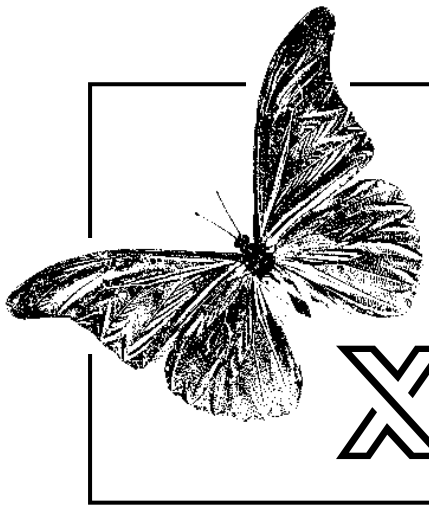

Centre de
Mathématiques

Ecole
Polytechnique

U.R.A. 169 du C.N.R.S.

Codes Géométriques Algébriques et Arithmétique sur les Corps Finis

Journées X-UPS 1993

Juillet 1993

F–91128 Palaiseau Cedex
Tél. : ((33)) (1) 69 33 40 88 • Fax : ((33)) (1) 69 33 30 19
Internet : secret@orphee.polytechnique.fr

Sommaire

Préface

Ce volume réunit les textes des conférences données lors des journées annuelles organisées par le Centre de Mathématiques de l'Ecole Polytechnique au mois de Mai 1993.

Les journées X-UPS 93 ont eu pour thème l'arithmétique et ses applications à la théorie de codes.

La théorie des codes est un sujet relativement jeune (et pour cause) et c'est seulement récemment que l'on s'est aperçu que des résultats difficiles d'arithmétique et de géométrie algébrique ont des conséquences intéressantes dans ce domaine (codes de Goppa).

Nous avons essayé au cours de ces journées de rassembler divers aspects de ces questions.

Le texte de G. Lachaud (reproduit avec l'autorisation de la Société Mathématique de France) présente les aspects algébriques de la théorie du codage. C'est un texte très accessible.

Il est prolongé par le texte de M. Martin-Deschamps qui en développe l'aspect "géométrie algébrique", en utilisant notamment le *théorème de Riemann-Roch*.

Le texte de M. Tsfasman montre les analogies de la théorie des codes avec le problème de *l'empilement des sphères* : comment trouver des empilements (packings) très denses. Ce texte contient aussi (dans son chapitre II) une introduction claire à la théorie des corps de nombres. On pourra, pour plus de détails, consulter le livre de P. Samuel [1] et celui de J. P. Serre [2]. On y trouvera de plus l'analogie avec celle des corps de fonctions rationnelles. Ces théories permettent de construire des réseaux dans $\mathbf{R}^n$ correspondant à des empilements denses à partir de corps de nombres ou de fonctions. On pourra consulter pour plus de détails la bibliographie donnée à la fin de ce texte, notamment le beau livre de Tsfasman et Vladut [3].

Le texte de M. Raynaud est une introduction rapide et condensée à la géométrie algébrique sur un corps commutatif quelconque. Il s'agit de comprendre les propriétés des courbes algébriques, analogues des surfaces de Riemann lorsque le corps est $\mathbf{C}$. Y est énoncé notamment le théorème de Riemann-Roch.

Enfin le texte de C. Houzel fait l'historique des "conjectures de Weil". Ce texte est d'un accès plus difficile. On pourra notamment se référer aux textes de Tsfasman (chapitre II) et Raynaud pendant sa lecture.

On "code" le nombre de points d'une courbe algébrique sur un corps fini ($\mathbf{F}_p$ par exemple) ainsi que le nombre de points de cette courbe sur les $\mathbf{F}_{p^m}$, sous la forme d'une fonction génératrice : c'est la fonction zêta de la courbe. On peut lui donner une forme tout à fait analogue à la classique fonction zêta de Riemann ($\zeta(s) = \sum 1/n^s$). Beaucoup de propriétés de la courbe se lisent sur cette fonction, du fait de l'équation

fonctionnelle qu'elle vérifie. Ce sont ces propriétés qui sont utilisées notamment en théorie des codes ("bornes de Weil").

On trouvera à la fin des textes de Raynaud et Houzel un aperçu des développements ultérieurs.

