Introduction à l'arithmétique

1 Corps finis

Définition 1.1. *Un anneau R est un ensemble muni de deux lois de composition $+$ et $\times$ telles que*
(i) $(R,+)$ est un groupe abélien. Son élément neutre est noté 0.
(ii) La multiplication $\times$ est associative
(iii) La multiplication est distributive : $a(b+c) = ab + ac$.
On dira
(a) Que l'anneau est commutatif si de plus la multiplication l'est.
(b) Que l'anneau est unitaire si de plus la multiplication possède un élément neutre.

Définition 1.2. *Un corps K est un anneau tel que $(K^*, \times)$ soit de plus un groupe. Par convention $K^* = K \setminus \{0\}$.*

Par convention, sauf mention explicite du contraire, *tous* les anneaux considérés seront commutatifs et unitaires.

Remarque 1.3. *Un anneau est nécéssairement non vide. Exercice : pourquoi ?*

Exemple 1.4. *L'anneau le plus important pour la théorie des nombres est $\mathbb{Z}$. D'autres exemples importants : $\mathbb{Z}[i], \mathbb{C}[X]$. L'anneau le plus simple est $(\{0\}, +, \times)$.*

Quelques anneaux courants $\mathcal{F}(\mathbb{R},\mathbb{R})$, $\mathcal{C}(\mathbb{R},\mathbb{R})$, $\mathcal{H}(\mathbb{R},\mathbb{R})$.

Des anneaux plus riches $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Remarque 1.5. *Un corps a nécessairement au moins deux éléments, $0, 1$.*

Proposition 1.6. *Soit R un anneau tel que $0 = 1$. Alors, $R = \{0\}$.*

Démonstration : Soit $a \in R$, alors, $0a + 0 = 0a = (0+0)a = 0a + 0a$. Par simplification,

$$0a = 0 \ .$$

On suppose maintenant que $0 = 1$. On a alors $a = 1a = 0a = 0$, donc $a = 0$. On a bien montré que $R = \{0\}$.

Proposition 1.7. *Soit R un anneau. Il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow R$.*

Démonstration : **(indications de démonstration, détails laissés en exercices)** Par définition, si φexiste, $\varphi(1) = 1$. Donc, par récurrence, en utilisant la définition d'un morphisme, $\varphi(n) = n1 = 1 + 1 + \cdots + 1$ (n fois). Ceci montre l'unicité de φ. On vérifie ensuite, que la définition $\varphi(n) = n1$ donne bien un morphisme d'anneau, et cela montre l'existence.

Définition 1.8. *La caractéristique d'un anneau est l'entier le plus petit entier strictement positif n tel que $n \in \ker(\varphi)$, s'il existe. Si aucun entier strictement positif n'appartient à $\ker(\varphi)$ on dit que l'anneau est de caractéristique nulle (égale à zéro). On la note $\mathrm{Car}(R)$.*

On suppose désormais dans cette partie que K est un corps fini.

Lemme 1.9. *La caractéristique de K est un nombre premier.*

Démonstration : on sait que la caractéristique n de K ne peut pas être nulle (car sinon φ serait injective et par suite K infini). Supposons que n n'est pas premier et soit $n = md$ avec $m, d \neq 1$. Alors

$$0 = \varphi(n) = \varphi(md) = \varphi(m)\varphi(d).$$

Comme K est un corps, $\varphi(m) = 0$ ou $\varphi(d) = 0$, contredisant la définition de n.

Proposition 1.10. *Soit K un corps fini, de caractéristique p. Il existe un entier $r \geq 1$ tel que le cardinal de K soit*

$$\#K = p^r \ .$$

Démonstration : par factorisation $\mathbb{Z}/\ker(\varphi) \simeq \mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ s'identifie à un sous-corps de K (car c'est un sous anneau). Comme $\mathbb{F}_p$ est un sous-corps de K, il s'ensuit (voir la multiplication par un élément de $\mathbb{F}_p$ comme une loi externe) que K est un $\mathbb{F}_p$-espace vectoriel.

Comme K est fini, il est *a fortiori* un K-espace vectoriel de dimension finie. Par suite,

$$\#K = p^{\dim_{\mathbb{F}_p}(K)} \ .$$

Exemple 1.11. *Posons $K = \mathbb{F}_2[X]/(X^2 + X + 1)$. Comme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ (exercice pourquoi ?), K est un corps. Son cardinal est 4. Si l'on α la classe de X dans le quotient, d'un point de vue ensembliste, $K = \{0, 1, \alpha, 1 + \alpha\}$.*

Nous allons maintenant démontrer un théorème qui contient l'essentiel des propriétés importantes des corps finis

Théorème 1.12. *Soit p un nombre premier et $r \geq 1$ un entier. Posons $q = p^r$. Alors*

(i) Il existe un corps de cardinal q.
(ii) Tous les corps de cardinal q sont isomorphes (on notera cet unique corps à isomorphisme près $\mathbb{F}_q$).
(iii) Le groupe multiplicatif K^* est cyclique.
(iv) D'un point de vue ensembliste, $K = \{\text{Racines de } X^q - X = 0\}$.
(v) Tout polynôme irréductible de degré r sur $\mathbb{F}_p$ est un facteur (simple) de $X^q - X$.
(vi) Les facteurs irréductibles de $X^q - X$ sont les polynômes irréductibles sur $\mathbb{F}_p$ de degré r' divisant r.
(vii) Un corps $\mathbb{F}$ de cardinal q' est contenu dans $\mathbb{F}_q$ (à isomorphisme près) si et seulement si $q' = p^k$ avec $k \mid r$.

Remarque 1.13. *Bien que K^* soit cyclique il n'est pas évident en pratique d'en trouver explicitement un générateur.*

Exemple 1.14. *$q = 4$, on a sur $\mathbb{F}_2$, $X^4 - X = X(X - 1)(X^2 + X + 1)$.*

Exemple 1.15. *$X^8 - X = X(X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$. En tant qu'espace vectoriel (sur $\mathbb{F}_2$), $\mathbb{F}_8$ a pour base $1, \beta, \beta^2$, où β ets une racine de $X^3 + X + 1$. En tant qu'ensemble,*

$$\mathbb{F}_8 = \{0, 1, \beta, 1 + \beta, \beta^2, 1 + \beta^2, \beta^2 + \beta, 1 + \beta + \beta^2\} \ .$$

Exemple 1.16. $X^{16}-X = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$.

Démonstration : Soit K un corps de cardinal q. Par suite, K^* est de cardinal $q-1$ et donc tout élément $\alpha \in K^*$ vérifie $\alpha^{q-1} = 1$ (l'ordre d'un élément divise l'ordre du groupe), par suite, α est une racine de $X^{q-1}-1$, donc par multiplication de $X^q - X$. Comme zéro est également racine de ce polynôme, on voit qu'il a exactement q racines dans le corps K. Cela montre (iv).

Pour montrer (iii), nous allons montrer l'énoncé plus général suivant

Proposition 1.17. *Soit K un corps et H un sous groupe fini de K^* de cardinal n. Alors, H est cyclique et contient toutes les racines n-ièmes de l'unité.*

Démonstration : soit $\alpha \in K$ d'ordredivisant n, donc $\alpha^n - 1 = 0$, mais ce polynôme contient déjà tous les éléments de H (donc n éléments) mais a auplus n racines. Il ne peut donc y avoir de racines n-ièmes de l'unité dans $K \setminus H$. Il nous faut encore montrer la partie la plus importante, à savoir que H est cyclique. Comme H est un groupe abélien, par le théorème de structure, on a un isomorphisme unique

$$H \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \ ,$$

avec $d_1 \mid \cdots \mid d_k$ et $n = d_1 \dots d_k$. En vertu de cette décomposition, pour tout élément $\alpha \in H$, $\alpha^{d_k} = 1$. Comme ce polynôme a au plus d_k racines, on en déduit l'inégalité

$$\#H \leq d_k \ ,$$

c'est-à-dire

$$d_1 \dots d_k \leq d_k \ .$$

Donc, $k = 1$ et H est cyclique.

Existence d'un corps à q éléments On sait, à supposer qu'un tel corps existe que ses éléments sont les racines de $X^q - X$. On va donc partir de ce constant pour notre construction. On admet provisoirement le lemme suivant

Lemme 1.18. *Soit K un corps et $P \in K[X]$, il existe un corps L contenant K tel que P soit scindé sur L.*

Notre stratégie est donc la suivante. On part de $\mathbb{F}_p$, on prend un corps contenant toutes les racines de $X^q - X$ et on «espère» que l'ensemble des racines forme un sous-corps de L.

Proposition 1.19. *Soit p un nombre premier, $r \geq 1$ et $q = p^r$. Alors*
(i) Le polynôme $X^q - X$ n'a pas de racines multiples sur un corps de caractéristique p.
(ii) Soit L un corps de caractéristique p, $K = \{x \in L, x^q - x = 0\}$ est un sous coprs de L.

Cette proposition, jointe au lemme précédent montre l'existence d'un corps à q éléments.

On admet aussi provisoirement le lemme

Lemme 1.20. *Si P, P' n'ont pas de facteurs en commun, alors P n'a pas de facteurs d'ordre ≥ 2.*

Nous pouvons maintenant démontrer la proposition. **Démonstration** : (proposition) la dérivée de $X^q - X$ est $qX^{q-1} - 1 = -1$ donc P, P' n'ont pas de racines communes, cela montre (i).

Soient α, β des racines de $X^q - X$ dans L. Alors $(\alpha\beta)^q = \alpha^q \cdot \beta^q = \alpha \cdot \beta$. Donc $\alpha\beta$ est aussi racine de $X^q - 1$. L'ensemble des racines de $X^q - X$ est donc stable par multiplication. De même$\alpha^{-q} = \alpha^{-1}$, donc α^{-1}. Donc l'ensemble de $X^q - X$ privé de zéro est un sous groupe multiplicatif de L^*. Reste la stabilité pour l'addition.

Proposition 1.21. *Soit L un coprs de caractéristique p, considérons $x^q + y^q \in L[x, y]$. On a $x^q + y^q = (x + y)^q$.*

Démonstration : si $q = p$ (c'est-à-dire si $r = 1$), cela suit trivialement de la formule du binôme. On démontre le cas général par récurrence sur r.

$$(x+y)^q = (x+y)^{p^{r-1}.p} = \left((x+y)^{p^{r-1}}\right)^p = \left(x^{p^{r-1}} + y^{p^{r-1}}\right)^p = x^q + y^q$$

(la troisième égalité vient de l'hypothèse de récurrence, la dernière du cas $r = 1$).

En appliquant la proposition, on en déduit que si α, β sont des racines de $X^q - X$, alors $\alpha + \beta$ aussi et donc, cet ensemble est stable par addition (la stabilité par multiplication par -1 se vérifie de la même manière).

Nous avons donc montré également le (i) du théorème.

Nous suppons maintenant donnés deux corps K, K' tels que

$$\#K = \#K' = q \ .$$

Soit α un générateur du groupe cyclique K^*. On a *a fortiori*

$$K = \mathbb{F}_p(\alpha) \ .$$

On note f le polynôme minimal de α sur $\mathbb{F}_p$. On en déduit

$$K \simeq \mathbb{F}_p(X]/(f) \ .$$

Comme $\alpha^q - \alpha = 0$, on dispose de la divisibilité (et f est un facteur irréductible)

$$f \mid X^q - X \ .$$

Soit maintenant dans K' une racine α' de f (un tel α' existe car $f \mid X^q - X$). On a les isomorphismes

$$K \simeq \mathbb{F}_p[X]/(f) \simeq \mathbb{F}_p(\alpha') \subset K' \ .$$

Mais comme K et K' ont même cardinal, la dernière inclusion est une inégalité. On a donc bien montré

$$K \simeq K' \ .$$

Soit maintenant f un polynôme irréductible de degré r sur $\mathbb{F}_p[X]$, et α une racine de f dans une extension appropriée L de $\mathbb{F}_p$. Par la construction précédente, $K = \mathbb{F}_p(\alpha)$ est un sous-corps de L de cardinal $q = p^r$.

Comme α est aussi une racine de $X^q - X$ (point (iv) du théorème), il est racine du pgcd [1].

Toutefois, f est irréductible donc $\mathrm{PGCD}(f, X^q - X) = f$.

On a maintenant

1. Le pgcd est l'abréviation de plus grand commun diviseur.

Lemme 1.22. *Soit k un entier divisant r, disons $r = ks$. On pose $q = p^r, q' = p^k$. Alors, $X^{q'} - X \mid X^q - X$ sur $\mathbb{F}_p[X]$. En particulier, si f est irréductible de degré k divisant r, il divise aussi $X^{q'} - X$ donc $X^q - X$.*

Démonstration : on rappelle

$$Y^d - 1 = (Y - 1)(Y^{d-1} + \cdots + 1) \ .$$

On pose d'abord $Y = q'$ et $d = s$. La formule précédente montre que $q' - 1$ divise $q'^d - 1 = q'^s - 1 = q - 1$. On pose ensuite $Y = x^{q'-1}$ et $d = \frac{q-1}{q'-1}$.

On en déduit que $Y^{q'-1} - 1$ divise $Y^{q-1} - 1$. On multiplie à gauche et à droite par x. CQFD $\square$[2].

Nous avons donc bien montré que tout polynôme de degré divisant r est un facteur de $X^q - X$. Inversement, supposons que f est irréductiblre de degré k, k ne divisant pas r.

Alors, f n'a pas de racines dans K. En effet, notons d'abord que $K = \mathbb{F}_p[X]/(g)$, avec g irréductible de degré r. Si f avait une racine β dans K, $\mathbb{F}_p(\beta) \simeq \mathbb{F}_p[X]/(g)$ est un sous-corps de K donc K est un $\mathbb{F}_p(\beta)$ espace vectoriel de simension s, donc

$$q = p^r = (p^k)^s \ ,$$

ce qui entraîne

$$r = ks \ .$$

Ainsi, si $k \nmid r$ $\mathbb{F}_{p^k}$ n'est pas un sous-corps de $\mathbb{F}_{p^r}$. Inversement, si $k \mid r$ le lemme précédent nous montrer que le polynôme $X^{q'} - X$ a toutes ses racines dans le corps $\mathbb{F}_q$, donc ce corps à q' éléments.

Preuve des lemmes admis

Lemme 1.23. *Soit F un corps, $f \in F[X]$ unitaire. Il existe une extension K de F tel que f est produit de facteurs linéaires sur K.*

Démonstration : si $\deg(f) = 1$, il n'y a rien à dire. Supposons par hypothèse de récurrence que la propriété est vraie en tout degré $< r$. On choisit une facteur irréductible g de f (il n'est pas interdit que $g = f$), et l'on pose $K = F[X]/(g)$; c'est une corps et f admet une racine $\alpha = \dot{X}$ dans K, donc la factorisation en facteurs irréductibles de f est composée de facteurs de degrés $< r$.

Lemme 1.24. *Soit F un corps, $f \in F[X]$ et $\alpha \in F$. Alors, $(X - \alpha)^2 \mid f$ si et seulement si $f(\alpha) = f'(\alpha) = 0$.*

Démonstration : si $f(\alpha) = 0$, $f(X) = (X - \alpha)g(X)$. L'élément α est une double de g si et seulement si α est une racine multiple de f. Mais

$$f'(X) = g(X) + (X - \alpha)g'(X) \ .$$

On fait $X = \alpha$, donc $f'\alpha) = g(\alpha)$ donc $f'(\alpha) = 0$ si et seulement si $g(\alpha) = 0$.

Proposition 1.25. *Soit f un polynôme de $F[X]$ et F un corps. Alors, il y a une extension K de F dans laquelle f a une racine double si et seulement si* $\mathrm{PGCD}(f, f') \neq 1$.

2. CQFD ce qu'il fallait démontrer.

Démonstration : par le lemme précédent, s'il y a une racine double, ils ne sont pas premiers entre eux, donc pas premiers entre eux sur une extension. Inversement, si $g \mid \mathrm{PGCD}(f, f')$, ils ont une racine commune dans une extension de F.

Proposition 1.26. *Soit f irréductible, alors f n'a pas de racines multiples (dans aucune extension) sauf si $f' = 0$ (en particulier, en caractéristique zéro, f n'a que des racines simples car la dérivée ne peut pas être nulle).*

Démonstration : exercice.

Exemple 1.27. *On pose $f(X) = X^{15} + aX^{10} + bX^5 + c$ considéré sur $\mathbb{F}_5$. On a $f'(X) = 0$. Exercice : vérifier qu'on peut trouver a, b tels que ce polynôme soit irréductible.*

Théorème 1.28. *Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre r , où $q = p^r$. Ce groupe est engendré par $F_p(x) = x^p$ (le morphisme de Frobenius).*

Démonstration : soit F_p le frobenius, et G le groupe cyclique engendré par F_p. Tout d'abord, F_p est un automorphisme (exercice : faire les détails), donc G est un sous-groupe du groupe des automorphismes.

On note k l'ordre de F_p, donc $F_p^k = \mathrm{Id}$. Donc tout $x \in \mathbb{F}_q$ est une racine de $X^{p^k} - X$. Comme cette équation a au plus p^k racines, on a $p^k \geq q$ c'est-à-dire

$$k \geq r \ .$$

Inversement, pas le théorème principal sur les corps finis,

$$\forall x \in \mathbb{F}_q, x^q - x = 0 \ .$$

Donc

$$k \leq r \ .$$

En conclusion, G est cyclique d'ordre r. Soit maintenant ψ un automorphisme de $\mathbb{F}_q$.

Si

$$\iota \mathbb{F}_p \hookrightarrow \overline{\mathbb{F}_p} \ ,$$

on sait que ι a au plus $[\mathbb{F}_q : \mathbb{F}_p]$ pronlongements, c'est-à-dire r prolongements, mais avec les puissances du Frobenius, on en a déjà trouvé r. Donc, $\psi \in G$.

Norme et trace

Soit $K \subset L$, $K = \mathbb{F}_q$, $q = p^r$ et $L = \mathbb{F}_{q'}$ avec $q' = q^s = p^{rs}$.

On définit la trace de L sur K par

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=0}^{s-1} x^{q^i} \ ,$$

$$\mathrm{N}_{L/K}(x) = \prod_{i=0}^{s-1} x^{q^i} \ .$$

On a

Proposition 1.29. *(i) La trace est une forme linéaire surjective.*
(ii) $\mathrm{Tr}(x^q) = \mathrm{Tr}(x)$.
(iii) La norme est un morphisme de groupes $L^* \longrightarrow K^*$ *surjectif et* $N(x)^q = N(x)$.

Démonstration : la linéarité de la trace est évidente (exercice) et il suffit de montrer qu'elle n'est pas identiquement nulle pour avoir la surjectivité (exercice). Maintenant $\mathrm{Tr}_{L/K}(\alpha) = 0$ si et seulement si α est une racine de $x + x^q + \cdots + x^{q^{s-1}}$ qui est de degré q^{s-1} donc ne peut s'annuler identiquement sur L qui a q^s éléments. Donc la trace est surjective. (ii) est évident, ainsi que le fait que la norme est un morphisme de groupes (exercices). Montrons la surjectivité, soit α un générateur de L^*. On a (somme géométrique)

$$N_{L/K}(\alpha) = \alpha^{\frac{q^s-1}{q-1}} \quad .$$

Comme α est d'ordre $q^s - 1$, $N_{L/K}(\alpha)$ est d'ordre $q - 1$. La dernière partie de la proposition est évidente (exercice).

Dénombrement

On note $I_q(n)$ le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$.

Théorème 1.30. *Pour tout $n \geq 1$, $I_q(n) > 0$.*

Démonstration : par le théorème sur les corps finis

$$q^n = \sum_{d|n} dI_q(d) \ .$$

Donc,

$$q^d = dI_q(d) + \sum_{d'|d, d'<d} d' I_q(d') \ .$$

En particulier

$$dI_q(d) \leq q^d \ .$$

On en déduit

$$\begin{array}{rcl} q^n & \leq & nI_q(n) + \sum_{d|n, d<n} q^d \\ & \leq & nI_q(n) + \sum_{k=0}^{n-1} q^k \\ & = & nI_q(n) + \frac{q^n-1}{q-1} \\ & < & nI_q(n) + q^n \ . \end{array}$$

En conclusion

$$I_q(n) > 0 \ .$$

Remarque 1.31. *Cela donne une autre démonstration de l'existence d'un coprs à q éléments.*

Théorème 1.32. *Pour tout $n \geq 1$,*

$$nI_q(n) = \sum_{d|n} \mu(d) q^{n/d} \ .$$

Rappel

Définition 1.33. *La fonction de Möbius est définie par $\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}$ avec les conditions*
(i) $\mu(n) = 0$ si n possède un facteur carré.
(ii) $\mu(n) = 1$) si n est le produit d'un nombre pair de nombres premiers (distincts).
(iii) $\mu(n) = -1$ sinon.

Lemme 1.34.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \ . \end{cases}$$

Lemme 1.35. *Soit G un groupe abélien et $f : \mathbb{N}^* \longrightarrow G$. On pose $g : \mathbb{N}^* \longrightarrow G$ par*

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

Alors,

$$f(n) = \sum_{d|n} \mu(d) g(n/d) \ .$$

Démonstration : (preuve du théorème en supposant les lemmes vrais) on applique juste la formule de Möbius.

Démonstration : (preuve des lemmes) Tout d'abord, on suppose $n \geq 2$, $n = p_1^{n_1} \dots p_r^{n_r}$. On trouve alors

$$\sum_{d|n} = \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^r \binom{r}{r} = (1-1)^n = 0 \ .$$

D'où le premier lemme. Passons au second.

On pose $\delta(r) = \sum_{k|r} \mu(k)$. On a donc par le premier lemme

$$f(n) = \sum_{d|n} \delta(d) f(n/d)$$

$$f(n) = \sum_{d|n} \sum_{k|d} \mu(k) f(n/d)$$

On pose maintenant $S_k = \{d \geq 1, k \mid d \text{ et } d \mid n\}$ (on suppose $k \mid n$). On voit donc que l'on dispose de la partition

$$\{(k,d), k \mid d, d \mid n\} = \bigsqcup_{k|n} \{(k,d), d \in S_k\} \ .$$

Donc,

$$f(n) = \sum_{k|n} \mu(k) \sum_{d \in S_k} f(n/d)$$

Si $k \mid n$,

$$\begin{array}{ccc} \{j \geq 1, j \mid n/k\} & \longrightarrow & S_k \\ j & \longmapsto & kj \end{array}$$

est une bijection. Par suite,

$$\sum_{d \in S_k} f(n/d) = \sum_{j|n/k} f(n/(kj)) \ .$$

Mais, pour tout $k \mid n$

$$g(n/k) = \sum_{j|n/k} f(n/kj) \ .$$

Polynômes cyclotomiques sur les corps finis

Proposition 1.36. *Soit K un corps fini, de cardinal q. Soit $n \geq 1$ un entier naturel premier à q. Les facteurs irréductibles de $\Phi_n(X)$ dans l'anneau $K[X]$ sont tous de même degré, égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\star$.*

En particulier, pour tout entier $n \geq 1$, les facteurs irréductibles de Φ_{q^n-1} dans $K[X]$ sont de degré n.

Remarque 1.37. *En faisant $n = 1$, on en déduit que Φ_{q-1} est scindé dans $K[X]$. On peut vérifier que chacune des racines de Φ_{q-1} est un générateur de $K^\star$.*

Démonstration : soit P un facteur irréductible de Φ_n dans $K[X]$ et soit $L = K[X]/(P)$ l'extension de K obtenue par adjonction d'une racine x de P. Notons que x est d'ordre n dans $L^\star$. En effet, par définition de x, $x^n = 1$, donc son ordre s divise n. Si $s < n$, alors, x est aussi racine de Φ_s, ce qui entraîne que x est une racine double de $X^n - 1$ puisque $\Phi_s \mid X^n - 1$; on, on a déjà vu que $X^n - 1$ n'a pas de facteur carré, en considérant sa dérivée.

Notons d le degré de P ; on a donc $[L : K] = d$, donc L est un corps fini de cardinal q^d. En particulier, puisque x n'est pas nul, $x^{q^d-1} = 1$. Par conséquent, n divise $q^d - 1$, c'est-à-dire

$$q^d = 1 \bmod n \ .$$

L'ordre de q dans $\mathbb{Z}/n\mathbb{Z}$ est donc un diviseur e de d. Mais, si $q^e = 1 \bmod n$, pour un diviseur e de d, alors $x^{q^e} = x$ et donc et x appartient au sous-corps K' de L de cardinal q^e, mais comme $K[x] = L$, $K' = L$ et donc par égalité des cardinaux, $e = d$.

La dernière remarque résulte de ce que l'ordre de q dans $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^\star$ est précisément n. En effet, $q, q^2, \ldots, q^{n-1}$ sont tous strictement plus petits que $q^n - 1$ et donc ne peuvent être congrus à 1 modulo $q^n - 1$ puisque $2 \leq q$. En revanche, $q^n = 1 \bmod (q^n - 1)$.

Lemme 1.38. *Soit K un corps de caractéristique p, et $n = mp^k$, avec $k \geq 1$ et m premier à p. Alors, sur $K[X]$, $\Phi_n = (\Phi_m)^{(p^k - p^{k-1})}$.*

Démonstration : on a $X^n - 1 = (X^m - 1)^{p^k}$ par la formule du binôme. Par ailleurs,

$$X^n - 1 = \prod_{d|n} \Phi_d \ ,$$

soit, en regrouppant,

$$X^n - 1 = \prod_{d|m} \prod_{i=0}^{k} \Phi_{dp^i} \ .$$

On suppose par récurrence la relation établie pour tout $s \leq n - 1$, ce qui donne

$$(X^m - 1)^{p^k} = \left(\prod_{d|m, d\neq m} \prod_{i=0}^{k} \Phi_{dp^i} \right) \left(\prod_{i=0}^{k-1} \Phi_{mp^i} \right) \Phi_n = \left(\prod_{d|m, d\neq m} \Phi_d^{p^k} \right) \Phi_m^{p^{k-1}} \Phi_n \ ;$$

l'assertion pour n suit alors en simplifiant l'équation. Comme il n'y a rien à dire pour les petites valeurs de n, le lemme est démontré.

Proposition 1.39. *Dans le cas général, si on ne suppose plus $(n,q)=1$, on a le même énoncé que ci-dessus en posant $m = n/p^{v_p(n)}$, où p est la caractéristique de K : les facteurs irréductibles de Φ_n sont de degré égal à l'ordre de q dans $(\mathbb{Z}/m\mathbb{Z})^\star$.*

Démonstration : le point où nous avons utilisé que $(n,q)=1$ est lorsque nous avons affirmé que x est d'ordre n. Ceci n'est évidemment plus vrai en général. Par exemple, si $n=p$, $X^p-1=(X-1)^p$ et donc Φ_p n'est rien d'autre que Φ_1^{p-1}. Pour avoir le cas général, il suffit donc de démontrer que si P est un facteur irréductible de Φ_n et $L=K[X]/(P)$ comme ci-dessus, l'ordre de la classe x de X dans L est exactement m. Tout d'abord, l'ordre de x divise n. Montrons qu'il divise m ; comme $x^{mp^{v_p(n)}}=1$, on a aussi $(x^m-1)^{p^{v_p(n)}}=0$ et donc $x^m=1$. Si l'ordre de x était strictement inférieur à m, on trouve une contradiction comme ci-dessus en montrant qu'alors X^m-1 aurait un facteur carré (on utilise le lemme 1.38 pour assurer que x est racine de Φ_m), ce qui est impossible puisque maintenant $(m,p)=1$.

Proposition 1.40. *Soit n un entier ≥ 1 ; il existe une infinité de nombres premiers $\equiv 1 \bmod n$.*

Démonstration : dire que $p \equiv 1 \bmod n$ reviens à dire que p est d'ordre 1 dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\star$, et donc par l'énoncé précédent que Φ_n est scindé sur $\mathbb{F}_p$. En d'autres termes, Φ_n a toutes ses racines dans $\mathbb{F}_p$. On en déduit qu'il existe un entier $k \in \mathbb{Z}$ tel que $\Phi_n(k) \equiv 0 \bmod p$.

Supposons maintenant que l'ensemble des nombres premiers $\equiv 1 \bmod n$ est majoré par N, et considérons $\Phi_n(m!)$ pour $m \geq N$; pour m assez grand, on sait que ce nombre n'est pas nul. Soit p un nombre premier divisant $\Phi_n(m!)$; d'après ce qui précéde, on sait que $p \equiv 1 \bmod n$ et donc $p \leq N$ et donc $p \mid m!$. Par suite, le terme constant de Φ_n est divisible par p ; ce qui n'est pas possible puisqu'il vaut 1.

Pour construire explicitement un corps fini K à $q=p^n$ éléments, il suffit de trouver un polynôme irréductible P de degré n à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ et de poser $K=\mathbb{Z}/p\mathbb{Z}[X]/(P)$. D'après la proposition précédente, on peut se contenter de trouver un facteur irréductible du polynôme cyclotomique Φ_{p^n-1}. D'un point de vue théorique, on retrouve l'existence d'un corps fini de cardinal p^n . D'un point de vue pratique, l'intérêt de cette construction est double : tout d'abord, dans la base $(1,x,\ldots,x^{n-1})$ de l'algèbre K sur $\mathbb{Z}/p\mathbb{Z}$, la table de multiplication est assez simple ; ensuite, x est un générateur du groupe multiplicatif $K^\star$. Mais factoriser en général un polynôme reste une question qui n'est pas facile, même si elle est plus simple sur un corps fini.

Théorème 1.41. *Soit K un corps non nécessairement commutatif, de cardinal fini. Alors, K est commutatif.*

Démonstration : notons Q le cardinal de K. L'homomorphisme naturel de $\mathbb{Z}$ dans K n'est pas injectif ; son image est un sous-anneau de K, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Pour $x \in K$, notons C_x l'ensemble des éléments $y \in K$ tels que $xy=yx$ (le commutant de x). C'est un sous-anneau de K ; de plus, si $y \in C_x$ n'est pas nul, alors $y^{-1}x = xy^{-1}$, donc $y^{-1} \in C_x$. Cela démontre que C_x est un sous-corps de K. L'intersection des C_x (c'est-à-dire le centre de K) est un aussi sous-corps Z de K qui contient le sous-corps $\mathbb{F}_p$. Nous devons montrer que $Z=K$.

Notons q le cardinal de Z. Considérons alors K comme un espace vectoriel sur Z ; on voit ainsi que le cardinal de K est une puissance de q, disons $Q=q^n$. De même, pour tout $x \in K$, le cardinal q_x de C_x est une puissance de q, notée $q_x = q^{m(x)}$. On a $m(x)=1$ si x appartient au centre de K,

et $m(x) > 1$ sinon. Considérons aussi K comme un espace vectoriel sur le sous-corps C_x ; ainsi, Q est une puissance de q_x pour tout x et il existe un entier $n(x)$ tel que $n = n(x)m(x)$.

Faisons opérer le groupe $K^\star$ sur K (en tant qu'ensemble) par conjugaison. Le stabilisateur d'un élément $x \in K$ est l'ensemble $C_x^\star$ des éléments non-nuls de C_x. Pour que l'orbite d'un élément x soit un singleton, il faut et il suffit que x appartienne au centre Z de K. Soient alors $x_1, \ldots, x_e$ des représentants des orbites de K qui ne sont pas des singletons. L'orbite $\mathcal{O}(x_i)$ de x_i est un sous-groupe de $K^\star$ isomorphe au groupe quotient $K^\star/C_{x_i}$. L'équation aux classes, qui traduit le fait que l'on obtient une partition de K par les orbites, s'écrit donc

$$q^n = q + \sum_{i=1}^{r} \frac{q^n - 1}{q^{n(x_i)} - 1} \quad .$$

Le numérateur $q^n - 1$ se décompose en produit $\prod_{d|n} \Phi_d(q)$. De même, le dénominateur $q^{n(x_i)} - 1$ est égal au produit des $\Phi_d(q)$ où cette fois, d parcourt l'ensemble des diviseurs de $n(x_i)$. Comme $n = n(x_i)m(x_i)$ est un multiple strict de $n(x_i)$, le quotient $(q^n - 1)/(q^{n(x_i)} - 1)$ est multiple de $\Phi_n(q)$.

Par conséquent, en ajoutant -1 à chaque membre de la formule des classes, et en injectant cette divisibilité, tout en se rappelant que $\Phi_n(q)$ divise aussi $q^n - 1$, on en déduit que $\Phi_n(q)$ divise la différence $q - 1$.

Pour finir, on reviens à la définition de $\Phi_n(q)$:

$$\Phi_n(q) = \prod_{(k,n)=1} \left(q - \exp\left(\frac{2ik\pi}{n} \right) \right) \quad .$$

Cette inégalité entraîne donc

$$\Phi_n(q) \geq (q-1)^{\varphi(n)}$$

et même inégalité stricte si $n > 1$. La divisibilité obtenue ne peut donc être vraie que si $n = 1$, c'est-à-dire si K est commutatif.

Symboles de Legendre et de Jacobi

Définition 1.42. *Soit p un nombre premier impair. Pour tout entier a, on définit le symbole de Legendre $\left(\frac{a}{p}\right)$ par :*

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

On a alors :

Théorème 1.43. *Si p est un nombre premier impair et a un nombre entier, on a :*

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

Démonstration : l'égalité est évidente si p divise a. Dans le cas contraire, on note que $(\mathbb{Z}/p\mathbb{Z})^\star$ est cyclique d'ordre $p-1$; donc si $x = a^{\frac{p-1}{2}}$, $x^2 = a^{(p-1)} = 1$. par suite, $x = \pm 1$. Maintenant, si est $a = b^2$ modulo p, on a $x = b^{(p-1)} = 1$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\star$, et écrivons $a = g^s$; comme a n'est pas un carré, s est impair. On a donc $x = g^{\frac{s(p-1)}{2}}$; si $x = 1$, $s(p-1)/2$ est un multiple de l'ordre de g qui est $p-1$, mais c'est absurde puisque $s/2$ n'est pas entier.

Corollaire 1.44. *Soit p un nombre premier ≥ 3 ; pour que -1 soit un carré modulo p, il faut et il suffit que $p \equiv 1 \bmod 4$.*

Démonstration : il suffit de calculer $(-1)^{\frac{(p-1)}{2}}$.

Notons que la multiplication m_a par a dans $(\mathbb{Z}/p\mathbb{Z})^\star$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\star$. On peut donc la voir comme une permutation de l'ensemble à $p-1$ lettres ($m_a \in \mathfrak{S}_{p-1}$).

Corollaire 1.45. *Soit p un nombre premier ≥ 3 et a un nombre entier qui n'est pas multiple de p. Le symbole $\left(\frac{a}{p}\right)$ est égal à la signature de m_a.*

Démonstration : l'ordre de a divise $p-1$; notons-le $(p-1)/d$. Pour que a soit un carré modulo p, il faut et il suffit que d soit pair. Nous allons vérifier que la décomposition en cycles de supports disjoints de m_a possède d orbites, toutes de cardinal $(p-1)/d$. Une fois ceci fait, le calcul est facile, puisque la signature d'un cycle de longueur s est $(-1)^{s+1}$. La signature de m_a est donc $(-1)^{d\left[\frac{(p-1)}{d}+1\right]} = (-1)^d$. Soit $\mathcal{O}$ une orbite de m_a, et $x \in \mathcal{O}$. Alors, $x, ax, \ldots, a^k x, \ldots$ sont tous des éléments de $\mathcal{O}$. Inversement, ce sont les seuls par définition de l'orbite. Donc, le cardinal de $\mathcal{O}$ est l'ordre de a, ce qui a été annoncé.

La loi de réciprocité quadratique est un théorème de Gauß, qui affirme :

Théorème 1.46. *Soient p et q des nombres premiers ≥ 3. Alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \ .$$

En particulier, si p ou q est congru à 1 modulo 4, p est un carré modulo q si et seulement si q est un carré modulo p. Sinon, si p et q sont tous deux congrus à -1 modulo 4, p est un carré modulo q si et seulement si q n'est pas un carré modulo p. Ce théorème, avait déjà été plus ou moins vu par Euler et Legendre, mais c'est Gauß qui en a donné la première preuve complète. Il ne s'est pas arrêté là, puisqu'il a rédigé 8 preuves différentes. C'est un des énoncés dont on connait le plus de démonstrations différentes (plus de 200 à ce jour). Nous en présenterons un (tout) petit échantillon.

Commençons par calculer le symbole $\left(\frac{2}{p}\right)$.

Proposition 1.47. *Soit p un nombre premier ≥ 3. On a*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \bmod 8 \ , \\ -1 & \text{si } p \equiv \pm 3 \bmod 8 \ . \end{cases}$$

Démonstration : soit ζ une racine primitive 8-ième de l'unité dans une extension K du corps $\mathbb{F}_p$. On a $\zeta^4 = -1$ et donc $(\zeta + \zeta^{-1})^2 = 2$. On a donc exhibé une racine carrée de 2, mais on ne sait pas encore si elle est dans $\mathbb{F}_p$.

On pose $u = \zeta + \zeta^{-1}$; on calcule maintenant $u^p = (\zeta^p + \zeta^{-p})$. Comme $\zeta^8 = 1$ si $p \equiv \pm 1 \bmod 8$, on a donc $u^p = u$ et donc $u \in \mathbb{F}_p$. Si par contre $p \equiv \pm 3 \bmod 8$, on a $u^p = \zeta^3 + \zeta^{-3} = \zeta^4(\zeta^{-1} + \zeta^{-7}) = -(\zeta^{-1} + \zeta) = -u$ et donc $u \notin \mathbb{F}_p$.

On généralise maintenant le symbole de Legendre : c'est le symbole de Jacobi qui autorise à prendre des entiers et non de se restreindre aux premiers.

Soit n un entier naturel impair et soit $n = \prod_{i=1}^{s} p_i^{m_i}$ sa décomposition en facteurs premiers ;

Définition 1.48. *Le symbole de Jacobi* $\left(\frac{a}{n}\right)$ *vaut :*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{m_i} .$$

Il coïncide évidemment avec le symbole de Legendre lorsque n est premier.

La loi de réciprocité quadratique continue à être valide pour le symbole de Jacobi, ce qui renforce son intérêt.

Proposition 1.49. *Soient m et n des entiers naturels impairs premiers entre eux ; on a :*

(i)

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{(n-1)}{2}} = \begin{cases} 1 & si\ n \equiv 1 \bmod 4 \ , \\ -1 & si\ n \equiv 3 \bmod 4 \ . \end{cases}$$

(ii)

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & si\ n \equiv \pm 1 \bmod 8 \ , \\ -1 & si\ n \equiv \pm 3 \bmod 8 \ . \end{cases}$$

(iii)

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} .$$

Démonstration : notons $n = \prod_{i=1}^{s} p_i^{m_i}$ la décomposition de n en facteurs premiers. Par définition,

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{s} \left(\frac{-1}{p_i}\right)^{m_i} .$$

Comme -1 est premier à tous les p_i, aucun des facteurs n'est nul. Les seuls facteurs non nuls égaux à moins un sont ceux pour lesquels $p_i \equiv 3 \bmod 4$ et m_i est impair. Donc,

$$\left(\frac{-1}{n}\right) = (-1)^{\kappa} ,$$

où κ est le nombre d'indices i tels que $p_i \equiv 3 \bmod 4$ et m_i est impair. Si κ est pair, alors on a $n \equiv 1 \bmod 4$ et bien sûr $(n-1)/2$ pair. Inversement, si κ est impair, $n \equiv 3 \bmod 4$ et par suite $(n-1)/2$ est impair.

On a donc démontré (i). Passons à (ii) et comme précédemment, soit $n = \prod_{i=1}^{s} p_i^{m_i}$ la décomposition de n en facteurs premiers et soit κ le nombre d'indices i tels que $p_i \equiv \pm 3 \bmod 8$ et m_i impair. On a de même $\left(\frac{2}{n}\right) = (-1)^{\kappa}$. Dire que κ est impair, reviens à dire que $n \equiv \pm 3 \bmod 8$ et dire que κ est pair reviens à dire que $n \equiv \pm 1 \bmod 8$, ce qui est annoncé.

Nous pouvons maintenant passer à (iii). Notons comme ci-dessus $m = \prod_{i=1}^{s} p_i^{m_i}$ et $n = \prod_{j=1}^{s'} q_j^{n_j}$ les décompositions de m et n en facteurs premiers.

Par définition du symbole de Jacobi et multiplicativité du symbole de Legendre, on a :

$$\left(\frac{m}{n}\right) = \prod_j \left(\frac{m}{q_j}\right)^{n_j} = \prod_{i,j} \left(\frac{p_i}{q_j}\right)^{m_i n_j} \quad .$$

Et, par symétrie,

$$\left(\frac{n}{m}\right) = \prod_j \left(\frac{n}{p_i}\right)^{m_i} = \prod_{i,j} \left(\frac{q_j}{p_i}\right)^{m_i n_j} \quad .$$

On forme le produit, et on obtient :

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j} \left(\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right)^{m_i n_j} \quad .$$

Comme m et n sont premiers entre eux, c'est un produit de facteurs égaux à ± 1. On applique maintenant la loi de la réciprocité quadratique pour (p_i, q_j) et l'on en tire :

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j} (-1)^{\frac{m_i n_j (p_i-1)(q_j-1)}{4}} \quad .$$

Un terme de ce produit vaut -1 si et seulement si on a à la fois

$$p_i \equiv q_j \equiv 3 \bmod 4 \ , \qquad \text{et} \qquad m_i n_j \text{ impair} \ .$$

On va noter κ le nombre d'indice i pour lesquels on a à la fois $p_i \equiv 3 \bmod 4$ et m_i impair et de même, μ le nombre d'indice pour lesquels on a à la fois $q_j \equiv 3 \bmod 4$ et n_j impair. Avec ces notations,

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

Cette expression vaut -1 si et seulement si $\kappa\mu$ est impair (elle vaut 1 dans l'autre cas). Il suffit donc de vérifier que

$$\kappa\mu \equiv \frac{(m-1)(n-1)}{4} \bmod 2 \ .$$

Mais, le membre de droite est impair si et seulement si les deux facteurs $(m-1)/2$ et $(n-1)/2$ le sont, c'est-à-dire si et seulement si $m \equiv n \equiv 3 \bmod 4$. Mais, par définition de κ et μ, $m \equiv (-1)^\kappa \bmod 4$ et $n \equiv (-1)^\mu \bmod 4$. Nous avons donc bien établi (iii) (modulo la preuve de la loi de la réciprocité quadratique pour le symbole de Legendre évidemment).

Remarque 1.50. *Dans le cas où n n'est pas premier, on notera que $\left(\frac{a}{n}\right) = 1$ n'entraîne pas du tout que a est un carré modulo n. Par exemple, faisons $n = 15$ et posons $a = 2$. Comme $\mathbb{Z}/15\mathbb{Z}$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, on voit facilement que 2 n'est pas un carré (il ne l'est dans aucun des deux facteurs). Mais, comme $15 \equiv -1 \bmod (8)$, par la proposition précédente, $\left(\frac{2}{15}\right) = 1$.*

Exemple 1.51. *A l'aide de la loi de la réciprocité, le calcul du symbole est très rapide, par division successive. Prenons par exemple $\left(\frac{51}{233}\right)$. On note que 233 est premier (il n'a pas de facteurs ≤ 17). On a*

$$\left(\frac{51}{233}\right) = \left(\frac{3}{233}\right)\left(\frac{17}{233}\right) \quad .$$

Maintenant,

$$\left(\frac{3}{233}\right)\left(\frac{233}{3}\right) = (-1)^{116} = 1 \ .$$

Comme $233 \equiv 2 \bmod 3$*, il n'est pas un carré modulo* 3 *et par suite,* $\left(\frac{3}{233}\right) = -1$*.*

De même,

$$\left(\frac{17}{233}\right)\left(\frac{233}{17}\right) = 1 \ .$$

Calculons $\left(\frac{233}{17}\right)$ *; comme* $233 \equiv -5 \bmod 17$*, il suffit de calculer* $\left(\frac{-5}{17}\right)$*. Par la loi de réciprocité encore, comme* $\left(\frac{-1}{17}\right) = 1$*, cela vaut* $\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$*. Au total, on a donc trouvé que*

$$\left(\frac{51}{233}\right) = 1 \ ,$$

et comme 233 *est premier,* 51 *est un carré modulo* 233*. Par contre, il est plus difficile d'exhiber de manière algorithmique une racine carrée.*

1.1 La loi de la réciprocité quadratique : quelques preuves

Première démonstration

On sait que $\left(\frac{p}{q}\right)$ est la signature de la multiplication par p dans $(\mathbb{Z}/q\mathbb{Z})^\star$. La multiplication par p dans $\mathbb{Z}/q\mathbb{Z}$ a une orbite et un élément de plus (puisque 0 est point fixe), donc a même signature. Remplaçons maintenant le groupe $\mathbb{Z}/q\mathbb{Z}$ par celui que nous noterons G des racines q-ièmes de l'unité dans une extension K du corps $\mathbb{Z}/p\mathbb{Z}$ (qui lui est isomorphe). La multiplication par p dans $\mathbb{Z}/q\mathbb{Z}$ est transformée en l'élévation à la puissance p dans G ; notons m_p cette dernière permutation. Par définition, la signature d'une permutation de $\{1, \ldots, n\}$ est égale à $(-1)^s$, où s est le nombre « d'inversions» (un ordre $\prec$ étant supposé fixé, ce que nous faisons). On peut donc écrire :

$$\left(\frac{p}{q}\right) = \prod_{x \prec y} \varepsilon(x, y) \ ,$$

où $\varepsilon(x, y) = 1$ si $m_p(x) \prec m_p(y)$ et $\varepsilon(x, y) = -1$ sinon. Comme K est un corps, les expressions de la forme $\frac{m_p(x) - m_p(y)}{x - y}$ pour $x \neq y$ sont bien définies.

Vérifions que l'on a l'égalité dans K :

$$\left(\frac{p}{q}\right) = \prod_{x \prec y} \frac{m_p(x) - m_p(y)}{x - y} \ .$$

En effet, en voyant m_p comme une permutation, on voit qu'au numérateur apparaissent toutes les différences $x - y$ avec éventuellement un changement de signe s'il y a inversion. Il y a donc simplification au signe près et le signe restant est exactement donné par le nombre d'inversions. Par ailleurs, le membre de gauche peut être vu comme un élément de K par réduction modulo p.

En se rappelant maintenant que m_p est donné par l'élévation à la puissance p, on a donc les égalités dans $\mathbb{Z}/p\mathbb{Z}$:

$$\left(\frac{p}{q}\right) = \prod_{x \prec y} \frac{x^p - y^p}{x - y} = \prod_{x \prec y} (x-y)^{p-1} \ .$$

Le nombre de termes dans le produit est $q(q-1)/2$; par contre, si l'on prend le produit sur tous les couples (x, y) avec $x \neq y$, chaque terme intervient avec son opposé. Par suite, en tenant compte de ce changement de signe, on a encore :

$$\left(\frac{p}{q}\right) = \left(\prod_{x \neq y} (x-y)(-1)^{\frac{q(q-1)}{2}} \right)^{\frac{p-1}{2}} = (-1)^{q\frac{(q-1)(p-1)}{4}} \Delta^{\frac{(p-1)}{2}} \ ,$$

où Δ est le discriminant du polynôme $Q(X) = X^q - 1$ dans $\mathbb{F}_p$. Il nous faut maintenant déterminer si Δ est un carré moulo p. Comme $Q'(X) = qX^{q-1}$, le discriminant est

$$\Delta = \prod_{x \in G} (qx^{q-1}) = q^q \ ,$$

puisque le produit des éléments de G vaut 1.

On obtient donc, en tenant compte du fait que q est impair :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} q^{\frac{q(p-1)}{2}} \ .$$

Mais, $q^{(p-1)/2} = \left(\frac{q}{p}\right)$ et sa puissance q-ième aussi puisque q est impair. Pour conclure, on obtient la loi de la réciprocité quadratique :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right) \ .$$

Pour etre plus précis, nous avons démontré une congruence modulo p entre deux nombres qui valent tous deux ± 1 ; comme $p > 2$, c'est une égalité.

Deuxième démonstration

Pour n entier impair, on note U_n le n-ième polynôme de Tchebychev de seconde espèce défini par

$$U_n(2\cos\theta) = \frac{\sin(n\theta/2)}{\sin(\theta/2)} \ ,$$

ou par la relation équivalente

$$U_n\left(X + \frac{1}{X}\right) X^{(n-1)/2} = \frac{X^n - 1}{X - 1} \ .$$

On vérifie $U_1 = 1$, $U_3 = X + 1$ et la relation de récurrence

$$U_{n+2} = XU_n - U_{n-2} \ .$$

De cette relation, découle le fait que U_n est pour tout n, un polynôme unitaire de degré $(n-1)/2$ à coefficients entiers.

Dans cette démonstration de la loi de réciprocité quadratique, nous allons calculer le résultant des polynômes U_p et U_q.

Tout d'abord, $\mathrm{Res}(U_p, U_q)$, étant le résultant de deux polynômes à coefficients entiers, est un nombre entier. Un diviseur premier ℓ de $\mathrm{Res}(U_p, U_q)$ est caractérisé par le fait que P et Q ont une racine commune dans une extension convenable de $\mathbb{F}_\ell$.

Traitons tout d'abord le cas où $\ell \neq p$ et $\ell \neq q$.

Soit α une racine de U_p ; on peut l'écrire sous la forme $\alpha = \beta + \frac{1}{\beta}$ et l'on a $\Phi_p(\beta) = 0$. De même, une racine α' de U_q est de la forme $\gamma + \frac{1}{\gamma}$, où γ est une racine primitive q-ième de l'unité.

Dire que $\alpha = \alpha'$ entraîne donc que γ est une racine de $T^2 - \alpha T + 1$, c'est-à-dire que γ vaut soit β soit $1/\beta$, et est donc également racine primitive d'ordre p, ce qui est impossible. Par suite, il n'est pas possible que $\ell \neq p$ et $\ell \neq q$ soit un diviseur du résultant $\mathrm{Res}(U_p, U_q)$.

Passons maintenant au cas $\ell = p$ et soit α une racine de U_p dans une extension convenable de $\mathbb{F}_p$. Comme ci-dessus, $\alpha = \beta + 1/\beta$ avec $\beta^p = 1$. Mais, cette fois, ceci entraîne que $\beta = 1$ et donc $\alpha = 2$. Si α était une racine de U_q, on pourrait l'écrire $\alpha = \gamma + \frac{1}{\gamma}$, avec γ racine primitive q-ième de l'unité. Mais γ est racine de $T^2 - \alpha T + 1$ et, sachant que $\alpha = 2$, on a $\gamma = 1$, ce qui est absurde.

Autrement dit, U_p et U_q n'ont pas non plus de racine commune dans une extension de $\mathbb{F}_p$ et p ne divise pas $\mathrm{Res}(U_p, U_q)$. Par symétrie, ceci est aussi vrai pour q.

En conclusion, $\mathrm{Res}(U_p, U_q)$ est un entier qui n'est divisible par aucun nombre premier. Il est donc égal à ± 1.

Nous allons déterminer le signe correct en calculant $\mathrm{Res}(U_p, U_q)$ modulo p. On sait déjà que la seule racine de U_p est 2 et donc, U_p étant unitaire,

$$U_p = (X-2)^{p-1} \ .$$

Notons $\beta_1, \ldots, \beta_{\frac{q-1}{2}}$ les racines de U_q. Le résultant est donc

$$\mathrm{Res}(U_p, U_q) = \prod_{j=1}^{\frac{q-1}{2}} (2 - \beta_j)^{(p-1)/2} = U_q(2)^{\frac{p-1}{2}} \ .$$

Comme $2 = 1 + \frac{1}{1}$, la définition de U_q donne $U_q(2) = \Phi_q(1) = q$. Par suite,

$$\mathrm{Res}(U_p, U_q) \equiv q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p \ .$$

Par symétrie,

$$\mathrm{Res}(U_q, U_p) \equiv \left(\frac{p}{q}\right) \bmod q \ .$$

Comme p, q sont impairs, ces congruences impliquent en fait l'égalité.

Il suffit maintenant de rappeler que si P, Q sont deux polynômes unitaires de degré m, n respectivement, on a par définition :

$$\mathrm{Res}(P, Q) = (-1)^{mn} \mathrm{Res}(Q, P) \ .$$

En conclusion,

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

ce qu'il fallait démontrer.

Troisième démonstration

On note G le groupe quotient

$$G = (\mathbb{F}_p^\star \times \mathbb{F}_q^\star)/\left\{(1,1),(-1,-1)\right\} \ .$$

Nous allons calculer de deux façons différentes le produit Π des éléments de G. Dans la suite, nous noterons π la surjection canonique de $\mathbb{F}_p^\star \times \mathbb{F}_q^\star$ vers G.

Un système de représentants de G dans $\mathbb{F}_p^\star \times \mathbb{F}_q^\star$ est donné par $\mathbb{F}_p^\star \times \{1,\ldots,(q-1)/2\}$.

En conclusion,

$$\Pi = \pi\left(\prod_{x\in\mathbb{F}_p^\star}\prod_{y=1}^{(q-1)/2}(x,y)\right) = \pi\left((p-1)!^{(q-1)/2}, \left[\left(\frac{q-1}{2}\right)!\right]^{p-1}\right) \ .$$

Par le théorème de Wilson, $(p-1)!^{(q-1)/2} = (-1)^{(q-1)/2}$ et

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

Donc,

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

grâce au lemme précédent.

D'autre part, lorsque z parcourt l'ensemble des nombres entiers $\{1,...,pq\}$ qui ne sont divisibles ni par p ni par q, les couples $(z \bmod p, z \bmod q)$ parcourent une fois et une seule les éléments de $\mathbb{F}_p^\star \times \mathbb{F}_q^\star$. À l'entier $pq-z$ correspond le couple opposé $(-z \bmod p, -z \bmod q)$. Lorsque z parcourt uniquement $1,...,(pq-1)/2$, les couples $(z \bmod p, z \bmod q)$ forment un système de représentants dans G du groupe $\mathbb{F}_p^\star \times \mathbb{F}_q^\star$. Notons c le produit de ces entiers. En rajoutant les multiples de q dans l'intervalle $[1,(pq-1)/2]$, on obtient

$$c = \frac{\prod_{z=1,(z,p)=1}^{(pq-1)/2} z}{q\cdot 2q\cdots\frac{(p-1)}{2}q} \ .$$

Les entiers z qui apparaissent au numérateur s'écrivent d'une part

$$z = pu + v$$

avec $0 \leq u < \frac{(q-1)}{2}$ et $1 \leq v \leq (p-1)$ et d'autre part $z = \frac{p(q-1)}{2} + v$ avec $1 \leq v \leq \frac{(p-1)}{2}$. Modulo p, l'entier u n'intervient pas et l'on a donc

$$c \equiv \frac{(1 \cdots (p-1))^{\frac{(q-1)}{2}} \left(1 \cdots \frac{(p-1)}{2}\right)}{q^{\frac{(p-1)}{2}} \left(1 \cdots \frac{(p-1)}{2}\right)} \equiv \left(\frac{q}{p}\right) (-1)^{\frac{(q-1)}{2}} \bmod p \ .$$

De même, par symétrie, on trouve

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

si bien que $\pi(c \bmod p, c \bmod q) = \Pi$. Par suite,

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

On en déduit que :

$$\left((-1)^{\frac{(q-1)}{2}}, (-1)^{\frac{(p-1)}{2}} \cdot (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}\right)^{-1} \cdot \left(\left(\frac{q}{p}\right)(-1)^{\frac{(q-1)}{2}}, \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)}{2}}\right) \in \ker(\pi) \ .$$

Après simplification, on en déduit donc :

$$\left(1, (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\right) \in \ker(\pi) \ .$$

Comme $\ker(\pi) = \{(1,1), (-1,-1)\}$, on en déduit la réciprocité quadratique.

1.2 Sommes de Gauß

Définition 1.52. *Pour tout entier naturel $n \geq 1$, on définit :*

$$G_n = \sum_{k=1}^{n} \exp\left(\frac{2i\pi k^2}{n}\right) \ .$$

On a alors :

Théorème 1.53. *Suivant les valeurs de n modulo 4, le nombre G_n vaut :*

$$G_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \bmod 4 \ , \\ 0 & \text{si } n \equiv 2 \bmod 4 \ , \\ i\sqrt{n} & \text{si } n \equiv 3 \bmod 4 \ , \\ (1+i)\sqrt{n} & \text{si } n \equiv 0 \bmod 4 \ . \end{cases}$$

Démonstration : on introduit la fonction $f : \mathbb{R} \longrightarrow \mathbb{C}$ définie par

$$f(x) = \sum_{k=0}^{n-1} \exp\left(\frac{2i\pi(x+k)^2}{n}\right) \ .$$

La fonction f est de classe $\mathcal{C}^\infty$ et périodique, de période 1 et bien sûr $G_n = f(0)$. Comme f est périodique, il est intéressant d'étudier sa série de Fourier ; notons la

$$f(x) = \sum_{m\in\mathbb{Z}} c_m \exp(2i\pi mx) \ .$$

Par définition, on a [3] :

$$\begin{aligned}
c_m &= \int_0^1 f(x)\exp(-2i\pi mx)dx \\
&= \sum_{k=0}^{n-1}\int_0^1 \exp\left(\frac{2i\pi(x+k)^2}{n} - 2i\pi mx\right)dx \\
&= \sum_{k=0}^{n-1}\int_0^1 \exp\left(\frac{2i\pi}{n}\left(x+\left(k-\frac{1}{2}mn\right)\right)^2\right)\exp\left(2i\pi\left(mk-\frac{1}{4}m^2n\right)\right)dx \\
&= \exp\left(-2i\pi\frac{m^2n}{4}\right)\sum_{k=0}^{n-1}\exp\left(2i\pi mk\right)\int_{k-\frac{mn}{2}}^{k+1-\frac{mn}{2}}\exp\left(\frac{2i\pi u^2}{n}\right)du \\
&= \exp\left(-2i\pi\frac{m^2n}{4}\right)\int_{-\frac{mn}{2}}^{n-\frac{mn}{2}}\exp\left(\frac{2i\pi u^2}{n}\right)du \\
&= n\exp\left(-2i\pi\frac{m^2n}{4}\right)\int_{-\frac{m}{2}}^{1-\frac{m}{2}}\exp\left(2i\pi nv^2\right)dv \ .
\end{aligned}$$

Comme f est de classe $\mathcal{C}^\infty$, elle est la somme de sa série de Fourier ; en particulier

$$G_n = f(0) = \sum_{m\in\mathbb{Z}} c_m \ .$$

On observe que $\exp\left(-2i\pi m^2n/4\right)$ vaut 1 quand m est pair, et vaut

$$\exp\left(-2i\pi n/4\right)$$

quand m est impair. Ainsi,

$$\begin{aligned}
G_n &= \sum_{m\in\mathbb{Z}} c_{2m} + \sum_{m\in\mathbb{Z}} c_{2m+1} \\
&= n\sum_{m\in\mathbb{Z}}\int_{-m}^{1-m}\exp\left(2i\pi nv^2\right)dv \\
&+ n\exp\left(-2i\pi n/4\right)\sum_{m\in\mathbb{Z}}\int_{-\frac{1}{2}-m}^{\frac{1}{2}-m}\exp\left(2i\pi nv^2\right)dv \ .
\end{aligned}$$

3. On notera pour la cinquième égalité que comme $mk \in \mathbb{Z}$, on a $\exp(2i\pi mk) = 1$.

Les deux séries de la dernière ligne de l'équation ci-dessus convergent et ont même somme, à savoir l'intégrale (généralisée)

$$I = \int_{-\infty}^{+\infty} \exp\left(2i\pi n v^2\right) dv \ .$$

Pour le vérifier, soient $a < b$ deux nombres réels de même signe de valeur absolue assez grande, et procédons par intégration par parties :

$$\begin{aligned} \int_a^b \exp\left(2i\pi n v^2\right) dv \ &= \ \int_a^b \frac{1}{4i\pi n v} \exp\left(2i\pi n v^2\right) 4i\pi n v dv \\ &= \left[\exp\left(2i\pi n v^2\right) \frac{1}{4i\pi n v}\right]_a^b + \int_a^b \frac{1}{4i\pi n v^2} \exp\left(2i\pi n v^2\right) \ . \end{aligned}$$

La dernière expression tends bien vers 0 lorsque $|a|, |b|$ tendent vers l'infini, et donc

$$\int_a^b \exp\left(2i\pi n v^2\right) dv$$

tends vers 0 pour a, b assez grand en valeur absolue. Le critère de Cauchy assure la convergence et on en déduit directement l'égalité de I et des deux séries que nous souhaitons calculer.

