Université Bordeaux I

Master CSI

Année 2004-2005

UE Arithmétique I

Christine Bachoc

Bibliography

[1] Cohen Arjeh M., ..*Algebra interactive*

[2] Kobliz Neal, *A course in number theory and cryptography*, Springer, 1987

[3] Lang Serge, *Algebra*

Chapter 1

Introduction

Ce cours comprend deux parties. Un premier chapitre traite des extensions de corps, en particulier des extensions algébriques et de leur manipulation algorithmique, en insistant sur le cas des corps finis. Un deuxième chapitre introduit la notion de modules, et étudie l'algorithmique des réseaux, qui sont les sous-$\mathbb{Z}$-modules de $\mathbb{R}^n$. En particulier, on discute l'algorithme LLL et ses applications.

Chapter 2

Corps

2.1 Rappels

Dans cette partie, on rappelle des notions essentielles pour la suite vues en Licence, et qui doivent être parfaitement connues et maîtrisées.

2.1.1 Quelques définitions

On rappelle ici quelques notions vues en Licence et qui doivent être parfaitement connues.

Un anneau est un triplet $(A, +, \times)$ où A est un ensemble, $+$ et $\times$ sont deux lois internes appelées addition et multiplication. $(A, +)$ est un groupe commutatif de neutre noté 0; la loi $\times$ possède un neutre noté 1 (d'autres auteurs disent que l'anneau est unitaire). Elle est associative et distributive sur l'addition (et on omet en général l'écriture du signe $\times$: $x \times y = xy$). On dit que l'anneau est commutatif si la multiplication est commutative.

Exemple: Voici des exemples classiques d'anneaux: $\mathbb{Z}/n\mathbb{Z}$, $M_n(A)$ les matrices $n \times n$ à coefficients dans un anneau A, l'anneau des polynômes $A[X]$.

Le groupe des unités A^* de l'anneau A est l'ensemble des éléments inversibles de A, c'est-à-dire l'ensemble des éléments x de A pour lesquels il existe $y \in A$ tel que $xy = yx = 1$. Comme son nom l'indique, c'est un groupe pour la multiplication.

Un élément x de A est appelé un diviseur de zéro s'il existe $y \in A \setminus \{0\}$ tel que $xy = 0$. Un anneau sans diviseur de zéro est appelé un anneau intègre.

Exercice: Décrire A^* dans les exemples précédents.

Définition 1 *Un corps K est un anneau commutatif dont tout élément non nul est inversible. Autrement dit, $K^* = K \setminus \{0\}$.*

Exemple: Les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ des nombres rationnels, réels, complexes. Les résultats suivants ont été vus en Licence: $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier et, si K est lui-même un corps, $K[X]/P(X)K[X]$ est un corps si et seulement si $P(X)$ est un polynôme irréductible.

2.1.2 Quelques constructions

Les lois seront toujours notées $+$ et $\times$ et par conséquent omises dans les notations. Ainsi, on remplace la notation $(L, +, \times)$ par son abrégé: L.

Définition 2 *Soit L un corps. Un sous-ensemble $K \subset L$ de L est appelé un sous-corps de L s'il est un corps pour les mêmes lois que celles de L. On dit aussi que L est une extension de K et on la note L/K.*

Remarque: Quand on manipule des extensions, il faut toujours préciser quels sont les deux corps dont on parle. Par exemple, $\mathbb{C}$ est une extension de $\mathbb{R}$ mais aussi de $\mathbb{Q}$. Dans l'extension L/K, K est appelé le corps de base.

Les propositions suivantes donnent des méthodes pour construire des corps:

Proposition 1 *Soit L un corps et K_1, K_2 deux sous-corps de L.*

- *L'intersection $K_1 \cap K_2$ est encore un sous-corps de L.*
- *Le compositum K_1K_2 de K_1 et K_2 est par définition le plus petit sous-corps de L qui contient K_1 et K_2. On a:*

$$K_1K_2 = \{\frac{s_1}{s_2} \mid s_i = \sum_{\text{finies}} xy, x \in K_1, y \in K_2 \text{ et } s_2 \neq 0\}.$$

Remarque: La notion de compositum de deux corps est un peu subtile. Attention aux erreurs classiques: la réunion de deux corps n'est pas en général un corps; l'ensemble des produits $\{xy \mid x \in K_1, y \in K_2\}$ non plus! Un exemple à avoir en tête est celui des fractions rationnelles: si $L = K(X, Y)$, prenons $K_1 = K(X)$ et $K_2 = K(Y)$. Alors $K_1K_2 = L$. On se convainc facilement que $K_1 \cup K_2$ n'est pas un corps, ni même l'ensemble des produits!

Une autre construction importante est celle du corps des fractions d'un anneau intègre. On en donne ici une définition informelle.

Définition 3 *Soit A un anneau intègre. Le corps des fractions de A, noté $Fr(A)$ est le plus petit corps contenant A. C'est l'ensemble*

$$Fr(A) = \{\frac{a}{b} \mid a \in A, b \in A \setminus \{0\}\}.$$

Exercice: Expliquez pourquoi cette construction ne marche pas si A n'est pas intègre.

Exercice: Quel est le corps de fractions de $\mathbb{Z}$? de $K[X]$?

2.1.3 La caractéristique

On définit la caractéristique d'un anneau A de neutre 1 de la façon suivante: l'application

$$\begin{aligned} \phi : \mathbb{Z} &\to A \\ n &\mapsto n.1 \end{aligned}$$

où $n.1 = 1 + 1 + \cdots + 1$ avec n termes si n est positif et $n.1 = (-1) + (-1) + \cdots + (-1)$ avec $-n$ termes si n est négatif, est un homomorphisme d'anneaux. Son noyau, qui est un idéal de $\mathbb{Z}$, est donc de la forme: $\ker \phi = c\mathbb{Z}$ où c est un entier positif.

Définition 4 *Ce nombre c est appelé la caractéristique de A, et est noté $\mathrm{car}(A)$. C'est le plus petit entier non nul tel que $c.1 = 0$, s'il existe. Si $c.1 \neq 0$ sauf pour $c = 0$, la caractéristique de A est égale à 0.*

Remarque: Si $\mathrm{car}(A) = 0$, alors l'homomorphisme ϕ est injectif, et l'anneau A contient un sous-anneau isomorphe à $\mathbb{Z}$. En particulier, l'anneau A est infini. La réciproque bien sûr est fausse: $\mathbb{Z}/2\mathbb{Z}[X]$ est un anneau infini de caractéristique 2. Si $\mathrm{car}(A) = c > 0$, l'anneau A contient un sous-anneau isomorphe à $\mathbb{Z}/c\mathbb{Z}$. Comme $\mathbb{Z}/c\mathbb{Z}$ n'est intègre que si c est un nombre premier, la carcatéristique d'un anneau intègre et donc en particulier d'un corps est nécessairement un nombre premier. Ainsi, on a:

Proposition 2 *Soit K un corps. La caractéristique de K est égale à 0 si et seulement si K contient un sous-corps isomorphe à $\mathbb{Q}$. Sinon, la caractéristique de K est un nombre premier p et K contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Ce sous-corps est appelé sous-corps premier de K.*

Si L/K est une extensions de corps, ils ont même caractéristique et même sous-corps premier.

2.1.4 Polynômes irréductibles

Soit $K[X]$ l'anneau des polynômes à coefficients dans le corps K. On rappelle que c'est un anneau euclidien, tout comme l'anneau $\mathbb{Z}$, et que par conséquent ces deux anneaux ont des propriétés très similaires. En particulier, la notion de polynôme irréductible est l'analogue de celle de nombre premier.

Définition 5 *Un polynôme $P(X) \in K[X]$ est appelé polynôme irréductible s'il est de degré au moins égal à 1 et s'il ne peut pas s'écrire $P(X) = A(X)B(X)$ où $A(X)$ et $B(X)$ sont des polynômes non constants.*

Remarque: On exclut dans la définition des polynômes irréductibles les polynômes de degré 0 car ce sont les inversibles de $K[X]$ ($K[X]^* = K^*$). De même on peut toujours écrire $P(X) = (\lambda)(\lambda^{-1}P(X))$ mais cela ne compte pas comme une décomposition de $P(X)$.

Remarque: Quand on discute de l'irréductibilité d'un polynôme, il est essentiel de préciser sur quel corps on se place. Ainsi, le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$!

Exercice: Trouvez tous les polynômes irréductibles de degré au plus 3 sur $\mathbb{F}_2$.

Remarque: Irréductibilité et racines: Si un polynôme $P(X)$ a une racine α dans K, alors il est divisible par $X - \alpha$. Il ne peut donc être irréductible sur K, sauf s'il est de degré 1. La réciproque est fausse: il ne suffit pas qu'un polynôme n'ait pas de racines dans K pour qu'il soit irréductible, sauf s'il est de degré au plus 3.

Un résultat essentiel, comme dans $\mathbb{Z}$, est la décomposition en produit d'irréductibles. Pour qu'elle soit unique, on se restreint aux polynômes irréductibles unitaires (voir la remarque précédente).

Théorème 1 *Tout polynôme $P(X)$ s'écrit de façon unique à l'ordre près des P_i:*

$$P(X) = \lambda P_1(X)^{n_1} \dots P_r(X)^{n_r}$$

où les P_i sont des polynômes irréductibles unitaires, deux à deux distincts, $\lambda \in K$ et $n_i \in \mathbb{N}$.

Comme dans $\mathbb{Z}$, on définit la notion de PGCD, PPCM (que l'on prend unitaires pour qu'ils soient uniques), et on a le théorème de Bezout:

Théorème 2 *Si $D(X) = PGCD(P(X), Q(X))$, il existe des polynômes U(X),V(X) tels que:*

$$D(X) = U(X)P(X) + V(X)Q(X).$$

De plus les polynômes $D(X)$, $U(X)$, $V(X)$ se calculent par l'algorithme d'Euclide.

2.1.5 Le quotient $K[X]/P(X)K[X]$

La construction générale du quotient d'un anneau par un idéal de cet anneau s'applique à l'anneau $K[X]$ et à l'idéal principal $P(X)K[X]$ qui est l'ensemble des multiples de $P(X)$. La surjection canonique

$$s : K[X] \to K[X]/P(X)K[X]$$

a pour noyau $\ker s = P(X)K[X]$.En supposant que le polynôme P est non constant, on voit que la restriction de s à K est injective. On peut donc identifier K et $s(K)$. Notons $x = s(X)$. On a donc les propriétés importantes suivantes:

- $P(x) = 0$.
- Si $Q(x) = 0$ alors $P(X)$ divise $Q(X)$.

Proposition 3 *Soit $A = K[X]/P(X)K[X]$. On pose $d = \deg(P)$.*

1. $\mathrm{car}(A) = \mathrm{car}(K)$.
2. *Tout élément y de A s'écrit de façon unique $y = a_0 + a_1x + a_2x + \ldots a_{d-1}x^{d-1}$.*
3. *Avec les notations précédentes, y est inversible si et seulement si le polynôme $a_0 + a_1X + a_2X + \ldots a_{d-1}X^{d-1}$ est premier à $P(X)$.*
4. *A est un corps si et seulement si $P(X)$ est irréductible.*

Remarque: Notons $y = Q(x) \in A$. Ainsi, pour savoir si y est inversible dans A, il suffit de calculer le pgcd de Q et P. De plus, le théorème de Bezout et l'algorithme d'Euclide fournissent une méthode algorithmique pour calculer effectivement l'inverse de y sous la forme (2). En effet, si U et V sont tels que $1 = U(X)P(X) + V(X)Q(X)$, alors on a dans A la relation: $1 = V(x)Q(x)$ (puisque $P(x) = 0$). L'inverse de y est donc égal à $V(x)$.