Nous tenons à remercier les conférenciers pour l'important travail qu'ils ont fourni. Nous remercions aussi G. Lachaud qui nous a permis d'utiliser le beau texte de la conférence qu'il avait donnée à la journée annuelle de la S.M.F. en 1988 et qui nous a utilement guidé pour la préparation de ces journées. Enfin nous remercions C. François, C. Harmide et P. Truc pour la frappe des manuscrits.

Nicole Berline et Claude Sabbah
Centre de Mathématiques
Ecole Polytechnique

Bibliographie succinte

[1] P. Samuel, *Théorie algébrique des nombres*, coll. Méthodes, Hermann, Paris, 1967.

[2] J.P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

[3] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht/Boston/London, 1991.

Avertissement

Le texte proposé par Gilles Lachaud fait partie de la publication de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE consacrée à la journée annuelle "Codage et transmission de l'information", Paris, janvier 1988.

Il n'est pas reproduit dans la version postscript du volume x-ups 1993.

On peut se procurer les publications de la S.M.F. à l'Ecole Normale Supérieure, Tour L, 1 rue Maurice Arnoux, 92120 Montrouge, et à partir de juillet 1993 à l'Institut Henry Poincaré, 11 rue P. et M. Curie 75005 Paris.

Codes géométriques

Mireille Martin-Deschamps

Les théorèmes généraux de théorie des codes qui ont été montrés par Shannon assurent l'existence de codes très performants (en ce sens qu'ils atteignent la borne de Varshamov-Gilbert

$$R = 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta)\log_q(1-\delta)$$

où R et δ sont les paramètres asymptotiques du code).

Malheureusement, ces théorèmes ne fournissent aucune indication sur la manière effective de construire de tels codes. Un pas important dans cette direction a été fait avec la construction des codes géométriques, construction qui utilise les objets et les méthodes de la géométrie algébrique, et qui permet de retrouver les résultats prédits par la théorie.

1. Exemple : Code de Reed-Solomon sur $\mathbf{F}_q$, $q = p^m$

On note $(0, \alpha_1, \ldots, \alpha_{q-1})$ les éléments de $\mathbf{F}_q$. Par exemple, si α est un élément primitif, on pourra choisir $\alpha_i = \alpha^{i-1}$ pour $i = 1, \ldots, q-1$.

Soit δ un entier compris entre 2 et $q-1$. Le code de Reed-Solomon sur $\mathbf{F}_q$ de paramètre δ est défini par la matrice de contrôle de parité :

$$H = \begin{pmatrix} \alpha_1 & \cdots & \alpha_{q-1} \\ \vdots & & \vdots \\ \alpha_1^{\delta-1} & \cdots & \alpha_{q-1}^{\delta-1} \end{pmatrix}$$

Autrement dit, les mots du code sont les $q-1$-uples $(a_1, \ldots, a_{q-1})$ de $\mathbf{F}_q^{q-1}$ tels que

$$\sum_{i=1}^{q-1} \alpha_i^j a_i = 0$$

pour $j = 1, \ldots, \delta-1$. C'est un code de longueur $n = q-1$, de dimension $k = n-\delta+1$.

Un encodeur peut être défini de la manière suivante : on considère l'espace vectoriel $\mathbf{F}_q[x]_{k-1}$ des polynômes en une variable de degré $\leq k-1$ sur $\mathbf{F}_q$, et l'application linéaire d'"évaluation :"

$$\begin{array}{rcll} \mathbf{F}_q[x]_{k-1} & \longrightarrow & \mathbf{F}_q^n & n = q-1 \\ f & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_n)). & \end{array}$$

En effet, on vérifie que c'est une injection, que l'image est contenue dans le code, donc lui est égale pour des raisons de dimension. On peut alors calculer facilement la distance minimale d : un polynôme de degré $\leq k-1$ ayant au plus $(k-1)$ zéros, le poids d'un mot du code est $\geq n-k+1=\delta$, donc on a : $d=\delta$.

Remarque. — Ces codes sont effectivement utilisés dans la pratique, par exemple on utilise un Reed-Solomon sur $\mathbf{F}_{64}$ pour corriger les informations contenues dans les disques numériques audio.

Afin de généraliser cette construction, on va en donner une interprétation un peu différente :

Soit $X=\mathbf{P}^1_{\mathbf{F}_q}$ la droite projective sur $\mathbf{F}_q$. On peut regarder $(\alpha_1,\ldots,\alpha_{q-1})$ non plus comme des éléments de $\mathbf{F}_q$, mais comme des points rationnels de X. On note $P_i=(\alpha_i,1)$ pour $i=1,\ldots,q-1$ et $P_\infty=(1,0)$.