On a donc

$$G_n = n\left(1 + \exp\left(-2i\pi n/4\right)\right) I = \sqrt{n}\left(1 + \exp\left(-2i\pi n/4\right)\right) J \ ,$$

où $J = \int_{-\infty}^{\infty} \exp\left(2i\pi u^2\right) du$. Mais, nous ne connaissons pas la valeur de I (ou de J)... Cependant, il est facile de calculer G_1 à partir de sa définition :

$$G_1 = \exp(2i\pi) = 1 \ .$$

Cela fournit directement

$$J = \frac{G_1}{1-i} = \frac{1+i}{2} \ .$$

Il suffit maintenant, pour conclure la démonstration du théorème, de disjoindre les cas :

- Si $n \equiv 0 \bmod 4$, $\exp\left(-2i\pi n/4\right) = 1$ et $G_n = (1+i)\sqrt{n}$;
- Si $n \equiv 1 \bmod 4$, $\exp\left(-2i\pi n/4\right) = -i$ et $G_n = \sqrt{n}$;
- Si $n \equiv 2 \bmod 4$, $\exp\left(-2i\pi n/4\right) = -1$ et $G_n = 0$;
- Si $n \equiv 3 \bmod 4$, $\exp\left(-2i\pi n/4\right) = i$ et $G_n = i\sqrt{n}$;

Lemme 1.54. *On a la relation :*

$$G_{pq} = G_p G_q \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) \ .$$

Démonstration : observons que si x et y sont des entiers égaux modulo n, alors

$$\exp\left(2i\pi x^2/n\right) = \exp\left(2i\pi y^2/n\right) \ .$$

Par suite, pour définir la somme de Gauß, on peut utiliser tout ensemble d'entiers représentant chaque classe de congruence une fois et une seule. Lorsque x et y parcourent $\{1, ..., p\}$ et $\{1, ..., q\}$ respectivement, les entiers $qx + py$ sont deux à deux distincts modulo pq. Par suite,

$$G_{pq} = \sum_{x=1}^{p}\sum_{y=1}^{q} \exp\left(2i\pi\frac{(qx+py)^2}{pq}\right) = \sum_{x=1}^{x=p} \exp\left(2i\pi\frac{qx^2}{p}\right)\sum_{y=1}^{q}\exp\left(2i\pi\frac{py^2}{q}\right) \ .$$

Lorsque x parcourt $\{1, ..., p-1\}$, qx^2 modulo p parcourt deux fois les carrés non nuls de $\mathbb{F}_p$ si q est un carré modulo p, et les non-carrés sinon. Dans le premier cas, on a $\sum_{x=1}^{p}\exp\left(2i\pi\frac{qx^2}{p}\right) = G_p$ et dans le second cas,

$$\begin{aligned}
\sum_{x=1}^{p}\exp\left(2i\pi\frac{qx^2}{p}\right) &= 1 + 2\sum_{x=1,\ x \text{ non carré modulo } p}^{p-1} \exp\left(2i\pi x/p\right) \\
&= 1 + 2\sum_{x=1}^{p-1}\exp\left(2i\pi x/p\right) - 2\sum_{x=1,\ x \text{ carré modulo } p}^{p-1} \exp\left(2i\pi x/p\right) \\
&= 2 + 2\sum_{x=1}^{p-1}\exp\left(2i\pi x/p\right) - G_p = -G_p \ .
\end{aligned}$$

Pour résumer, nous avons montré :

$$\sum_{x=1}^{p}\exp\left(2i\pi\frac{qx^2}{p}\right) = \left(\frac{q}{p}\right) G_p \ .$$

Par symétrie, la même relation est vraie pour G_p. Le lemme suit en faisant le produit.

Le calcul de la somme de Gauß entraîne une démonstration immédiate de la loi de réciprocité quadratique :

Quatrième démonstration

Comme p et q sont impairs, G_p, G_q et G_{pq} sont tous les trois non nuls. On réécrit alors la relation du lemme sous la forme

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{G_{pq}}{\sqrt{pq}} \cdot \frac{\sqrt{p}}{G_p} \cdot \frac{\sqrt{q}}{G_q} \ .$$

Supposons d'abord que $p \equiv 1 \bmod 4$. Dans ce cas, $pq \equiv q \bmod 4$ et donc

$$\frac{G_{pq}}{\sqrt{pq}} = \frac{G_q}{\sqrt{q}} \ , \qquad \text{et} \qquad \frac{G_p}{\sqrt{p}} = 1 \ .$$

Par suite, comme souhaité dans la loi de la réciprocité quadratique,

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

De même, par symétrie, si q est congru à 1 modulo 4, alors la réciprocité quadratique est vraie. On peut donc supposer qu'ils sont tous les deux congrus à trois modulo 4. Dans ce cas, $pq \equiv 1 \bmod 4$ et :

$$\frac{G_p}{\sqrt{p}} = \frac{G_q}{\sqrt{q}} = i \ , \qquad \text{et} \qquad \frac{G_{pq}}{\sqrt{pq}} = 1 \ .$$

Le membre de droite vaut donc -1, de même que le membre de gauche, d'où le dernier cas à démontrer.

1.3 Généralisations des sommes de Gauß

On peut en fait définir une variante de la somme de Gauß dans tout corps qui contient une racine primitive n-ième de l'unité. Soit K un corps et soit $\zeta \in K$ une racine primitive p-ième de l'unité. On définit

$$G(\zeta) = \sum_{x=1}^{p} \zeta^{x^2} = 1 + 2 \sum_{x=1,\ x \text{ carré modulo } p}^{p-1} \zeta^x = \sum_{x \in \mathbb{F}_p^\star} \left(\frac{x}{p}\right) \zeta^x \ .$$

Les trois expressions ci-dessus sont égales. C'est trivial pour les deux premières ; pour la troisième, on observe que comme $\zeta^p = 1$, ζ^x ne dépend que de la classe de x modulo p et que la somme des racines d'ordre p est nulle. Lorsque $K = \mathbb{C}$ et $\zeta = \exp(2i\pi/p)$ pour p impair, nous avons vu que $G(\zeta)^2 = \pm p$, le signe dépendant de la congruence de p modulo 4. C'est un fait général :

Proposition 1.55. *On a les relations pour p premier impair :*

(i)

$$G(\zeta)^2 = (-1)^{\frac{(p-1)}{2}} p \ ;$$

(ii) pour tout $a \in \mathbb{F}_p^\star$,

$$G(\zeta^a) = \left(\frac{a}{p}\right) G(\zeta) \ .$$

Démonstration : commençons par (ii) et soit $a \in (\mathbb{Z}/p\mathbb{Z})^\star$; on a :

$$G(\zeta^a) \ = \ \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\star} \left(\frac{x}{p}\right) \zeta^{ax} = \sum_{y \in (\mathbb{Z}/p\mathbb{Z})^\star} \left(\frac{y/a}{p}\right) \zeta^y = \left(\frac{a}{p}\right) G(\zeta) \ .$$

Passons maintenant à (i).

$$\begin{aligned} G(\zeta)^2 &= \left(\frac{-1}{p}\right) G(\zeta) G\left(\zeta^{-1}\right) \\ &= \left(\frac{-1}{p}\right) \sum_{x,y \in \mathbb{Z}/p\mathbb{Z}} \zeta^{x^2 - y^2} \\ &= \left(\frac{-1}{p}\right) \sum_{x,y \in \mathbb{Z}/p\mathbb{Z}} \zeta^{(x-y)(x+y)} \ . \end{aligned}$$

On remarque que l'application :

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 \\ (x,y) \longmapsto & (x-y, x+y) & \end{array}$$

est une bijection car p est impair. Par suite, on a :

$$G(\zeta)^2 = \left(\frac{-1}{p}\right) \sum_{u,v\in\mathbb{Z}/p\mathbb{Z}} \zeta^{uv} = \left(\frac{-1}{p}\right) \sum_{u\in\mathbb{Z}/p\mathbb{Z}} \sum_{v\in\mathbb{Z}/p\mathbb{Z}} \zeta^{uv} \ .$$

Mais, si $u \neq 0$ la dernière somme est la somme de toutes les racines p-ièmes l'unité ; elle est donc nulle. Si par contre, $u = 0$, cette somme vaut p. Par conséquent,

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

D'où le point (i) et donc la proposition.

Cinquième démonstration

Supposons que K soit un corps de caractéristique q ; on a alors

$$G(\zeta)^q = \left(\sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} \left(\frac{x}{p}\right) \zeta^x \right)^q = \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} \left(\frac{x}{p}\right) \zeta^{qx} \ ,$$

car l'élévation à la puissance q est un endomorphisme du corps K et que $\left(\frac{x}{p}\right)^q = \left(\frac{x}{p}\right)$ puisque $q \neq 2$.

D'après la proposition, on a donc

$$G(\zeta)^q = G\left(\zeta^q\right) = \left(\frac{q}{p}\right) G(\zeta) \ .$$

Mais, par ailleurs,

$$\begin{array}{rcl} G(\zeta)^q & = & G(\zeta) G(\zeta)^{q-1} \\ & = & G(\zeta) \left(G(\zeta)^2\right)^{\frac{(q-1)}{2}} \\ & = & \left(\frac{-1}{p}\right)^{\frac{(q-1)}{2}} \cdot p^{\frac{(q-1)}{2}} \cdot G(\zeta) \\ & = & \left(\frac{-1}{p}\right)^{\frac{(q-1)}{2}} \cdot \left(\frac{p}{q}\right) \cdot G(\zeta) \ . \end{array}$$

Comme $G(\zeta)^2 = \left(\frac{-1}{p}\right) p \neq 0$ dans K, $G(\zeta)$ n'est pas nul non plus et l'on peut simplifier par cette quantité. On a donc

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

Pou conclure, distinguons les cas : lorsque p est congru à 1 modulo 4, $\left(\frac{-1}{p}\right) = 1$ et $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$; lorsque q est congru à 1 modulo 4, $(q-1)/2$ est pair et l'on a encore $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$; enfin, lorsque p et q sont tous deux congrus à 3 modulo 4, $\left(\frac{-1}{p}\right) = -1$, $(q-1)/2$ est impair et $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ comme on le souhaite et la réciprocité quadratique en découle encore.

2 Critères de primalité

En sus de l'intérêt théorique des nombres premiers, ce sont aussi des outils important pour des applications de la vie courante (sécurité bancaire, signature électronique, codes correcteurs d'erreurs utilisés en télécommunication numérique.

La « production industrielle » de nombres premiers « aléatoires » de grande taille est ainsi devenue une activité courante, rendant nécessaire le développement de méthodes efficaces permettant d'affirmer qu'un nombre entier donné n est, ou n'est pas un nombre premier.

La méthode naïve (crible d'Eratosthène) qui consiste à essayer successivement toutes les divisions par les entiers inférieurs à $\sqrt{n}$, est rapidement impraticable si n a plus de quelques chiffres. En effet, le nombre d'opérations croit polynômialement en n : même pour un nombre ayant 100 chiffres décimaux, ce qui est très peu pour la cryptographie, il faudrait une puissance de calcul irréaliste. On souhaite donc pouvoir gagner un ordre de grandeur et disposer de méthodes ne nécessitant pas plus qu'une puissance du logarithme de n (nombre de chiffres) d'opérations élémentaires.

Les algorithmes expliqués ici résultent le plus souvent de théorèmes qui prennent une forme proche de la suivante : « si n est premier, tout entier a tel que $1 \leq a \leq f(n)$ vérifie une certaine propriété $P(a)$ ». Dans ce cas, il suffit d'exhiber un entier a tel que la propriété ne soit pas satisfaite pour en déduire que n n'est pas premier ; un tel a sera appelé témoin de non-primalité. En revanche, savoir que tout entier a dans l'intervalle vérifie $P(a)$ n'implique pas forcément que n est un nombre premier (parfois on dit que n est très probablement premier).

« si n est premier, il existe un entier b, dans $[1, g(n)]$ vérifiant une propriété $Q(b)$ ». On dira que b est un témoin de primalité. Le second cas est symétrique : exhiber un entier b vérifiant $Q(b)$ prouve que b est un nombre premier....mais si on n'en trouve pas, on ne sait pas forcément qu'il est composé ! Il n'est cependant pas raisonnable de tester tous les entiers successivement, à moins de savoir qu'il existe un entier b vérifiant $Q(b)$ qui soit assez petit (sinon, on n'a pas amélioré la méthode d'Erathosthène qui elle, est sûre). Si l'on sait qu'une proportion importante d'entiers b est constitué de témoins de primalité, on peut tester la propriété $Q(b)$ sur des entiers b pris au hasard : si n est premier, la probabilité qu'aucun des entiers choisis ne soit un témoin de primalité, est égale à $(1-p)^{-k}$ si p est la densité des témoins de primalité et k le nombre d'essais, donc décroît très rapidement avec k (et en plus formalise la notion intuitive de forte probabilité pour que le nombre soit premier. Le test obtenu est ainsi appelé probabiliste.

2.1 Critère de Fermat

Ce test repose sur le « petit théorème de Fermat » :

Proposition 2.1. *Soit p un nombre premier ; pour tout entier a premier à p, on a :*

$$a^{p-1} \equiv 1 \bmod p \ .$$

Démonstration : le groupe $\mathbb{F}_p^\star$ est cyclique d'ordre $p-1$.

Cette proposition fournit un test de non-primalité : si n est un nombre entier, il suffit d'exhiber un nombre entier a dans l'intervalle $[1, n-1]$ tel que $a^{n-1} \neq 1 \bmod n$ pour en déduire que n est composé : c'est le test de Fermat. On notera que trouver un tel a montre que n est composé, mais pas l'inverse.

On sait même qu'il existe des nombres (les nombres de Carmichael), qui sont composé, mais qui passent le test de Fermat. Le plus petit nombre de Carmichael est 561. On sait qu'il existe une infinité de nombres de Carmichael (depuis seulement 15 ans). Toutefois, il y a très peu de nombres de Carmichael. Ainsi, certains logiciels de cryptage se contentent du test de Fermat, considérant que la probabilité d'échouer le test est négligeable... On sait en effet démontrer que si n n'est ni un Carmichael, ni un nombre premier, la moitié au moins des nombres $1 \leq a \leq n-1$ premiers à n sont des témoins de non primalité (exercice). Ainsi, au bout de k essais, on a une « probabilité » $\leq 1/2^k$ d'avoir un nombre qui est composé, mais non de Carmichael sans l'avoir démontré.

Un petite variante qui repose sur une remarque d'Euler est le test de Soloway-Strassen :

Lemme 2.2. *Si n est premier et si $(a,n)=1$, alors,*

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

Démonstration : c'est la définition du symbole.

Ce test est plus rapide que celui de Fermat, sachant qu'il est en pratique très facile de calculer le symbole.

2.2 Test de Miller-Rabin

C'est un raffinement du test de Fermat qui repose sur la remarque suivante : si p est un nombre premier et a un entier tel que $a^2 = 1 \bmod p$, alors $a = \pm 1 \bmod p$. En effet, l'hypothèse est que p divise $a^2 - 1 = (a-1)(a+1)$; il divise donc l'un des facteurs d'après le lemme d'Euclide.

Lemme 2.3. *Soit n un entier impair ≥ 1 ; on note H le sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\star$ donné par :*

$$H = \left\{ a \in (\mathbb{Z}/n\mathbb{Z})^\star, a^{\frac{(n-1)}{2}} \equiv \left(\frac{a}{n}\right) \bmod n \right\} \ .$$

Alors, $H = (\mathbb{Z}/n\mathbb{Z})^\star$ si et seulement si n est premier.

Démonstration : on sait déjà que si n est premier, alors $H = (\mathbb{Z}/n\mathbb{Z})^\star$. Pour la réciproque, montrons d'abord que n est sans facteurs carrés. En effet si $p \geq 3$ est premier et $p^2 \mid n$, alors, il existe un élément d'ordre $p(p-1)$ dans $(\mathbb{Z}/n\mathbb{Z})^\star$. Comme $p \nmid n-1$, on ne peut donc pas avoir $a^{n-1} \equiv 1 \bmod n$, ce qui est le cas pour tous les éléments de H. Donc, $a \notin H$. On peut donc supposer $n = p_1 \dots p_r$ où les p_i sont deux à deux distincts. On peut donc trouver un entier a tel que $a \equiv 1 \bmod (p_2 \dots p_r)$ et tel que a ne soit pas un carré modulo p_1. Dans ce cas, le symbole $\left(\frac{a}{n}\right) = -1$ par multiplicativité, mais comme $a^{(n-1)/2} \equiv 1 \bmod (p_2 \dots p_r)$, on ne peut pas avoir $a^{(n-1)/2} \equiv -1 \bmod n$.

On peut maintenant énoncer le test de Miller-Rabin

Proposition 2.4. *Soit p un nombre premier impair et soit a un entier $(a,p)=1$. Notons $r = v_2(p-1)$, et posons $m = (p-1)/2^r$. Soit s le plus petit entier ≥ 0 tel que $a^{m2^s} \equiv 1 \bmod p$. Si $s > 0$, alors $a^{m2^{s-1}} \equiv -1 \bmod p$.*

Démonstration : l'ordre de a dans $(\mathbb{Z}/n\mathbb{Z})^\star$ est exactement $2^t m'$, où $t \leq r$ et $m' \mid m$. Par suite, sit $t = 0$, on a $a^m \equiv 1 \bmod n$ et il n'y a rien à dire. Si $t > 0$, on a $t = s$ et $a^{2^{s-1}m}$ est d'ordre 2 dans $(\mathbb{Z}/n\mathbb{Z})^\star$ et donc vaut -1 puisque c'est le seul élément d'ordre 2 dans ce groupe.

Soit n un nombre entier impair, $r = v_2(n-1)$ et $m = (n-1)/2^r$. Un témoin de non-primalité de Miller-Rabin pour n est donc une paire d'entiers (a, s) telle que $a^{m2^{s-1}} \not\equiv \pm 1 \bmod n$ mais $a^{m2^s} \equiv 1 \bmod n$. L'intérêt de ce test est qu'il est fiable : le phénomène des nombres de Carmichael ne se produit plus. Plus précisément, si n est un nombre entier impair tel que $n > 1$, au moins trois quarts des nombres entiers a dans $[1, n]$ sont des témoins de non-primalité de Miller-Rabin. On dispose ainsi d'un algorithme de primalité de nature probabiliste : tirons k nombres entiers au hasard dans $[1, n]$; si n n'est pas premier, la probabilité qu'aucun ne soit un témoin de non-primalité est inférieure ou égale à $1/4^k$. Autrement dit, si l'on tire au hasard k nombres entiers et qu'aucun n'est un témoin de non-primalité de Miller-Rabin, il y a de fortes chances pour que n soit premier. Si l'on admet l'hypothèse de Riemann généralisée, un théorème de 1990 affirme que dès qu'un entier $n > 1$ n'est pas un nombre premier, il y a un témoin de non-primalité inférieur à $2(\log n)^2$. Cela permet d'envisager essayer les entiers dans l'ordre et de tester si ce sont des témoins de non-primalité et fournit, sous l'hypothèse de Riemann généralisée, un algorithme déterministe pour décider de la primalité d'un entier n en ne faisant qu'un nombre d'opérations élémentaires polynomial en $\log n$.

On peut également remarquer que dans le cas particulier où $n \equiv 3 \bmod 4$, le test de Miller-rabin et celui de Soloway-Strassen sont en fait identiques et se traduisent par $a^{(n-1)/2} \equiv \pm 1 \bmod n$. Plus généralement, si a passe le test de Miller-Rabin, alors, il passe celui de Soloway-Strassen. On peut même être plus précis en introduisant les ensembles suivants pour n impair :

$$\begin{cases} G_0 = (\mathbb{Z}/n\mathbb{Z})^\star \\ G_1 = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^\star,\ \ a^{n-1} \equiv 1 \bmod n\right\}\ , \\ G_2 = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^\star,\ \ a^{(n-1)/2} \equiv \pm 1 \bmod n\right\}\ , \\ G_3 = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^\star,\ \ a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n\right\}\ , \\ \mathcal{M} = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^\star,\ \ a^m \equiv 1 \bmod n,\ \text{ou } \exists\, 0 \leq s \leq r, a^{2^s m} \equiv -1 \bmod n\right\}\ . \end{cases}$$

On dispose alors des énoncés suivants :

Lemme 2.5. *Les ensembles G_0, G_1, G_2 sont des groupes, mais $\mathcal{M}$ ne l'est pas nécessairement.*

Démonstration : tous ces ensembles contiennent 1 et sont donc non vides. La stabilité par le passage à l'inverse est claire pour tous ces ensembles et la stabilité par la multiplication est triviale pour G_1, G_2 ; elle découle découle de la multiplicativité du symbole pour G_3. Par contre, pour $\mathcal{M}$, on a vu qu'il était égal à G_2 si $n \equiv 3 \bmod 4$: dans ce cas, c'est donc un groupe. Prenons par contre $n = 85 = 5 \times 17$; on a $n - 1 = 21 \times 2^2$. Dans ce cas, si l'on pose a tel que $a^{21} = 13$, on a $a^{42} = 13^2 = -1$ donc $a \in \mathcal{M}$. De même, si l'on pose $b = 16$, on a $b^2 = 1$ donc $(ab)^{42} \in \mathcal{M}$. Mais, $c = a \cdot (ab)$ vérifie $c^{42} = 1$, donc, pour qu'il soit dans $\mathcal{M}$, il faudrait que $c^{21} = -1$. Comme l'application de $(\mathbb{Z}/85\mathbb{Z})^\star$ dans lui-même donnée par $x \longmapsto x^{21}$ est une bijection (21 est premier à l'ordre de ce groupe), cela impliquerait que $c = -1$ et donc $-1 = 16a^2$. Mais modulo 5, cette relation donne $a^2 = -1$, donc $a = -1$, ce qui interdit $a^{21} = -2$. Donc, $\mathcal{M}$ n'est pas stable par multiplication.

Lemme 2.6. *On a les inclusions $\mathcal{M} \subset G_3 \subset G_2 \subset G_1 \subset G_0$. On a l'égalité $\mathcal{M} = G_0$ si et seulement si n est premier.*

Démonstration : l'inclusion $G_1 \subset G_0$ est triviale. L'inclusion $G_2 \subset G_1$ aussi, de même que $G_3 \subset G_2$. Montrons donc $\mathcal{M} \subset G_3$. Soit donc $a \in \mathcal{M}$. Supposons tout d'abord que $a^m \equiv 1 \bmod n$. Dans ce cas, $a^{(n-1)/2} \equiv 1 \bmod n$ et il convient de vérifier que $\left(\frac{a}{n}\right) = 1$.

Calculons le symbole $\left(\frac{a}{n}\right)$. Comme m est impair,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^m = \left(\frac{a^m}{n}\right) = 1 \ ,$$

ce que l'on voulait. On peut donc supposer qu'il existe $0 \leq s \leq r-1$ tel que $a^{2^s m} \equiv -1 \bmod n$.

Soit p un nombre premier divisant n et écrivons $p - 1 = 2^\alpha u$, avec u impair ; comme $a^{2^s m} \equiv -1 \bmod n$, ceci est aussi vrai modulo p et donc, l'ordre de a dans $(\mathbb{Z}/p\mathbb{Z})^\star$ est de la forme $2^{s+1}v$ où v divise u et m. On en déduit la valeur du symbole $\left(\frac{a}{p}\right)$:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv a^{2^{\alpha-1}u} \equiv \begin{cases} 1 \bmod p & \text{si } \alpha > s+1 \ , \\ -1 \bmod p & \text{si } \alpha = s+1 \ . \end{cases}$$

Si l'on note t le nombre de diviseurs premiers p de n (comptés avec leur ordre de divisibilité) tels que $v_2(p-1) = s+1$, le calcul ci-dessus nous assure que

$$\left(\frac{a}{n}\right) = (-1)^t \ .$$

Par ailleurs,

$$n = \prod_{p|n} \left(1 + 2^{v_2(p)} u(p)\right)^{l_p} \equiv 1 + t2^{s+1} \bmod 2^{s+2} \ .$$

Donc, dire que $s+1 < r$ reviens à dire que t est pair et $s+1 = r$ force t à être impair. Maintenant, si $a \in \mathcal{M}$ et $s+1 < r$ alors, $a^{(n-1)/2} \equiv 1 \bmod n$ et le symbole de Jacobi vaut aussi 1 donc $a \in G_3$. Par contre, si $a \in \mathcal{M}$ et $s+1 = r$, alors $a^{(n-1)/2} \equiv -1 \bmod n$ et le symbole vaut aussi -1, donc $a \in G_3$ dans les deux cas. On a donc bien montré la dernière inclusion.

Supposons maintenant que $\mathcal{M} = G_0$. En particulier $G_3 = G_0$, mais ceci entraîne que n est premier par l'énoncé ci-dessus. La réciproque a déjà été vue.

Nous allons maintenant estimer le ratio $\mathrm{Card}(\mathcal{M})/\mathrm{Card}(G_0)$ pour formaliser l'affirmation que nous avons au moins $3/4$ de témoins de non primalité de n.

Définition 2.7. *Soient n, m des entiers. On pose*

$$\phi(n,m) = \mathrm{Card}\left(\{a \in (\mathbb{Z}/n\mathbb{Z})^\star, a^m \equiv 1 \bmod n\}\right) \ ;$$

de même, on pose,

$$\phi'(n,m) = \mathrm{Card}\left(\{a \in (\mathbb{Z}/n\mathbb{Z})^\star, a^m \equiv -1 \bmod n\}\right) \ .$$

Lemme 2.8. *Soit n un entier impair, et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On pose également $n = 1 + 2^r m$, avec m impair et $p_i = 1 + 2^{r_i} m_i$ (m_i impair). Enfin, on introduit $u_i = \mathrm{PGCD}(m, m_i)$ et, pour $t \geq 0$ un entier quelconque $r_i' = \min(t, r_i)$. Avec toutes ces notations,*

$$\phi(n, 2^t m) = 2^{r_1' + \cdots r_k'} u_1 \ldots u_k \ .$$

De plus,

$$\phi'(n, 2^t m) = \begin{cases} 0 & \text{si } t \geq \min_{1 \leq i \leq k} r_i \ , \\ \phi(n, 2^t m) & \text{si } t < \min_{1 \leq i \leq k} r_i \ . \end{cases}$$

Démonstration : on veut compter pour chaque p_i le nombre d'éléments de $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\star$ dont l'ordre est un diviseur de $2^t m$. Comme ce groupe est cyclique, c'est tout simplement

$$\mathrm{PGCD}\left(2^t m, (p_i - 1) p_i^{\alpha_i - 1}\right) = \mathrm{PGCD}\left(2^t m, 2^{r_i} m_i\right) \ ,$$

puisque p_i est premier à $2^t m$. On a donc :

$$\mathrm{PGCD}\left(2^t m, (p_i - 1) p_i^{\alpha_i - 1}\right) = 2^{\min(t, r_i)} u_i \ .$$

Par le lemme chinois, $\phi\left(n, 2^t m\right)$ est tout simplement le produit des nombres ci-dessus, d'où la première partie du lemme. Pour la deuxième, le nombre $\phi'(n, 2^t m)$ est l'ensemble des antécédants de -1 par le morphisme de groupe $m_t : x \longmapsto x^{2^t m}$ de $(\mathbb{Z}/n\mathbb{Z})^\star$ dans lui-même. On en déduit que $\phi'(n, 2^t m)$ est soit égal au cardinal du noyau de ce morphisme, c'est-à-dire à $\phi(n, 2^t m)$ si -1 est dans l'image et vaut 0 si -1 n'a pas d'antécédents.

Si $t \geq \min_{1 \leq i \leq k} r_i$, alors, il existe au moins un indice i_0 pour lequel $t \geq r_{i_0}$. Regardons alors la multiplication m_t (encore notée par la même lettre) modulo p_{i_0} :

$$\begin{array}{ccc} \left(\mathbb{Z}/p_{i_0}^{\alpha_{i_0}}\mathbb{Z}\right)^\star & \longrightarrow & \left(\mathbb{Z}/p_{i_0}^{\alpha_{i_0}}\mathbb{Z}\right)^\star \\ x & \longmapsto & x^{2^t m} \ . \end{array}$$

Le noyau de ce morphisme est un sous-groupe (cyclique) de $\left(\mathbb{Z}/p_{i_0}^{\alpha_{i_0}}\mathbb{Z}\right)^\star$ d'ordre

$$\mathrm{PGCD}(2^t m, 2^{r_{i_0}} m_{i_0} p_{i_0}^{\alpha_{i_0} - 1})$$

et son image est un sous-groupe d'ordre $2^{r_{i_0}} m_{i_0} / \mathrm{PGCD}(2^t m, 2^{r_{i_0}} m_{i_0} p_{i_0}^{\alpha_{i_0} - 1})$. Comme $t \geq r_{i_0}$, l'image est donc un sous-groupe d'ordre impair. Il n'a donc pas d'éléments d'ordre 2. Par conséquent, -1 n'est pas dans l'image du morphisme et $\phi'(n, 2^t m) = 0$. Inversement, si $t < \min_{1 \leq i \leq k}$, le même raisonnement montre que l'image de m_t est d'ordre pair modulo tout facteur (une puissance d'un) premier de n ; elle a donc un élément d'ordre 2. Par le lemme chinois, on en déduit l'existence d'un antécédent à -1. D'où le lemme.

Proposition 2.9. *Si n n'est pas premier,*

$$\mathrm{Card}(\mathcal{M})/\mathrm{Card}(G_0) \leq \frac{1}{4} \ ,$$

sauf si $n = 9$ auquel cas, le quotient vaut $1/3$.

Démonstration : quitte à réordonner les indices, on peut supposer que $r_1 = \min_{1\leq i\leq k}\{r_i\}$. Par définition de $\mathcal{M}$,

$$\mathrm{Card}(\mathcal{M}) = \phi(n,m) + \sum_{j=0}^{r_1-1} \phi'(n, 2^j m) \ .$$

Par suite, en tenant compte du lemme,

$$\mathrm{Card}(\mathcal{M}) = u_1 \dots u_k \left(1 + \sum_{j=0}^{r_1-1} 2^{kj}\right) \ .$$

Supposons $k \geq 3$; on utilise maintenant l'inégalité triviale $u_i \leq m_i$, et l'on en déduit :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{\left(1 + \sum_{j=0}^{r_1-1} 2^{kj}\right)}{2^{r_1+\dots+r_k} \prod_{i=1}^{k} p_i^{\alpha_i - 1}} \ .$$

Comme $\alpha_i \geq 1$, cette inégalité entraîne :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{\left(1 + \sum_{j=0}^{r_1-1} 2^{kj}\right)}{2^{kr_1}} \leq \frac{1}{2^{kr_1}} + \frac{2^{kr_1}-1}{2^{kr_1}(2^k-1)} \ ;$$

si $r_1 \geq 2$, on en tire :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{1}{2^{kr_1}} + \frac{2^{kr_1}-1}{2^{kr_1}(2^k-1)} \leq \frac{1}{64} + \frac{1}{7} \leq \frac{1}{4} \ ,$$

et enfin si $r_1 = 1$, on a :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{1}{2^k} + \frac{2^k-1}{2^k(2^k-1)} = \frac{1}{2^{k-1}} \leq \frac{1}{4} \ .$$

Supposons maintenant $k = 2$; si $u_1 = m_1$ et $u_2 = m_2$, alors, $r_2 \geq r_1 + 1$ (sinon, on aurait [4] $p_1 = p_2$) ; on a alors (en utilisant encore $\alpha_i \geq 1$) :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{\left(1 + \sum_{j=0}^{r_1-1} 2^{2j}\right)}{2^{2r_1+1} \prod_{i=1}^{2} p_i^{\alpha_i - 1}} \leq \frac{2}{3 \times 2^{2r_1+1}} + \frac{1}{2\times 3} \leq \frac{1}{12} + \frac{1}{6} \leq \frac{1}{4} \ .$$

4. En effet, dans le cas où $\alpha_1 = \alpha_2 = 1$, si $r_2 = r_1$, $p_i - 1$ divise $n - 1$ puisque la valuation en 2 de $n - 1$ est supérieure à r_1. Supposons $p_2 > p_1$; $p_2 - 1$ divise $n - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) + p_1 - 1$. Donc, $p_2 - 1$ divise $p_1 - 1$, ce qui est absurde. Si l'un des α_i est > 1, alors l'inégalité voulue est triviale.

Enfin, si $u_1 < m_1$ ou $u_2 < m_2$, le quotient $u_1u_2/(m_1m_2) \leq \frac{1}{3}$. Donc,

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{\left(1+\sum_{j=0}^{r_1-1} 2^{2j}\right)}{3\times 2^{2r_1}\prod_{i=1}^{2} p_i^{\alpha_i-1}} \leq \frac{1}{12}+\frac{1}{9} \leq \frac{1}{4} \ .$$

Pour finir, supposons $k = 1$. Dans ce cas, comme n n'est pas premier, $\alpha_1 \geq 2$ et par suite

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} \leq \frac{1}{p_1} \leq \frac{1}{5}$$

sauf si $n = 3^\alpha$, si $n \neq 9$ on a $\alpha \geq 3$ et le ratio est $\leq \frac{1}{9}$. Si $n = 9$, on a $u_1 = m_1 = m = 1$ et on a une formule exacte :

$$\frac{\mathrm{Card}(\mathcal{M})}{\mathrm{Card}(G_0)} = \frac{2}{6} = \frac{1}{3} \ .$$

2.3 Critère de Lucas

On rappelle l'énoncé classique de théorie des groupes

Lemme 2.10. *Soit G un groupe abélien fini et $S \subset G$, il existe un élément de G dont l'ordre est le* PPCM *des éléments de S. En particulier, il existe dans G un élément a dont l'ordre est multiple de l'ordre de chaque élément de G.*

Démonstration : par récurrence, il suffit de démontrer si G possède deux éléments g, h d'ordre respectivement m et n, il possède un élément d'ordre $\mathrm{PPCM}(m,n)$. Comme $v_p(\mathrm{PPCM}(m,n)) = \max(v_p(m), v_p(n))$, on peut écrire $m = m'm''$ et $n = n'n''$, où les facteurs premiers de m' et n' sont ceux tels que $v_p(m) \geq v_p(n)$, ceux de m'' et n'' étant ceux tels que $v_p(n) > v_p(m)$. Dans ces conditions, on a $\mathrm{PPCM}(m,n) = m'n''$. Posons $a = g^{m''}$ et $b = h^{n'}$; l'ordre de a est exactement m' et celui de b vaut n''. Comme m' et n'' sont premiers entre eux, l'ordre de ab est $m'n''$, ce que l'on voulait.

Nous pouvons maintenant énoncer le théorème qui donne le critère de primalité de Lucas-Lehmer.

Théorème 2.11. *Soit n un entier > 1. Supposons que pour tout facteur premier p de $n-1$, il existe un entier a tel que $a^{n-1} \equiv 1 \bmod n$ et $a^{(n-1)/p} \not\equiv 1 \bmod n$. Alors, n est un nombre premier.*

Démonstration : soit p un facteur premier de $n-1$ et a_p un entier vérifiant l'hypothèse du théorème. On remarque que forcément (a_p, n) sont premiers entre eux car a_p est inversible dans $(\mathbb{Z}/n\mathbb{Z})^\star$. Il existe donc un élément $a \in (\mathbb{Z}/n\mathbb{Z})^\star$ dont l'ordre est le PPCM des ordres des a_p. Comme l'ordre de a_p divise $(n-1)$ mais pas $(n-1)/p$; il en est de même pour leur PPCM d. Ainsi, $d \mid n-1$ mais ne divise aucun diviseur strict de $(n-1)$ (ils divisent tous l'un au moins des $(n-1)/p$). En conclusion, $d = n-1$ et $n-1 \geq \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\star) \geq \mathrm{ordre}(a) = n-1$. On a donc égalité, ce qui force n à être premier.

Dans la pratique ce critère marche très bien si l'on connait la factorisation de $n-1$... Ce qui fait son défaut, car il existe de nombreux cas où l'on ne sait pas factoriser rapidement $n-1$.

Exemple 2.12. *Prenons* $n = 19$ *; on a* $n-1 = 2\times 3^2$*. Il faut trouver un élément* a_2 *dont l'ordre divise* 18 *mais pas* 9 *et un élément* a_3 *dont l'ordre divise* 18 *mais pas* 6*. Pour* a_2*, c'est facile, il suffit de prendre* $a_2 = -1$ *son ordre est deux, donc il divise 18 mais pas* 9*. Prenons maintenant* $a_3 = 2$*. On a* $2^6 = 64 = 7 \neq 1 \bmod 19$*, donc son ordre ne divise pas* 6*, mais* $7^3 \equiv 7\times 49 \equiv 7\times 11 \equiv 77 \equiv 1 \bmod 19$*, donc l'ordre de* 2 *divise* 18*. Par conséquent* 19 *est premier.*

L'autre qualité de ce critère est qu'il fournit un certificat de primalité. N'importe qui à qui on donne $a_2 = -1$, $a_3 = 2$ (et la décomposition en facteurs premiers de 18) peut vérifier instantanément que 19 est premier. Un autre avantage du critère est qu'il s'applique fort bien au cas particulier des nombres de Fermat.

Il est néanmoins utile lorsque n est un nombre de Fermat (critère de Pépin et Proth).

Définition 2.13. *Soit r un entier ≥ 0 le r-ième nombre de Fermat est*

$$F_r = 2^{2^r} + 1 \ .$$

Corollaire 2.14. *Soit r un nombre entier ≥ 2. Pour que le nombre de Fermat F_r soit un nombre premier, il faut et il suffit que l'on ait l'une des congruences suivantes :*

(i)

$$3^{(F_r-1)/2} \equiv -1 \bmod F_r \ ;$$

(ii)

$$5^{(F_r-1)/2} \equiv -1 \bmod F_r \ .$$

Démonstration : comme 2 est le seul facteur premier de $F_r - 1$, les conditions suivantes nous assurent que l'ordre de 3 et celui de 5 ne divisent pas $(F_r - 1)/2$. Elles assurent aussi que l'ordre de 3 et de 5 divisent $F_r - 1$ (il suffit d'élever au carré les hypothèses). Le critère de Lucas nous garantit donc que sous l'une de ces hypothèses, F_r est premier. Inversement supposons que F_r est premier. Nous allons montrer que ces congruences sont vraies. Calculons le symbole $\left(\frac{3}{F_r}\right)$. Par la loi de la réciprocité quadratique,

$$\left(\frac{3}{F_r}\right) = (-1)^{2^{2^r-1}} \left(\frac{F_r}{3}\right) = \left(\frac{F_r}{3}\right) \ .$$

Comme $F_r \equiv 1 + (-1)^{2^r} \equiv 2 \bmod 3$,

$$\left(\frac{F_r}{3}\right) = -1 \ .$$

Comme F_r est premier, 3 n'est pas un carré modulo F_r et la congruence (i) est automatique. Passons maintenant à 5. On a de même :

$$\left(\frac{5}{F_r}\right) = (-1)^{2\times 2^{2^r-1}} \left(\frac{F_r}{5}\right) = \left(\frac{F_r}{5}\right) \ .$$

Calculons maintenant le symbole $\left(\frac{F_r}{5}\right)$. Comme $F_r \equiv 1 + 4^{2^{r-1}} \equiv 1 + (-1)^{2^{r-1}} \equiv 2 \bmod 5$ (car $r \geq 2$), et comme 2 n'est pas un carré modulo 5, on a aussi

$$\left(\frac{5}{F_r}\right) = -1 \ ,$$

Nous allons maintenant, pour son intérêt algorithmique donner une nouvelle preuve du résultat que nous avons déjà vu sur les sous-groupes multiplicatifs finis d'un corps.

Théorème 2.15. *Soit K un corps et soit G un sous-groupe fini de $K^\star$. Alors G est cyclique.*

Démonstration : soit n l'ordre de G. D'après le lemme précédent et par récurrence, il suffit de produire, pour tout facteur premier p de n, un élément g_p de G dont l'ordre est $p^{v_p(n)}$. En effet, le produit des g_p sera un élément de G d'ordre égal au PPCM de ces ordres, c'est à dire à leur produit qui vaut n.

Comme K est un corps, l'équation polynomiale $x^{n/p} = 1$ a au plus n/p racines ; comme G est d'ordre $n > n/p$, il existe donc un élément x de G tel que $x^{n/p} \neq 1$ (sinon, tous les éléments de G seraient racine de l'équation, ce qui donnerait $n > n/p$ racines). Posons alors $g_p = x^{n/p^r}$. On a $g_p^{p^r} = x^n = 1$ par le théorème de Lagrange, mais $g_p^{p^{r-1}} = x^{n/p} \neq 1$. Par suite, l'ordre de g_p est un diviseur de p^r qui ne divise pas p^{r-1} ; c'est donc exactement p^r et g_p est bien l'élément cherché si l'on a pris soin de prendre $r = v_p(n)$.

L'intérêt de la seconde démonstration est qu'elle se prête au calcul effectif d'un générateur. Montrons-le sur un exemple.

Exemple 2.16. *Considérons le groupe multplicatif $(\mathbb{Z}/71\mathbb{Z})^\star$. Son ordre est $70 = 2 \times 5 \times 7$. D'après notre travail précédent, nous devons trouver des éléments g_2, g_5, g_7 d'ordre respectivement 2, 5 et 7. Pour 2, c'est facile, il suffit de poser $g_2 = -1$ qui est d'ordre 2. Passons à 5 et posons $x = 2$. On a*

$$2^{14} = 2^6 \times 2^6 \times 4 \equiv (-7)^2 \times 4 = 54 \bmod 71 \ .$$

Donc, l'ordre de 2 est un multiple de 5. Comme 5 est premier et comme $2^{5\times 14} = 1$, on sait que $q_5 = 54$ conviens. Passons maintenant à 7. Essayons encore avec $x = 2$. On a

$$2^{10} \equiv 2^6 \times 16 \equiv -7 \times 16 \equiv 30 \bmod 71 \ .$$

Donc, l'ordre de 2 est un multiple de 7 et $g_7 = 30$ conviens.

Par conséquent,

$$g_2 g_5 g_7 \equiv 13 \bmod 71$$

est un générateur de $(\mathbb{Z}/71\mathbb{Z})^\star$.

Remarque 2.17. *On peut raisonner à l'envers et se demander, un entier a étant donné, pour quels nombres premiers p est-ce que a est un générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\star$. Pour qu'un tel nombre premier impair existe, une condition nécessaire évidente est que a ne soit pas un carré : si p est impair, les carrés de $(\mathbb{Z}/p\mathbb{Z})^\star$ forment un sous-groupe strict. De même, $a = -1$ n'est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\star$ que si $p = 2$ ou $p = 3$. Une conjecture du mathématicien Emil Artin est que ces deux conditions nécessaires sont suffisantes pour qu'il existe une infinité de tels nombres premiers. Cette conjecture est toujours ouverte : on ne connaît à ce jour aucun nombre entier a pour lequel on sache qu'elle est vérifiée. Cependant, C. Hooley a démontré en 1967 qu'elle est vérifiée si l'hypothèse de Riemann généralisée l'est, tandis que R. Heath-Brown (1985), généralisant des travaux de R. Gupta et M. Ram Murty (1984), a montré qu'elle est vérifiée pour tout nombre premier a sauf au plus 2. Par exemple, des entiers $3, 5$ et 7, au moins l'un est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\star$ pour une infinité de nombre premiers p.*

2.4 Critère d'Agrawal-Kayal-Saxena

Nous présentons maintenant le critère dit « AKS », d'Agrawal, Kayal et Saxena. c'est un théorème très récent (2002) et le seul connu à ce jour qui permet de déterminer en « temps polynomial » (c'est-à-dire avec un nombre d'opérations élémentaires polynomial en $\log(n)$) de manière inconditionnelle

si n est premier ou non. Tous les autres tests, fonctionnent soit de manière certaine, mais avec des temps non polynomiaux en $\log(n)$ (par exemple le test de Fermat) ou de manière rapide, mais seulement pour une classe de nombres (pour Lucas, ce sont les entiers n dont on connait la factorisation de $n-1$), ou encore de manière probabiliste (Miller-Rabin), ou conditionnelle à une conjecture non connue (Hypothèse de Riemann pour Miller- Rabin). Nous démontrerons tout d'abord une version élémentaire, mais conditionnelle du résultat, puis une preuve élémentaire, mais inconditionnelle.

L'idée de départ de l'algorithme est de faire des tests sur l'anneau $\mathbb{Z}[X]$. Par exemple, on a

Lemme 2.18. *Soit n un entier ≥ 2 et $a \in \mathbb{Z}$, premier à n. Alors,*

$$(X-a)^n \equiv x^n - a \bmod n$$

pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^\star$ si et seulement si n est premier.

Démonstration : supposons que n est premier. Alors, par la formule du binôme,

$$(X-a)^n \equiv X^n - (a^n) \equiv X^n - a \bmod n$$

puisque tous les coefficients binomiaux intermédiaires sont nuls modulo n. Inversement, si cette relation est vraie, tous les coefficients binomiaux $\left(\begin{array}{c} n \\ i \end{array}\right)$ pour $i \neq 0, n$ sont des multiples de n. Soit donc p un nombre premier divisant n et $k = v_p(n)$. Considérons alors le binomial $\left(\begin{array}{c} n \\ p \end{array}\right)$. Il est facile de vérifier encore que la valuation en p de ce coefficient est exactement :

$$v_p(n) - 1 = k - 1 \ .$$

Ainsi, ce coefficient binomial n'est pas nul modulo n et le polynôme $(X-a)^n$ a donc un coefficient de degré p non nul modulo n.

L'ennui de ce lemme, est qu'il nécessite de faire déjà $n+1$ identifications de monômes, soit certainement un temps exponentiel.

On peut facilement réduire ce temps de calcul en remarquant :

Lemme 2.19. *Soit n un nombre premier, $h(X) \in \mathbb{Z}[X]$ un polynôme et a un entier ; alors,*

$$(x-a)^n \equiv x^n - a \bmod (n, h(X)) \ ,$$

où la congruence est cette fois prise modulo l'idéal de $\mathbb{Z}[X]$ engendré par n et $h(X)$.

Démonstration : elle est immédiate par le lemme précédent. L'ennui est que maintenant la réciproque n'est pas toujours vraie. Le but du jeu sera de montrer que pour h astucieusement choisi et si la relation ci-dessus est vraie pour un nombre suffisant de classes a modulo n, alors, pour n assez grand, n est forcément une puissance d'un nombre premier. Si le degré de h est assez petit, le nombre d'opérations élémentaires nécessaires pour vérifier l'égalité est polynomial. On peut vérifier que pour tout $\varepsilon > 0$, ce dernier est un $O_\varepsilon((\deg(h)\log(n)^2)^{1+\varepsilon})$.

Passons maintenant aux préliminaires proprement dit.

Définition 2.20. *Soit p un nombre premier. On dit que p est un premier de Sophie Germain si $\ell = (p-1)/2$ est aussi premier.*

On dispose alors de la conjecture de Sophie Germain :

Conjecture 2.21. *Soit x un nombre réel ≥ 2. On note*

$$G(x) = \mathrm{Card}\left(\{p \leq x, p \text{ de Sophie Germain}\}\right) \ .$$

Alors, il existe une nombre réel $c_0 > 0$ tel que :

$$G(x) \sim_{x\to\infty} \frac{c_0 x}{\log(x)^2} \ .$$

Lemme 2.22. *Supposons la conjecture de Sophie Germain vraie, et soit n un entier ≥ 2. Soit encore m un entier $\geq \log(n)\log\log(n)^2$, et $c > 0$ un nombre réel assez grand. Alors, pour tout $M \geq cm$, il existe un nombre premier de Sophie Germain r, $M \leq r \leq 2M$ tel que*

$$n^2 - 1 \not\equiv 0 \bmod r \ .$$

Démonstration : soit n, m, M comme dans le lemme. Comme n^2-1 a au plus $2\log(n)$ facteurs premiers, il suffit de montrer qu'il existe plus de premiers de Sophie Germain dans l'intervalle considéré.

Pour M assez grand, $G(2M) \geq \frac{1.5c_0M}{\log(M)^2}$ et $G(M) \leq \frac{1.25c_0M}{\log(M)^2}$. La différence

$$G(2M) - G(M) \geq \frac{c_0 M}{4\log(M)^2} \ .$$

En conclusion, si

$$\frac{c_0 M}{4\log(M)^2} > 2\log(n) \ ,$$

on est sûr de pouvoir trouver un premier de Sophie Germain vérifiant les propriétés requises. Mais, cette inégalité est surement vraie dès que m dépasse l'ordre de grandeur de $\log(n)\log\log(n)^2$. C'est précisément l'hypothèse qui est faite pour m. D'où le lemme.

Nous énonçons maintenant un lemme de nature combinatoire très classique :

Lemme 2.23. *Soient s, k des entiers ≥ 1. Alors,*

$$\mathrm{Card}\left(\left\{(m_1,\ldots,m_s) \in \mathbb{N}^s, \sum_{j=1}^{s} m_j \leq k\right\}\right) = \left(\begin{array}{c} s+k \\ k \end{array}\right) \geq 2^{\min\{s,k\}} \ .$$

On notera que le cardinal calculé est aussi celui des monômes en s variables de degré total $\leq k$.

Démonstration : on calcule le cardinal par récurrence. Si on note $f(s,k)$ ce nombre, on a facilement $f(s,0) = 1$, $f(1,k) = k+1$. On vérifie ensuite que

$$f(s,k) = f(s,k-1) + f(s-1,k) \ .$$

En effet, l'ensemble $\mathcal{A}(s,k)$ qui nous intéresse se décompose en une union disjointe :

$$\mathcal{A}(s,k) = \mathcal{A}(s,k-1) \cup \mathcal{B}(s,k) \ ,$$

où $\mathcal{B}(s,k) = \left\{(m_1,\ldots,m_s) \in \mathbb{N}^s, \sum_{j=1}^s m_j = k\right\}$. Mais, $k - m_s$ parcourt toutes les valeurs de 0 à k une et une seule fois quand m_s parcourt $\{0,\ldots,k\}$. Par suite, $\mathcal{B}(s,k)$ est en bijection avec $\mathcal{A}(s-1,k)$ et a donc même cardinal. Ceci montre la relation par récurrence.

Par les relations connues sur le triangle de Pascal :

$$\left(\begin{array}{c} s+k \\ k \end{array}\right) = \left(\begin{array}{c} s+k-1 \\ k-1 \end{array}\right) + \left(\begin{array}{c} s+k-1 \\ k \end{array}\right) \ ,$$

on peut donc identifier les deux membres puisque $\mathcal{A}(s,k)$ plus les binomiaux vérifient les mêmes conditions initiales.

Pour la minoration, on utilise tout simplement en supposant $k \leq s$:

$$\begin{aligned} \left(\begin{array}{c} s+k \\ k \end{array}\right) &= \frac{(s+k)\cdot(s+k-1)\cdots(s+2)\cdot(s+1)}{k\cdot(k-1)\cdots 2\cdot 1} \\ &= \prod_{i=0}^{k-1}\left(\frac{s+k-i}{k-i}\right) \\ &\geq 2^k \ . \end{aligned}$$

Nous donnons maintenant le théorème d'arithmétique voulu. Dans tout la suite, si a, r sont deux entiers premiers entre eux, on notera $o_r(n)$ l'ordre de n dans le groupe $(\mathbb{Z}/r\mathbb{Z})^\star$.

Théorème 2.24. *Soit $n \geq 2$ un entier ; on suppose*
(i) n n'est pas une puissance pure (c'est-à-dire que $n \neq b^t$, avec b entier et $t \geq 2$) ;
On se donne maintenant un entier r tel que $o_r(n) \geq 16\log(n)^2+1$ et l'on pose $S = [4\sqrt{\varphi(r)}\log(n)]$ où $[\cdot]$ désigne la partie entière de $\cdot$. On suppose de plus :
(ii) n n'a pas de facteurs premiers $\leq r$.
Alors,
(a) si $n \leq r$, alors n est premier ;
(b) si pour tout $1 \leq a \leq S$, on a

$$(x-a)^n \equiv x^n - a \bmod (n, (X^r-1)) \ ,$$

n est premier.
(c) n est composé dans tous les autres cas.

Démonstration : soit p un nombre premier divisant n ; nous savons que le polynôme cyclotomique Φ_r est produit de k facteurs tous de degré $d_p = o_r(p)$. Notons $h(X)$ l'un de ces facteurs et $d = \text{PPCM}(o_r(p), o_r(n))$. Soit $h(X)$ un facteur irréductible de $X^r - 1$ sur $\mathbb{F}_p$ de degré d_p et posons $K = \mathbb{F}_p[X]/(h(X))$. C'est un corps à p^{d_p} éléments.

Notons maintenant G le sous-groupe de $K^\star$ engendré par les $X - a$, $1 \leq a \leq S$. Nous allons maintenant minorer le cardinal de G.

Lemme 2.25. *Avec les notations ci-dessus,*

$$\text{Card}(G) \geq 2^{\min\{S, d-1\}} \ .$$

Démonstration : considérons deux monômes de la forme

$$g_1(X) = \prod_{1 \leq a \leq S} (X-a)^{\alpha_a}, \qquad g_2(X) = \prod_{1 \leq b \leq S} (X-b)^{\alpha_b} \ .$$

Tout d'abord, comme $a, b \leq S$, on a $a, b \leq r$. En effet, par hypothèse $a, b \leq S \leq 4\sqrt{r}\log(n)$. Mais $r \geq o_r(n) \geq 16\log(n)^2 + 1$. Par conséquent, $S \leq r$. Comme par hypothèse, n n'a pas de diviseur premier $\leq r$, on en déduit que $a \equiv b \bmod p$ si et seulement si $a = b$. Il suit que deux tels monômes ne peuvent être égaux sur $\mathbb{F}_p[X]$ que s'il le sont sur $\mathbb{Z}[X]$.

On note maintenant que l'on a à la fois

$$g_i(X)^n \equiv g(X^n) \bmod (p, h(X)) \ , \qquad g_i(X)^p \equiv g(X^p) \bmod (p, h(X)) \ .$$

Le première relation vient de notre hypothèse et la seconde est l'action du Frobenius. Par récurrence, pour tout $n^i p^j$, on a encore :

$$g_i(X)^{n^i p^j} \equiv g(X^{n^i p^j}) \bmod (p, h(X)) \ .$$

Supposons maintenant que

$$g_1(X) \equiv g_2(X) \bmod (p, h(X)) \ ,$$

et notons x la classe de X dans le quotient $K = \mathbb{F}_p[X]/(h)$. On a donc d'une part $x^r = 1$ (x est une racine primitive r-ième de l'unité), et

$$(g_1 - g_2)(x^{n^i p^j}) = 0 \ , \qquad \text{pour tout } (i,j) \in \mathbb{N}^2 \ .$$

L'ensemble de $n^i p^j$ décrivant un sous-groupe d'ordre d de $(\mathbb{Z}/r\mathbb{Z})^\star$, le polynôme $g_1 - g_2$ possède au moins d racines dans K. Ceci entraîne donc que son degré est au moins d.

Par conséquent, si on suppose que $\deg(g) \leq d - 1$, on est certain que les monômes écrit ci-dessus sont deux à deux distincts dans K.

Le lemme combinatoire ci-dessus nous assure donc que

$$\text{Card}(G) \geq \mathcal{A}(S, d-1) \geq 2^{\min(S, d-1)} \ .$$

Dans un deuxième temps, nous allons majorer le cardinal de G. Soit donc g un générateur de G et $o(g)$ son ordre.

On introduit l'ensemble :

$$\mathcal{I} = \{m \in \mathbb{N}, g(X)^m = g(X^m) \bmod (n, h(X))\} \ .$$

On dispose alors du lemme

Lemme 2.26. *L'ensemble $\mathcal{I}$ vérifie les propriétés suivantes :*
(i) $n \in \mathcal{I}$, $p \in \mathcal{I}$;
(ii) l'ensemble $\mathcal{I}$ est multiplicatif (stable par multiplication) ;
(iii) si $m_1, m_2 \in \mathcal{I}$ vérifient $m_1 \equiv m_2 \bmod r$, alors $o(g) \mid (m_1 - m_2)$.

Démonstration : on a déjà vu (i) et implicitement (ii). Précisons ce point : soient m_1, m_2 deux éléments de $\mathcal{I}$:

$$g(X)^{m_1 m_2} \equiv g(X^{m_1})^{m_2} \bmod (p, h(X)) \ .$$

Comme $m_2 \in \mathcal{I}$, en faisant le changement de variables $Y = X^{m_1}$, on en déduit :

$$g(Y)^{m_2} \equiv g(Y^{m_2}) \bmod (p, h(X)) \ .$$

Le point (ii) en découle en remplaçant Y par sa valeur.

Passon à (iii), et posons $m_2 = m_1 + \ell r$ avec ℓ entier. On a

$$g(X)^{m_2} \equiv g(X^{m_1 + r\ell}) \equiv g(X^{m_1}) \bmod (p, h(X)) \ ,$$

puisque x est une racine de l'unité d'ordre r. Comme $m_1 \in \mathcal{I}$, on a donc

$$g(X)^{m_2} \equiv g(X)^{m_1} \bmod (p, h(X)) \ ,$$

et donc $o(g) \mid m_1 - m_2$. On en déduit la majoration suivante pour $\mathrm{Card}(G)$:

Lemme 2.27. *On a*

$$\mathrm{Card}(G) \leq \exp(2\sqrt{d}\log(n)) \ .$$

Démonstration : considérons l'ensemble $\{n^i p^j, 0 \leq i \leq \sqrt{d}, 0 \leq j \leq \sqrt{d}\}$. Cet ensemble de couples d'entiers est de cardinal $([\sqrt{d}]+1)^2 > d$. On peut donc trouver (i_1, j_1) et (i_2, j_2) avec $(i_1, j_1) \neq (i_2, j_2)$ dans cet ensemble qui vérifient

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \bmod r \ ,$$

puisque l'ordre du groupe engendré par n et p dans $(\mathbb{Z}/r\mathbb{Z})^\star$ est précisément d.

Par le lemme précédent,

$$\mathrm{Card}(G) = o(g) \mid \left| n^{i_1} p^{j_1} - n^{i_2} p^{j_2} \right| \ .$$

Le membre de droite ne peut pas être nul car sinon, n serait une puissance de p, ce que nous avons exclu. Par suite, l'inégalité triangulaire assure :

$$\mathrm{Card}(G) \leq \exp(2\sqrt{d}\log(n)) \ .$$

Nous pouvons maintenant conclure. On a :

$$2^{\min(S,d-1)} \leq \mathrm{Card}(G) \leq \exp(2\sqrt{d}\log(n)) \ .$$

Ceci se traduit par :

$$\log(2)\min(S, d-1) \leq 2\sqrt{d}\log(n) \ .$$

L'inégalité est impossible si le minimum est atteint pour d car par hypothèse $d \geq 16\log(n)^2 + 1$ et donc

$$4\log(2)\log(n) - \frac{\log(2)}{4\log(n)} \leq 2\log(n) \ ,$$

qui est absurde. De même si $S \leq d-1$, on doit avoir

$$\log 2(4\sqrt{\varphi(r)}\log(n) - 1) \leq 2\sqrt{d}\log(n) \ .$$

Cette dernière inégalité est également absurde puisque $\varphi(r) \geq d$. Le théorème est donc entièrement établi.

Nous allons maintenant passer à la deuxième partie de la preuve : montrer que l'on peut effectivement trouver un entier r vérifiant les hypothèses requises. Nous décrirons ensuite brièvement l'algorithme et discuterons de sa « complexité».

Proposition 2.28. *Supposons la conjecture de Sophie Germain vraie. Alors, Il existe une constante $c_1 > 0$, tel que pour tout entier $n \geq c_1$, on puisse trouver un nombre premier de Sophie Germain r avec*

$$r \leq c_1 \log(n)^2 \ , \qquad et \qquad o_r(n) \geq 16 \log(n)^2 + 1 \ .$$

Démonstration : on applique le lemme ci-dessus avec

$$M = \max\{32 \log(n)^2 + 2, c \log(n) \log\log(n)^2\} \ .$$

Il existe donc un nombre de Sophie Germain r compris entre M et $2M$ tel que $n^2 - 1 \not\equiv 1 \bmod r$. Posons $\ell = (r-1)/2$. Comme $(\mathbb{Z}/r\mathbb{Z})^\star$ est cyclique d'ordre 2ℓ, avec ℓ premier, et comme n n'est pas d'ordre 1 ou 2 dans ce groupe cyclique, il est d'ordre ℓ ou 2ℓ qui est par choix de M surement $\geq 16 \log(n)^2 + 1$. D'où la proposition.

Comme la conjecture de Sophie Germain n'est pas connue, on est obligé de prendre r sensiblement plus grand pour assurer un ordre de n assez grand dans le groupe cyclique $(\mathbb{Z}/r\mathbb{Z})^\star$.

On a toutefois :

Proposition 2.29. *Il existe des nombres réels c_1, c_2 tel que pour tout entier $n \geq c_1$, il existe un nombre premier r,*

$$r \leq c_2 \log(n)^5 \ , \qquad et \qquad o_r(n) \geq 16 \log(n)^2 + 1 \ .$$

Démonstration : fixons un entier $a \geq 1$; dire que $o_r(n) \geq a + 1$ reviens à dire que

$$B(a) = \prod_{j=1}^{a} (n^j - 1) \not\equiv 0 \bmod r \ ;$$

Par ailleurs,

$$\log(B(a)) \leq \sum_{j \leq a} j \log(n) \leq \frac{a(a+1)\log(n)}{2} \ .$$

De plus, on sait que qu'il existe $c > 0$ tel que pour tout $x \geq 2$,

$$\sum_{p \in \mathcal{P},\ p \leq x} \log(p) \geq cx \ ,$$

il en résulte que si

$$cx > \frac{a(a+1)\log(n)}{2} \ ,$$

alors, il existe un premier $r \leq x$ qui ne divise pas $B(a)$. En faisant, $a = 16 \log(n)^2 + 1$, la proposition suit.

D'un point de vue algorithmique, on procède comme suit étant donné un entier n.

(i) si n est une puissance pure, alors, n est composé. Sinon, on passe à l'étape (ii).
(ii) On recherche le plus petit premier r tel que $o_r(n) \geq 16\log(n)^2 + 1$.
(iii) On teste les PGCD (a, n) pour tous les $a \leq r$. Si l'un deux est > 1 alors n est composé ; sinon on passe à l'étape suivante.
(iv) si $n \leq r$, alors, n est premier ; sinon on passe à l'étape suivante.
(v) Pour $a = 1, \ldots, S = [2\sqrt{\varphi(r)}\log(n)]$, on teste

$$(x-a)^n - x^n - a \bmod (n, X^r - 1) \ .$$

Si l'une des congruences est non nulle, n est composé ; sinon, il est premier.

