5. Complément I : Déterminant d'un groupe abélien fini

Soit G un groupe fini. Suivant Dedekind, le *déterminant de* G est le polynôme

$$\det G := \det(X_{gh^{-1}})_{g,h\in G},$$

où les X_g sont des indéterminées indexées par les éléments de G. C'est donc un polynôme homogène de degré $|G|$ en les X_g, et la question posée par Dedekind est de le factoriser dans $\mathbb{C}[\{X_g,\, g\in G\}]$. Par exemple, $\det \mathbb{Z}/n\mathbb{Z}$ est le déterminant de la matrice circulante $(X_{i-j \bmod n})_{1\le i,j\le n}$, et pour le groupe de Klein on a

$$\det \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} = \det\begin{bmatrix} E & A & B & C\\ A & E & C & B\\ B & C & E & A\\ C & B & A & E\end{bmatrix},$$

avec $E = X_{(\bar 0,\bar 0)}$, $A = X_{(\bar 1,\bar 0)}$, $B = X_{(\bar 0,\bar 1)}$ et $C = X_{(\bar 1,\bar 1)}$.

Proposition 5.1. (Dedekind) *Si G est un groupe abélien fini, on a*

$$\det G = \prod_{\chi\in\widehat{G}}\Big(\sum_{g\in G}\chi(g)X_g\Big).$$

Démonstration — Soit $(x_g)_g \in \mathbb{C}^G$. Il suffit de montrer l'égalité des deux polynômes de l'énoncé aprés évaluation des X_g en x_g. Considérons l'endomorphisme $u = \sum_{g\in G} x_g \mathrm{R}_g$ de $\mathrm{L}^2(G)$. Notons $e_h : G\to\mathbb{C}$ la fonction caractéristique du singleton $\{h\}$. Les e_h, $h\in H$, forment une base de $\mathrm{L}^2(G)$. On a $\mathrm{R}_g(e_h) = e_{hg^{-1}}$, et donc $u(e_h) = \sum_{g\in G} x_g e_{hg^{-1}} = \sum_{g\in G} x_{g^{-1}h}e_g$. On en déduit que $\det(G)$, évalué en les x_g, coïncide avec $\det u$. Mais on a aussi $u(\chi) = (\sum_g x_g\chi(g))\chi$ pour tout $\chi\in\widehat{G}$. D'après le Théorème 2.1, cela conclut si G est abélien, car les χ forment une base de $\mathrm{L}^2(G)$ constituée de vecteurs propres de u, de valeurs propres les $\sum_g \chi(g)x_g$. □

Exemple 5.2. Par exemple, on retrouve la formule classique pour le déterminant circulant $\det \mathbb{Z}/n\mathbb{Z} = \prod_{\zeta^n=1}(\sum_{i\in\mathbb{Z}/n\mathbb{Z}}\zeta^i X_i)$, et on a aussi la formule $\det \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} = (E+A+B+C)(E-A+B-C)(E+A-B-C)(E-A-B+C)$ (pourquoi ?).

Pour G non commutatif, la démonstration ci-dessus montre que $\det G$ est divisible par $\prod_{\chi\in\widehat{G}}(\sum_{g\in G}\chi(g)X_g)$, mais qu'il a d'autres facteurs. C'est en souhaitant déterminer ces facteurs que Frobenius a inventé la théorie des représentations des groupes finis : nous reviendrons sur ce point dans le dernier chapitre. Par exemple pour $G = \mathrm{S}_3$, alors $\det G$ contient aussi un facteur irréductible de degré 2 (avec multiplicité 2).

6. Complément II : Réseaux et sous-groupes fermés de $\mathbb{R}^n$

Soit V un $\mathbb{R}$-espace vectoriel de dimension finie, que l'on munit de sa topologie d'espace vectoriel normé. On se propose dans ce complément de déterminer les sous-groupes fermés du groupe additif de V. Le cas de la dimension 1 a déjà été traité dans la Proposition 7.3 : un sous-groupe fermé de $\mathbb{R}$ est soit égal à $\mathbb{R}$, soit de la forme $a\mathbb{Z}$ avec $a\in\mathbb{R}$. Une notion clé en général est celle de sous-groupe *discret*.

PROPOSITION-DÉFINITION 6.1. *Soit H un sous-groupe de V. On dit que H est* discret *dans V si les propriétés équivalentes suivantes sont satisfaites :*

(i) il existe un voisinage U de 0 dans V avec $U \cap H = \{0\}$,

(ii) pour tout compact K de V alors $K \cap H$ est fini.