2.2 Extensions algébriques

À partir de maintenant, on fait des démonstrations...

2.2.1 Degré d'une extension

Soit L/K une extension de corps. Alors L est aussi un espace vectoriel sur K! En effet, puisqu'on peut multiplier entre eux les éléments de K et ceux de L, cette multiplication définit la loi externe d'espaces vectoriels. Ce point de vue est très important pour l'étude des extensions.
Exemple: Le corps $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2. Une base est $(1, i)$. Le corps $\mathbb{C}$ est aussi un $\mathbb{Q}$-espace vectoriel, cette fois-ci de dimension infinie (car il est non dénombrable..).

Exemple: Le corps des fractions rationnelles $K(X)$ est un K-espace vectoriel de dimension infinie.

Exemple: Si $L = K[X]/P(X)K[X]$, et si P est de degré d, L est un K-espace vectoriel de base $(1, x, \ldots, x^{d-1})$ (c'est exactement ce que dit la Proposition 3).

Définition 6 *Soit L/K une extension de corps. On appelle degré de l'extension, et on note $[L : K]$, la dimension de L comme K-espace vectoriel ($[L : K] = \infty$ si cette dimension est infinie).*

Exemple: $[\mathbb{C} : \mathbb{R}] = 2$.

Proposition 4 *Soit $K \subset M \subset L$. Supposons que l'extension L/K soit de degré fini. Alors les extensions L/M et M/K sont de degrés finis, et on a: $[L : K] = [L : M][M : K]$.*

Preuve: M est un K-sous-espace vectoriel de L. Si L est de dimension finie sur K, a fortiori M aussi. Une base de L sur K est une famille génératrice de L sur M; L est donc aussi de dimension finie sur M.

Soit maintenant $(e_1, \ldots, e_r)$ une base de L sur M et soit $(f_1, \ldots, f_s)$ une base de M sur K. Nous allons montrer que l'ensemble des $e_i f_j$ avec $1 \leq i \leq r$ et $1 \leq j \leq s$ est une base de L sur K. Cela fait bien rs élément, ce qui démontre la proposition.

Montrons que c'est une famille génératrice de L sur K: soit $x \in L$. Par définition des e_i, il existe $\lambda_i \in M$ tels que

$$x = \sum_{i=1}^{r} \lambda_i e_i.$$

Comme les λ_i appartiennent à M, par définition des f_j, il existe des $\mu_{i,j} \in K$ tels que

$$\lambda_i = \sum_{j=1}^{s} \mu_{i,j} f_j.$$

Finalement, on a:

$$x = \sum_{i,j} \mu_{i,j} e_i f_j$$

et les $\mu_{i,j}$ étant dans K, cela montre bien que la famille des $e_i f_j$ est génératrice de L sur K.

Pour montrer que ces éléments sont libres sur K, partons d'une combinaison linéaire nulle

$$\sum_{i,j} \mu_{i,j} e_i f_j = 0$$

que l'on peut écrire

$$\sum_i (\sum_j \mu_{i,j} f_j) e_i = 0.$$

On utilise le fait que les e_i sont libres sur M pour conclure que, pour tout $1 \leq i \leq r$,

$$\sum_j \mu_{i,j} f_j = 0,$$

puis que les f_j sont libres sur K pour obtenir que $\mu_{i,j} = 0$ pour tout $1 \leq i \leq r$ et tout $1 \leq j \leq s$.

□

2.2.2 Élément algébrique, extension algébrique

Soit L/K une extension de corps.

Définition 7 *Un élément α de L est dit algébrique sur K s'il existe un polynôme $P(X) \in K[X]$ non nul tel que $P(\alpha) = 0$. Si α n'est pas algébrique, on dit qu'il est transcendant.*

Si tout élément de L est algébrique sur K, on dit que l'extension L/K est algébrique.

Exemple: Si $\alpha \in K$, il est algébrique sur K puisque racine du polynôme $X - \alpha \in K[X]$!

Exemple: Les éléments i, $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$ car racine respectivement des polynômes $X^2 + 1$ et $X^2 - 2$.

Si $z \in \mathbb{C}$, le polynôme $(X - z)(X - \overline{z})$ est à coefficients réels. Cela montre que tout nombre complexe est algébrique sur $\mathbb{R}$, et que l'extension $\mathbb{C}/\mathbb{R}$ est algébrique. Par contre, l'extension $\mathbb{C}/\mathbb{Q}$ n'est pas algébrique (on peut montrer que si elle l'était, $\mathbb{C}$ serait dénombrable). Cette argument de dénombrabilité montre l'existence de nombres transcendants sur $\mathbb{Q}$, et même dans un certain sens montre que presque tous les nombres complexes sont transcendants. Toutefois, il est en général difficile pour un nombre donné de démontrer qu'il est transcendant (par exemple e et π le sont mais cela n'a été démontré qu'au XIXème).

Le fait que l'extension $\mathbb{C}/\mathbb{R}$ soit algébrique est aussi une conséquence du théorème plus général suivant:

Théorème 3 *Toute extension de degré fini est algébrique.*

Preuve: Soit L/K une extension de degré fini, et notons $n = [L : K]$. Soit $\alpha \in L$. Il faut donc trouver un polynôme P non nul, à coefficients dans K, tel que $P(\alpha) = 0$. Mais la condition $P(\alpha) = 0$ revient à dire que les puissances successives de α sont liées sur K. L'idée est que, si l'on prend plus de puissances que la dimension n de L sur K, elles sont en effet nécessairement liées.

□

Remarque: Il ne faut pas croire que la réciproque soit vraie. En effet, il existe des extensions algébriques de degré infini, bien que nous ne nous en préoccuperons pas trop ici.

2.2.3 Polynôme minimal

Si α est algébrique, il y a en fait une infinité de polynômes tels que $P(\alpha) = 0$ puisque les multiples de P vont aussi vérifier cette propriété. On peut facilement décrire tous ces polynômes:

Proposition 5 *Soit L/K une extension et soit $\alpha \in L$ un élément algébrique sur K. Il existe un unique polynôme unitaire non nul $P_\alpha(X) \in K[X]$ de degré minimal tel que $P_\alpha(\alpha) = 0$. Pour tout polynôme $Q \in K[X]$, la condition $Q(\alpha) = 0$ équivaut à $P_\alpha(X)$ divise $Q(X)$. On dit que P_α est le polynôme minimal de α sur K.*

Preuve: L'ensemble $I = \{Q(X) \in K[X] \mid Q(\alpha) = 0\}$ est un idéal de $K[X]$, qui est un anneau principal. Cet idéal est donc principal, non réduit à $\{0\}$ si α est algébrique, et donc engendré par le polynôme unitaire de plus petit degré qu'il contient.

□

Définition 8 *On appelle degré de α sur K, le degré de son polynôme minimal sur K, et on le note $\deg_K(\alpha)$, ou $\deg(\alpha)$ quand il n'y a pas d'ambiguité sur K.*

Proposition 6 *Soit L/K une extension et soit $\alpha \in L$. On note $K[\alpha]$ l'ensemble*

$$K[\alpha] = \{Q(\alpha) \mid Q \in K[X]\}.$$

C'est le plus petit sous-anneau de L contenant K et α.

On note $K(\alpha)$ l'ensemble

$$K(\alpha) = \{\frac{P(\alpha)}{Q(\alpha)} \mid P, Q \in K[X] \text{ et } Q(\alpha) \neq 0\}.$$

C'est le plus petit sous-corps de L contenant K et α.

Preuve: Soit A un sous-anneau de L contenant K et α. Alors A contient les puissances de α, les produits de ces puissances avec des éléments de K, et les sommes de ces termes. Bref, A contient tous les $Q(\alpha)$ avec $Q \in K[X]$, soit $K[\alpha]$. Clairement, $K[\alpha]$ est un sous-anneau de L, c'est donc le plus petit. Les propriétés de $K(\alpha)$ se montrent de la même manière.

□

Remarque: On généralise facilement ses notions au cas de d éléments $\alpha_1, \ldots, \alpha_d$. On note $K[\alpha_1, \ldots, \alpha_d]$ et $K(\alpha_1, \ldots, \alpha_d)$ respectivement le plus petit sous-anneau et le plus petit sous-corps de L contenant K et $\alpha_1, \ldots, \alpha_d$.

Théorème 4 *Soit L/K une extension et soit $\alpha \in L$ un élément algébrique .*

1. *Le polynôme minimal de α sur K, P_α, est irréductible sur K, et*

$$K[\alpha] \simeq K[X]/P_\alpha(X)K[X].$$

2. $K[\alpha] = K(\alpha)$

3. $[K(\alpha) : K] = \deg(P_\alpha) = \deg(\alpha)$.

Preuve: On définit un homomorphisme d'anneaux de $K[X]$ dans L en posant:

$$\phi : K[X] \to L \tag{2.1}$$
$$P(X) \mapsto P(\alpha) \tag{2.2}$$

Clairement, $\mathrm{Im}\,\phi = K[\alpha]$ et $\ker\phi = P_\alpha(X)K[X]$. Par le théorème de factorisation, on obtient l'isomorphisme annoncé.

Comme $K[\alpha] \subset L$, c'est un anneau intègre. Ainsi, le quotient $K[X]/P_\alpha(X)K[X]$ est intègre, ce qui équivaut au fait que P_α soit irréductible sur K. Alors, ce quotient est un corps, et donc également $K[\alpha]$. Comme $K[\alpha] \subset K(\alpha)$, et que ce dernier est d'après la Proposition précédente le plus petit corps contenant K et α, on a l'égalité $K[\alpha] = K(\alpha)$.

□

Remarque: D'après la démonstration précédente, lorsque α est transcendant, $K[X] \simeq K[\alpha]$.

Le théorème précédent montre que la manipulation pratique des éléments de $K[\alpha]$ est très facile à partir du polynôme minimal de α. En effet, si $d = \deg(\alpha)$, la donnée d'un élément y de $K[\alpha]$ est équivalente à celle d'un d-uplet $(\lambda_0, \ldots, \lambda_{d-1}) \in K^d$ tel que $y = \lambda_0 + \lambda_1\alpha + \cdots + \lambda_{d-1}\alpha^{d-1}$. L'addition de deux éléments s'effectue terme à terme; la multiplication fait intervenir la réduction modulo P_α. Enfin, comme expliqué au paragraphe 2.1.5, l'inverse d'un élément se calcule grâce à l'algorithme d'Euclide étendu.

Ces considérations expliquent pourquoi on s'intéresse à la question suivante: étant donnée une extensions algébrique finie L/K, existe-t-il un élément α tel que $L = K[\alpha]$, et mieux encore, peut-on calculer algorithmiquement un tel élément ainsi que son polynôme minimal? Par exemple, peut-on trouver un tel élément pour $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$? Le théorème de l'élément primitif donne une réponse à ces questions. Nous allons en donner une version restreinte, mais suffisante pour les cas que nous rencontrerons. Avant cela, nous avons besoin de la notion de corps de décomposition d'un polynôme.