Il est facile de voir que c'est l'étape (v) qui demande le plus d'opérations élémentaires. Nous allons rapidement expliquer comment on estime ces dernières. Il faut faire S opérations successives. Chacune d'elle est une élévation à la puissance n (ce qui donne de l'ordre de grandeur de $\log(n)$ opérations élémentaires). Multiplier des polynômes de degré r avec des coefficients de l'ordre de grandeur de n demande de l'ordre de grandeur de $r\log(n)$ opérations élémentaires (avec une transformée de Fourier rapide) ou $r^2\log(n)$ opérations élémentaires (avec une multiplication standard). Au total, on voit que l'ordre de grandeur de la complexité de l'algorithme tel qu'il est esquissé ici est $\log(n)^{10,5}$. On peut améliorer cette dernière soit en utilisant des conjectures (Sophie Germain donne un exposant 6, un théorème de théorie analytique des nombres joint à des arguments plus sophistiqués permet d'atteindre la même complexité inconditionnellement, on peut même descendre conditonnellement à un exposant 4. Nous ne rentrerons pas dans ces détails ici.

2.5 Factorisation de polynômes sur les corps finis

Nous allons maintenant décrire comment on peut décider si un polynôme sur un corps fini est irréductible ou non et dans ce cas, comment le factoriser. En principe, comme il n'y a qu'un nombre fini de facteurs possibles, il suffit de tous les tester. Mais, comme dans le cas des entiers, cette méthode est très vite impraticable dès que le cardinal du corps est grand ou que le degré du polynôme est important.

Soit F un corps fini de cardinal q et soit $f \in F[x]$ un polynôme de degré n. Il s'agit pour l'instant de décider si f est irréductible ou non.

Le premier pas consiste à détecter les facteurs multiples en dérivant. Un polynôme g tel que $g' = 0$ est un polynôme en x^p (où p est la caractéristique) ; comme tout élément de F est une puissance p-ième, chacun des monômes de g est une puissance de p, donc g aussi. En particulier, g n'est pas irréductible. Inversement, la dérivée d'un polynôme irréductible est non nulle.

Notons $f = \prod_{i=1}^r f_i^{e_i}$ la décomposition de f en facteurs irréductibles. Supposons $f' \neq 0$, de sorte qu'au moins un des e_i n'est pas multiple de p. On a

$$f' = \sum_{i=1}^r e_i f_i^{e_i - 1} f_i' \prod_{j \neq i} f_i^{e_j} \ .$$

Ainsi, un facteur irréductible commun de f et f' étant l'un des f_i, sa multiplicité se lit dans la formule ci-dessus : f_i apparait toujours avec une multiplicité au moins $e_i - 1$ et exactement $e_i - 1$ une et une seule fois si e_i n'est pas un multiple de p.

En comparant avec f, on en déduit donc que

$$\mathrm{PGCD}(f, f') = \prod_{i=1, p\nmid e_i}^{r} f_i^{e_i - 1} \prod_{i=1, p|e_i} f_i^{e_i} \ .$$

On introduit maintenant :

$$g_1 = f/\mathrm{PGCD}(f, f') \ ;$$

g_1 est exactement le produit des facteurs irréductibles f_i pour lesquels e_i n'est pas multiple de p.

On peut réitérer le procédé avec f/g_1 qui a la même décomposition en facteurs irréductibles que f, les exposants non multiples de p ayant simplement diminué de 1. On obtient alors le produit g_2 des facteurs irréductibles f_i pour lesquels $e_i \geq 2$ et $e_i(e_i - 1)$ n'est pas multiple de p. Au bout de $p - 1$ opérations, l'exposant de f_i dans la décomposition de $f/(g_1 ... g_{p-1})$ est un multiple de p. Ce polynôme est donc la puissance p-ième d'un polynôme h qu'on peut déterminer explicitement et avec lequel on continue.

Proposition 2.30. *Pour que f soit irréductible, il faut et il suffit que les polynômes $x^{q^e} - x$ et f soient premiers entre eux pour tout $1 \leq e \leq [n/2]$.*

Démonstration : soit ξ une racine de f dans une clôture algébrique $\bar{F}$ de F. Son polynôme minimal g est irréductible et divise f, donc est un facteur irréductible de f. De plus, le corps $F[\xi]$ est un corps fini de cardinal q^e , où $e = \deg(g)$. On en déduit que $\xi^{q^e} = \xi$, et donc que les polynômes $x^{q^e} - x$ et f ont une racine commune dans $F[\xi]$. Cela entraîne que leur pgcd n'est pas égal à 1. Si g est le facteur irréductible de plus petit degré de f, on a $e \leq n/2$. Inversement, si f et $x^{q^e} - x$ ont un facteur irréductible commun, celui-ci sera de degré au plus e, donc distinct de f si $\leq n/2$.

On peut généraliser ce résultat pour obtenir une factorisation de f en un produit de polynômes f_e, chaque facteur irréductible de f_e étant de degré e. Pour simplifier, on suppose que f est sans facteur multiple.

Proposition 2.31. *Soit $f \in F[x]$ un polynôme sans facteur multiple. Posons $g_0 = f$; pour $e \geq 1$, posons $f_e = \mathrm{PGCD}(x^{q^e} - x, g_{e-1})$ et $g_e = g_{e-1}/f_e$. On a $f = f_1 f_2 ...$ et pour tout $e \geq 1$, chaque facteur irréductible de f_e est degré e.*

Démonstration : fixons pour la démonstration une clôture algébrique Ω de F et notons $\mathbb{F}_{q^e}$ l'unique sous-corps de Ω de cardinal $\mathbb{F}_{q^e}$. Comme dans la démonstration précédente, les racines de f_1 sont les racines de f qui appartiennent à $\mathbb{F}_q$. Comme les racines de f sont simples, il en est de même de celles de f_1 et le polynôme f_1 est le produit des facteurs linéaires qui divisent f. Les racines de f_2 sont les racines de $g_1 = f/f_1$ qui appartiennent à $\mathbb{F}_{q^2}$; ce sont donc les racines de f qui appartiennent à $\mathbb{F}_{q^2}$ mais pas à $\mathbb{F}_q$ (ces dernières sont racines de f_1 et ne sont plus racines de g_1 car les racines de f sont simples). Par récurrence, les racines de f_e sont les racines de f qui appartiennent à $\mathbb{F}_{q^e}$ mais à aucun des corps $\mathbb{F}_{q^r}$ pour $1 \leq r < e$; l'extension de $\mathbb{F}_q$ engendrée par une telle racine est $\mathbb{F}_{q^e}$, si bien que son polynôme minimal est de degré e sur F.

On en déduit le nombre de facteurs irréductibles de f.

Proposition 2.32. *Supposons que f soit sans facteur carré et notons n son degré. Pour $1 \leq e < n$, soit g_e le reste de la division euclidienne du polynôme $x^{qe} - x^e$ e par f. Soit k le rang du sous-espace de $F[x]$ engendré par les polynômes $g_1, \ldots, g_{n-1}$. Le nombre de facteurs irréductibles distincts de f est égal à $n - k$.*

Démonstration : soit A l'algèbre $F[x]/(f)$ et munissons-la de la base standard sur F, à savoir $(1, x, \ldots, x^{n-1})$. Soit σ l'application de A dans elle-même donnée par $\sigma(a) = a^q$. C'est un homomorphisme d'algèbres. On a par définition $\sigma(1) - 1 = 0$ et $g_e = \sigma(x^e) - x^e$ pour tout $1 \leq e < n$.

Nous devons donc démontrer que le noyau de $\sigma - \mathrm{Id}$ est un F-espace vectoriel de dimension égale au nombre r de facteurs irréductibles de f. Notons $B = \ker(\sigma - \mathrm{Id})$; c'est donc une sous-algèbre de A qu'on appelle la sous-algèbre de Berlekamp de A. Nous allons montrer qu'elle est isomorphe à F^r. écrivons la décomposition de f en produits de facteurs irréductibles, $f = f_1 \ldots f_r$. Ils sont deux à deux premiers entre eux ; d'après le lemme chinois, l'algèbre A est donc isomorphe à

$$\prod_{i=1}^{r} F[x]/(f_i)$$

et σ s'identifie à l'endomorphisme $(a_1, \ldots, a_r) \longmapsto (a_1^q, \ldots, a_r^q)$. Par suite, l'image de B par l'isomorphisme chinois est l'ensemble des $(a_1, \ldots, a_r)$ tels que $a_i^q = a_i$ pour tout i. Comme f_i est irréductible, $F[x]/(f_i)$ est un corps fini de cardinal $q^{\deg(f_i)}$ et l'ensemble des $a_i \in F[x]/(f_i)$ tels que $a_i^q = a_i$ est le sous-corps à q éléments, c'est-à-dire F. Autrement dit, l'image de B est l'algèbre $F \times \cdots \times F$; elle est de dimension r sur F.

Remarque 2.33. *Il convient de noter qu'en pratique il faut calculer x^q dans $F[x]/(f)$ à l'aide de l'algorithme d'exponentiation rapide puis calculer ses puissances. Ce n'est qu'ensuite qu'on peut passer au calcul des g_e.*

Montrons maintenant comment, étant donné un polynôme sans racines multiples f, à coefficients dans un corps fini F, le factoriser (algorithme de Cantor-Zassenhaus). On suppose que tous ses facteurs irréductibles sont de même degré, ce qui est loisible compte tenu des résultats du paragraphe précédent.

Notons $f = f_1 \ldots f_r$ la factorisation de f et e le degré des f_i, de sorte que $n = \deg(f) = er$. L'algèbre$A = F[x]/(f)$ est isomorphe à $(F_{q^e})^r$.

Lemme 2.34. *Soit K un corps fini de cardinal q. Supposons q impair. L'application $u \longmapsto u^{(q-1)/2}$ de K dans lui-même prend une fois la valeur 0 (pour $u = 0$), $(q-1)/2$ fois la valeur 1 (lorsque u est un carré non nul) et $(q-1)/2$ fois la valeur -1 sinon.*

Lorsque $q = 2^m$, l'application $u \longmapsto u + u^2 + \cdots + u^{2^{m-1}}$ de K dans lui-même prend 2^{m-1} fois la valeur 0 et 2^{m-1} fois la valeur 1.

Démonstration : notons φ cette application. Dans le cas où q est impair, on a $\varphi(u)^2 = 1$ si $u \neq 0$ et $\varphi(u) = 0$ si $u = 0$; par suite, $\varphi(u)$ vaut ± 1 ou 0. Comme φ est une application polynomiale de degré $(q-1)/2$, elle prend au plus $(q-1)/2$ fois les valeurs -1 et 1, donc exactement $(q-1)/2$ fois chacune d'elles (en fait, $\varphi(u)$ est une généralisation du symbole de Legendre qui vaut 1 si u est un carré non nul, 0 si $u = 0$ et -1 si u n'est pas un carré).

Lorsque q est une puissance de 2, on a

$$\varphi(u)^2 = u^2 + u^{2^2} + \cdots + u^{2^m} = \varphi(u) + u^{2^m} - u = \varphi(u) \ .$$

Par conséquent, $\varphi(u)(\varphi(u) - 1) = 0$ et $\varphi(u)$ vaut 0 ou 1. En outre, φ prend au plus 2^{m-1} fois chaque valeur, donc exactement 2^{m-1} fois la valeur 0 et 2^{m-1} fois la valeur 1.

Proposition 2.35. *Soit F un corps fini de cardinal q, soit $f \in F[x]$ un polynôme sans facteurs carrés dont tous les facteurs irréductibles sont de degré e.*

(i) Si q est impair et si g est un polynôme non nul de degré $< n$, notons h le reste de la division par f du polynôme $g^{(q^e-1)/2}$. Alors, f est le produit de $\mathrm{PGCD}(f, h)$, *de* $\mathrm{PGCD}(f, h-1)$ *et de* $\mathrm{PGCD}(f, h+1)$. *En outre, parmi les $q^n - 1$ polynômes possibles g, $2((q^e-1)/2)^r$ fournissent une factorisation triviale.*

(ii) Supposons que $q = 2^m$ est une puissance de 2. Soit g un polynôme de degré $< n$ et soit h le reste de la division par f du polynôme $g + g^2 + \cdots + g^{2^{em-1}}$. Alors, f est le produit de $\mathrm{PGCD}(f, h)$ *et de* $\mathrm{PGCD}(f, h-1)$. *En outre, parmi les q^n polynômes g possibles, seuls $2(2^{em-1})^r$ fournissent une factorisation triviale.*

Démonstration : notons A l'algèbre $F[x]/(f)$; comme f est produit de r polynômes irréductibles de degré e deux à deux distincts, le théorème chinois entraîne que A est isomorphe à K^r , où K est un corps à q^e éléments. étant donné un polynôme g de degré $< n$, identifié à un élément de A, donc à une famille $(u_1, \ldots, u_r)$ d'éléments de K, le calcul de l'énoncé revient à celui de $(\varphi(u_1), \ldots, \varphi(u_r))$ dans K^r , où φ est l'application du lemme précédent. Par suite, $\varphi(u_i) \in \{0, 1, -1\}$ dans le cas où q est impair, et $\varphi(u_i) \in \{0, 1\}$ quand q est une puissance de 2.

Cela revient à dire que $h \equiv \varphi(u_i) \bmod f_i$, donc que h est multiple des polynômes f_i tels que $\varphi(u_i) = 0$, $h-1$ est multiple des polynômes f_i tels que $\varphi(u_i) = 1$, et $h+1$ est multiple des polynômes f_i tels que $\varphi(u_i) = -1$. Comme les f_i sont premiers entre eux deux à deux, $h, h-1$ et $h+1$ sont en fait multiples des produits correspondants (ce dernier polynôme n'intervient pas lorsque q est une puissance de 2).

La première partie de la proposition en découle immédiatement. Pour la seconde, il s'agit de dénombrer les familles $(u_1, \ldots, u_r)$ tels que

$$(\varphi(u_1), \ldots, \varphi(u_r))$$

soit $(0, \ldots, 0)$, $(1, \ldots, 1)$ ou $(-1, \ldots, -1)$. On trouve exactement les valeurs indiquées. Le cas particulier d'un polynôme scindé dans F est très important. C'est en effet à lui qu'on se ramène dans l'algorithme de Berlekamp exposé ci-dessous, c'est aussi ce qui se passe pour un polynôme de petit degré.

Remarque 2.36. *Lorsque q est impair, la probabilité d'obtenir une factorisation triviale est donc égale à*

$$2^{1-r}\frac{(q^e-1)^r}{q^{er}-1} \leq 2^{1-r} \quad .$$

Lorsque q est une puissance de 2, elle est encore $\leq 2^{1-r}$. Par conséquent, si $r \geq 2$, on peut espérer, en tirant des polynômes g au hasard, factoriser f très rapidement. Il est cependant possible de n'avoir trouvé aucun facteur non trivial au bout disons de 1000 essais, mais la probabilité est de l'ordre de $2^{1000(1-r)}$, donc extrêmement faible.

Proposition 2.37. *Soit F un corps fini de cardinal q et soit $f \in F[x]$ un polynôme de degré n sans facteurs carrés qui est scindé dans F.*

(i) Supposons q impair. Pour $a \in F$, posons $h_a = (x-a)^{(q-1)/2} \bmod f$. Alors, f est le produit de $\mathrm{PGCD}(h_a, f)$, $\mathrm{PGCD}(h_a - 1, f)$ *et* $\mathrm{PGCD}(h_a + 1, f)$. *En outre, au plus la moitié des valeurs de a fournit une factorisation triviale.*

(ii) Supposons que $q = 2^m$ est une puissance de 2. Pour $a \in F^\star$, posons $h_a = (ax) + (ax)^2 + \cdots + (ax)^{2^{m-1}}$. Alors, f est le produit de $\mathrm{PGCD}(h_a, f)$ et de $\mathrm{PGCD}(h_a + 1, f)$. En outre, au plus la moitié des valeurs de a fournit une factorisation triviale.

Démonstration : notons $x_1, \ldots, x_n$ les racines de f dans F. étudions d'abord le cas où q est impair. Dire que a fournit une factorisation triviale, signifie que $x_i - a$ est identiquement nul, carré ou non carré lorsque i parcourt $\{1, \ldots, n\}$. Autrement dit, les « mauvaises » valeurs de a sont celles pour lesquelles $x_i - a$ est non nul, et toujours carré ou toujours non carré. En particulier, l'élément $(x_2 - a)/(x_1 - a) \in F \cup \{\infty\}$ doit toujours être carré (∞ étant considéré comme un carré par convention). Comme l'application $a \longmapsto (x_2 - a)/(x_1 - a)$ est une homographie, c'est une application bijective de $F \cup \{\infty\}$ dans lui-même et au plus $(q-1)/2$ valeurs de a sont mauvaises, soit moins de la moitié.

Le cas où q est une puissance de 2 est analogue. Soit S l'ensemble des $2^m - 1$ solutions (dans F) de l'équation $\varphi(u) = u + u^2 + \cdots + u^{2^{m-1}}$; c'est un sous-groupe de F car φ est un morphisme de groupes. En outre, $h_a(x_i)$ vaut 0 si ax_i appartient à S et vaut 1 sinon. En particulier, si $a(x_2 - x_1) \notin S$, ax_1 et ax_2 n'appartiennent pas tous deux à S, $h_a(x_1) \neq h_a(x_2)$, et donc l'une des racines, x_1 et x_2, est racine de $\mathrm{PGCD}(h_a, f)$ tandis que l'autre est racine de $\mathrm{PGCD}(h_a + 1, f)$. Ainsi, la factorisation n'est triviale que dans au plus $(2^{m-1} - 1)$ cas, c'est-à-dire moins de la moitié.

Remarque 2.38. *Dans les deux cas, la probabilité, tirant a au hasard, d'obtenir une factorisation triviale est donc inférieure ou égale à 1/2.*

Nous pouvons maintenant revenir au problème de la factorisation d'un polynôme f de degré n, à coefficients dans un corps fini F de cardinal q, supposé sans racines multiples. Notons encore A l'algèbre $F[x]/(f)$ et B la sous-algèbre de Berlekamp, noyau de l'endomorphisme d'espaces vectoriel $a \longmapsto a^q - a$. Par la méthode de Gauss, on peut trouver une base $b_1, \ldots, b_r$ de B sur le corps de base F représentée par des polynômes de $F[x]$ de degrés $< n$.

Si on décompose f en produit de facteurs irréductibles $f = \prod_{i=1}^{r} f_i$, le lemme chinois identifie A au produit $K_1 \times \cdots \times K_r$ des corps finis $F[x]/(f_i)$ et identifie B à la sous-algèbre F^r.

Soit b un élément de B. Par définition, il existe pour tout $i \in \{1, \ldots, r\}$ un unique élément $\varphi_i(b) \in F$ tel que $b \equiv \varphi_i(b) \bmod f_i$. Alors, f_i est un facteur de $b - \varphi_i(b)$ si bien que la connaissance des $\varphi_i(b)$ permet de factoriser f. On a la formule :

$$f = \prod_{u \in F} \mathrm{PGCD}(f, b - u) \ .$$

Pour que l'on obtienne une factorisation non triviale, il faut et il suffit que les $\varphi_i(b)$ ne soient pas tous égaux, c'est-à-dire que b n'appartienne pas à la sous-algèbre diagonale (identifiée à F) de B.

Toutefois, la formule donnée est totalement inutilisable dans les applications pratiques où le cardinal q de F est très grand ; en effet elle suppose de calculer q PGCD, ce qui est prendra bien trop de temps.

Il convient donc de déterminer efficacement les $\varphi_i(b)$. On s'inspire pour cela de l'argument déjà utilisé dans l'algorithme de Cantor-Zassenhaus.

Supposons d'abord q impair. Comme $b^q - b$ est multiple de f, on a l'égalité

$$f = \mathrm{PGCD}(f, b^{(q-1)/2} - 1)\mathrm{PGCD}(f, b^{(q-1)/2} + 1)\mathrm{PGCD}(f, b) \ .$$

Il s'agit de voir à quelle probabilité cette factorisation est non triviale. Observons que pour tout i, la quantité $\varphi_i(b)^{(q-1)/2}$ vaut $0, 1$ ou -1. Il s'agit de trouver b de sorte que ces valeurs ne soient pas toutes égales. Si b est choisi au hasard dans $B \simeq F^r$, $(\varphi_i(b)^{(q-1)/2})_{1 \leq i \leq r}$ vaut $(1, \ldots, 1)$ si et seulement si tous les $\varphi_i(b)$ sont des carrés non nuls, $(-1, \ldots, -1)$ si et seulement aucun des $\varphi_i(b)$ n'est un carré, et enfin $(0, \ldots, 0)$ si et seulement si $\varphi_i(b) = 0$ pour tout i. Il y a donc $2\left((q-1)/2\right)^r + 1$ tels éléments b, qui aboutissent à une factorisation triviale de f, parmi lesquels tous les éléments de la sous-algèbre F. En dehors de ces choix, la factorisation n'est pas triviale, ce qui arrive avec une probabilité supérieure à $1 - 2^{1-r}$.

Pour traiter le cas où q est pair, on remplace le polynôme $X^{(q-1)/2}$ par le polynôme $T = X + X^2 + X^4 + \cdots + X^{2^{s-1}}$, où $q = 2^s$ qui vérifie $T(T-1) = T^2 - T = X^q - X$, d'où l'égalité

$$f = \mathrm{PGCD}(f, T(b))\mathrm{PGCD}(f, T(b) - 1) \ ,$$

si b est un élément arbitraire de B. Il s'agit encore de voir si cette factorisation peut être non triviale lorsque b est choisi au hasard. Lorsque b est choisit au hasard dans $B \simeq F^r$, $T(b)$ vaut $(0, \ldots, 0)$ ou $(1, \ldots, 1)$ si et seulement si tous les $\varphi_i(b)$ ont même image par T. Or, 0 et 1 ont tous deux 2^{s-1} antécédents ; il y a donc $2(2^{s-1})r$ éléments de B dont l'image est $(0, \ldots, 0)$ ou $(1, \ldots, 1)$. Ainsi, prenant b au hasard, la probabilité d'obtenir une factorisation non triviale est au moins égale à $1 - 2^{1-r}$ parmi lesquels les $q = 2^s$ éléments de F. Parmi les éléments $q^r - q$ éléments de $B \setminus F$, $2^{rs-r+1} - 2^s = q^r 2^{1-r} - q$ fournissent une factorisation triviale, et donc $q(1 - 2^{1-r})$ une factorisation non triviale. Là encore, la probabilité d'obtenir une factorisation non triviale est supérieure à $1 - 2^{1-r}$.

Pour résumer, la méthode est la suivante : compléter la famille (1) en une base de l'espace vectoriel des polynômes $Q \in F[X]$ de degrés $< n$ tels que $Q^q \equiv Q \bmod f$, espace identifié à B et dont on note r la dimension ; choisir un élément Q au hasard dans $B \setminus F$ puis calculer le PGCD de f et de $Q^{(q-1)/2} - 1$ (si q est impair) ou de $Q + Q^2 + \cdots + Q^{2^{s-1}}$ (si $q = 2^s$ est pair), d'où, avec probablité au moins $1 - 2^{1-r}$, un facteur non trivial de f.

3 Corps p-adiques

3.1 Limite projective

Définition 3.1. *On suppose donné un ensemble E_0 et, pour tout entier $n \geq 1$, une paire (E_n, φ_n) où E_n est un ensemble et φ_n une application $\varphi_n : E_n \longrightarrow E_{n-1}$. Une telle donnée est appelée système projectif.*

Définition 3.2. *Soit (E_n, φ_n) un système projectif. On dit qu'un ensemble E muni d'une suite d'applications $\psi_n : E \longrightarrow E_n$ est une* limite projective *de (E_n, φ_n) si d'une part les compatibilités $\psi_{n+1} \circ \varphi_{n+1} = \psi_n$ sont vérifiées et d'autre part si pour tout ensemble X et toutes applications $f_n : X \longrightarrow E_n$ telles que pour tout $n \in \mathbb{N}$, on ait $f_n = \varphi_{n+1} \circ f_{n+1}$, il existe une unique factorisation $f : X \longrightarrow E$ telle que :*

$$f_n = \psi_n \circ f \text{ pour tout } n \geq 0 \ .$$

Une limite projective est notée $\varprojlim E_n$.

Notation 3.3. *Soit E_n une suite d'ensemble, on note π_n la projection $\prod_{n\geq 0} E_n \longrightarrow E_n$ définie par $x = (x_1, \ldots, x_n, \ldots) \longmapsto \pi_n(x) = x_n$.*

Proposition 3.4. *Soit (E_n, φ_n) un système projectif. Il existe alors une limite projective $\varprojlim E_n \subset \prod_n E_n$, les applications ψ_n étant données par la restriction de la projection à $\varprojlim$: $\psi_n = \pi_n | \varprojlim E_n$.*

De plus, si (E'_n, ψ'_n) est une autre limite projective du même système, alors il existe une unique bijection $f' : E' \longrightarrow E)$ telle que $\psi'_n = \psi_n \circ f$.

Démonstration : commençons par l'existence. On pose

$$E = \{(x_n)_{n\geq 0}, \varphi_n(x_n) = x_{n-1}, \text{pour tout } n \geq 1\} \ .$$

Par définition de E, on a donc pour tout $x = (x_n) \in E$,

$$\varphi_{n+1} \circ \pi_{n+1}(x) = x_n = \pi_n(x) = \psi_n(x) \ .$$

On a donc $\varphi_n \circ \psi_n = \psi_{n-1}$.

Montrons que l'ensemble E ainsi construit muni des ψ_n possède la propriété universelle requise. Soit donc un ensemble X et des applications $f_n : X \longrightarrow E_n$ telles que $\varphi_n \circ f_n = f_{n-1}$. On peut ainsi définir

$$\begin{array}{rccc} \boldsymbol{f} : & X & \longrightarrow & \prod_{n\geq 0} E_n \\ & y & \longmapsto & \boldsymbol{f}(y) = (f_n(y)) \ . \end{array}$$

La relation $f_{n-1} = \varphi_n \circ f_n$ implique que l'image de $\boldsymbol{f}$ est incluse dans E. L'application $\boldsymbol{f}$ peut donc être vue comme allant de X vers $\varprojlim E_n$.

Par définition, pour tout $x \in X$,

$$\psi_n \circ \boldsymbol{f}(x) = \psi_n((f_n(x))_{n\geq 0}) = f_n(x) \ .$$

La propriété universelle est donc bien satisfaite, d'où l'existence de la limite projective.

Passons à l'unicité. Si $(E, (\psi_n))$ et $(E', (\psi'_n))$ sont deux limites projectives du même système projectif alors il y a aussi une unique application $f' : E \longrightarrow E'$ tel que $\psi_n = \psi'_n \circ f'$. Par substitution :

$$\psi'_n = \psi_n \circ f = \psi' n \circ f' \circ f$$

et donc $f' \circ f$ est donc une factorisation de l'identité, et puisque $(E', (\psi'_n))$ est une limite projective du système, nécessairement $f \circ f = \mathrm{Id}_{E'}$. De la même manière, $f \circ f' = \mathrm{Id}_E$. D'où l'unicité.

Corollaire 3.5. *Si pour un système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$, les applications φ_n sont surjectives et E_0 est non vide, alors les projections ψ_n de la limite projective $(\varprojlim E_n, \psi_n)$ le sont aussi. En particulier, E est non vide.*

Démonstration : par construction de $\varprojlim E_n$ comme sous-ensemble de $\prod_{n\geq 0} E_n$, il suffit de montrer que pour tout $x_n \in E_n$, il existe un élément de E avec x_n pour n-ième composante. Par surjectivité des φ_n, on choisit $x_{n+1} \in E_{n+1}$ tel que $\varphi_{n+1}(x_{n+1}) = x_n$ et l'axiome du choix dénombrable permet de conclure par récurrence.

Si le système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$ est formé d'espaces métriques et d'applications continues, alors la construction précédente assure que la limite projective $(\varprojlim E_n, \psi_n)$ est un espace topologique (pour la topologie induite par la topologie produit sur $\prod_{n\geq 0} E_n$) muni d'applications continues. On suppose par la suite que tous les espaces considérés sont métriques.

Proposition 3.6. *Une limite projective de compacts non vides est non vide.*

Démonstration : Soit (K_n, φ_n) un sytème projectif constitué d'ensembles compacts. Alors,

$$\prod_{n\geq 0} K_n$$

est compact par le théorème de Tychonoff, et la limite projective du système est un fermé par construction. En effet,

$$\varprojlim K_n = \bigcap_{n\geq 0} \{x \in \prod_{m\geq 0}, \pi_n(x) = \varphi_{n+1} \circ \pi_{n+1}(x)\} \ .$$

Donc $\varprojlim K_n$ est compact. Posons pour $n \geq 0$,

$$K_n^{[0]} = K_n, \quad \text{et par récurrence,} \quad K_n^{[k+1]} = \varphi_{n+k+1} \circ \varphi_{n+k} \circ \cdots \circ \varphi_{n+1}(K_{n+k+1}) \ .$$

Ces ensembles sont compacts et non vides par hypothèse sur les compacts K_n. Leurs intersection L_n est non vide dans K_n. De plus $\varphi_{n+1}(L_{n+1}) = L_n$, et les restrictions des φ_n aux L_n nous donnent un système projectif avec des applications surjectives. Par le corollaire précédent on peut en déduire que la limite projective de ce système est non vide. De plus, lim $\varprojlim L_n \subset \varprojlim K_n$ ce qui permet de conclure.

Exercice 3.7. *Une limite projective d'ensembles finis non vides est non vide.*

3.2 Les entiers p-adiques

Nous supposons que p est un nombre premier. Pour tout entier $n \geq 1$, on considère le quotient $\mathbb{Z}/p^n\mathbb{Z}$. Il s'agit d'un anneau (quotient d'anneau par un idéal, non nécessairement intègre). Par réduction modulo p^{n-1}, on obtient un morphisme d'anneaux évident :

$$\varphi_n \, : \, \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \ ,$$

On vérifie facilement que :
1 le morphisme φ_n est surjectif.
2 le noyau de φ_n est $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$ (isomorphe à $\mathbb{Z}/p\mathbb{Z}$).
On dispose alors d'une suite exacte longue :

$$\cdots \xrightarrow{\varphi_{n+1}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\varphi_n} \mathbb{Z}/p^{n-1}\mathbb{Z} \xrightarrow{\varphi_{n-1}} \cdots \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varphi_2} \mathbb{Z}/p\mathbb{Z} \ .$$

Il s'agit d'un système projectif d'anneaux.

Définition 3.8. *L'anneau $\mathbb{Z}_p$ est la limite projective du système $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$ défini ci-dessus.*

Plus concrètement, par définition, un élément de $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n))$ est une suite $x = (\ldots, x_n, \ldots, x_1)$ vérifiant $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ et $\varphi_n(x_n) = x_{n-1}$ pour tout $n \geq 2$.

Définition 3.9. *Si $x = (\ldots, x_n, \ldots, x_1)$ et $y = (\ldots, y_n, \ldots, y_1)$ sont des éléments de $\mathbb{Z}_p$ on définit l'addition*

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

et

$$x \cdot y = (\ldots, x_n y_n, \ldots, x_1 y_1)$$

(addition et multiplication terme à terme).

Lemme 3.10. *Avec ces lois, $\mathbb{Z}_p$ est un sous-anneau de l'anneau produit $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$.*

Définition 3.11. *On munit $\mathbb{Z}/p^n\mathbb{Z}$ de la topologie discrète et $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ de la toologie produit. La topologie sur $\mathbb{Z}_p$ est la topologie induite sur $\mathbb{Z}_p$ par que l'on vient de définir sur $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ qui contient $\mathbb{Z}_p$.*

Exercice 3.12. *Montrer que $\mathbb{Z}_p$ est compact (indication : fermé dans un produit d'espaces compacts).*

Constructions alternatives

On note[5] :

$$\begin{array}{rccc} |\cdot|_p \, : & \mathbb{Z} & \longrightarrow & \mathbb{R} \\ & n & \longmapsto & |n|_p = p^{-v_p(n)} \ . \end{array}$$

Exercice 3.13. *Verifier que $|\cdot|_p$ est une valeur absolue.*

5. On convient que $v_p(0) = \infty$.

L'ensemble $\mathbb{Z}$ munit de la métrique induite par $|\cdot|$ est ainsi un espace topologique. On définit alors $\mathbb{Z}_p$ comme le complété de $\mathbb{Z}$ pour cette métrique (c'est-à-dire le quotient de l'ensemble des suites de Cauchy par l'ensemble des suites convergeant vers 0).

On note $\mathbb{Z}_p$ l'ensemble des séries formelles à coefficients entiers $\sum_{i\geq 0} a_i p^i$, avec $0 \leq a_i < p$, et pour $x \in \mathbb{Z}_p$, on note $|x|_p = p^{-v_p(x)}$ où cette fois, $v_p(x) = \inf\{i, a_i \neq 0\}$.

Exercice 3.14. *Monter que l'on peut munir $\mathbb{Z}_p$ d'une structure d'anneau naturelle.*

Exercice 3.15. *Montrer que les trois constructions sont équivalentes, et produisent des espaces complets.*

Définition 3.16. *$\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$.*

Exercice 3.17. *Montrer que $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$.*

Soit ε_n la fonction

$$\begin{array}{rccc} \varepsilon_n : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & x = (\ldots, x_n, \ldots, x_1) & \longmapsto & x_n \ . \end{array}$$

Exercice 3.18. *La fonction ε_n est un morphisme d'anneaux pour tout $n \geq 1$.*

Proposition 3.19. *La suite*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

est une suite exacte de groupes abéliens. En particulier, il est possible d'identifier $\mathbb{Z}_p/p^n\mathbb{Z}_p$ à $\mathbb{Z}/p^n\mathbb{Z}$.

Démonstration : soit $(x) = (\ldots, x_n, \ldots, x_1)$ un élément de $\mathbb{Z}_p$ tel que $px = 0$. Par définition de la multiplication par p, on en déduit que $px_n = 0$ pour tout n, donc que pour tout $n \geq 1$, x_n est de la forme $p^{n-1}y_n$ avec $y_n \in \mathbb{Z}/p^n\mathbb{Z}$. Mais

$$x_n = \varphi_{n+1}(x_{n+1}) = p^n\varphi_{n+1}(y_{n+1}) = 0 \ .$$

Par suite, $x = 0$ et donc, la multiplication par p est injective sur $\mathbb{Z}_p$. Par récurrence, pour tout $m \geq 1$, la multiplication par p^m est injective.

Supposons maintenant que $x \in \ker(\varepsilon_n)$, c'est-à-dire que $x_n = 0$. En utilisant la construction de $\mathbb{Z}_p$ via les séries formelles, on peut donc écrire $x = \sum_{i\geq n} a_i p^i$. Posons $y = \sum_{i\geq 0} a_{n+i} p^i$. De manière évidente,

$$x = p^n y \ .$$

On en déduit que x est dans l'image de la multiplication par p^n.

Exercice 3.20. *Adapter cette preuve pour n'utiliser que la définition de $\mathbb{Z}_p$ comme limite projective.*

On en déduit que pout tout y_n dans $\mathbb{Z}/p^n\mathbb{Z}$, $x_n = p^n y_n$. En conlusion, $\ker(\varepsilon_n) \subset \mathrm{Im}([p^n])$. Inversement, si $x = p^n y$, la valuation de x est $\geq n$ et par suite $\varepsilon_n(x) = 0$. On a donc égalité.

Enfin, si $z \in \mathbb{Z}/p^n\mathbb{Z}$ et $\sum_{i=0}^{n-1} a_i p^i$ avec $0 \leq a_i < p$ est un système de représentants de z, définissons la série formelle $\sum_{j\geq 0} b_j p^j$ où

$$\left\{ \begin{array}{rcll} b_j & = & a_j & \text{si } j \leq n-1 \\ b_j & = & 0 & \text{sinon} \ . \end{array} \right.$$

Il est facile de vérifier que $\varepsilon_n(y) = x$. Donc, ε_n est bien surjective, ce qui termine la démonstration.

Proposition 3.21. *(i) Un élément x de $\mathbb{Z}_p$ est inversible si et seulement s'il n'est pas dans l'image de la multiplication par p (il en est de même pour un élément de $\mathbb{Z}/p^n\mathbb{Z}$).*

(ii) Soit $\mathbb{U}$ le groupe des éléments inversibles de $\mathbb{Z}_p$. Pour tout $x \in \mathbb{Z}_p$, $x \neq 0$, il existe un entier $n \geq 0$ et un élément $u \in \mathbb{U}$ tel que $x = p^n u$ (terminologie, les éléments de $\mathbb{U}$ sont appelés, des unités p-adiques). Il y a unicité de la paire (n, u).

Démonstration : soit $x \in \mathbb{Z}/p^n\mathbb{Z}$ n'appartenant pas à $p\mathbb{Z}/p^n\mathbb{Z}$, sa réduction $\bar{x}$ modulo p est un élément de $\mathbb{F}_p^*$ donc inversible. Soit $y \in \mathbb{Z}/p^n\mathbb{Z}$ dont la réduction modulo p notée aussi $\bar{y}$ est $\bar{x}^{-1}$. On en déduit la relation :

$$xy = 1 - pz$$

pour un certain $z \in \mathbb{Z}/p^n\mathbb{Z}$. Posons $Y = y\left(1 + pz + (pz)^2 + \cdots + (pz)^{n-1}\right)$. Un calcul direct montre alors

$$xY = (1 - pz)\left(1 + pz + (pz)^2 + \cdots + (pz)^{n-1}\right) = 1 \ .$$

Donc x est bien inversible.

Soit maintenant $x = (\ldots, x_n, \ldots, x_1) \in \mathbb{Z}_p$. Si $x \notin p\mathbb{Z}_p$, par la proposition précédente, $x_1 \neq 0$ et par suite pour tout n, on au aussi $x_n \notin p\mathbb{Z}/p^n\mathbb{Z}$ (car l'image de x_n par la réduction modulo p n'est pas nulle). Par suite, chacun des x_n est inversible et donc possède un inverse $y_n \in \mathbb{Z}/p^n\mathbb{Z}$. Posons $y = (\ldots, y_n, \ldots, y_1)$. La multiplication se faisant terme à terme, y est bien un inverse de x.

Exercice 3.22. *Montrer que y est bien dans $\mathbb{Z}_p$, c'est-à-dire que $\varphi_n(y_n) = y_{n-1}$.*

Inversement, il est facile de montrer que si $x \in p\mathbb{Z}/p^n\mathbb{Z}$ est un multiple de p (c'est-à-dire dans l'image de la multiplication par p), alors, il n'est pas inversible (c'est un diviseur de zéro, exercice). On en déduit le cas d'un élément de $\mathbb{Z}_p$. Cela montre la partie (i).

Soit maintenant $x \in \mathbb{Z}_p \setminus \{0\}$ et n le plus grand entier tel que $x \in p^n\mathbb{Z}_p$. Ecrivons $x = p^n y$. Par définition, $y \notin p\mathbb{Z}_p$ donc $y \in \mathbb{U}$. Cela montre l'existence. Si maintenant

$$x = p^n u = p^m v \ ,$$

avec $n, m \geq 0$ et $u, v \in \mathbb{U}$, il n'y a pas de restriction à supposer $n \leq m$ et $p^n(u - p^{m-n}v) = 0$. Commela multiplication par p est injective, $u - p^{m-n}v = 0$. Si $m > n$, $u - p^{m-n}v$ est inversible par la partie (i) (ce n'est pas un multiple de p) donc il ne peut être nul. Par suite, $n = m$. Mais alors $u = v$. S'où l'unicité.

Exercice 3.23. *Montrer que $v_p(x) = \infty$ si et seulement si x est nul. Montrer que $\mathbb{Z}_p$ est un anneau intègre. On utilisera la construction via les séries formelles. Pouvez-vous le faire avec les autres constructions ?*

Nous allons maintenant construire la topologie à partir de la construction algébrique (*confer* exercices précédents).

Notation 3.24. *Soit $x \in \mathbb{Z}_p \setminus \{0\}$, on écrit x sous la forme $p^n u$ avec $u \in \mathbb{U}$. On appelle l'entier n la* valuation *p-adique de x et on le note $v_p(x)$. On pose $v_p(0) = \infty$.*

Propriétés 3.25. *Si*[6] *$x, y \in \mathbb{Z}_p$,*

$$v_p(xy) = v_p(x) + v_p(y), \qquad et \qquad v_p(x+y) \geq \inf(v_p(x), v_p(y)) \ .$$

Exercice 3.26. *Avec la définition de $\mathbb{Z}_p$ via la limite projective et la valuation, montrer que $\mathbb{Z}_p$ est intègre.*

Définition 3.27. *On introduit l'application d définie par*

$$\begin{array}{rccl} d: & \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & \mathbb{R}^+ \\ & (x,y) & \longmapsto & d(x,y) = p^{-v_p(x-y)} \ . \end{array}$$

Exercice 3.28. *La fonction d est une distance sur $\mathbb{Z}_p$. Cette distance est ultramétrique (c'est-à-dire que l'inégalité triangulaire est remplacée par l'inégalité plus forte $d(x,y) \leq \max(d(x,z), d(y,z))$ pour tout triplet x, y, z.*

Lemme 3.29. *Soit (X, d) un espace ultramétrique. Alors,*
(i) Pour qu'une suite soit de Cauchy, il faut et il suffit que $\lim_{n\to\infty} d(x_{n+1}, x_n) = 0$.
(ii) Tout point d'une boule est un centre de cette dernière.
(iii) Toute boule ouverte est fermée. Toute boule fermée est ouverte.

Démonstration : si (x_n) est de Cauchy, il suit de la définition même que $\lim_{n\to\infty} d(x_{n+1}, x_n) = 0$. Inversement, soit $\varepsilon > 0$ et n_0 tel que pour tout $n \geq n_0$, $d(x_n, x_{x+1}) < \varepsilon$. Pour $p, q \in \mathbb{N}$, $p > q \geq n_0$, on a :

$$d(x_p, x_q) \leq \max\{d(x_p, x_{p-1}), \ldots, d(x_{q+1}, x_q)\} < \varepsilon \ .$$

Donc, la suite est de Cauchy.

Soient $x \in \mathbb{Z}_p, r \in \mathbb{R}, r > 0$, et y un point de la boule centrée en x et de rayon r, notée $B(x, r)$. Soit $z \in B(y, r)$. On a

$$d(x, z) \leq \max\{d(x, y)d(y, z)\} < r \ .$$

Donc $B(y, r) \subset B(x, r)$. L'inclusion inverse suit par symétrie.

Soit $x \in \mathbb{Z}_p$, $r > 0$ et soit $B_f(x, r)$ la boule fermée de $\mathbb{Z}_p$, de centre x et de rayon r. Soit $y \in B_f(x, r)$ et $z \in B(y, r/2)$. On a

$$d(x, z) \leq \max\{d(x, y); d(y, z)\} \leq r$$

6. On conviens que pour tout $n \in \mathbb{N}$, $n < \infty$.

donc $z \in B_f(x,r)$. On en déduit que $B(y,r/2) \subset B_f(x,r)$ et donc que pour tout point de cette dernière, $B_f(x,r)$ en est un voisinage. C'est donc un ouvert. Inversement, soit (x_n) une suite convergente (vers l) d'éléments de $B(x,r)$. On a

$$d(x,l) \leq \max\{d(x,x_n), d(x_n,l)\} < r \qquad \text{(pour } n \text{ assez grand)} \ .$$

Donc, $l \in B(x,r)$ et par suite $B(x,r)$ est un fermé.

Exercice 3.30. *Traiter le cas des boules de rayon nul dans le (iii) du lemme précédent.*

3.3 Groupes, anneaux topologiques

Définition 3.31. *Un groupe topologique G est un groupe muni d'une topologie qui rend l'application $(x, y) \in G \times G \longmapsto xy$ et l'application $x \in G \longmapsto x^{-1}$ continues.*

Remarque 3.32. *Dans un groupe topologique, les les translations et le passage à l'inverse sont des homéomorphismes. Un sous-groupe H d'un groupe topologique G est un groupe topologique pour la topologie induite par G sur H.*

Exemple 3.33. $(\mathbb{Z}_p, +)$, $(\mathbb{R}+)$ *et* $(\mathbb{Z}_p^*, \times)$ *sont des groupes topologiques.*

Proposition 3.34. *Si un groupe topologique admet un voisinage compact d'un de ses points, alors il est localement compact.*

Rappel 3.35. *Un espace est dit localement compact si chacun de ses points admet un voisinage compact.*

Démonstration : Les translations (homéomorphismes) envoient ce voisinage compact sur un voisinage compact de tout point du groupe topologique.

Lemme 3.36. *Soit G un groupe topologique. Soit H un sous-groupe de G. Alors,*
(i) L'adhérence $\bar{H}$ de H est un sous-groupe de G.
(ii) G est séparé si et seulement si l'élément neutre $\{e_G\}$ est fermé.

Démonstration : notons $\varphi : (x, y) \in G \times G \longmapsto xy^{-1}$. Comme H est un sous-groupe, $\varphi(H \times H) \subset H$. Mais, on a :

$$\varphi(\bar{H} \times \bar{H}) = \varphi(\overline{H \times H}) \subset \overline{\varphi(H \times H)} \subset \bar{H} \ .$$

Cela montre que $\bar{H}$ est un sous-groupe de G, d'où (i).

Rappelons que G est séparé si et seulement si la diagonale Δ_G est fermée dans $G \times G$ et que de plus, si G est séparé, tout singleton est fermé. De là :

G séparé entraîne $\{e_G\}$ fermé entraîne $\Delta_G = \varphi^{-1}(\{e_G\})$ fermé dans $G \times G$ entraîne G séparé .

Théorème 3.37. *Soit H un sous-groupe d'un groupe topologique G. Si H contient un voisinage du neutre e_G, alors, H est à la fois ouvert et fermé dans G.*

Démonstration : notons V un ouvert de e_G contenu dans H. Puisque $V \subset H$ et puisque les translations sont des homéomorphismes, pour tout $h \in H$, hV est un ouvert contenant h et toujours contenu dans H. Donc H est ouvert.

Pour $g \in G$, gH est un ouvert de H puisque la translation est un homéomorphisme. De plus $gH = H$ si et seulement si $g \in H$ et si $g \notin H, gH \cap H = \emptyset$. Donc

$$\left(\bigcup_{gH \neq H} gH \right)$$

est un ouvert (comme réunion d'ouverts) et son complémentaire est exactement H. Donc H est fermé.

Exemple 3.38. *Les sous-groupes $p^n\mathbb{Z}_p$ sont des sous-groupes de $\mathbb{Z}_p$ et et $1+p^n\mathbb{Z}_p$ sont des sous-groupes du groupe multiplicatif $1+p\mathbb{Z}_p$. En effet, $\mathcal{O}_n = \prod_{m\geq n+1}\mathbb{Z}/p^m\mathbb{Z}\times\{0\}^n \subset \prod_{m\geq 1}\mathbb{Z}/p^m\mathbb{Z}$ est un ouvert puisque la topologie est discrète sur chaque facteur donc $\mathcal{O}_n \cap \varprojlim(\mathbb{Z}/p^n\mathbb{Z},\varphi_n))$ est un ouvert de $\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z},\varphi_n))$ contenant l'origine et contenu dans $p^n\mathbb{Z}_p$, donc $p^n\mathbb{Z}_p$ contient un voisinage de l'origine et est dont ouvert et fermé dans $\mathbb{Z}_p$. Raisonner de même pour $1+p\mathbb{Z}_p$ (exercice).*

Proposition 3.39. *Un sous-groupe localement fermé d'un groupe topologique est fermé.*

Rappel 3.40. *Un sous-espace topologique Y de X est dit localement fermé dans X si tout point $y\in Y$ admet un voisinage V dans X tel que $V\cap Y$ est fermé de V.*

Démonstration : comme H est localement fermé dans G il ouvert dans $\bar{H}$ Détails pour cette affirmation

Lemme 3.41. *Soit X un espace topologique et $Y\subset X$ un sous-espace topologique.Les propriétés suivantes sont équivalentes :*

(i) Y est localement fermé dans X.

(ii) Il existe un ouvert U de X et un fermé F de X tels que $Y = U\cap F$.

(iii) Y est ouvert dans son adhérence $\overline{Y}$.

Démonstration : supposons (ii) vrai et soit $y\in Y$, comme U est ouvert et $Y\subset U$, U est un voisinage de y et $U\cap Y = U\cap(U\cap F) = U\cap F$ est bien un fermé de U par définition de la topologie induite sur U. Donc (i) est vrai. Supposons (i) vrai. Soit x un point de Y et V un voisinage de x tel que $Y\cap V$ est fermé dans V. Comme V est un voisinage, il existe un ouvert U tel que $x\in U\subset V$. Comme $Y\cap U = (Y\cap V)\cap U$ est un fermé de U, il n'y a pas de restriction à supposer que $V=U$, c'est-à-dire que V est ouvert.

On a

$$Y = (Y\cap V)\cup(Y\cap(X\setminus V))$$

donc

$$\overline{Y}\subset\overline{(Y\cap V)}\cup\overline{(Y\cap(X\setminus V))}$$

Toutefois, V est ouvert, donc

$$\overline{(Y\cap(X\setminus V))}\subset X\setminus V\ ,$$

par suite,

$$V\cap\overline{(Y\cap(X\setminus V))} = \emptyset$$

donc,

$$\overline{Y}\cap V\subset\overline{V\cap Y}\cap V\ .$$

Inversement, il est clair que

$$\overline{Y\cap V}\cap V\subset\overline{Y}\cap\overline{V}\cap V = \overline{Y}\cap V\ .$$

Donc,

$$\overline{Y\cap V}\cap V = \overline{Y}\cap V\ .$$

comme $Y \cap V$ est fermé dans V, on a maintenant

$$\overline{Y} \cap V = \overline{Y \cap V} \cap V = Y \cap V \subset Y \ .$$

Donc, si $x \in Y$, $\overline{Y} \cap V$ est un voisinage de $x \in \overline{Y}$ contenu dans Y, en d'autres termes, Y est ouvert dans $\overline{Y}$ et (iii) est vrai.

Supposons maintenant (iii) vrai. Comme Y est ouvert dans $F = \overline{Y}$, il existe un ouvert U de X tel que $\overline{Y} \cap U = Y$. En d'autres termes, Y est l'intersection d'un ouvert par un fermé et (ii) est vrai.

Or, $\bar{H}$ est un sous-groupe topologique de G, donc H est fermé dans $\bar{H}$, c'est-à-dire, $H = \bar{H}$, et H fermé dans G.

Corollaire 3.42. *Soit G un groupe topologique. Soit H un sous-groupe de G. Alors,*
(i) Si G est séparé et H localement compact, alors H est fermé.
(ii) Si G est séparé et H discret, alors H est fermé.
iii) G/H est séparé si et seulement si H est fermé.

Proposition 3.43. *Tout groupe topologique métrique localement compact est complet.*

Démonstration : le complété de G, est également groupe topologique métrique, G est localement compact, donc G est fermé dans son complété, il lui est donc égal.

Pour résumer :

$$\begin{array}{ccc} G/H \text{ fini et séparé} & \Longleftrightarrow & H \text{ fermé d'indice fini} \\ \Downarrow & & \Downarrow \\ G/H \text{ discret} & \Longleftrightarrow & H \text{ ouvert} \\ \Downarrow & & \Downarrow \\ G/H \text{ séparé} & \Longleftrightarrow & H \text{ fermé} \quad . \end{array}$$

3.4 Anneaux topologiques

Définition 3.44. *Un anneau topologique est un anneau $(A, +, .)$ muni d'une topologie qui rend les applications $(x, y) \longmapsto x + y$ et $(x, y) \longmapsto x.y$ continues sur $A \times A$.*

En particulier, un anneau topologique est un groupe topologique muni d'une multiplication continue sur $A \times A$.

Proposition 3.45. *La topologie sur $\mathbb{Z}_p$ peut-être définie par la distance d. Elle fait de $\mathbb{Z}_p$ un espace complet dans lequel $\mathbb{Z}$ est dense.*

Démonstration : les idéaux $p^n\mathbb{Z}_p$ forment une base de voisinage de l'origine $\{0\}$ (voir exemple 3.38). Comme $x \in p^n\mathbb{Z}_p$ est équivalent à $v_p(x) \geq n$, $p^n\mathbb{Z}_p = B\left(0, p^{-n}\right)$. Comme $\mathbb{Z}_p$ est compact, il est aussi complet (toute suite de Cauchy admettant une valeur d'adhérence est convergente).

Soit maintenant $x = (x_n)$ un élément de $\mathbb{Z}_p$. On choisit pour tout n un élément y_n de $\mathbb{Z}$ tel que $y_n \equiv x_n \bmod (p^n)$. La suite y_n converge vers x puisque $d(x, y_n) \leq p^{-n}$.

3.5 Sous-groupes fermés de $\mathbb{Z}_p$

Proposition 3.46. *Les sous-groupes fermés de $(\mathbb{Z}_p, +)$ sont $\{0\}$ et les $p^n\mathbb{Z}_p$, $n \in \mathbb{N}$. Ce sont des idéaux.*

Démonstration : un sous-groupe H de $\mathbb{Z}_p$ vérifie $\mathbb{Z}H = H$ donc pour $h \in H$, $h\mathbb{Z}_p \subset \overline{h\mathbb{Z}}$ car $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$ et H est fermé, puis $\overline{h\mathbb{Z}} \subset \overline{H} = H$. Donc tout sous-groupe fermé de $\mathbb{Z}_p$ est un idéal de $\mathbb{Z}_p$. Il est facile de vérifier que les $p^n\mathbb{Z}_p$ sont des idéaux de $\mathbb{Z}_p$. Inversement, soit I un idéal non nul de $\mathbb{Z}_p$ et $n = \min\{v_p(x), x \in I\}$. Soit de plus a un élément de I de valuation n. On peut donc écrire $a = p^n u$ avec u inversible. Donc, comme I est un idéal, $p^n \in I$. Maintenant, pour tout $x \in I$, on peut écrire $x = p^n y$ par définition de n. Donc $I \subset p^n\mathbb{Z}_p$. L'inclusion inverse est triviale puisque $p^n \in I$.

Corollaire 3.47. *Le quotient de $\mathbb{Z}_p$ par un sous-groupe fermé H non trivial est discret.*

3.6 Le corps $\mathbb{Q}_p$

Définition 3.48. *Le corps des nombres p-adiques, noté $\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$.*

Lemme 3.49. *On a $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.*

Démonstration : on écrit un élément x de $\mathbb{Q}_p$ sous la forme $x = a/b$, avec $a, b \in \mathbb{Z}_p$. On pose ensuite $v_p(b) = n$ et donc $b = p^n u$ avec u inversible dans $\mathbb{Z}_p$. Donc $a/u \in \mathbb{Z}_p$ et $x = p^{-n}(a/u)$.

Plus généralement, tout élément $x \in \mathbb{Q}_p^*$ peut s'écrire de manière unique sous la forme $x = p^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{U}$. On note $n = v_p(x)$, et l'on a la relation $v_p(x) \geq 0$ si et seulement si $x \in \mathbb{Z}_p$.

Proposition 3.50. *On introduit sur $\mathbb{Q}_p$ la fonction $d(x, y) = p^{-v_p(x-y)}$. Il s'agit d'une distance, et le corps $\mathbb{Q}_p$ muni de la topologie induite est complet, localement compact et contient $\mathbb{Z}_p$ comme sous-anneau ouvert. Le corps $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$.*

Exercice 3.51. *Démontrer la proposition 3.50.*

Exercice 3.52. *Construire $\mathbb{Q}_p$ comme le complété de $\mathbb{Q}$ pour la valeur absolue p-adique et vérifier que la construction est équivalente.*

Exercice 3.53. *démontrer qu'une série d'éléments de $\mathbb{Q}_p$ converge si et seulement si son terme général tends vers 0.*

3.7 Equations p-adiques

Notation 3.54. *Soient $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ un polynôme à coefficients dans $\mathbb{Z}_p$ et $n \geq 1$ un entier. On note f_n le polynôme à coefficients dans $\mathbb{Z}/p^n\mathbb{Z}$ déduit de f par réduction modulo p^n.*

Proposition 3.55. *Soient $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ des polynômes à coefficients dans $\mathbb{Z}_p$. Les affirmations suivantes sont équivalentes :*

(i) Les $f^{(i)}$ ont un zéro en commun dans $\mathbb{Z}_p^m$.

(ii) Pour tout $n \geq 1$, les polynômes $f_n^{(i)}$ ont un zéro commun dans $\mathbb{Z}/p^n\mathbb{Z}$.

Démonstration : on note D le lieu des zéros communs des $f^{(i)}$ et de la même manière D_n celuis des zéros communs des $f_n^{(i)}$. On vérifie que les D_n sont finis et par constructions, $D = \varprojlim D_n$. Par la proposition 3.6, D est non vide si et seulement si les D_n sont non vides.

Définition 3.56. *Un point $x = (x_1, \ldots, x_m)$ de $\mathbb{Z}_p)^m$ est dit primitif si l'une de ses coordonnées x_i est inversible dans $\mathbb{Z}_p$, c'est-à-dire si toutes ses coordonnées ne sont pas divisibles par p. De la même manière, on définit les éléments primitifs de $(\mathbb{Z}/p^n\mathbb{Z})^m$ en demandant que toutes les coordonnées ne soinet pas dans l'image de la multiplication par p.*

Proposition 3.57. *Soient $f^{(i)}$ des polynômes homogènes de $\mathbb{Z}_p[X_1, \ldots, X_m]$. Les propriétés suivantes sont équivalentes :*

(i) Les $f^{(i)}$ ont un zéro non trivial en commun dans $(\mathbb{Q}_p)^m$.

(ii) Les $f^{(i)}$ ont un zéro primitif en commun.

(iii) Les $f_n^{(i)}$ ont un zéro primitif en commun pour tout $n \geq 1$.

Démonstration : l'implication (ii) entraîne (i) est triviale. Inversement, si $x = (x_1, \ldots, x_m)$ est une solution, si $h = \inf(v_p(x_i))$, on pose, $y = p^{-h}x$. Comme les $f^{(i)}$ sont homogènes, y est également solutionet est par construction primitive. Enfin, le fait que (iii) et (ii) soient équivalent provient de la proposition précédente.

3.8 Des solutions approchées aux solutions globales

On va essayer de passer d'une solution approchée (c'est-à-dire modulo p^n) à une vraie solution, c'est-à-dire sur $\mathbb{Z}_p$. Cela se fait par une simple adaptation de la méthode de Newton.

Lemme 3.58. *Soit $f \in \mathbb{Z}_p[x]$, et f' la dérivée de f. Soient $x \in \mathbb{Z}_p$, et $n, k \in \mathbb{Z}$ des entiers tels que $0 \leq 2k < n$,*

$$f(x) \equiv 0 \bmod p^n, \qquad v_p(f'(x)) = k \ .$$

Alors, il existe $y \in \mathbb{Z}_p$ tel que

$$f(y) \equiv 0 \bmod p^{n+1}, \quad v_p(f')(y) = k \quad \text{et } y \equiv x \bmod p^{n-k} \ .$$

Démonstration : on écrit la formule de Taylor en écrivant $y = x + p^{n-k}z$

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-k} a$$

avec $a \in \mathbb{Z}_p$.

Par hypohtèse, $f(x) = p^n b$ et $f'(x) = p^k c$ avec $b \in \mathbb{Z}_p$ et $c \in \mathbb{U}$. On choisit maintenant z de la forme

$$b + zc \equiv 0 \bmod p$$

de telle sorte que la formule de Taylor s'écrive

$$f(y) = pn(b + zc) + p^{2n-2k} a = 0 \bmod pn + 1$$

puisque $2n - 2k > n$.

Pour conclure, la formule de Taylor appliquée à f' montrer que

$$f'(y) \equiv p^k c \bmod p^{n-k} \ .$$

On compare les valuations. Comme $n - k > k$, on en déduit que $v_p(f'(y)) = k$.

Théorème 3.59. *Soit $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_1, \ldots, x_m) \in \mathbb{Z}_p^m$, n et $k \in \mathbb{Z}$ et enfin j un entier tel que $0 \leq j \leq m$. On suppose que $0 < 2k < n$ et que*

$$f(x) \equiv 0 \bmod p^n \quad \text{et } v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k \ .$$

Alors, il existe un zéro z de $f \in \mathbb{Z}_p^m$ tel que $x \equiv z \bmod p^{n-k}$.

Démonstration : on suppose tout d'abord que $m = 1$. On applique le lemme précédent à $x^{(0)} = x$, et l'on obtient $x^{(1)} \in \mathbb{Z}_p$ qui est congru à $x^{(0)}$ modulo p^{n-k} et tel que

$$f(x^{(1)} = 0 \bmod p^{n+1} \quad \text{et } v_p(f'(x^{(1)})) = k \ .$$

On applique ensuite le lemme à $x^{(1)}$ après remplacement de n par $n + 1$ et, par récurrence, on construit une suite $x^{(0)}, x^{(1)}, \ldots, x^{(q)}, \ldots$ telle que

$$x^{(q+1)} \equiv x^{(q)} \bmod p^{n+q-k}, \quad \text{et } f(x^{(q)}) \equiv 0 \bmod p^{n+q} \ .$$

C'est une suite de Cauchy (la distance $d(x^{(q)}, x^{(q+1)}) \leq p^{-n-q+k}$). Elle a donc une limite ($\mathbb{Z}_p$ est complet) notée y et $f(y) = 0$ et $y \equiv x \bmod p^{n-k}$, d'où le théorème pour $m = 1$.