DÉMONSTRATION — Il est clair que l'on a (ii) $\implies$ (i) pour tout sous-ensemble H de V. Soient U comme au (i) et K un compact de V. Si $K \cap H$ est infini, il existe une suite d'éléments distincts k_n de $K \cap H$. Quitte à extraire, on peut la supposer convergente dans V par compacité. Les éléments $k_{n+1} - k_n$ sont dans H, non nuls, tendent vers 0, et sont donc dans U pour n assez grand : une contradiction. □

On rappelle qu'un *réseau* de V est un sous-groupe de V de la forme

$$H = \bigoplus_{i=1}^{n} \mathbb{Z} e_i$$

où $e_1, \ldots, e_n$ une base de l'espace vectoriel V. Un réseau est discret. En effet, par équivalence des normes il suffit d'observer que pour $\|\cdot\|$ la norme sup. dans la base des e_i, et $m \geq 0$ entier, on a $|\{h \in H \mid \|h\| \leq m\}| = (2m+1)^n < +\infty$. Le résultat remarquable est que la réciproque est aussi vraie.

THÉORÈME 6.2. *Soient H un sous-groupe discret d'un $\mathbb{R}$-espace vectoriel de dimension finie et V le sous-espace engendré par H. Alors H est un réseau de V. En particulier, H est un groupe abélien libre de rang* $\dim V$.

DÉMONSTRATION — Comme H engendre V comme $\mathbb{R}$-espace vectoriel, il contient une $\mathbb{R}$-base de V (base incomplète). Fixons $(e_1, \ldots, e_n)$ une base de V avec $e_i \in H$ pour tout i. Tout élément $v = \sum_{i=1}^n v_i e_i$ de V, avec $v_i \in \mathbb{R}$, s'écrit aussi $v = [v] + \{v\}$ avec $[v] := \sum_{i=1}^n \lfloor v_i \rfloor e_i \in H$ et $\{v\} := \sum_{i=1}^n \{v_i\} e_i$, où $\lfloor x \rfloor$ et $\{x\}$ désignent respectivement la partie entière inférieure et la partie fractionnaire du réel x. Notons que $\{v\}$ est un élément du compact

$$\Pi = \{\sum_{i=1}^{n} x_i e_i \mid 0 \leq x_i \leq 1\}.$$

Pour $v \in H$ on constate $\{v\} = v - [v] \in H \cap \Pi$. Mais H étant discret, l'ensemble $X := H \cap \Pi$ est fini. Regardons alors la projection linéaire

$$f : V \to \mathbb{R},\ \sum_{i=1}^{n} v_i e_i \mapsto v_1.$$

Pour $h \in H$ on a $f(h) = f([h]) + f(\{h\})$ avec $f([h]) \in \mathbb{Z}$ et $f(\{h\}) \in f(X)$. Ainsi, $f(H)$ est un sous-groupe de $\mathbb{R}$, inclus dans la réunion finie des $\mathbb{Z} + f(x)$ avec $x \in X$. Il est donc discret dans $\mathbb{R}$, puis de la forme $\mathbb{Z}\lambda$ pour un certain $\lambda \in \mathbb{R}$ par la Proposition 7.3. On a aussi $f(H) \neq \{0\}$ car H n'est pas inclus dans l'hyperplan $U := \ker f$. Fixons $h_0 \in H$ tel que $\lambda = f(h_0)$. On a alors

$$H = \mathbb{Z} h_0 \oplus (H \cap U).$$

En effet, on a bien sûr $V = \mathbb{R} h_0 \oplus U$, donc la somme de droite est directe (et incluse dans H). Enfin, pour $h \in H$ il existe $n \in \mathbb{Z}$ avec $f(h) = n\lambda = f(nh_0)$, et donc on a bien $h = nh_0 + (h - nh_0) \in \mathbb{Z}h_0 + (H \cap U)$. On conclut par récurrence sur $\dim V$

car $H \cap U$ est clairement discret dans U, et engendre U comme $\mathbb{R}$-espace vectoriel. □

COROLLAIRE 6.3. *Tout sous-groupe de $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^m$ pour $m \leq n$.*

DÉMONSTRATION — Le groupe $\mathbb{Z}^n$ peut être vu comme un réseau de $\mathbb{R}^n$. Ses sous-groupes sont donc discrets dans $\mathbb{R}^n$, et engendrent un sous-espace vectoriel réel de dimension $m \leq n$. On conclut par le théorème. □

Pour une démonstration plus directe de ce résultat nous renvoyons à l'Exercice 3.11. Nous en verrons une généralisation lorsque nous parlerons de *modules sur les anneaux principaux*. On peut déduire enfin du Théorème 6.2 une classification de tous les sous-groupes *fermés* de $\mathbb{R}^n$.