2.2.4 Corps de rupture, de décomposition, algébriquement clos

Un polynôme P à coefficients dans un corps K n'a pas forcément de racines dans K, ce qui est parfois fort génant. En fait, on peut toujours augmenter le corps K

pour y trouver des racines de P. Typiquement, le corps $\mathbb{C}$ des nombres complexes a été construit pour y avoir les racines de $X^2 + 1$.

Proposition 7 *Soit K un corps et soit $P(X) \in K[X]$.*

1. *Il existe une extension finie L/K telle que $P(X)$ a au moins une racine a dans L. Un tel corps L s'appelle un corps de rupture de P. Dans $L[X]$, $P(X)$ est divisible par $X - a$.*

2. *Il existe une extension finie L/K telle que $P(X)$ a exactement $\deg(P)$ racines dans L (comptées avec leur multiplicité). Un tel corps L s'appelle un corps de décomposition de P. Dans $L[X]$, $P(X)$ est produit de facteurs de degré 1.*

3. *Un corps L est dit algébriquement clos si tout polynôme de $L[X]$ a au moins une racine dans L. Alors tout polynôme de $L[X]$ a toutes ses racines dans L, et se factorise dans $L[X]$ en un produit de polynômes du premier degré.*

4. *Tout corps K possède une clôture algébrique c'est-à-dire un sur-corps algébriquement clos, et minimal pour cette propriété. De plus celle-ci est unique à isomorphisme près.*

Preuve: La construction d'un corps de rupture pour P est facile. En effet, considérons $R(X)$ un facteur irréductible de $P(X)$. Soit $L := K[X]/R(X)K[X]$. C'est un corps contenant K, et si x est l'image dans L de X, $R(x) = 0$ donc aussi $P(x) = 0$. L est donc un corps de rupture de P. Remarquez que si on considère directement le quotient $K[X]/P(X)K[X]$, on obtient un anneau qui n'est pas en général un corps. C'est pour cela qu'on passe par un facteur irréductible de P.

On peut itérer cette construction en remplaçant K par L et $P(X)$ par $P(X)/(X - x)$; en au plus $\deg(P)$ étapes, on obtient un corps extension finie de K qui contient toutes les racines de P.

La construction d'une clôture algébrique est plus subtile et nous ne la démontrerons pas ici. Toutefois son existence est assez intuitive.

□

Exemple: Le premier exemple de corps algébriquement clos est le corps $\mathbb{C}$ des nombres complexes. C'est donc une clôture algébrique pour $\mathbb{R}$ (il est minimal puisque de degré 2!). On peut montrer qu'une clôture algébrique de $\mathbb{Q}$ est de dimension infinie sur $\mathbb{Q}$ mais est dénombrable. Ce n'est donc pas $\mathbb{C}$!

2.2.5 Théorème de l'élément primitif

Théorème 5 *[Théorème de l'élément primitif] Soit L/K une extension finie. On suppose soit que K est fini, soit que $\mathrm{car}(K) = 0$. Alors, il existe un élément α de L tel que $L = K(\alpha)$. Un tel élément α est appelé un élément primitif de l'extension L/K.*

Preuve: On va laisser pour le prochain chapitre le cas des corps finis. Supposons que $\mathrm{car}(K) = 0$; alors le corps K est infini, ce qui va être crucial dans la suite.

Montrons d'abord qu'un polynôme irréductible P sur K a des zéros simples. En effet, si $(X-a)^n$ divise P dans un corps F de décomposition de P, avec $n \geq 2$, alors on peut écrire $P = (X-a)^n S$ et son polynôme dérivé $P' = (X-a)^n S' + n(X-a)^{n-1} S$. Il est important de remarquer que P' est non nul parce que $\mathrm{car}(K) = 0$ (en effet le polynôme dérivé de $X^6 + X^3$ sur F_3 est nul! mais cela ne peut arriver en caractéristique 0 car le coefficient dominant X^d se dérive en dX^{d-1} et que $d \neq 0$). Ainsi $X - a$ divise P et P' et donc divise le pgcd D de P et P'. Mais ces deux polynômes sont à coefficients dans K donc leur pgcd aussi. On aurait trouvé un diviseur D de P dans $K[X]$, de degré supérieur à 1 puisque divisible par $X - a$ sur F, et de degré strictement inférieur à P puisque divisant P'. Cela n'est pas possible puisque P est supposé irréductible sur K.

Supposons maintenant que $L = K(x, y)$. On va construire un z tel que $L = K[z]$. Notons P le polynôme irréductible de x sur K et Q celui de y. Soit M un corps de décomposition de P et Q. On peut écrire sur M $P = \prod_{i=1}^{n}(X - x_i)$ avec $x_1 = x$, et $Q = \prod_{i=1}^{m}(X - y_i)$ avec $y_1 = y$.

Alors il existe $t \in K$ tel que $x + ty \neq x_i + ty_j$ pour tout $i \geq 1$, $j \geq 2$. En effet, il suffit de choisir t distinct de tous les $\{-\frac{x-x_i}{y-y_j} \mid 1 \leq i \leq n, 2 \leq j \leq m\}$. Et c'est toujours possible puisque K est infini alors que l'ensemble des $-\frac{x-x_i}{y-y_j}$ lui est fini (noter que $y - y_j \neq 0$ parce que les zéros de Q sont simples).

Soit donc $t \in K$ tel que $x + ty \neq x_i + ty_j$ pour tout $i \geq 1$, $j \geq 2$. Soit $z = x + ty$. Montrons que $L = K[z]$. Soit $K' = K[z]$. Soit $F(X) := P(z - tX)$. Ce polynôme est à coefficients dans K'. Montrons que y est la seule racine de Q qui soit aussi racine de F. En effet, on vérifie aisément que les conditions sur t montrent que $F(y) = 0$ alors que $F(y_i) \neq 0$ pour $i \geq 2$. Cela prouve que $X - y$ est le pgcd de F et Q, et donc que ce polynôme est à coefficients dans K' (rappelons que le pgcd de deux polynômes dont les coefficients sont dans un corps k, est à coefficients dans k, comme le montre l'algorithme d'Euclide). Ainsi, on obtient que $y \in K'$. Comme $x = z - ty$, x appartient également à K' et on a démontré que $L = K[z]$.

Dans le cas général, L est une extension finie de K, donc il existe $x_1, \ldots, x_d$ tels que $L = K(x_1, \ldots, x_d)$. Par itération du cas $d = 2$, on trouve d'abord un générateur z_1 de $K(x_1, x_2)$, puis un générateur z_2 de $K(z_1, x_3)$, etc..

□

L'énoncé précédent fournit un algorithme permettant de calculer effectivement un tel α, si on sait calculer les racines de P et Q dans L. Par exemple, c'est le cas si x et y sont quadratiques dur K. De plus, on peut aussi s'interroger sur des critères définissant un meilleur choix parmis tous les α possibles. Par exemple, il peut être intéressant pour effectuer les calculs dans L, de trouver un élément primitif dont le polynôme minimal a beaucoup de coefficients nuls. Dans la pratique on s'appuie sur le lemme suivant:

Lemme 1 *Soit L/K une extension finie de degré n. Soit $\alpha \in L$. On a $L = K[\alpha]$ si et seulement si $\deg_K(\alpha) = n$.*

Preuve: A priori on a $K[\alpha] \subset L$. La condition $\deg_K(\alpha) = n$ implique $\dim_K(K[\alpha]) = \dim_K(L)$ (par Th 4.3) et donc $K[\alpha] = L$.

□

Ainsi trouver un élément primitif de L équivaut à trouver un élément dont le polynôme minimal a même degré que l'extension. En fait presque tout α va marcher, encore faut-il savoir calculer son polynôme minimal. Une méthode élémentaire consiste à chercher une combinaison linéaire nulle entre les puissances successives de α.

Exercice: Soit $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1. Montrez que $[L : \mathbb{Q}] = 4$
2. Montrez que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une base de L sur $\mathbb{Q}$.
3. Soit $\alpha = \sqrt{2} + \sqrt{3}$. Montrez que α est soit de degré 2 soit de degré 4.
4. Exprimez α sur cette base et montrez que $(1, \alpha, \alpha^2)$ sont $\mathbb{Q}$-linéairement indépendants.
5. Montrez que $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ sont liés sur $\mathbb{Q}$ et en déduire le polynôme minimal de α.
6. En déduire que $L = \mathbb{Q}[\alpha]$.

7. Décrire tous les corps intermédiaires (i.e. les corps M tels que $K \subset M \subset L$).

2.3 Corps finis

Les corps finis sont très importants pour les applications pratiques, en particulier pour la cryptographie et la théorie des codes correcteurs d'erreurs. On sait déjà qu'un corps fini à p éléments où p est un nombre premier, est isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +, \times)$. On note $\mathbb{F}_p$ un tel corps. On sait aussi qu'il existe des corps finis dont le cardinal n'est pas un nombre premier, comme par exemple $\mathbb{F}_2[X]/(X^2+1)\mathbb{F}_2[X]$ qui a 4 éléments. Nous allons décrire tous ces corps et leur structure.

On va appliquer les résultats du paragraphe précédent.

Théorème 6 *Soit L un corps fini, de cardinal q.*

1. *Il existe un nombre premier p tel que L contienne un sous-corps isomorphe à $\mathbb{F}_p$. L'extension $L/\mathbb{F}_p$ est de degré fini. Si r est le degré de cette extension, $q = p^r$.*

2. *Tout élément x de L vérifie $x^q = x$. Si M est un sur-corps de L contenant les racines du polynôme $X^q - X \in \mathbb{F}_p[X]$, alors L est exactement égal à l'ensemble des racines de ce polynôme.*

3. *Réciproquement, l'ensemble des racines du polynôme $X^q - X$ dans une clôture algébrique de $\mathbb{F}_p$ est un corps à q éléments.*

4. *Le groupe multiplicatif $(L^*, \times)$ est un groupe cyclique d'ordre $q - 1$.*

Preuve: Un corps fini ne peut être de caractéristique zéro. Le sous-corps premier de L est donc isomorphe à $\mathbb{F}_p$ pour un certain nombre premier p (voir Proposition 2 et la remarque qui la précède). Puisque L est fini, il est à fortiori de dimension finie sur $\mathbb{F}_p$. Si r est cette dimension, L est isomorphe *comme espace vectoriel* à $\mathbb{F}_p^r$ et est donc de cardinal p^r.

Puisque L est un corps, tout élément non nul est inversible. Le groupe multiplicatif L^* est donc d'ordre $q - 1$. Par le théorème de Lagrange, tout élément non nul de L vérifie donc $x^{q-1} = 1$. Ainsi, tout élément de L vérifie $x^q = x$, et est donc une racine du polynôme $X^q - X$. Comme un polynôme de degré q a au

plus q racines dans un corps, et que L possède q éléments, L est exactement égal à l'ensemble des racines de ce polynôme, dans un corps qui les contienne.

