CHAPITRE 2

Géométrie des nombres

Ce chapitre a pour but d'introduire la *géométrie des nombres*. Inventée[1] par Minkowski en 1896, elle consiste à donner une minoration du nombre des points d'un réseau de l'espace euclidien $\mathbb{R}^n$ appartenant à une partie convexe donnée, et ce en fonction de leurs volumes. Appliquées à certains réseaux de nature arithmétique, ces estimations ont des conséquences nombreuses et spectaculaires appartenant à la théorie des nombres. En guise d'illustrations, nous retrouverons dans ce chapitre les deux résultats classiques suivants, et bien d'autres du même genre :

Théorème 2.1. (Fermat, Euler) *Tout nombre premier congru à* 1 *modulo* 4 *est la somme de deux carrés d'entiers.*

Théorème 2.2. (Lagrange) *Tout entier est la somme de quatre carrés d'entiers.*

Les démonstrations originales de ces deux résultats (par Euler et Lagrange) étaient basées notamment sur un argument de "descente infinie". Il y en a eu depuis beaucoup d'autres. Dans la suite du cours, la théorie de Minkowski aura une autre application importante : elle nous permettra de borner de manière efficace le *nombre de classes* d'un corps de nombres. Elle permettrait aussi de démontrer le "sens difficile" du *théorème des unités* de Dirichlet.

Références : P. Samuel, *Théorie algébrique des nombres*, Éd. Hermann, chapitre 4.1.

I. Stewart & D. Tall, *Algebraic number theory*, Éd. Chapman & Hall, chapitres 6 et 7. Les preuves que nous donnerons des deux théorèmes ci-dessus sont notamment issues du chapitre 7 de ce livre.

1. Réseaux de $\mathbb{R}^n$

Fixons $n \geq 1$ un entier. Dans tout ce chapitre, V désignera l'espace vectoriel $\mathbb{R}^n$ muni d'une norme $|.|$ fixée quelconque. Rappelons qu'une partie $D \subset V$ est *discrète* si pour tout réel $r > 0$, l'ensemble $\{v \in D, |v| \leq r\}$ est fini. Cette propriété ne dépend pas du choix de $|.|$ par équivalence des normes sur V.

Définition 2.3. *Un réseau de V est un sous-groupe discret qui engendre V comme $\mathbb{R}$-espace vectoriel.*

1. Minkowski, "Geometrie der Zahlen", http://www.archive.org/details/geometriederzahl00minkrich.

Autrement dit, c'est une partie discrète $L \subset V$ telle que pour tout $a, b \in L$ alors $a - b \in L$, et telle qu'il existe $e_1, \ldots, e_n \in L$ qui est une base du $\mathbb{R}$-espace vectoriel V. L'exemple typique est le sous-groupe $\mathbb{Z}^n$ des éléments à coordonnées entières. En guise d'autre exemple, l'ensemble

$$L_0 := \{(a, b) \in \mathbb{Z}^2, a \equiv 2b \bmod 3\}$$

est aussi un réseau de $\mathbb{R}^2$. En effet, il est discret (car inclus dans $\mathbb{Z}^2$) et contient une base de $\mathbb{R}^2$, par exemple $(3, 0)$, $(0, 3)$.

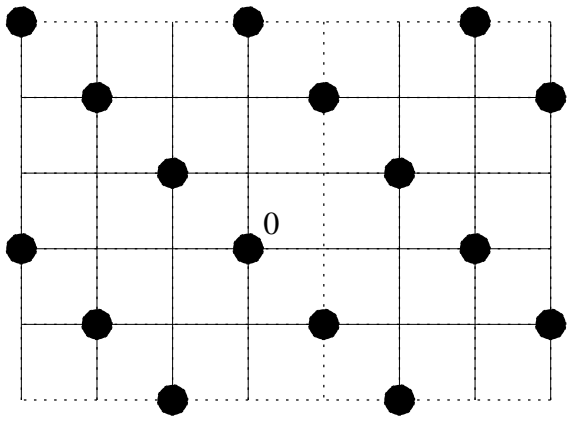

FIGURE 1. Le réseau L_0

On rappelle qu'une famille $e_1, \ldots, e_r$ d'un groupe abélien G est dite $\mathbb{Z}$-génératrice (ou simplement génératrice si le contexte ne prête pas à confusion) si tout élément de g s'écrit sous la forme $\sum_{i=1}^{r} m_i e_i$ avec $m_i \in \mathbb{Z}$ pour $i = 1, \ldots, r$. On dit que c'est une $\mathbb{Z}$-base si de plus une telle écriture est unique.

Théorème 2.4. *(Caractérisation algébrique des réseaux) Soit $L \subset V$ un sous-groupe. Les conditions suivantes sont équivalentes.*

(i) L est un réseau.

(ii) L admet une famille finie $\mathbb{Z}$-génératrice qui est une $\mathbb{R}$-base de V.

En particulier, tout réseau de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base à n éléments.

Donnons quelques exemples avant d'entamer la démonstration. Tout d'abord, il est évident que la base canonique $e_1, \ldots, e_n$ de $\mathbb{R}^n$ est une $\mathbb{Z}$-base de son sous-groupe $\mathbb{Z}^n$: on a $(m_i) = \sum_i m_i e_i$ pour tout $m_1, \ldots, m_n \in \mathbb{Z}$. De plus, remarquons aussi que $(1, -1)$ et $(2, 1)$ forment une $\mathbb{Z}$-base du réseau L_0 ci-dessus, de même que $(3, 0)$ et $(2, 1)$. Cela résulte en effet des écritures :

$$(a, b) = \frac{a - 2b}{3}\,(3, 0) + b\,(2, 1), \quad \text{et} \quad (a, b) = \frac{a - 2b}{3}\,(1, -1) + \frac{a + b}{3}\,(2, 1).$$

Le sens (ii) implique (i) du théorème est le plus simple, résulte de la proposition-definition qui suit.

Proposition-Définition 2.5. *Soit $e = \{e_1, \dots, e_n\}$ une base de l'espace vectoriel V, on note*

$$L(e) = \{m_1 e_1 + m_2 e_2 + \cdots + m_n e_n, \quad m_1, m_2, \dots, m_n \in \mathbb{Z}\}$$

le sous-groupe engendré par e, c'est un réseau de V.

Notons qu'il est évident que e est aussi une $\mathbb{Z}$-base de $L(e)$. En considérant la norme $|\sum_i v_i e_i| = \sup_i |v_i|$ sur V, il est clair que $L(e)$ est une partie discrète de V : $L(e)$ est bien un réseau. Le théorème ci-dessus affirme que tout réseau est de la forme $L(e)$ pour une certaine $\mathbb{R}$-base e de V.