Le cas $m > 1$ se déduit en modifiant juste un x_j. Plus précisément, on choisit un indice $j \leq m$ et on note $\tilde{f}(X_j) \in \mathbb{Z}_p[X_j]$ obtenu en remplçant les variables X_i pour $i \neq j$ par x_i. On applique alors le cas $m = 1$ et on en déduit l'existence d'un y_j tel que

$$y_j \equiv x_j \bmod p^{n-k}$$

tel que $\tilde{f}(y_j) = 0$. Si l'on pose $y_i = x_i$ pour $i \neq j$, le point $y = (y_i)$ vérifier les conclusions du théorème.

Corollaire 3.60. *Tous les zéros simples de la réduction modulo p d'un polynôme f à coefficients dans $\mathbb{Z}_p$ se relèvent en un zéro de f dans $\mathbb{Z}_p$*

Démonstration : ceci est les cas particulier du théorème avec $n = 1$, $k = 0$.

Corollaire 3.61. *On suppose $p \neq 2$, et l'on pose $f(X_1, \ldots, X_m) = \sum_{i,j} a_{i,j} X_i X_j$, avec $a_{i,j} = a_{j,i}$ (en d'autres termes, f est une forme quadratique à coefficients dans $\mathbb{Z}_p$). On suppose que le discriminant de f, $\Delta(f) = \det(a_{i,j})$ est inversible. Soit enfin $a \in \mathbb{Z}_p$. Toute solution de l'équation*

$$f(x) \equiv a \bmod p$$

se relève en une solution de $f(x) = 0$ dans $\mathbb{Z}_p$.

Démonstration : a tenant compte du corollaire précédent, il suffit de vérifier que x n'est pas un point critique (zéro de toutes les dérivées partielles modulo p). Mais,

$$\frac{\partial f}{\partial X_i} = 2 \sum_j a_{i,j} X_j \ .$$

Comme le déterminant $\det(a_{i,j})$ n'est pas nul (modulo p), l'une au moins des dérivées partielles est non nulle modulo p.

Corollaire 3.62. *On suppose maintenant $p = 2$. Soit de même $f(X_1, \ldots, X_m) = \sum_{i,j} a_{i,j} X_i X_j$, avec $a_{i,j} = a_{j,i}$ une forme quadratique à coefficients dans $\mathbb{Z}_2$ et soit $a \in \mathbb{Z}_2$. Soit x une solution primitive de $f(x) \equiv a \bmod 8$. Alors, on peut relever x en une vraie solution sur $\mathbb{Z}_2$ sous réserve que x n'est pas une racine commune de toutes les dérivées partielles :*

$$\frac{\partial f}{\partial X_j}(x) \neq 0 \bmod 4, \qquad \textit{pour au moins une valeur de } j,\ 1 \leq j \leq m \ .$$

Cette condition de non nullité est satisfaite si $\det(a_{i,j}) \neq 0$.

Démonstration : on montre la première partie en appiquant le théorème avec $n = 3$ et $k = 1$. La deuxième partie se prouve comme le cas $p \geq 3$ en tenant compte du facteur non inversible 2.

4 Le groupe multiplicatif de $\mathbb{Q}_p$

4.1 Une filtration du groupe des unités

On rappelle que $\mathbb{U}$ désigne le groupe des unités p-adiques. Pour tout $n \geq 1$, on pose $\mathbb{U}_n = 1+p^n\mathbb{Z}_p$. On a

$$\mathbb{U}_n = \ker(\varepsilon_n) \ ,$$

où

$$\begin{array}{rccc} \varepsilon_n \ : & \mathbb{U} & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})^* \\ & x & \longmapsto & \varepsilon_n(x) = x \bmod p^n\mathbb{Z}_p \ . \end{array}$$

En particulier,

$$\mathbb{U}/\mathbb{U}_1 \simeq \mathbb{F}_p^* \ ,$$

et $\mathbb{U}/\mathbb{U}_1$ est cyclique d'ordre $p-1$. les goupes $\mathbb{U}_n$ vérifient de manière évidente $\mathbb{U}_{n+1} \subset \mathbb{U}_n$ et sont ouverts (paragraphe précédent).

Exercice 4.1. *Montrer que* $\mathbb{U} = \varprojlim \mathbb{U}/\mathbb{U}_n$.

L'application

$$\begin{array}{rccc} \pi_n \ : & \mathbb{U}_n & \longrightarrow & : \mathbb{F}_p \\ & x & \longmapsto \pi_n(1+p^n x) = x \bmod p \ , & \end{array}$$

définit un morphisme de groupes surjectifs de $\mathbb{U}_n$ vers $\mathbb{F}_p$. Son noyau est (exercice) $\mathbb{U}_{n+1}$. On dispose donc d'un isomorphisme de groupes additifs

$$\mathbb{U}_n/\mathbb{U}_{n+1} \simeq \mathbb{F}_p \ .$$

Indication : utiliser la formule

$$(1+p^n x)(1+p^n y) \equiv 1 + p^n(x+y) \bmod p^{n+1} \ .$$

Par récurrence, on en déduit que le cardinal de $\mathbb{U}_1/\mathbb{U}_n$ est p^{n-1}.

Lemme 4.2. *Soit* $0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0$ *une suite exacte de groupes abéliens (notés additivement). On suppose* $\mathrm{Card}(A) = a$, $\mathrm{Card}(B) = b$ *et* (a,b) *premiers entre eux. Soit* B' *l'ensemble des éléments de* E *tels que* $bx = 0$.

Alors, E *est la somme directe de* A *et de* B'. *de plus,* B' *est le seul sous-groupe de* E *de cardinal* b.

Démonstration : comme a, b sont premiers entre eux, il existe des entiers r, s tels que $ar + bs = 1$. En identifiant A à un sous groupe de E, si $x \in A \cap B'$, on a donc $ax = bx = 0$ donc, $0 = (ar+bs)x = x$ et par suite $A \cap B' = \{0\}$.

Soit $x \in E$, on peut écrire $x = arx + bsx$ et comme $bB' = \{0\}$, on en déduit $bE \subset A$. d'aute part, comme $abE = \{0\}$, on en déduit que $arx \in B'$. On en déduit que E est somme directe de A et de B' et que la projection $B' \to B$ est un isomorphisme. réciproquement, si B'' est un sous-groupe de E isomorphe à B, on a $bB'' = 0$ et donc $B'' \subset B'$ et $B'' = B'$ par égalité des cardinaux.

Proposition 4.3. *On a* $\mathbb{U} = \mathbb{V} \times \mathbb{U}_1$, *où* $\mathbb{V} = \{x \in \mathbb{U}, x^{p-1} = 1\}$ *est l'unique sous-groupe de* $\mathbb{U}$ *isomorphe à* $\mathbb{F}_p^*$.

Démonstration : on applique le lemme à la suite exacte

$$1 \longrightarrow \mathbb{U}_1/\mathbb{U}_n \longrightarrow \mathbb{U}/\mathbb{U}_n \longrightarrow \mathbb{F}_p^* \longrightarrow 1 \ .$$

En effet, l'ordre de $\mathbb{U}_1/\mathbb{U}_n$ est p^{n-1} et l'ordre de $\mathbb{F}_p^*$ est $p-1$ qui sont premiers entre eux. On en déduit que $\mathbb{U}/\mathbb{U}_n$ contient un unique sous-groupe $\mathbb{V}_n$ isomorphe à $\mathbb{F}_p^*$. De plus, la projection

$$\mathbb{U}/\mathbb{U}_n \longrightarrow \mathbb{U}/\mathbb{U}_{n-1}$$

restreinte à $\mathbb{V}_n$ est un isomorphisme sur $\mathbb{V}_{n-1}$.

Comme $\varprojlim \mathbb{U}_n$,on en déduit par passage à la limite un sous-groupe $\mathbb{V}$ de $\mathbb{U}$ isomorphe à $\mathbb{F}_p^*$. On a bien, toujours par passage à la limite $\mathbb{U} \simeq \mathbb{V} \times \mathbb{U}_1$. l'unicité se déduit de l'unicité de $\mathbb{V}_n$.

Corollaire 4.4. *Le corps $\mathbb{Q}_p$ contient toutes les racines $p-1$-ièmes de l'unité.*

Remarque 4.5.
- *On appelle souvent de groupe $\mathbb{V}$ le groupe des représentants de $\mathbb{F}_p^*$ dans $\mathbb{Q}_p$.*
- *On peut aussi prouer l'existence de $\mathbb{V}$ en appliquant le théorème de relèvement des équations diophantiennes à $x^{p-1}-1=0$ (Exercice).*

4.2 Structure du groupe $\mathbb{U}_1$

Lemme 4.6. *Soit $x \in \mathbb{U}_n \setminus \mathbb{U}_{n+1}$ avec $n \geq 1$ si $p \neq 2$ et $n \geq 2$ si $p = 2$. Alors*

$$x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2} \ .$$

Démonstration : par hypothèse, on a $x = 1 + kp^n$ avec $k \not\equiv 0 \bmod p$. La formule du binôme donne

$$x^p = 1 + kp^{n+1} + \cdots + k^p p^{np} \ .$$

Les exposants négligés sont tous $\geq 2n+1$ et par suite également $\geq n+2$. de plus, $np \geq n+2$ (car $n \geq 2$ si $p = 2$). Ceci montre que

$$x^p = 1 + kp^{n+1} \bmod p^{n+2}$$

et par suite $x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2}$ puisque k est non nul.

Proposition 4.7. *Si $p \neq 2$, $\mathbb{U}_1$ est isomorphe à $\mathbb{Z}_p$. Si par contre $p = 2$, $\mathbb{U}_1 \simeq \{\pm\} \times \mathbb{U}_2$ et $\mathbb{U}_2$ est isomorphe à $\mathbb{Z}_2$.*

Démonstration : on considère tout d'abord le cas $p \neq 2$. On choisit un élément $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, par exemple, on prend $\alpha = 1 + p$. Par le lemme précédent, $\alpha^{p^i} \in \mathbb{U}_{i+1} \setminus \mathbb{U}_{i+2}$. On note α_n l'image de α dans le quotient $\mathbb{U}_1/\mathbb{U}_n$. On a

$$\alpha_n^{p^{n-2}} \neq 1 \quad \text{et } \alpha_n^{p^{n-1}} = 1 \ .$$

Mais $\mathbb{U}_1/\mathbb{U}_n$ est cyclique d'ordre p^{n-1}. Donc, il est cyclique engendré par α_n. On note $\theta_{n,\alpha}$ le morphisme

$$\begin{array}{rccc} \theta_{n\alpha} : & \mathbb{Z}/p^{n-1}\mathbb{Z} & \longrightarrow & \mathbb{U}_1/\mathbb{U}_n \\ & z & \longmapsto & \theta_{n,\alpha}(z) = \alpha_n^z \ . \end{array}$$

le diagramme suivant est donc commutatif :

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \stackrel{\theta_{n+1,\alpha}}{\longrightarrow} & \mathbb{U}_1/\mathbb{U}_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^{n-1}\mathbb{Z} & \stackrel{\theta_{n,\alpha}}{\longrightarrow} & \mathbb{U}_1/\mathbb{U}_n \ . \end{array}$$

On en déduit que les $\theta_{n,\alpha}$ induisent un isomorphisme θ de $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ et $\mathbb{U}_1 = \varprojlim \mathbb{U}_1/\mathbb{U}_n$. D'où la proposition pour $p \geq 3$.

On suppose maintenant $p = 2$. On choisit un élément de $\mathbb{U}_2 \setminus \mathbb{U}_3$, c'est-à-dire $\alpha \equiv 5 \bmod 8$. On définit comme ci-dessus les isomorphismes

$$\theta_{n,\alpha} : \mathbb{Z}/p^{n-2}\mathbb{Z} \longrightarrow \mathbb{U}_2/\mathbb{U}_n \ ,$$

et on en déduit un isomorphisme $\theta_\alpha : \mathbb{Z}_2 \simeq \mathbb{U}_2$.

Par ailleur, le morphisme :

$$\mathbb{U}_1 \longrightarrow \mathbb{U}_1/\mathbb{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$$

induit un isomorphisme de $\{\pm\}$ sur $\mathbb{Z}/2\mathbb{Z}$ et l'on en tire

$$\mathbb{U}_1 \simeq \{\pm\} \times \mathbb{U}_2 \ .$$

Théorème 4.8. *Le groupe $\mathbb{Q}_p^*$ est isomorphe à $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ si $p \geq 3$ et à $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/2\mathbb{Z}$ si $p = 2$*

Démonstration : tout élément de $\mathbb{Q}_p^*$ s'écrit de manière unique $x = p^n u$ avec $u \in \mathbb{U}$ et $n \in \mathbb{Z}$. On en déduit que $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}$. Mais, la proposition précédente assure que $\mathbb{U} \simeq \mathbb{V} \times \mathbb{U}_1$ où $\mathbb{V}$ est cyclique d'ordre $p-1$ et la structure de $\mathbb{U}_1$ est donnée par le résultat qui précède.

4.3 Carrés de $\mathbb{Q}_p$

Théorème 4.9. *On suppose $p \neq 2$ et soit $x = p^n u$ un élement de $\mathbb{Q}_p^*$ ($n \in \mathbb{Z}, u \in \mathbb{U}$). Pour que x soit un carré dans $\mathbb{Q}_p$, il faut et il suffit que n soit pair et que l'image $\bar{u}$ de u dans $\mathbb{U}/\mathbb{U}_1 \simeq \mathbb{F}_p^*$ soit un carré. La deuxième condition signifie simplement que le symbole de Legendre $\left(\frac{\bar{u}}{p}\right) = 1$, on le notera plus simplement $\left(\frac{u}{p}\right)$.*

Démonstration : on décompose u sous la forme $u = v \cdot u_1$ avec $v \in \mathbb{V}$ et $u_1 \in \mathbb{U}_1$ en utilisant l'isomorphisme ci-dessus. La décomposition $\mathbb{Q}_p^* \simeq \mathbb{Z} \times V \times \mathbb{U}_1$ du théorème précédent entraîne que u est un carré si et seulement s'il est contenu dans l'image par la multiplication par 2 dans $\mathbb{Z} \times V \times \mathbb{U}_1$, c'est-à-dire si et seulement si n est pair et v, u_1 sont des carrés. Toutefois, $\mathbb{U}_1 \simeq \mathbb{Z}_p$. Comme 2 est inversible dans $\mathbb{Z}_p$ (car $p \neq 2$), le groupe $\mathbb{Z}_p$ est 2-divisible (tous les éléments sont des carrés). La condition se réduit donc v carré. Mais $\mathbb{V}$ est isomoprhe à $\mathbb{F}_p^*$, d'où le résultat.

Corollaire 4.10. *Si $p \neq 2$, le groupe $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ est de type $(2,2)$. Un système de représentants est donné par $\{1,p\} \times \{1,u\} = \{1,p,u,up\}$, où $u \in \mathbb{F}_p^*$ est tel que $\left(\frac{u}{p}\right) = -1$.*

Démonstration : laissée en exercice.

Théorème 4.11. *Supposons maintenant $p = 2$. Un élément $x = p^n u \in \mathbb{Q}_p^*$ est un carré si et seulement si n est pair et $u \equiv 1 \bmod 8$.*

Démonstration : la décomposition $\mathbb{U} \simeq \{\pm\} \times \mathbb{U}_2$ montre que u est un carré si et seulement si $u \in \mathbb{U}_2$ et u est un carré dans $\mathbb{U}_2$. Mais l'isomorphisme $\theta : \mathbb{Z}_2 \longrightarrow \mathbb{U}_2$ construit ci-dessus envoie $2^n\mathbb{Z}_2$ surjectivement sur $\mathbb{U}_{n+2}$. Prenant $n = 1$, on voit que l'ensemble des carrés de $\mathbb{U}_2$ est égal à $\mathbb{U}_3$. En d'autres termes, un élément u de $\mathbb{U}$ est un carré si et seulement s'il est $\equiv 1 \bmod 8$, d'où le résultat (en raisonnant comme pour le cas impair pour assurer la parité de n).

Remarque 4.12. *Le fait qu'un élément de $\mathbb{U}_3$ est un carré résulte aussi du résultat sur le relèvement des solutions d'équations diophantiennes appliqué à la forme quadratique $f(x) = x^2$.*

Corollaire 4.13. *Le groupe $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ est de type $(2, 2, 2)$. Il admet pour système de représentants $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Démonstration : cela suit du fait que $\{\pm 1, \pm 5\}$ est un système de représentants de $\mathbb{U}/\mathbb{U}_3$.

Remarque 4.14. *(i) Pour $p = 2$, on définit les homomorphismes ϵ, ω :*

$$\begin{array}{rccl} \epsilon : & \mathbb{U}/\mathbb{U}_3 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & z & \longmapsto & \epsilon(z) = \frac{z-1}{2} \bmod 2 \quad = \quad \left\{ \begin{array}{llll} 0 & si & z \equiv 1 \bmod 4 \\ 1 & si & z \equiv -1 \bmod 4 \end{array} \right. \\ \omega : & \mathbb{U}/\mathbb{U}_3 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & z & \longmapsto & \omega(z) = \frac{z^2-1}{8} \bmod 2 \quad = \quad \left\{ \begin{array}{llll} 0 & si & z \equiv \pm 1 \bmod 8 \\ 1 & si & z \equiv \pm 5 \bmod 8 \end{array} \right. \end{array}$$

Le morphisme ϵ définit un isomorphisme de $\mathbb{U}/\mathbb{U}_2$ vers $\mathbb{Z}/2\mathbb{Z}$ et le morphisme ω un isomorphisme de $\mathbb{U}_2/\mathbb{U}_3$ vers $\mathbb{Z}/2\mathbb{Z}$. La paire (ϵ, ω) définit par suite un isomorphisme de $\mathbb{U}/\mathbb{U}_3$ vers $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. En particulier, une unité 2-adique z est un carré si et seulement si $\epsilon(z) = \omega(z) = 0$.

(ii) Les théorèmes précédents montrent que $(\mathbb{Q}_p^*)^2$ est un sous-groupe ouvert de $\mathbb{Q}_p^*$.

Exercice 4.15. *Démontrer les assertions de la remarque ci-dessus.*

5 Théorie analytique

Rappelons que l'on note $\mathcal{P}$ l'ensemble des nombres premiers et $\pi(x)$ le cardinal de $\mathcal{P} \cap [1, x]$. L'objectif de ce paragraphe est la preuve du théorème des nombres premiers. Nous aurons besoin de faire appel à l'analyse complexe (il existe des démonstrations qui l'évitent).

Théorème 5.1. *On a l'équivalent, lorsque x tend vers $+\infty$,*

$$\pi(x) \sim x/\log x \ .$$

5.1 La fonction Zêta de Riemann

Définissons, pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 1$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \ .$$

La fonction ainsi définie est appelée fonction zêta de Riemann.

Par comparaison à l'intégrale $\int_1^\infty dt/t^a$, pour $a > 1$, on voit que cette série converge normalement dans le demi-plan fermé d'équation

$$\mathfrak{Re}(s) \geq a \ .$$

Comme chaque terme de la série est une fonction holomorphe dans le demi-plan ouvert $\mathfrak{Re}(s) > a$, la fonction zêta de Riemann est une fonction holomorphe sur ce demi-plan, donc sur leur réunion qui est le demi-plan ouvert d'équation $\mathfrak{Re}(s) > 1$. Son comportement au bord de ce demi-plan va s'avérer crucial. Pour $a \in \mathbb{R}$, on notera Ω_a le demi-plan ouvert d'équation $\mathfrak{Re}(s) > a$.

Le lien avec les nombres premiers provient de la formule :

Proposition 5.2. *Pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 1$, on a*

$$\zeta(s) = \frac{1}{(1-2^{-s})} \times \frac{1}{(1-3^{-s})} \times \cdots = \prod_{p \in \mathcal{P}} \frac{1}{(1-p^{-s})} \ .$$

Le produit infini converge absolument sur Ω_1 et uniformément dans chaque demi-plan Ω_a avec $a > 1$.

Démonstration : pour $\mathfrak{Re}(s) > 1$, $|p^{-s}| < 1$ et l'on a la somme géométrique :

$$\frac{1}{1-p^{-s}} = \sum_{m=0}^{\infty} p^{-ms} \ .$$

On déduit donc de la convergence absolue (respectivement uniforme) de la série de Riemann, la convergence absolue (respectivement uniforme) du produit infini en remarquant :

$$\left| \frac{1}{1-p^{-s}} - 1 \right| \leq \frac{2}{|p^s|} \ ,$$

et en passant au logarithme.

Soit T un nombre entier. On peut alors développer le produit des facteurs $\frac{1}{(1-p^{-s})}$ pour en déduire (en limitant le produit aux premiers plus petit que T) :

$$\prod_{p\in\mathcal{P},p\leq T}\frac{1}{1-p^{-s}}=\prod_{i\leq t}\sum_{m_i=0}^{\infty}p_i^{-m_i s}=\sum_{m_1=0}^{\infty}\cdots\sum_{m_t=0}^{\infty}(p_1^{m_1}\dots p_t^{m_t})^{-s}\ ,$$

où $t=\pi(T)$.

C'est une sous-série de la série qui définit la fonction zêta de Riemann : seuls sont présents les termes n^{-s} où n est un entier dont tous les facteurs premiers sont inférieurs à T, et ces termes apparaissent une fois et une seule d'après le théorème de décomposition en facteurs premiers.

En particulier, cette série multiple converge absolument si $\mathfrak{Re}(s)>1$, ce qui justifie le développement fait. En outre,

$$\left|\zeta(s)-\prod_{p\leq T}\frac{1}{1-p^{-s}}\right|\leq\sum_{P(n)>T}\left|n^{-s}\right|\ ;$$

ce dernier terme tend vers 0 quand T tend vers l'infini en vertu de la convergence de la série de Riemann. Par suite, le produit infini écrit vaut $\zeta(s)$.

Proposition 5.3. *La fonction ζ s'étend en une fonction méromorphe sur $\mathbb{C}$. Ce prolongement a un unique pôle en $s=1$, simple et de résidu égal à 1.*

Démonstration : on se contente de montrer l'existence d'un prolongement à l'ouvert Ω_0. Pour cela, observons que pour $\mathfrak{Re}(s)>1$,

$$\zeta(s)-\frac{1}{s-1}=\sum_{n=1}^{\infty}n^{-s}-\int_1^{\infty}x^{-s}dx=\sum_{n=1}^{\infty}\int_n^{n+1}\left(\frac{1}{n^s}-\frac{1}{x^s}\right)dx\ .$$

Notons $f_n(s)$ l'intégrale figurant au n-ième terme de cette série. Par intégration par parties, on a :

$$\begin{aligned}f_n(s)&=\int_n^{n+1}\left(\frac{1}{n^s}-\frac{1}{x^s}\right)dx\\&=-\left[\left(\frac{1}{n^s}-\frac{1}{x^s}\right)(n+1-x)\right]_n^{n+1}+s\int_n^{n+1}(n+1-x)x^{-s-1}dx\\&=s\int_n^{n+1}(n+1-x)x^{-s-1}dx\ ,\end{aligned}$$

si bien que

$$|f_n(s)|\leq\frac{|s|}{n^{\mathfrak{Re}(s)+1}}\ .$$

La fonction f_n est holomorphe sur Ω_0 et la majoration précédente entraîne que la série $\sum_n f_n(s)$ converge pour tout $s\in\Omega_0$, uniformément dans tout ouvert Ω_a avec $a>0$. La somme de cette série définit donc une fonction holomorphe f sur le demi-plan Ω_0. Pour $\mathfrak{Re}(s)>1$, on a

$$\zeta(s)=\frac{1}{s-1}+f(s)\ ;$$

cette dernière expression fournit le prolongement voulu. De même que la précision souhaitée sur le pôle (nature, valeur du résidu).

Dans la suite, on notera encore ζ le prolongement méromorphe de la fonction zêta de Riemann. Nous laissons en exercice le soin de démontrer l'existence d'un prolongement pour $\mathfrak{Re}(s) \leq 0$.

Le point crucial de la démonstration du théorème des nombres premiers, même s'il est difficile de le concevoir au premier abord, est la propriété suivante : la fonction ζ ne s'annule pas sur la droite $\mathfrak{Re}(s) = 1$:

Proposition 5.4. *Pour tout nombre complexe $s \neq 1$ tel que $\mathfrak{Re}(s) \geq 1$, on a $\zeta(s) \neq 0$.*

Démonstration : lorsque $\mathfrak{Re}(s) > 1$, cela résulte de l'expression de $\zeta(s)$ comme produit infini, aucun facteur n'étant nul. Toujours pour $\mathfrak{Re}(s) > 1$, la dérivée logarithmique du produit infini $\prod_{p\in\mathcal{P}}(1-p^{-s})^{-1}$ s'écrit

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{p\in\mathcal{P}} \frac{\log(p)}{p^s-1} = -\sum_{p\in\mathcal{P}} \frac{\log(p)}{p^s} - \sum_{p\in\mathcal{P}} \frac{\log(p)}{p^s(p^s-1)} \ .$$

Comme $\log p$ croit plus lentement que toute puissance de p, les deux séries du second membre convergent pour $\mathfrak{Re}(s) > 1$ et $\mathfrak{Re}(s) > 1/2$ (et même uniformément sur tout demi-plan strictement inclus dans ces derniers), par comparaison avec la série de Riemann et définissent des fonctions holomorphes dans les ouverts Ω_1 et $\Omega_{1/2}$ respectivement. On notera ces séries $\Phi(s)$ et $\Psi(s)$

L'expression $\Phi(s) = -\frac{\zeta'(s)}{\zeta(s)} - \Psi(s)$ montre que $\Phi(s)$ possède également un prolongement méromorphe dans le demi-plan $\Omega_{1/2}$. Ses pôles proviennent du pôle simple de ζ en $s = 1$, avec résidu 1, et, pour chaque $m \geq 1$, des zéros d'ordre m de ζ dans le demi-plan $\Omega_{1/2}$, avec résidu $-m$.

Autrement dit,

$$\lim_{s\longrightarrow 1}(s-1)\Phi(s) = 1 \ , \qquad \lim_{\sigma\longrightarrow 1}(\sigma-1)\Phi(\sigma+i\tau) = -m \ ,$$

si ζ possède un zéro d'ordre m en $1+i\tau$. Supposons donc que ζ ait un zéro d'ordre m en $s = 1+i\tau$ et un zéro d'ordre n en $1+2i\tau$. Comme $\zeta(\overline{s}) = \overline{\zeta(s)}$, ζ a aussi un zéro d'ordre m en $s = 1-i\tau$ et un zéro d'ordre n en $1-2i\tau$.

On procède maintenant au calcul suivant, pour tout réel $\sigma > 0$,

$$\begin{aligned}
\sum_{k=-2}^{2} \left(\begin{array}{c} 4 \\ k+2 \end{array} \right) \Phi(\sigma+i\tau k) &= \sum_{p\in\mathcal{P}} \frac{\log(p)}{p^\sigma}\big(p^{-2i\tau} + 4p^{-i\tau} + 6 + 4p^{i\tau} + p^{2i\tau}\big) \\
&= \sum_{p\in\mathcal{P}} \frac{\log(p)}{p^\sigma}\left(p^{-i\tau} + p^{i\tau}\right)^4 \\
&= \sum_{p\in\mathcal{P}} \frac{\log(p)}{p^\sigma}\left(2\cos(\tau\log(p)\right)^4 \geq 0 \ .
\end{aligned}$$

Lorsque l'on multiplie cette expression par $\sigma - 1$, pour un nombre réel $\sigma > 1$, et que l'on fait tendre σ vers 1, on obtient

$$-n - 4m + 6 - 4m - n \geq 0 \ ,$$

c'est-à-dire $8m + 2n \leq 6$. Nécessairement, $m = 0$: la fonction ζ ne s'annule pas en $1 + i\tau$.

Pour tout nombre réel $x > 0$, on pose

$$\theta(x) = \sum_{p \leq x} \log(p) \ .$$

Nous allons voir que la connaissance du comportement de $\theta(x)$ équivaut à celle du comportement de la fonction $\pi(x)$, mais elle est plus facile à étudier.

Lemme 5.5. *Si* $\theta(x) \sim_{x \longrightarrow \infty} x$, *alors*

$$\pi(x) \sim_{x \longrightarrow \infty} \frac{x}{\log(x)} \ .$$

Démonstration : supposons donc $\theta(x) \sim x$ (on sous entendra par la suite que l'équivalent est pris pour $x \longrightarrow \infty$). On a donc

$$\theta(x) = \sum_{p \leq x} \log(p) \leq \sum_{p \leq x} \log(x) \leq \pi(x) \log(x) \ .$$

En particulier,

$$\liminf_{x \longrightarrow \infty} \frac{\pi(x) \log(x)}{x} \geq \lim_{x \longrightarrow \infty} \frac{\theta(x)}{x} = 1 \ .$$

Dans l'autre sens, si ε est un nombre réel tel que $0 < \varepsilon < 1$,

$$\begin{aligned}
\theta(x) &\geq \sum_{x^{1-\varepsilon} \leq p \leq x} \log(p) \\
&\geq \sum_{x^{1-\varepsilon} \leq p \leq x} (1-\varepsilon) \log(x) \\
&\geq (1-\varepsilon) \log(x) \left(\pi(x) - \pi\left(x^{1-\varepsilon}\right) \right) \\
&\geq (1-\varepsilon) \pi(x) \log(x) + O\left(x^{1-\varepsilon/2}\right) \ ,
\end{aligned}$$

puisque $\pi(x) = O(x)$ par[7] définition même de $\pi(x)$. Il en résulte que :

$$1 = \lim_{x \longrightarrow \infty} \frac{\theta(x)}{x} \geq (1-\varepsilon) \limsup_{x \longrightarrow \infty} \frac{\pi(x) \log(x)}{x} \ ,$$

c'est-a-dire, en faisant tendre ε vers 0,

$$1 = \lim_{x \longrightarrow \infty} \frac{\theta(x)}{x} \geq \limsup_{x \longrightarrow \infty} \frac{\pi(x) \log(x)}{x} \ ,$$

et le lemme suit.

7. Si f est une fonction à valeur réelles positive, on dit qu'un fonction g à valeur réelle est $O(f)$ s'il existe un nombre réel $c > 0$ tel que $|g| \leq cf$ lorsque x tends vers la limite prescrite, souvent implicite et déduite du contexte ; comme c'est le cas ici où $x \longrightarrow \infty$.

Il suffit donc de démontrer l'équivalent $\theta(x) \sim x$, ce qui va passer par une forme apparemment plus faible :

Lemme 5.6. *Si l'intégrale*

$$\int_1^\infty \frac{\theta(x)-x}{x^2}dx \tag{5.1}$$

converge, alors $\theta(x) \sim x$ au voisinage de $+\infty$.

Démonstration : soit $\lambda > 1$ un nombre réel ; si x est un nombre réel tel que $\theta(x) > \lambda x$, alors :

$$\int_x^{\lambda x} \frac{\theta(t)-t}{t^2}dt \geq \int_x^{\lambda x} \frac{\theta(x)-t}{t^2}dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}dt = \int_1^\lambda \frac{\lambda - u}{u^2}du > 0 \ .$$

La première inégalité provient de ce que θ est croissante.

L'existence de tels nombres réels arbitrairement grands contredit donc le critère de Cauchy pour la convergence de l'intégrale de $(\theta(x)-x)/x^2$. On a donc

$$\limsup_{x\longrightarrow} \frac{\theta(x)}{x} \leq 1 \ .$$

De même, si x est un nombre réel tel que $\theta(x) < \lambda x$, avec $\lambda < 1$, alors

$$\int_{\lambda x}^x \frac{\theta(t)-t}{t^2}dt \leq \int_{\lambda x}^x \frac{\theta(x)-t}{t^2}dt \leq \int_{\lambda x}^x \frac{\lambda x - t}{t^2}dt \leq \int_\lambda^1 \frac{\lambda - t}{t^2}dt < 0 \ .$$

Là encore, l'existence de tels nombres réels arbitrairement grands contredit le critère de Cauchy. Cela démontre le lemme puisque l'on a obtenu

$$\liminf_{x\longrightarrow\infty} \frac{\theta(x)}{x} \geq 1 \ .$$

La relation entre l'intégrale (5.1) et notre problème vient de la relation suivante, pour $\mathfrak{Re}(s) > 1$. Notons $p_1, p_2, \ldots$ la suite (croissante) des nombres premiers ; posons aussi $p_0 = 1$. Via une transformation d'Abel, on a donc, pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 1$,

$$\begin{aligned}
\Phi(s) &= \sum_{i=1}^\infty \frac{\log(p_i)}{p_i^s} \\
&= \sum_{i=1}^\infty \frac{\theta(p_i)-\theta(p_{i-1})}{p_i^s} \\
&= \sum_{i=1}^\infty \theta(p_i)\left(\frac{1}{p_i^s} - \frac{1}{p_{i+1}^s}\right) - \frac{\theta(p_0)}{p_1^s} \\
&= \sum_{i=1}^\infty \theta(p_i)\int_{p_i}^{p_{i+1}} \frac{sdx}{x^{s+1}} \\
&= \int_2^\infty \theta(x)\frac{sdx}{x^{s+1}} \ .
\end{aligned}$$

On peut réduire la borne inférieure de cette dernière intégrale à 1 puisque $\theta(x) = 0$ pour $x < 2$, et en tirer

$$\Phi(s) = s \int_1^\infty \theta(x) x^{-s-1} dx \ .$$

Comme $1/(s-1) = \int_1^\infty x^{-s} dx$, on a donc :

$$\Phi(s) - \frac{s}{s-1} = s \int_1^\infty \frac{\theta(x) - x}{x^{s+1}} dx \ .$$

Lorsque s tend vers 1, le membre de gauche a une limite car Φ a un pôle simple de résidu 1 en $s = 1$ qui s'est retrouvé simplifié ; il s'agit de démontrer que cette limite est obtenue en passant à la limite sous le signe somme.

Via le changement de variables $x = e^t$, on écrit alors

$$\frac{\Phi(s)}{s} - \frac{1}{s-1} = \int_0^\infty l(t) e^{-st} dt \ ,$$

où l'on a posé $l(t) = \theta(e^t) - e^t$. Effectuons maintenant le changement de variables $s \longmapsto s+1$. On a donc

$$\frac{\Phi(s+1)}{s} - \frac{1}{s} = \int_0^\infty f(t) e^{-st} dt \ ,$$

où $f(t) = l(t)/e^t = \theta(e^t)e^{-t} - 1$.

Le résultat voulu découle alors du théorème taubérien suivant, de nature purement analytique.

Théorème 5.7. *Soit $f : \mathbb{R}^+ \longrightarrow \mathbb{C}$ une fonction mesurable bornée, de sorte que, pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 0$, l'intégrale $g(s) = \int_0^\infty f(t)e^{-st}dt$, converge et définit une fonction holomorphe dans le demi-plan Ω_0. Supposons que cette fonction g s'étende en une fonction holomorphe, toujours notée g, définie au voisinage du demi-plan $\{\mathfrak{Re}(s) \geq 0\}$. Alors, l'intégrale $\int_0^\infty f(t)dt$ existe et vaut $g(0)$.*

Pour conclure, il reste à vérifier que la fonction f est bornée ; cela fait l'objet du dernier lemme de ce paragraphe.

Lemme 5.8. *Il existe un nombre réel $c > 0$ tel que $\theta(x) \leq cx$, pour $x \geq 2$.*

Démonstration : pour $n \in \mathbb{N}$, la formule du binôme entraîne l'inégalité

$$2^{2n} = (1+1)^{2n} \geq \left(\begin{array}{c} 2n \\ n \end{array} \right) \ .$$

Décomposons (partiellement) ce coefficient binomial en facteurs premiers. Par définition,

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) = \frac{(n+1)(n+2)\cdots(2n)}{1 \cdot 2 \cdots n} \ ,$$

tout nombre premier p tel que $n < p < 2n$ divise (avec valuation 1) $\left(\begin{array}{c} 2n \\ n \end{array} \right)$. Par suite,

$$\left(\begin{array}{c} 2n \\ n \end{array} \right) \geq \prod_{n<p<2n} p \ ,$$

d'où, en prenant les logarithmes, l'inégalité

$$\theta(2n) - \theta(n) \leq 2n \log(2) \ .$$

Soit x un nombre réel et soit n la «partie entière supérieure» de $x/2$ (le plus petit entier $\geq x/2$) ; on a donc $n - 1 < x/2 \leq n$ et donc $2n - 2 < x \leq 2n$; par suite

$$\begin{aligned} \theta(x) - \theta(x/2) &\leq \theta(2n) - \theta(n-1) \\ &\leq 2n\log(2) + \theta(n) - \theta(n-1) \\ &\leq n(2\log(2)+1) \\ &\leq x(1+\log(2)) \ . \end{aligned}$$

puisque $n < 1 + x/2$ (ce qui suffit pour justifier la dernière inégalité pour $x \geq 5$). Pour $2 \leq x < 5$, on la vérifie à la main et l'on note que par ailleurs cette inégalité est évidemment vérifiée pour x tel que $0 < x < 2$ puisqu'alors $\theta(x) = 0$.

En conclusion, pour $x > 1$,

$$\theta(x) \leq \sum_{n=0}^{\infty} \left(\theta(x/2^n) - \theta(x/2^{n+1}) \right) \leq (1+\log(2)) \sum_{n=0}^{\infty} \frac{x}{2^n} \leq 2(1+\log(2))x \ .$$

Le lemme est ainsi démontré.

Pour tout nombre réel $T > 0$ et tout nombre complexe s, posons $g_T(s) = \int_0^T f(t)e^{-st}dt$. La fonction g_T est holomorphe sur $\mathbb{C}$ et il s'agit de démontrer que l'on a $\lim_{T \longrightarrow \infty} g_T(0) = g(0)$.

Par hypothèse, la fonction f est bornée ; posons donc

$$B = \max_{|t| \geq 0} (|f(t)|) \ .$$

Pour $R > 0$ assez grand et $\delta > 0$ assez petit, soit Ω l'ouvert du plan formé des nombres complexes z tels que $|z| < R$ et $\mathfrak{Re}(z) > -\delta$. Lorsque R est fixé, et $\delta > 0$ est assez petit (dépendant de R), la fonction g est définie et holomorphe au voisinage de $\overline{\Omega}$. Notons C la frontière de Ω et considérons-la comme un lacet. D'après le théorème des résidus,

$$g(0) - g_T(0) = \frac{1}{2i\pi} \int_C (g(z) - g_T(z)) \, e^{zT} \left(1 + \frac{z^2}{R^2} \right) \frac{dz}{z} \ . \tag{5.2}$$

Pour $\mathfrak{Re}(z) > 0$, $g(z)$ est égale à l'intégrale $\int_0^\infty f(t)e^{-zt}dt$, si bien que l'on a

$$|g(z) - g_T(z)| = \left| \int_T^\infty f(t)e^{-zt}dt \right| \leq B \int_T^\infty e^{-\mathfrak{Re}(z)t}dt = \frac{B}{\mathfrak{Re}(z)} e^{-\mathfrak{Re}(z)T} \ .$$

Toujours pour $\mathfrak{Re}(z) > 0$, on a

$$\left| e^{zT} \left(1 + \frac{z^2}{R^2} \right) \frac{1}{z} \right| = \frac{1}{R} e^{\mathfrak{Re}(z)T} \left| \frac{R}{z} + \frac{z}{R} \right| = \frac{2\mathfrak{Re}(z)}{R^2} e^{\mathfrak{Re}(z)T}$$

si, de plus $|z| = R$. La contribution à l'intégrale (5.2) du demi-arc de cercle C_+ formé des $z \in C$ tels que $\mathfrak{Re}(z) \geq 0$ est ainsi majorée par

$$\left| \frac{1}{2i\pi} \int_{C_+} |g(z) - g_T(z)| e^{zT} \left(1 + \frac{z^2}{R^2} \right) \frac{dz}{z} \right| \leq \frac{l(C_+)}{2\pi} \times \frac{2B}{R^2} = \frac{B}{R} \ .$$

Soit C_- la partie du lacet C contenue dans le demi-plan $\mathfrak{Re}(z) \leq 0$. Pour calculer l'intégrale

$$I_T = \frac{1}{2i\pi} \int_{C_-} g_T e^{zT} \left(1 + \frac{z^2}{R^2} \right) \frac{dz}{z} \ ,$$

on peut remplacer le lacet C_- par le demi-arc de cercle C'_- car l'intégrande n'a pas de pôle dans le demi-plan $\mathfrak{Re}(z) < 0$, g_T étant holomorphe sur $\mathbb{C}$. Sur cet arc de cercle C'_-, on a

$$|g_T(z)| = \left| \int_0^T f(t) e^{-zt} dt \right| \leq B \int_0^T e^{-\mathfrak{Re}(z)t} dt \leq \frac{B}{-\mathfrak{Re}(z)} e^{-\mathfrak{Re}(z)T} \ .$$

Pour tout $z \in C'_-$, on a comme précédemment la majoration

$$\left| e^{zT} \left(1 + \frac{z^2}{R^2} \right) \frac{1}{z} \right| = \frac{1}{R} e^{\mathfrak{Re}(z)T} \left| \frac{R}{z} + \frac{z}{R} \right| = \frac{2|\mathfrak{Re}(z)|}{R^2} e^{\mathfrak{Re}(z)T} \ .$$

Ainsi,

$$I_T \leq \frac{l(C'_-)}{2\pi} \times \frac{2B}{R^2} \leq \frac{B}{R} \ .$$

Majorons enfin l'intégrale

$$I'_T = \frac{1}{2i\pi} \int_{C_-} g(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \ .$$

Posons,

$$B' = \max_{z \in C'_-} \left| g(z) \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z} \right| \ .$$

Le lacet C_- est formé de deux bouts d'arcs de cercles de longueurs au plus $R \arcsin(\delta) \leq 2R\delta$ et d'un segment de droite contenu dans la droite d'équation $\mathfrak{Re}(z) = -\delta$ et de longueur $2\sqrt{R^2 - \delta^2} \leq 2R$. La partie de l'intégrale I'_T correspondant aux deux arcs de cercles est ainsi majorée par

$$\frac{4R\delta}{2\pi} B' \ ,$$

tandis que la partie de l'intégrale correspondant au segment de droite est majorée par

$$\frac{2R}{2\pi} B' e^{-\delta T} \ .$$

Ainsi,

$$\left|I'_T\right| \leq B' \frac{R}{\pi} \left(2\delta + e^{-\delta T}\right) \ .$$

Mettant bout à bout les trois majorations obtenues, nous pouvons donc affirmer que

$$|g(0) - g_T(0)| \leq 2\frac{B}{R} + B' \frac{R}{\pi} \left(2\delta + e^{-\delta T}\right) \ .$$

Soit $\varepsilon > 0$ et montrons que pour T assez grand, $|g(0) - g_T(0)|$ est inférieur à ε. Commençons par poser $R = 2B/\varepsilon$ puis $\delta > 0$ de sorte que $2R\delta B'/\pi \leq \varepsilon$. Comme $e^{-\delta T}$ tend vers 0 en décroissant quand T tend vers l'infini, il existe T_0 tel que $(RB'/\pi)e^{-\delta T_0} < \varepsilon$. Alors, pour tout $T \geq T_0$, on a

$$|g(0) - g_T(0)| \leq \varepsilon + \varepsilon + \varepsilon = 3\varepsilon \ .$$

Cela démontre que

$$\lim_{T \longrightarrow \infty} g_T(0) = g(0)$$

et conclut la démonstration du théorème taubérien ainsi que celle du théorème des nombres premiers.

Nous avons vu que le théorème des nombres premiers repose sur la non-annulation de la fonction ζ de Riemann sur la droite $\{\mathfrak{Re}(s) = 1\}$. L'hypothèse de Riemann affirme qu'en fait la fonction ζ ne s'annule pas dans le demi-plan $\Omega_{1/2}$. On peut démontrer que cela entraîne le développement asymptotique suivant :

$$\pi(x) \sim \int_2^x \frac{dt}{\log(t)} + O_\varepsilon(x^{1/2+\varepsilon}) \ ,$$

où $\varepsilon > 0$ est un nombre réel arbitraire (l'intégrale du second membre, appelée logarithme intégral, est équivalente à $x/\log x$ au voisinage de $+\infty$). Inversement, s'il existe un zéro de la fonction zêta

de Riemann dont la partie réelle est égale à a avec $\frac{1}{2} < a < 1$, alors on ne peut pas choisir $\varepsilon < a - \frac{1}{2}$ dans le développement asymptotique ci-dessus.

Cette hypothèse figure dans l'article de Riemann de 1859 mais n'est toujours pas démontrée.

L'hypothèse de Riemann généralisée est l'extension de cette conjecture aux fonctions L de Dirichlet qui sont introduites au paragraphe suivant, et plus généralement, aux fonctions zêta de Dedekind associées aux corps de nombres.

5.2 Le théorème de la progression arithmétique

Le but de ce paragraphe est de prouver le théorème de la progression arithmétique, conjecturé par Euler en 1775 et démontré pour la première fois par Dirichlet en 1837. Il s'agit du théorème suivant :

Théorème 5.9. *Soient a et n des entiers naturels premiers entre eux. Pour $x > 0$, notons $\pi(x; n, a)$ le cardinal de l'ensemble des nombres premiers p tel que $p \equiv a \bmod n$ et $p \leq x$. Alors, lorsque x tend vers $+\infty$, on a l'équivalent*

$$\pi(x; n, a) \sim \frac{x}{\varphi(n) \log(x)} \ .$$

En particulier, l'ensemble des nombres premiers congrus à a modulo n est infini.

Dans ce théorème, l'hypothèse que n et a sont premiers entre eux est cruciale : comme tout nombre entier qui est congru à a modulo n est multiple du PGCD de n et a, il n'y aurait sinon qu'au plus un nombre fini de premiers vérifiant la congruence donnée.

Si l'on veut adapter les méthodes analytiques utilisées pour démontrer le théorème des nombres premiers, on est tenté d'introduire des variantes de la fonction zêta, notamment les fonctions d'une variable s données par

$$\zeta_a(s) = \prod_{p \equiv a \bmod n} \frac{1}{1 - p^{-s}} \ ,$$

dont le produit est la fonction zêta de Riemann à quelques facteurs près. Mais on ne sait pas comment étudier cette fonction holomorphe si l'on ne sait rien des nombres premiers congrus à a modulo n. L'idée remarquable de Dirichlet a consisté à transformer des propriétés multiplicatives en propriétés additives en introduisant les caractères du groupe abélien $(\mathbb{Z}/n\mathbb{Z})^\star$.

Soit G un groupe abélien fini, noté multiplicativement. On appelle caractère de G tout homomorphisme de G dans $\mathbb{C}^\star$. Comme G est fini, les valeurs prises par un caractère sont des racines de l'unité. L'ensemble des caractéres de G est noté $\hat{G}$; c'est un sous-groupe de l'ensemble des fonctions de G dans $\mathbb{C}^\star$ et son élément neutre est la fonction 1 constante de valeur 1. Le conjugué $\overline{\chi}$ d'un caractère χ est aussi un caractère, d'ailleurs égal à l'inverse χ^{-1} de χ. Supposons que G soit cyclique d'ordre n, engendré par un élément g. Tout élément de G est alors de la forme g^a, pour un entier $a \in \mathbb{Z}$ bien défini modulo n. Un caractère de G est ainsi déterminé par l'image de g qui est une racine n-ième de l'unité. Inversement, pour toute racine n-ième de l'unité z, l'application de G dans $\mathbb{C}^\star$ qui applique g^a sur z^a, pour $0 \leq a < n$, est un caractère de G.

Le groupe $\hat{G}$ est ainsi identifié au groupe des racines n-ièmes de l'unité, qui est un groupe cyclique d'ordre n. Plus généralement :

Proposition 5.10. *Soit G un groupe abélien fini ; le groupe $\hat{G}$ a même cardinal que G.*

Remarque 5.11. *Comme dans le cas d'un groupe cyclique, on peut démontrer que les groupes G et $\hat{G}$ sont isomorphes. Cette assertion est laissée en exercice.*

La démonstration de cette proposition utilise un lemme, d'intérêt général.

Lemme 5.12. *Soit G un groupe abélien fini et soit H un sous-groupe de G. Pour tout caractère χ_1 de H, il existe un caractère χ de G tel que $\chi_1 = \chi_{|H}$.*

Démonstration : démontrons ce lemme par récurrence sur l'indice

$$(G : H) = \mathrm{Card}(G)/\mathrm{Card}(H) \ .$$

Il n'y a rien à démontrer si $(G : H) = 1$. Considérons sinon un élément $g \in G \setminus H$ et soit m le plus petit entier > 1 tel que $g^m \in H$. Comme G est commutatif, l'ensemble des produits $g^a h$, où $0 \leq a < m$ et $h \in H$ est un sous-groupe H' de G. En outre, l'égalité $g^a h = g^b k$ avec $0 \leq a, b < m$ et $h, k \in H$ entraine $g^{b-a} = hk^{-1}$, d'où $a = b$ et $h = k$. Tout élément de H' s'écrit donc d'une seule manière sous la forme $g^a h$.

Soit z un nombre complexe tel que $z^m = \chi_1(g^m)$. Pour $h' = g^a h \in H'$, posons $\chi'(h') = z^a \chi_1(h)$.

L'application $\chi' : H' \longrightarrow \mathbb{C}^\star$ est un caractère. En effet, si $h' = g^a h$ et $k' = g^b k$ sont des éléments de H, on a $h'k' = g^{a+b} hk$ car le groupe est abélien. Si $a + b < m$, il vient

$$\chi'(h'k') = \chi'(g^{a+b} hk) = z^{a+b} \chi_1(hk) = z^a \cdot z^b \cdot \chi_1(h) \cdot \chi_1(k) = \chi'(h) \cdot \chi'(k) \ ,$$

tandis que si $a + b > m$, on a aussi $a + b < 2m$ et

$$\begin{aligned} \chi'(h'k') &= \chi'(g^{a+b-m} g^m hk) = z^{a+b-m} \chi_1(g^m hk) \\ &= z^{a+b-m} \cdot \chi_1(g^m) \cdot \chi_1(h) \cdot \chi_1(k) = z^{a+b} \chi_1(h) \chi_1(k) \\ &= \chi'(h) \cdot \chi'(k) \ . \end{aligned}$$

Comme l'indice $(G : H')$ de H' dans G est égal à $(G : H)/m < (G : H)$, il existe par récurrence un caractère χ de G dont la restriction à H' est égale à χ'. En particulier, $\chi_{|H} = \chi_1$.

Démonstration de la proposition 5.10 : nous avons déjà vu que cette proposition est vraie lorsque G est cyclique. Dans le cas général, démontrons-la par récurrence sur l'ordre de G. Les cas $\mathrm{Card}(G) = 1, 2, 3$ résultent du cas cyclique, puisque tous les groupes de tels cardinaux sont cycliques.

Soit h un élément de G non réduit à l'identité et soit H le sous-groupe cyclique engendré par h. Si m désigne son ordre, on a $m > 1$. Le groupe H étant cyclique, il existe pour toute racine m-ième de l'unité z, un unique caractère $\tilde{\chi}_z$ de H tel que $\tilde{\chi}_z(h) = z$. Prolongeons-les en un caractère χ_z de G. Par ailleurs, le groupe G/H est d'ordre $k = \mathrm{Card}(G)/m < \mathrm{Card}(G)$ et il existe par récurrence $\mathrm{Card}(G)/m$ caractères de ce groupe ; notons-les $\tilde{\theta}_1, \ldots, \tilde{\theta}_k$. Pour $1 \leq i \leq k$, la composition θ_i de l'homomorphisme de G dans G/H et de $\tilde{\theta}_i$ est un caractère de G dont la restriction à H est constante de valeur 1. Alors, pour tout couple (z, i) formé d'une racine m-ième de l'unité et d'un entier i tel que $1 \leq i \leq k$, l'application $\chi_z \theta_i$ est un caractère de G. Ces caractères sont deux à deux distincts.

Supposons en effet que $\chi_z\theta_i = \chi_u\theta_j$; par restriction à H, on trouve $z = u$; alors, $\theta_i = \theta_j$, ce qui entraîne par passage au quotient $\tilde{\theta}_i = \tilde{\theta}_j$, puis $i = j$. Nous avons ainsi construit $mk = \mathrm{Card}(G)$ caractères distincts de G. Inversement, si χ est un caractère de G, sa restriction à H est de la forme $\tilde{\chi}_z$, où z est une racine m-ième de l'unité. Alors, $\chi \cdot \chi_z^{-1}$ est un caractère de G qui applique tout élément de H sur 1. Ce caractère définit donc, par passage au quotient, un caractère du groupe G/H. Autrement dit, il existe un unique entier $i \in \{1, \ldots, k\}$ tel que $\chi \cdot \chi_z^{-1} = \theta_i$, d'où $\chi = \chi_z\theta_i$. Cela démontre que tout caractère de G est parmi ceux que nous avons construit. Par conséquent, $\mathrm{Card}(\hat{G}) = \mathrm{Card}(G)$.

Dans la démonstration, les caractères χ_z prennent la valeur $z \neq 1$ en l'élément h de G. Par conséquent :

Lemme 5.13. *Soit G un groupe abélien fini et soit h un élément de G distinct de l'élément neutre. Il existe un caractère χ de G tel que $\chi(h) \neq 1$.*

La proposition suivante explique pourquoi les caractères permettent de transormer propriétés multiplicatives en propriétés additives.

Proposition 5.14. *Soit G un groupe abélien fini. Pour tout caractère χ de G, on a*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \ , \\ \mathrm{Card}(G) & \text{si } \chi = 1 \ . \end{cases}$$

De manière analogue, on a pour tout élément g de G :

$$\sum_{\chi\in\hat{G}} \chi(g) = \begin{cases} 0 & \text{si } g \neq 1 \ ; \\ \mathrm{Card}(G) & \text{si } g = 1 \ . \end{cases}$$

Démonstration : le cas $\chi = 1$ est évident. Supposons $\chi \neq 1$ et soit $h \in G$ tel que $\chi(h) \neq 1$. Comme $g \longmapsto hg$ est une permutation de G,

$$\sum_{\chi\in\hat{G}} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g) \ .$$

Puisque $\chi(h) \neq 1$, nécéssairement, la somme est nulle. L'autre égalité se démontre de même en utilisant que si $g \neq 1$, il existe un caractère ψ tel que $\psi(g) \neq 1$: alors,

$$\sum_{\chi\in\hat{G}} \chi(g) = \sum_{\chi\in\hat{G}} \chi \cdot \psi(g) = \psi(g) \sum_{\chi\in\hat{G}} \chi(g) \ ,$$

d'où l'annulation de $\sum_\chi \chi(g)$ pour $g \neq 1$. Lorsque $g = 1$, on a évidemment

$$\sum_{\chi\in\hat{G}} \chi(g) = \mathrm{Card}(\hat{G}) = \mathrm{Card}(G) \ .$$

Soit N un entier naturel tel que $N > 1$. Le groupe abélien fini qui va nous intéresser maintenant est le groupe $(\mathbb{Z}/N\mathbb{Z})^\star$ est entiers modulo N qui sont inversibles. Comme la classe d'un entier a est

inversible dans $\mathbb{Z}/N\mathbb{Z}$ si et seulement si a et N sont premiers entre eux, le cardinal de ce groupe $(\mathbb{Z}/N\mathbb{Z})^\star$ est égal à $\varphi(N)$. Si ϕ est une fonction du groupe $(\mathbb{Z}/N\mathbb{Z})^\star$ dans $\mathbb{C}$, on identifiera ϕ à la fonction de $\mathbb{Z}$ dans $\mathbb{C}$ qui envoie un entier a sur l'image par ϕ de la classe de a modulo N lorsque a est premier à N, et sur 0 sinon. En particulier, les caractères de $(\mathbb{Z}/N\mathbb{Z})^\star$ sont identifiés aux fonctions $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ vérifiant les propriétés suivantes :

(i) $\chi(1) = 1$;

(ii) si $(a, N) \neq 1$, $\chi(a) = 0$;

(iii) pour tout $(a, b) \in \mathbb{Z}^2$, $\chi(ab) = \chi(a)\chi(b)$.

Ces fonctions sont appelées caractères de Dirichlet modulo N et sont en nombre $\varphi(N)$; soit χ_0 la fonction qui envoie un entier sur 1 s'il est premier à N et sur 0 sinon. On l'appelle le caractère principal et correspond au caractère trivial de $(\mathbb{Z}/N\mathbb{Z})^\star$.

De plus, pour tout caractère modulo N, disons χ, on a

$$\sum_{a=0}^{N-1} \chi(a) = \begin{cases} 0 & \text{si } \chi \neq \chi_0 \ , \\ \varphi(N) & \text{si } \chi = \chi_0 \ . \end{cases}$$

Pour tout caractère de Dirichlet χ modulo N (et $s \in \mathbb{C}$), on pose

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \ ;$$

cette série converge absolument si $\mathfrak{Re}(s) > 1$, et la convergence est normale dans tout demi-plan Ω_a avec $a > 1$. Comme pour la fonction ζ de Riemann, le lien avec les nombres premiers provient de la décomposition en produit eulérien :

Proposition 5.15. *Pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 1$, on a*

$$L(\chi, s) = \prod_{p \in \mathcal{P},\, p \nmid N} \frac{1}{(1 - \chi(p) p^{-s})} \ .$$

Démonstration : la démonstration est presque identique à celle de la proposition 5.2. Elle résulte de l'unicité de la décomposition en facteurs premiers et de la propriété de multiplicativité satisfaite par les caractères de Dirichlet.

Lorsque $\chi = \chi_0$, on voit donc que

$$L(\chi_0, s)/\zeta(s) = \prod_{p|N} \left(1 - p^{-s}\right)$$

est une fonction holomorphe sur le plan complexe ; en particulier, $L(\chi_0, s)$ a un prolongement méromorphe à $\mathbb{C}$, avec un unique pôle en $s = 1$, simple et de résidu égal à

$$\prod_{p|N} \left(1 - \frac{1}{p}\right) = \frac{\varphi(N)}{N} \ .$$

Proposition 5.16. *Pour tout caractère de Dirichlet modulo N distinct du caractère principal, la fonction $s \longmapsto L(\chi, s)$ s'étend en une fonction holomorphe sur $\mathbb{C}$.*

Démonstration : contentons-nous de démontrer l'existence d'un prolongement à l'ouvert Ω_0. Nous effectuons une sommation d'Abel. Posons donc

$$F(n) = \sum_{m=1}^{n} \chi(m) \ .$$

Pour $\mathfrak{Re}(s) > 1$, on a alors

$$\begin{aligned} L(\chi, s) &= \sum_{n=1}^{\infty} \chi(n) n^{-s} \\ &= \sum_{n=1}^{\infty} \left((F(n) - F(n-1)) \, n^{-s} \right. \\ &= \sum_{n=1}^{\infty} F(n) \left(n^{-s} - (n+1)^{-s} \right) \ . \end{aligned}$$

Comme $\sum_{m=1}^{N} \chi(m) = 0$, on a $F(n) = \sum_{m=1}^{n \bmod N} \chi(m)$, et la fonction F est bornée, majorée en module par $\varphi(N)$. En outre, lorsque n tend vers l'infini,

$$n^{-s} - (n+1)^{-s} = n^{-s}\left(1 - \left(1 + \frac{1}{n}\right)^{-s}\right) = O(n^{-s-1}) \ .$$

Par suite, la série de terme général $F(n)(n^{-s} - (n+1)^{-s})$ converge absolument pour $\mathfrak{Re}(s) > 0$, uniformément dans tout demi-plan Ω_a avec $a > 0$. Sa somme est une fonction holomorphe dans le demi-plan Ω_0 qui fournit le prolongement cherché de la fonction $L(\chi, s)$.

Une variante de l'argument qui précède fournit une précision importante, à savoir que pour tout caractère non principal χ, la fonction $L(\chi, s)$ est égale à la somme de la série de terme général $\chi(n)/n^s$ pour tout nombre complexe s tel que $\mathfrak{Re}(s) > 0$.

Le reste de la démonstration est très proche de celle du théorème des nombres premiers, le point crucial est la non-annulation des fonctions L de Dirichlet sur l'axe $\{\mathfrak{Re}(s) = 1\}$.

Nous verrons cependant que l'existence d'une infinité de nombres premiers dans une progression arithmétique (par opposition au dénombrement asymptotique de tels nombres premiers) ne requiert « que » la non-annulation de $L(\chi, 1)$, lorsque χ est un caractère non-principal. Cela explique que le théorème de la progression arithmétique ait précédé celui des nombres premiers de près de 60 ans.

Proposition 5.17. *Pour tout caractère de Dirichlet χ modulo N, distinct du caractère principal, et pour tout nombre complexe s tel que $\mathfrak{Re}(s) \geq 1$, on a $L(\chi, s) \neq 0$.*

Lorsque $\chi = \chi_0$ est le caractère principal, la même assertion vaut si l'on suppose de plus que $s \neq 1$.

Démonstration : cela résulte de l'expression de $L(\chi, s)$ comme produit infini si $\mathfrak{Re}(s) > 1$, la difficulté étant concentrée sur l'axe $\mathfrak{Re}(s) = 1$. Plutôt que de traiter séparément les diverses fonctions L, faisons leur produit et posons

$$Z(s) = \prod_{\chi} L(\chi, s) \ .$$

Pour $\mathfrak{Re}(s) > 1$, on a

$$-\frac{Z'(s)}{Zs)} = \sum_{\chi}\sum_{p} \frac{\chi(p)\log(p)}{p^s - \chi(p)} = \sum_{p}\left(\sum_{\chi}\chi(p)\right)\frac{\log(p)}{p^s} + \sum_{\chi}\sum_{p}\frac{\chi(p)^2\log(p)}{p^s(p^s - \chi(p))} \ .$$

Notons $\Phi(s)$ le premier terme ; si le second définit une fonction holomorphe dans le demi-plan $\Omega_{1/2}$, Φ n'est a priori holomorphe que dans Ω_1 et nous devons prouver qu'elle n'a pas de pôle sur l'axe $\mathfrak{Re}(s) = 1$. On a en outre

$$\Phi(s) = \varphi(N) \sum_{p \equiv 1 \bmod N} \frac{\log(p)}{p^s} \ .$$

Les pôles de Φ sur cet axe sont simples et proviennent du pôle simple de $L(\chi_0, s)$ en $s = 1$ et des zéros éventuels des fonctions L associées aux caractères non-principaux (le cas du caractère principal résulte de ce qui a été fait pour la fonction zêta).