Réciproquement, soit L l'ensemble des racines de $X^q - X$ dans une clôture algébrique de $\mathbb{F}_q$, montrons que L forme un corps à q éléments. D'abord, L a bien q éléments car $X^q - X$ n'a que des racines simples. En effet, il faut pour cela vérifier que ce polynôme est premier avec son polynôme dérivé; or celui-ci est $qX^{q-1} - 1 = -1$ (on est en caractéristique p). Ensuite, il faut montrer que L est un corps. Ce qui est facile à montrer, c'est que le produit et l'inverse d'éléments de L est encore dans L. En effet, supposons α, β appartenant à L, c'est-à-dire $\alpha^q = \alpha$ et $\beta^q = \beta$. Alors: $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$ et $(\alpha^{-1})^q) = (\alpha^q)^{-1} = (\alpha)^{-1}$. Il reste à montrer que L est stable par addition, ce qui est un peu moins évident. Cela résulte du lemme suivant, qui est d'autre part extrêmement utile:

Lemme 2 *Soit K un corps de caractéristique $p > 1$. Pour tout $x, y \in K$ et tout $r \geq 0$, si $q = p^r$, on a:*

$$(x + y)^q = x^q + y^q.$$

Preuve: Démontrons cette formule pour $q = p$. Comme dans tout anneau commutatif, on peut appliquer la formule du binôme de Newton:

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

Pour $1 \leq i \leq p - 1$, $\binom{p}{i} \equiv 0 \mod p$, et donc $\binom{p}{i} = 0$ dans $\mathbb{F}_p$. Ainsi, les "termes du milieu" s'annulent et il reste la relation $(x + y)^p = x^p + y^p$.

On obtient la formule annoncée pour $q = p^2$ en itérant ce calcul:
$(x + y)^{p^2} = ((x + y)^p)^p = (x^p + y^p)^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$. Une démonstration par récurrence s'impose pour le cas général.. que nous laisserons rédiger au lecteur.

□

Revenons à notre ensemble de racines L: on peut donc écrire $(\alpha+\beta)^q = \alpha^q+\beta^q = \alpha + \beta$ et on obtient que $\alpha + \beta \in L$. On a donc bien démontré que L est un corps à q éléments.

Il reste à démontrer que L^* est cyclique, c'est-à-dire qu'il contient un élément d'ordre q. Soit $x \in L^*$ un élément d'ordre d. On sait que d divise $q - 1$. Le sous-groupe engendré par x est lui-même cyclique, et donc contient $\phi(d)$ éléments d'ordre d (ce sont les x^a avec $(a, d) = 1$). Montrons que L^* ne peut pas contenir

d'autres éléments d'ordre d. En effet, si y est d'ordre d, y est une racine du polynôme $X^d - 1$. Mais ce polynôme est de degré d donc il ne peut pas avoir plus de d racines dans L. Or il en a déjà d, ce sont les puissances de x: $1, x, \ldots, x^{d-1}$. Ainsi tous les éléments d'ordre d de L^* sont des puissances de x et il y en a $\phi(d)$. On vient de démontrer que, pour tout diviseur d de $q-1$, L^* contient soit aucun soit $\phi(d)$ éléments d'ordre d. Mais la formule:

$$q - 1 = \sum_{d|q-1} \phi(d)$$

montre que pour aucun diviseur de $q-1$ il n'y a pas d'elément d'ordre ce diviseur (puisqu'un élément de L^* doit bien avoir un ordre, diviseur de $q-1$). Appliquant cela au diviseur $q-1$ lui-même, on obtient que L^* contient bien des éléments d'ordre $q-1$.

□

Remarque: La formule du lemme précédent s'appelle aussi *formule du binôme des cancres*. Sans commentaires ...

Remarque: D'après le théorème précédent, un corps fini est uniquement déterminé par son cardinal, dans une clôture algébrique de $\mathbb{F}_p$. On note $\mathbb{F}_q$ un tel corps.

Remarque: Une autre approche de l'existence d'un corps à q éléments consiste à démontrer l'existence d'un polynôme irréductible sur $\mathbb{F}_p$ de degré r (où $q = p^r$) et à considérer le corps $\mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$. Remarquons bien que le choix du polynôme irréductible de degré r ne change pas le corps puisqu'on vient de démontrer qu'à cardinal fixé il n'y en a qu'un !

Un petit exemple concret: Il est facile de voir que, sur $\mathbb{F}_2$, les seuls polynômes de degré 3 irréductibles sont: $P_1 = X^3 + X + 1$ et $P_2 = X^3 + X^2 + 1$. Le corps $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ avec $\alpha^3 + \alpha + 1 = 0$ a 8 éléments. Ce qui précède permet de prédire que, parmi les 6 éléments différents de 0 et 1, il y a trois racines de P_1 et trois racines de P_2.

Un bon exercice de calcul dans $\mathbb{F}_8$ montre que les racines de P_1 sont: α, α^2 et $\alpha^4 = \alpha^2 + \alpha$ et les racines de P_2 sont les trois autres. Ainsi, si $\beta = \alpha + 1$, on a :

$$\mathbb{F}_2[\alpha] = \mathbb{F}_2[\beta]$$

avec $\alpha^3 + \alpha + 1 = 0$ et $\beta^3 + \beta^2 + 1 = 0$.

Puisque $\mathbb{F}_8$ est l'ensemble des racines de $X^8 - X$, on obtient aussi que:

$$X^8 - X = X(X+1)P_1(X)P_2(X)$$

ce qui peut bien sûr se vérifier directement.

Nous sommes en mesure maintenant de démontrer le théorème de l'élément primitif dans le cas des corps finis.

Théorème 7 *Soit L/K une extension de corps finis. Il existe $\alpha \in L$ tel que $L = K[\alpha]$.*

Preuve: On peut écrire $\mathrm{card}(K) = p^r$ et $\mathrm{card}(L) = p^s$. On sait par le Théorème 6 que le groupe multiplicatif de L est cyclique d'ordre $p^s - 1$. Soit α un générateur de ce groupe, on va montrer que cet α convient. (Attention, la réciproque est fausse: un élément primitif de l'extension L/K n'est pas nécessairement un générateur du groupe multiplicatif). Si ce n'est pas le cas, α engendre un sous-corps strict de L, c'est-à-dire $K[\alpha] = M$, avec $\mathrm{card}(M) = p^u$ et $u < s$. Mais alors $\alpha \in M^*$, donc $\alpha^{p^u-1} = 1$. Comme $p^u - 1 < p^s - 1$, cela contredit l'hypothèse suivant laquelle α est d'ordre $p^s - 1$.

Remarque: Le théorème précédent montre que $\mathbb{F}_q$ s'écrit $\mathbb{F}_q = \mathbb{F}_p[\alpha]$ avec $P(\alpha) = 0$, et P irréductible sur $\mathbb{F}_p$ de degré r ($q = p^r$). Changer de polynôme irréductible revient à changer l'élément primitif α (comme dans le "petit exemple concret").

On étudie maintenant les propriétés d'inclusion des corps finis.

Théorème 8 *$\mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$ si et seulement si r divise s.*

Preuve: Comme $r = [\mathbb{F}_{p^r} : \mathbb{F}_p]$, et d'après la Proposition 4, la condition r divise s est nécessaire à l'inclusion $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$. Réciproquement, supposons que r divise s. et posons $s = rt$. Alors, $p^r - 1$ divise $p^s - 1$: en effet, on a l'identité:

$$p^s - 1 = (p^r - 1)(p^{r(t-1)} + p^{r(t-2)} + \cdots + p^r + 1).$$

Posons $d = p^r - 1$. On sait que le groupe $\mathbb{F}_{p^s}^*$ est cyclique d'ordre $p^s - 1$; donc, puisque d divise son ordre, ce groupe contient exactement d éléments d'ordre divisant d. En rajoutant 0, on voit que $\mathbb{F}_{p^s}$ contient les p^r racines de $X^{p^r} - X$. D'après le Théorème 6, $\mathbb{F}_{p^s}$ contient donc $\mathbb{F}_{p^r}$.

□

Un outil très utile pour travailler sur les corps finis est l'automorphisme de Frobenius.

Définition 9 *Soit $\mathbb{F}_q$ un corps à $q = p^r$ éléments. On pose $\sigma(x) = x^p$. σ est appelé l'automorphisme de Frobenius de $\mathbb{F}_q$.*

Théorème 9 *Avec les notations précédentes:*

1. *σ est un automorphisme du corps $\mathbb{F}_q$.*
2. *On a $\sigma^s(x) = x^{p^s}$ pour tout s, et $\sigma^r = \mathrm{Id}_{\mathbb{F}_q}$.*
3. *Pour tout $x \in \mathbb{F}_q$, et u divisant r, $x \in \mathbb{F}_{p^u}$ si et seulement si $\sigma^u(x) = x$.*

Preuve: La propriété $\sigma(xy) = \sigma(x)\sigma(y)$ est évidente. La propriété $\sigma(x+y) = \sigma(x) + \sigma(y)$ résulte du Lemme 2. Le fait que σ soit injectif est clair; comme $\mathbb{F}_q$ est fini, il est donc aussi bijectif.

Les points 2 et 3 du théorème sont clairs, compte tenu du Théorème 6.2

□

En particulier, le Frobenius est utile pour exprimer le polynôme minimal d'un élément sur un sous-corps.

Théorème 10 *Soit $\mathbb{F}_q$ un corps à $q = p^r$ éléments. Soit $\alpha \in \mathbb{F}_q$, et posons $\alpha_i = \sigma^i(\alpha)$.*

1. *Soit $P \in \mathbb{F}_p[X]$ tel que $P(\alpha) = 0$. Alors, pour tout i, $P(\alpha_i) = 0$.*
2. *Soit P_α le polynôme minimal de α sur $\mathbb{F}_p$. Il existe un plus petit entier s tel que $\alpha_s = \alpha$, et on a:*

$$P_\alpha = \prod_{i=0}^{s-1}(X - \alpha_i).$$

Preuve: On a la relation $P(\alpha) = 0$. On applique σ à cette égalité; comme P est à coefficients dans $\mathbb{F}_p$, et que $\sigma(x) = x$ si $x \in \mathbb{F}_p$, on a $\sigma(P(\alpha)) = P(\sigma(\alpha)) = 0$ donc $\sigma(\alpha)$ est racine de P, ainsi que, par itération, tous les $\sigma^i(\alpha)$. Cela démontre la première partie du théorème.

En particulier, si $P = P_\alpha$, on peut appliquer le 1., qui montre que les α_i sont racines de P_α. Comme $\alpha^q = \alpha$, on a $\sigma^r(\alpha) = \alpha$, soit $\alpha_r = \alpha$. Il existe donc un plus petit entier s tel que $\alpha_s = \alpha$. Notons que la minimalité de s implique que les éléments $\alpha_0, \alpha_1, \ldots, \alpha_{s-1}$ sont deux à deux distincts. Soit $Q := \prod_{i=0}^{s-1}(X - \alpha_i)$. Montrons que ce polynôme est à coefficients dans $\mathbb{F}_p$. Pour cela, la bonne méthode est de montrer qu'il est invariant par σ. Or $\sigma(Q) = \prod_{i=0}^{s-1}(X - \sigma(\alpha_i))$. Mais

$\sigma(\alpha_i) = \alpha_{i+1}$ pour $i \leq s-2$ et $\sigma(\alpha_{s-1}) = \alpha_s = \alpha = \alpha_0$. Les racines de Q sont permutées circulairement, donc Q est laissé invariant.

Le polynôme Q est à coefficients dans $\mathbb{F}_p$ et $Q(\alpha) = 0$ donc, d'après la Proposition 5, P_α divise Q. D'autre part, les éléments $\alpha_0, \alpha_1, \ldots, \alpha_{s-1}$ sont deux à deux distincts et sont racines de P_α. Donc $\deg(P_\alpha) \geq s$. Comme Q est de degré s, on a forcément $Q = P_\alpha$.

□

Remarque: Dans le théorème précédent, on peut remplacer l'extension $\mathbb{F}_q/\mathbb{F}_p$ par une extension relative $\mathbb{F}_q/\mathbb{F}_{q'}$, à condition de remplacer σ par $\sigma' : x \to x^{q'}$.