Un polynôme de $\mathbf{F}_q[x]$ définit une fonction rationnelle sur X, ayant en P_∞ un pôle d'ordre égal à son degré. En particulier, on identifie ainsi l'ensemble $\mathbf{F}_q[x]_{k-1}-\{0\}$ avec l'ensemble des fonctions rationnelles f non nulles sur X telles que le diviseur $(f)+(k-1)P_\infty$ soit positif. Autrement dit, on a un isomorphisme linéaire :

$$\mathbf{F}_q[x]_{k-1}\xrightarrow{\sim} H^0(X,\mathcal{O}_X((k-1)P_\infty)).$$

On va alors pouvoir définir les codes géométriques.

2. Codes géométriques de Goppa

Soient X une courbe lisse et projective sur $\mathbf{F}_q$, de genre g, (D,G) un couple de diviseurs sur X satisfaisant les conditions suivantes :

$$(*)\quad\begin{cases} D=P_1+\cdots+P_n \quad \text{où } P_1,\ldots,P_n \text{ sont } n \text{ points distincts de } X(\mathbf{F}_q)\\ G>0\\ \operatorname{Supp}D\cap\operatorname{Supp}G=\varnothing. \end{cases}$$

On considère l'application linéaire d'"évaluation" :

$$\begin{array}{rcl} H^0(X,\mathcal{O}_X(G)) & \xrightarrow{\varphi} & \mathbf{F}_q^n \\ f & \longmapsto & (f(P_1),\ldots,f(P_n)). \end{array}$$

Elle est bien définie car toute fonction rationnelle $f\neq 0$ qui vérifie $(f)+G\geq 0$ n'a pas de pôle en $P_1,\ldots,P_n$. L'image de φ est un code sur $\mathbf{F}_q$, noté C_L, dont on va calculer les paramètres asymptotiques en utilisant des résultats de géométrie algébrique.

PROPOSITION. — *Soit $[n,k,d]$ le type de C_L. Si $\deg G<n$, on a :*

- $k\geq \deg G+1-g$ *avec égalité si* $\deg G>2g-2$,
- $d\geq n-\deg G$.

Démonstration. — Soit $f \neq 0$ qui vérifie les conditions :

$$(f) + G \geq 0 \qquad f(P_i) = 0 \qquad i = 1, \ldots, n.$$

Alors, puisque les supports de D et G sont distincts, on a aussi

$$(f) + G - D \geq 0 \quad \text{donc} \quad \deg G \geq \deg D = n$$

donc si on a $\deg G < n$, φ est injective.

D'après le théorème de Riemann-Roch, on a :

$$h^0(\mathcal{O}_X(G)) = \deg G + 1 - g + h^0(\omega_X \otimes \mathcal{O}_X(-G))$$

où ω_X est le faisceau des formes différentielles sur X,

$$\deg(\omega_X \otimes \mathcal{O}_X(-G)) = 2g - 2 - \deg G$$

d'où l'assertion sur k.

Soit $f \neq 0$, $f \in H^0(\mathcal{O}_X(G))$, et $w(f)$ le poids de $\varphi(f)$. Il existe des indices $i_1, \ldots, i_{n-w(f)}$ tels que :

$$f(P_{i_1}) = \cdots = f(P_{i_{n-w(f)}}) = 0$$

donc le diviseur $(f) + G - (P_{i_1} + \cdots + P_{i_{n-w(f)}})$ est ≥ 0, ainsi que son degré, d'où :

$$\begin{aligned} \deg G &\geq n - w(f) \\ w(f) &\geq n - \deg G. \end{aligned}$$

Pour obtenir une matrice génératrice, on choisit une base $(f_1, \ldots, f_\ell)$ de $H^0(\mathcal{O}_X(G))$, et on obtient :

$$\begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & & \vdots \\ f_\ell(P_1) & \cdots & f_\ell(P_n) \end{pmatrix}$$

Exemple. — Code sur la cubique d'équation :

$$X^3 + Y^3 + Z^3 = 0 \quad \text{sur} \quad \mathbf{F}_4 = \{0, 1, \alpha, \alpha^2\}.$$

Elle est lisse de genre 1, elle a 9 points rationnels, dont 3 à l'infini.