THÉORÈME 6.4. *Soient V un $\mathbb{R}$-espace vectoriel de dimension finie et $H \subset V$ un sous-groupe fermé. Soient A le plus grand sous-espace vectoriel de V inclus dans H, W le sous-espace de V engendré par H, et B un supplémentaire de A dans W. Alors $H \cap B$ est un réseau de B, on a $H = A \oplus (H \cap B)$, et*

$$H \simeq \mathbb{R}^a \times \mathbb{Z}^b, \text{ avec } a = \dim A \text{ et } b = \dim B.$$

Nous allons d'abord montrer le lemme suivant.

LEMME 6.5. *Soit H un sous-groupe fermé du $\mathbb{R}$-espace vectoriel de dimension finie V. Si H n'est pas discret alors H contient une droite de V.*

DÉMONSTRATION — On fixe une norme $\|\cdot\|$ sur V. Si x est un réel, on notera $\lfloor x \rfloor \in \mathbb{Z}$ sa partie entière inférieure, vérifiant $x - \lfloor x \rfloor \in [0, 1[$. Si H n'est pas discret, il existe une suite $(h_n)_{n\geq 1}$ d'éléments de $H \smallsetminus \{0\}$ avec $h_n \to 0$ dans V. Si l'on pose $k_n = \lfloor 1/\|h_n\| \rfloor$ on a alors

$$k_n \in \mathbb{Z}_{\geq 0},\ k_n \to \infty \ \text{ et } \ \|k_n h_n\| \to 1$$

(car $|\,\|k_n\, h_n\| - k_n|h_n|| \leq |h_n|$). Par compacité des fermés bornés de V, et quitte à extraire une sous-suite, on peut supposer $k_n h_n \to e$, pour un certain $e \in V$ de norme 1. On a $e \in H$ car H est fermé dans V et $k_n h_n \in H$. Montrons $\mathbb{R}e \subset H$. Soit $\lambda \in \mathbb{R}$. On pose $a_n = \lfloor \lambda k_n \rfloor$ et $b_n = \lambda k_n - a_n \in [0, 1[$. On a alors $\lambda k_n h_n = a_n h_n + b_n h_n$, et en faisant tendre n vers l'infini on en déduit $a_n h_n \to \lambda e$, puis $\lambda e \in H$. □

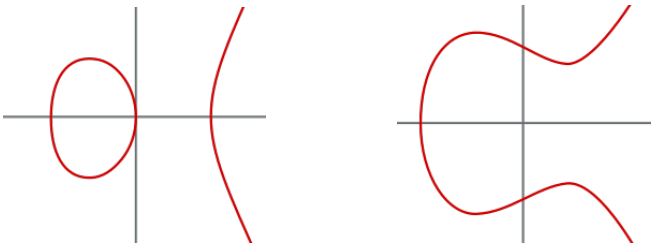
DÉMONSTRATION — (du Théorème 6.4) Comme la somme de deux sous-espaces de V inclus dans H est encore inclus dans H, le sous-espace A de l'énoncé existe, et coïncide avec le sous-espace de dimension maximale de V inclus dans H. Si B est un supplémentaire de A dans W, on constate que l'on $H = A \oplus (H \cap B)$. En effet, tout élément w de W s'écrit $w = a + b$ avec $a \in A$ et $b \in B$. Comme on a $A \subset H$, on a $w \in H$ si, et seulement si $b \in H$. Enfin, $H \cap B$ est un sous-groupe fermé de B (comme intersection), et il engendre B car H engendre W. Enfin, $H \cap B$ est discret dans B par le Lemme 6.5 et par définition de A. On conclut par le Théorème 6.2. □

7. Complément III : Courbes elliptiques (culturel)

On fixe un corps k, supposé de caractéristique $\neq 2, 3$ pour simplifier. Une *courbe elliptique* sur k est une courbe plane de la forme

$$C = \{(x, y) \in k^2 \mid y^2 = f(x)\},$$

où $f \in k[X]$ un polynôme de degré 3 *donné* et supposé sans racine double dans k. Par exemple pour $k = \mathbb{R}$, la courbe C est une courbe lisse qui a l'une des deux allures suivantes, selon que f a 3 ou 1 racines réelles.



L'ensemble C a une involution naturelle, $(x, y) \mapsto (x, -y)$, que l'on note simplement $P \mapsto -P$. Il sera important aussi de rajouter un point supplémentaire à C, noté O, auquel on pense comme étant à « l'infini verticalement », et on pose $E = C \coprod \{O\}$. La méthode des *cordes et des tangentes*[8] permet alors de définir une loi de composition $E \times E \to E, (P, Q) \mapsto P + Q$, de neutre O, de la manière suivante.[9] Si P et Q sont deux points de C, la *corde-tangente* associée est la droite affine (PQ) dans le cas $P \neq Q$, et la tangente à C en $P = Q$ sinon. Cette tangente est bien définie par les hypothèses sur f et k, et on la note encore (PQ).