Encore le petit exemple: Soit toujours $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ avec $\alpha^3 + \alpha + 1 = 0$. On comprend mieux pourquoi les racines de P_1 sont α, α^2 et $\alpha^4 = \alpha^2 + \alpha$. Ce sont les images successives de α par le Frobenius. Et bien sûr $\alpha^8 = \alpha$! De même, les racines de P_2 sont: $\beta = \alpha + 1$, β^2, β^4.

Chapter 3

Réseaux et algorithme LLL

Un module n'est autre qu'un espace vectoriel sur un anneau. Le passage d'un corps à un anneau fait toute la richesse de cette notion; en particulier, il ne faut pas tomber dans le piège des automatismes acquis dans l'étude en premier cycle des espaces vectoriels.

Dans ce chapitre, après quelques généralités sur les modules sur un anneau quelconque, nous allons rapidement nous concentrer sur les réseaux, qui sont des $\mathbb{Z}$-modules libres munis d'une structure Euclidienne. L'algorithme LLL permet de construire efficacement des bases de petits vecteurs d'un réseau. Cet algorithme polynomial est extrêmemnt utile notamment en cryptographie, et nous en verrons des applications.

3.1 Modules: généralités

Dans tout ce qui suit, A est un anneau.

Définition 10 *Un ensemble M est un A-module (à gauche) si $(M, +)$ est un groupe commutatif, muni d'une loi externe $A \times M \to M$, $(a, x) \mapsto ax$ vérifiant les axiomes suivants:*

1. *Pour tout $x \in M$, $1x = x$*
2. *Pour tout $a, b \in A$, $x \in M$, $a(bx) = (ab)x$ et $(a + b)x = ax + bx$*
3. *Pour tout $a \in A$, $x, y \in M$, $a.(x + y) = a.x + a.y$*

Exercice: : Montrez que $a(-x) = -ax$ et $0x = 0$.

Exemple: Quelques exemples de modules, qui montrent que cette notion regroupe un grand nombre de situations:

- Le module trivial: $M = \{0\}$.
- $M = A^n$
- Les espaces vectoriels (i.e. A est un corps).
- Les groupes abéliens sont exactement les $\mathbb{Z}$-modules.
- La donnée d'un espace vectoriel E sur un corps K et d'un endomorphisme u de E est un $K[X]$-module pour la multiplication: $P(X)x = P(u)(x)$. La plupart des résultats de la théorie de la réduction des endomorphismes peuvent être vus comme des résultats de structure des $K[X]$-modules.
- Les sous-modules d'un anneau A sont les idéaux à gauche de A.

Quelques définitions et propriétés standards:

Définition 11 *Soit M un A-module.*

1. *Un sous-module N de M est un sous-groupe de M, vérifiant: pour tout $a \in A$, $x \in N$, $ax \in N$. De façon équivalente, N est un sous-ensemble non vide de M, vérifiant $ax + by \in N$ pour tout $a, b \in A$, $x, y \in N$.*
2. *Un homomorphisme de modules $f : M_1 \to M_2$ entre deux A-modules est une application vérifiant: $f(ax + by) = af(x) + bf(y)$ pour tout $a, b \in A$ et $x, y \in M_1$. Son noyau et son image sont respectivement*

$$\ker f := \{x \in M_1 \mid f(x) = 0\} \text{ et } \operatorname{Im} f := \{f(x) \mid x \in M_1\}$$

3. *Le produit direct de deux A-modules M et N est l'ensemble $M \times N = \{(x, y) \mid x \in M, y \in N\}$. C'est un A-module pour: $a(x, y) = (ax, ay)$.*

Proposition 8 *1. Soit N, N' deux sous-modules de M. L'intersection $N \cap N'$ et la somme $N + N' = \{x + y \mid x \in N \text{ et } y \in N'\}$ sont des sous-modules de M. Si $N \cap N' = \{0\}$, alors $N + N'$ est isomorphe au produit direct de N et N'. On note alors $N \oplus N'$.*

Le quotient $M/N := \{x + N \mid x \in M\}$ est un A-module pour la loi: $a(x + N) = ax + N$.

2. *Soit $f : M_1 \to M_2$ un homomorphisme de modules. Le noyau de f est un sous-module de M_1 et l'image de f est un sous-module de M_2. L'homomorphisme f est injectif si et seulement si $\ker f = \{0\}$ et il est surjectif si et seulement si $\mathrm{Im}\, f = M_2$. Il induit un isomorphisme: $\overline{f} : M_1/\ker f \to \mathrm{Im}\, f$ (théorème de factorisation).*

3. *L'application $s : M \to M/N$ définie pas $s(x) = x + N$ est un homomorphisme de modules, surjectif et de noyau N.*

Comme pour les espaces vectoriels, on peut définir les notions de famille libre, génératrice et de base d'un A-module.

Définition 12 *Soit M un A-module et soit $\{e_i\}_{i\in I} \subset M$. On dit que:*

1. *C'est une famille libre de M si: $\sum_{i\in I_f} a_i e_i = 0$ avec $a_i \in A$ et $I_f \subset I$ une sous-partie finie, entraîne: $a_i = 0$ pour tout $i \in I_f$.*

2. *C'est une famille génératrice de M si tout élément $x \in M$ s'écrit $x = \sum_{i\in I_f} a_i e_i$ avec $a_i \in A$ et $I_f \subset I$ une sous-partie finie.*

3. *C'est une base de M si c'est une famille libre et génératrice.*

Définition 13 *Un module possédant une partie génératrice finie est dit* de type fini. *Un module possédant une base est dit* libre.

Proposition 9 1. *L'ensemble $\{e_i\}_{i\in I} \subset M$ est une base de M sur A, si et seulement si, pour tout $x \in M$, il existe un unique $(a_i)_{i\in I_f}$ avec $a_i \in A$ et I_f finie tels que $x = \sum_{i\in I_f} a_i e_i$.*

2. *Si M est un module libre et de type fini, ses bases sont de cardinal fini. Si $\{e_1, \ldots, e_n\} \subset M$ est une base de M, alors M est isomorphe à A^n par l'isomorphisme: $(a_1, \ldots, a_n) \in A^n \to a_1 e_1 + \cdots + a_n e_n \in M$.*

Preuve: 1. est clair. Pour 2., supposons que $(e_i)_{i\in I}$ soit une base de M et que $(v_1, \ldots, v_m)$ soit une partie génératrice. Chaque v_j est une combinaison linéaire d'un nombre fini des e_i, et comme il y a un nombre fini de v_j, il existe une partie finie $I_f \subset I$ telle que pour tout j, $v_j = \sum_{k\in I_f} a_{j,k} e_k$. Mais, si $i \notin I_f$, $e_i = \sum_{u=1}^m b_u v_u = \sum_{u=1}^m b_u (\sum_{k\in I_f} a_{u,k} e_k)$ ce qui donne une combinaison linéaire nulle non triviale (le coefficient de e_i est 1) des e_i.

L'isomorphisme est clair.

□

Du point de vue de ces notions, les modules sont beaucoup plus complexes que les espaces vectoriels. En premier lieu, il y a dans un module la possibilité que: $ax = 0$ alors que $x \neq 0$ et $a \neq 0$. Par exemple, si $M = \mathbb{Z}/6\mathbb{Z}$, considéré comme $\mathbb{Z}$-module, on a $6x = 0$ pour tout x. Cela arrive bien sûr si a n'est pas inversible dans A. Si a a un inverse, l'équation $ax = 0$ multipliée par a^{-1} conduit à $x = 0$. Ainsi, un groupe abélien fini ne contient aucune famille libre. Par contre il est de type fini, puisque il est fini.

Considérons une situation radicalement différente: $M = A^n$, avec A un anneau intègre. Il est facile de voir que la situation précédente ne peut pas arriver: on a bien $ax = 0$ si et seulement si $a = 0$. Le module M est libre, de type fini, et il a une base à n éléments. Malgré tout, il ne se comporte pas comme un espace vectoriel:

1. Une partie libre à n éléments n'est pas toujours une base. Par exemple, $\{2\}$ est une famille libre du $\mathbb{Z}$-module $\mathbb{Z}$ mais pas une base.

2. D'une famille génératrice on ne peut pas toujours extraire une base. Par exemple, $\{2, 3\}$ engendre $\mathbb{Z}$ mais ni $\{2\}$ ni $\{3\}$ n'est une base de $\mathbb{Z}$.

3. On ne peut pas toujours compléter une famille libre en une base. Par exemple, on peut démontrer qu'un élément $x = (x_1, \ldots, x_n)$ non nul de $\mathbb{Z}^n$ peut être complété en une base de $\mathbb{Z}^n$ si et seulement si les x_i sont premiers entre eux dans leur ensemble.

4. Un sous-module de M n'est pas toujours libre! En effet, le cas de $n = 1$ montre que pour cela, il est nécessaire que A soit principal, puisque les sous-modules de A sont les idéaux et que les sous-modules libres sont les idéaux principaux. Par exemple les modules sur l'anneau $A = K[X, Y]$ n'ont pas cette propriété.

L'étude des propriétés de $M = A^n$ se traduit aussi en termes matriciels. L'ensemble $M_n(A)$ des matrices $n \times n$ à coefficients dans A est un anneau pour les opérations usuelles. Lorsque l'anneau A est commutatif, on peut définir le déterminant d'une matrice, en prenant les formules connues pour les matrices à coefficients dans un corps. Si $M \in M_n(A)$, $\det(M) \in A$ et on a la propriété: $\det(MN) = \det(M)\det(N)$. Un élément de $M_n(A)$ est inversible dans cet anneau si et seulement si son déterminant est inversible dans A. On note $GL_n(A)$ le

groupe des matrices inversibles de $M_n(A)$. Par exemple, $GL_n(\mathbb{Z})$ est l'ensemble des matrices à coefficients dans $\mathbb{Z}$ de déterminant égal à ± 1.

Proposition 10 *Soit A un anneau commutatif, et soit $b_1, b_2, \ldots, b_n \in A^n$. Soit B la matrice dont les colonnes sont les b_i. L'ensemble $\{b_1, b_2, \ldots, b_n\}$ est une base de A^n si et seulement si B est inversible sur A, i.e. si et seulement si $\det(A) \in A^*$.*

Preuve: Posons $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ et supposons que $\mathcal{B}$ soit une base de $M = A^n$. La base "canonique" $\mathcal{E} = \{e_1, e_2, \ldots, e_n\}$ dont la matrice associée est la matrice identité s'exprime sur $\mathcal{B}$, ce qui se traduit par l'existence d'une matrice $P \in M_n(A)$ telle que:

$$\mathrm{Id}_n = BP$$

ce qui montre que B est inversible.

Réciproquement, si B est inversible, il existe une matrice P telle que $\mathrm{Id}_n = BP$, ce qui montre que $\mathcal{B}$ est génératrice de M. Pour montrer que $\mathcal{B}$ est libre, considérons une combinaison linéaire nulle $a_1 b_1 + \cdots + a_n b_n = 0$. C'est-à-dire: $BX = 0$, où X est le vecteur colonne des a_i. En multipliant à gauche par P, on obtient $X = 0$.

