geq 3$ deux entiers impairs premiers entre eux. On a les résultats suivants.*

(i) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

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

(iii) Soient p et q deux nombres premiers impairs distincts. Alors,

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

Remarque. Comme pour le symbole de Legendre, la propriété (*iii*) est ce qu'on appelle généralement la loi de réciprocité quadratique.

Démonstration. (*i*) Notons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Selon, la première première loi de réciprocité quadratique,

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{r} \left((-1)^{\frac{p_i-1}{2}}\right)^{\alpha_i} = (-1)^{\frac{n-1}{2}}.$$

En effet, l'application $\varepsilon : x \longmapsto (-1)^{\frac{x-1}{2}}$ est mutiplicative sur l'ensemble des entiers impairs (c'est la classe de x modulo 4 qui vaut ± 1).

(*ii*) La démonstration est la même avec $\omega : x \longmapsto (-1)^{\frac{x^2-1}{8}}$, qui est aussi multiplicative sur l'ensemble des entiers impairs (c'est la classe modulo 8).

(*iii*) On a que

$$(-1)^{\frac{n-1}{2}}(-1)^{\frac{m-1}{2}} = \left(\frac{\varepsilon(n)}{m}\right).$$

Il suffit donc de voir que

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \left(\frac{\varepsilon(n)}{m}\right) \iff \left(\frac{n\varepsilon n}{m}\right) = \left(\frac{m}{n}\right).$$

Notons donc $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $m = q_1^{\beta_1} \cdots q_r^{\beta_r}$. Alors,

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{q_i^{\beta_i}}{p_j^{\alpha_j}}\right) = \prod_{i,j} \left(\frac{q_i}{p_j}\right)^{\beta_j \alpha_j}.$$

Par loi de réciprocité quadratique,

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_j \varepsilon(p_j)}{q_i}\right)^{\beta_j \alpha_j} = \prod_{i,j} \left(\frac{p_j^{\alpha_j} \varepsilon\left(p_j^{\alpha_j}\right)}{q_i^{\beta_i}}\right) = \left(\frac{n\varepsilon(n)}{m}\right).$$

□