Fixons un nombre réel $\tau > 0$. Notons q, m, n la somme des ordres des zéros des fonctions $L(\chi, s)$ en $s = 1$, $s = 1 + i\tau$ et $s = 1 + 2i\tau$ lorsque χ parcourt l'ensemble des caractères de Dirichlet modulo N. Autrement dit, on a $\mathrm{ord}_{s=1} Z(s) = q$, $\mathrm{ord}_{s=1+i\tau} Z(s) = m$ et $\mathrm{ord}_{s=1+2i\tau} Z(s) = n$. On a $q \geq -1$ (en $s = 1$, le caractère principal fournit un pôle simple, les autres fonctions L n'ont pas de pôle) et $m, n \geq 0$; il s'agit de prouver que $q = -1$ et $m = 0$. Comme $\overline{L(\chi, s)} = L(\overline{\chi}, \overline{s})$, les ordres d'annulation de $Z(s)$ en $s = 1 - i\tau$ et $s = 1 - 2i\tau$ sont égaux à m et n respectivement.

Reprenons l'astuce utilisée pour la fonction zêta de Riemann, observons que pour $\sigma > 1$,

$$\sum_{k=-2}^{2} \Phi(\sigma + i\tau k) = \sum_{p \equiv 1 \bmod N} \frac{\log(p)}{p^{\sigma}} \left(2\cos(\tau \log(p))\right)^4 \geq 0 \ .$$

Par suite, multipliant par $(\sigma - 1)$ et faisant tendre σ vers 1, on obtient

$$-n - 4m - 6q - 4m - n \geq 0 \ ,$$

d'où $8m + 2n \leq -6q$. Nécessairement, $q \leq 0$. Si $q = -1$ (ce qu'on veut), il vient $m = 0$. Il reste à exclure le cas où $q = 0$: dans ce cas, il existe un caractère modulo N, et un seul, disons χ, tel que $L(\chi, s)$ ait un zéro simple en $s = 1$. Alors, $L(\overline{\chi}, 1) = \overline{L(\chi, 1)} = 0$, donc $\overline{\chi} = \chi$ et le caractère χ est à valeurs réelles.

L'assertion voulue résulte alors de la proposition suivante.

Proposition 5.18. *Si χ est un caractère modulo N, non principal et réel, on a $L(\chi,1)\neq 0$.*

Démonstration : pour $t\in[0,1[$, posons

$$f(t)=\sum_{d=1}^{\infty}\chi(d)\frac{t^d}{1-t^d}\ .$$

La série converge pour tout t dans l'intervalle indiqué, et la convergence est normale sur chaque intervalle $[0,a]$ avec $a<1$. En développant $1/(1-t^d)$ en série, on obtient

$$f(t)=\sum_{d=1}^{\infty}\sum_{m=1}^{\infty}\chi(d)t^{dm}=\sum_{n=1}^{\infty}t^n\sum_{d|n}\chi(d)$$

en regroupant les termes de même valeur $n=dm$.

Posons $c_n=\sum_{d|n}\chi(d)$. Montrons que $c_n\geq 0$ pour tout entier n. Si $n=p^a$ est une puissance d'un nombre premier, on a

$$c_{p^a}=1+\chi(p)+\chi(p^2)\cdots+\chi(p^a)\geq 0\ .$$

Plus précisément, la somme vaut $a+1$ si $\chi(p)=1$, 1 si $p\mid N$; si $\chi(p)=-1$, elle vaut 1 ou 0 suivant que a est pair ou impair. En outre, si $n=\prod_i p_i^{a_i}$ est la décomposition en facteurs premiers de l'entier n, un diviseur d de n est de la forme $\prod_i p_i^{m_i}$ avec $0\leq m_i\leq a_i$, d'où

$$c_n=\sum_{m_1=0}^{a_1}\cdots\sum_{m_r=0}^{a_r}\chi\left(p_1^{m_1}\cdots p_r^{m_r}\right)=\prod_{i=1}^{r}c_{p_i}^{a_i}\geq 0\ .$$

Nous avons remarqué que $c_n=1$ si n est une puissance d'un nombre premier qui divise N ; en particulier, $\sum c_n=+\infty$. Par suite, lorsque t tend vers 1 par valeurs inférieures, $f(t)$ tend vers $+\infty$. Lorsque $t\longrightarrow 1$, $t^n/(1-t^n)$ est équivalent à $1/n(1-t)$. Posons ainsi

$$b_n=(1-t)\left(\frac{t^n}{1-t^n}-\frac{1}{n(1-t)}\right)=\frac{t^n}{1+t+\cdots+t^{n-1}}-\frac{1}{n}\ .$$

Démontrons que la suite (b_n) est croissante. En effet, on a

$$b_{n+1}-b_n=\frac{-t^n}{(1+t+\cdots+t^{n-1})(1+t+\cdots+t^n)}+\frac{1}{n(n+1)}\ .$$

L'inégalité entre moyennes arithmétique et géométriques entraîne par ailleurs

$$1+t+\cdot+t^{n-1}\geq nt^{(n-1)/2}\qquad\text{et}\qquad 1+t+\cdots+t^n\geq(n+1)t^{(n)/2}\ ,$$

si bien que

$$b_{n+1}-b_n\geq\frac{-t^n}{n(n+1)t^{n-\frac{1}{2}}}+\frac{1}{n(n+1)}=\frac{1}{n(n+1)}\left(1-\sqrt{t}\right)\geq 0\ ,\ \text{pour } t\leq 1\ .$$

Supposons par l'absurde que $L(\chi,1)=0$; alors $\sum_{n=1}^{\infty}\chi(n)/n=0$ et

$$f(t)=\sum_{n=1}^{\infty}\chi(n)\left(\frac{t^n}{1-t^n}-\frac{1}{n(1-t)}\right)=\frac{1}{1-t}\sum_{n=1}^{\infty}b_n\chi(n)\ .$$

Puisque χ est périodique de période N et que $\sum_{n=1}^{N}\chi(n)=0$, on a

$$\left|\sum_{d=1}^{n}\chi(d)\right|\leq N$$

pour tout entier n. Effectuons alors une transformation d'Abel :

$$\left|\sum_{n=1}^{\infty}b_n\chi(n)\right|=\left|\sum_{d=1}^{\infty}\left(\sum_{n=1}^{d}\chi(n)-\sum_{n=1}^{d-1}\chi(n)\right)b_d\right|=\left|\sum_{d=1}^{\infty}\left(\sum_{n=1}^{d}\chi(n)\right)(b_d-b_{d+1})\right|\ .$$

Soit :

$$\left|\sum_{n=1}^{\infty}b_n\chi(n)\right|\leq\sum_{d=1}^{\infty}\left|\sum_{n=1}^{d}\chi(n)\right||b_d-b_{d+1}|\leq N\sum_{d=1}^{\infty}(b_{d+1}-b_d)=N(-b_1+\lim_{d\longrightarrow\infty}b_d)\ .$$

En notant que $\lim_{d\longrightarrow\infty}b_d=0$ et que $b_1=t-1$, on a donc

$$\left|\sum_{n=1}^{\infty}b_n\chi(n)\right|\leq N(1-t)\leq N\ .$$

On a donc $|f(t)|\leq N$ pour tout $t\in[0,1[$ ce qui contredit le fait que $f(t)\longrightarrow\infty$ pour $t\longrightarrow 1$.

Soit a un entier qui est premier à N. Pour $\mathfrak{Re}(s)>1$, posons

$$\Phi(s;a)=\sum_{p\equiv a \bmod N}\frac{\log(p)}{p^s}\ .$$

Posons aussi, pour tout nombre réel $x>0$,

$$\theta(x;a)=\sum_{p\leq x,p\equiv a \bmod N}\log(p)\ .$$

On a alors :

Proposition 5.19. *La série qui définit Φ_a converge pour $\mathfrak{Re}(s)>1$; sa somme se prolonge en une fonction méromorphe dans l'ouvert $\Omega_{1/2}$ qui n'a pas de pôle dans un voisinage du demi-plan $\{\mathfrak{Re}(s)\geq 1\}$, excepté un pôle simple en $s=1$, de résidu $1/\varphi(N)$.*

Démonstration : si χ est un caractère de Dirichlet modulo N et s un nombre complexe de partie réelle >1, la dérivée logarithmique de $L(\chi,s)$ admet le développement en série

$$-\frac{L'(\chi,s)}{L(\chi,s)}=\sum_p\chi(p)\frac{\log(p)p^{-s}}{1-\chi(p)p^{-s}}=\sum_p\chi(p)\frac{\log(p)}{p^s}+\sum_p\chi^2(p)\frac{\log(p)}{p^s(p^s-\chi(p))}\ .$$

Le membre de gauche est méromorphe dans le demi-plan Ω_0 et n'a pas de pôle dans un voisinage du demi-plan $\{\mathfrak{Re}(s) = 1\}$, hormis, si $\chi = \chi_0$ est le caractère principal, un pôle simple de résidu 1 en $s = 1$ causé par le pôle simple de $L(\chi_0, s)$ en $s = 1$. Le second terme du second membre définit une fonction holomorphe $\Psi(\chi, s)$ dans le demi-plan $\Omega_{1/2}$; par suite, le premier terme du second membre définit une fonction méromorphe dans $\Omega_{1/2}$ qui n'a pas de pôle au voisinage du demi-plan fermé $\{\mathfrak{Re}(s) = 1\}$, sauf en $s = 1$ si $\chi = \chi_0$. Par suite, sommant sur l'ensemble des caractères de Dirichlet modulo N, il vient

$$\begin{aligned} -\sum_{\chi} \frac{L'(\chi, s)}{L(\chi, s)} \chi(a)^{-1} &= \sum_{p} \left(\sum_{\chi} \chi(p)\chi(a)^{-1} \right) \frac{\log(p)}{p^s} + \sum_{\chi} \Psi(\chi, s)\chi(a)^{-1} \\ &= \varphi(N) \sum_{p \equiv a \bmod N} \frac{\log(p)}{p^s} + \sum_{\chi} \Psi(\chi, s)\chi(a)^{-1} \\ &= \varphi(N)\Phi(s, a) + \sum_{\chi} \Psi(\chi, s)\chi(a)^{-1} \ . \end{aligned}$$

Puisque pour tout nombre entier p, notant b un inverse de a modulo N, on a

$$\sum_{\chi} \chi(p)\chi(a)^{-1} = \sum_{\chi} \chi(pb) = \begin{cases} \varphi(N) & \text{si } pb \equiv 1 \bmod N \ , \\ 0 & \text{sinon} \ . \end{cases}$$

Par conséquent, la fonction $\Phi(s; a)$ s'étend en une fonction méromorphe dans le demi-plan $\Omega_{1/2}$ sans pôle au voisinage du demi-plan fermé $\{\mathfrak{Re}(s) = 1\}$ excepté en $s = 1$ où elle a un pôle simple de résidu $1/\varphi(N)$ issu du terme pour $\chi = \chi_0$ (comme a est premier à N, $\chi_0(a) = 1$).

À ce stade, il ne reste plus qu'à recopier ce qu'on avait fait pour le théorème des nombres premiers. On démontre successivement, par les mêmes arguments, que l'intégrale

$$\int_1^{\infty} \left(\theta(x, a) - \frac{x}{\varphi(N)} \right) \frac{dx}{x^2}$$

converge, qu'au voisinage de $+\infty$,

$$\theta(x, a) \sim \frac{x}{\varphi(N)}$$

et enfin que

$$\pi(x; a) \sim \frac{x}{\varphi(N) \log(x)} \ .$$

Si l'on souhaite éviter l'emploi du théorème taubérien mais ne démontrer en contre partie que l'existence d'une infinité de nombres premiers congrus à a modulo N, il suffit d'observer que $\Phi(s; a)$ tend vers l'infini quand s tend vers 1, alors qu'il aurait une limite finie si la progression arithmétique considérée était finie.

6 Extensions de corps

6.1 Préliminaires

Soit K un corps. Une extension du corps K est un corps E muni d'un homomorphisme de K dans E. Un tel homomorphisme est injectif, ce qui permet en pratique de considérer que K est un sous-corps de E, ou que E est un sur-corps de K. Lorsque $K \hookrightarrow E$ est une extension de corps, on considère E comme une K-algèbre et comme un espace vectoriel sur K ; on note $[E : K]$ sa dimension, et on l'appelle le degré de l'extension $K \hookrightarrow E$.

Soit $K \hookrightarrow E$ une extension de corps ; un élément x de E est dit algébrique sur K s'il existe un polynôme non nul P à coefficients dans K tel que $P(x) = 0$ (plus rigoureusement, si $\iota : K \hookrightarrow E$ est l'homomorphisme qui définit l'extension, il faudrait noter $\iota(P)(x) = 0$, où $\iota(P)$ désigne le polynôme à coefficients dans E dont les coefficients sont les images par ι des coefficients de P). On s'autorisera dans la suite ce genre d'abus de langage, pour alléger la présentation à moins que cela puisse créer des confusions dangereuses. Si x n'est pas algébrique, on dit qu'il est transcendant.

Exemple 6.1. *Soit $K(X)$ le corps des fractions rationnelles en une variable. C'est une extension de K et X est transcendant sur K.*

Plus difficile, π, e sont transcendants sur $\mathbb{Q}$.

Si $x \in E$ est algébrique sur K, l'ensemble des polynômes $P \in K[X]$ tels que $P(x) = 0$ est un idéal de $K[X]$, non réduit à 0. Il est donc formé des multiples d'un polynôme unitaire M_x, qu'on appelle le polynôme minimal de x et qui est le polynôme unitaire de degré minimal P tel que $P(x) = 0$. Le degré de M_x est appelé le degré de x.

Lemme 6.2. *Soit $K \hookrightarrow E$ une extension et $x \in E$ un élément algébrique de E sur K. Alors, le polynôme minimal M_x est irréductible.*

Démonstration : si l'on avait une factorisation non triviale $M_x = PQ$, on aurait $P(x)Q(x) = 0$, d'où $P(x) = 0$ ou $Q(x) = 0$ ce qui contredit l'hypothèse que M_x est de degré minimal.

Soit $K \hookrightarrow E$ une extension de corps et soit x un élément de E. L'ensemble $K[x]$ des éléments de E de la forme $P(x)$, où $P \in K[X]$, est une sous-algèbre de E. Si x est transcendant, elle est isomorphe à $K[X]$; elle est donc de dimension infinie sur K et n'est pas un corps. Si x est algébrique, elle est isomorphe à l'anneau quotient $K[X]/(M_x)$. C'est un sous-corps de E puisque M_x est irréductible.

Une extension $K \hookrightarrow E$ est dite algébrique si tout élément de E est algébrique sur K.

Proposition 6.3. *Toute extension de degré fini est algébrique. Plus généralement, soit $K \hookrightarrow E$ une extension de corps. Toute sous K-algèbre A de E qui est de dimension finie est un corps et tout élement de A est algébrique sur K.*

Démonstration : Soit $K \hookrightarrow E$ une extension de degré fini n, et soit x un élément de E. On a vu que si $x \in E$ est transcendant, alors $K[x]$ est un sous-espace vectoriel de E de dimension infinie, ce qui contredit $[E : K] = n < \infty$. On voit même que $\deg(x) \leq n$ par cet argument.

Soit $K \hookrightarrow E$ une extension de corps et soit A une sous-algèbre de E qui est un K-espace vectoriel de dimension finie. Soit x un élément non nul de A. La multiplication par x est un endomorphisme injectif du K-espace vectoriel A car A est un anneau intègre. Cet endomorphisme est donc surjectif

et, en particulier, x est inversible dans A. Cela démontre que A est un corps. Alors, $K \hookrightarrow A$ est une extension de degré fini. D'après la première partie de la proposition, tout élément de A est algébrique sur K.

Corollaire 6.4. *Soit $K \hookrightarrow E$ une extension de corps. L'ensemble des éléments de E qui sont algébriques sur K est un sous-corps de E. En particulier, la somme, le produit de deux éléments algébriques de E est algébrique ; l'inverse d'un élément algébrique non nul de E est algébrique.*

Démonstration : soient x, y des éléments de E qui sont algébriques sur K ; notons m et n leurs degrés. Soit alors A l'ensemble des éléments de E de la forme $P(x, y)$, où $P \in K[X, Y]$. Par définition, c'est une sous K-algèbre de E. Comme x est de degré n et y est de degré m, tout élément de A peut s'écrire sous la forme $P(x, y)$, avec $P \in K[X, Y]$ tel que $\deg_X(P) < n$ et $\deg_Y(P) < m$. Donc, tout élément de A est combinaison linéaire des $x^i y^j$ avec $0 \leq i < n$ et $0 \leq j < m$. L'algèbre A est donc de dimension finie sur K et est donc un corps par l'énoncé précédent. Toujours par la proposition précédente, comme $x + y, xy, x^{-1}$ (si $x \neq 0$ pour la dernière assertion) sont dans A, ils sont tous algébriques.

Il en résulte aussitôt que l'ensemble des éléments de E qui sont algébriques sur K est un sous-corps de E.

Soit $K \hookrightarrow E$ une extension de corps et soit x, y des éléments de E qui sont algébriques. Si l'on souhaite déterminer explicitement un polynôme annulateur de $x + y$, le théorème de Cayley-Hamilton s'avère très utile. Connaissant des polynômes P et Q qui annulent x et y, il est en effet très aisé d'écrire une matrice $(a_{(i,j)}(k, l))$ de taille mn, indexée par l'ensemble des couples (i, j) avec $0 \leq i < m$ et $0 \leq j < n$, telle que

$$(x + y)x^k y^l = \sum_{0 \leq i < n, 0 \leq j < m} a_{(i,j)}(k, l) x^i y^j \ , \ \ \forall (k, l) \in \mathbb{N}^2, 0 \leq k < n, 0 \leq l < m \ . \tag{6.1}$$

Soit Π le polynôme caractéristique de la matrice A. D'après la proposition suivante, le polynôme Π annule l'endomorphisme de multiplication par $x + y$. En particulier, $P(x + y) = 0$.

Proposition 6.5. *Soit V un espace vectoriel sur un corps K, soit*

$$v = (v_1, \ldots, v_n)$$

une famille génératrice de V. Soit f un endomorphisme de V et soit A une matrice telle que

$$f(v_j) = \sum_{i=1}^{n} a_{i,j} v_i \qquad \forall 1 \leq j \leq n \ .$$

Si P est le polynôme caractéristique de A, on a $P(f) = 0$.

Démonstration : on note u la surjection de K^n sur V envoyant la base canonique de K^n sur v, et ϕ l'endomorphisme de K^n de matrice A. On a $u \circ \phi = f \circ u$. Le théorème de Cayley-Hamilton assure que $P(\phi) = 0$ et donc $0 = u \circ P(\phi) = P(f) \circ u$. Comme u est surjective, $P(f) = 0$.

Exemple 6.6. *Choisissons $K = \mathbb{Q}$, $x = \sqrt{2}$ et $y = \sqrt{3}$. Une famille génératrice de l'algèbre $K[x, y]$ est donc $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. On a les relations :*

$$\begin{cases} (\sqrt{2}+\sqrt{3})\cdot 1 &= 0\cdot 1 + 1\cdot\sqrt{2} + 1\cdot\sqrt{3} + 0\cdot\sqrt{6}\ , \\ (\sqrt{2}+\sqrt{3})\cdot\sqrt{2} &= 2\cdot 1 + 0\cdot\sqrt{2} + 0\cdot\sqrt{3} + 1\cdot\sqrt{6}\ , \\ (\sqrt{2}+\sqrt{3})\cdot\sqrt{3} &= 3\cdot 1 + 0\cdot\sqrt{2} + 0\cdot\sqrt{3} + \sqrt{6} \\ (\sqrt{2}+\sqrt{3})\cdot\sqrt{6} &= 0\cdot 1 + 3\cdot\sqrt{2} + 2\cdot\sqrt{3} + 0\cdot\sqrt{6}, \end{cases}$$

La matrice

$$A = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}\ ,$$

représente la multiplication par $\sqrt{2}+\sqrt{3}$ sur le système générateur fixé et elle a pour polynôme caractéristique $X^4 - 10X^2 + 1$. On vérifie facilement

$$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0\ .$$

Une autre méthode, plus systématique, consiste à utiliser la théorie des résultants que nous verrons un peu plus tard.

Soit K un corps et soit P un polynôme irréductible à coefficients dans K, notons d son degré. Si $d \geq 2$, alors P n'a pas de racine dans K. Nous allons construire une extension de K dans laquelle P a une racine et qui est « universelle » pour cette propriété.

Notons L l'anneau $K[X]/(P)$, quotient de l'anneau des polynômes par l'idéal principal engendré par P. Comme l'anneau $K[X]$ est un anneau principal et que P est irréductible, cet idéal est un idéal maximal ; autrement dit l'anneau L est un corps. C'est donc une extension de K. Notons x la classe de X dans L ; la division euclidienne par P entraîne que $(1, x, \ldots, x^{d-1})$ est une base de L sur K. Par suite, le degré $[L : K]$ de cette extension est égal à d.

De plus, comme $P(x)$ est la classe du polynôme $P(X)$ dans L, on a $P(x) = 0$; ainsi, x est une racine de P dans le corps L. Enfin, tout élément de L est un polynôme en x. Nous dirons que L, et plus généralement toute extension de K qui est engendrée par une racine de P, est une extension de K obtenue par adjonction d'une racine de P, ou une extension de rupture du polynôme P, ou encore un corps de rupture du polynôme P.

Si E est une extension de K et $f : L \hookrightarrow E$ est un morphisme d'extensions, $f(x)$ est une racine de P dans E. Comme tout élément de L est un polynôme en x, l'homomorphisme f est déterminé par cette racine $f(x)$.

Inversement, soit E une extension de K et y une racine de P dans E. Notons g l'application de $K[X]$ dans E donnée par $g(Q) = Q(y)$ si $Q \in K[X]$; c'est un homomorphisme de K-algèbres. En outre, $P(x) = 0$ si bien que tout élément de l'idéal (P) a pour image 0 par g. Par passage au quotient, on en déduit donc un homomorphisme f de L dans E tel que $f(x) = g(X) = y$. Si E est engendrée par y, alors g est surjectif, donc f est surjectif. Par suite, c'est un isomorphisme d'extensions.

Nous avons ainsi démontré le résultat suivant :

Proposition 6.7. *Soit L une extension de rupture d'un polynôme irréductible $P \in K[X]$, et soit x une racine de P dans L.*

(i) Pour tout couple (E, y) formé d'une extension E de K et d'une racine y de P dans E, il existe un et un seul homomorphisme d'extensions $f : L \longrightarrow E$ tel que $f(x) = y$.

(ii) Si E est une extension de rupture de P et y une racine de P dans E, cet homomorphisme f est un isomorphisme.

Soit K un corps et soit P un polynôme à coefficients dans K ; on ne suppose pas P irréductible. Si P n'est pas scindé dans K, choisissons un facteur irréductible Q de P de degré $d \geq 2$ et soit $K \hookrightarrow L$ une extension de rupture de Q et x une racine de Q dans L. Dans $L[X]$, le polynôme P est multiple de $X - x$; appliquons alors cet argument au polynôme quotient $P(X)/(X - x)$. On construit ainsi par récurrence une extension E de K dans laquelle le polynôme P est scindé. Notons $x_1, \ldots, x_d$ ses racines dans E, répétées suivant leur multiplicité, de sorte que $P(X) = a(X - x_1) \ldots (X - x_d)$ dans $E[X]$. Quitte à remplacer E par sa sous-extension engendrée par les x_i, on peut supposer que $E = K[x_1, \ldots, x_d]$.

Une telle extension, dans laquelle P est scindé et qui est engendrée par les racines de P, est appelée extension de décomposition du polynôme P.

Pour toute extension F de K dans laquelle P est scindé, on construit maintenant, par récurrence descendante sur le nombre de racines de P dans K, un homomorphisme d'extensions de E dans F. Si P est scindé dans K, on a $E = K$ et il n'y a rien à démontrer. Soit sinon Q un facteur irréductible de P dans $K[X]$ dont le degré est supérieur ou égal à 2 et soit x une racine de Q dans E. Alors, $K[x]$ est une extension de rupture du polynôme Q. Choisissons arbitrairement une racine y de Q dans F ; il en existe puisque Q divise P est que P est scindé dans F. Il existe alors un homomorphisme d'extensions f_1 de $K[x]$ dans F qui applique x sur y. Comme P a au moins une racine de plus dans $K[x]$ qu'il n'en avait dans K, on en conclut par récurrence que l'on peut prolonger l'homomorphisme f_1 en un homomorphisme d'extensions de E dans F.

Les racines de P dans F sont les images $f(x_1), \ldots, f(x_d)$ par f des racines de P dans E. Par conséquent, si l'on suppose de plus que F est une extension de décomposition de P, F est engendrée par ces racines $f(x_i)$ et f est surjectif ; c'est donc un isomorphisme.

Nous avons donc :

Proposition 6.8. *Soit P un polynôme à coefficients dans K et soit $K \hookrightarrow E$ une extension de décomposition de P. Soit Ω une extension de K ; Pour qu'il existe un homomorphisme d'extensions de E dans Ω, il faut et il suffit que P soit scindé dans Ω. Si, de plus, Ω est une extension de décomposition, un tel homomorphisme est un isomorphisme.*

Soit K un corps. On dit que K est algébriquement clos si tout polynôme non constant (à coefficients dans K) a une racine dans K. Rappelons que le corps $\mathbb{C}$ des nombres complexes est algébriquement clos (théorème de d'Alembert-Gauß). Une clôture algébrique de K est une extension algébrique Ω de K dans laquelle tout polynôme à coefficients dans K est scindé.

Proposition 6.9. *Soit K un corps et soit Ω une extension de K qui est un corps algébriquement clos. Soit E l'ensemble des éléments de Ω qui sont algébriques sur K ; alors E est une clôture algébrique de K.*

Démonstration : cela résulte des définitions.

Concernant l'existence et l'unicité des clôtures algébriques, on a le résultat suivant :

Théorème 6.10. *Tout corps possède une clôture algébrique. En outre, si K est un corps et si Ω_1, Ω_2 sont des clôtures algébriques de K, il existe un isomorphisme d'extensions entre Ω_1 et Ω_2.*

Nous admettrons ce résultat ; il n'est pas difficile mais sa démonstration rigoureuse requiert un peu de théorie des ensembles. Signalons notamment qu'il requiert de l'axiome du choix.

6.2 Norme, trace

Soit K un corps et soit E une K-algèbre de dimension finie. La multiplication m_a par un élément a de E définit un endomorphisme du K-espace vectoriel E, donné par $x \longmapsto ax$.

Le déterminant et la trace (dans une base arbitraire de E) de cet endomorphisme sont appelés norme et trace de a et sont notés $\mathrm{N}_{E/K}(a)$ et $\mathrm{Tr}_{E/K}(a)$. Comme l'application $a \longmapsto m_a$ envoie la somme $a + a'$ de deux éléments de E sur la somme $m_a + m_{a'}$ des endomorphismes m_a et $m_{a'}$ (distributivité de la multiplication), on a $\mathrm{Tr}_{E/K}(a + a') = \mathrm{Tr}_{E/K}(a) + \mathrm{Tr}_{E/K}(a')$.

Si a appartient à K, on a $\mathrm{Tr}_{E/K}(a) = [E : K]a$ et $\mathrm{N}_{E/K}(a) = a^{[E:K]}$.

Lemme 6.11. *Soit $K \hookrightarrow L$ une extension de corps de degré fini d et soit E une L-algèbre de dimension finie e. Alors, E est une K-algèbre de dimension $= de$. De plus, pour tout élément $a \in E$, on a les relations*

$$\mathrm{Tr}_{E/K}(a) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{E/L}(a)) \qquad et \qquad \mathrm{N}_{E/K}(a) = \mathrm{N}_{L/K}(\mathrm{N}_{E/L}(a)) \ .$$

Démonstration : soit $(x_1, \ldots, x_d)$ une base de L sur K et soit $(y_1, \ldots, y_e)$ une base de E sur L. Alors, la famille $(x_i y_j)_{i,j}$ est une base de E sur K.

Soit a un élément de E et soit $A = (a_{i,j})$ la matrice dans la base fixée $(y_1, \ldots, y_e)$ de la multiplication par a dans le L-espace vectoriel E. La matrice dans la base $(x_i y_j)$ de la multiplication par a du K-espace vectoriel E s'écrit par blocs $d \times d$, le bloc $A_{i,j}$ étant la matrice de la multiplication par $a_{i,j}$ dans la base $(x_1, \ldots, x_d)$.

On a donc déjà

$$\begin{aligned}
\mathrm{Tr}_{E/K}(a) &= \sum_{i=1}^{e} \mathrm{Tr}(A_{i,i}) \\
&= \sum_{i=1}^{e} \mathrm{Tr}_{L/K}(a_{i,i}) \\
&= \mathrm{Tr}_{L/K}\left(\sum_{i=1}^{e} a_{i,i}\right) \\
&= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{E/L}(a)) \ .
\end{aligned}$$

D'autre part, comme les matrices $A_{i,j}$ commutent deux à deux, le déterminant de la matrice par blocs $(A_{i,j})$ se calcule par la formule (lemme 6.12 ci-dessous) :

$$\det\left((A_{i,j})\right) = \det\left(\sum_{\sigma \in \mathfrak{S}_e} \varepsilon(\sigma) \prod_{i=1}^{e} A_{i,\sigma(i)}\right) \ .$$

La matrice dont on prend le le déterminant dans le second membre est celle de la multiplication par $\mathrm{N}_{E/L}(a)$; le second membre est donc égal à $\mathrm{N}_{L/K}(\mathrm{N}_{E/L}(a))$. Par suite, $\mathrm{N}_{E/K}(a) = \det((A_{i,j})) = \mathrm{N}_{L/K}(\mathrm{N}_{E/L}(a))$ comme annoncé.

Il reste à démontrer le lemme :

Lemme 6.12. *Soit K un corps ; soit $(A_{i,j})_{1\leq i,j\leq e}$ une famille de matrices de taille $d\times d$, à coefficients dans K, commutant deux à deux ; et soit A la matrice par blocs $(A_{i,j})$, de taille de $\times$ de . Alors, le déterminant de A est égal au déterminant de la matrice*

$$\sum_{\sigma\in\mathfrak{S}_e}\varepsilon(\sigma)\prod_{i=1}^{e}A_{i,\sigma(i)}\ .$$

Démonstration : se fait en revenant à la définition du déterminant.

soit K un corps, soit $K\hookrightarrow L$ une extension finie et soit a un élément de L. Nous allons calculer norme et trace de a en fonction du polynôme minimal de a et de ses racines dans une extension algébriquement close de K.

Proposition 6.13. *Soit K un corps, soit $K\hookrightarrow L$ une extension finie. Soit a un élément de L et soit $P\in K[X]$ son polynôme minimal, noté $P=X^d+p_1X^{d-1}+\cdots+p_d$; soit e l'entier tel que $de=[L:K]$. Alors,*

$$\mathrm{Tr}_{L/K}(a)=-ep_1\ ,\qquad \mathrm{N}_{L/K}=\prod_{j=1}^{d}a_j^e\ .$$

En outre, soit Ω une extension algébriquement close de K et notons $a_1,\dots,a_d$ les racines de P dans Ω. On a alors

$$\mathrm{Tr}_{L/K}(a)=e\sum_{j=1}^{d}a_j\ ,\qquad \mathrm{N}_{L/K}=\prod_{j=1}^{d}a_j^e\ .$$

Démonstration : on a l'égalité $[K(a):K]=d$ et $(1,x,\dots,x^{d-1})$ est une base de $K(a)$ sur K. Dans cette base, la matrice de la multiplication par a est la matrice compagnon C_P du polynôme P :

$$C_P=\begin{pmatrix}0&\cdots&\cdots&0&-p_d\\1&\ddots&&\vdots&-p_{d-1}\\0&\ddots&\ddots&\vdots&\vdots\\\vdots&\ddots&\ddots&0&-p_2\\0&\cdots&0&1&-p_1\end{pmatrix}$$

dont la trace vaut $-p_1$ et le déterminant $(-1)^dp_d$. On a aussi $[L:K(a)]=[L:K]/[K(a):K]=e$; soit $(x_1,\dots,x_e)$ une base de L sur $K(a)$. Dans la base (x^ix_j) de L sur K, la matrice A de la multiplication par a est diagonale par blocs, chaque bloc étant égal à C_P. On a alors $\det(A)=(\det C_P)^e=\big((-1)^dp_d\big)^e$ et $\mathrm{Tr}(A)=e\mathrm{Tr}(A)=-ep_1$.

La dernière formule résulte alors des relations coefficients-racines, elles-mêmes conséquences de l'identification des coefficients dans l'égalité

$$P(X)=(X-a_1)\dots(X-a_d)=X^d+p_1X^{d-1}+\cdots+p_d\ .$$

6.3 Résultant, discriminant

Soit K un corps ; on désigne par $K[X]_{<n}$ l'espace vectoriel des polynômes de degrés $<n$. Soient A,B des polynômes à coefficients dans K de degrés $\leq n,m$ respectivement ; notons-les $A=a_0+a_1X+\cdots+a_nX^n$ et $B=b_0+b_1X+\cdots+b_mX^m$.

On appelle résultant (en degrés (n,m)) des polynômes A et B, et on note $\mathrm{Res}_{n,m}(A,B)$, le déterminant de l'application linéaire de $K[X]_{<m} \times K[X]_{<n}$ dans $K[X]_{<m+n}$ donnée par $(U,V) \longmapsto UA+VB$, pris dans les bases évidentes $(X^{m-1},\dots,X,1;X^{n-1},\dots,X,1)$ et $(X^{m+n-1},\dots,X,1)$. Dans ces bases, la matrice de cette application linéaire (appelée application résultante) est la transposée de la matrice de Sylvester :

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_m & b_{m-1} & \cdots & b_0 \end{pmatrix} ,$$

où il y a m lignes de a_i et n lignes de b_j. Si l'on échange les rôles de A et B, la matrice de Sylvester subit une permutation des lignes : il suffit de remonter successivement chaque ligne de b_j de n positions. On a ainsi la relation :

$$\mathrm{Res}_{n,m}(A,B) = (-1)^{nm}\mathrm{Res}_{m,n}(B,A) \ . \tag{6.2}$$

Proposition 6.14. *Si* $\deg(A) < n$ *et* $\deg(B) < m$, *alors* $\mathrm{Res}_{n,m}(A,B) = 0$. *Supposons que l'on a* $\deg(A) = n$ *ou* $\deg(B) = m$ *; alors* $\mathrm{Res}_{n,m}(A,B) = 0$ *si et seulement si* A *et* B *ont un facteur commun.*

Démonstration : soit D le PGCD de A et B et notons $A = DA_1$ et $B = DB_1$. Si U et V sont des polynômes, la relation $UB+VA = 0$ équivaut aux relations $U = WB_1$, $V = -WA_1$, où $W \in K[X]$.

Si $\deg(A_1) < n$ et $\deg(B_1) < m$, le couple (B_1, A_1) est un élément non nul du noyau de l'application résultante, par suite, $\mathrm{Res}_{n,m}(A,B) = 0$. En particulier, $\mathrm{Res}_{n,m}(A,B)$ s'annule lorsque A et B ont un facteur commun, ou lorsque $\deg(A) < n$ et $\deg(B) < m$. Si $D = 1$ et que l'on a $\deg(A) = n$, alors tout couple (U,V) appartenant au noyau de l'application résultante vérifie $\deg(V) \geq n$ ou $V = 0$; cette application est donc injective, d'où $\mathrm{Res}_{n,m}(A,B) \neq 0$. On raisonne de même lorsque $D = 1$ et $\deg(B) = m$.

Donnons maintenant une formule pour le résultant en fonction des racines de A et B dans une extension de K.

Proposition 6.15. *Soit* Ω *une extension de* K *dans laquelle on a*

$$A(X) = a_n \prod_{i=1}^{n}(X - x_i) \ , \qquad B(X) = b_m \prod_{j=1}^{m}(X - y_j) \ ,$$

Alors,

$$\mathrm{Res}_{n,m}(A,B) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j) = a_n^m \prod_{i=1}^{n} B(x_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} A(y_j) \ .$$

Démonstration : notons S la matrice de Sylvester introduite ci-dessus et V la matrice de Vander-

monde

$$V = \begin{pmatrix} y_1^{n+m-1} & \cdots & y_m^{m+n-1} & x_1^{n+m-1} & \cdots & x_1^{m+n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ y_1^2 & \cdots & y_m^2 & x_1^2 & \cdots & x_n^2 \\ y_1 & \cdots & y_m & x_1 & \cdots & x_n \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix} .$$

Calculons le produit SV ; on a :

$$SV = \begin{pmatrix} y_1^{m-1}A(y_1) & \cdots & y_m^{m-1}A(y_m) & & & \\ \vdots & \vdots & \vdots & & 0 & \\ y_1A(y_1) & \cdots & y_mA(y_m) & & & \\ A(y_1) & \cdots & A(y_m) & & & \\ & & & x_1^{n-1}B(x_1) & \cdots & x_n^{n-1}B(x_n) \\ & 0 & & \vdots & \vdots & \vdots \\ & & & B(x_1) & \cdots & B(x_n) \end{pmatrix} .$$

Les colonnes sont multiples de $A(y_1), \ldots, A(y_m), B(x_1), \ldots, B(x_n)$. Par suite, en appliquant la formule classique pour le déterminant de Vandermonde, il vient

$$\det(S)\det(V) = \prod_{j=1}^{m} A(y_j) \prod_{i=1}^{n} B(x_i) \prod_{j'<j} (y_{j'} - y_j) \prod_{i'<i} (x_{i'} - x_i) \ .$$

Par ailleurs,

$$\det(V) = \prod_{j'<j} (y_{j'} - y_j) \prod_{i'<i} (x_{i'} - x_i) \prod_{i,j} (x_i - y_j) \ .$$

En outre, pour tout $i \in \{1, \ldots, n\}$ et pour tout $j \in \{1, \ldots, m\}$, on a

$$B(x_i) = b_m \prod_{j=1}^{m} (x_i - y_j) \ , \quad \text{et} \quad A(y_j) = a_n \prod_{i=1}^{n} (y_j - x_i) = (-1)^n a_n \prod_{i=1}^{n} (x_i - y_j) \ .$$

Par conséquent, lorsque les x_i et y_j sont deux à deux distincts, on a les égalités

$$\mathrm{Res}_{n,m}(A, B) = \det(S) = b_m^n (-1)^{mn} \prod_{j=1}^{m} A(y_j) = a_n^m \prod_{i=1}^{n} B(x_i) \ ,$$

d'où la proposition dans ce cas. Pour démontrer que ces égalités restent vraies sans cette hypothèse, le plus simple est peut-être d'utiliser le raisonnement algébrique suivant. Plaçons-nous dans le cas où les coefficients de A et B sont des indéterminées : leur résultant apparaît comme un polynôme « universel » $R_{n,m}(a_0, \ldots, a_n; b_0, \ldots, b_m)$ en ces coefficients. Supposons maintenant que le corps de base soit celui des fractions rationnelles

$$K(a_n, x_1, \ldots, x_n, y_1, \ldots, y_m, b_m) \ ,$$

de sorte que les coefficients dominants et les racines de A et B sont des indéterminées, distinctes par hypothèse. Les coefficients de A et B s'expriment alors en fonction des polynômes symétriques élémentaires :

$$A(X)=\sum_{k=0}^{n}(-1)^{n-k}a_n\sigma_k(x_1,\ldots,x_n)X^k, B(X)=\sum_{k=0}^{m}(-1)^{m-k}a_n\sigma_k(y_1,\ldots,y_m)X^k.$$

En substituant les coefficients de A et B dans le polynôme $R_{n,m}$, on obtient l'égalité (avec les conventions $\sigma_0 = 1$, $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_m)$)

$$\begin{aligned} R_{n,m}(a_n, \sigma_0(x), \ldots, a_n\sigma_n(x); b_m\sigma_0(y), \ldots, b_m\sigma_m(y)) &= \mathrm{Res}_{n,m}(A, B) \\ &= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j) \ . \end{aligned}$$

C'est une égalité entre polynômes, égalité dans laquelle il est loisible de spécifier des valeurs pour les x_i et les y_j. Le membre de gauche fournit le résultant des deux polynômes considérés et celui de droite l'expression voulue en fonction des racines.

L'intérêt de ces formules est de permettre un calcul récursif des résultants. En effet, l'expression $\prod_{i=1}^{n} B(x_i)$ peut se calculer en remplaçant B par le reste B_1 de la division euclidienne de B par A. On obtient alors

$$\mathrm{Res}_{n,m}(A, B) = a_n^m \prod_{i=1}^{n} B(x_i) = a_n^m \prod_{i=1}^{n} B_1(x_i) = a_n^{m-m_1}\mathrm{Res}_{n,m_1}(A, B_1) \ ,$$

où m_1 désigne le degré de B_1. On peut alors échanger les rôles de A et B_1 et continuer le calcul.

Le discriminant d'un polynôme A de degré n est défini par la formule

$$\mathrm{disc}(A) = (-1)^{n(n-1)/2}\mathrm{Res}_{n,n-1}(P, P')/a_n \ ,$$

où a_n est le coefficient dominant de A. Si $A = a_n \prod_{i=1}^{n} n(X - x_i)$, on a ainsi

$$\mathrm{disc}(A) = (-1)^{n(n-1)/2}a_n^{n-2}\prod_{i=1}^{n} P'(x_i) = a_n^{2n-2}\prod_{i=1}^{n}\prod_{j<i}(x_i - x_j)^2 \ .$$

Exemple 6.16. *Soient a et b des éléments de K et soit n un entier. Calculons le discriminant du polynôme $A(X) = aX^2 + bX + c$. Si $A(X) = a(X - u)(X - v)$,*

$$\mathrm{disc}(A) = a^2(u - v)^2 = a^2(u + v)^2 - 4a^2u^2v^2 = b^2 - 4ac \ .$$

7 Nombres algébriques, entiers algébriques

7.1 Préliminaires

Définition 7.1. *On dit qu'un nombre complexe z est un nombre algébrique s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(z) = 0$. Un nombre complexe qui n'est pas algébrique est appelé transcendant. On dit qu'un nombre complexe z est un entier algébrique s'il existe un polynôme $P \in \mathbb{Z}[X]$, unitaire (donc non nul), tel que $P(z) = 0$.*

Exemple 7.2. *Les nombres complexes i, $\sqrt{2}$, $3 + i\sqrt{5}$, etc. sont des nombres algébriques, puisqu'il sont racines des polynômes $X^2 + 1$, $X^2 - 2$ et $(X-3)^2 + 5 = X^2 - 6X + 14$ respectivement. Ce sont même des entiers algébriques.*

On observera que les nombres transcendants e, π ne sont pas définis par l'algèbre ou l'arithmétique, mais par l'analyse : ce sont les valeurs de séries $e = \sum_{n=1}^{\infty} \frac{1}{n!}$ ou d'intégrales $\pi = 4 \int_0^1 \sqrt{1 - x^2} dx$.

D'autres exemples de nombres transcendants sont les valeurs de logarithmes $\log(2), \log(3)$ etc. Ils sont aussi définis à l'aide de formules analytiques.

Rappelons le résultat obtenu au chapitre précédent :

Proposition 7.3. *L'ensemble des nombres algébriques forment donc un sous-corps du corps $\mathbb{C}$ des nombres complexes que l'on note $\overline{\mathbb{Q}}$; les entiers algébriques forment un sous- anneau de $\overline{\mathbb{Q}}$ qui est noté $\overline{\mathbb{Z}}$. Plus généralement, si K est un sous-corps de $\mathbb{C}$, on note $\mathbb{Z}_K$ l'anneau des éléments de K qui sont des entiers algébriques.*

Démonstration : il suffit de vérifier que la preuve déjà donnée de la première partie s'adapte au cas entier. Soient x et y des entiers algébriques, annulés par des polynômes unitaires à coefficients entiers P et Q. Par récurrence, il existe pour tout couple (m, n) d'entiers naturels, un polynôme $P_{m,n} \in \mathbb{Z}[X, Y]$, de degré au plus $\deg(P) - 1$ en X et de degré au plus $\deg(Q) - 1$ en Y, tel que $x^m y^n = P_{m,n}(x, y)$ (il suffit de prendre pour $P_{m,n}$ le produit des restes des divisions euclidiennes du polynôme X^m par P et du polynôme Y^n par Q). Si $z = x + y$ ou $z = xy$, on en déduit ainsi l'existence d'une matrice carrée $A = (a_{(i,j),(k,l)})$ de taille $\deg(P)\deg(Q)$, à coefficients entiers, indexée par l'ensemble des couples (i, j) tels que $0 \leq i < \deg(P)$ et $0 \leq j < \deg(Q)$, telle que

$$zx^k y^l = \sum_{(i,j)} a_{(i,j),(k,l)} x^i y^j \ .$$

Le polynôme caractéristique de la matrice A est à coefficients entiers et est unitaire. D'après la proposition6.5, il annule z, donc z est un entier algébrique.

Le polynôme minimal d'un nombre algébrique z est le polynôme unitaire à coefficients rationnels de plus petit degré qui annule z (il n'y en a qu'un seul : si $P(z) = Q(z) = 0$, P et Q étant de mêmes degrés, $P - Q$ est un polynôme qui annule z et est de degré strictement inférieur ; c'est donc le polynôme nul). Son degré est appelé degré du nombre algébrique.

Le polynôme minimal d'un nombre algébrique est un polynôme irréductible de $\mathbb{Q}[X]$. Les polynômes à coefficients entiers qui annulent un nombre algébrique sont exactement les multiples de son polynôme minimal.

Lemme 7.4. *Soient P et Q des polynômes à coefficients entiers tels que Q divise P dans l'anneau $\mathbb{Q}[X]$. Si les coefficients de Q sont premiers entre eux (on dit que Q est primitif), alors Q divise P dans l'anneau $\mathbb{Z}[X]$.*

Démonstration : soit $R \in \mathbb{Q}[X]$ tel que $P = QR$. Nous devons démontrer que R appartient à $\mathbb{Z}[X]$. Soit $a \in \mathbb{N}^*$ un dénominateur commun de ses coefficients, de sorte que $aR \in \mathbb{Z}[X]$, minimal. On a ainsi $aP = QaR$. Soit p un facteur premier de a et considérons l'égalité précédente modulo p. On a ainsi $(Q \bmod p)(aR \bmod p) = 0$. Le polynôme $Q \bmod p$ n'est pas nul car les coefficients de Q sont premiers entre eux. Comme l'anneau des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre, $aR \equiv 0 \bmod p$. Les coefficients de aR sont ainsi tous multiples de p, ce qui entraîne que $(a/p)R$ est à coefficients entiers, mais contredit l'hypothèse de minimalité faite sur a. Donc a n'a pas de facteur premier, c'est-à-dire $a = 1$ et $R \in \mathbb{Z}[X]$.

Corollaire 7.5. *Soit $P \in \mathbb{Z}[X]$ un polynôme primitif qui est irréductible dans $\mathbb{Z}[X]$. Le polynôme P est irréductible dans $\mathbb{Q}[X]$.*

Démonstration : soit Q un facteur de P dans $\mathbb{Q}[X]$; nous devons prouver que $\deg Q = 0$ ou $\deg Q = \deg P$. Quitte à remplacer Q par aQ, où $a \in \mathbb{Z}$ est un dénominateur commun des coefficients

de Q, on peut supposer que $Q \in \mathbb{Z}[X]$. Quitte à le remplacer alors par Q/b, où $b \in \mathbb{Z}$ est un facteur commun de ses coefficients, on peut supposer que Q est primitif. Alors, Q divise P dans $\mathbb{Z}[X]$. Comme P est irréductible dans cet anneau, ou bien Q, ou bien P/Q est inversible dans cet anneau. En particulier, $\deg Q = 0$ ou $\deg Q = \deg P$.

Corollaire 7.6. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers. Soit $Q \in \mathbb{Q}[X]$ un polynôme unitaire qui divise P. Alors, Q appartient à $\mathbb{Z}[X]$.*

Démonstration : comme dans la preuve du corollaire précédent, introduisons des entiers a et b tels que aQ/b soit un polynôme primitif. Il est loisible de choisir a et b premiers entre eux. D'après le lemme, aQ/b divise P dans $\mathbb{Z}[X]$; soit donc $R \in \mathbb{Z}[X]$ tel que $P = (aQ/b)R$. On a donc $bP = aQR$. Comparons les coefficients dominants, on voit que b est multiple de a, donc $a = 1$ puisque a et b sont premiers entre eux. Le polynôme Q/b apaprtient en particulier à $\mathbb{Z}[X]$ et il en est a fortiori de même du polynôme Q.

Proposition 7.7. *Pour qu'un nombre algébrique soit un entier algébrique, il faut et il suffit que son polynôme minimal soit à coefficients entiers.*

Démonstration : un sens est évident : si le polynôme minimal P d'un nombre algébrique z est à coefficients entiers, la relation $P(z) = 0$ entraîne que z est un entier algébrique par définition. La réciproque est plus subtile ; soit z un entier algébrique, soit P son polynôme minimal et soit Q un polynôme unitaire à coefficients entiers tel que $Q(z) = 0$. D'après le corollaire précédent, P est à coefficients entiers.

Corollaire 7.8. *Soit z un nombre algébrique et P son polynôme minimal, noté*

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \ .$$

Soit d un entier relatif non nul ; pour que dz soit un entier algébrique, il faut et il suffit que que $d^i a_{n-i}$ soit un entier relatif, pour tout entier i tel que $1 \leq i \leq n$.

Supposons que z soit un entier algébrique non nul. Pour que $1/z$ soit un entier algébrique, il faut et il suffit que $a_0 = \pm 1$.

Démonstration : le polynôme $d^n P(X/d)$ est unitaire, irréductible de degré n ; c'est le polynôme minimal de dz. De plus, on a

$$d^n P(X/d) = X^n + da_{n-1}X^{n-1} + \cdots + d^n a_0 \ ,$$

d'où la première assertion. Si $z \neq 0$, on a $a_0 \neq 0$. Le polynôme $Q = a_0^{-1} X^n P(1/X)$ est irréductible, unitaire, de degré n, et s'annule en $1/z$. Son terme constant est a_0^{-1} ; pour que Q soit à coefficients entiers, il est nécessaire que l'on ait $a_0 = \pm 1$. Si c'est le cas, Q est à coefficients entiers, donc $1/z$ est un entier algébrique. Inversement, si $1/z$ est un entier algébrique, Q est à coefficients entiers et $a_0 = \pm 1$.

Avec les notations du corollaire, observons que si d est un dénominateur commun de $a_0, \ldots, a_{n-1}$, alors dz est un entier algébrique. De plus, l'entier d est le plus petit entier naturel non nul tel que le polynôme $dP(X)$ appartienne à $\mathbb{Z}[X]$; ses coefficients sont des entiers relatifs premiers entre eux.

Corollaire 7.9. *Soit z un nombre rationnel. Pour que z soit un entier algébrique, il faut et il suffit que ce soit un entier relatif.*

Démonstration : en effet, si $z \in \mathbb{Q}$, son polynôme minimal est $X - z$.

D'après le lemme ci-dessous, le polynôme minimal d'un nombre algébrique n'a que des racines simples dans $\mathbb{C}$; ces racines sont appelées les conjugués du nombre algébrique considéré.

Lemme 7.10. *Soit F un corps de caractéristique zéro et soit Ω une extension algébriquement close de F. Soit P un polynôme irréductible à coefficients dans F. L'ensemble des racines de P dans Ω est de cardinal* $\deg(P)$.

Démonstration : pour simplifier les notations, on suppose que P est unitaire. Il s'agit de démontrer que P n'a pas de racine multiple. Une telle racine serait une racine commune à P et P'. Posons $D = \mathrm{PGCD}(P, P')$; c'est un polynôme à coefficients dans F qui divise P et est unitaire. Comme P est irréductible a donc $D = P$ ou $D = 1$. Comme F est de caractéristique 0, P' est de degré $\deg(P) - 1$: si le terme de plus haut degré de P est aX^n (avec $a \neq 0$), on a $na \neq 0$ donc le terme de plus haut degré de P' est naX^{n-1} et P' est de degré $n - 1$. Cela empêche que P' soit multiple de P si bien que $D = 1$. Autrement dit, P et P' n'ont pas de racine commune.

Définition 7.11. *Soit z un nombre algébrique ; notons n son degré, $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ son polynôme minimal et $z_1, \ldots, z_n$ ses conjugués. Le dénominateur de z, noté* $\mathrm{den}(z)$*, est le plus petit entier $d > 1$ tel que d soit un entier algébrique. On appelle alors taille de z l'expression :*

$$\mathfrak{t}(z) = \max(\mathrm{den}(z), |z_1|, \ldots, |z_n|) \ .$$

Notons d_0 le plus petit commun dénominateur de P. On appelle hauteur de z l'expression :

$$h(z) = \frac{1}{n}\left(\log(d_0) + \sum_{i=1}^{n} \log\max(1, |z_i|)\right) \ .$$

On peut comparer la taille et la hauteur :

Lemme 7.12. *Soit z un nombre algébrique, alors,*

$$\frac{h(z)}{2} \leq \log \mathfrak{t}(z) \leq nh(z) \ .$$

Démonstration : par définition, $\mathrm{den}(z) \leq d_0 \leq \mathrm{den}(z)^n$. De même

$$\max(\mathrm{den}(z), |z_1|, \ldots, |z_n|) \leq \max(1, \mathrm{den}(z)) \prod_{1 \leq i \leq n} \max(1, |z_i|) \ ,$$

et donc

$$\log \mathfrak{t}(z) \leq \log\max(1, \mathrm{den}(z)) + \sum_{i=1}^{n} \log\max(1, |z_i|) \leq nh(z) \ .$$

Inversement,

$$\begin{aligned} nh(z) &= \log(d_0) + \sum_{i=1}^{n} \log \max(1, |z_i|) \\ &\leq n\mathrm{den}(z) + n \log \max_{1 \leq i \leq n} (1, |z_i|) \\ &\leq 2n \log \mathfrak{t}(z) \ . \end{aligned}$$

Soient $n \geq 1$ un entier et $h \geq 0$ un nombre réel. On note $B(n,h)$, l'ensemble des nombres algébriques de degré $\leq n$ et de hauteur $\leq h$.

Proposition 7.13. *Soit $h \geq 0$ un nombre réel et $n \geq 1$ un entier. L'ensemble $B(n,h)$ est fini.*

Démonstration : soit z un tel nombre algébrique, soit d_0 le plus petit commun dénominateur de son polynôme minimal et $z_1, \ldots, z_n$ ses conjugués. On a donc $d_0 \leq \exp(nh)$ et $|z_i| \leq \exp(nh)$ pour $1 \leq i \leq n$. Si a_k est le coefficient de degré $n-k$ du polynôme minimal P de z, $(-1)^k a_k$ est la k-ième fonction symétrique élémentaire des z_i ; par suite,

$$|a_k| \leq \sum_{i_1 < \cdots < i_k} |z_{i_1}| \cdots |z_{i_k}| \leq \left(\begin{array}{c} n \\ k \end{array} \right) \exp(nkh) \ .$$

Ces inégalités montrent que les coefficients du polynôme minimal de z sont des nombres rationnels de dénominateur et valeur absolue bornés indépendemment de z ; ils sont donc en nombre fini. Il n'y a donc qu'un nombre fini polynômes qui peuvent être le polynôme minimal d'un élément de $B(n,h)$. Comme chacun d'eux n'a qu'un nombre fini de racines ($\leq n$), il n'y a au total qu'un nombre fini de nombres algébriques possibles.

7.2 Corps quadratiques

Le début de ce paragraphe est consacré à déterminer les entiers algébriques d'un corps quadratique, c'est-à-dire un sous-corps de $\mathbb{C}$ qui est une extension de degré 2 du corps $\mathbb{Q}$.

Proposition 7.14. *Soit K un corps quadratique. Il existe un unique entier relatif d sans facteurs carrés tel que $K = \mathbb{Q}(\sqrt{d})$.*

Tout élément z de K s'écrit de manière unique sous la forme $a + b\sqrt{d}$, avec $a, b \in \mathbb{Q}$. S'il n'appartient pas à $\mathbb{Q}$, le polynôme minimal d'un tel élément est $X^2 - 2aX + a^2 - db^2$.

Démonstration : soit z un élément de $K \backslash \mathbb{Q}$. Comme $\mathbb{Q} \subsetneq \mathbb{Q}(z) \subset K$, on a $[\mathbb{Q}(z) : \mathbb{Q}] \geq 2 = [K : \mathbb{Q}]$, d'où $K = \mathbb{Q}(z)$. En particulier, z est degré 2 sur $\mathbb{Q}$ et son polynôme minimal est de la forme $X^2 + aX + b$, avec $a, b \in \mathbb{Q}$. Alors, $(z + \frac{a}{2})^2 = -b + \frac{a^2}{4}$. Posons $D = -b + \frac{a^2}{4}$; c'est un nombre rationnel. Il n'est pas nul car sinon, on aurait $z = -\frac{a}{2}$, d'où $z \in \mathbb{Q}$. Notons $D = \varepsilon \prod_{i=1}^{k} p_i^{n_i}$ sa décomposition en facteurs premiers, avec $\varepsilon \in \{\pm 1\}$ et $n_i \in \mathbb{Z}^\star$. Posons $m_i = 1$ si n_i est impair et $m_i = 0$ sinon et posons alors $d = \varepsilon \prod_{i=1}^{k} p_i^{m_i}$. Le nombre d est par construction sans facteur carré ; de plus, $D/d = \prod_{i=1}^{k} p_i^{n_i - m_i} = \left(\prod_{i=1}^{k} p_i^{(n_i - m_i)/2} \right)^2$ est un carré, disons $D = dr^2$ avec $d \in \mathbb{Z}^\star, r \in \mathbb{Q}$.

Vérifions que $K = \mathbb{Q}(\sqrt{d})$. Tout d'abord, $(z + \frac{a}{2})^2 = dr^2 = (\sqrt{d}r)^2$. Par suite, $\sqrt{d} = \pm(z + \frac{a}{2})/r$ appartient à K ; en outre, $\sqrt{d} \notin \mathbb{Q}$ car sinon cela entraînerait $z = -\frac{a}{2} \pm r\sqrt{d} \in \mathbb{Q}$. Reprenant l'argument initial, on voit que $K = \mathbb{Q}(\sqrt{d})$.

Alors, $(1, \sqrt{d})$ est une famille de K libre sur $\mathbb{Q}$, donc une base de K car $[K : \mathbb{Q}] = 2$. Tout élément z de K s'écrit donc de façon unique $a + b\sqrt{d}$,avec $a, b \in \mathbb{Q}$. Si $z \in \mathbb{Q}$, on a $b \neq 0$, et réciproquement. Supposons $z \notin \mathbb{Q}$. Alors, $(z - a)^2 = b^2 d$, si bien que z est racine du polynôme $X^2 - 2aX + a^2 - db^2$. L'autre racine de ce polynôme est $a - b\sqrt{d}$. Par suite, ce polynôme n'a pas de racine dans $\mathbb{Q}$; comme il est de degré 2, il est irréductible et c'est le polynôme minimal de z. Démontrons finalement l'unicité d'un tel entier d : supposons $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$, d et d' étant des entiers relatifs sans facteurs carrés. On peut donc écrire $\sqrt{d'} = a + b\sqrt{d}$, avec $a, b \in \mathbb{Q}$ et $d' = (a^2 + b^2 d) + 2ab\sqrt{d} = (a^2 + b^2 d) + 2ab\sqrt{d}$. Par suite, $2ab = 0$ et $a^2 + b^2 d = d'$. Comme $\sqrt{d'} \notin \mathbb{Q}$, on a $b \neq 0$, d'où $a = 0$ et $d' = b^2 d$. D'après le lemme ci-dessous, b est un entier relatif. On peut écrire de même $d = (1/b)^2 d'$ donc $1/b$ est aussi un entier relatif. On a donc $b = \pm 1$, $b^2 = 1$ et $d = d'$.

Lemme 7.15. *Soit d un entier relatif non nul sans facteur carré. Si x est un nombre rationnel tel que $dx^2 \in \mathbb{Z}$, c'est un entier relatif.*

Démonstration : posons $n = dx^2$ et écrivons $x = p/q$, où p et q sont des entiers relatifs premiers entre eux ; il vient $p^2 d = q^2 n$, si bien que q^2 divise $p^2 d$ en étant premier avec p^2. Par suite, q^2 divise d. Comme d est sans facteur carré, $q^2 = 1$ et $x \in \mathbb{Z}$.

Corollaire 7.16. *Soit d un entier relatif sans facteur carré. Pour qu'un élément $z = a + b\sqrt{d}$ de $\mathbb{Q}(\sqrt{d})$ soit un entier algébrique, il faut et il suffit que l'on ait :*

(i) $a, b \in \mathbb{Z}$ si $d \not\equiv 1 \bmod 4$;

(ii) $2a, 2b \in \mathbb{Z}$, et $a - b \in \mathbb{Z}$ si $d \equiv 1 \bmod 4$.

Démonstration : on doit déterminer les couples (a, b) de nombres rationnels tels que $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$.