Nous serons amené à introduire le *pavé fondamental* de V associé à la base $e = \{e_1, \dots, e_n\}$: c'est l'ensemble

$$\Pi(e) = \{\sum_{i=1}^{n} v_i e_i, v_i \in [0, 1[\} \subset V.$$

Sa propriété principale est la suivante :

Lemme 2.6. *Soit $e = \{e_1, \dots, e_n\}$ une base de V. Tout $v \in V$ s'écrit de manière unique sous la forme $\lambda + x$ avec $\lambda \in L(e)$ et $x \in \Pi(e)$.*

Démonstration — Désignons par $[t] \in \mathbb{Z}$ la partie entière inférieure du nombre réel t : c'est l'unique entier relatif m tel que $m \leq t < m + 1$. Si $v = \sum_{i=1}^{n} v_i e_i \in V$ alors $v = \lambda + x$ avec $\lambda = \sum_i [v_i] e_i \in L$ et $x = \sum_i (v_i - [v_i]) e_i \in \Pi(e)$. L'unicité de cette écriture se déduit coordonnée par coordonnée de celle de la partie entière inférieure, car (e_i) est une base de V. □

Le théorème résultera du lemme et de la proposition suivants.

Lemme 2.7. *Soient L un réseau de V et $e_1, \dots, e_n$ une base de $\mathbb{R}^n$ telle que $e_i \in L$ pour tout i. Alors $L(e)$ est d'indice fini dans L et il existe un entier $N \geq 1$ tel que $L \subset \frac{1}{N} L(e)$.*

Démonstration — Il est clair que l'on a $L(e) \subset L$. Vérifions tout d'abord que $L/L(e)$ est fini. En effet, d'après le lemme 2.6 tout élément $v \in V$ s'écrit de manière unique sous la forme $v = \lambda(v) + x(v)$ où $\lambda(v) \in L(e)$ et $x(v) \in \Pi(e)$. Comme $L(e) \subset L$, on en tire que $x(v) = v - \lambda(v) \in L \cap \Pi(e)$ si $v \in L$. Mais L est discret et $\Pi(e)$ est borné, et donc $L \cap \Pi(e)$ est fini ! En particulier, $|L/L(e)| \leq |L \cap \Pi(e)| < +\infty$.

D'après le théorème de Lagrange appliqué au groupe quotient fini $L/L(e)$, on constate que si l'on pose $N := |L/L(e)|$ alors $N \cdot L/L(e) = 0$, c'est-à-dire que $NL \subset L(e)$. □

Proposition 2.8. *Soit L un réseau de V et soit $\mathcal{B}$ l'ensemble des bases $e = \{e_1, \dots, e_n\}$ de V telles que $e_i \in L$ pour tout i. Alors il existe $e \in \mathcal{B}$ telle que $|\det(e_1, \dots, e_n)|$ est minimal, et pour tout tel e on a $L = L(e)$.*

Le déterminant de la famille de vecteurs e_i ci-dessus est pris de manière sous-entendue relativement à la base canonique de $V = \mathbb{R}^n$.

Démonstration — Comme L engendre l'espace vectoriel V, il contient une base de V, et donc $\mathcal{B}$ est non vide. Fixons $e \in \mathcal{B}$. Il est clair que $L(e) \subset L$. Soit $N \geq 1$ tel que $L \subset \frac{1}{N} L(e)$ (Lemme 2.7). Tout élément de L sécrit donc sous la forme $\sum_i \frac{m_i}{N} e_i$ avec $m_i \in \mathbb{Z}$ pour tout i. En particulier, pour tout $f = \{f_1, \dots, f_n\} \in \mathcal{B}$, on a par multi-linéarité de det

$$\det(f) \in N^{-n} \det(e)\mathbb{Z}.$$

Cet ensemble de valeurs est discret dans $\mathbb{R}$, on peut donc bien choisir $e \in \mathcal{B}$ tel que $|\det(e)|$ est minimal (nécessairement non nul).

Comme nous l'avons vu plus haut, tout élément $v \in L$ se décompose sous la forme $\lambda + x$ avec $\lambda \in L(e)$ et $x \in \Pi(e) \cap L$. Il suffit donc de voir $\Pi(e) \cap L = \emptyset$. Soit $v = \sum_i v_i e_i \in \Pi(e) \cap L$, de sorte que $v_i \in [0, 1[$ pour tout i. On cherche à montrer $v_i = 0$ pour tout i. Soit $1 \leq i \leq n$. Si $v_i \neq 0$, alors $v, e_1, \dots, \hat{e_i}, \dots, e_n$ est dans $\mathcal{B}$. Mais le caractère multi-linéaire alterné du déterminant entraîne

$$|\det(e_1, \dots, e_{i-1}, v, e_{i+1}, \dots, e_n)| = v_i |\det(e_1, \dots, e_n)| < |\det(e_1, \dots, e_n)|,$$

ce qui est absurde par minimalité de $\det(e)$. □ □

Proposition 2.9. *Soient $L \subset \mathbb{R}^n$ un réseau et $e = \{e_1, \dots, e_m\}$ une famille $\mathbb{Z}$-génératrice de L. Alors $m \geq n$. De plus, les conditions suivantes sont équivalentes :*

(i) e est une $\mathbb{Z}$-base de L,

(ii) e une base de l'espace vectoriel $\mathbb{R}^n$,

(iii) $m = n$.

En particulier, toutes les $\mathbb{Z}$-bases de L ont même cardinal n.

Démonstration — En effet, comme L engendre l'espace vectoriel $\mathbb{R}^n$, e est une famille génératrice de ce dernier, et donc $m \geq n$. L'équivalence de (ii) et (iii) est alors bien connue. De plus, (ii) implique trivialement (i).

Montrons enfin que (i) entraîne (iii). Si e est une $\mathbb{Z}$-base de L, alors $\psi : \mathbb{Z}^m \to L$, $(m_i) \mapsto \sum_i m_i e_i$ est un isomorphisme de groupes. Soit f une $\mathbb{Z}$-base de L à n éléments (Théorème 2.4). Il vient que $\psi^{-1}(f)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^m$ à n éléments. Mais $\mathbb{Z}^m$ est un réseau de $\mathbb{R}^m$ de manière naturelle, donc la première inégalité démontrée entraîne que $n \geq m$, et donc $n = m$. □

On se propose enfin de décrire toutes les $\mathbb{Z}$-bases d'un réseau à partir d'une seule. Considérons

$$\mathrm{GL}_n(\mathbb{Z}) := \{M \in \mathrm{M}_n(\mathbb{Z}) \mid \exists N \in \mathrm{M}_n(\mathbb{Z}), MN = \mathrm{I}_n\}.$$

Autrement dit, $\mathrm{GL}_n(\mathbb{Z})$ est le sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ constitué des matrices à coefficients entiers, et dont l'inverse aussi est à coefficients entiers.

Proposition 2.10. *(i)* $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathrm{M}_n(\mathbb{Z}),\ \det(M) = \pm 1\}$.

(ii) Soient $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ deux bases de V, et soit $P = (p_{i,j})$ la matrice des vecteurs f_j dans la base e_i, i.e. $f_j = \sum_i p_{i,j} e_i$. Alors e et f engendrent le même réseau, c'est-à-dire $L(e) = L(f)$, si, et seulement si, on a $P \in \mathrm{GL}_n(\mathbb{Z})$.