(i) Si (PQ) n'est pas verticale, donc d'équation $y = ax + b$ avec $a, b \in k$, on constate que le système d'équations $y = ax+b$ et $y^2 = f(x)$, définissant l'intersection $C \cap (PQ)$, a toujours exactement trois solutions (avec possibles multiplicités), disons $\{\{P, Q, R\}\}$, et on pose $P + Q = -R$.

(ii) Si (PQ) est verticale, on pose $P + Q = O$.

Il se trouve que cette loi est associative, un fait géométrique peu évident que l'on peut vérifier péniblement par calcul direct, ou de manière plus élégante en utilisant le théorème de Bézout en géométrie projective. La loi $+$ est par définition commutative, et même alors une loi de groupe, l'inverse d'un point P étant le point $-P$ par définition. Voici quelques résultats connus remarquables sur ce groupe :

THÉORÈME 7.1. (Culturel) *Soit E une courbe elliptique sur le corps k.*

(i) (Weierstrass) *Si $k = \mathbb{C}$, alors $E \simeq \mathbb{C}/\Lambda$ pour un certain réseau Λ de $\mathbb{C}$.*

(ii) Si $k = \mathbb{R}$, alors E est isomorphe à $\mathrm{S}^1 \times \mathbb{Z}/2\mathbb{Z}$ ou à S^1.

(iii) (Mordell) *Si $k = \mathbb{Q}$, alors E est un groupe abélien de type fini.*

(iv) (Hasse) *Si $k = \mathbb{Z}/p\mathbb{Z}$, alors E est un groupe abélien fini à ≤ 2 générateurs, et on a $|p + 1 - |E|| < 2\sqrt{p}$.*

Les (i) et (ii) sont parfois vus dans le cours d'analyse complexe de première année. Notons que l'on en déduit par exemple $E[N] \simeq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ pour tout

8. Certains auteurs l'appellent aussi *méthode des sécantes et tangentes*.

9. Avec des connaissances élémentaires de géométrie projective on pourrait mieux comprendre l'apparition du point O et éviter la disjonction des cas (i) et (ii).

$N \geq 1$ dans le cas $k = \mathbb{C}$. (Que vaut $E[2]$ en général ? et $E[3]$?) Dans le cas $k = \mathbb{R}$, on est bien sûr dans le premier cas si f a 3 racines réelles, et dans le second s'il en a une seule. (Voyez-vous bien les cercles ?).

Dans le cas $k = \mathbb{Q}$, le (iii) exprime le fait remarquable que toutes les solutions de E s'expriment à partir d'un nombre fini d'entre elles par la méthode des cordes et tangentes. Nous renvoyons par exemple au livre assez élémentaire de Silverman-Tate *Rational points on elliptic curves* pour une démonstration. Pour $y^2 = x^3 + 1$ on peut par exemple montrer que l'on a $E \simeq \mathbb{Z}/6\mathbb{Z}$, avec pour générateur le point $(2, 3)$. En guise d'autre exemple (Billing, 1938), pour la courbe $y^2 = x^3 - 82x$ on a $E \simeq \mathbb{Z}^3$ avec pour $\mathbb{Z}$-base les points

$$P_1 = (-8, 12),\ P_2 = (-1, 9) \text{ et } P_3 = (49/4, 231/8).$$

Toujours dans le cas $k = \mathbb{Q}$, un résultat fameux (et difficile) de Mazur [10] décrit tous les cas possibles pour le groupe fini E_{tor} : ce sont les groupes cycliques $\mathbb{Z}/m\mathbb{Z}$ avec $m \leq 12$ et $m \neq 11$, ainsi que les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ avec $m \leq 4$. En revanche, on ne sait encore que peu de choses sur le rang de E. Le record, dû à Elkies, est un exemple de E dont le rang est 28. On conjecture maintenant que le rang ne prend qu'un nombre fini de valeurs possibles, alors qu'il y a quelques années on conjecturait le contraire ! Surtout, la fameuse *conjecture de Birch-Swinnerton Dyer* (une conjecture à un million de dollars) relie ce rang aux propriétés analytiques de la *fonction ζ de Hasse-Weil de E*.

L'inégalité de Hasse dans le cas particulier $y^2 = x^3 + 1$ du (iv) est le théorème principal du §1. Les courbes elliptiques sur les corps finis sont très utilisées en cryptographie.

10. Mazur, Barry, *Modular curves and the Eisenstein ideal*, Publ. Math. IHÉS. 47 (1) : 33–186 (1977).