La première condition entraîne $a \in \mathbb{Z}$ ou $a + \frac{1}{2} \in \mathbb{Z}$. Plaçons-nous dans le premier cas. Alors, la seconde condition montre que db^2 est un entier, donc b est un entier d'après le lemme ci-dessus. Inversement, si $(a, b) \in \mathbb{Z}^2$, $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$ ce qui démontre que $a + b\sqrt{d}$ est un entier algébrique.

Plaçons-nous maintenant dans le second cas et posons $n = a^2 - db^2$. Alors, $4n = (2a)^2 - d(2b)^2$ ce qui entraîne que $d(2b)^2$ est un entier. Par suite, $2b$ est un entier. Posons $A = 2a$ et $B = 2b$; A est impair et $dB^2 = 4n - A^2$ est impair ; par suite, d et B sont impairs. D'après la première partie de la démonstration, $\frac{A-1}{2} + \frac{B-1}{2}\sqrt{d}$ est un entier algébrique, donc $z - \frac{A-1}{2} - \frac{B-1}{2}\sqrt{d} = \frac{1+\sqrt{d}}{2}$ aussi. Le polynôme minimal de $(1 + \sqrt{d})/2$ est $X^2 - X + \frac{1-d}{4}$. Par suite, comme il est à coefficients entiers, $d \equiv 1 \bmod 4$. Cela démontre que si $d \not\equiv 1 \bmod 4$, ce cas ne se produit pas et les éléments de K qui sont des entiers algébriques sont les $a + b\sqrt{d}$ avec $(a, b) \in \mathbb{Z}^2$.

Supposons maintenant que $d \equiv 1 \bmod 4$. Alors, $(1 + \sqrt{d})/2$ est un entier algébrique, et ce qui précède démontre que les entiers algébriques sont les éléments de K de la forme $a + b\sqrt{d}$, avec $(a, b) \in Z^2$ ou de la forme $\frac{A}{2} + \frac{B}{2}\sqrt{d}$, où A, B sont des entiers relatifs de même parité. Posant $a = A/2$ et $b = B/2$, cela signifie $2a, 2b, a - b \in \mathbb{Z}$.

Remarque 7.17. *Soit d un entier relatif sans facteur carré. Posons $K = \mathbb{Q}(\sqrt{d})$ soit $\mathbb{Z}_K$ l'ensemble des entiers algébriques de K. Le sous-anneau $\mathbb{Z}[\sqrt{d}]$ engendré par $\sqrt{d}$ dans K est contenu dans $\mathbb{Z}_K$;*

il est égal à $\mathbb{Z} \oplus \sqrt{d}\mathbb{Z}$. *Dans le cas où* $d \not\equiv 1 \bmod 4$, *il résulte de la proposition précédente que* $\mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$.

Dans le cas où $d \equiv 1 \bmod 4$, $(1+\sqrt{d})/2$ *est un élément de* $\mathbb{Z}_K$ *qui n'appartient pas à* $\mathbb{Z}[\sqrt{d}]$. *Plus généralement, soit* $z = a + b\sqrt{d}$ *un élément de* $\mathbb{Z}_K$. *On peut écrire* $z = (a-b) + 2b(1+\sqrt{d})/2$. *Les conditions* $2a, 2b, a-b \in \mathbb{Z}$ *équivalent à* $(a-b) \in \mathbb{Z}$ *et* $2b \in \mathbb{Z}$. *Par conséquent,* $\mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}(1+\sqrt{d})/2$.

Dans les deux cas, l'anneau $\mathbb{Z}_K$ *est un groupe abélien libre de rang 2. C'est un cas particulier d'un résultat important que nous démontrerons plus tard.*

7.3 Corps de nombres

Rappelons qu'on appelle corps de nombres un sous-corps de $\mathbb{C}$ qui est une extension finie de $\mathbb{Q}$ (autrement dit, un $\mathbb{Q}$-espace vectoriel de dimension finie). Tout élément d'un corps de nombres est un nombre algébrique.

Proposition 7.18. *Soit* K *un corps de nombres et soit* d *son degré. L'ensemble des homomorphismes de corps de* K *dans* $\mathbb{C}$ *est de cardinal* d. *Plus généralement, soient* K *et* L *deux corps de nombres tels que* $L \subset K$. *Soit* $\varphi : L \subset \mathbb{C}$ *un homomorphisme de corps. L'ensemble des homomorphismes de corps* ψ *de* K *dans* $\mathbb{C}$ *tels que* $\psi_{|L} = \varphi$ *est de cardinal* $[K : L]$.

Démonstration : la première assertion est un cas particulier de la seconde, appliquée avec $L = \mathbb{Q}$ et φ l'inclusion de $\mathbb{Q}$ dans $\mathbb{C}$ qui est, du reste, l'unique homomorphisme de corps de $\mathbb{Q}$ dans $\mathbb{C}$. On va démontrer la seconde par récurrence sur $[K : L]$. Elle est évidente si $[K : L] = 1$; supposons-la démontrée pour toute inclusion de corps de nombres de degré strictement inférieur à $[K : L]$.

Soit α un élément de K qui n'appartient pas à L. On dispose alors d'une extension intermédiaire $L(\alpha)$, $L \subset L(\alpha) \subset K$. La restriction à $L(\alpha)$ d'un homomorphisme de corps ψ de K dans $\mathbb{C}$ tel que $\psi_{|L} = \varphi$ est un homomorphisme de corps ψ' de $L(\alpha)$ dans $\mathbb{C}$ dont la restriction à L est φ. Commençons par déterminer ces homomorphismes ψ'.

Soit P le polynôme minimal de α sur L, de sorte que $L(\alpha) \simeq L[X]/(P)$. Un homomorphisme de corps $\psi' : L(\alpha) \longrightarrow \mathbb{C}$ tel que $\psi'_{|L} = \varphi$ est induit, par passage au quotient, d'un homomorphisme de $L[X]$ dans $\mathbb{C}$ de la forme $a_0 + a_1X + \cdots \longmapsto \varphi(a_0) + \varphi(a_1)z + \cdots$. Que cet homomorphisme passe au quotient signifie exactement que z est racine du polynôme $\varphi(P)$ obtenu en apppliquant φ aux coefficients de P.

Le polynôme P est irréductible dans $L[X]$; le polynôme $\varphi(P)$ est donc irréductible dans $\varphi(L)[X]$. Comme $\varphi(L)$ est de caractéristique zéro, le polynôme $\varphi(P)$ a exactement $\deg(P)$ racines (lemme 7.10). Par conséquent, l'ensemble des homomorphismes ψ' convenables est de cardinal $\deg(P)$. Par l'hypothèse de récurrence, appliquée à l'extension $L(\alpha) \subset L$ et aux homomorphismes $\psi' : L(\alpha) \longrightarrow \mathbb{C}$, il existe pour chacun d'entre eux exactement $[K : L(\alpha)]$ prolongements à K , d'où au total $[K : L(\alpha)] \deg(P) = [K : L]$ homomorphismes de K dans $\mathbb{C}$ dont la restriction à L est l'homomorphisme φ. Cela conclut la démonstration de la proposition.

Soit K un corps de nombres, soit d son degré. Soit Φ l'ensemble des homomorphismes de corps de K dans $\mathbb{C}$; on dira aussi plongements de K dans $\mathbb{C}$. Parmi les éléments de Φ, certains sont à valeurs dans $\mathbb{R}$, on les appelle plongement réels. Les autres prennent des valeurs complexes et on les appelle plongements complexes. Si $\varphi : K \hookrightarrow \mathbb{C}$ est un plongement, $z \longmapsto \overline{\varphi(z)}$ est encore un plongement de K dans $\mathbb{C}$, noté $\overline{\varphi}$, le plongement conjugué de φ. Dire que φ est réel signifie

que $\varphi = \overline{\varphi}$. Ainsi, les plongements complexes se regroupent par paires formées d'un plongement complexe et du plongement complexe conjugué.

Conformément à la tradition, on note r_1 le nombre de plongements réels de K et $2r_2$ le nombre de plongements complexes. Ainsi, $r_1 + 2r_2 = n$ et l'on peut numéroter les plongements de K par

$$(\varphi_1, \ldots, \varphi_{r_1}, \varphi_{r_1+1}, \overline{\varphi_{r_1+1}}, \ldots, \varphi_{r_1+r_2}, \overline{\varphi_{r_1+r_2}}) \ .$$

Exemple 7.19. *Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique ; si $d > 0$ les deux plongements $a + b\sqrt{d} \longmapsto a \pm b\sqrt{d}$ sont réels et ils sont tous les deux complexes conjuqués si $d < 0$. Dans le premier cas, $n = 2 = r_1$ et dans le deuxième $r_2 = 1 = n/2$.*

Proposition 7.20. *Soit K un corps de nombres de degré n, soient $\varphi_1, \ldots, \varphi_n$ les plongements de K dans $\mathbb{C}$. Soit de plus α un élément de K, et d son degré et soit enfin $P \in \mathbb{Q}[X]$ son polynôme minimal. Alors, on a*

$$\prod_{i=1}^{n}(X - \varphi_i(\alpha)) = P(X)^{n/d} \ .$$

Démonstration : les éléments $\varphi_i(\alpha) \in \mathbb{C}$ sont des racines de P ; ils sont donc en nombre au plus d. Inversement, chaque racine β de P fournit un plongement de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$ en posant $\alpha \longmapsto \beta$. Chacun de ces plongements se prolonge en exactement n/d plongements de K dans $\mathbb{C}$, fournissant ainsi les n homomorphismes de K dans $\mathbb{C}$. Par suite, dans la suite $(\varphi_i(\alpha))_{1 \leq i \leq n}$, chaque racine de P apparaît exactement n/d fois. Si $\alpha_1, \ldots, \alpha_d$ désignent les racines de P, on a donc

$$\prod_{i=1}^{n}(X - \varphi_i(\alpha)) = \prod_{i=1}^{d}(X - \alpha_i)^{n/d} = P(X)^{n/d} \ .$$

Corollaire 7.21. *Soit K un corps de nombres de degré n et soit $\varphi_1, \ldots, \varphi_n$ les plongements de K dans $\mathbb{C}$. Soit α un élément de K tel que $\varphi_i(\alpha) \neq \varphi_1(\alpha)$ si $i \neq 1$. Alors, $K = \mathbb{Q}(\alpha)$.*

Démonstration : d'après la proposition précédente, l'ensemble des entiers $i \in \{1, \ldots, n\}$ tels que $\varphi_i(\alpha) = \varphi_1(\alpha)$ est de cardinal n/d, où d est le degré de α. Par hypothèse, cet ensemble est de cardinal 1 ; on a donc $n = d$.

Corollaire 7.22. (Théorème de l'élément primitif) *Soit K un corps de nombres. Il existe un élément $\alpha \in K$ tel que $K = \mathbb{Q}(\alpha)$.*

Démonstration : avec les notations du corollaire précédent, il suffit de démontrer qu'il existe un élément $\alpha \in K$ tel que $\varphi_i(\alpha) \neq \varphi_1(\alpha)$ si $i \neq 1$. Soit $i \in \{2, \ldots, n\}$; l'ensemble des $\alpha \in K$ tels que $\varphi_i(\alpha) = \varphi_1(\alpha)$ est un sous-Q-espace vectoriel V_i de K. Il est distinct de K car $\varphi_i \neq \varphi_1$. D'après le lemme ci-dessous, leur réunion $V_2, \ldots, V_n$ est distincte de K, d'où le corollaire.

Lemme 7.23. *Soit F un corps infini, soit V un F-espace vectoriel et soit $V_1, \ldots, V_n$ des sous-espaces vectoriels de V distincts de V. Alors $V_1 \cup \cdots \cup V_n$ est distinct de V.*

Démonstration : elle est laissée en exercice.

7.4 Normes, traces et discriminants

Définition 7.24. *Soit K un corps de nombres, et $w \in K$. On appelle trace de w et norme de w, la trace et le déterminant respectivement de l'endomorphisme $\mathbb{Q}$-linéaire de K donné par la multiplication par w. On les note $\mathrm{Tr}_K(w)$ et $\mathrm{N}_K(w)$. Ce sont des nombres rationnels.*

Pour tout $w \in K$, notons m_w l'endomorphisme de multiplication par w dans K. On a $m_{w+w'} = m_w + m_{w'}$. Par suite,

$$\mathrm{Tr}_K(w + w') = \mathrm{Tr}_K(w) + \mathrm{Tr}_K(w')$$

De même, on a $m_{ww'} = m_w \circ m_{w'}$ si bien que

$$\mathrm{N}_K(ww') = \mathrm{N}_K(w)\mathrm{N}_K(w') \ .$$

Si $a \in \mathbb{Q}$, on a $m_{aw} = am_w$, d'où $\mathrm{Tr}_K(aw) = a\mathrm{Tr}_K(w)$ et $\mathrm{N}_K(aw) = a^n\mathrm{N}_K(w)$ (n est le degré de K).

Proposition 7.25. *Soit K un corps de nombres de degré n soient $\varphi_1, \ldots, \varphi_n$ les n plongements de K dans $\mathbb{C}$. On a alors, pour tout $w \in K$, si l'on note W la matrice de m_w, cette dernière est semblable (sur $\mathbb{C}$) à la matrice diagonale* $\mathrm{diag}(\varphi_1(w), \ldots, \varphi_n(w))$. *En particulier, on a les égalités*

$$\mathrm{Tr}_K(w) = \sum_{i=1}^{n} \varphi_i(w) \ , \qquad \textit{et} \qquad \mathrm{N}_K(w) = \prod_{i=1}^{n} \varphi_i(w) \ .$$

Démonstration : soit α un élément primitif de K ; le polynôme minimal de α est donc $\prod_{i=1}^{n}(X - \varphi_i(\alpha))$; il est à racines simples et la matrice A de la multiplication par α (dans une base arbitraire mais fixée) est diagonalisable (sur $\mathbb{C}$), ses valeurs propres étant les $\varphi_i(\alpha)$. Autrement dit, la matrice A est semblable sur $\mathbb{C}$ à la matrice diagonale $D = \mathrm{diag}(\varphi_1(\alpha), \ldots, \varphi_n(\alpha))$.

Le cas d'un élément arbitraire de K s'en déduit facilement : si $w \in K$, il existe un polynôme $P \in \mathbb{Q}[X]$ tel que $w = P(\alpha)$. Alors, la matrice W de la multiplication par w dans la base fixée de K est égale à $P(A)$. Le changement de base qui diagonalise A la transforme en la matrice $P(D)$ qui est diagonale, de coefficients $P(\varphi_i(\alpha)) = \varphi_i(P(\alpha)) = \varphi_i(w)$, pour $1 \leq i \leq n$.

Corollaire 7.26. *Si w est un entier algébrique de K, alors $\mathrm{Tr}_K(w)$ et $\mathrm{N}_K(w)$ sont des entiers relatifs.*

Démonstration : notons $P = X^d + a_1X^{d-1} + \cdots + a_d$ le polynôme minimal de w. Alors, $\mathrm{Tr}_K(w) = -(n/d)a_1$ et $\mathrm{N}_K(w) = a^{n/d}$. Comme d divise n, ce sont des entiers.

Définition 7.27. *Soit K un corps de nombres de degré n, et soit $B = (z_1, \ldots, z_n)$ une base de K. On définit le discriminant de B par la formule* $\mathrm{disc}(B) = \det((\varphi_i(z_j))_{i,j})^2$.

Remarque 7.28. *Lorsqu'on change l'ordre des φ_i, le déterminant* $\det(\varphi_i(z_j))$ *est multiplié par ± 1 ; le discriminant de B est donc bien défini.*

Exemple 7.29. *Soit α un élément primitif de K et soit B la base naturelle $(1, \alpha, \ldots, \alpha^{n-1})$. On a donc*

$$\mathrm{disc}(B) = \det(\varphi_i(\alpha^{j-1}))^2 = \det(\varphi_i(\alpha)^{j-1})^2 = V(\varphi_1(\alpha), \ldots, \varphi_n(\alpha))^2 \ ,$$

où $V(\ldots)$ désigne le déterminant de Vandermonde. Par conséquent,

$$\mathrm{disc}(B) = \prod_{j>i} (\varphi_j(\alpha) - \varphi_i(\alpha))^2 \ .$$

Ainsi, $\mathrm{disc}(B)$ *est égal au discriminant du polynôme minimal de α. Il n'est pas nul.*

Proposition 7.30. *Soit K un corps de nombres, n son degré. Soit $z_1, \ldots, z_n$ des éléments de K et soit D la matrice* $(\mathrm{Tr}_K(z_iz_j))$. *Alors,*

$$\det(D) = \det(\varphi_i(z_j))^2$$

En particulier, le discriminant d'une base de K est un élément non nul de $\mathbb{Q}$.

Démonstration : notons $\varphi_1, \ldots, \varphi_n$ les plongements de K dans $\mathbb{C}$. D'après la proposition précédente, on a

$$\mathrm{Tr}_K(z_iz_k) = \sum_{j=1}^{n} \varphi_j(z_iz_k) = \sum_{j=1}^{n} \varphi_j(z_i)\varphi_j(z_k) \ .$$

Par conséquent, la matrice D est égale à ${}^tAA$, où A est la matrice $(\varphi_i(z_j))$. En particulier, $\det(D) = \det(A)^2$.

Supposons par l'absurde que $(z_1, \ldots, z_n)$ soit une base de K de discriminant nul. Alors, la matrice $(\varphi_i(z_j))$ n'est pas inversible ; il existe donc des nombres complexes $(c_1, \ldots, c_n)$ tels que $\sum_{i=1}^n c_i\varphi_i(z_j) = 0$ pour tout entier j tel que $1 \leq j \leq n$. L'application $\sum_i c_i\varphi_i$ de K dans $\mathbb{C}$ étant $\mathbb{Q}$-linéaire et nulle en tout élément d'une base de K, elle est identiquement nulle. Or, $\varphi_1, \ldots, \varphi_n$ sont n homomorphismes distincts dans $\mathbb{C}$ et, à ce titre, sont linéairement indépendants sur $\mathbb{C}$

Corollaire 7.31. *Soit K un corps de nombres de degré n et soit B, B' des bases de K. Alors,*

$$\mathrm{disc}(B') = \det_B(B')^2 \mathrm{disc}(B) \ .$$

Démonstration : posons $B = (z_1, \ldots, z_n)$, $B' = (z'_1, \ldots, z'_n)$ et soit P la matrice de passage de la base B à la base B' de sorte que $z'_j = \sum_{k=1}^n p_{k,j}\varphi(z_k)$ pour tout entier $j \in \{1, \ldots, n\}$. Soient A et A' les matrices $(\varphi_i(z_j))$ et $(\varphi_i(z'_j))$. Les égalités $\varphi_i(z_j) = \sum_{k=1}^n p_{k,j}\varphi_i(z_k)$ entraînent $A' = PA$, d'où

$$\mathrm{disc}(B') = \det(A')^2 = \det(P)^2 \det(A)^2 = \det{}_B(B')^2 \mathrm{disc}(B) \ .$$

Comme le discriminant de la base donnée par les puissances d'un élément primitif n'est pas nul, il en est de même du discriminant d'une base arbitraire.

Remarque 7.32. *La proposition 4.1.25 peut être interprétéé en disant que* $\mathrm{disc}(B)$ *est le discriminant de la forme quadratique* $w \longmapsto \mathrm{Tr}_K(w^2)$ *dans la base* B*. Cette forme quadratique est donc non dégénérée. De plus, le corollaire précédent n'est autre que la formule classique comparant les discriminants d'une forme quadratique dans deux bases.*

7.5 L'anneau des entiers d'un corps de nombres : ordres

Soit K un corps de nombres et $\mathbb{Z}_K$ son anneau d'entiers ; notons n le degré de K et $\varphi_1, \ldots, \varphi_n$ les plongements de K dans $\mathbb{C}$, ordonnés de telle sorte que les r_1 premiers soient les plongements réels, et les suivants les plongements complexes, eux même ordonnés de telle sorte que $\varphi_{r_1+i} = \overline{\varphi_{r_1+r_2+i}}$ soient des plongements complexes conjugués pour $1 \leq i \leq r_2$. Soit V l'espace vectoriel réel $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ et $\Phi : K \longrightarrow V$ donné par

$$\Phi(z) = (\varphi_1(z), \ldots, \varphi_{r_1+r_2}(z)) \ .$$

C'est une application $\mathbb{Q}$-linéaire de K dans V ; elle est injective car chacun des φ_i l'est.

Théorème 7.33. *L'image de* $\mathbb{Z}_K$ *par l'application* Φ *est un réseau de rang* n *de l'espace vectoriel* V*.*

Démonstration : démontrons d'abord que l'image de $\mathbb{Z}_K$ est un sous-groupe discret de V. D'après la proposition 9.24, il suffit de démontrer que pour tout nombre réel R, l'ensemble des $z \in \mathbb{Z}_K$ tels que $\|\Phi(z)\| \leq R$ est fini. Le choix de la norme sur V n'importe pas, nous choisirons la norme du sup. Soit $z \in \mathbb{Z}_K$, et d son degré, $z_1, \ldots, z_d$ ses conjugués. Les ensembles $\{z_1, \ldots, z_d\}$ et $\{\varphi_1(z), \ldots, \varphi_n(z)\}$ coïncident. Par conséquent,

$$\max(|z_1|, \ldots, |z_d|) = \max(|\varphi_1(z)|, \ldots, |\varphi_n(z)|) = \|\Phi(z)\| \ .$$

De plus, le dénominateur de z est égal à 1, car z est un entier algébrique. Ainsi, si $z \in \mathbb{Z}_K$, sa taille est égale à $\|\Phi(z)\|$. D'aprs la proposition 7.13, il n'y a donc qu'un nombre fini d'entiers algébriques tels que $\|\Phi(z)\| \leq R$ et donc $\Phi(\mathbb{Z}_K)$ est un sous-groupe discret de V. D'après la proposition 9.24, $\Phi(\mathbb{Z}_K)$ est un réseau de V. Son rang est la dimension maximale d'une famille $\mathbb{Q}$-linéairement indépendante de $\Phi(\mathbb{Z}_K)$; il est inférieur ou égal à $\dim_{\mathbb{R}} V = n$. Or, K est un espace vectoriel de dimension n sur $\mathbb{Q}$; considérons-en une base $(\alpha_1, \ldots, \alpha_n)$ et soit D le PPCM des dénominateurs des α_i. Alors, $(D\alpha_1, \ldots, D\alpha_n)$ est une base de K sur $\mathbb{Q}$ formée d'entiers algébriques. L'image de ces éléments par Φ est une famille libre de cardinal n de $\Phi(\mathbb{Z}_K)$. Par conséquent, $\Phi(\mathbb{Z}_K)$ est de rang $n = [K : \mathbb{Q}]$.

Corollaire 7.34. *Soit* K *un corps de nombres de degré* n*. En tant que groupe abélien,* $\mathbb{Z}_K$ *est isomorphe à* $\mathbb{Z}^n$*.*

Définition 7.35. *Soit K un corps de nombres et soit A un sous-anneau de K. On dit que A est un ordre de K s'il vérifie les deux propriétés suivantes :*
(i) comme $\mathbb{Q}$-espace vectoriel, A engendre K ;
(ii) comme groupe abélien, A est de type fini.

Exemple 7.36. *(i) D'après le corollaire précédent, $\mathbb{Z}_K$ est un ordre de K.*
(ii) Soit α un entier algébrique tel que $K = \mathbb{Q}(\alpha)$; posons $n = [K : \mathbb{Q}]$. Démontrons que $\mathbb{Z}[\alpha]$ est un ordre de K. Puisque $\mathbb{Z}[\alpha]$ contient une base de K, comme $\mathbb{Q}$-espace vectoriel, il engendre K. Soit en outre P le polynôme minimal de α ; c'est un polynôme à coefficients entiers, unitaire, de degré d. Par suite, pour tout entier $k \geq 0$, α^k est combinaison linéaire à coefficients entiers de $1, \alpha, \ldots, \alpha^{n-1}$; ainsi, $\mathbb{Z}[\alpha]$ est engendré comme groupe abélien par $1, \alpha, \ldots, \alpha^{n-1}$.

Remarque 7.37. *(i) Tout ordre de K est contenu dans $\mathbb{Z}_K$. Soit en effet A un ordre de K et soit $z_1, \ldots, z_n$ une famille génératrice de A comme groupe abélien. Soit w un élément de A ; définissons une matrice $M = (m_{ij}) \in M_n(\mathbb{Z})$ de sorte que pour tout $j \in \{1, \ldots, n\}$, on ait $wz_j = \sum_{i=1}^n a_{i,j} z_i$. Soit P le polynôme caractéristique de M. D'après la proposition 6.5, P annule l'endomorphisme m_w de A donné par la multiplication par w ; en particulier, $P(m_w)(1) = 0$, c'est-à-dire $P(w) = 0$. Comme P est un polynôme unitaire à coefficients entiers, w est un entier algébrique, c'est-à-dire $w \in \mathbb{Z}_K$.*
(ii) Inversement, un sous-groupe de $\mathbb{Z}_K$ qui contient 1 et est stable par produit est un ordre de K dès qu'il contient une base de K. Sous ces hypothèses en effet, un tel sous-groupe abélien est un sous-anneau de K et engendre K comme espace vectoriel. De plus, étant un sous-groupe d'un groupe isomorphe à $\mathbb{Z}^n$, il est de type fini.

Corollaire 7.38. *Soit K un corps de nombres, soit n son degré et soit A un ordre de K. Comme groupe abélien, A est isomorphe à $\mathbb{Z}^n$.*

Démonstration : en effet, A est contenu dans $\mathbb{Z}_K$ d'après la remarque ci-dessus. C'est en particulier un groupe abélien libre, c'est-à-dire isomorphe à $\mathbb{Z}^m$ pour un entier m tel que $0 \leq m \leq n$. Comme A engendre K comme $\mathbb{Q}$-espace vectoriel, il contient n éléments linéairement indépendants et l'on a $m = n$.

Soit K un corps de nombres et A un ordre de K. Soient B et B' des bases du groupe abélien A. On a donc $\det_B(B') = \pm 1$ si bien que $\mathrm{Disc}(B) = \mathrm{Disc}(B')$.

Définition 7.39. *La valeur commune de ces discriminants est appelée discriminant de l'ordre A et notée* $\mathrm{Disc}(A)$. *Par abus de langage, on appelle discriminant de K le discriminant de $\mathbb{Z}_K$.*

Proposition 7.40. *Soit K un corps de nombres et A un ordre de K. On a l'égalité* $\mathrm{Disc}(A) = \mathrm{Disc}(K)\mathrm{Card}(\mathbb{Z}_K/A)^2$.

Démonstration : notons n le degré de K. D'après le théorème de la base adaptée, il existe une base $(w_1, \ldots, w_n)$ de $\mathbb{Z}_K$ et des entiers non nuls $d_1, \ldots, d_n$ tels que $(d_1 w_1, \ldots, d_n w_n)$ soit une base de A. On a donc $\mathrm{Disc}(A) = (d_1 \ldots d_n)^2 \mathrm{Disc}(K)$. En outre, $\mathbb{Z}_K/A$ est un groupe abélien isomorphe au produit des groupes $\mathbb{Z}/d_i\mathbb{Z}$, donc est de cardinal $d_1 \ldots d_n$. La proposition est ainsi démontrée.

Corollaire 7.41. *Si* $\mathrm{Disc}(A)$ *est sans facteur carré, alors $A = \mathbb{Z}_K$.*

Exemple 7.42. *Soit K le corps $\mathbb{Q}(\alpha)$ où α est une racine du polynôme $P = X^3 + X + 1$. Comme P est irréductible modulo 2 (il est de degré 3 et n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$), P est irréductible dans $\mathbb{Q}[X]$ et est le polynôme minimal de α. Ainsi, $[K : \mathbb{Q}] = 3$. De plus, α est un entier algébrique, donc $\mathbb{Z}[\alpha]$ est un ordre de K. Son discriminant est donné par*

$$\mathrm{Disc}(\mathbb{Z}[\alpha]) = \det \begin{pmatrix} \mathrm{Tr}_K(1) & \mathrm{Tr}_K(\alpha) & \mathrm{Tr}_K(\alpha^2) \\ \mathrm{Tr}_K(\alpha) & \mathrm{Tr}_K(\alpha^2) & \mathrm{Tr}_K(\alpha^3) \\ \mathrm{Tr}_K(\alpha^2) & \mathrm{Tr}_K(\alpha^3) & \mathrm{Tr}_K(\alpha^4) \end{pmatrix} .$$

Mais, $\mathrm{Tr}_K(1) = 3$ et $\mathrm{Tr}_K(\alpha) = 0$ (c'est le terme en X^2 du polynôme minimal). On a $\alpha^4 = -\alpha - \alpha^2$ et $\alpha^5 = -\alpha^2 - \alpha^3 = -\alpha^2 + \alpha + 1$. Dans la base $(1, \alpha, \alpha^2)$ de K, la matrice de la multiplication par α^2 est donc

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

donc $\mathrm{Tr}_K(\alpha^2) = -2$. Par suite, $\mathrm{Tr}_K(\alpha^3) = \mathrm{Tr}_K(-1 - \alpha) = -3$ et $\mathrm{Tr}_K(\alpha^4) = \mathrm{Tr}_K(-\alpha - \alpha^2) = 2$. Ainsi,

$$\mathrm{Disc}(Z[\alpha]) = \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & -3 & 2 \end{pmatrix} = -31 .$$

Comme $\mathrm{Disc}(Z[\alpha])$ est sans facteur carré, on en déduit que $\mathbb{Z}_K = Z[\alpha]$.

Dans la suite de ce paragraphe, on relie $\mathrm{Disc}(A)$ au volume du domaine fondamental du réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ associé à A. Soient $\varphi_1, \dots, \varphi_n$ les plongements réels de K et $\varphi_{r_1+1}, \dots, \varphi_{r_1+r_2}$ des plongements complexes, deux à deux non conjugués. Si n désigne le degré de K, on a donc $n = r_1 + 2r_2$. Soit $\Phi : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ l'application donnée par $w \longmapsto (\varphi_j(w))_{1 \le j \le r_1+r_2}$. On a vu que Φ est $\mathbb{Q}$-linéaire, injective. En outre, $\Phi(A)$ est contenu dans $\Phi(\mathbb{Z}_K)$, donc est un sous-groupe discret de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Par ailleurs, A contient une base de K, donc $\Phi(A)$ contient n vecteurs linéairement indépendants sur $\mathbb{Q}$. Cela entraîne que $\Phi(A)$ est un réseau de rang n de l'espace vectoriel $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Proposition 7.43. *Identifions $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ à $\mathbb{R}^n$ par l'application*

$$\theta : (\boldsymbol{x}, \boldsymbol{z}) \longmapsto (x_1, \dots, x_{r_1}, \mathfrak{Re}(z_{r_1+1}), \mathrm{Im}(z_{r_1+1}), \dots, \mathfrak{Re}(z_{r_1+r_2}), \mathrm{Im}(z_{r_1+r_2})) ,$$

où $\boldsymbol{x} = (x_1, \dots, x_{r_1}) \in \mathbb{R}^{r_1}$ et $\boldsymbol{z} = (z_{r_1+1}, \dots, z_{r_1+r_2}) \in \mathbb{C}^{r_2}$, et soit P un domaine fondamental de $\Phi(A)$ dans $\mathbb{R}^n$. On a $|\mathrm{Disc}(A)| = 4^{r_2}\mathrm{Vol}(P)^2$.

Démonstration : pour tout entier j tel que $1 \le j \le r_2$, posons $\varphi_{r_1+r_2+j} = \overline{\varphi_{r_1+j}}$. Soit $w_1, \dots, w_n$ une base de A. Par définition, on a

$$\mathrm{Disc}(A) = \det(\varphi_j(w_k))^2 .$$

Soit D la matrice $(\varphi_j(w_k))$. Si j vérifie $1 \le j \le r_2$, ses lignes d'indices $r_1 + j$ et $r_1 + r_2 + j$ sont conjuguées l'une de l'autre. L'opération $L_{r_1+j} \longleftarrow (L_{r_1+j} + L_{r_1+r_2+j})/2$ remplace la ligne L_{r_1+j} par sa partie réelle et divise le déterminant par 2. L'opération $L_{r_1+r_2+j} \longleftarrow i(L_{r_1+r_2+j} - L_{r_1+j})$ remplace alors la ligne $L_{r_1+r_2+j}$ par la partie imaginaire de l'ancienne ligne L_{r_1+j} et multiplie le déterminant par i. Par r_2 échanges de lignes, on obtient donc une matrice D' dont le déterminant $|\det(D')|$ est

égal en valeur absolue au volume du domaine fondamental $P = [0,1]w_1 + \cdots + [0,1]w_n$ de $\Phi(A)$ dans $\mathbb{R}^n$. On a donc $\mathrm{vol}(P) = |\det(D')|$, d'où $\det(D')^2 = \mathrm{vol}(P)^2$. Comme $\det(D') = (-i/2)^{r_2}\det(D)$, on a

$$\mathrm{vol}(P)^2 = (-1/4)^{r_2}\det(D)^2 = (-1/4)^{r_2}\mathrm{Disc}(A) \ ,$$

autrement dit $\mathrm{Disc}(A) = (-4)^{r_2}\mathrm{vol}(P)^2$.

Corollaire 7.44. *Soit K un corps de nombres ; le signe du discriminant de tout ordre de K est égal à $(-1)^{r_2}$, où r_2 est la moitié du nombre de plongements complexes de K.*

8 Le théorème des unités, le groupe des classes

8.1 Le théorème des unités

Soit K un corps de nombres. Dans ce paragraphe, on étudie le groupe des éléments inversibles (ou unités) de l'anneau $\mathbb{Z}_K$. On note n le degré de K, r_1 le nombre de plongements réels de K, r_2 la moitié du nombre de plongements complexes de K et on fixe des plongements $\varphi_1, \ldots, \varphi_{r_1+r_2}$ comme précédemment. On note aussi $\Phi : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, l'application $w \longmapsto (\varphi_j(w))$.

Notons Λ l'application de $K^\star$ dans $\mathbb{R}^{r_1+r_2}$ donnée par

$$\Lambda(w) = (\log|\varphi_1(w)|, \ldots, \log|\varphi_{r_1}(w)|, \log|\varphi_{r_1+1}(w)|^2, \ldots, \log|\varphi_{r_1+r_2}(w)|^2) \ .$$

C'est un homomorphisme de groupes qu'on appelle l'application logarithmique.

Proposition 8.1. *L'intersection de* $\ker(\Lambda)$ *avec $\mathbb{Z}_K$ est l'ensemble des racines de l'unités contenues dans K ; c'est un groupe fini.*

Démonstration : soit $w \in \ker(\Lambda) \cap \mathbb{Z}_K$; on a $|\varphi_j(w)| = 1$ pour tout j et la taille de w est égale à 1. Comme il n'y a qu'un nombre fini de nombres algébriques de K de taille bornée, $\ker(\Lambda) \cap \mathbb{Z}_K$ est un ensemble fini. Comme c'est un sous-groupe de $K^\star$, ce sont des racines de l'unité. Inversement, si w est une racine de l'unité contenue dans K, il existe un entier $d > 0$ tel que $w^d = 1$ et donc $|\varphi_j(w)| = 1$ pour tout j ; en outre, w est un entier algébrique. Par suite, $w \in \ker(\Lambda) \cap \mathbb{C}_K$.

Notons U_K le groupe des éléments inversibles de $\mathbb{Z}_K$, qu'on appelle aussi unités. Rappelons qu'un élément w de $\mathbb{Z}_K$ est inversible si et seulement si $\mathrm{N}_K(w) = \pm 1$. Ainsi, si $w \in U_K$, $\Lambda(w)$ est un élément de l'hyperplan H de $\mathbb{R}^{r_1+r_2}$ d'équation $t_1 + \cdots + t_{r_1+r_2} = 0$.

Théorème 8.2. *L'image de U_K par Λ est un réseau de rang $r_1 + r_2 - 1$ de H.*

Corollaire 8.3. *(Théorème des unités de Dirichlet) Soit K un corps de nombres ; soit μ_K le groupe fini des racines de l'unité de K. Le groupe U_K est isomorphe au produit $\mu_K \times \mathbb{Z}^{r_1+r_2-1}$.*

Démonstration : (en supposant vrai le théorème 8.2) posons $r = r_1 + r_2 - 1$ et soit $w_1, \ldots, w_r$ des éléments de U_K tels que $\Lambda(w_1), \ldots, \Lambda(w_r)$ forment une base de $\Lambda(U_K)$. Démontrons que l'application θ de $\mu_K \times \mathbb{Z}^r$ dans U_K donnée par $(z, n_1, \ldots, n_r) \longmapsto z \cdot w^{n_1} \cdots w^{n_r}$ est un isomorphisme. Soit $(z, n_1, \ldots, n_r)$ un élément du noyau de θ. On a $\Lambda(\theta(z, n_1, \ldots, n_r)) = n_1\Lambda(w_1) + \cdots + n_r\Lambda(w_r)$. Par suite, $n_1 = \cdots = n_r = 0$ puis $z = 1$. Autrement dit, θ est injectif. Soit alors $w \in U_K$. Soit $n_1, \ldots, n_r$

des entiers relatifs tels que $\Lambda(w) = n_1\Lambda(w_1) + \cdots + n_r\Lambda(w_r)$. Alors, $w \cdot w^{-n_1} \dots w^{-n_r}$ est une unité w' telle que $\Lambda(w') = 0$; on a donc $w' \in \mu_K$ ce qui entraîne que θ est surjectif.

La fin de ce paragraphe est consacrée à la démonstration du théorème 8.2. Démontrons d'abord que $\Lambda(U_K)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2}$. Il suffit pour cela de vérifier que pour tout nombre réel $c > 0$ l'ensemble des éléments $w \in U_K$ tels que $|\log|\varphi_j(w)|| \leq c$ est fini, car cela démontrera que l'ensemble des éléments $(t_1, \dots, t_{r_1+r_2})$ de $\Lambda(U_K)$ tels que $|t_j| \leq c$ pourtout j est un ensemble fini.

Or, l'inégalité $|\log|\varphi_j(w)|| \leq c$ implique $|\varphi_j(w)| \leq e^c$; comme c'est un entier algébrique, la taille d'une telle unité est donc majorée par e^c. On conclut en rappelant qu'il n'y a qu'un nombre fini de nombres algébriques de K de taille majorée par e^c.

Comme $\Lambda(U_K)$ est contenu dans l'hyperplan H, il reste à démontrer que $\Lambda(U_K)$ contient r_1+r_2-1 éléments linéairement indépendants, c'est-à-dire à construire $r_1 + r_2 - 1$ unités multiplicativement indépendantes :

Proposition 8.4. *Pour tout entier $j \in \{1, \dots, r_1 + r_2\}$, il existe une unité $w_j \in U_K$ telle que $\log|\varphi_k(w_j)| < 0$ si $k \neq j$.*

Bien sûr, la relation $|\mathrm{N}_K(w_j)| = 1$ entraîne alors que $\log|\varphi_j(w_j)| > 0$.

Démonstration : soit $c = (c_1, \dots, c_{r_1+r_2})$ une famille de nombres réels strictement positifs et soit $\|\cdot\|_c$ la norme sur $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ donnée par

$$\begin{aligned}\|(x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2})\|_c \\ = \max\left\{|x_1|c_1^{-1}, \dots, |x_{r_1}|c_{r_1}^{-1}, |z_{r_1+1}|c_{r_1+1}^{-1/2}, \dots, |z_{r_1+r_2}|c_{r_1+r_2}^{-1/2}\right\} .\end{aligned}$$

La boule unité B_c de cet espace vectoriel est l'ensemble des $(x_1, \dots, z_{r_1+r_2})$ tels que $|x_k| \leq c_k$ pour $1 \leq k \leq r_1$ et $|z_{r_1+k}| \leq c_{r_1+k}^{1/2}$ pour $1 \leq k \leq r_2$. Son volume est donc

$$\mathrm{Vol}(B_c) = 2^{r_1}c_1 \dots c_{r_1}(\pi c_{r_1+1}) \dots (\pi c_{r_1+r_2}) = 2^{r_1}\pi^{r_2}(c_1 \dots c_{r_1+r_2}) .$$

Soit P un domaine fondamental du réseau $\Phi(\mathbb{Z}_K)$ de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. D'après le théorème de Minkowski, il existe, si $\mathrm{Vol}(B_c) \geq 2^n\mathrm{Vol}(P)$ (il n'y a pas de restriction à supposer qu'on est en situation d'égalité), un entier algébrique non nul $a_c \in \mathbb{Z}_K$ tel que $\phi(a_c) \in B_c$. On a en outre

$$\begin{aligned}|\mathrm{N}_K(a_c)| &= |\varphi_1(a_c)| \dots |\varphi_{r_1}(a_c)| \cdot |\varphi_{r_1+1}(a_c)|^2 \dots \varphi_{r_1+r_2}(a_c)|^2 \\ &\leq c_1 \dots c_{r_1+r_2} \\ &= \pi^{-r_2}\mathrm{Vol}(B_c) \\ &\leq 2^n\pi^{r_2}\mathrm{Vol}(P) .\end{aligned}$$

On a toute latitude pour choisir le paramètre c ; on choisit tous les c_k (pour $k \neq j$) égaux à un nombre réel $t > 0$, supposé petit et on pose ensuite $c_j = \pi^{-r_2}2^{2r_2}\mathrm{Vol}(P)/t^{r+r_2-1}$ et on pose $a_t = a_c$.

Lorsque t tend vers 0, $|\varphi_k(a_t)|$ tend vers 0 si $k \neq j$ et $|\varphi_j(a_t)|$ tend vers $+\infty$; cela prouve que l'on a construit une infinité d'entiers algébriques distincts dont les normes sont toutes majorées par un

même nombre réel. Comme ces normes sont des entiers, on a ainsi construit une suite infinie d'entiers algébriques de K de même norme N. Le groupe abélien $\mathbb{Z}_K/N\mathbb{Z}_K$ est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^n$; il est en particulier fini. Quitte à considérer une sous-suite de la suite précédente, on voit qu'il existe une suite infinie $(a_{t_m})_m$ d'entiers algébriques non nuls de K de même norme N et qui sont deux à deux congrus modulo N.

Lemme 8.5. *Soient a et b des éléments non nuls de $\mathbb{Z}_K$ et N un entier relatif. On suppose que $\mathrm{N}_K(a) = \mathrm{N}_K(b) = N$ et que $a - b \in N\mathbb{Z}_K$. Alors, a/b est une unité de K.*

Démonstration : posons $w = a/b$ et écrivons $a = b + Nc$, avec $c \in \mathbb{Z}_K$. Comme $N = \mathrm{N}_K(b)$, il existe un entier algébrique $b' \in \mathbb{Z}_K$ tel que $N = bb'$. Alors, $a = b + bb'c = b(1 + b'c)$ et $w = 1 + b'c$. Par suite, w est un entier algébrique. On démontre de même que b/a est un entier algébrique, ce qui conclut la démonstration que w est une unité de K.

Pour tout entier $m \geq 0$, posons $w_m = a_{t_m}/a_{t_1}$. D'après le lemme précédent, w_m est une unité de K pour tout $m \in \mathbb{N}$; ces unités sont deux à deux distinctes. En outre, si $k \in \{1, \dots, r_1 + r_2\}$ est distinct de j, $|\varphi_k(w_m)|$ tend vers 0. Il existe en particulier une unité $u_j \in U_K$ telle que $|\varphi_k(u_j)| < 1$ pour tout entier $k \in \{1, \dots, r_1 + r_2\}$ qui est distinct de j. Cela termine la démonstration de la proposition.

Pour finir la démonstration du théorème des unités, il suffit de démontrer que les unités

$$u_1, \dots, u_{r_1+r_2-1}$$

construites dans la proposition précédente sont multiplicativement indépendantes, ou encore, que leurs images par Λ sont linéairement indépendantes dans $\mathbb{R}^{r_1+r_2}$. Considérons la matrice M de taille $(r_1 + r_2) \times (r_1 + r_2 - 1)$ formée par ces images et extrayons-en une matrice carrée $M' = (m_{i,j})_{1 \leq i,j \leq r_1+r_2-1}$ en étant la dernière ligne. Si $i \neq j$, on a $m_{i,j} = \log|\varphi_i(u_j)|$ (lorsque $1 \leq j \leq r_1$) et $m_{i,j} = 2\log|\varphi_i(u_j)|$ sinon ; dans tous les cas, $m_{i,j} < 0$. En outre, pour tout entier j, on a $m_{1,j} + \cdots + m_{r,j} = -m_{r_1+r_2,j} > 0$. D'après le lemme suivant, M' est inversible donc M est de rang $r_1 + r_2 - 1$, ce qu'il fallait démontrer.

Lemme 8.6. *Soit M une matrice $n \times n$ à coefficients réels. On suppose que $m_{i,j} < 0$ si $i \neq j$ et que la somme des coefficients de chaque colonne est strictement positive. Alors, M est inversible.*

Démonstration : considérons une relation de dépendance linéaire entre les lignes de M et démontrons qu'elle est triviale. Soit donc $x_1, \dots, x_n$ des nombres réels tels que

$$\sum_{i=1}^{n} x_i m_{i,j} = 0 \qquad \text{pour } j \in \{1, \dots, n\} \ .$$

Soit j un entier tel que $x_j = \max(x_1, \dots, x_n)$. Alors

$$0 = \sum_{i=1}^{n} x_i m_{i,j} = \sum_{i=1}^{n} (x_i - x_j) m_{i,j} + x_j \sum_{i=1}^{n} m_{i,j} \geq x_j \sum_{i=1}^{n} m_{i,j}$$

puisque $(x_i - x_j)m_{i,j}$ est positif ou nul pour $i \neq j$, et est nul si $i = j$. Comme $\sum_{i=1}^{n} m_{i,j} > 0$, il vient $x_j \leq 0$ et tous les x_i sont négatifs ou nuls. Le même argument appliqué à leurs opposés démontre qu'ils sont tous positifs ou nuls. Par suite, $x_1 = \cdots = x_n = 0$, ce qu'il fallait démontrer.

8.2 Anneaux euclidiens, anneaux principaux

Soit A un anneau intègre. Rappelons qu'on dit que A est un anneau euclidien s'il existe une jauge (ou jauge euclidienne, ou encore un stathme euclidien) sur A est une fonction $j : A \setminus \{0\} \longrightarrow \mathbb{N}$ vérifiant la propriété suivante : pour tout $a \in A$ et tout $b \in A \setminus \{0\}$, il existe q et r dans A tels que $a = bq + r$ et tels que $j(r) < j(b)$ ou $r = 0$. On exige aussi que $j(ab) \geq \max(j(a), j(b))$ pour tous a et b dans $A \setminus \{0\}$ mais cette dernière propriété n'est pas essentielle ; en effet, la fonction donnée par $j_{\max}(a) = \min_{b \neq 0} j(ab)$ est encore une jauge qui satisfait à cette condition supplémentaire.

L'anneau $\mathbb{Z}$ des entiers relatifs est un anneau euclidien pour la jauge $j = |\cdot|$; si k est un corps, l'anneau $k[X]$ des polynômes en une variables à coefficients dans k est un anneau euclidien pour la jauge $j = \deg$.

Un anneau euclidien est un anneau principal. La démonstration est la même que celle utilisée pour les anneaux $\mathbb{Z}$ et $k[X]$. Soit en effet A un anneau euclidien pour une jauge j et soit I un idéal de A. L'idéal 0 étant principal, supposons $I \neq 0$ et considérons un élément $b \in I \setminus \{0\}$ de jauge minimale. Soit $a \in I$; soient q et $r \in A$ tels que $a = bq + r$ et $r = 0$ ou $j(r) < j(b)$. Comme $b \in I$, $bq \in I$ et $r = a - bq \in I$; l'inégalité $j(r) < j(b)$ et la définition de b entraînent $r = 0$, c'est-à-dire $a \in (b)$. Inversement, tout multiple de b appartient à I, d'où $I = (b)$.

Un anneau principal est un anneau factoriel. Là encore, la démonstration est la même que pour les entiers ou les polynômes. Donnons quelques exemples de corps de nombres K pour lesquels l'anneau $\mathbb{Z}_K$ est un anneau euclidien, la jauge étant la fonction norme N_K.

Proposition 8.7. *Soit K un corps de nombres. Supposons que pour tout élément $z \in K$, il existe un élément $a \in \mathbb{Z}_K$ tel que $\mathrm{N}_K(z - a) < 1$. Alors, N_K définit une jauge euclidienne sur $\mathbb{Z}_K$.*

Démonstration : soit a et b des éléments de $\mathbb{Z}_K$, avec $b \neq 0$; posons $z = a/b$ et soit $q \in \mathbb{Z}_K$ tel que $\mathrm{N}_K(z - q) < 1$.Posons alors $r = a - bq$; c'est un élément de $\mathbb{Z}_K$ tel que $r = b(z - q)$, donc $\mathrm{N}_K(r) < \mathrm{N}_K(b)$. Cela démontre que N_K est une jauge.

Exemple 8.8. *(i) L'anneau $\mathbb{Z}[i] = \mathbb{Z}_{\mathbb{Q}}(i)$ est euclidien pour la norme. En effet, si $z = x + iy \in \mathbb{Q}(i)$, posons $a = \xi + i\eta$, où ξ, η sont les entiers les plus proches de x et y respectivement. On a donc $|\xi - x| \leq 1/2$ et $|\eta - y| \leq 1/2$. Alors, $\mathrm{N}_K(z - a) = |\xi - x|^2 + |y - \eta|^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$.*

(ii) Soit j une racine cubique primitive de l'unité. De même, l'anneau $\mathbb{Z}[j] = \mathbb{Z}_{\mathbb{Q}}(j)$ est euclidien pour la norme. On raisonne de même : soit $z = x + jy \in \mathbb{Q}(i)$ et posons $a = \xi + j\eta$, où ξ, η sont les entiers les plus proches de x et y. On a

$$\mathrm{N}(z - a) = (x - \xi)^2 + (x - \xi)(y - \eta) + (y - \eta)^2 \leq \frac{3}{4} < 1 \ .$$

Exemple 8.9. *Soit K le corps $\mathbb{Q}(\sqrt{-19})$ et $\mathbb{Z}_K = \mathbb{Z}[\omega]$ son anneau d'entiers, où l'on a posé $\omega = \frac{1+\sqrt{-19}}{2}$. Démontrons que $\mathbb{Z}_K$ ne possède pas de jauge, donc n'est pas un anneau euclidien.*

Considérons, par l'absurde, une jauge j sur $\mathbb{Z}_K$. Soit $a \in \mathbb{Z}_K$ un élément qui n'est ni nul ni inversible et tel que $j(a)$ soit minimal. Soit $z \in \mathbb{Z}_K$ et considérons une division euclidienne $z = aq + r$ avec $r = 0$ ou $j(r) < j(a)$. On a donc $r = 0$ ou r inversible. Autrement dit, tout élément de $\mathbb{Z}_K$ est congru modulo a à un élément qui est nul ou inversible. En particulier, $\mathrm{Card}(\mathbb{Z}_K/(a)) \leq \mathrm{Card}(\mathbb{Z}_K^\star) + 1$. *Comme K est un corps quadratique imaginaire, $\mathbb{Z}_K^\star$ est un groupe fini, en l'occurrence réduit à $\{\pm 1\}$; ainsi,* $\mathrm{Card}(\mathbb{Z}_K/(a)) \leq 3$. *Or, $\mathbb{Z}_K/(a)$ est de cardinal $\mathrm{N}_K(a)$. Si l'on écrit $a = x + y\omega$,*

avec x et $y \in \mathbb{Z}$, on a $\mathrm{N}_K(a) = x^2 + xy + 5y^2$. Si $|y| \geq 1$, on a $\mathrm{N}_K(a) \geq (x^2 + xy + y^2) + 4y2 \geq 4$; si $y = 0$, alors $|x| \geq 2$ car $a = x$ n'est ni nul, ni inversible, et $\mathrm{N}_K(a) \geq 4$. Cette contradiction démontre que j n'existe pas. En revanche, on peut démontrer que $\mathbb{Z}_K$ est néanmoins un anneau principal.

8.3 Idéaux d'un anneau d'entiers algébriques

Soit K un corps de nombres et $\mathbb{Z}_K$ son anneau d'entiers. On cherche à comprendre la relation de divisibilité dans $\mathbb{Z}_K$, en particulier lorsque cet anneau n'est pas factoriel, ou n'est pas principal. La théorie des idéaux a déjà démontré son intérêt, même dans le cas « facile » des anneaux principaux ; pensons par exemple à l'égalité de Bézout. Comme nous le verrons plus loin, il se trouve que les notions d'anneau factoriel et d'anneau principal vont coïncider pour $\mathbb{Z}_K$, mais la théorie des idéaux est l'outil privilégié pour cette étude.

Nous reprenons les notations du paragraphe précédent en notant $n = [K : \mathbb{Q}]$, r_1 et $2r_2$ les nombres de plongements réels, respectivement complexes, de K et Φ l'application canonique de K dans l'espace vectoriel $V_K = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Proposition 8.10. *Soit I un idéal non nul de $\mathbb{Z}_K$. L'anneau $\mathbb{Z}_K/I$ est fini et l'entier $\mathrm{Card}(\mathbb{Z}_K/I)$ appartient à I.*

Démonstration : soit a un élément non nul de I. Il existe un élément b de I tel que $\mathrm{N}_K(a) = ab$. En effet, $\mathrm{N}_K(a)/a$ est le produits de $(n-1)$ entiers algébriques (conjugués de a) donc est un entier algébrique ; comme c'est un élément de K, il appartient à $\mathbb{Z}_K$. Cela démontre que l'entier $\mathrm{N}_K(a)$ appartient à I. Par suite, l'anneau $\mathbb{Z}_K/I$ est quotient de l'anneau $\mathbb{Z}_K/\mathrm{N}_K(a)$; en tant que groupe abélien, ce dernier est isomorphe à $(\mathbb{Z}/\mathrm{N}_K(a)\mathbb{Z})^n$, donc est fini. Par conséquent, $\mathbb{Z}_K/I$ est fini.

Soit N son cardinal ; d'après le théorème de Lagrange, on a $N\overline{a} = 0$ pour tout $a \in \mathbb{Z}_K$, $\bar{\cdot}$ désignant la classe modulo I. En particulier, prenant $a = 1$, on a $N \equiv 0 \bmod I$ c'est-à-dire $N \in I$.

Corollaire 8.11. *Un idéal premier non nul de $\mathbb{Z}_K$ est maximal.*

Démonstration : soit I un idéal premier de $\mathbb{Z}_K$, supposé différent de l'idéal nul. Alors, $\mathbb{Z}_K/I$ est un anneau intègre (car I est premier) et fini. C'est donc un corps (si $a \in \mathbb{Z}_K/I$ n'est pas nul, la multiplication par a est un endomorphisme injectif de l'anneau fini $\mathbb{Z}_K/I$, donc est bijectif, donc a est inversible) ce qui signifie que l'idéal I est un idéal maximal.

Corollaire 8.12. *L'anneau $\mathbb{Z}_K$ est noethérien : toute suite croissante (I_n) d'idéaux de $\mathbb{Z}_K$ est stationnaire.*

Démonstration : considérons, par l'absurde, une suite strictement croissante (I_n) d'idéaux de $\mathbb{Z}_K$. Pour $n \geq 1$, $I_n \neq 0$ donc $\mathbb{Z}_K/I_n$ est un ensemble fini. L'inclusion $I_n \subset I_{n+1}$ entraîne qu'il existe un homomorphisme surjectif de $\mathbb{Z}_K/I_n$ sur $\mathbb{Z}_K/I_{n+1}$; comme $I_n \neq I_{n+1}$, cet homomorphisme n'est pas injectif. On a donc $\mathrm{Card}(\mathbb{Z}_K/I_{n+1}) < \mathrm{Card}(\mathbb{Z}_K/I_n)$.

La suite des nombre entiers $(\mathrm{Card}(\mathbb{Z}_K/I_n))_{n\geq 1}$ est ainsi strictement décroissante, d'où la contradiction recherchée.

Corollaire 8.13. *Tout idéal de $\mathbb{Z}_K$, distinct de $\mathbb{Z}_K$, est contenu dans un idéal maximal de $\mathbb{Z}_K$.*

Démonstration : soit I un idéal de $\mathbb{Z}_K$ tel que $I \neq \mathbb{Z}_K$. Démontrons par récurrence sur $\mathrm{Card}(\mathbb{Z}_K/I)$ qu'il existe un idéal maximal P de $\mathbb{Z}_K$ tel que $I \subset P$.

Si I est maximal, il suffit de poser $P = I$. Sinon, il existe un idéal I_1 de $\mathbb{Z}_K$ tel que $I \subsetneq I_1 \subsetneq \mathbb{Z}_K$ et donc $\mathrm{Card}(\mathbb{Z}_K/I_1) < \mathrm{Card}(\mathbb{Z}_K/I)$. Par récurrence, il existe un idéal maximal P de $\mathbb{Z}_K$ tel que $I_1 \subset P$, et l'on a donc $I \subset P$.

Corollaire 8.14. *Soit I un idéal non nul de $\mathbb{Z}_K$. Alors, $\Phi(I)$ est un réseau de rang n de V_K ; le volume d'un domaine fondamental de ce réseau est égal à*

$$\mathrm{Vol}(\Phi(I)) = \mathrm{Card}(\mathbb{Z}_K/I)\mathrm{Vol}(\Phi(\mathbb{Z}_K)) = \mathrm{Card}(\mathbb{Z}_K/I)2^{-r_2}\sqrt{|\mathrm{Disc}(K)|}\ .$$

De plus, il existe un élément non nul $a \in I$ de taille

$$\mathfrak{t}(a) \leq (2/\pi)^{r_2/n}|\mathrm{Disc}(K)|^{1/2n}\mathrm{Card}(\mathbb{Z}_K/I)^{1/n}\ .$$

En particulier, il existe un élément non nul $a \in I$ tel que

$$\mathrm{N}_K(a) \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{Disc}(K)|}\mathrm{Card}(\mathbb{Z}_K/I)\ .$$

Démonstration : on a $\Phi(I) \subset \Phi(\mathbb{Z}_K)$; comme $\Phi(\mathbb{Z}_K)$ est un réseau de V_K, il en est de même de $\Phi(I)$. Comme $\mathbb{Z}_K/I$ est fini, $\Phi(I)$ est de rang n et ses domaines fondamentaux ont un volume donné par la formule $V(\Phi(I)) = \mathrm{Card}(\mathbb{Z}_K/I)V(\Phi(\mathbb{Z}_K))$.

Munissons $V_K = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de la norme définie par $\|(z_1, \dots, z_{r_1+r_2})\| = \max_{1\leq j\leq r_1+r_2}(\|z_j|)$. Sa boule unité est égale à $[-1,1]^{r_1} \times B(0,1)^{r_2}$ et son volume vaut $2^{r_1}\pi^{r_2}$. D'après le théorème de Minkowski, le réseau $\Phi(I)$ contient un élément non nul $\Phi(a)$ tel que

$$\begin{aligned}\|\Phi(a)\| &\leq 2\left(\frac{\mathrm{Vol}(\Phi(I))}{\mathrm{Vol}(B)}\right)^{1/n}\\ &\leq \left(2^{n-r_1}\pi^{-r_2}2^{-r_2}\sqrt{|\mathrm{Disc}(K)|}\mathrm{Card}(\mathbb{Z}_K/I)\right)^{1/n}\\ &\leq \left(\frac{2}{\pi}\right)^{r_2/n}|\mathrm{Disc}(K)|^{1/2n}\,\mathrm{Card}(\mathbb{Z}_K/I)^{1/n}\ .\end{aligned}$$

Cela signifie que tous les conjugués de a sont de valeur absolue majorée par le membre de droite X de l'expression précédente. En particulier, la norme de a est majorée par sa puissance n-ième. En outre, la taille de a est majorée par $\max(1, X)$, car a est un entier algébrique.

Si I est un idéal non nul de l'anneau $\mathbb{Z}_K$, on appelle norme de l'idéal I, que l'on note $\mathrm{N}(I)$, le cardinal de l'anneau quotient $\mathbb{Z}_K/I$. Notons tout de suite le lien avec la norme d'un élément de K.

Proposition 8.15. *Soit a un élément non nul de $\mathbb{Z}_K$. On a $\mathrm{N}(a\mathbb{Z}_K) = |\mathrm{N}_K(a)|$. Plus généralement, pour tout idéal non nul I de $\mathbb{Z}_K$, on a $\mathrm{N}(aI) = |\mathrm{N}_K(a)|\mathrm{N}(I)$.*

Démonstration : soit $(z_1, \dots, z_n)$ une base de I. Alors, $(az_1, \dots, az_n)$ est une base de aI. Compte tenu de la formule donnée pour le volume du réseau défini par un idéal, il suffit de vérifier que $\mathrm{Vol}(\Phi(aI)) = |\mathrm{N}_K(a)|\mathrm{Vol}(\Phi(I))$. À son tour, cette dernière formule résultera de l'égalité de discriminants

$$\mathrm{Disc}((az_1, \dots, az_n)) = \mathrm{N}_K(a)^2\mathrm{Disc}((z_1, \dots, z_n))\ .$$

Or, notant $(\varphi_j)_{1\leq j\leq n}$ les plongements de K dans $\mathbb{C}$, on a

$$\begin{aligned}\mathrm{Disc}((az_1,\dots,az_n)) &= \det(\varphi_i(az_j))^2\\ &= \det((\varphi_i(a)\varphi_i(z_j)))^2\\ &= (\varphi_1(a)\dots\varphi_n(a))^2\det((\varphi_i(z_j)))^2\\ &= \mathrm{N}_K(a)^2\mathrm{Disc}((z_1,\dots,z_n))\ .\end{aligned}$$

Cela conclut la démonstration de la proposition.