Démonstration — Vérifions le (i). Si $M, N \in \mathrm{M}_n(\mathbb{Z})$ satisfont $MN = \mathrm{I}_n$, alors $\det(M)\det(N) = 1$ avec $\det(M), \det(N) \in \mathbb{Z}$, donc $\det(M) = \pm 1$. Réciproquement, si $M \in \mathrm{M}_n(\mathbb{Z})$ et $\det(M) = \pm 1$, la relation $M\,{}^t\mathrm{Co}(M) = \det(M)\mathrm{I}_n$ assure que $M^{-1} = {}^t\mathrm{Co}(M)\det(M)^{-1} \in \mathrm{M}_n(\mathbb{Z})$.

Montrons le (ii). Remarquons que f_j appartient au réseau engendré par les e_i si, et seulement si, la j-ième colonne de P est à coefficients entiers. Introduisons par symmétrie la matrice $Q \in \mathrm{GL}_n(\mathbb{R})$ des vecteurs e_j dans la base f_i, on a donc $PQ = \mathrm{I}_n$. D'après la remarque ci-dessus, les e_i et les f_j engendrent le même réseau si, et seulement si, P et Q sont à coefficients entiers, c'est-à-dire si $P \in \mathrm{GL}_n(\mathbb{Z})$. □

Exemple 2.11. *Les éléments (a, b) et (c, d) de $\mathbb{Z}^2$ engendrent $\mathbb{Z}^2$ si, et seulement si, on a $ad - bc = \pm 1$.*

2. Lemme du corps convexe de Minkowski

Nous aurons besoin de considérer le volume (ou "mesure") de certaines parties de $\mathbb{R}^n$. On munit donc dans ce qui suit l'espace vectoriel $V = \mathbb{R}^n$ de la mesure de Lebesgue [2] que l'on notera μ, vérifiant $\mu([0,1]^n) = 1$.

Définition 2.12. *Soient L un réseau de $\mathbb{R}^n$ et X un sous-ensemble mesurable de $\mathbb{R}^n$. On dit que X est un* domaine fondamental *(pour l'action) de L si tout $v \in \mathbb{R}^n$ s'écrit de manière unique sous la forme $\lambda + x$ avec $\lambda \in L$ et $x \in X$.*

Il existe des domaines fondamentaux, d'après la caractérisation algébrique des réseaux et le :

Lemme 2.13. *Si e est une base de V alors $\Pi(e)$ est un domaine fondamental de $L(e)$ de mesure $|\det(e_1, \ldots, e_n)| \in \mathbb{R}_{>0}$.*

Démonstration — La mesurabilité de $\Pi(e)$ et la formule donnée pour sa mesure sont conséquences de la formule du jacobien ("changement de variables") en théorie de l'intégration. Le reste se déduit du lemme 2.6. □

2. Nous renvoyons par exemple au cours de W. Rudin *Real and complex analysis* pour la construction de la mesure de Lebesgue.

On constate, en considérant par exemple les pavés associés à différentes $\mathbb{Z}$-bases d'un réseau L, qu'il existe une multitude de domaines fondamentaux différents. Il en existe en fait encore bien plus qui ne sont pas des pavés (pourquoi ?). Remarquons cependant que les différents pavés fondamentaux de L ont tous même mesure. En effet, observons que si e et f sont des bases de V, et $P \in \mathrm{GL}_n(\mathbb{R})$ est la matrice des f_j dans la base e_i comme dans la proposition 2.10, le lemme ci-dessus entraîne

$$\mu(\Pi(f))) = |\det(P)|\mu(\Pi(e)) \tag{1}$$

En particulier, si $L(e) = L(f)$ alors $\det(P) = \pm 1$ car $P \in \mathrm{GL}_n(\mathbb{Z})$, et donc $\mu(\Pi(f)) = \mu(\Pi(e))$ comme il était annoncé. Cette observation est en fait un cas particulier du résultat suivant :

Lemme 2.14. (Blichfeldt) *Soient L un réseau de V, et $X, Y \subset V$ deux parties mesurables. On suppose que X est un domaine fondamental de V, et que $\forall x, y \in Y$, $x - y \in L \Rightarrow x = y$. Alors $\mu(Y) \leq \mu(X)$.*

En particulier, tous les domaines fondamentaux de L ont même mesure, égale à celle d'un pavé fondamental de L, et qui est donc finie et non nulle.

Il sera commode d'adopter la notation suivante : pour toute partie $A \subset V$ et pour $v \in V$, on notera $A + v = \{a + v, a \in A\}$. De même, $A - v = A + (-v)$.

Démonstration — En effet, X étant un domaine fondamental de L, V admet la décomposition en réunion dénombrable disjointe [3]

$$V = \coprod_{\lambda \in L} (X + \lambda).$$

En prenant l'intersection avec Y, on obtient $Y = \coprod_{\lambda \in L} Y \cap (X + \lambda)$. La relation évidente

$$(Y \cap (X + \lambda)) - \lambda = X \cap (Y - \lambda),$$

combinée avec l'invariance par translation de la mesure de Lebesgue, assure

$$\mu(Y) = \sum_{\lambda \in L} \mu(X \cap (Y - \lambda)).$$

Mais par hypothèse sur Y, les $Y - \lambda$ sont des parties disjointes de V quand λ varie dans L, de sorte que la somme de droite dans l'égalité ci-dessus est $\leq \mu(X)$, ce qui conclut. □

Définition 2.15. (Covolume d'un réseau) *Le covolume* $\mathrm{covol}(L)$ *d'un réseau $L \subset V$ est la mesure commune des domaines fondamentaux de L, c'est un élément de $\mathbb{R}_{>0}$.*

La proposition suivante est un résultat fondamental en géométrie des nombres. On rappelle qu'une partie $C \subset V$ est dite convexe si pour tous $v, v' \in C$, et tout $\lambda \in [0, 1]$, on a $\lambda v + (1 - \lambda)v' \in C$. Elle est dite symétrique si pour tout $v \in C$, alors $-v \in C$. L'exemple typique de partie convexe symétrique est obtenu en considérant une boule de V centrée en l'origine, relativement à une norme quelconque de l'espace V. Remarquons que si C est convexe symétrique, et si $x, y \in C$, alors $\frac{x-y}{2} = \frac{1}{2}x + \frac{1}{2}(-y) \in C$.

3. Le symbole $\coprod$ désigne une réunion disjointe.

Proposition 2.16. *(Lemme du corps convexe de Minkowski) Soit $C \subset V$ une partie mesurable symétrique convexe et soit L un réseau de V. Si* $\mathrm{covol}(L) < \frac{\mu(C)}{2^n}$, *ou si C est compact et* $\mathrm{covol}(L) \leq \frac{\mu(C)}{2^n}$, *alors il existe un élément non nul dans $L \cap C$.*

Démonstration — En effet, $L' := 2L \subset L$ est un réseau de V : si la base (e_i) engendre L alors la base $(2e_i)$ engendre L'. La formule du jacobien (1) montre $\mathrm{covol}(L') = 2^n \mathrm{covol}(L)$.