□

3.2 Réseaux

On va étudier maintenant les $\mathbb{Z}$-modules libres munis d'une structure Euclidienne. De façon intuitive, certaines bases sont meilleures que d'autres, si elles se rapprochent d'une base orthogonale; l'algorithme LLL permet de trouver une telle base en temps polynomial. Bien sûr, un réseau ne possède pas toujours une base orthogonale. On va s'appuyer sur l'orthogonalisation de Gram-Schmidt, un algorithme orthogonalisant une base *sur* $\mathbb{R}$. Le processus de transformation d'une $\mathbb{Z}$-base en une autre $\mathbb{Z}$-base du réseau plus "orthogonale" conduit à raccourcir les vecteurs. Toutefois, l'algorithme LLL ne conduit pas automatiquement à une base du réseau contenant un vecteur minimal. Malgré tout, à cause de sa rapidité, il est souvent utilisé pour trouver des vecteurs courts du réseau (la recherche des vecteurs minimaux d'un réseau est exponentielle).

3.2.1 Définitions

$\mathbb{R}^n$ est muni de sa structure Euclidienne habituelle $x \cdot y = x_1y_1 + \cdots + x_ny_n$. Si $x \in \mathbb{R}^n$, on appelle norme de x la valeur de $x \cdot x$.

Définition 14 *Un réseau L de $\mathbb{R}^n$ est l'ensemble des combinaisons linéaires à coefficients entiers d'une base de $\mathbb{R}^n$*

$$L = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2 \oplus \cdots \oplus \mathbb{Z}b_n.$$

Il est clair que L est une partie discrète de $\mathbb{R}^n$ (nous allons revenir là-dessus un peu plus loin). Pour tout M, l'ensemble des éléments x de L vérifiant $x \cdot x \leq M$ est fini; cela nous permet de définir le minimum de L, qui est atteint pour un nombre fini de vecteurs de L.

Définition 15 *Le minimum de L est défini par:*

$$\min(L) = \min\{x \cdot x \mid x \in L \setminus \{0\}\}.$$

L'ensemble des vecteurs minimaux de L est l'ensemble fini

$$S(L) = \{x \in L \mid x \cdot x = \min(L)\}.$$

Une matrice de Gram de L est la matrice des produits scalaires d'une base de L:

$$G = (b_i \cdot b_j)_{1 \leq i,j \leq n}.$$

Le déterminant du réseau L est le déterminant d'une matrice de Gram de L, et ne dépend pas du choix de la base de L.

En effet, si G' est la matrice de Gram d'une autre base de L, la matrice de passage P appartient à $GL_n(\mathbb{Z})$ donc est de déterminant ± 1. Comme $G' = P^tGP$, $\det(G') = (\det(P))^2 \det(G) = \det(G)$.

□

On classe les réseaux à équivalence orthogonale près. Une matrice symétrique définie positive définit un réseau à équivalence près puisque c'est la matrice de Gram d'une base de $\mathbb{R}^n$, définie modulo une transformation orthogonale.

On peut aussi définir les réseaux comme étant les $\mathbb{Z}$-modules libres de $\mathbb{R}^n$, non contenus dans un sous-espace strict de $\mathbb{R}^n$. Cette définition plus abstraite a l'avantage de ne pas faire appel à une base particulière.

3.2.2 Orthogonalisation de Gram-Schmidt

Soit $\{b_1, \ldots, b_n\}$ une base de $\mathbb{R}^n$. L'orthogonalisation de Gram-Schmidt de cette base est une base de $\mathbb{R}^n$ notée $\{b_1^*, \ldots, b_n^*\}$, qui vérifie les propriétés suivantes:

1. Elle est orthogonale, i.e. $b_i^* \cdot b_j^* = 0$ si $i \neq j$
2. Pour tout $i \geq 1$, $\{b_1^*, \ldots, b_i^*\}$ engendre le même sous-espace vectoriel que $\{b_1, \ldots, b_i\}$
3. (Normalisation) Les deux propriétés précédentes caractérisent les vecteurs b_i^* à multiplication par un scalaire près. Nous supposerons donc que $b_i^* = b_i$ plus une combinaison linéaire des b_j avec $j < i$.

Proposition 11 *On a* $b_i = \sum_{j=1}^{i} u_{i,j} b_j^*$ *avec* $u_{i,i} = 1$ *et* $u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.

Preuve: D'après la condition 2., il existe des coefficients $u_{i,j}$ tels que

$$b_i = \sum_{j=1}^{i} u_{i,j} b_j^*. \tag{3.1}$$

La condition 3. équivaut à $u_{i,i} = 1$. Si on calcule le produit scalaire avec b_j^* de cette égalité, puisque les b_j^* sont deux à deux orthogonaux, on trouve

$$b_i \cdot b_j^* = u_{i,j} b_j^* \cdot b_j^*$$

et donc

$$u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}. \tag{3.2}$$

□

La proposition précédente permet de calculer les $u_{i,j}$ par récurrence sur i facilement. Posons

$$a_i^2 := b_i^* \cdot b_i^* \text{ avec } a_i > 0.$$

En effet, pour $i = 1$, il n'y a que $u_{1,1} = 1$ ($b_1^* = b_1$) et donc $a_1^2 = b_1 \cdot b_1$. L'équation (3.2) nous permet de calculer $u_{2,1}$, puis a_2^2 puisque $b_2 \cdot b_2 = b_2^* \cdot b_2^* + u_{2,1}^2 a_1^2$, et ainsi de suite.

Réciproquement, en inversant la matrice triangulaire des $u_{i,j}$, on peut calculer les b_i^* en fonction des b_i. Retenons pour usage ultérieur la formule:

$$b_i \cdot b_i = \sum_{j=1}^{i} u_{i,j}^2 a_j^2. \tag{3.3}$$

Interprétation matricielle: Soit B la matrice dont les colonnes sont les vecteurs b_i, B^* la matrice dont les colonnes sont les vecteurs b_i^*, et A la matrice diagonale dont les coefficients diagonaux sont $a_1, a_2, \ldots, a_n$.

On a : $(B^*)^t B^* = A^2$. Si on pose $K = B^* A^{-1}$, cette matrice vérifie $K^t K = \mathrm{Id}$ et est donc orthogonale. D'autre part, si U est la matrice transposée des $u_{i,j}$, complétée par des zéros en posant $u_{i,j} = 0$ si $i < j$ (U est donc une matrice triangulaire supérieure, avec des 1 sur la diagonale), on a $B = B^* U$, et donc finalement

$$B = KAU$$

(décomposition d'Iwasawa de B).

En particulier, de $B = B^* U$ il vient $G = B^t B = U^t A^2 U$, et, comme la matrice U est de déterminant égal à 1,

$$\det(L) = \prod_{i=1}^{n} a_i^2. \tag{3.4}$$

Application: l'orthogonalisation de Gram-Schmidt correspond aussi à la "décomposition en somme de carrés" de $x \cdot x$. Elle permet de calculer effectivement l'ensemble $\{x \in L \mid x \cdot x \leq M\}$, et de se convaincre que c'est bien un ensemble fini. En effet, si $x = \sum_{i=1}^{n} x_i b_i \in L$, $x_i \in \mathbb{Z}$:

$$\begin{aligned} x = \sum_{i=1}^{n} x_i b_i &= \sum_{i=1}^{n} x_i \sum_{j=1}^{i} u_{i,j} b_j^* \\ &= \sum_{j=1}^{n} (\sum_{i=j}^{n} x_i u_{i,j}) b_j^* \end{aligned}$$

donc

$$x \cdot x = \sum_{j=1}^{n} (\sum_{i=j}^{n} x_i u_{i,j})^2 a_j^2$$
$$= (x_1 + x_2 u_{2,1} + \dots)^2 a_1^2 + \dots + (x_{n-1} + x_n u_{n,n-1})^2 a_{n-1}^2 + x_n^2 a_n^2$$

et la condition $x \cdot x \leq M$ implique:

$$-\sqrt{M}/a_n \leq x_n \leq \sqrt{M}/a_n$$
$$-\sqrt{M}/a_{n-1} - x_n u_{n,n-1} \leq x_{n-1} \leq \sqrt{M}/a_{n-1} - x_n u_{n,n-1}$$
$$\dots$$

ce qui conduit à un nombre fini de possibilités pour les valeurs entières de x_n, $x_{n-1}, \dots, x_1$. Il reste à parcourir cet ensemble fini pour finalement déterminer les valeurs de $x_1, \dots, x_n$ pour lesquelles $x \cdot x \leq M$. En particulier, nous avons démontré que l'ensemble des vecteurs minimaux $S(L)$ d'un réseau L est fini.

3.2.3 Sous-groupes discrets de $\mathbb{R}^n$

Dans ce paragrapphe, on montre l'équivalence entre les notions de réseau, tels que définis ici, et de sous-groupe discret de $\mathbb{R}^n$. Rappelons que le rang d'un sous-ensemble de $\mathbb{R}^n$ est la dimension du $\mathbb{R}$-espace vectoriel engendré par cet ensemble. D'un ensemble de rang n, on peut toujours extraire une $\mathbb{R}$-base (mais pas une $\mathbb{Z}$-base!).

Théorème 11 *Soit L un réseau de $\mathbb{R}^n$; alors L est un sous-groupe discret de $\mathbb{R}^n$. Réciproquement, soit L un sous-groupe discret de $\mathbb{R}^n$, non contenu dans un sous-espace vectoriel strict de $\mathbb{R}^n$ (i.e. de rang n). Alors L possède une Z-base qui est aussi une base de $\mathbb{R}^n$, i.e. L est un réseau au sens de la définition 14.*

Preuve: On a démontré au paragraphe précédent que $\{x : x \in L \mid x \cdot x \leq M\}$ est un ensemble fini. Cela montre bien que 0 est isolé dans L. Plus généralement, la même démonstration, en remplaçant x par $x - y$ avec $x \in L$, $y \in \mathbb{R}^n$, montre que l'intersection $L \cap B(y, M)$ est finie. Remarquons qu'il n'est pas vrai qu'un sous-groupe de $\mathbb{R}^n$ est toujours discret. Par exemple, le $\mathbb{Z}$-sous-module de $\mathbb{R}$ engendré par 1 et π (ou 1 et n'importe quel nombre irrationnel) contient une infinité d'éléments dans l'intervalle $]0, 1[$: par exemple $\{n\pi - [n\pi] : n \in \mathbb{N}\}$.

Réciproquement, soit L un sous-groupe discret de $\mathbb{R}^n$. Supposons d'abord $n = 1$. Pour tout intervalle compact $[a, b]$, l'ensemble $L \cap [a, b]$ est fini. On peut en déduire que $L \cap \mathbb{R}^{*+}$ possède un plus petit élément a. On a bien sûr $a\mathbb{Z} \subset L$. Montrons que $L = a\mathbb{Z}$: pour tout élément $x \in L$, il existe un entier k tel que $ka \leq x < (k+1)a$. Alors $0 \leq x - ka < a$; mais $x - ka \in L$ et a est le plus petit élément positif de L. Donc $x - ka = 0$.

Nous allons maintenant considérer le cas général, et construire par récurrence une $\mathbb{Z}$-base de L. Tout d'abord, observons que L contient nécessairement une $\mathbb{R}$-base. En effet, on peut définir une suite emboitée de sous-espaces vectoriels $V_1 \subset V_2 \subset \cdots \subset V_k$ en posant $V_k =$ le sous-espace vectoriel engendré par l'ensemble (fini) $\{x \in L \mid x \cdot x \leq k\}$. En considérant la suite des dimensions de V_k, qui est une suite croissante d'entiers entre 0 et n, on conclut que, soit il existe un entier k_0 à partir duquel $V_k = \mathbb{R}^n$, et dans ce cas on peut extraire de $\{x \in L \mid x \cdot x \leq k_0\}$ une base de $\mathbb{R}^n$ formée de vecteurs de L, soit la suite V_k est stationnaire à un sous-espace W strict de $\mathbb{R}^n$. Dans ce cas, $L \subset W$ ce qui contredit l'hypothèse.