Corollaire 8.16. *Pour qu'un idéal non nul I de $\mathbb{Z}_K$ soit principal, il faut et il suffit qu'il existe un élément $a\in I$ tel que $\mathrm{N}_K(a)=\pm\mathrm{N}(I)$; un tel élément est alors un générateur de I.*

Démonstration : supposons que I soit un idéal principal et soit a un générateur de I ; on a donc $a\in I$ et $|\mathrm{N}_K(a)|=\mathrm{N}(I)$, ce qu'il fallait démontrer. Inversement, soit a un élément de I tel que $\mathrm{N}_K(a)=\pm\mathrm{N}(I)$. L'inclusion d'idéaux $(a)\subset I$ et l'égalité $\mathrm{N}((a))=|\mathrm{N}_K(a)|=\mathrm{N}(I)$ entraînent que $I=(a)$; en particulier, I est principal.

8.4 Groupe des classes d'idéaux

Notons $\mathcal{I}_K$ l'ensemble des idéaux non nuls de $\mathbb{Z}_K$ et munissons-le de la relation suivante : si $I, J \in \mathcal{I}_K$, on dit que $I \sim J$ s'il existe des éléments non nuls a et b de $\mathbb{Z}_K$ tels que $aI = bJ$. C'est une relation d'équivalence. Notons $\mathcal{C}_K$ l'ensemble des classes d'équivalence.

Si $\mathbb{Z}_K$ est un anneau principal, tous les éléments de $\mathcal{I}_K$ sont équivalents entre eux. Inversement, Si I est un idéal non nul tel que $I \sim \mathbb{Z}_K$, démontrons que I est un idéal principal. Soit en effet a et $b \in \mathbb{Z}_K$ tels que $aI = b\mathbb{Z}_K = (b)$, avec $a, b \neq 0$. Comme $b \in aI$, il existe $w \in I$ tel que $b = aw$ et l'on a $aI = (aw)$, d'où l'on déduit facilement que $I = (w)$.

Proposition 8.17. *Posons $c = (2/\pi)^{r_2}\sqrt{|\mathrm{Disc}(K)|}$. Tout idéal non nul de $\mathbb{Z}_K$ est équivalent à un idéal contenant un entier $1 \leq t \leq c$. L'ensemble $\mathcal{C}_K$ des classes d'idéaux de $\mathbb{Z}_K$ est fini.*

Démonstration : pour tout entier naturel t tel que $1 \leq t \leq c$, les idéaux de $\mathbb{Z}_K$ contenant t sont en bijection avec les idéaux de l'anneau fini $\mathbb{Z}_K/(t)$; il n'y en a qu'un nombre fini. Démontrons que tout idéal non nul de $\mathbb{Z}_K$ est équivalent à l'un de ces idéaux.

Soit donc I un idéal non nul de $\mathbb{Z}_K$; d'après le corollaire ci-dessus, il existe un élément non nul a de I tel que $|\mathrm{N}_K(a)| \leq c\mathrm{N}(I)$. Considérant la suite de groupes abéliens $a\mathbb{Z}_K \subset I \subset \mathbb{Z}_K$, on voit que $I/a\mathbb{Z}_K$ est un groupe de cardinal inférieur ou égal à c. Il existe donc un entier naturel t tel que $1 \leq t \leq c$ et tel que $tI \subset a\mathbb{Z}_K$. Notons J la partie $a^{-1}tI$ de $\mathbb{Z}_K$; c'est un idéal tel que $tI = aJ$. En particulier, I et J sont équivalents. Comme $a \in I$, $t \in J$. La proposition est ainsi démontrée.

Définition 8.18. *On appelle nombre de classes de K le cardinal de $\mathcal{C}_K$, c'est- à-dire le nombre de classes d'équivalences pour la relation d'équivalence introduite dans $\mathcal{I}_K$; on le note h_K.*

Ainsi, $h_K = 1$ signifie exactement que $\mathbb{Z}_K$ est un anneau principal. L'ensemble $\mathcal{I}_K$ possède une structure de monoïde commutatif, associatif et unitaire donnée par le produit des idéaux : si I et J sont des idéaux, l'idéal IJ est l'idéal engendré par les produits ab, où $a \in I$ et $b \in J$. La commutativité vient de ce que $IJ = JI$, l'associativité de la relation $(II')I'' = I(I'I'')$; enfin, l'élément neutre est l'idéal $\mathbb{Z}_K$.

En outre, la relation d'équivalence introduite ci-dessus est compatible au produit des idéaux : si $I \sim I'$ et $J \sim J'$, alors $IJ \sim I'J'$ (en effet, choisissons a, a', b, b' dans $\mathbb{Z}_K$, non nuls, tels que $aI = a'I'$ et $bJ = b'J'$; alors, $abIJ = (aI)(bJ) = (a'I')(b'J') = a'b'I'J'$).

L'ensemble quotient $\mathcal{C}_K$ hérite donc d'une structure de monoïde commutatif, associatif et unitaire.

Le but de ce paragraphe est d'élucider la structure des monoïdes $\mathcal{I}_K$ et $\mathcal{C}_K$.

Théorème 8.19. *(i) Le monoïde $\mathcal{C}_K$ est un groupe fini.*
(ii) Dans le monoïde $\mathcal{I}_K$, tout élément est simplifiable : si I, I', J sont des idéaux non nuls de $\mathbb{Z}_K$ tels que $IJ = I'J$, alors $I = I'$.

On démontre ce théorème par une série de lemmes.

Lemme 8.20. *Soit I et J des idéaux non nuls de $\mathbb{Z}_K$ et soit a un élément non nul de $\mathbb{Z}_K$. On suppose que $IJ = aJ$. Alors, $I = (a)$.*

Démonstration : soit $z \in I$, posons $w = z/a$ et démontrons que $w \in \mathbb{Z}_K$. On remarque que $wJ \subset J$. Soit $(z_1, \ldots, z_n)$ une base de J. écrite dans cette base, la matrice M_w de l'endomorphisme

de multiplication par w est donc à coefficients entiers ; si P désigne le polynôme caractéristique de M_w, on a donc $P(w) = 0$ donc w est un entier algébrique. Par conséquent, $w \in \mathbb{Z}_K$. Ainsi, $I \subset (a)$.

Pour démontrer l'autre inégalité, notons I' le sous-ensemble $a^{-1}I$ de $\mathbb{Z}_K$ et prouvons que $I' = \mathbb{Z}_K$. Il est clair que I' est un idéal tel que $I'J = J$. Il existe donc des éléments $a_{i,j} \in I'$ tels que $z_j = \sum_{i=1}^{n} a_{i,j} z_i$. Notant $Q = X^n + q_1 X^{n-1} + \cdots + q_n$ le polynôme caractéristique de la matrice $(a_{i,j})$, le théorème de Cayley-Hamilton (ou la définition d'une valeur propre) entraîne que $Q(1) = 0$. Comme les q_i appartiennent à l'idéal I', cela entraîne que $1 \in I'$, d'où $I' = \mathbb{Z}_K$, ce qu'il fallait démontrer.

Lemme 8.21. *Pour tout idéal non nul I de A, il existe un entier t tel que $1 \leq t \leq h_K$ et tel que l'idéal I^t soit un idéal principal.*

Démonstration : parmi les $h_K + 1$ idéaux, $\mathbb{Z}_K, I, \ldots, I^{h_K}$, deux au moins ont même classe dans $\mathcal{C}_K$, disons I^m et I^{m+p}, avec $0 \leq m < m + p \leq h_K$. Il existe donc des éléments non nuls a et b dans $\mathbb{Z}_K$ tels que $aI^m = bI^{m+p}$, ce qu'on écrit $bI^p I^m = aI^m$. D'après le lemme précédent, $bI^p = (a)$ et I^p est principal.

Démonstration du théorème : (i) tout d'abord, le monoïde $\mathcal{C}_K$ est commutatif, associatif et unitaire. D'après le lemme précédent, tout élément de $\mathcal{C}_K$ possède un inverse. Cela signifie que $\mathcal{C}_K$ est un groupe abélien. Il est fini d'après la proposition ci-dessus.

(ii) Soient I, I', J des idéaux non nuls de $\mathbb{Z}_K$ tels que $IJ = I'J$; démontrons que $I = I'$. Soit J' un idéal non nul de $\mathbb{Z}_K$ tel que JJ' soit un idéal principal, disons (a), avec $a \in \mathbb{Z}_K$. Alors, $IJJ' = I'JJ'$, d'où $aI = aI'$. Multipliant cette égalité par a^{-1} , on a $I = I'$.

8.5 Factorisation

Nous démontrons dans ce paragraphe que les anneaux d'entiers de corps de nombres jouissent d'une propriété très proche de celle des anneaux factoriels : les idéaux d'un tel anneau se décomposent de manière unique en produit d'idéaux maximaux.

On conserve les notations précédentes : K est un corps de nombres de degré n, $\mathcal{I}_K$ est le monoïde des idéaux non nuls de l'anneau des entiers $\mathbb{Z}_K$ et $\mathcal{C}_K$ est le groupe des classes d'idéaux.

Commençons par un lemme qui relie les relation d'inclusion et de divisibilité dans les idéaux. Si un idéal I est produit de deux idéaux J et J', alors I est contenu dans J.

Lemme 8.22. *Soient I et J deux idéaux non nuls de $\mathbb{Z}_K$. Pour que $I \subset J$, il faut et il suffit qu'il existe un idéal J' de $\mathbb{Z}_K$ tel que $I = JJ'$.*

Démonstration : supposons d'abord $I = JJ'$. Cela signifie que I est l'idéal engendré par les produits ab, avec $a \in J$ et $b \in J'$. Chacun de ces produits ab est contenu dans J, par définition d'un idéal. Donc l'idéal qu'ils engendrent est aussi contenu dans J, c'est-à-dire $I \subset J$.

Pour la réciproque, nous devrons utiliser l'hypothèse que K est un anneau d'entiers de corps de nombres. Soit J_1 un idéal non nul de $\mathbb{Z}_K$ tel que l'idéal JJ_1 soit un idéal principal ; soit alors $\alpha \in \mathbb{Z}_K$ un générateur de l'idéal JJ_1, de sorte que $JJ_1 = (\alpha)$. Comme $I \subset J$, on a $IJ_1 \subset JJ_1 = \alpha\mathbb{Z}_K$. La partie $\alpha^{-1}IJ_1$ de K est donc contenue dans $\mathbb{Z}_K$ et est un idéal de $\mathbb{Z}_K$. Notons-la J'. On a donc

$\alpha J' = IJ_1$. Multiplions cette égalité par l'idéal J ; on trouve $\alpha JJ' = IJ_1J = I(\alpha) = \alpha I$. On peut alors simplifier par α (qui n'est pas nul), d'où l'égalité $JJ' = I$, ce qui démontre le lemme.

Théorème 8.23. *(i) Tout idéal non nul de $\mathbb{Z}_K$ est produit d'idéaux maximaux.*
(ii) Si $P_1, \dots, P_t$ et $Q_1, \dots, Q_s$ sont des idéaux maximaux de $\mathbb{Z}_K$ tels que $P_1 \dots P_t = Q_1 \dots Q_s$, alors $t = s$ et il existe une permutation σ de $\{1, \dots, t\}$ telle que $Q_i = P_{\sigma(i)}$ pour tout i.

Démonstration : (i) Soit I un idéal non nul de $\mathbb{Z}_K$. Démontrons par récurrence sur $\mathrm{N}(I)$ qu'il existe des idéaux maximaux $P_1, \dots, P_t$ de $\mathbb{Z}_K$ tels que $I = P_1 \dots P_t$. Supposons le résultat vrai pour les idéaux de norme $< \mathrm{N}(I)$. Si $\mathrm{N}(I) = 1$, c'est-à-dire $I = \mathbb{Z}_K$, on prend $t = 0$ (produit vide). Sinon, $I \neq \mathbb{Z}_K$ et il existe d'après le corollaire 8.13 un idéal maximal P_1 de $\mathbb{Z}_K$ tel que $I \subset P_1$. D'après le lemme précédent, il existe un idéal I_1 de $\mathbb{Z}_K$ tel que $I = P_1 I_1$. On a $I \subset I_1$; si l'on avait $I = I_1$, on aurait alors $P_1 = \mathbb{Z}_K$ d'après le corollaire ci-dessus, ce qui est absurde. Par suite, $I \subsetneq I_1$ et $\mathrm{N}(I_1) < \mathrm{N}(I)$. Par récurrence, il existe des idéaux maximaux $P_2, \dots, P_t$ de $\mathbb{Z}_K$ tels que $I_1 = P_2 \dots P_t$ et $I = P_1 I_1 = P_1 P_2 \dots P_t$.

(ii) Démontrons le résultat voulu par récurrence sur t. Posons $I = P_1 \dots P_t = Q_1 \dots Q_s$. Si $t = 0$, $I = \mathbb{Z}_K$. Si l'on avait $s > 0$, on aurait $I \subset Q_1 \subsetneq \mathbb{Z}_K$, d'où une contradiction, on a donc $s = 0$.

Supposons maintenant $t > 0$. Par hypothèse, $Q_1 \dots Q_s \subset P_t$. D'après le lemme ci-dessous, il existe un entier $j \in \{1, \dots, s\}$ tel que $Q_j \subset P_t$, d'où $Q_j = P_t$ car Q_j est un idéal maximal de $\mathbb{Z}_K$. Quitte à renuméroter les Q_i, on peut supposer que $j = s$. Posons alors $I_1 = P_1 \dots P_{t-1}$ et $I_1' = Q_1 \dots Q_{s-1}$; on a $I_1 P_t = I_1' Q_s$, d'où $I_1 = I_1'$ d'après le corollaire ci-dessus. Par récurrence, $s-1 = t-1$ et il existe une permutation σ_1 de $\{1, \dots, t-1\}$ tel que $Q_i = P_{\sigma_1(i)}$ pour tout $i \in \{1, \dots, s-1\}$. On a donc $t = s$; prolongeons σ en une permutation de $\{1, \dots, t\}$ en posant $\sigma(i) = \sigma_1(i)$ pour $i \in \{1, \dots, t-1\}$ et $\sigma(t) = t$. On a ainsi $Q_i = P_{\sigma(i)}$ pour $i \in \{1, \dots, t\}$.

Lemme 8.24. *Soit Q un idéal premier de $\mathbb{Z}_K$ et $I_1, \dots, I_n$ des idéaux de $\mathbb{Z}_K$ tels que $I_1 \dots I_n \subset Q$. Il existe un entier $j \in \{1, \dots, n\}$ tel que $I_j \subset Q$.*

Démonstration : le cas $n = 0$ ne se produit pas car l'hypothèse entraînerait $\mathbb{Z}_K \subset Q$ et donc $Q = \mathbb{Z}_K$, contrairement à l'hypothèse de primalité pour Q. Si $n = 1$, il suffit de poser $j = 1$.

Par récurrence, il suffit alors de traiter le cas où $n = 2$. Si $I_1 \not\subset Q$ et $I_2 \not\subset Q$, choisissons des éléments $a_1 \in I_1$ et $a_2 \in I_2$ qui n'appartiennent pas à Q. Comme Q est un idéal premier de $\mathbb{Z}_K$, $a_1 a_2 \notin Q$. Mais $a_1 a_2$ appartient à $I_1 I_2$, par définition de l'idéal produit, donc appartient à Q puisque $I_1 I_2 \subset Q$. Cette contradiction démontre que $I_1 \subset Q$ ou $I_2 \subset Q$.

Corollaire 8.25. *Posons $c = (2/\pi)^{r_2} \sqrt{|\mathrm{Disc}(K)|}$. Le groupe $\mathcal{C}_K$ est engendré par les classes d'idéaux maximaux de $\mathbb{Z}_K$ contenant un entier $\leq c$. En particulier, pour que $\mathbb{Z}_K$ soit un anneau principal, il faut et il suffit que les idéaux maximaux contenant un eniter $\leq c$ soient principaux.*

Démonstration : posons $c = (2/\pi)^{r_2} \sqrt{|\mathrm{Disc}(K)|}$. D'après la proposition du paragraphe précédent, tout idéal non nul I de $\mathbb{Z}_K$ est équivalent à un idéal J contenant un entier $a \leq c$. Décomposons alors J en produit d'idéaux maximaux, disons $J = P_1 \dots P_t$; pour tout j, $J \subset P_j$ donc $a \in P_j$. Par suite, la classe de J, et donc celle de I, appartient au sous-groupe de $\mathcal{C}_K$ engendré par les idéaux maximaux de $\mathbb{Z}_K$ contenant un entier $\leq c$. Le corollaire est ainsi démontré.

Remarque 8.26. *La condition I contient un entier $\leq c$ entraîne que $N(I) \leq c^{[K:\mathbb{Q}]}$ (exercice).*

Remarque 8.27. *On peut raisonner légèrement différemment et obtenir directement un peu mieux (sans grand importance puisque seule la finitude compte). Soit I un idéal et $0 \neq \alpha \in I$. Ecrivons $I = \prod_{i=1}^{m} \mathfrak{P}_i^{a_i}$ et $(\alpha) = \prod_{i=1}^{m} \mathfrak{P}_i^{b_i}$, comme $\alpha \in I$, $0 \leq a_i \leq b_i$ pour tout i. Posons $I^\star = \prod_{i=1}^{m} \mathfrak{P}^{b_i - a_i}$, c'est un idéal de $\mathbb{Z}_K$ et on a $II^\star = (\alpha)$ est principal. Soit $\gamma \in I^\star$; comme $(\gamma) \subset I^\star$, il existe J idéal de $\mathbb{Z}_k$ tel que*

$$(\gamma) = I^\star J \ .$$

Donc,

$$(\gamma)I = II^\star J = (\alpha)J \ .$$

Donc, les idéaux I et J sont équivalents. Par ailleurs (on utilise la multiplicativité des normes d'idéaux)

$$N(J)N(I^\star) = N(\gamma) \ .$$

On choisit maintenant γ tel que $N(\gamma) \leq cN(I^\star)$ (c'est possible grâce au corollaire 8.14 précédent) et l'on en déduit que I est équivalent à un idéal J de norme

$$\leq c \ .$$

Corollaire 8.28. *Soit K un corps de nombres. Si l'anneau d'entiers $\mathbb{Z}_K$ est un anneau factoriel, c'est un anneau principal.*

Démonstration : soit P un idéal maximal de $\mathbb{Z}_K$. Soit a un élément non nul de P tel que $|\mathrm{N}K(a)|$ soit minimal et observons que a est un élément irréductible. Soit en effet une factorisation $a = a_1 a_2$ de a en produit d'éléments de $\mathbb{Z}_K$. Comme P est un idéal maximal, on a donc $a_1 \in P$ ou $a_2 \in P$; supposons pour fixer les idées que $a_1 \in P$ et démontrons que a_2 est un élément inversible de $\mathbb{Z}_K$. Compte-tenu de l'égalité $\mathrm{N}_K(a) = \mathrm{N}_K(a_1)\mathrm{N}_K(a_2)$ et de l'inégalité $|\mathrm{N}_K(a_2)| \geq 1$, la minimalité de $|\mathrm{N}_K(a)|$ entraîne que $|\mathrm{N}_K(a_1)| = |\mathrm{N}_K(a)|$, d'où $|\mathrm{N}_K(a_2)| = 1$. Par suite, a_2 est un élément inversible de $\mathbb{Z}_K$, ce qu'il fallait démontrer.

Comme $\mathbb{Z}_K$ est un anneau factoriel, l'idéal (a) engendré par a est un idéal premier, non nul puisque $a \neq 0$, donc maximal. L'inclusion évidente $a\mathbb{Z}_K \subset P$ entraîne alors que $P = a\mathbb{Z}_K$, autrement dit P est un idéal principal.

D'après le corollaire précédent, tout idéal non nul de $\mathbb{Z}_K$ est principal et $\mathbb{Z}_K$ est un anneau principal.

8.6 Quelque exemples

Voyons des exemples comment utiliser les résultats précédents pour déterminer la structure du groupe de classes d'idéaux.

Nous aurons besoin, un nombre entier naturel n étant donné, de trouver explicitement tous les idéaux maximaux de norme n. Faisons pour cela quelques remarques générales. Soit K un corps de nombres et $\mathbb{Z}_K$ son anneau d'entiers. Soit P un idéal maximal de $\mathbb{Z}_K$.

(i) L'anneau quotient $\mathbb{Z}_K/P$ est un corps fini ; son cardinal est donc une puissance d'un nombre premier p. On peut donc supposer que n est de la forme p^f.

(ii) Comme le corps $\mathbb{Z}_K/P$ est de caractéristique p, p est nul dans ce corps et l'on a $p \in P$.

(iii) Supposons que l'on connaisse un entier algébrique α de K tel que $\mathbb{Z}_K = \mathbb{Z}[\alpha]$; soit A le polynôme minimal de α ; l'anneau $\mathbb{Z}_K$ est donc isomorphe à $\mathbb{Z}[X]/(A(X))$. L'image réciproque I dans $Z[X]$ de l'idéal P est un idéal de $\mathbb{Z}[X]$ qui contient p et $A(X)$; on a en outre un isomorphisme d'anneaux $\mathbb{Z}_K/P \simeq \mathbb{Z}[X]/I$. Soit J l'image de I dans l'anneau $\mathbb{F}_p[X]$ par l'homomorphisme de réduction modulo p ; c'est un idéal de $\mathbb{F}_p[X]$ car cet homomorphisme est surjectif ; il existe donc un polynôme $R \in \mathbb{F}_p[X]$ tel que $J = (R(X))$. De plus, on a un isomorphisme d'anneaux $\mathbb{Z}[X]/I \simeq \mathbb{F}_p[X]/(R(X))$; par suite, R est un polynôme irréductible de $\mathbb{F}_p[X]$. Comme $A(X)$ appartient à I, sa réduction modulo p appartient à $J = (R(X))$ ce qui entraîne que R divise A. En remontant les calculs et en notant $\tilde{R}$ un polynôme de $\mathbb{Z}[X]$ arbitraire dont la réduction modulo p est égale à R, on a $P = (p, \tilde{R}(\alpha))$. Inversement, par cette formule, tout facteur irréductible R de A mod p définit un idéal maximal de $\mathbb{Z}_K$ de caractéristique p.

(iv) Avec les notations précédentes, le corps fini $\mathbb{Z}_K/P$ est isomorphe à $\mathbb{F}_p[X]/(R(X))$. On a donc $N(P) = p^{\deg(R)}$.

Récapitulons : les idéaux maximaux de $\mathbb{Z}_K$ contenant un nombre premier p sont en bijection avec les facteurs irréductibles de degré f du polynôme $A(X)$ mod p.

Exemple 8.29. *Soit $P = X^3 + X + 1$; comme $P' = 3X^2 + 1$, P définit une fonction strictement croissante sur $\mathbb{R}$ et a donc une unique racine réelle, α. Posons $K = Q(\alpha)$. C'est un corps de nombres de degré 3 ; on a $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ et $\mathrm{Disc}(K) = -31$. Comme P possède une seule racine réelle, on a $r_1 = r_2 = 1$. Posons alors $c = (2/\pi)^{r_2}\sqrt{|\mathrm{Disc}(K)|}$; on a $c \approx 3,5$. Par conséquent, le groupe des classes C_K est engendré par les idéaux maximaux de $\mathbb{Z}_K$ de normes 2 ou 3. Soit M un idéal maximal contenant 2. Sur $\mathbb{F}_2$, le polynôme P n'a pas de racine ; come il est de degré 3, P est irréductible modulo 2. Par suite, $M = (2)$ et $N(M) = 8$.*

Soit maintenant M un idéal maximal contenant 3. Sur $\mathbb{F}_3$, 1 est racine de P et l'on a $P = (X-1)(X^2+X-1)$, le polynôme X^2+X-1 étant irréductible. On a donc deux cas :

(i) soit $M = (3, \alpha - 1)$ et alors $N(M) = 3$;

(ii) soit $M = (3, \alpha^2 + \alpha - 1)$ et $N(M) = 9$.

Cela démontre que $\mathcal{C}_K$ est engendré par la classe de l'idéal $M = (3, \alpha - 1)$. Comme $N_K(1-\alpha) = P(1) = 3 = N(M)$, $1 - \alpha$ est un générateur de M. Par suite, l'anneau $\mathbb{Z}_K$ est principal.

Exemple 8.30. *Soit K le corps quadratique $\mathbb{Q}(\sqrt{-5})$; on a $\mathbb{Z}_K = Z[\sqrt{-5}]$ et $\mathrm{Disc}(\mathbb{Z}_K) = -20$. Le groupe des classes $\mathcal{C}_K$ est donc engendré par les idéaux maximaux de $\mathbb{Z}_K$ de norme $\leq (2/\pi)\sqrt{20} \approx 2,8$, autrement dit par les idéaux maximaux de $\mathbb{Z}_K$ de norme 2.*

Déterminons ces derniers ; le polynôme minimal de $\sqrt{5}$ est égal à $X^2 + 5$ et l'on a $X^2 + 5 \equiv (X + 1)^2 \bmod 2$. Ainsi, le seul idéal maximal de $\mathbb{Z}_K$ qui contienne 2 est l'idéal $M = (2, 1 + \sqrt{-5})$; sa norme est effectivement 2.

Il nous rest à voir si cet idéal est ou non principal. Cherchons pour cela un élément de norme 2 dans M. Si $z = x + y\sqrt{-5}$, $N_K(z) = x^2 + 5y^2$. Par suite, si $y \neq 0$, on a $|N_K(z)| = x^2 + 5y^2 \geq 5$; l'égalité $NK(z) = \pm 2$ entraîne donc $z \in \mathbb{Z}$, mais alors $N_K(z) = z^2$ n'est pas égale à ± 2. Par conséquent, l'idéal $M = (2, 1 + \sqrt{-5})$ n'est pas principal.

L'idéal M^2 est engendré par $4, 2(\alpha + 1)$ et $(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha - 4$. On a alors $M^2 = (4, 2\alpha + 2, 2\alpha - 4) = (4, 2\alpha + 2, 2\alpha) = (4, 2\alpha, 2) = (2, 2\alpha) = (2)$ ce qui démontre que M^2 est un idéal principal. Par conséquent, le groupe des classes d'idéaux de l'anneau $\mathbb{Z}_K$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$et la classe de l'idéal $(2, 1\sqrt{-5})$ en est un générateur.

8.7 Multiplicativité des normes des idéaux

Lemme 8.31. *Soient I et J des idéaux non nuls de $\mathbb{Z}_K$ tels que $I + J = \mathbb{Z}_K$. On a $N(IJ) = N(I)N(J)$.*

Démonstration : soit φ l'application de $\mathbb{Z}_K$ dans $(\mathbb{Z}_K/I)\times(\mathbb{Z}_K/J)$ telle que $\varphi(a) = (\mathrm{cl}_I(a), \mathrm{cl}_J(a))$ pour $a \in \mathbb{Z}_K$. C'est un homomorphisme d'anneaux. Démontrons qu'il est surjectif. Soient a et b des éléments de I et J respectivement tels que $1 = a + b$. Si $z \in \mathbb{Z}_K$, on a donc $\mathrm{cl}_I(az) = 0$, $\mathrm{cl}_J(bz) = 0$ tandis que $\mathrm{cl}_I(bz) = \mathrm{cl}_I((1-a)z) = \mathrm{cl}_I(z)$ et $\mathrm{cl}_J(az) = \mathrm{cl}_J(z)$. Par suite, si $z, w \in \mathbb{Z}_K$, $\varphi(bz + aw) = (\mathrm{cl}_I(z), \mathrm{cl}_J(w))$. Cela entraîne que φ est surjectif.

Soit z un élément du noyau de φ, c'est-à-dire un élément de $I \cap J$. Écrivons $z = z(a+b) = az + bz$: comme $z \in J$, il vient $az \in IJ$; comme $z \in I$, on a $bz \in IJ$; en déduit que z appartient à IJ. Inversement, si $z \in IJ$, on a $z \in I$ et $z \in J$, donc $\varphi(z) = 0$.

Il résulte de φ un isomorphisme d'anneaux de $\mathbb{Z}_K/IJ$ sur $(\mathbb{Z}_K/I)\times(\mathbb{Z}_K/J)$. En particulier, $N(IJ)$, qui est le cardinal de $\mathbb{Z}_K/IJ$, est égal au produit de $N(I)$ par $N(J)$.

Lemme 8.32. *Soit P un idéal maximal de $\mathbb{Z}_K$. Pour tout entier naturel e, on a $N(P^e) = N(P)^e$.*

Démonstration : on démontre ce résultat par récurrence sur e. De la suite d'idéaux $P^{e+1} \subset P^e \subset \mathbb{Z}_K$, on déduit une égalité de cardinaux

$$\mathrm{Card}(\mathbb{Z}_K/P^{e+1}) = \mathrm{Card}(\mathbb{Z}_K/P^e)\mathrm{Card}(P^e/P^{e+1})$$

et il suffit de démontrer que $\mathrm{Card}(P^e/P^{e+1}) = \mathrm{Card}(\mathbb{Z}_K/P)$.

Soit a un élément de P^e qui n'appartient pas à P^{e+1} ; il en existe car si l'on avait $P^e = P^{e+1}$, l'idéal P^e aurait deux décompositions distinctes en produit d'idéaux maximaux, à savoir P^e et P^{e+1}.

Soit $\varphi : \mathbb{Z}_K \longrightarrow P^e/P^{e+1}$ l'application telle que $\varphi(z) = \mathrm{cl}_{P^{e+1}}(az)$. C'est un homomorphisme de groupes abéliens ; son noyau Q est un sous-groupe de P^e ; c'est même un idéal de $\mathbb{Z}_K$ car si $z \in Q$ et $\lambda \in \mathbb{Z}_K$, $\varphi(\lambda z) = \mathrm{cl}(a\lambda z) = \lambda \mathrm{cl}(az) = 0$. En outre, Q contient P. Cependant, $\varphi(1) = \mathrm{cl}(a) \neq 0$, donc $Q \neq \mathbb{Z}_K$. Les inclusions $P \subset Q \subsetneq \mathbb{Z}_K$ et l'hypothèse que P est un idéal maximal de $\mathbb{Z}_K$ entraînent alors $Q = P$.

Démontrons que φ est surjectif. Soit J l'idéal $P^{e+1} + (a)$. Il contient P^{e+1} donc il existe un idéal J' de $\mathbb{Z}_K$ tel que $P^{e+1} = JJ'$. La décomposition de J en produit d'idéaux maximaux est donc de la forme $J = P^f$, où f est un entier naturel tel que $0 \leq f \leq e+1$. De plus, J est contenu dans P^e (car P^{e+1} et (a) le sont), donc $f \geq e$. Toutefois, J n'est pas égal à P^{e+1} car $a \notin P^{e+1}$; ainsi, $f \neq e+1$. On a donc $f = e$ et $J = P^e$.

Soit $x \in P^e$; démontrons que $\mathrm{cl}(x)$ appartient à l'image de φ. Comme $x \in J = P^{e+1} + (a)$, il existe donc $z \in P^{e+1}$ et $w \in \mathbb{Z}_K$ tels que $x = z + aw$; alors $\mathrm{cl}(x) = \mathrm{cl}(z) + \mathrm{cl}(aw) = \varphi(w)$, comme il fallait démontrer, et φ est surjective.

Par conséquent, $\mathbb{Z}_K/P$ est un groupe abélien isomorphe à P^e/P^{e+1}. En particulier, $N(P) = \mathrm{Card}(\mathbb{Z}_K/P) = \mathrm{Card}(P^e/P^{e+1})$. Par récurrence,

$$N(P^{e+1}) = \mathrm{Card}(\mathbb{Z}_K/P^e)\mathrm{Card}(P^e/P^{e+1}) = N(P)^{e+1} \ ,$$

d'où le lemme.

Théorème 8.33. *Soit I et J des idéaux non nuls de $\mathbb{Z}_K$. On a l'égalité $N(IJ) = N(I)N(J)$.*

Démonstration : écrivons $I = P_1^{m_1} \dots P_t^{m_t}$ la décomposition de l'idéal I en produits d'idéaux maximaux, où on suppose que $P_1, \dots, P_t$ sont deux à deux distincts. Nous allons démontrer l'égalité

$$N(I) = N(P_1)^{m_1} \dots N(P_t)^{m_t} \ ;$$

le théorème en découlera en appliquant cette égalité ainsi que les deux égalités analogues pour $N(J)$ et $N(IJ)$.

Lorsque $t = 1$, l'assertion résulte du lemme précédent. On raisonne en général par récurrence sur t. Posons en effet $I_1 = P^{m_1}$, $I_2 = P_2^{m_2} \dots P_t^{m_t}$. Vérifions que $I_1 + I_2 = \mathbb{Z}_K$. Comme $P_1^{m_1} \subset I_1 + I_2$, il existe un entier e tel que $0 \leq e \leq m_1$ de sorte que $I_1 + I_2 = P_1^e$. Par construction, I_2 n'est pas contenu dans P_1 (sinon, P_1 apparaîtrait dans la décomposition de I_2 en produit d'idéaux maximaux) ; en particulier, $I_1 + I_2$ n'est pas contenu dans P_1 ce qui entraîne $e = 0$. Autrement dit, $I_1 + I_2 = \mathbb{Z}_K$.

D'après le lemme ci-dessus, $N(I) = N(I_1 I_2) = N(I_1)N(I_2)$; par récurrence, on a aussi $N(I_2) = N(P_2)^{m_2} \dots N(P_t)^{m_t}$, tandis que le cas $t = 1$ implique $N(I_1) = N(P_1)^{m_1}$. L'égalité voulue en résulte, d'où le théorème.

9 Géométrie des nombres

9.1 Formes quadratiques binaires

Dans ce paragraphe, nous présentons quelques résultats classiques concernant la théorie arithmétique des formes quadratiques en deux variables. La motivation essentielle de cette étude est de trouver des conditions nécessaires ou suffisantes pour qu'un entier n s'écrive sous la forme $ax^2+bxy+cy^2$, pour $(x,y) \in \mathbb{Z}^2$, où a, b, c sont des nombres entiers fixés. Nous allons voir que le résultat est intimement lié à l'ensemble des formes quadratiques qu'on obtient à partir de $ax^2 + bxy + cy^2$ par changement de variables dans $\mathrm{SL}_2(\mathbb{Z})$.

Le Minimum d'une forme quadratique binaire :

Soit $q(x,y) = ax^2 + bxy + cy^2$ une forme quadratique en deux variables, à coefficients (a,b,c) réels. Son discriminant est défini par la formule $D = b^2 - 4ac$; il s'agit du discriminant au sens des polynômes du second degré, c'est-à-dire -4 fois le déterminant de la matrice $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ de la forme quadratique q. On dit que q est non dégénérée si $D \neq 0$. On dit que q est définie positive si $q(x,y) > 0$ pour tout couple (x,y) de nombres réels distinct de $(0,0)$; cela équivaut aux inégalités $a > 0$ et $D < 0$.

Théorème 9.1. *Soit $q(x,y) = ax^2 + bxy + cy^2$ une forme quadratique définie positive, de discriminant $D = b^2 - 4ac < 0$. Alors, il existe un couple $(x,y) \in \mathbb{Z}^2$, distinct de $(0,0)$, tel que*

$$0 < q(x,y) \leq \sqrt{|D|/3} \ .$$

Démonstration : comme q est définie positive, $a > 0$ et $D < 0$. La décomposition de Gauß

$$q(x,y) = a\left(x + \frac{b}{2a}y\right)^2 + \left(c - \frac{b^2}{4a}\right)y^2 = a\left(x + \frac{b}{2a}y\right)^2 - \frac{1}{4a}Dy^2$$

montre que $q(x,y)$ tend vers l'infini quand x ou y tend vers l'infini. Par suite, $q(x,y)$ atteint sa borne inférieure sur l'ensemble $\mathbb{Z}^2 \setminus \{(0,0)\}$; soit $(\xi,\eta) \in \mathbb{Z}^2$ un couple non nul où q soit minimale.

Observons que ξ et η sont premiers entre eux. En effet, si d désigne leur pgcd, on a $q(\xi,\eta) = d^2 q(\xi/d, \eta/d)$ et $(\xi/d, \eta/d)$ est un couple en lequel q prend la valeur $q(\xi,\eta)/d^2$ qui est $< q(\xi,\eta)$ si $d \neq 1$. D'après le théorème de Bézout, il existe donc des entiers u et v tels que $u\xi - v\eta = 1$. Faisons dans q le changement de variables

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \xi & v \\ \eta & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \ .$$

Comme la matrice $\begin{pmatrix} \xi & v \\ \eta & u \end{pmatrix}$ est dans $\mathrm{Mat}_2(\mathbb{Z})$, elle induit une application de $\mathbb{Z}^2$ dans lui-même ; puisque son déterminant est égal à 1, son inverse est aussi dans $\mathrm{Mat}_2(\mathbb{Z})$ et ce changement de variables induit un automorphisme du groupe abélien $\mathbb{Z}^2$. Après ce changement de variables, q

s'écrit $q(x,y) = Q(X,Y) = AX^2 + BXY + CY^2$, avec $A = q(\xi,\eta)$. De plus, le discriminant de la forme Q est égal à celui de q car le déterminant du changement de variables est de carré 1. Effectuons alors une réduction de Gauß en écrivant

$$Q(X,Y) = A\left(X + \frac{B}{2A}Y\right)^2 - \frac{1}{4A}DY^2 \ .$$

Par hypothèse, $Q(X,Y) \geq A$ si $(X,Y) \neq (0,0)$. Prenons par exemple $Y = 1$ et choisissons $X \in \mathbb{Z}$ de sorte que $\left|X + \frac{B}{2A}Y\right| \leq \frac{1}{2}$; il suffit de prendre pour X l'entier le plus proche de $-B/2A$. Comme $D < 0$, on obtient

$$Q(X,Y) \leq \frac{1}{4}A + \frac{1}{4A}|D| \ ,$$

d'où, puisque $Q(X,Y) \geq A$, l' inégalité $\frac{3A}{4} \leq \frac{D}{4A}$, soit encore $A^2 \leq D/3$, ce qu'il fallait démontrer. Voyons-en tout de suite quelques applications.

Proposition 9.2. *(i) Pour qu'un nombre premier p s'écrive sous la forme $x^2 + y^2$, avec $(x,y) \in \mathbb{Z}^2$, il faut et il suffit que $p = 2$ ou $p \equiv 1 \bmod 4$.*

(ii) Pour qu'un nombre premier p s'écrive sous la forme $x^2 + 2y^2$, avec $(x,y) \in \mathbb{Z}^2$, il faut et il suffit que $p = 2$ ou que p soit congru à 1 ou 3 modulo 8.

(iii) Pour qu'un nombre premier p s'écrive sous la forme $x^2 + 3y^2$, avec $(x,y) \in \mathbb{Z}^2$, il faut et il suffit que $p = 3$ ou $p \equiv 1 \bmod 3$.

Démonstration : (i) Si $p = x^2 + y^2$, x et y ne sont pas multiples de p (si p divise x, alors p divise $y^2 = px^2$, donc p divise y et p^2 divise aussi $p = x^2 + y^2$, ce qui est absurde). On a alors $x^2 \equiv -y^2$ dans $\mathbb{Z}/p\mathbb{Z}$ et le quotient x/y vérifie $(x/y)^2 \equiv -1 \bmod p$; autrement dit, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et cela entraîne $p = 2$ ou $p \equiv 1 \bmod 4$.

Établissons la réciproque. On a déjà $2 = 1^2 + 1^2$; supposons maintenant que p soit congru à 1 modulo 4. Il existe alors un entier a tel que $a^2 \equiv -1 \bmod 4$; introduisons la forme quadratique $q(x,y) = x^2 + (ax + py)^2$ (c'est, après changement de variables, la restriction de la forme $x^2 + y^2$ à l'ensemble des couples (x,y) de $\mathbb{Z}^2$ qui vérifient $y \equiv a \bmod 4$). On a

$$q(x,y) = (1 + a^2)x^2 + 2apxy + p^2y^2$$

et le discriminant de q est égal à $4a^2p^2 - 4p^2(1 + a^2) = 4p^2$. D'après le théorème précédent, il existe un couple $(x,y) \in \mathbb{Z}^2$, non nul, tel que $q(x,y) \leq p\sqrt{4/3} < 2p$.

Puisque $(x,y) \neq (0,0)$, $q(x,y) \neq 0$. On a en outre $q(x,y) \equiv x^2(1 + a^2) \equiv 0 \bmod p$: $q(x,y)$ est multiple de p, or le seul multiple de p non nul inférieur à $p\sqrt{4/3}$ est p donc $q(x,y) = p$. En particulier, $p = x^2 + (ax + py)^2$ est somme de deux carrés d'entiers.

(ii) On a $2 = 0^2 + 2 \cdot 1^2$; supposons désormais que p soit impair. Supposons de plus $p = x^2 + 2y^2$, avec $(x,y) \in \mathbb{Z}^2$. Comme précédemment, y n'est pas multiple de p (sinon $0 \equiv x^2 \bmod p$, donc x serait aussi multiple de p et $p = x^2 + 2y^2$ serait multiple de p^2). Modulo p, la relation $p = x^2 + 2y^2$ devient alors $x^2 = -2y^2$ et x/y est une racine carrée de -2. D'après la loi de réciprocité quadratique, cela équivaut à $p \equiv 1, 3 \bmod 8$.

Pour démontrer la réciproque, introduisons la forme quadratique $q(x,y) = 2x^2 + (ax + py)^2$, où a est un entier tel que $a^2 \equiv -2 \bmod p$ (compte tenu de la loi de réciprocité quadratique, l'existence d'un tel entier provient de la congruence vérifiée par p). Son discriminant est $-8p^2$; il existe donc

un couple non nul $(x,y) \in \mathbb{Z}^2$ tel que $q(x,y) \leq p\sqrt{8/3} < 2p$. Par construction, $q(x,y) \equiv 0 \bmod p$ et $q(x,y) > 0$; nécessairement, $q(x,y) = p$ et $p = (ax+py)^2 + 2x^2$ est de la forme x^2+2y^2.

(iii) Supposons $p = x^2+3y^2$; alors p ne divise pas y puis -3 est un carré modulo p comme ci-dessus. D'après la loi de réciprocité quadratique, cela entraîne $p = 3$ ou $p \equiv 1 \bmod 3$.

Inversement, on a $3 = 0^2 + 3 \cdot 1^2$; lorsque $p \neq 3$, introduisons la forme quadratique $q(x,y) = 3x^2 + (ax+py)^2$, où a est un entier tel que $a^2 \equiv -3 \bmod p$. Le discriminant de cette forme est égal à $-12p^2$. Il existe ainsi un couple non nul $(x,y) \in \mathbb{Z}^2$ tel que $q(x,y) \leq p\sqrt{4 \cdot 3/3} = 2p$, d'où l'on déduit que $q(x,y) = p$ ou $q(x,y) = 2p$. Il faut exclure ce dernier cas. Or, si $2p = 3x^2 + (ax+py)^2$, il vient $(ax+py)^2 \equiv 2p \equiv 2 \bmod 3$, ce qui est absurde puisque 2 n'est pas un carré modulo 3. Nécessairement, $q(x,y) = p$ et p est de la forme x^2+3y^2.

C'est ici que la méthode atteint ses limites. Par exemple, il est facile de vérifier que 23 ne s'écrit pas sous la forme x^2+5y^2 bien que -5 soit un carré modulo 23.

9.2 Formes quadratiques réduites

Au paragraphe précédent, nous avons pu voir l'utilité d'écrire une forme quadratique $q(x,y) = ax^2+bxy+cy^2$ dans une autre base, le changement de base étant cependant donné par une matrice de $\mathrm{SL}_2(\mathbb{Z})$.

Nous dirons ainsi que deux formes quadratiques binaires q et q' sont équivalentes s'il existe une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$ telle que $q(x,y) = q'(A \cdot (x',y'))$.

Cette notion est évidemment une relation d'équivalence ; deux formes équivalentes ont même discriminant.

Nous dirons enfin qu'une forme définie positive $q(x,y) = ax^2+bxy+cy^2$, est réduite si ses coefficients vérifient $|b| \leq a \leq c$ et si l'on a de plus $b \geq 0$ si $c = a$ ou $a = |b|$.

Proposition 9.3. *Supposons que $q(x,y) = ax^2+bxy+cy^2$ soit une forme réduite et notons $D = b^2-4ac$ son discriminant. Alors, $a \leq \sqrt{D/3}$. De plus, pour tout couple $(x,y) \in \mathbb{Z}^2$ distinct de $(0,0)$ et $(\pm 1,0)$, on a $q(x,y) \geq a$. L'inégalité est toujours stricte à moins que l'on ne soit dans l'un des cas suivants :*

(i) On a l'égalité $c = a$ et $(x,y) = (0,\pm 1)$;

(ii) On a les égalités $c = a = b$ (autrement dit, q est multiple de la forme x^2+xy+y^2) et $(x,y) = \pm(1,1)$.

Démonstration : observons que l'on a les inégalités $b^2 \leq a^2 \leq ac$, d'où $3b^2 = 4b^2 - b^2 \leq -D$. De plus, $12ac = -3D + 3b^2 \leq -4D$ et, comme $a \leq c$, $a \leq \sqrt{D/3}$.

Par ailleurs, on a pour tout $(x,y) \in \mathbb{R}^2$ l'inégalité $|xy| \geq \min(x^2,y^2)$ si bien que pour tout $(x,y) \in \mathbb{Z}^2$ non nul,

$$q(x,y) \geq (a - |b| + c)\min(x^2,y^2) \ .$$

Si ni x ni y n'est nul, on en déduit que $q(x,y) \geq a - |b| + c \geq a$, l'égalité ne pouvant avoir lieu que si $a = c = |b|$; dans ce cas, $b \geq 0$, donc $a = b = c$ et $q(x,y) = a(x^2+xy+y^2)$ ne vaut a que pour les couples $(x,y) = \pm(1,1)$, $(x,y) = \pm(0,1)$ et $(x,y) = \pm(1,0)$. Si $x = 0$ (mais $y \neq 0$), on a $q(x,y) = cy^2 \geq c$, l'égalité n'ayant lieu que si $c = a$, en le couple $(x,y) = \pm(0,1)$; si $y = 0$ (mais $x \neq 0$), on a $q(x,y) = ax^2 \geq a$, avec égalité pour $(x,y) = \pm(1,0)$.

L'intérêt de la notion de forme réduite provient du théorème suivant, dû à Gauß.

Théorème 9.4. *Toute forme quadratique définie positive est équivalente à une forme réduite et une seule.*

Démonstration : soit q une forme quadratique définie positive. Comme dans la démonstration du théorème ci-dessus, on peut, quitte à effectuer un changement de base dans $\mathrm{SL}_2(\mathbb{Z})$, supposer que $q(1,0)$ est le minimum des valeurs de q aux couples non nuls $(x,y) \in \mathbb{Z}^2$; cela modifie q en une forme équivalente, disons $ax^2+2bxy+cy^2$. Pour $u \in \mathbb{Z}$, écrivons alors

$$\begin{aligned} q(x,y) &= a(x+uy)^2 + (b-2au)xy + (c-au^2)y^2 \\ &= a(x+uy)^2 + (b-2au)(x+uy)y + c'y^2 \ , \end{aligned}$$

avec $c' = q(-u,1) = au^2 - bu + c$. Le changement de variables $x' = x+uy$, $y' = y$ est dans $\mathrm{SL}_2(\mathbb{Z})$; en choisissant u égal à l'entier le plus proche de $b/2a$ (choisi inférieur à $b/2a$ s' il y en a deux), on se ramène au cas où l'on a de plus $-a < b \leq a$. Comme a est le minimum de q, on a aussi $a \leq q(0,1) = c$, d'où les inégalités $|b| \leq a \leq c$.

Si $|b| = a$, on a de plus l'inégalité $b \geq 0$. Supposons que l'on ait $a = c$, c'est-à-dire que q soit équivalente à $ax^2+bxy+ay^2$ mais que $b < 0$. Comme le changement de variables $x = y'$ et $y = -x'$ transforme cette dernière forme en $ax^2-bxy+ay^2$, on voit que q est aussi équivalente à $ax^2-bxy+ay^2$ qui est une forme réduite.

9.3 Représentation des nombres premiers par des formes réduites

Nous pouvons maintenant aborder le problème de la représentation d'un nombre premier par une forme quadratique binaire, définie positive et à coefficients entiers, c'est-à-dire de la forme $q(x,y) = ax^2+bxy+cy^2$ avec $a,b,c \in \mathbb{Z}$.

Si q est une forme à coefficients entiers et $U \in \mathrm{Mat}_2(\mathbb{Z})$, alors $q(U \cdot (x,y))$ est encore à coefficients entiers (changement de variables linéaire dans un polynôme homogène de degré 2). Par conséquent, une forme équivalente à une forme à coefficients entiers est à coefficients entiers.

Le discriminant $D = b^2-4ac$ d'une forme entière vérifie la congruence $D \equiv b^2 \equiv 0,1 \bmod 4$. Si $D \equiv 0 \bmod 4$, cela signifie que b est pair (on dit que q est paire), si $D \equiv 1 \bmod 4$, que b est impair (on dit que q est impaire). Comme les discriminants de deux formes équivalentes sont égaux, cette propriété est conservée par équivalence ; autrement dit, une forme équivalente à une forme paire est paire, une forme équivalente à une forme impaire est impaire.

Inversement, si D est un entier qui vérifie cette congruence, il existe une forme quadratique entière de discriminant D, par exemple la forme $q(x,y) = x^2+Dy^2$ si D est multiple de 4, et $q(x,y) = x^2+xy+\frac{D-1}{4}$ si $D \equiv 1 \bmod 4$. Cette forme est appelée la forme principale. Nous dirons qu'un nombre entier n est <u>représenté</u> par la forme q s'il existe un couple $(x,y) \in \mathbb{Z}^2$ tel que $q(x,y) = n$, et qu'il est <u>proprement représenté</u> par q s'il existe un tel couple formé d'entiers premiers entre eux.

Supposons que n soit représenté par q et soit $(x,y) \in \mathbb{Z}^2$ tel que $q(x,y) = n$. On a nécessairement $n \geq 0$ car q est définie positive ; de plus, si $n = 0$, il vient $x = y = 0$. On supposera donc dans la suite que $n > 0$ et $(x,y) \neq (0,0)$. Soit d le pgcd de x et y et posons $x' = x/d$, $y' = y/d$. Alors, $n = q(x,y) = d^2 q(x',y')$ et n/d^2 est un entier qui est proprement représenté par q.

Il se trouve que la propriété, pour un entier n, d'être proprement représenté par une forme q est plus maniable que la notion naïve ; les calculs précédents montrent qu'il n'y a pas grand dommage à se cantonner à cette notion.

Théorème 9.5. *Soit D un entier < 0 et soit n un nombre entier strictement positif. Pour qu'il existe une forme quadratique binaire, définie positive, à coefficients entiers et de discriminant D qui représente proprement n, il faut et il suffit que D soit un carré dans $\mathbb{Z}/4n\mathbb{Z}$.*

Le discriminant D d'une forme entière est congru à 0 ou 1 modulo 4 ; cette congruence est bien vérifiée si n est un entier tel que D soit un carré dans $\mathbb{Z}/n\mathbb{Z}$.

Démonstration : soit q une telle forme quadratique et soit (ξ, η) un couple d'entiers premiers entre eux tels que $q(\xi, \eta) = n$. Puisque ξ et η sont premiers entre eux, on peut effectuer un changement de coordonnées dans $\mathrm{SL}_2(\mathbb{Z})$ et supposer que $(\xi, \eta) = (1, 0)$. Alors, q est de la forme $q(x, y) = ax^2 + bxy + cy^2$, et $a = q(1, 0) = n$. Le discriminant de q est donné par la formule $D = b^2 - 4ac$; autrement dit, $b^2 = D + 4nc \equiv D \bmod 4n$.

Inversement, supposons que D soit un carré dans $\mathbb{Z}/4n\mathbb{Z}$ et choisissons des entiers b et c tels que $D = b^2 - 4nc$; alors, la forme quadratique $q(x, y) = nx^2 + bxy + cy^2$ est entière, de discriminant D, définie positive et représente proprement n puisque $q(1, 0) = n$.

Pour que ce théorème soit réellement utile, il faut ramener l'ensemble des formes q dont le théorème affirme l'existence à un ensemble contrôlable. Pour cela, la première remarque est que deux formes équivalentes représentent proprement les mêmes entiers. Par suite, dans le théorème précédent, on peut rajouter la condition que la forme quadratique soit réduite.

Enfin, on a la propriété :

Proposition 9.6. *Pour tout entier $D < 0$, l'ensemble des classes d'équivalence de formes quadratiques binaires, entières et de discriminant D, est fini.*

Démonstration : puisque toute forme est équivalente à une forme réduite, il suffit de démontrer que l'équation $D = b^2 - 4ac$ n'a qu'un nombre fini de solutions $(a, b, c) \in \mathbb{Z}^3$ vérifiant les conditions $|b| \leq a \leq c$ qui assurent que la forme quadratique $ax^2 + 2bxy + cy^2$ est réduite.

On a déjà vu que ces relations entraînent l'inégalité $|b| \leq \sqrt{D/3}$: il n'y a donc qu'un nombre fini d'entiers b possibles. Alors, b étant fixé, l'équation $4ac = -D + b^2$ n'a elle aussi qu'un nombre fini de solutions (a, c) (majoré par le nombre de diviseurs de $-D + b^2$), a fortiori qu'un nombre fini de solutions telles que $|b| \leq a \leq c$.

Au moins lorsque $-D$ n'est pas trop grand, il n'est pas difficile d'exhiber la liste des formes réduites de discriminant D. Traitons par exemple les cas $D = -3$, $D = -4, -8, -20, -23$ et -76.

Exemple 9.7. *(Formes réduites de discriminant $D = -3$) L'inégalité $|b| \leq \sqrt{D/3}$ implique $b = 0$ ou $b = \pm 1$, mais $b = 0$ ne convient pas car une forme de discriminant -3 est impaire. L'équation pour (a, c) est alors $4ac = 4$, d'où $ac = 1$ et l'inégalité $0 < a \leq c$ entraîne $a = c = 1$. Par suite, $q(x, y) = x^2 \pm xy + y^2$. Par conséquent, la forme $x^2 + xy + y^2$ est la seule forme réduite de discriminant -3.*

Exemple 9.8. *(Formes réduites de discriminant $D = -4$) Soit $q = ax^2 + bxy + cy^2$ une forme réduite de discriminant -4 ; alors q est paire, donc b est pair. L'inégalité $|b| \leq \sqrt{D/3}$ implique*

$|b| \leq 1$, *d'où* $b = 0$. *Ensuite,* $4ac = 4$, *d'où* $a = c = 1$. *Il n'y a donc qu'une forme réduite de discriminant* 1, *la forme* $x^2 + y^2$.

Par suite, cette forme représente un nombre premier p *si et seulement si* -1 *est un carré modulo* p, *c'est-à-dire* $p = 2$ *ou* $p \equiv 1 \bmod 4$. *On retrouve un résultat déjà démontré.*

Exemple 9.9. *(Formes réduites de discriminant* $D = -20$*) Soit* $q = ax^2 + bxy + cy^2$ *une forme réduite entière de discriminant* -20 *; elle est paire. L'inégalité* $|b| \leq \sqrt{|D|/3}$ *implique* $b \in \{0, -2, 2\}$. *Pour* $b = 0$, *il vient* $ac = D = 5$, *d'où* $a = 1$ *et* $c = 5$ *; pour* $b = \pm 2$, *on trouve* $4ac = 20 + 4 = 24$, *donc* $ac = 6$ *et, compte tenu de l'inégalité* $|b| \leq a \leq c$, *la seule solution* $a = 2$ *et* $c = 3$ *; come* $|b| = a$, *seule la solution* $b = 2$ *convient. Les formes réduites de discriminant* -20 *sont donc les formes* $x^2 + 5y^2$ *et* $2x^2 + 2xy + 3y^2$.

Exemple 9.10. *(Formes réduites de discriminant* $D = -23$*) Soit* $q = ax^2 + bxy + cy^2$ *une forme réduite de discriminant* -23 *; c'est une forme impaire. L'inégalité* $|b| \leq \sqrt{|D|/3}$ *entraîne* $|b| \leq 2$, *donc* $b = \pm 1$. *Il vient alors* $4ac = 24$, *donc* $ac = 6$ *puis, comme* $a \leq c$, $(a, c) = (1, 6)$ *ou* $(a, c) = (2, 3)$. *La première solution impose en outre* $b = 1$ *; les formes réduites de discriminant* -23 *sont donc les trois formes* $x^2 + xy + 6y2$, $2x^2 + xy + 3y^2$ *et* $2x^2 - xy + 3y^2$.

Exemple 9.11. *(Formes réduites de discriminant* $D = -19$*) Supposons que l'on ait* $D = -19$. *L'inégalité* $|b| \leq \sqrt{|D|/3}$ *entraîne* $|b| \leq 2$, *donc* $b = \pm 1$. *Lorsque* $b = \pm 1$, *on a* $4ac = 20$ *soit* $ac = 5$ *puis* $a = 1$ *et* $c = 5$. *Finalement la seule forme réduite de discriminant* -19 *est la forme principale* $x^2 + xy + 5y^2$.

Exemple 9.12. *(Formes réduites de discriminant* $D = -76$*) Supposons que l'on ait* $D = -76$. *L'inégalité* $|b| \leq \sqrt{|D|/3}$ *entraîne* $|b| \leq 5$, *donc* $b = 0$ *ou* $b = \pm 2$. *Si* $b = 0$, *il vient* $4ac = 76$, *d'où* $ac = 19$ *et* $(a, c) = (1, 19)$. *Si* $b = \pm 2$, *on a* $4ac = 80$, *donc* $ac = 20$ *et, compte tenu de l'inégalité* $|b| \leq a \leq c$, *les solutions* $(a, c) = (2, 10)$ *et* $(a, c) = (4, 5)$. *Les formes réduites de discriminant* -19 *sont ainsi les formes* $x^2 + 19y^2$, $2x^2 + 2xy + 10y^2$ *et* $4x^2 \pm 2xy + 5y^2$.

Pour tout entier $D < 0$, notons $h(D)$ le nombre de formes quadratiques entières, réduites et de discriminant D.

9.4 Forme d'Hermite d'une matrice à coefficients entiers

Définition 9.13. *Soit $A \in \mathrm{Mat_{m,n}}(\mathbb{Z})$ une matrice $m \times n$ à coefficients entiers. On dit que A est sous forme normale de Hermite s'il existe un entier r tel que $1 \leq r \leq n$ et une suite $(m_1, \ldots, m_r)$ d'entiers tels que $1 \leq m_1 < \cdots < m_r \leq m$ de sorte que les coefficients $(a_{i,j})$ de A vérifient les propriétés suivantes :*

(i) Pour tout entier j tel que $r < j \leq n$ et tout entier $i \in \{1, \cdots, m\}$, on a $a_{i,j} = 0$ (seules les r premières colonnes de A sont non nulles) ;

(ii) Pour tout entier j tel que $1 \leq j \leq r$ et tout entier i tel que $1 \leq i < m_j$, on a $a_{i,j} = 0$ (les r premières colonnes sont échelonnées) ;

(iii) Pour tout entier j tel que $1 \leq j \leq r$, on a $a_{m_j,j} > 0$ (les premiers coefficients non nuls de chaque colonne, appelés pivots, sont strictement positifs) ;

(iv) Pour tout entier j tel que $1 \leq j \leq r$ et tout entier k tel que $1 \leq k < m_j$, on a $0 \leq a_{m_j,k} < a_{m_j,j}$ (les coefficients de la ligne de pivot m_j sont positifs ou nuls et sont strictement inférieurs au pivot $a_{m_j,j}$).

Cette notion, introduite par Hermite en 1851, tire son intérêt du théorème suivant.

Théorème 9.14. *Soit A une matrice $m \times n$ à coefficients entiers. Il existe une unique matrice H de même taille, sous forme normale de Hermite et une matrice $U \in \mathrm{GL}_n(\mathbb{Z})$ telle que $A = HU$.*

La matrice H est appelée forme normale de Hermite de la matrice A.

Démonstration : l'existence d'un tel couple (H, U) se démontre par récurrence, en effectuant sur les colonnes de la matrice A une successions d'opérations élémentaires. Introduisons quelques notations. Si (i, j) est un couple d'entiers distincts dans $\{1, \ldots, n\}$ et $a \in \mathbb{Z}$, on note $E_{i,j}(a)$ la matrice $n \times n$ dont la diagonale est formée de 1 et tous les autres coefficients sont nuls sauf celui de coordonnées (i, j) qui est égal à a. Elle appartient à $\mathrm{SL}_n(\mathbb{Z})$, son inverse étant $E_{i,j}(-a)$. La méthode va consister à partir du couple $(H, U) = (A, I_n)$, formé d'une matrice entière et d'une matrice de $\mathrm{SL}_n(\mathbb{Z})$, et à multiplier à droite H par une matrice $E_{i,j}(a)$; l'égalité évidente $HU = (HE_{i,j}(a))(E_{i,j}(-a)U)$ montre comment obtenir un autre couple de même nature et de même produit.

D'autre part, pour tout entier i, on note S_i la matrice diagonale $n \times n$ dont tous les coefficients diagonaux sont égaux à 1 sauf celui de coordonnées (i, i) qui est égal à -1. Si H est une matrice ayant n colonnes, la matrice $HE_{i,j}(a)$ est obtenue à partir de H en ajoutant à la colonne C_j de H la colonne C_i multipliée par a (en abrégé, $C_j \leftarrow C_j + aC_i$). La matrice HS_i est obtenue en multipliant la colonne i par -1 (ce qu'on note $C_i \leftarrow C_i$). Si U est une matrice ayant n lignes, la matrice $E_{i,j}(-a)U$ est obtenue à partir de U en ajoutant à la ligne L_i la ligne L_j multipliée par $(-a)$ (en abrégé, $L_i \leftarrow L_i - aL_j$) ; la matrice S_iU se déduit de U en multipliant la ligne i par -1 (noté $L_i \leftarrow -L_i$).