Supposons pour commencer $\mathrm{covol}(L') < \mu(C)$. Le lemme de Blichfeldt assure alors qu'il existe $x, y \in C$ distincts tels que $x - y \in 2L$. Mais C est convexe symétrique, donc l'élément $(x-y)/2$ est dans $C \cap L$ et non nul, ce que l'on cherchait.

Supposons maintenant $\mathrm{covol}(L') \leq \mu(C)$ mais que C est compact. Pour tout réel $\varepsilon > 0$, on considère

$$C_\varepsilon = \{v \in V \mid \exists x \in C, |v - x| < \varepsilon\}.$$

On vérifie immédiatement que c'est un ouvert borné convexe symétrique de mesure $> \mu(C)$. Le cas précédent montre donc $(L\backslash\{0\}) \cap C_\varepsilon \neq \emptyset$. Comme L est discret et C_ε est borné, $(L\backslash\{0\}) \cap C_\varepsilon$ est fini. Enfin, il décroît (pour l'inclusion) avec ε : il est donc constant pour ε assez petit, nécessairement égal à $(L\backslash\{0\}) \cap C$ car $\cap_\varepsilon C_\varepsilon = C$ (C est fermé), ce qui termine la preuve. □

Le lemme suivant est utile au calcul du covolume de certains réseaux.

Proposition 2.17. *Soient L un réseau de $\mathbb{R}^n$ et $L' \subset L$ un sous-groupe. Les assertions suivantes sont équivalentes :*

(i) L' est un réseau,

(ii) L' est d'indice fini dans L.

Si elles sont satisfaites, alors $\mathrm{covol}(L') = |L/L'| \,\mathrm{covol}(L)$.

Démonstration — Le sous-groupe L' est discret car L l'est. Supposons qu'il est d'indice fini dans L, disons h. Le théorème de Lagrange montre $hL \subset L'$. Comme L engendre $\mathbb{R}^n$ comme espace vectoriel, il en va de même pour hL puis de L'. Cela montre que (ii) entraîne (i). La réciproque se déduit du lemme 2.7. Vérifions maintenant l'assertion sur le covolume. Soit $h = |L/L'|$. Par définition il existe des éléments $\lambda_1, \ldots, \lambda_h \in L$ tels que

$$L = \coprod_{i=1}^{h} (L' + \lambda_i).$$

Soit X un domaine fondamental pour L. Considérons $X' = \coprod_{i=1}^{h} (\lambda_i + X)$. Il est mesurable de mesure $\mu(X') = h\mu(X)$ par invariance de la mesure par translations. On conclut car c'est un domaine fondamental [4] pour L. En effet,

$$\mathbb{R}^n = \coprod_{\lambda \in L} (X + \lambda) = \coprod_{i=1}^{h} \coprod_{\lambda' \in L'} (X + \lambda_i + \lambda') = \coprod_{\lambda' \in \Lambda'} (X' + \lambda').$$

4. Remarquons que ce n'est pas nécessairement un pavé, même si X en est un !

□

Calculons par exemple, le covolume du réseau $L_0 = \{(a,b) \in \mathbb{Z}^2, a \equiv 2b \bmod 3\}$ considéré au premier paragraphe. Soit on invoque le fait que $(1,-1)$, $(2,1)$ en est une $\mathbb{Z}$-base, et donc que l'on a

$$\mathrm{covol}(L) = |\det \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}| = 3$$

par le lemme 2.13, soit on constate que le morphisme de groupes : $\mathbb{Z}^2 \to \mathbb{Z}/3\mathbb{Z}$, $(a,b) \mapsto a - 2b$, est surjectif de noyau L, de sorte que l'on a un isomorphisme de groupes $\mathbb{Z}^2/L \simeq \mathbb{Z}/3\mathbb{Z}$, et on applique la proposition précédente.

3. Quelques applications arithmétiques

Théorème 2.18. (Fermat, Euler) *Soit p nombre premier $\equiv 1 \bmod 4$. Il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.*

Fixons donc un nombre premier $p \equiv 1 \bmod 4$. Le point de départ est le résultat de Fermat-Euler suivant, démontré au premier chapitre.

Lemme 2.19. *-1 est un carré modulo p.*

Nous allons considérer maintenant un réseau judicieux du plan euclidien $\mathbb{R}^2$. D'après le lemme, il existe un entier $u \in \mathbb{Z}$ tel que $u^2 \equiv -1 \bmod p$.

Lemme 2.20. *Soit $L = \{(a,b) \in \mathbb{Z}^2, a \equiv ub \bmod p\}$. C'est un réseau de $\mathbb{R}^2$ de covolume p. De plus, pour tout $(a,b) \in L$ on a la congruence $a^2 + b^2 \equiv 0 \bmod p$.*

Démonstration — Considérons en effet l'application $\psi : \mathbb{Z}^2 \to \mathbb{Z}/p\mathbb{Z}$ envoyant (a,b) sur $a - bu \bmod p$. C'est un morphisme de groupes manifestement surjectif (considérer par exemple les $(a,0)$), dont le noyau est exactement L par définition. Ainsi, ψ induit un isomorphisme $\mathbb{Z}^2/L \simeq \mathbb{Z}/p\mathbb{Z}$, et le premier point découle donc de la proposition 2.17. Pour le second point, on constate que si $(a,b) \in L$, on a $a^2 + b^2 \equiv (u^2+1)b^2 \equiv 0 \bmod p$. □

On considère maintenant le disque euclidien $C(r) = \{(x,y) \in \mathbb{R}^2,\ x^2 + y^2 < r\}$. Il est clair que $C(r)$ est un ouvert convexe, symétrique, de mesure πr.

Lemme 2.21. *$L \cap C(2p) \neq \{0\}$.*

Démonstration — En effet, d'après le lemme du corps convexe de Minkowski il suffit de voir $2p\pi > 4\mathrm{covol}(L) = 4p$; on conclut car $\pi > 2$. □

Terminons la démonstration du théorème. Soit $(a,b) \in L \cap C(2p)\backslash\{0\}$. Alors d'une part $0 < a^2+b^2 < 2p$ et d'autre part $a^2+b^2 \equiv 0 \bmod p$: la seule possibilité est donc $p = a^2+b^2$!

Théorème 2.22. (Lagrange) *Tout entier ≥ 0 est somme de quatre carrés.*

Il suffit évidemment de le démontrer pour les entiers $n \geq 1$ qui sont sans facteur carré, ce que nous supposons désormais. [5]

Lemme 2.23. *Si $n \in \mathbb{Z}$ est sans facteur carré alors -1 est somme de deux carrés dans $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration — Le théorème des restes chinois permet de se ramener au cas où n est un nombre premier. En effet, supposons $-1 \equiv x^2+y^2 \bmod M$ et $-1 \equiv (x')^2+(y')^2 \bmod N$ avec $(M,N) = 1$. On peut trouver d'après les restes chinois $x'' \in \mathbb{Z}$ tels que $x'' \equiv x \bmod M$ et $x'' \equiv x' \bmod N$. De même, il existe $y'' \in \mathbb{Z}$ tel que $y'' \equiv y \bmod M$ et $y'' \equiv y' \bmod M$. On constate alors que $(x'')^2+(y'')^2 \equiv -1 \bmod M$, mod$N$ et donc modMN.