Soit donc $\{e_1, e_2, \ldots, e_n\}$ une $\mathbb{R}$-base contenue dans L. Bien sûr, il n'y a pas de raisons pour que ces vecteurs forment une $\mathbb{Z}$-base de L. Soit W le sous-espace vectoriel de $\mathbb{R}^n$ engendré par $\{e_1, e_2, \ldots, e_{n-1}\}$. Clairement, W est de dimension $n-1$; soit ϵ_n une base de $W^\perp$. Soit $M := L \cap W$. Alors M est un sous-groupe de W, qui est discret dans W puisque L l'est. En identifiant W et $\mathbb{R}^{n-1}$, on peut trouver par récurrence une base $\{b_1, b_2, \ldots, b_{n-1}\}$ de M, qui soit une $\mathbb{R}$-base de W. D'autre part, tout élément $x \in L$ s'écrit $x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda_n \epsilon_n$. Les λ_i ne sont pas des entiers à priori. Considérons

$$\Lambda := \{\lambda \in \mathbb{R} \mid \text{ il existe } x \in L \mid x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda \epsilon_n\}.$$

Clairement, Λ est un sous-groupe de $\mathbb{R}$; montrons qu'il est discret. Supposons par l'absurde que $\Lambda \cap [a, b]$ soit infini. Chaque $\lambda \in \Lambda \cap [a, b]$ est associé à un $x \in L$ avec $x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda \epsilon_n$. Quitte à soustraire $[\lambda_i] b_i$, qui appartient à L, on peut se ramener à $0 \leq \lambda_i < 1$. Alors x appartient à un ensemble compact K; on aurait donc $K \cap L$ infini, ce qui contredit l'hypothèse suivant laquelle L est discret. On peut donc conclure qu'il existe $a > 0$ tel que $\Lambda = a\mathbb{Z}$ (c'est le cas $n = 1$). Soit alors $b_n \in L$ tel que

$$b_n = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + a\epsilon_n. \tag{3.5}$$

Nous allons montrer que $\{b_1, b_2, \ldots, b_n\}$ est une base de L. D'abord, par construction, $\{b_1, b_2, \ldots, b_n\}$ forme une famille libre sur $\mathbb{R}$, donc à fortiori sur $\mathbb{Z}$. Il

reste à montrer qu'elle engendre L. Soit donc $x \in L$ quelconque. On peut écrire x comme combinaison linéaire des b_i *à coefficients réels*; $x = x_1 b_1 + \cdots + x_n b_n$. En remplaçant b_n par son expression (3.5), on voit que $x_n a \in \Lambda = a\mathbb{Z}$, donc que $x_n \in \mathbb{Z}$. Alors $y := x - x_n b_n$ appartient à $M = L \cap W$, donc on a aussi $x_1, \ldots, x_{n-1} \in \mathbb{Z}$.

□

Corollaire 1 *Si L est un réseau de $\mathbb{R}^n$, tout sous-$\mathbb{Z}$-module M contenu dans L et de rang n est un réseau. En particulier, M possède une $\mathbb{Z}$-base.*

Si L et M sont deux réseaux de $\mathbb{R}^n$, tels qu'il existe un entier k tel que $kM \subset L$, alors $L \cap M$ et $L + M$ sont aussi des réseaux.

Preuve: Si $M \subset L$ et si L est un réseau, alors M est discret. La première assertion résulte directement du théorème précédent.

Les inclusions $kM \subset L \cap M \subset M$ montrent que d'une part $L \cap M$ est de rang n et d'autre part est un sous-module de L. Donc $L \cap M$ est un réseau.

Montrons maintenant qu'il existe un entier l tel que $L + M \subset \frac{1}{l} M$, et par le même argument on pourra conclure que $L + M$ est un réseau. Choisissons une base $e_1, \ldots, e_n$ de L et une base $f_1, \ldots, f_n$ de M. Soit P la matrice de passage exprimant $f_1, \ldots, f_n$ sur $e_1, \ldots, e_n$. Comme $kM \subset L$, la matrice kP est à coefficients entiers. Donc la matrice P^{-1} est à coefficients rationnels. Il existe un entier l tel que lP^{-1} soit à coefficients entiers; alors $lL \subset M$, et $L + M \subset \frac{1}{l} M$.

□

3.2.4 Algorithme LLL

LLL=Lenstra, Lenstra, Lovacz (1982).

Définition 16 *Avec les notations du paragraphe précédent, une base $\{b_1, \ldots, b_n\}$ d'une réseau L est dite* LLL réduite *si elle vérifie les conditions suivantes:*

1. $|u_{i,j}| \leq 1/2$ *pour tout* $j < i$.
2. *Pour tout* $i \geq 2$, $a_i^2 \geq (3/4 - u_{i,i-1}^2) a_{i-1}^2$.

Le théorème suivant mesure la "qualité" d'une base LLL-réduite.

Théorème 12 *Soit $\{b_1, \ldots, b_n\}$ une base LLL-réduite. Alors:*

1. $\det(L) \leq \prod_{i=1}^{n}(b_i \cdot b_i) \leq 2^{\frac{n(n-1)}{2}} \det(L)$
2. $b_j \cdot b_j \leq 2^{i-1} a_i^2$ *pour tout* $j \leq i$
3. $b_1 \cdot b_1 \leq 2^{\frac{n-1}{2}} \det(L)^{1/n}$
4. $b_1 \cdot b_1 \leq 2^{n-1} \min(L)$

Preuve: La relation (3.3) montre que $b_i \cdot b_i \geq a_i^2$ ce qui montre que

$$\det(L) = \prod_{i=1}^{n} a_i^2 \leq \prod_{i=1}^{n} b_i \cdot b_i.$$

Les conditions 1. et 2. de réduction LLL montrent que

$$a_i^2 \geq a_{i-1}^2/2,$$

et donc par induction que

$$a_i^2 \geq a_j^2/2^{i-j}, \text{ pour tout } i > j. \tag{3.6}$$

En remplaçant dans (3.3), on obtient

$$b_i \cdot b_i \leq (1 + 1/4(2 + 2^2 + \cdots + 2^{i-1}))a_i^2 = \frac{2^{i-1}+1}{2} a_i^2 \leq 2^{i-1} a_i^2$$

ce qui démontre les points 1. et 2.

D'autre part, $b_1 \cdot b_1 = a_1^2 \leq 2^{i-1} a_i^2$ (par (3.6)). En multipliant membre à membre, on obtient

$$(b_1 \cdot b_1)^n \leq 2^{\frac{n(n-1)}{2}} \det(L)$$

soit le point 4.

Soit $x \in L$, $x \neq 0$. On peut écrire d'une part $x = x_1 b_1 + \cdots + x_n b_n$ avec les x_i entiers, d'autre part $x = \lambda_1 b_1^* + \cdots + \lambda_n b_n^*$ avec les λ_i réels. Soit i_0 le plus grand indice tel que $\lambda_{i_0} \neq 0$. Alors: $\lambda_{i_0} = x_{i_0}$, et

$$x \cdot x = \lambda_{i_0}^2 a_{i_0}^2 + \sum_{j<i_0} \lambda_j^2 a_j^2 \geq a_{i_0}^2 \geq b_1 \cdot b_1 / 2^{i_0 - 1}$$

où la dernière inégalité se déduit de (3.6). En prenant $x \in S(L)$ et en utilisant $i_0 \leq n$, on obtient bien l'inégalité du point 5.

Remarque 1 *On peut définir des conditions de réduction d'une base d'un réseau plus fortes, mais la réduction LLL est la seule pour laquelle un algorithme polynomial construit une base LLL-réduite à partir d'une base quelconque. D'autre part, dans la pratique, la norme des vecteurs obtenus par réduction LLL est meilleure que la borne théorique du théorème précédent. Nous allons maintenant décrire cet algorithme.*

Algorithme LLL: il prend en entrée une base $\{b_1, \ldots, b_n\}$ d'un réseau L, et sort une base $\{b'_1, \ldots, b'_n\}$ de ce même réseau, LLL-réduite.

Supposons que les $k-1$ premiers vecteurs $b_1, b_2, \ldots, b_{k-1}$ vérifient les conditions de réduction LLL. On suppose avoir calculé les coefficients $u_{i,j}$ pour $i \leq j \leq k-1$ ainsi que les a_i^2 pour $1 \leq i \leq k-1$.

On s'occupe d'abord de la condition 1., qui est facile à obtenir. En effet, supposons que l'on remplace le vecteur b_k par un vecteur de la forme $b_k - qb_l$ avec $l < k$ et q entier. Alors:

- Le réseau engendré par $b_1, \ldots, b_k$ reste le même
- L'orthogonalisation de Gram-Schmidt $b_1^*, \ldots, b_k^*$ reste la même
- Les coefficients $u_{k,k}, \ldots, u_{k,l+1}$ sont inchangés; $u_{k,l}$ est remplacé par $u_{k,l} - q$.

Le dernier point est conséquence de l'égalité: $b_k - qb_l = \sum_{j=1}^{k}(u_{k,j} - qu_{j,l})b_j^*$. Ainsi, on voit que l'on peut obtenir successivement les conditions: $|u_{k,k-1}| \leq 1/2$ en remplaçant b_k par $b_k - \lfloor u_{k,k-1} \rceil b_{k-1}$, puis $|u_{k,k-2}| \leq 1/2$ en remplaçant b_k par $b_k - \lfloor u_{k,k-2} \rceil b_{k-2}$, et ainsi de suite.

RED(k,l) est la procédure qui remplace b_k par $b_k - \lfloor u_{k,l} \rceil b_l$, et met à jour les coefficients $u_{k,j}$ pour $j \leq l$.

Ainsi, pour obtenir la condition 1., il faut exécuter successivement
RED(k,k-1), RED(k,k-2), jusqu'à RED(k,1). Mais il faut remarquer que la condition 2. peut être testée dès que RED(k,k-1) est exécutée, puisque ensuite le coefficient $u_{k,k-1}$ ne bouge plus.

On procède donc de la façon suivante: on exécute RED(k,k-1), puis, juste après, on teste la condition 2. Si elle est vérifiée, on exécute RED(k,k-2), ..., RED(k,1) puis on passe bien sûr au vecteur suivant b_{k+1}.

Si elle n'est pas vérifiée: on échange b_k et b_{k-1} et on redescend au cran précédent. Remarquer qu'après cet échange, on a toujours une base de L. Par

contre, seulement les $k-2$ premiers vecteurs sont LLL-réduits. D'autre part, b^*_{k-1} est modifié.

SWAP(k) est la procédure qui échange b_{k-1} et b_k, et met à jour les b^*_i et les coefficients $u_{i,j}$. Les vecteurs $b^*_1, \ldots, b^*_{k-2}$ n'ont pas bougé, ni les $u_{i,j}$ pour $i \leq k-2$. Comme

$$b_k = b^*_k + u_{k,k-1}b^*_{k-1} + u_{k,k-2}b^*_{k-2} + \ldots,$$

b^*_{k-1} est remplacé par $b^*_k + u_{k,k-1}b^*_{k-1}$, et les coefficients $u_{k-1,j}$ par $u_{k,j}$ pour $j < k-1$.