Cela montre que l'on passe d'un couple (H, U) au suivant par des opérations élémentaires sur les colonnes de H et sur les lignes de U.

Commençons par démontrer qu'il existe une matrice $H \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, échelonnée et à pivots positifs, et un produit de matrices élémentaires $U \in \mathrm{GL}_n(\mathbb{Z})$ tels que $A = HU$. On procède par récurrence sur la taille $m + n$ de A.

Démontrons alors par récurrence sur la somme des valeurs absolue des coefficients de la première ligne de A que l'on peut supposer que $a_{1,1} \geq 0$ et $a_{1,j} = 0$ si $2 \leq j \leq n$.

Si cette propriété n'est pas vérifiée, notons j l'indice de colonne du coefficient non nul de la première ligne qui est de plus petite valeur absolue. Pour $k \neq j$, l'opération $C_k \leftarrow C_k - qC_j$, sur les colonnes de A, où $q = [a_{1,k}/a_{1,j}]$ est la partie entière du quotient de $a_{1,k}$ par $a_{1,j}$ ramène la matrice A à une matrice dont le coefficient $a_{1,k}$ vérifie $0 \leq a_{1,k} < |a_{1,j}|$. Par récurrence, on se ramène ainsi au cas où $a_{1,j}$ est le seul coefficient non nul de la première ligne ; notons ε son signe. Si $j \neq 1$, les opérations $C_1 \leftarrow C_1 + \varepsilon C_j$ puis $C_j \leftarrow C_j - \varepsilon C_1$ ramènent au cas où $j = 1$ et $a_{1,j} > 0$. Supposons $j = 1$et $\varepsilon = -1$. Si $n \geq 2$, on effectue successivement les opérations $C_2 \leftarrow C_2 + C_1$, $C_1 \leftarrow C_1 - C_2$ qui nous ramènent au cas $j = 2$. Si $n = 1$, la seule possibilité est de multiplier la première colonne par -1.

Nous sommes donc réduits à traiter le cas où, à l'exception du coefficient $a_{1,1}$ qui est positif ou nul, tous les coefficients la première ligne de A sont nuls, on écrit $A = \begin{pmatrix} a_{1,1} & 0 \\ \star & A' \end{pmatrix}$ puis $A' = H'U'$, où $H' \in \mathrm{Mat}_{m-1,n-1}(\mathbb{Z})$ est échelonnée à pivots positifs. Posons $U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix}$; c'est un produit de matrices élémentaires : le même que U' où les indices de lignes et de colonnes sont augmentés de 1 et un calcul par blocs montre que la matrice $H = AU^{-1}$ est échelonnée à pivots positifs.

Il reste à mettre sous forme normale de Hermite une matrice échelonnée H autrement dit à faire en sorte que sur la ligne d'un pivot, tous les coefficients soient inférieurs au pivot.

Supposons cette propriété satisfaite pour les lignes des pivots d'indices de colonnes $> j$ et soit m_j l'indice de ligne du pivot de colonne j. Pour tout entier i tel que $1 \leq i < j$, remplaçons la colonne C_k de H par la colonne $C_k - qC_j$, où $q = [a_{k,j}/a_{m_j,j}]$ est la partie entière du quotient de $a_{k,j}$ par $a_{m_j,j}$. Tous les coefficients de la ligne m_j appartiennent alors à l'intervalle $[0, \ldots, a_{m_j,j-1}]$ et ceux des lignes des pivots ultérieurs ($a_{m_t,k}$, pour tout entier t tel que $j < t \leq r$ et tout entier k tel que $1 \leq k < m_t$ n'ont pas été modifiés puisque, la matrice H étant échelonnée, $a_{m_t,j} = 0$ si $t > j$.

Cela conclut, par récurrence, la démonstration qu'il existe une matrice $U \in \mathrm{GL}_n(\mathbb{Z})$ et une matrice sous forme normale de Hermite $H \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ telles que $A = HU$.

Démontrons maintenant que si (H, U) et (H', U') sont deux couples de matrices tels que $HU = H'U'$, où H et $H' \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ sont sous forme normale de Hermite et $U, U' \in \mathrm{GL}_n(\mathbb{Z})$, alors $H = H'$ (et $U = U'$). Quitte à remplacer U par $U(U')^{-1}$, on suppose que $H' = HU$ et l'on doit démontrer que $H = H'$.

Notons r le nombre de pivots de H et $m_1, \ldots, m_r$ les indices de lignes correspondants. Notons $(a_{i,j)}, (a'_{i,j})$ et $(u_{i,j})$ les coefficients des matrices H, H' et U ; notons aussi $L_1, \ldots, L_n$ les lignes de la matrice U. Si $m_t \leq i < m_{t+1}$, la t-ième ligne de la matrice HU est donnée par $L'_i = a_{i,1}L_1 + \cdots + a_{i,t}L_t$. Puisque $H' = HU$ est échelonnée, il vient déjà que les lignes $L_1, \ldots, L_r$ de U le sont aussi : $u_{i,j} = 0$ si $1 \leq i \leq r$ et $j > i$. De plus, la positivité de $a_{m_t,t}$ et $a'_{m_t,t}$ implique que les r premiers coefficients diagonaux de U sont positifs ou nuls. On peut donc écrire $U = \begin{pmatrix} U_1 & 0 \\ U_3 & U_4 \end{pmatrix}$, où U_1 est triangulaire inférieure. Démontrons que $U_1 = I_r$.

On a pour commencer l'égalité $1 = \det(U) = \det(U_1)\det(U_4)$ si bien que $\det(U_1) = \pm 1$. Puisque $\det(U_1)$ est égal au produit des coefficients diagonaux de U_1, ceux-ci sont égaux à 1. Alors, la forme de la matrice HU montre que les pivots de $H' = HU$ sont aux mêmes positions que ceux de H, chacun étant égal au pivot de H correspondant. Nous allons démontrer par récurrence sur $t \in \{1, \ldots, r\}$ que $L_t = (0, \ldots, 0, 1, 0, \ldots, 0)$, le 1 étant en colonne t.

Supposons que ce soit vrai aux rangs $< t$ et démontrons-le au rang t. On a déjà prouvé que $u_{t,t} = 1$; considérons, s'il en existe, un entier j dans $\{1, \ldots, t-1\}$ tel que $u_{t,j} \neq 0$ et maximal pour cette propriété(en particulier, $a'_{m_t,k} = a_{m_t,k}$ si $j < k \leq t$). Par hypothèse, on a alors $a'_{m_t,j} = a_{m_t,t}u_{t,j} + a_{m_t,j}$. Comme $a_{m_t,t} = a'_{m_t,t}$, les inégalités $0 \leq a_{m_t,j} < a_{m_t,t}$ et $0 \leq a_{m_t,j} < a_{m_t,t}$ impliquent $\left|a_{m_t,j} - a'_{m_t,j}\right| < a_{m_t,t}$; puisque cette différence est un multiple entier de $a_{m_t,t}$, elle est nulle, d'où $u_{t,j} = 0$. Cela démontre que L_t est de la forme annoncée, puis, par récurrence sur t , que $U_1 = I_r$. Alors, $H' = HU = H$, ce qu'il fallait démontrer.

Remarque 9.15. *(i) L'entier r est égal au rang de la matrice A. Sauf si $r = n$, on n'a pas unicité de la matrice U.*

(ii) Supposons $r = n$ et $A \in \mathrm{SL}_n(\mathbb{Z})$. Comme $1 = \det(A) = \det(H)$, la matrice H est de déterminant 1 ; comme elle est échelonnée, ses coefficients diagonaux sont donc égaux à 1 et les autres sont nécessairement nuls. Autrement dit, $H = I_n$ et $A = U$. La démonstration assure que A est produit de matrices élémentaires de types $E_{i,j}(a)$ et S_i. L'usage des matrices S_i n'est en fait pas nécessaire : le groupe $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les matrices $E_{i,j}(1)$. Notons $E \subset \mathrm{SL}_n(\mathbb{Z})$ le sous-groupe engendré par ces matrices ; il contient les matrices $E_{i,j}(a)$ pour tout $a \in \mathbb{Z}$. Pour tout k, $S_k E_{i,j}(a) S_k^{-1}$ est égal à $E_{i,j}(a)$ si $k \notin \{i,j\}$, à $E_{i,j}(-a)$ sinon ; par conséquent, les matrices S_k appartiennent au normalisateur de E. Dans une expression de U comme produit de matrices élémentaires, on peut de proche en proche les repousser à la fin. Comme $\det(A) = 1$, le nombre de telles matrices qui restent à la fin est pair et il suffit de montrer que le produit de deux d'entre elles appartient à E. Or, la suite de matrices 2×2,

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

où chacune se déduit de la précédente par une opération élémentaire du type $C_i \leftarrow C_i + aC_j$ démontre que c'est bien le cas, au moins si $n = 2$. Dans le cas général, il suffit d'effectuer les opérations correspondantes sur les colonnes concernées.

(iii) L'énoncé et sa démonstration s'étendent au cas d'un anneau euclidien R arbitraire. L'hypothèse de positivité sur les pivots doit être remplacée par l'hypothèse que les pivots appartiennent à un système de représentants d'éléments de R modulo l' action par multiplication des éléments inversibles de R ; quant à l'hypothèse que les coefficients $a_{m_j,k}$ (avec $1 \leq k < j$) d'une ligne de pivot sont positifs ou nuls et inférieurs au pivot, elle est remplacée par celle que $a_{m_j,k}$ appartient à un système de représentants des restes des divisions euclidiennes par $a_{m_j,j}$.

(iv) La démonstration donnée est algorithmique : elle fournit un moyen effectif de calculer des matrices H et U. Lorsque les coefficients sont réels, les erreurs d'arrondis la rendent peu praticable. La situation n'est guère meilleure lorsque A est à coefficients entiers. En effet, même si un calcul exact est alors possible, l'algorithme que nous avons décrit peut faire apparaître, au cours du calcul, des coefficients de taille démesurément grande comparée à celle des coefficients de A. Hafner et McHurley ont donné l'exemple d'une matrice 20×20 de coefficients entre 0 et 10 pour laquelle ce calcul requiert des nombres entiers de 5000 chiffres décimaux... Signalons qu'il existe aujourd'hui des algorithmes efficaces.

Lemme 9.16. *Soit $A \in \mathrm{Mat}_n(\mathbb{R})$. Pour que l'on ait $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$, il faut et il suffit que $A \in \mathrm{Mat}_n(\mathbb{Z})$; pour que l'on ait $A(\mathbb{Z}^n) = \mathbb{Z}^n$, il faut et il suffit que l'on ait $A \in \mathrm{GL}_n(\mathbb{Z})$, c'est-à-dire que $A \in \mathrm{Mat}_n(\mathbb{Z})$ et $\det(A) \in \{\pm 1\}$.*

Démonstration : si $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$, les colonnes de A, qui sont les images des vecteurs de base de $\mathbb{R}^n$, appartiennent à $\mathbb{Z}^n$; la réciproque est évidente.

Si $A \in \mathrm{GL}_n(\mathbb{Z})$, alors A et A^{-1} appartiennent à $\mathrm{Mat}_n(\mathbb{Z})$, d'où les deux inclusions $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$ et $A^{-1}(\mathbb{Z}^n) \subset \mathbb{Z}^n$. Par suite, $A(\mathbb{Z}^n) = \mathbb{Z}^n$. La réciproque se démontre de même : si $A(\mathbb{Z}^n) = \mathbb{Z}^n$, on a déjà $A \in \mathrm{Mat}_n(\mathbb{Z})$; d'autre part, l'image de A contenant n vecteurs linéairement indépendants, $A(\mathbb{R}^n) = \mathbb{R}^n$ et A est aussi injective. Par hypothèse, les antécédents des éléments de $\mathbb{Z}^n$ appartiennent à $\mathbb{Z}^n$, donc $A^{-1}(\mathbb{Z}^n) \subset \mathbb{Z}^n$, puis $A^{-1} \in \mathrm{Mat}_n(\mathbb{Z})$.

Enfin, si $A \in \mathrm{GL}_n(\mathbb{Z})$, donc $A^{-1} \in \mathrm{Mat}_n(\mathbb{Z})$, on a $1 = \det(A \cdot A^{-1}) = \det(A)\det(A^{-1})$, d'où $\det(A) \in \{\pm 1\}$. Inversement, si $A \in \mathrm{Mat}_n(\mathbb{Z})$ vérifie $\det(A) \in \{\pm 1\}$, les formules de Cramer ($A^{-1} = (\det A)^{-1}\,{}^t\mathrm{Com}(A)$) entraînent que A^{-1} appartient à $\mathrm{Mat}_n(\mathbb{Z})$, d'où $A \in \mathrm{GL}_n(\mathbb{Z})$.

Théorème 9.17. *Soit G un sous-groupe abélien de $\mathbb{Z}^m$. Alors G est un groupe abélien libre de rang fini : il existe un entier $r \in \{0, \dots, n\}$ et des vecteurs $u_1, \dots, u_r \in \mathbb{R}^m$ appartenant à G tels que tout élément de G s'écrive de manière unique sous la forme $\sum_{j=1}^{r} a_j u_j$, avec $(a_1, \dots, a_r)\mathbb{Z}^r$.*

Démonstration : soit A la matrice de taille $m \times n$ dont les colonnes sont les vecteurs $v_1, \dots, v_n$, générateurs de G comme groupe abélien, soit H sa forme normale de Hermite et soit $U \in \mathrm{GL}_n(\mathbb{Z})$ une matrice telle que $A = HU$. Par hypothèse, $G = A(\mathbb{Z}^n)$. Comme on a $U(\mathbb{Z}^n) = \mathbb{Z}^n$, il vient $G = H(\mathbb{Z}^n)$. Notons r le rang de H et $u_1, \dots, u_r$ ses r premières colonnes. Comme les autres colonnes sont nulles, on a aussi $G = (u_1 \dots u_r)(\mathbb{Z}^r)$: tout vecteur de G est combinaison linéaire à coefficients entiers de $u_1, \dots, u_r$. Comme ces r vecteurs sont échelonnés, ils sont linéairement indépendants dans $\mathbb{R}^m$. Autrement dit, tout vecteur de G est de manière unique combinaison linéaire à coefficients entiers de $u_1, \dots, u_r$, ce qui démontre que G est un groupe abélien libre, de base $(u_1, \dots, u_r)$.

Nous avons utilisé ci-dessus de G est un $\mathbb{Z}$-module de type fini. Complétons ce point, à l'aide d'un rappel d'algèbre.

Proposition 9.18. *Soit V un module de type fini sur un anneau nœthérien A. Alors tout sous-module est de type fini.*

Démonstration : Soit $V = A^n$ pour un entier $n \in \mathbb{N}$. On fait maintenant une récurrence sur n. Par hypothèse, c'est vrai pour $n = 1$ car A est noethérien et les sous-modules sont les idéaux.

Soit $\pi : A^n \to A^{n-1}$(on oublie la dernière coordonnée). Par définition, $\ker(\varphi) = \{(0, \dots, 0, x)\} \simeq A$. Soit W un sous-module de A^n. Alors $\pi(W) = \mathrm{Im}(\pi|_W)$ est de type fini par hypothèse de récurrence. Comme $\ker(\pi|_W) = W \cap \ker(\pi)$ est un sous-module de A, il est également de type fini. Le prochain lemme montre que W est donc de type fini.

Soit V un A-module général. Soit W un sous-module de V. Si V est de type fini alors il existe un $n \geq 1$ tel que V est généré par n générateurs. Soit $\varphi : A^n \to V$ la fonction surjective générée par un système de générateurs de V (choisi arbitrairement). Soit $L = \varphi^{-1}(W)$. C'est un sous-module de A^n, donc de type fini, comme justement démontré, et $\varphi|_L : L \to W$ est surjective donc W est de type fini.

Lemme 9.19. *a) Soit $\varphi : V \to W$ un morphisme de A-modules. Si $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ sont de type fini, alors V est de type fini.*
b) Soit W un sous-module de V. Si W et V/W sont de type fini, alors V est de type fini.

Démonstration : a) On choisit un système générateur $(u_1, \dots, u_k)$ de $\ker(\varphi)$ et un système générateur $(w_1, \dots, w_m)$ de $\mathrm{Im}(\varphi)$.
On prend $v_i \in V$ tel que $\varphi(v_i) = w_i$. Alors $(u_1, \dots, u_k, v_1, \dots, v_m)$ est un système générateur de V. En effet si $v \in V$, $\varphi(v) = \sum_i a_i w_i$, donc $v - \sum_i a_i v_i \in \ker(\varphi)$. Donc $v - \sum_i a_i v_i \in \ker(\varphi)$ est une combinaison linéaire des $u_1, \dots, u_k$.

b) On applique a) à $\pi : V \to V/W$.

On a donc bouché le dernier trou qui restait dans la démonstration précédente.

Exercice 9.20. *Donnez un exemple d'un sous-module d'un module de type fini qui n'est pas de type fini.*

Corollaire 9.21. *Soit G un groupe abélien engendré par un nombre fini $\{g_1, \dots, g_n\}$ de ses éléments. Si G est sans torsion, alors G est un groupe abélien libre : il existe un entier $r \in \{0, \dots, n\}$ et des éléments $h_1, \dots, h_r$ de G tels que tout élément de G s'écrive de manière unique sous la forme $\sum_{i=1}^{r} a_i h_i$, avec $(a_1, \dots, a_r)\mathbb{Z}^r$.*

Démonstration : laissée en exercice.

Soit A une matrice de taille $m \times n$ à coefficients entiers. Pour tout entier r tel que $1 \leq r \leq \min(m, n)$, on définit $\mathcal{F}_r(A)$ comme le groupe abélien engendré par les mineurs $r \times r$ extraits de A.

Soit $U \in \mathrm{Mat}_n(\mathbb{Z})$ une matrice à coefficients entiers ; par multi-linéarité du déterminant, on a $\mathcal{F}_r(AU) \subset \mathcal{F}_r(A)$. En particulier, si $U \in \mathrm{GL}_n(\mathbb{Z})$ est inversible, on a $\mathcal{F}_r(AU) = \mathcal{F}_r(A)$. De même, pour toute matrice $V \in \mathrm{Mat}_m(\mathbb{Z})$, on a $\mathcal{F}_r(VA) \subset \mathcal{F}_r(A)$, et $\mathcal{F}_r(VA) = \mathcal{F}_r(A)$ si V appartient à $\mathrm{GL}_m(\mathbb{Z})$.

En outre, le développement d'un mineur $r \times r$ suivant une ligne montre que $\mathcal{F}_r(A)$ est contenu dans $\mathcal{F}_{r-1}(A)$. Autrement dit, les groupes abéliens $\mathcal{F}_0(A) = \mathbb{Z}$, $\mathcal{F}_1(A), \dots$ obéissent aux inclusions $\mathbb{Z} \supset \mathcal{F}_1(A) \supset \dots$; ils sont appelés idéaux de Fitting de la matrice [8] A.

Si A est de rang r, les idéaux de Fitting $\mathcal{F}_s(A)$ sont nuls pour $s > r$; en outre, $\mathcal{F}_r(A) \neq 0$.

Théorème 9.22. *Soit $A \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ avec $n \geq m$. Pour qu'il existe une matrice $B \in \mathrm{GL}_n(\mathbb{Z})$ dont A constitue les m premières lignes, il faut et il suffit que l'idéal de Fitting $\mathcal{F}_m(A)$ soit égal à $\mathbb{Z}$, c'est-à-dire que les mineurs $m \times m$ extraits de A soient premiers entre eux.*

Démonstration : soit $B \in \mathrm{Mat}_n(\mathbb{Z})$ une matrice carrée dont A constitue les m premières lignes et soit H la forme normale de Hermite de B et U une matrice de $\mathrm{GL}_n(\mathbb{Z})$ telle que $B = HU$. Soit $S \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ la matrice formée des m premières lignes de H ; on a donc $A = SU$.

Si B appartient à $\mathrm{GL}_n(\mathbb{Z})$, la relation $\det(B) = \det(H)\det(U)$ entraîne que $\det(H) \in \{\pm 1\}$, donc $H \in \mathrm{GL}_n(\mathbb{Z})$. Comme H est échelonnée, ses coefficients diagonaux sont donc égaux à ± 1. En particulier, le mineur principal $m \times m$ de S est donc égal à ± 1. On a donc $\mathcal{F}_m(S) = \mathbb{Z}$, d'où $\mathcal{F}_m(A) = \mathcal{F}_m(SU) = \mathcal{F}_m(S) = \mathbb{Z}$.

Inversement, supposons que $\mathcal{F}_m(A) = \mathbb{Z}$; soit S la forme normale de Hermite de A et soit $U \in \mathrm{GL}_n(\mathbb{Z})$ telle que $A = SU$. Si $\mathcal{F}_m(A) = \mathbb{Z}$, il en est de même de $\mathcal{F}_m(S)$. Or, S est de rang m,

8. Les propriétés que nous avons démontrées sont valables, avec la même preuve, lorsque l'anneau $\mathbb{Z}$ est remplacé par un anneau commutatif arbitraire ; les $\mathcal{F}_r(A)$ sont alors définis comme les idéaux engendré par les mineurs $r \times r$ extraits de A, d'où la terminologie.

échelonnée, donc $\mathcal{F}_m(S)$ est engendré par le mineur principal de S : les autres sont nuls ! Par conséquent, les coefficients diagonaux de S sont égaux à ± 1. Soit $H \in \mathrm{Mat}_n(\mathbb{Z})$ la matrice dont les m premières lignes sont celles de S et les $n-m$ dernières sont celles de la matrice I_n . C'est une matrice triangulaire supérieure, à coefficients diagonaux ± 1 ; elle appartient donc à $\mathrm{GL}_n(\mathbb{Z})$, de même que la matrice HU. Un calcul par bloc entraîne alors que les m premières lignes de HU sont celles de A, d'où le théorème.

Corollaire 9.23. *Soit $u \in \mathbb{Z}^n$; pour qu'il existe une matrice $A \in \mathrm{GL}_n(\mathbb{Z})$ dont u soit le premier vecteur colonne, il faut et il suffit que les coordonnées de u soient premières entre elles.*

Démonstration : quitte à transposer les matrices en jeu, ce qui échange lignes et colonnes, c'est le cas $m = 1$ du théorème.

9.5 Sous-groupes discrets de $\mathbb{R}^n$ et réseaux

Rappelons qu'on dit qu'un espace topologique X est discret si, pour tout point x de X, la partie $\{x\}$ est ouverte dans X. Cela revient à dire que toute partie de X est ouverte et fermée. Une partie S d'un espace topologique X est discrète si, pour la topologie induite, c'est un espace topologique discret ; cela revient à dire que pour tout point x de S, la partie $\{x\}$ de S est ouverte dans S, autrement dit, qu'il existe un ouvert U de X tel que $U \cap S = \{x\}$.

Proposition 9.24. *Soit G un sous-groupe de $\mathbb{R}^n$. Les conditions suivantes sont équivalentes :*
(i) L'espace G est discret dans $\mathbb{R}^n$.
(ii) pour $r > 0$ assez petit, l'intersection de G et de la boule de centre 0 et de rayon r est réduite au point 0 ;
(iii) pour tout R, l'intersection de G et de la boule de rayon R n'a qu'un nombre fini de points.

Démonstration : l'implication (i)$\Longrightarrow$ (ii) résulte de la définition. Inversement, soit $r > 0$ tel que la boule de centre 0 et de rayon r dans $\mathbb{R}^n$ ne rencontre G qu'en 0. Soit $g \in G$; pour tout point x de $G \cap B(g, r)$, $x - g$ appartient à $G \cap B(0, r)$, donc $x = g$ si bien que $G \cap B(g, r) = \{g\}$. Par suite, G est discret, d'où (i).

Avec ces notations, les boules de centres $g \in G$ et de rayon $r/2$ sont disjointes : si $x \in B(g, r/2) \cap B(g', r/2)$, alors $\|g - g'\| < r$, donc $g' \in B(g, r) \cap G$, d'où $g' = g$. Par conséquent, si $B(0, R)$ contient N points, la boule $B(0, R + r/2)$ contient N boules disjointes de rayon r. Comme elles ont même volume, on a donc $N\mathrm{Vol}(B(0, r)) \leq \mathrm{Vol}(B(0, R + r/2))$; en particulier, $N \neq +\infty$. Cela démontre (iii).

Inversement, supposons que $G \cap B(0, R)$ soit fini. Si $G = \{0\}$, alors G est discret. Sinon, soit g un élément non nul de G et posons $R = \|g\| + 1$. Comme $G \cap B(0, R)$ privé de 0 est fini (par hypothèse) et non vide (il contient g), l'ensemble des normes $\|g\|$ des points $g \neq 0$ de $G \cap B(0, R)$ admet un plus petit élément r. On a donc $G \cap B(0, r) = \{0\}$. Cela démontre (i).

Définition 9.25. *Soit V un espace vectoriel réel de dimension finie. On appelle réseau de V tout sous-groupe de V formé des combinaisons linéaires à coefficients entiers d'une famille libre de V.*

On appelle rang d'un réseau la dimension de l'espace vectoriel réel qu'il engendre. Soit G un réseau d'un espace vectoriel de dimension finie V. Soit $(v_1, \ldots, v_r)$ une famille libre de V qui engendre G comme sous-groupe de V. Alors, $G \subset \mathrm{vect}(v_1, \ldots, v_r)$ donc $\mathrm{vect}(G) \subset \mathrm{vect}(v_1, \ldots, v_r)$;

inversement, comme G contient $v_1, \dots, v_r$, l'espace $\mathrm{vect}(G)$ contient $\mathrm{vect}(v_1, \dots, v_r)$. On a donc $\mathrm{vect}(G) = \mathrm{vect}(v_1, \dots, v_r)$ et $\dim \mathrm{vect}(G) = r$. Cela démontre que le rang d'un réseau est égal au cardinal de toute famille libre qui engendre ce réseau.

Théorème 9.26. *Soit G un sous-groupe discret de $\mathbb{R}^n$. Alors, G est un réseau de $\mathbb{R}^n$. Il existe un entier $r \in \{0, \dots, n\}$ et une famille libre $(g_1, \dots, g_r)$ de $\mathbb{R}^n$ qui est une $\mathbb{Z}$-base de G.*

Inversement, observons que le groupe abélien engendré par une famille libre de $\mathbb{R}^n$ est un sous-groupe discret : quitte à effectuer un changement de base, on peut supposer que cette famille libre est formée des r premiers vecteurs de la base canonique de $\mathbb{R}^n$; alors, $G = \mathbb{Z}^r \times \{0\}^{n-r}$ est un sous-groupe discret de $\mathbb{R}^n$.

Nous allons en fait démontrer un résultat plus précis qui fournit un procédé constructif de base.

Théorème 9.27. *Soit G un sous-groupe discret de $\mathbb{R}^n$, soit V le sous-espace vectoriel réel de $\mathbb{R}^n$ engendré par G et soit $(g_1, \dots, g_r)$ une base de V formée d'éléments de G. Pour $i \in \{0, \dots, r\}$, posons $V_i = \mathrm{vect}(g_1, \dots, g_i)$.*

Pour tout $i \in \{1, \dots, r\}$, il existe un élément $v_i \in V_i \cap G$ tel que l'on ait $\|v - w\| \geq \|v_i - w\|$ pour tous $w, w' \in V_{i-1}$ et tout $v \in G \in (V_i \setminus V_{i-1})$. Alors, $(v_1, \dots, v_r)$ est une base de V formée d'éléments de G et tout élément de G est combinaison linéaire de $v_1, \dots, v_r$. En particulier, G est un réseau de rang r.

Démonstration : on va démontrer par récurrence sur i l'existence de v_i et le fait que $V_i \cap G$ (qui est manifestement un sous-groupe discret de $\mathbb{R}^n$ contenu dans V_i) est un réseau de base $(v_1, \dots, v_i)$.

Pour $i = 0$, on a $V_0 = \{0\}$, donc $V_0 \cap G = \{0\}$ est un réseau de $\mathbb{R}^n$ de base la famille vide.

Soit alors $i \in \{1, \dots, r\}$; supposons construite une base $(v_1, \dots, v_{i-1})$ de V_{i-1} telle que $V_{i-1} \cap G$ soit un réseau de base $(v_1, \dots, v_{i-1})$. Démontrons l'existence d'un vecteur $vi \in G \cap (V_i \setminus V_{i-1})$ tel que $\|v_i - w\| \leq \|v - w\|$ pour tous $w, w' \in V_{i-1}$ et tout $v \in G \cap (V_i \setminus V_{i-1})$.

Soit (g_n) une suite d'éléments de $G \cap (V_i\ V_{i-1})$ et (w_n) une suite d'éléments de V_{i-1} telles que $\|g_n - w_n\|$ tende vers la borne inférieure m des $\|g - w\|$ pour $g \in G \cap (V_i \setminus V_{i-1})$ et $w \in V_{i-1}$.

Décomposons w_n dans la base $(v_1, \dots, v_{i-1})$ de V_{i-1}, $w_n = \sum_{k<i} x_{k,n} v_k$. Posons $h_n = \sum_{k<i} [x_{k,n}] v_k$. Quitte à remplacer g_n par $g_n - h_n$ et w_n par $w_n - h_n$, on peut supposer que $0 \leq x_{k,n} < 1$ pour tous k, n. La suite (w_n) est donc bornée, de même que la suite (g_n) puisque $\|g_n\| \leq \|g_n - w_n\| + \|w_n\|$ et que $\|g_n - w_n\|$ tend vers m. Comme les g_n appartiennent à G, qui est un sous-groupe discret de $\mathbb{R}^n$, ils ne peuvent donc prendre qu'un nombre fini de valeurs. Quitte à considérer une sous-suite de la suite (g_n), on peut supposer qu'elle est constante. Notons g sa valeur et démontrons que l'on peut poser $v_i = g$. Il est clair que $g \in G \cap V_i$ mais que $g \notin V_{i-1}$ car c'est le cas de chaque g_n.

Par compacité de l'intervalle $[0, 1]$, on peut, quitte à en considérer successivement des sous-suites, supposer que les $x_{k,n}$ convergent tous ; alors, la suite (w_n) converge vers un élément w de V_{i-1}. On a donc $\|g - w_n\| \longrightarrow m$, donc $\|g - w\| \geq m$, donc l'égalité $\|g - w\| = m$ par définition de m, ce qui démontre l'existence de v_i.

Comme $v_i \notin V_i \setminus V_{i-1}$, on a

$$\dim V_i \geq \dim \mathrm{vect}(v_1, \dots, v_i) \geq \dim \mathrm{vect}(v_1, \dots, v_{i-1}) + 1 \geq \dim V_{i-1} + 1 \ ;$$

comme, par définition, $\dim V_i = \dim V_{i-1} + 1$, chacune de ces inégalités est une égalité et $(v_1, \dots, v_i)$ est une base de V_i.

Soit maintenant $v \in V_i$ et faisons l'observation suivante concernant $\|v - w\|$ lorsque w parcourt V_{i-1}. Notons $x_1, \ldots, x_i$ les coordonnées de v dans la base $(g_1, \ldots, g_i)$, de sorte que $v = x_1 g_1 + \cdots + x_i g_i$; démontrons que $d(v, V_{i-1}) = |x_i| d(g_i, V_{i-1})$. En effet, pour tout $w \in V_{i-1}$, on a $\|v - w\| = \|x_i g_i - w'\|$, avec $w' = w - \sum_{k<i} x_k g_k$. Ainsi, $w \in V_{i-1}$, de même que w'/x_i si $x_i \neq 0$, si bien que $\|v - w\| \geq |x_i| d(g_i, V_{i-1})$. L'autre inégalité se démontre de façon similaire : si (w_n) est une suite de vecteurs de V_{i-1} telle que $\|g_i - w_n\|$ converge vers $d(g_i, V_{i-1})$, alors $\|v - w'_n\|$ converge vers $|x_i| d(g_i, V_{i-1})$, où w'_n est défini par $w'_n = x_i w_n + \sum_{k<n} x_k g_k$. Par conséquent, $|x_i| d(g_i, V_{i-1}) \geq d(v, V_{i-1})$.

Supposons de plus que v appartienne aussi à G et démontrons qu'il est combinaison linéaire à coefficients entiers de $v_1, \ldots, v_i$. Notons $\alpha_1, \ldots, \alpha_i$ les coordonnées de v_i dans la base $(g_1, \ldots, g_i)$, de sorte que $v_i = \alpha_1 g_1 + \cdots + \alpha_i g_i$. Comme $v_i \notin V_{i-1}, \alpha_i \neq 0$; posons $q = [x_i/\alpha_i]$ et $v' = v - q v_i = \sum x'_k g_k$ avec $x'_k = x_k - q\alpha_k$. Alors, $v' \in V_i \cap G$ et

$$d(v', V_{i-1}) = \left|x'_i\right| d(g_i, V_{i-1}) = \frac{x'_i}{\alpha_i} d(v_i, V_{i-1}) \ .$$

Puisque $0 \leq x'_i < \alpha_i$ et $d(v_i, V_{i-1}) > 0$, on a $d(v', V_{i-1}) < d(v_i, V_{i-1})$. Par définition de v_i, cela entraîne $v' \in V_{i-1}$. Par récurrence, v' est une combinaison linéaire à coefficients entiers de $v_1, \ldots, v_{i-1}$: soient $q_1, \ldots, q_{i-1}$ des entiers tels que $v' = q_1 v_1 + \cdots + q_{i-1} v_{i-1}$. Posons aussi $q_i = q$. On a donc $v = \sum_{k \leq i} q_k v_k$, d'où la conclusion voulue.

Corollaire 9.28. *Soit G un sous-groupe discret de $\mathbb{R}^n$. Pour que G soit un réseau de $\mathbb{R}^n$ de rang n, il faut et il suffit qu'il existe une partie bornée P de $\mathbb{R}^n$ telle que $G + P = \mathbb{R}^n$ (autrement dit, que G soit co-compact).*

Démonstration : soit $(g_1, \ldots, g_r)$ une base de G. Si G est un réseau de rang n, on a $r = n$ et on peut prendre pour P le parallélépipède de côtés $g_1, \ldots, g_n$, c'est-à-dire l'ensemble des $\sum_{i=1}^n x_i g_i$, avec $x_i \in [0, 1]$ pour tout i.

Inversement, soit P une partie compacte de $\mathbb{R}^n$ telle que $G + P = \mathbb{R}^n$. Soit$v$ un vecteur quelconque de $\mathbb{R}^n$. Pour tout entier $m \geq 1$, on peut écrire $mv = g_m + p_m$, où $g_m \in G$ et $p_m \in P$; comme P est borné, on en déduit que $v = \frac{1}{m} g_m + O(1/m)$ lorsque m tend vers $+\infty$. En outre, $\frac{1}{m} g_m$ appartient au sous-espace vectoriel V engendré par $(g_1, \ldots, g_r)$. Passant à la limite, il vient $v \in V$ (regarder les coordonnées de v après avoir complété $(g_1, \ldots, g_r)$ en une base ; se rappeler éventuellement qu'un sous-espace de $\mathbb{R}^n$ est fermé). Comme v est arbitraire, $V = \mathbb{R}^n$ et $(g_1, \ldots, g_r)$ engendre $\mathbb{R}^n$. Puisque c'est une famille libre, c'est une base de $\mathbb{R}^n$ et G est un réseau de rang n.

9.6 Volumes et indices

Soit G un réseau de $\mathbb{R}^n$ de rang n et soit $(v_1, \ldots, v_n)$ une base de G qui est une famille libre de $\mathbb{R}^n$. Posons $V(G) = |\det(v_1, \ldots, v_n)|$, le déterminant étant pris par rapport à la base canonique de $\mathbb{R}^n$. C'est le volume du parallélépipède de $\mathbb{R}^n$ de côtés $v_1, \ldots, v_n$.

Si $(u_1, \ldots, u_n)$ est une autre base de G, il existe une matrice $A \in \mathrm{GL}_n(\mathbb{Z})$ telle que $(u_1, \ldots, u_n) = (v_1, \ldots, v_n)$. Par conséquent,

$$\det(u_1, \ldots, u_n) = \det(A) \det(v_1, \ldots, v_n) = \pm \det(v_1, \ldots, v_n) \ .$$

En particulier, $|\det(u_1,\dots,u_n)| = |\det(v_1,\dots,v_n)|$ ce qui montre que $V(G)$ ne dépend pas du choix de la base $(v_1,\dots,v_n)$ et justifie la notation adoptée. On appelle $V(G)$ le covolume du réseau G. On a par exemple, $V(\mathbb{Z}^n) = 1$. Si G est un réseau et λ un nombre réel non nul, l'ensemble λG des λg, pour $g \in G$, est un réseau et $V(\lambda G) = |\lambda^n| V(G)$. En effet, si $(u_1,\dots,u_n)$ est une base de G, $(\lambda u_1,\dots,\lambda u_n)$ est une base de λG.

Soit G' un sous-groupe de G. C'est en particulier un sous-groupe discret de $\mathbb{R}^n$ et, d'après le théorème ci-dessus, c'est un groupe abélien libre engendré par une famille libre $(u_1,\dots,u_r)$ de $\mathbb{R}^n$. Pour que G' engendre $\mathbb{R}^n$, il faut et il suffit que l'on ait $r = n$.

Proposition 9.29. *Le groupe quotient G/G' est fini si et seulement si $r = n$, c'est-à-dire si et seulement si G' est aussi un réseau de $\mathbb{R}^n$ de rang n. Le cardinal de G/G' est alors égal à $V(G')/V(G)$.*

Démonstration : laissée en exercice.

9.7 Minimas d'une forme quadratique définie positive

Soit q une forme quadratique sur $\mathbb{R}^n$ et soit Q sa matrice dans la base canonique. On a donc $q(x) = {}^t xQx$ pour tout vecteur colonne $x \in \mathbb{R}^n$. Définissons le discriminant de q, noté $\mathrm{Disc}(q)$, comme le déterminant de Q.

Supposons q définie positive, c'est-à-dire $(x) > 0$ pour tout $x \in \mathbb{R}^n$, $x \neq 0$. Alors, $\mathrm{Disc}(q) > 0$.

Le premier énoncé généralise en toute dimension le théorème que nous avons vu en dimension 2 au début du chapitre.

Théorème 9.30. *(Hermite, 1854) Il existe un vecteur $u \in \mathbb{Z}^n$, $u \neq 0$, tel que*

$$q(u) \leq \left(\frac{4}{3}\right)^{(n-1)/2} \mathrm{Disc}(q)^{1/n} \ .$$

Plus généralement, il existe n vecteurs $u_1,\dots,u_n \in \mathbb{Z}^n$, linéairement indépendants, tels que

$$q(u_1)\cdots q(u_n) \leq \left(\frac{4}{3}\right)^{n(n-1)/2} \mathrm{Disc}(q) \ .$$

Démonstration : comme q est définie positive, $q(x)$ tend vers l'infini lorsque $\|x\| \longrightarrow \infty$; en particulier, il existe un vecteur non nul $u \in \mathbb{Z}^n$ en lequel $q(u)$ est minimale.

Les coordonnées de u sont premières entre elles : sinon, il existerait un entier $d > 1$ et un vecteur $u' \in \mathbb{Z}^n$ tel que $u = du'$; alors, $q(u) = d^2 q(u')$, d'où $0 < q(u') < q(u)$ ce qui contredit le choix de u. D'après le corollaire ci-dessus, il existe une matrice $U \in \mathrm{GL}_n(\mathbb{Z})$ dont u est la première colonne. La forme quadratique $q(Uy)$ est définie positive, de même discriminant que q ; puisque $U \in \mathrm{GL}_n(\mathbb{Z})$, elle atteint son minimum sur $\mathbb{Z}^n \setminus \{0\}$ en $(1,0,\dots,0)$.

Notons $(b_{i,j})$ la matrice de la forme quadratique $q(Uy)$; on a donc

$$q(Uy) = \sum_{i,j=1}^{n} b_{i,j} y_i y_j = b_{1,1}\left(y_1 + \sum_{i=2}^{n} \frac{b_{1,i}}{b_{1,1}} y_i\right)^2 + q'(y') \ ,$$

où q' est une forme quadratique sur $\mathbb{R}^{n-1}$ en la variable $y' = (y_2, \ldots, y_n)$.

Si l'on pose $y'_1 = y_1 + \sum_{i=2}^n \frac{b_{1,i}}{b_{1,1}} y_i$, le changement de variables

$$(y_1, \ldots, y_n) \longmapsto (y'_1, y_2, \ldots, y_n)$$

transforme la forme $q(Uy)$ en la forme $b_{1,1}(y'_1)^2 + q'(y')$ dont le discriminant est $b_{1,1}\mathrm{Disc}(q')$. Comme ce changement de variables est de déterminant 1, on a on a $b_{1,1}\mathrm{Disc}(q'(y')) = \mathrm{Disc}(q(Uy)) = \mathrm{Disc}(q)$.

Par récurrence, il existe un vecteur $y' = (y_2, \ldots, y_n) \in \mathbb{Z}^{n-1}$, non nul, tel que $q'(y') \leq \left(\frac{4}{3}\right)^{(n-2)/2} \mathrm{Disc}(q')^{1/(n-1)}$. Soit y_1 l'entier le plus proche de $-\sum_{i=2}^n \frac{b_{1,i}}{b_{1,1}} y_i$ et posons $y = (y_1, y_2, \ldots, y_n)$. Alors,

$$q(Uy) \leq \frac{b_{1,1}}{4} + \left(\frac{4}{3}\right)^{(n-2)/2} \mathrm{Disc}(q')^{1/(n-1)} \ .$$

En outre $q(Uy) \geq b_{1,1}$. On en déduit que

$$\frac{3b_{1,1}}{4} \leq \left(\frac{4}{3}\right)^{(n-2)/2} (\mathrm{Disc}(q)/b_{1,1})^{1/(n-1)} \ .$$

Mettant cette expression à la puissance $n-1$, on trouve

$$\left(\frac{3b_{1,1}}{4}\right)^{n-1} b_{1,1} \leq \left(\frac{4}{3}\right)^{(n-1)(n-2)/2} \mathrm{Disc}(q) \ ,$$

d'où

$$b_{1,1}^n \leq \left(\frac{4}{3}\right)^{(n-1)(n-2)/2+(n-1)} \mathrm{Disc}(q) = \left(\frac{4}{3}\right)^{n(n-1)/2} \mathrm{Disc}(q) \ .$$

La première partie du théorème suit.

Démontrons aussi la seconde assertion par récurrence. Il existe ainsi des vecteurs $u'_2, \ldots, u'_n \in \mathbb{Z}^{n-1}$, linéairement indépendants, tels que

$$q'(u'_2) \ldots q'(u'_n) \leq \left(\frac{4}{3}\right)^{(n-1)(n-2)/2} \mathrm{Disc}(q') \ .$$

Pour $i \in \{2, \ldots, n\}$, définissons un vecteur $u_i \in \mathbb{Z}^n$ comme suit : si u'_i a pour coordonnées $(y_2, \ldots, y_n)$, choisissons pour y_1 l'entier le plus proche de $-\sum_{i=2}^n \frac{b_{1,i}}{b_{1,1}} y_i$ et posons $u_i = (y_1, \ldots, y_n)$. Alors, pour tout $i \in \{2, \ldots, n\}$,

$$q(Uu_i) \leq \frac{b_{1,1}}{4} + q'(u'_i) \leq \frac{q(Uu_i)}{4} + q'(u'_i)$$

et $q(Uu_i) \leq \frac{4}{3} q'(u'_i)$. On a ainsi

$$\begin{aligned} q(Uu_1)q(Uu_2)\ldots q(Uu_n) &\leq b_{1,1}\left(\frac{4}{3}\right)^{n-1} q'(u'_2)\ldots q'(u'_n) \\ &\leq \left(\frac{4}{3}\right)^{n-1}\left(\frac{4}{3}\right)^{(n-1)(n-2)/2} \mathrm{Disc}(q')b_{1,1} \\ &\leq \left(\frac{4}{3}\right)^{n(n-1)/2} \mathrm{Disc}(q) \ . \end{aligned}$$

Les vecteurs $u'_2, \ldots, u'_n$ sont linéairement indépendants, donc les vecteurs $u_2, \ldots, u_n$ aussi. Comme seule la première coordonnée de u_1 n'est pas nulle, u_1 n'appartient pas à l'espace engendré par les vecteurs $u_2, \ldots, u_n$ et la famille $(u_1, \ldots, u_n)$ est libre. Le théorème est ainsi démontré.

Le théorème précédent concerne le comportement d'une forme quadratique définie positive vis à vis du réseau $\mathbb{Z}^n$. Dans la pratique, il convient d'en énoncer une variante où interviennent un réseau et une forme quadratique arbitraires.

Corollaire 9.31. *Soit G un réseau de $\mathbb{R}^n$ de rang n et soit q une forme quadratique définie positive sur $\mathbb{R}^n$. Il existe un élément $g \in G$, non nul, tel que $q(g) \leq \left(\frac{4}{3}\right)^{(n-1)/2} (\mathrm{Disc}(q)V(G)^2)^{1/n}$. Il existe des éléments $g_1, \ldots, g_n$ de G, linéairement indépendants, tels que*

$$q(g_1) \ldots q(g_n) \leq \left(\frac{4}{3}\right)^{n(n-1)/2} \mathrm{Disc}(q)V(G)^2 \ .$$

Démonstration : soit $(v_1, \ldots, v_n)$ une base du réseau G et considérons la forme quadratique q' sur $\mathbb{R}^n$ donnée par

$$q'(x_1, \ldots, x_n) = q(x_1 v_1 + \cdots + x_n v_n) \ .$$

Son discriminant est égal à $\mathrm{Disc}(q) \det(v_1, \ldots, v_n)^2 = \mathrm{Disc}(q)V(G)^2$. Le corollaire en découle aussitôt.

Corollaire 9.32. *Tout réseau G de $\mathbb{R}^n$ contient un point non nul g tel que $\|g\| \leq (4/3)^{(n-1)/4} V(G)^{1/n}$.*

Démonstration : c'est le cas particulier où q est la forme quadratique donnée par $q(v) = \|v\|^2$.

On appelle constante de Hermite le plus petit nombre réel γ_n tel que tout réseau G de $\mathbb{R}^n$ contienne un point non nul g tel que $\|g\|^2 \leq \gamma_n V(G)^{2/n}$. On a donc surement $\gamma_n \leq (4/3)^{(n-1)/2}$.

Si cette majoration est une égalité pour $n = 1$ ou 2 (considérer le réseau de base 1 et $e^{2i\pi/3}$ dans $\mathbb{C} \simeq \mathbb{R}^2$), elle est très grossière lorsque n grandit. On peut en effet démontrer que lorsque n tend vers l'infini,

$$\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1,744}{2\pi e} \ ;$$

la croissance de γ_n est donc linéaire et non exponentielle ! Signalons qu'on en connaît la valeur exacte jusque $n = 8$, mais pas au-delà.

9.8 Somme de quatre carrés

Dans ce paragraphe, on démontre par les méthodes de géométrie des nombres le théorème de Lagrange selon lequel tout entier positif est somme de quatre carrés.

Lemme 9.33. *Considérons r formes linéaires $\ell_1, \ldots, \ell_r$ sur $\mathbb{Z}^n$ et des entiers strictement positifs $d_1, \ldots, d_r$. L'ensemble G des éléments $x \in \mathbb{Z}^n$ tels que $l_i(x) \equiv 0 \bmod d_i$ est un réseau de $\mathbb{R}^n$ tel que $V(G) \leq d_1 \ldots d_r$.*

Démonstration : d'après la proposition ci-dessus, il suffit de démontrer que le groupe $\mathbb{Z}^n/G$ est fini de cardinal au plus $d_1 \ldots d_r$. Or, l'application $L : \mathbb{Z}^n \longrightarrow \prod_{i=1}^r (\mathbb{Z}/d_i\mathbb{Z})$ donnée par $L(x) = (\ell_i(x) \bmod d_i)$ est un homomorphisme de groupes abéliens dont le noyau est égal à G. Par suite, $\mathbb{Z}^n/G$ est isomorphe à un sous-groupe de $\prod_{i=1}^r (\mathbb{Z}/d_i\mathbb{Z})$. Il est en particulier fini et son cardinal divise le produit $d_1 \ldots d_r$.

Lemme 9.34. *Pour tout nombre premier p, il existe des entiers a et b tels que $a^2 + b^2 + 1$ soit multiple de p.*

Démonstration : en effet, il y a $1+(p-1)/2=(p+1)/2$ éléments de la forme a^2, avec $a\in\mathbb{Z}/p\mathbb{Z}$, et autant d'éléments de la forme $1-b^2$, avec $b\in\mathbb{Z}/p\mathbb{Z}$. Puisque $(p+1)/2+(p+1)/2=p+1>p$, il existe a et b dans $\mathbb{Z}/p\mathbb{Z}$ tels que $a^2=1-b^2$, d'où le lemme.

Théorème 9.35. *(Lagrange)Tout entier positif est somme de quatre carrés : pour tout entier $n>0$, il existe des nombres entiers x,y,z,t tels que $n=x^2+y^2+z^2+t^2$.*

Démonstration : il suffit de traiter le cas où n est sans facteur carré. Pour tout facteur premier p de n, choisissons des entiers a_p et b_p tels que $a_p^2+b_p^2+1$ soit multiple de p. Considérons alors l'ensemble G des éléments (x,y,z,t) de $\mathbb{Z}^2$ vérifiant les congruences suivantes :

$$x=a_pz+b_pt \bmod p\ ,\qquad y=b_pz-a_pt \bmod p\ .$$

D'après le lemme ci-dessus, G est un réseau de $\mathbb{R}^4$ tel que $V(G)$ est majoré par le produit des carrés des facteurs premiers de n ; en particulier, $V(G)\leq n^2$.

D'après le théorème d'Hermite, il existe un élément non nul (x,y,z,t) de G tel que

$$x^2+y^2+z^2+t^2\leq(4/3)^{3/2}V(G)^{1/2}<2n\ ,$$

puisque $(4/3)^3=64/27\leq 3<4$. Posons $N=x^2+y^2+z^2+t^2$ et démontrons que $N=n$. Pour tout facteur premier p de n,

$$\begin{aligned}N=x^2+y^2+z^2+t^2 &\equiv (a_pz+b_pt)^2+(b_pz-a_pt)^2+z^2+t^2\\ &\equiv (a_p^2+b_p^2+1)z^2+(b_p^2+a_p^2+1)t^2 \bmod p\ ,\end{aligned}$$

donc $x^2+y^2+z^2+t^2$ est multiple de p. Par conséquent, N est multiple de n. Puisque $0<N<2n$, on a nécessairement $N=n$, ce qui conclut la démonstration du théorème de Lagrange.

9.9 Les théorèmes de Minkowski

Les théorèmes de Minkowski auquel ce paragraphe est consacré généralisent du cas d'une norme euclidienne au cas d'une norme quelconque les théorèmes de Hermite. La méthode inaugurée par Minkowski, mélangeant géométrie et théorie des nombres, était d'une très grande innovation au point qu'elle provoqua l'apparition d'une nouvelle branche de l'arithmétique : la géométrie des nombres.

Proposition 9.36. *Soit $\|\cdot\|$ une norme sur $\mathbb{R}^n$ et soit V le volume de la boule unité B. Soit r un entier naturel. Si $V\geq r2^n$, il existe dans $\mathbb{Z}^n$ des vecteurs $\pm u_1,\ldots,\pm u_r$ de normes ≤ 1 et deux à deux distincts.*

Démonstration : supposons d'abord que $V>r2^n$. Soit f la fonction indicatrice de la boule de centre 0 et de rayon $1/2$ et posons, pour $x\in\mathbb{R}^n$, $F(x)=\sum_{u\in\mathbb{Z}^n}f(x-u)$. Comme f est à support compact, c'est une somme finie ; plus précisément, les termes d'indice u sont nuls dès que

$\|u\| \geq \|x\| + 1$. Intégrons F sur le parallélépipède $P = [0,1]^n$; on trouve

$$\begin{aligned}
\int_P F &= \sum_{u\in\mathbb{Z}^n} \int_P f(x-u)dx \\
&= \sum_{u\in\mathbb{Z}^n} \int_{u+P} f(x)dx \\
&= \int_{\mathbb{R}^n} f(x)dx \\
&= \mathrm{Vol}(B(0,1/2)) \\
&= V/2^n \\
&> r \ .
\end{aligned}$$

Comme le volume de P est égal à 1, il existe au moins un point x de P tel que $F(x) > r$; comme F est à valeurs entières, on a donc $F(x) \geq r+1$ et il existe des éléments distincts $u_0, \ldots, u_r$ de $\mathbb{Z}^n$ tels que $f(x-u_i) \geq 1$, c'est-à-dire $\|x-u_i\| \leq 1/2$. Ordonnons les u_i suivant l'ordre lexicographique de leurs coordonnées. Alors, pour tout $i \in \{1,\ldots,r\}$, $u_i - u_0$ est un point de $\mathbb{Z}^n$ tel que $\|u_i - u_0\| \leq 1$. Ces vecteurs $u_i - u_0$ sont non nuls et deux-à- deux distincts ; de plus, si $u_i - u_0 = -(u_j - u_0)$, alors $u_0 = (u_i + u_j)/2$, ce qui contredit le fait que u_0 est le vecteur dont les coordonnées sont les plus petites dans l'ordre lexicographique. Les $2r$ vecteurs $\pm(u_i - u_0)$ sont donc non nuls, deux à deux distincts, à coordonnées entières et de normes ≤ 1. Cela conclut la démonstration lorsque $V > r2^n$.

Supposons maintenant que l'on ait l'égalité $V = r2^n$ et considérons les normes $\alpha\|\cdot\|$, où α est un nombre réel > 1. Comme le volume de la boule unité pour cette nouvelle norme est $\alpha^n V > r2^n$, il existe $2r$ vecteurs $\pm v_{1,\alpha}, \ldots, \pm v_{r,\alpha}$, non nuls et deux à deux distincts dans $\mathbb{Z}^n$ tels que $\|v_{i,\alpha}\| \leq \alpha$ pour tout i. Faisons tendre α vers 1 ; comme les parties fermées bornées de $\mathbb{R}^n$ sont compactes, on peut trouver une suite de nombres réels (α_n) tels que $\alpha_n > 1$ et $\alpha_n \longrightarrow 1$ de sorte que pour tout i, la suite (v_{i,α_n}) converge ; notons v_i sa limite ; on a $\|v_i\| \leq 1$. Une suite convergente de vecteurs à coordonnées entières est stationnaire ; on a donc $v_{i,\alpha_n} = v_i$ pour n assez grand. En particulier, les $2r$ vecteurs $\pm v_1, \ldots, \pm v_r$ sont non nuls et deux à deux distincts. Cela termine la démonstration.

Théorème 9.37. *Soit G un réseau de $\mathbb{R}^n$; soit $\|\cdot\|$ une norme sur $\mathbb{R}^n$, B sa boule unité et* $\mathrm{Vol}(B)$ *son volume. Il existe un vecteur non nul $u \in G$ tel que $\|u\| \leq 2(V(G)/\mathrm{Vol}(B))^{1/n}$.*

Démonstration : soit A la matrice d'une base $(u_1, \ldots, u_n)$ de G et considérons la norme $\|\cdot\|'$ sur $\mathbb{R}^n$ donnée par $\|x\|' = \alpha\|Ax\|$, où

$$\alpha = \frac{1}{2}(\mathrm{Vol}(B)/V(G))^{1/n} \ .$$

La boule unité B' pour cette norme est égale à $\alpha^{-1}A^{-1}B$, son volume $\mathrm{Vol}(B')$ est donc égal à $\mathrm{Vol}(B)/\alpha^n|\det A| = 2^n V(G)/|\det A|$. Par ailleurs, on a $V(G) = |\det A|$ par définition, d'où $\mathrm{Vol}(B') = 2^n$. D'après la proposition, il existe un vecteur non nul $x \in \mathbb{Z}^n$ tel que $\|x'\| \leq 1$. Alors, le vecteur $u = x_1u_1 + \cdots + x_nu_n$ de G vérifie

$$\|u\| = \|Ax\| = \|x\|'/\alpha \leq 2(V(G)/\mathrm{Vol}(B))^{1/n} \ .$$

Le théorème est ainsi démontré.

Dans le cas où la norme est euclidienne, il convient de comparer le théorème de Minkowski avec celui d'Hermite. Commençons par rappeler le volume d'un ellipsoïde :

Lemme 9.38. *Soit q une forme quadratique définie positive sur $\mathbb{R}^n$ et soit B l'ensemble des $x \in \mathbb{R}^n$ tels que $q(x) \leq 1$. Alors,* $\mathrm{Vol}(B) = \pi^{n/2}\Gamma(1+n/2)^{-1}\mathrm{Disc}(q)^{-1/2}$.

Démonstration : la forme q définit un produit scalaire sur $\mathbb{R}^n$. Soit A la matrice d'une base orthonormée pour q, de sorte que $q(Ax) = \|x\|^2$, où $\|\cdot\|$ désigne la norme euclidienne usuelle sur $\mathbb{R}^n$. Si B_1 désigne la boule unité de $\mathbb{R}^n$ (pour la norme euclidienne), on a donc $B = A(B_1)$ et $\mathrm{Vol}(B) = |\det A|\mathrm{Vol}(B_1)$. D'autre part, $\mathrm{Disc}(q) = |\det A|^{-2}$ car le discriminant de la forme quadratique $\|\cdot\|^2$ est égal à 1.

Il suffit donc de démontrer que $\mathrm{Vol}(B_1) = \pi^{n/2}/\Gamma(1+n/2)$. Pour cela, on calcule $I_n = \int_{\mathbb{R}^n} \exp(-\|x\|^2)dx$. Un changement de variables en coordonnées polaires fournit

$$I_n = S_n \int_0^\infty \exp(-r^2) r^{n-1} dr \ ,$$

où S_n est la surface de la sphère unité de $\mathbb{R}^n$. On a donc

$$I_n = S_n \int_0^\infty \exp(-x) x^{(n-1)/2} \frac{dx}{2\sqrt{x}} = \frac{S_n}{2} \int_0^\infty \exp(-x) x^{n/2-1} dx = \frac{S_n \Gamma(n/2)}{2} \ ,$$

où Γ désigne la fonction Γ d'Euler. D'autre part, le volume de la boule unité se calcule comme suit :

$$\mathrm{Vol}(B_1) = S_n \int_0^1 r^{n-1} dr = \frac{S_n}{n} \ .$$

Par suite,

$$\mathrm{Vol}(B_1) = \frac{2I_n}{n\Gamma(n/2)} = \frac{I_n}{\Gamma(1+n/2)} \ .$$

Enfin, le théorème de Fubini assure que $I_n = (I_1)^n$; de même, $I_2 = (I_1)^2$ d'où $I_n = (I_2)^{n/2}$. En dimension 1 et 2, le volume de la boule unité vaut respectivement 2 et π. Par suite,

$$I_1 = 2\Gamma(1+1/2) = 2\Gamma(3/2) = \Gamma(1/2) \qquad \text{et} \qquad I_2 = \pi\Gamma(2) = \pi \ .$$

On en déduit $\Gamma(1/2) = \sqrt{\pi}$ et $\mathrm{Vol}(B_1) = \pi/\Gamma(1+n/2)$.

La constante c_M figurant au membre de droite du théorème de Minkowski est donc égale à

$$\begin{aligned} c_M - 2V(G)/\mathrm{Vol}(B)^{1/n} &= 2V(G)\pi^{-1/2}\Gamma(1+n/2)^{1/n}\mathrm{Disc}(q)^{1/2n} \\ &= V(G)\mathrm{Disc}(q)^{1/2n}\left(\frac{2}{\sqrt{\pi}}\Gamma(1+n/2)^{1/n}\right) \ . \end{aligned}$$

D'après la formule de Stirling,

$$\Gamma(1+n/2) = (n/2)\Gamma(n/2) \sim (n/2)^{1+n/2} e^{-n/2}\sqrt{\pi n}$$

et il en résulte

$$\Gamma(1+n/2)^{1/n} \sim (n/2)^{1/2} e^{-1/2} \sim \frac{\sqrt{n}}{\sqrt{2e}} \ .$$

Autrement dit, lorsque n tend vers l'infini,

$$c_M^2 \sim V(G)^2 \mathrm{Disc}(q)^{1/n} \frac{4n}{2\pi e}$$

et le théorème de Minkowski implique l'inégalité

$$\gamma_n \leq \frac{4n}{2\pi e} + o(n) \ .$$

Ce résultat est d'une bien meilleure qualité que ce que fournit le théorème de Hermite qui se contente d'affirmer que $\gamma_n \leq (4/3)^{(n-1)/2}$. Cependant, on observera que lorsque $n = 2$, le théorème de Minkowski fournit la majoration $\gamma_2 \leq 4\pi\Gamma(3) = 2/\pi$ alors que l'on a $\gamma_2 = 2/\sqrt{3}$.

De manière analogue au théorème de Hermite, Minkowski a aussi démontré l'existence d'une base de $\mathbb{R}^n$ formé de vecteurs entiers d'un réseau et de normes petites. La démonstration étant nettement plus délicate, nous nous contentons de l'énoncer :

Théorème 9.39. *Soit G un réseau de $\mathbb{R}^n$; soit $\|\cdot\|$ une norme sur $\mathbb{R}^n$, B sa boule unité et $\mathrm{Vol}(B)$ son volume. Il existe une base $(u_1, \ldots, u_n)$ de $\mathbb{R}^n$ formée de vecteurs de G tels que*

$$\|u_1\| \ldots \|u_n\| \leq 2^n \mathrm{Vol}(B)/V(G) \ .$$