Comme le lemme est évident si $p = 2$ (et faux si $p = 4$!), on suppose maintenant p impair. Dans ce cas, cela résulte par exemple de l'exercice 1.9 (prendre $\alpha = \beta = -1$). On peut aussi raisonner comme suit. Soit $C = \{x^2, x \in \mathbb{Z}/p\mathbb{Z}\}$ l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ (zéro inclus). D'après la proposition 1.2, $|C| = \frac{p+1}{2}$. On en déduit que C, ainsi que son "opposé translaté " $-1-C = \{-1-c, c \in C\}$ ont tous deux $\frac{p+1}{2}$ éléments, et ne peuvent donc être disjoints, il existe donc $x^2, y^2 \in C$ tels que $-1-x^2 = y^2$. □

D'après ce lemme, on peut trouver $u, v \in \mathbb{Z}$ tels que $-1+u^2+v^2 \equiv 0 \bmod n$.

Lemme 2.24. *Soit $L = \{(a,b,c,d) \in \mathbb{Z}^4, c \equiv au+bv \bmod n, d \equiv av-bu \bmod n\}$. C'est un réseau de $\mathbb{R}^4$ de covolume n^2. De plus, pour tout $(a,b,c,d) \in L$ on a $a^2+b^2+c^2+d^2 \equiv 0 \bmod n$.*

Démonstration — En effet, L est le noyau du morphisme de groupes $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/n\mathbb{Z})^2$ défini par $(a,b,c,d) \mapsto (c-au-bv, d-av+bu)$. Comme ψ est clairement surjectif, L est d'indice n^2 dans $\mathbb{Z}^4$, ce qui prouve le premier point. Enfin, si $(a,b,c,d) \in L$, alors $a^2+b^2+c^2+d^2 \equiv a^2(1+u^2+v^2)+b^2(1+v^2+u^2) \equiv 0 \bmod n$. □

On rappelle que si $r \geq 0$, le disque euclidien $C(r) = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4,\ \sum_i x_i^2 < r\}$ est de mesure $\frac{\pi^2}{2}r^2$ (voir l'exercice 2.12).

Lemme 2.25. $L \cap C(2n) \neq 0$.

5. D'après une identité remarquable classique due à Lagrange, que l'on peut aussi voir comme conséquence de la "multiplicativité de la norme des quaternions de Hamilton", il suffirait de le démontrer pour les nombres premiers. Cette réduction ne sera en fait pas nécessaire.

Démonstration — En effet, $C(r)$ est un ouvert convexe symétrique de mesure $\pi^2 r^2/2$. On déduit du lemme de Minkowski que si $\frac{\pi^2 r^2}{2} > 16p^2$, c'est-à-dire si $r > \frac{4\sqrt{2}}{\pi}\, p$, alors $C(r) \cap L$ contient un élément non nul. On conclut car $\frac{4\sqrt{2}}{\pi} < 2$. □

Soit $(a, b, c, d) \in L \cap C(2n)$ non nul. On a alors $0 < a^2 + b^2 + c^2 + d^2 < 2n$ et $a^2+b^2+c^2+d^2 \equiv 0 \bmod n$, puis $n = a^2+b^2+c^2+d^2$, ce qui conclut la démonstration du théorème de Lagrange. □

Ces deux démonstrations présentent des similarités frappantes. Elles sont en fait tout à fait typiques de nombreuses démonstrations en théorie des nombres : elles comportent tout d'abord un argument de congruence (dit aussi "local" dans le jargon) qui consiste ici à établir l'identité cherchée modulo un entier bien choisi, et il y a ensuite un argument "global", ici de géométrie des nombres, nous permettant de passer d'une solution modulaire à une vraie solution. La définition du réseau L à partir de $\mathbb{Z}^2$ ou $\mathbb{Z}^4$ pourrait paraître astucieuse, notamment dans le second cas ; elle s'expliquerait en fait très simplement dans le language de la théorie des formes quadratiques sur $\mathbb{Z}/p\mathbb{Z}$. Au final, on constate que la "raison" pour laquelle les deux résultats forts célèbres ci-dessus sont vrais est que les nombres $\frac{4}{\pi}$ et $\frac{4\sqrt{2}}{\pi}$ sont tous deux < 2 !

4. Les nombres premiers de la forme $a^2 + db^2$

Soit $d \geq 1$ un entier, un problème bien naturel dans la continuité des précédents théorèmes est d'essayer de décrire les nombres premiers p de la forme $a^2 + db^2$. Comme les carrés modulo 8 sont $\equiv 0, 1, 4$, un tel nombre satisfera en général des congruences particulières modulo 8. Il satisfera aussi les conditions suivantes :

Proposition 2.26. *Si un entier n sans facteur carré est de la forme $a^2 + db^2$, alors n est un carré modulo d et $-d$ est un carré modulo n.*

Démonstration — Il est évident que si $n = a^2 + db^2$ alors n est un carré modulo d. De plus, n et b sont premiers entre eux, car si p premier divise b et n, alors p divise a^2, puis p divise a, et donc p^2 divise n : absurde. On en déduit que $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ puis $-d \equiv (ab^{-1})^2 \bmod n$. □

Remarquons que les résultats du premier chapitre, notamment la loi de réciprocité quadratique, nous permettent de décrire très simplement ces conditions. Sur le problème nettement plus difficile de la réciproque, la méthode du chapitre précédent conduit au résultat général suivant.

Théorème 2.27. *Soient $d \geq 1$ un entier et p un nombre entier > 0 tel que $-d$ est un carré modulo p. Alors l'un au moins des nombres*

$$p,\ 2p,\ 3p,\ \ldots,\ hp$$

est de la forme $a^2 + db^2$, où h désigne la partie entière inférieure de $4\frac{\sqrt{d}}{\pi}$.

Notons que p n'est pas nécessairement un nombre premier dans cet énoncé.

Démonstration — En effet, on imite essentiellement verbatim la démonstration donnée au chapitre précédent dans le cas $d = 1$. Par hypothèse, il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv -d \bmod p$ et on considère

$$L = \{(a, b) \in \mathbb{Z}^2, a \equiv ub \bmod p\}.$$

C'est un réseau de covolume p tel que $a^2 + db^2 \equiv 0 \bmod p$ pour tout $(a, b) \in L$. Soit

$$C_d(r) = \{(x, y) \in \mathbb{R}^2, x^2 + dy^2 \leq r\},$$

c'est l'image du disque euclidien de rayon $\sqrt{r}$ par la dilatation $(x, y) \mapsto (x, y/\sqrt{d})$, sa surface est donc $\frac{\pi r}{\sqrt{d}}$ (remarquer d'ailleurs que cela tend vers 0 quand d grandit).