Preuve de l'algorithme: Il est clair que, si cet algorithme termine, il sort bien une base LLL-réduite.. Ce qui n'est pas du tout évident, c'est qu'il termine bien, c'est-à-dire qu'il ne poursuit pas indéfiniment une succession de montées et de descentes dans les indices de 1 à n. Il faut donc démontrer qu'il ne passe par la procédure SWAP qu'un nombre fini de fois.

Posons $L_k = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_k$ et $D_k = \det(L_k)$. On a, en vertu de (3.4), $D_k = \prod_{i=1}^k a_i^2$. La valeur prise par le n-uplet $(D_1, D_2, \ldots, D_n)$ ne change que dans la procédure SWAP. Lors de l'échange de b_{k-1} et b_k, les réseaux L_1,...,L_{k-2} sont inchangés, ainsi que L_k,...,L_n. Seul L_{k-1} est modifié. Plus précisément, on garde b^*_1,...,b^*_{k-2}, et b^*_{k-1} devient ${b'_{k-1}}^* = b^*_k + u_{k,k-1}b^*_{k-1}$, donc a^2_{k-1} devient ${a'_{k-1}}^2 = a^2_k + u^2_{k,k-1}a^2_{k-1}$. Donc D_{k-1} est remplacé par

$$D'_{k-1} = D_{k-1}\frac{a^2_k + u^2_{k,k-1}a^2_{k-1}}{a^2_{k-1}}.$$

Mais justement, si on passe dans SWAP, c'est parce que la condition 2. de réduction LLL n'est pas vérifiée, c'est-à-dire parce que

$$a^2_k < (3/4 - u^2_{k,k-1})a^2_{k-1},$$

soit

$$\frac{a^2_k + u^2_{k,k-1}a^2_{k-1}}{a^2_{k-1}} < \frac{3}{4}.$$

On a donc: $D'_{k-1} < \frac{3}{4}D_{k-1}$.

Ainsi, chaque passage par SWAP multiplie le produit $D_1D_2 \ldots D_n$ par un facteur $3/4$. Il suffit donc de montrer que ce produit est minoré par une constante ne dépendant que du réseau L.

Proposition 12 *Si L est un réseau de dimension n, le quotient*

$$\gamma(L) := \frac{\min(L)}{\det(L)^{1/n}}$$

est majoré par une constante ne dépendant que de n.

Preuve: En effet, ce quotient mesure la densité Δ de l'empilement de sphères associé à L. Soit $r = \sqrt{\min(L)}/2$. Les sphères de centre les points du réseau L et de rayon r sont d'intérieurs disjoints (c'est le plus grand rayon possible..). Soit $\mathcal{E}$ la réunion de ces sphères et soit $\mathcal{P}$ le parallélotope construit sur une base $\{b_1, \ldots, b_n\}$:

$$\mathcal{P} = \{x_1 b_1 + \cdots + x_n b_n \mid 0 \leq x_i \leq 1\}.$$

Le volume de $\mathcal{P}$ est égal à $\sqrt{\det(L)}$. Le volume de $\mathcal{P} \cap \mathcal{E}$ est égal au volume d'une sphère de rayon r, c'est-à-dire à $r^n \pi_n$ où π_n est le volume de la sphère de rayon 1 et de dimension n. On a bien sûr

$$\Delta = \frac{\mathrm{vol}(\mathcal{P} \cap \mathcal{E})}{\mathrm{vol}(\mathcal{P})} \leq 1$$

soit

$$\frac{r^n \pi_n}{\sqrt{\det(L)}} \leq 1$$

ou encore

$$\left(\frac{\min(L)}{\det(L)^{1/n}}\right)^{n/2} \frac{\pi_n}{2^n} \leq 1.$$

□

Terminons maintenant la démonstration de l'algorithme LLL: La proposition précédente montre que

$$\gamma_k := \sup_{L \subset \mathbb{R}^k} \gamma(L)$$

est fini. On a donc, pour les réseaux L_k,

$$D_k \geq \left(\frac{\min(L_k)}{\gamma_k}\right)^k \geq \left(\frac{\min(L)}{\gamma_k}\right)^k$$

et le produit $D_1 \dots D_n$ est bien minoré par une constante positive ne dépendant que du réseau L.

□

3.2.5 Applications

L'algorithme LLL permet de résoudre des problèmes, qui peuvent se ramener à la recherche de petits vecteurs dans un réseau. Initialement, les trois auteurs ont obtenu grâce à lui un algorithme polynomial pour la factorisation des polynômes à coefficients entiers. Ce sujet nous entrainerait trop loin, nous décrivons maintenant quelques applications de LLL, notamment à la cryptographie.

Le problème du sac à dos L'un des premiers cryptosystèmes à clé publique proposé était basé sur le problème du sac à dos. Ce système a été "cassé" par l'algorithme LLL.

Soit $a_1, a_2, \dots, a_n$ et s des nombres entiers positifs. Il s'agit de répondre à la question:

Existe-t-il un sous-ensemble $I \subset \{1, \dots, n\}$ tel que $s = \sum_{i \in I} a_i$?

Ce problème est connu pour être NP-complet. Cela signifie que tout problème NP peut se réduire à celui-ci. En particulier, comme on pense que NP $\neq$ P, il n'aurait pas de solution polynomiale. Toutefois, il existe des cas particuliers pour lesquels il est très facile de répondre - on parle d'instances faibles.

Définition 17 *On dit que le sac à dos est à super-croissance si* $a_j > \sum_{i=1}^{j-1} a_i$ *pour tout* j.

Dans ce cas, il est trivial de reconnaitre si un entier s donné est ou non la somme d'un sous-ensemble des a_i. En effet, il suffit de procéder de la façon suivante (appelée em algorithme glouton):

- Déterminer le plus grand des a_i tel que $a_i \leq s$
- Remplacer s par $s - a_i$
- Recommencer tant que s n'est pas plus petit que tous les a_i.

Si, à la fin de la procédure, $s \neq 0$ c'est que s ne se décompose pas en sous-somme des a_i; sinon, c'est qu'on a effectivement trouvé une telle décomposition.

En effet, si $s = a_{i_1} + a_{i_2} + \dots a_{i_s}$, avec $a_{i_1} < a_{i_2} < \cdots < a_{i_s}$, on a bien $a_{i_s} \leq s$, et $s \leq \sum_{i=1}^{i_s} a_i < a_{i_s+1}$. Donc $a_{i_s} \leq s < a_{i_s+1}$, et a_{i_s} est bien le plus grand des a_i plus petits que s. Noter que, dans le cas d'un sac à dos à super-croissance, la décomposition si elle existe est unique.

Le cryptosystème proposé par Merkle et Hellmann en 1978 est le suivant: Alice veut envoyer un message confidentiel à Bob. Bob choisit un sac à dos à super-croissance $a_1, \dots, a_n$ ainsi que w et m, avec $m > \sum_{i=1}^{n} a_i$, et $(w, m) = 1$. Il calcule $b_i = a_i w \mod m$.

- La clé publique est: $b_1, b_2, \dots, b_n$
- La clé privée est: m, w.

Lorsque Alice veut envoyer un message $\epsilon_1, \dots, \epsilon_n$ avec $\epsilon_i = 0, 1$ à Bob, elle calcule $s := \sum_{i=1}^{n} \epsilon_i b_i$ et envoit s à Bob. Bob calcule sw^{-1} modulo m, puis résoud $sw^{-1} = \sum_{i=1}^{n} \epsilon_i a_i$ suivant l'algorithme glouton. Un attaquant est confronté au pb de résoudre $s = \sum_{i=1}^{n} \epsilon_i b_i$ pour le sac à dos donné par $b_1, \dots, b_n$ qui n'est plus à croissance rapide. Merkle et Hellmann proposent comme choix de paramètres $a_1 \simeq 2^n, a_2 \simeq 2^{n+1}, \dots, a_n \simeq 2^{2n}$.

Lagarias et Odlysko ont montré comment utiliser LLL pour résoudre une certaine famille de sac à dos: les sac à dos de basse densité.

Définition 18 *La densité d'un sac à dos $a_1, a_2, \dots, a_n$ est la valeur $d = n/\log(\max(a_i, 1 \leq i \leq n))$.*

À $a_1, a_2, \dots, a_n, s$ on associe le réseau L de dimension $n+1$ de $\mathbb{R}^{n+2}$ engendré par les colonnes de la matrice:

$$B = \begin{pmatrix} Ka_1 & Ka_2 & \dots & Ka_n & -Ks \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Si on note $e_1, e_2, \dots e_{n+1}$ les colonnes de B, et si $x = \sum_{i=1}^{n} x_i e_i \in L$, on a

$$x \cdot x = x_1^2 + x_2^2 + \cdots + x_{n+1}^2 + K^2(x_1 a_1 + \cdots + x_n a_n - x_{n+1} s)^2.$$

Une solution du sac à dos $s = \sum_{i=1}^{n} \epsilon_i a_i$ correspond à un vecteur $x = \epsilon_1 e_1 + \cdots + \epsilon_n e_n + e_{n+1}$ appartenant à L, avec $x \cdot x = wt(\epsilon) + 1 \leq n+1$. Quitte à changer s en $\sum_{i=1}^{n} a_i - s$, on peut même se ramener à $x \cdot x \leq (n+1)/2$. Si on choisit K tel que $K^2 > (n+1)/2$, tout vecteur $x = \sum_{i=1}^{n} x_i e_i$ de L vérifiant $x \cdot x \leq (n+1)/2$ est tel que: $x_1 a_1 + \cdots + x_n a_n = x_{n+1} s$. L'idée est donc de rechercher par LLL des vecteurs de petite norme dans ce réseau, qui auront de bonnes chances de fournir une solution au sac à dos.

Plus rigoureusement, on peut montrer que, si le sac à dos est de basse densité, la probabilité d'existence d'un vecteur du réseau de norme inférieure à $(n+1)/2$, qui n'est pas une solution du sac à dos (i.e. dont le coefficients ne sont pas des 0 et des 1), tend vers 0 quand n tend vers $+\infty$.

Relations de dépendance linéaire ou algébrique: soit $z_1, \ldots, z_n \in \mathcal{C}$ des nombres complexes. On cherche une relation de dépendance $x_1 z_1 + \cdots + x_n z_n = 0$ avec les x_i entiers. Par exemple, si les z_i sont les puissances successives d'un même nombre algébrique α, cela revient à chercher un (multiple du) polynôme minimal de α. On considère la forme quadratique sur $\mathbb{Z}^n$

$$q(x) = x_1^2 + \cdots + x_n^2 + N \mid x_1 z_1 + \cdots + x_n z_n \mid^2 .$$

Pour N assez grand, les $x \in \mathbb{Z}^n$ tels que $q(x)$ soit petit vont certainement vérifier $x_1 z_1 + \cdots + x_n z_n = 0$. Par l'algorithme LLL, on réduit la base canonique de $\mathbb{Z}^n$, et les vecteurs de la base réduite contiennent très probablement des petits vecteurs, vérifiant $x_1 z_1 + \cdots + x_n z_n = 0$ (remarquons que, une fois trouvés des x_i candidats, on peut toujours vérifier *à postériori* la relation). Cette méthode donne même un algorithme de factorisation des polynômes à coefficients dans $\mathbb{Z}$, en appliquant ce qui précède à une racine du polynôme.