Le lemme de Minkowski assure alors l'existence d'un élément non nul dans $L \cap C_d(\frac{4\sqrt{d}}{\pi}p)$. Si $(a, b) \in \mathbb{Z}^2$ est un tel élément, alors $a^2 + db^2 = kp$ où k est un entier tel que $0 < k \leq \frac{4\sqrt{d}}{\pi}$, ce qui conclut. (En fait, $\frac{4\sqrt{d}}{\pi}$ n'est jamais entier car π est transcendant, mais nous n'avons pas besoin de ceci). □

d	1 et 2	3 à 5	6 à 9	10 à 15	16 à 22	23 à 30	31 à 39	40 à 49
h	1	2	3	4	5	6	7	8

Table 1. Quelques valeurs de $h := \frac{4}{\pi}\sqrt{d}$.

Le théorème 2.27 a de nombreuses conséquences, et nous allons en explorer quelques-unes.

Corollaire 2.28. (Gauss) *Un nombre premier impair est de la forme $a^2 + 2b^2$ si, et seulement si, il est $\equiv 1, 3 \bmod 8$.*

Par exemple, on a $3 = 1 + 2.1$, $11 = 9 + 2.1$, $17 = 9 + 2.4$, $19 = 1 + 2.9$...

Démonstration — La loi de réciprocité quadratique montre que -2 est un carré modulo p si, et seulement si, $p \equiv 1, 3 \bmod 8$. Le théorème 2.27 conclut car $h = 1$ pour $d = 2$. □

Corollaire 2.29. (Euler, Lagrange) *Un nombre premier $\neq 3$ est de la forme $a^2 + 3b^2$ si et seulement s'il est $\equiv 1 \bmod 3$.*

Démonstration — En effet, $\left(\frac{-3}{p}\right) = 1$ si, et seulement si, $p \equiv 1 \bmod 3$ d'après la loi de réciprocité quadratique. Le théorème 2.27 montre donc que si $p \equiv 1 \bmod 3$, soit p soit $2p$ est de la forme $a^2 + 3b^2$ car $h = 2$. Mais $2p = a^2 + 3b^2$ est absurde modulo 4. □

L'énoncé particulièrement beau suivant fait suite à la discussion précédent le théorème. On prétend qu'Euler en aurait longtemps cherché une démonstration sans jamais y parvenir !

Corollaire 2.30. (Lagrange, Gauss) *Soit $p \neq 5$ un nombre premier. Alors p (resp. $2p$) est de la forme $a^2 + 5b^2$ si, et seulement si, $p \equiv 1, 9 \bmod 20$ (resp. $p \equiv 3, 7 \bmod 20$).*

Démonstration — La loi de réciprocité quadratique assure que $\left(\frac{-5}{p}\right) = 1$ si, et seulement si,

$$p \equiv 1, 3, 7, 9 \bmod 20.$$

Le théorème 2.27 assure alors que pour ces p, soit p soit $2p$ est de la forme $a^2 + 5b^2$. Mais si $n = a^2 + 5b^2$ est impair, on constate que $n \equiv 1 \bmod 4$. Si $2n = a^2 + 5b^2$ avec n impair, on constate aussi que a et b sont impairs, puis que $2n \equiv 6 \bmod 8$, c'est-à-dire $n \equiv 3 \bmod 4$. Le résultat s'en déduit. □

Ce résultat admet un addendum intéressant. Remarquons que si $2p = a^2 + 5b^2$ avec p impair, nous avons vu que a et b sont impairs. On peut donc écrire $a = b + 2c$, puis $2p = (b + 2c)^2 + 5b^2 = 2(2c^2 + 2bc + 3b^2)$, et enfin $p = 2c^2 + 2bc + 3b^2$. Comme l'argument se renverse, on constate que :

Remarque 2.31. *(suite) De plus, $2p$ est de la forme $a^2 + 5b^2$ si et seulement si p est de la forme $2a^2 + 2ab + 3b^2$.*

Nous verrons au chapitre suivant que l'apparition ici des deux formes quadratiques $a^2 + 5b^2$ et $2a^2 + 2ab + 3b^2$ n'est pas un hasard !

Par des arguments tout à fait similaires à ceux que nous venons d'introduire, et que nous laissons au lecteur le soin de vérifier, on pourrait démontrer les énoncés suivants, tous dûs à Gauss.

Corollaire 2.32. *Soit p un nombre premier tel que $\left(\frac{-6}{p}\right) = 1$. Alors p (resp. $2p$) est de la forme $a^2 + 6b^2$ si et seulement si $p \equiv \pm 1 \bmod 8$ (resp $p \equiv \pm 3 \bmod 8$). De plus, $2p$ est de la forme $a^2 + 6b^2$ si, et seulement si, p est de la forme $2a^2 + 3b^2$.*

Corollaire 2.33. *Un nombre premier p est de la forme $a^2 + 7b^2$ si, et seulement si, $p = 7$ ou $p \equiv 1, 2, 4 \bmod 7$.*

Corollaire 2.34. *Soit p un nombre premier impair. Alors p (resp. $2p$) est de la forme $a^2 + 8b^2$ si, et seulement si, $p \equiv 1 \bmod 8$ (resp. $p \equiv 3 \bmod 8$). De plus, $2p$ est de la forme $a^2 + 8b^2$ si, et seulement si, p est de la forme $3a^2 + 2ab + 3b^2$.*

Corollaire 2.35. *Soit $p > 3$ un nombre premier. Alors p (resp. $2p$) est de la forme $a^2 + 9b^2$ si, et seulement si, $p \equiv 1 \bmod 12$ (resp. $p \equiv 5 \bmod 12$). De plus, $2p$ est de la forme $a^2 + 9b^2$ si, et seulement si, p est de la forme $2a^2 + 2ab + 5b^2$.*

Corollaire 2.36. *Soit p un nombre premier tel que $\left(\frac{-10}{p}\right) = 1$. Alors p (resp. $2p$) est de la forme a^2+10b^2 si, et seulement si, $p \equiv 1, 3 \bmod 8$ (resp $p \equiv -1, -3 \bmod 8$). De plus, $2p$ est de la forme $a^2 + 10b^2$ si, et seulement si, p est de la forme $2a^2 + 5b^2$.*

Le cas $d = 11$ réserve cependant une surprise. On doit en effet a priori se contenter du résultat suivant :

Corollaire 2.37. *Soit $p > 2$ un nombre premier tel que $\left(\frac{-11}{p}\right) = 1$. Alors soit p, soit $3p$, est de la forme $a^2 + 11b^2$. De plus, le second cas se produit si, et seulement si, p est de la forme $3a^2 + 2ab + 4b^2$.*

La différence essentielle avec les cas précédemment étudiés, notamment le cas $d = 5$, est que l'analyse des congruences ne semble pas permettre de trancher entre les deux possibilités. Nous verrons en fait dans l'exercice 2.10 que pour tout entier $N \geq 2$, un élément de $(\mathbb{Z}/N\mathbb{Z})^\times$ est de la forme $a^2 + 11b^2$, avec $a, b \in \mathbb{Z}/N\mathbb{Z}$, si et seulement s'il est de la forme $3u^2 + 2uv + 4v^2$, avec $u, v \in \mathbb{Z}/N\mathbb{Z}$. Ce que le corollaire ne nous dit pas mais que nous démontrerons plus tard, c'est que les deux possibilités sont exclusives (choses que nous avions conclues dans les cas précédents par un argument de congruence) : p et $3p$ ne peuvent pas être simultanément de la forme $a^2 + 11b^2$.

La table suivante donne, parmi les nombres premiers p tels que $\left(\frac{-11}{p}\right) = 1$, c'est-à-dire $p \equiv 1, 3, 4, 5, 9 \bmod 11$, ceux de la forme $a^2 + 11b^2$ (type A), et ceux tels que $3p$ est de la forme $a^2 + 11b^2$ (type B).

p	3	5	23	31	37	47	53	59	67	71	89	97	103	113	137	157	163
type	B	B	B	B	B	A	A	B	B	B	B	B	A	B	B	B	A
p	179	181	191	199	223	229	251	257	269	311	313	317	331	353	367	379	383
type	B	B	B	A	B	B	B	A	A	A	B	B	B	B	B	B	B
p	389	397	401	419	421	433	443	449	463	467	487	499	509	521	577	587	599
type	B	A	A	A	A	B	B	B	B	B	B	A	B	B	B	A	A

TABLE 2. Nombres premiers < 600 de type A ou B

La théorie de la multiplication complexe (Kronecker) fait apparaître un lien tout particulier (mais bien caché !) avec le polynôme $x^3 - x^2 + x + 1$, duquel on pourrait déduire le théorème suivant :

Théorème 2.38. *Soit p un nombre premier $\equiv 1, 3, 4, 5, 9 \bmod 11$. Alors p est de type A si, et seulement si, le polynôme $x^3 - x^2 + x + 1$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$.*

La démonstration de ce résultat va cependant au-delà des méthodes développées dans ce cours. Il serait facile de le vérifier à l'aide d'un ordinateur pour tous les nombres premiers du tableau ci-dessus. Remarquons enfin que parmi les 51 nombres premiers étudiés, on constate que 15 sont de type A, soit une proportion d'environ $1/3$. On pourrait en fait démontrer que la densité de Dirichlet (voir les exercices

du Chapitre 9 pour cette notion) de l'ensemble des nombres premiers p de type A parmi ceux $\equiv 1, 3, 4, 5, 9 \bmod p$ est exactement $1/3$, mais c'est aussi au-delà des thèmes abordés dans ce cours : c'est une conséquence du théorème ci-dessus et du théorème de Cebotarev.

En revanche, nous allons expliquer plus loin dans ce cours, suivant Gauss et sa théorie du genre des formes binaires, pourquoi cet exemple d'apparence pourtant bien similaire aux précédents (par exemple au cas $d = 5$) est en fait radicalement différent !

Notons que nous pourrions étendre sans trop de difficulté l'analyse précédente à une poignée de $d \geq 15$, bien que ce soit de plus en plus fastidieux quand h grandit. Nous verrions que les disjonctions des cas grandissent et qu'il y a de plus en plus de possibilités distinctes, parfois déterminées par des congruences, parfois non. La théorie des formes quadratiques binaires (Lagrange, Gauss, Legendre) étudiée au chapitre qui suit s'avèrera un outil bien plus efficace pour toutes ces questions.

5. Exercices

Exercice 2.1. *Soient $m, n \in \mathbb{Z}$ avec $n \geq 1$ et soit le réseau $L = \{(a, b) \in \mathbb{Z}^2,\ a \equiv mb \bmod n\}$ de $\mathbb{R}^2$. Donner une $\mathbb{Z}$-base de L.*

Exercice 2.2. *Montrer que $\{(a, b, c) \in \mathbb{Z}^3, a \equiv b \bmod 5, b \equiv a + c \bmod 2\}$ est un réseau de $\mathbb{R}^3$, calculer son covolume, et en donner une $\mathbb{Z}$-base.*

Exercice 2.3. *Montrer qu'un element $(a, b) \in \mathbb{Z}^2$ se complète en une $\mathbb{Z}$-base de $\mathbb{Z}^2$ si, et seulement si, a et b sont premiers entre eux.*

Exercice 2.4. *Donner un exemple de famille génératrice du groupe $\mathbb{Z}$ dont on ne peut extraire aucune $\mathbb{Z}$-base.*

Exercice 2.5. *Soit $L \subset \mathbb{R}^n$ un réseau et soit $e_1, \ldots, e_n$ une famille d'éléments de L. Montrer que c'est une $\mathbb{Z}$-base de L si, et seulement si, $|\det(e_1, \ldots, e_n)| = \mathrm{covol}(L)$.*

Exercice 2.6. *Soit G un groupe abélien. Si $N \geq 1$ on pose $NG = \{Ng, g \in G\}$, c'est un sous-groupe de G.*

(i) On suppose $G = \mathbb{Z}^n$. Montrer que $2G$ est d'indice 2^n dans G.

(ii) En déduire que si $m, n \geq 1$, alors $\mathbb{Z}^n \simeq \mathbb{Z}^m$ entraîne $n = m$.

(iii) Re-démontrer à l'aide de ce résultat la proposition 2.9.

Exercice 2.7. *Soit V un $\mathbb{Q}$-espace vectoriel et soit $A \subset V$ un sous-groupe finiment engendré. On se propose de démontrer que A admet une $\mathbb{Z}$-base de cardinal égal à la dimension du $\mathbb{Q}$-espace vectoriel $\mathrm{Vect}_{\mathbb{Q}}(A)$ engendré par A.*

(i) Expliquer pourquoi $\mathrm{Vect}_{\mathbb{Q}}(A)$ est de dimension finie. On notera n cette dimension.

(ii) Montrer qu'il existe une injection $\mathbb{Q}$-linéaire $f : \mathbb{Q}^n \to V$ et un entier $N \geq 1$ tels que

$$f(\mathbb{Z}^n) \subset A \subset f(\frac{1}{N}\mathbb{Z}^n).$$

(iii) En déduire que le groupe abélien A est isomorphe à un réseau de $\mathbb{R}^n$ et conclure.

(iv) (Application) Montrer que tout sous-groupe finiment engendré de $\mathbb{C}$ admet une $\mathbb{Z}$-base finie.

Exercice 2.8. *Démontrer le corollaire 2.32.*

Exercice 2.9. (Retour sur le cas $d = 11$).

(i) Soit n un entier. Montrer que $3n$ (resp. $4n$) est de la forme $a^2 + 11b^2$ si, et seulement si, n est de la forme $3a^2 + 2ab + 4b^2$ (resp. $a^2 + ab + 3b^2$).

(ii) Montrer que si un entier impair est de la forme $a^2+ab+3b^2$, alors il est soit de la forme $3a^2 + 2ab + 4b^2$, soit de la forme $a^2 + 11b^2$ (non nécessairement exclusivement).

On pourra remarquer les identités $(b+3a)^2+11b^2 = 3(3a^2+2ab+4b^2)$ et $(a+\frac{b}{2})^2+\frac{11}{4}b^2 = a^2 + ab + 3b^2 = (a + b)^2 - (a + b)b + 3b^2$.

(iii) Démontrer le corollaire 2.37 .

(iv) En déduire que si p est premier tel que $\left(\frac{-11}{p}\right) = 1$, alors p est de la forme $a^2 + ab + 3b^2$.

Exercice 2.10. *Si $N \geq 1$ est un entier, on considère l'ensemble $P(N)$ (resp. $Q(N)$) des éléments de $(\mathbb{Z}/N\mathbb{Z})^\times$ qui sont de la forme $a^2 + 11b^2$ (resp. $3a^2 + 2ab + 4b^2$) avec $a, b \in \mathbb{Z}/N\mathbb{Z}$.*

(i) Montrer que $P(N)$ et $Q(N)$ sont non vides.

(ii) Montrer $P(N) = Q(N)$ pour tout N en utilisant (et vérifiant ?) les identités :

$$(a^2 + 11b^2)(\alpha^2 + 11\beta^2) = (a\alpha + 11b\beta)^2 + 11(a\beta - b\alpha)^2,$$

$$(3a^2 + 2ab + 4b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = (3a\alpha + a\beta + b\alpha + 4b\beta)^2 + 11(a\beta - b\alpha)^2,$$

$$(a^2 + 11b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = 3A^2 + 2AB + 4B^2,$$

$$(3a^2 + 2ab + 4b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = 3C^2 + 2CD + 4D^2,$$

où $A = a\alpha + b\alpha + 4b\beta$, $B = a\beta - 3\alpha b - b\beta$, $C = a\alpha + 2a\beta + 2\alpha b$ et $D = a\alpha - a\beta - \alpha b - 2b\beta$.

(iii) Donner une autre démonstration de ce résultat en utilisant le résultat de l'exercice 1.9. On montrera en fait que l'on a $P(N) = Q(N) = (\mathbb{Z}/N\mathbb{Z})^\times$*, à moins que* 11 *ne divise* N *auquel cas* $P(N) = Q(N)$ *est l'ensemble des éléments de* $(\mathbb{Z}/N\mathbb{Z})^\times$ *qui sont des carrés modulo* 11*.*

Exercice 2.11. *Soit* p *un nombre premier.*

(i) Vérifier que si $p \neq 2$ *alors* $\left(\frac{-14}{p}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{7}\right)$*.*

On suppose désormais[6] $\left(\frac{-14}{p}\right) = 1$*.*

(ii) Montrer que p*,* $2p$ *ou* $3p$ *est de la forme* $a^2 + 14b^2$*.*

(iii) Vérifier par des exemples que les trois cas sont possibles, et que pour chaque nombre premier testé un seul de p*,* $2p$ *ou* $3p$ *est de la forme* $a^2 + 14b^2$*.*

(iv) Montrer que $3p$ *est de la forme* $a^2 + 14b^2$ *si, et seulement si,* $p \equiv \pm 3 \bmod 8$*, et qu'il est équivalent au fait que* p *soit de la forme* $3a^2 + 2ab + 5b^2$*.*

(v) Montrer que $2p$ *est de la forme* $a^2 + 14b^2$ *si, et seulement si,* p *est de la forme* $2a^2 + 7b^2$*.*

Exercice 2.12. (Volume des sphères euclidiennes) *Soit* $n \geq 1$ *un entier. Pour* $r > 0$ *réel on pose*

$$C_n(r) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n, \sum_i x_i^2 < r^2\}.$$

(i) Soit $c_n = \mu(C_n(1))$*. Montrer* $\mu(C_n(r)) = c_n r^n$*, et pour* $n > 1$ *la relation* $c_n = 2c_{n-1}I_n$ *où* $I_n = \int_0^{\pi/2} \cos(t)^n dt$ *(intégrale de Wallis).*

(ii) Montrer $(n+1)I_{n+1} = nI_{n-1}$ *pour tout* $n \geq 2$*, puis* $nI_nI_{n-1} = \pi/2$*.*

(iii) En déduire le calcul de c_n*, et notamment* $c_{2n} = \frac{\pi^n}{n!}$*.*

(iv) Montrer $c_n \to 0$ *quand* $n \to \infty$*.*

n	1	2	3	4	5	6	7	8	9	10
c_n	2	3.141	4.188	4.934	5.263	5.167	4.724	4.058	3.298	2.550

TABLE 3. Volume c_n de la sphère euclidienne de rayon 1 dans $\mathbb{R}^n$ à 10^{-3} près.

Exercice 2.13. *(Réseaux entiers unimodulaires de petite dimension) On munit* $\mathbb{R}^n$ *du produit scalaire euclidien standard* $(x_i) \cdot (y_i) = \sum_i x_i y_i$*. On suppose que* $L \subset \mathbb{R}^n$ *est un réseau de covolume* 1*, et que de plus* $v \cdot w \in \mathbb{Z}$ *pour tout* $v, w \in L$ *(réseau dit* "entier"*).*

(i) Montrer que si $n \leq 4$*, il existe* $v \in L$ *tel que* $v \cdot v = 1$*.*

6. D'après la question précédente, c'est équivalent à $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \bmod 56$.

(ii) On suppose qu'il existe $v \in L$ tel que $v \cdot v = 1$. Montrer que tout élément de L sécrit de manière unique sous la forme $mv + u$ avec $m \in \mathbb{Z}$ et $u \in L \cap v^\perp$.

(iii) (suite) Montrer que $L \cap v^\perp$ est un réseau entier de covolume 1 dans l'espace euclidien $v^\perp$ (muni du produit scalaire induit de $\mathbb{R}^n$).

(iv) En déduire que si $n \leq 4$, il existe $g \in \mathrm{O}_n(\mathbb{R})$ tel que $L = g(\mathbb{Z}^n)$.

En utilisant d'autres techniques, il est possible de démontrer que ce résultat subsiste jusqu'en dimension $n = 7$. L'exercice suivant donne un contre-exemple fameux en dimension 8.

Exercice 2.14. (Le réseau E_8) *Soit $\mathrm{D}_8 = \{(x_1, \ldots, x_8) \in \mathbb{Z}^8, \sum_i x_i \equiv 0 \bmod 2\}$ et soit $e \in \mathbb{R}^8$ le vecteur $\frac{1}{2}(1,1,1,1,1,1,1,1)$. On munit $\mathbb{R}^8$ du produit scalaire euclidien standard.*

(i) Montrer que D_8 est un réseau de $\mathbb{R}^8$ de covolume 2.

(ii) En déduire que $\mathrm{E}_8 := \mathbb{Z}e + \mathrm{D}_8$ est un réseau de $\mathbb{R}^8$ de covolume 1.

(iii) Vérifier que pour tout $v, w \in \mathrm{E}_8$, on a $v \cdot v \in 2\mathbb{Z}$ et $v \cdot w \in \mathbb{Z}$.

(iv) En déduire que E_8 n'est pas de la forme $g(\mathbb{Z}^8)$ pour $g \in \mathrm{O}_8(\mathbb{R})$.