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
X	0	0	0	α^2	α	1	α^2	α	1
Y	α^2	α	1	0	0	0	1	1	1
Z	1	1	1	1	1	1	0	0	0

On considère alors les diviseurs :

$$\begin{aligned} D &= P_1 + \cdots + P_8 \\ G &= 3P_9 \end{aligned}$$

Puisque $0 < \deg G < 8$, on a $h^0(\mathcal{O}_X(G)) = 3$, donc il faut trouver 3 éléments indépendants de $H^0(\mathcal{O}_X(G))$. On choisit

$$\begin{aligned} f &= 1 && (f) = 0 \\ g &= \frac{X}{X+Y} && (g) = P_1 + P_2 + P_3 - 3P_9 \\ h &= \frac{X}{X+Y} && (h) = P_1 + P_2 + P_3 - 3P_9. \end{aligned}$$

On obtient alors la matrice génératrice :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & 1 & \alpha & \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & \alpha & \alpha^2 \end{pmatrix}$$

C'est un code de type [8,3,5] sur $\mathbf{F}_4$.

Remarque. — La courbe elliptique considérée est un cas particulier de "courbe d'Hermite" sur $\mathbf{F}_q$. Lorsque q est un carré et $d = \sqrt{q}+1$, la courbe d'Hermite est la courbe X d'équation : $X^d + Y^d + Z^d = 0$. C'est une courbe lisse de genre

$$g = \frac{(d-1)(d-2)}{2} = \frac{q - \sqrt{q}}{2}.$$

Il est facile de voir qu'une telle courbe a $q\sqrt{q}+1$ points rationnels, donc qu'elle atteint la borne de Weil :

$$\#X(\mathbf{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Il existe une deuxième manière d'associer à un couple de diviseurs (D, G) qui vérifie les conditions $(*)$ un code linéaire sur $\mathbf{F}_q$. On considère l'application linéaire "résidu" :

$$\begin{aligned} H^0(\omega_X \otimes \mathcal{O}_X(D-G)) &\xrightarrow{\psi} \mathbf{F}_q^n \\ \omega &\longmapsto (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)). \end{aligned}$$

L'image de ψ est un code sur $\mathbf{F}_q$, noté C_Ω.

PROPOSITION. — *Soit $[n, k', d']$ le type de C_Ω. Si $2g - 2 < \deg G$, on a :*

- $k' \geq n - \deg G - 1 + g$ *avec égalité si* $\deg G < n$,
- $d' \geq \deg G - 2g + 2$.

Démonstration. — Soit $\omega \neq 0$ qui vérifie les conditions :

$$(\omega) + D - G \geq 0 \quad \text{et} \quad \mathrm{Res}_{P_i}\omega = 0 \qquad i - 1, \ldots, n.$$

Alors ω n'a pas de pôle en $P_1, \ldots, P_n$, donc on a aussi :

$$(\omega) - G \geq 0 \quad \text{et} \quad \deg G \leq 2g - 2.$$

Donc si on a $\deg G > 2g - 2$, ψ est injective.

D'après le théorème de Riemann-Roch, on a :

$$h^0(\omega_X \otimes \mathcal{O}_X(D - G)) = -\deg(G - D) + g - 1 + h^0(\mathcal{O}_X(G - D))$$

d'où l'assertion sur k'.

Enfin, soit $\omega \neq 0$, $\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D - G))$ et $w(\omega)$ le poids de $\psi(\omega)$. Il existe des indices $i_1, \ldots, i_{w(\omega)}$ tels que le diviseur $(\omega) + P_{i_1} + \cdots + P_{i_{w(\omega)}} - G$ soit positif ainsi que son degré, d'où :

$$w(\omega) \geq \deg G + 2 - 2g.$$

Le fait que les démonstrations de ces deux propositions soient très voisines n'est pas étonnant, car ces deux codes sont liés. Plus précisément, on a le résultat suivant :

PROPOSITION. — *Si $2g - 2 < \deg G < n$, les codes C_L et C_Ω sont duaux l'un de l'autre.*

Démonstration. — Soit $f \in H^0(\mathcal{O}_X(G))$, $\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D - G))$, alors

$$f\omega \in H^0(\omega_X \otimes \mathcal{O}_X(D))$$

donc les pôles de $f\omega$ sont contenus dans le support de D. Mais on a :

$$(\varphi(f) \mid \psi(\omega)) = \sum_{i=1}^{n} f(P_i)\mathrm{Res}_{P_i}\omega = \sum_{i=1}^{n} \mathrm{Res}_{P_i}(f\omega) = 0$$

d'après la formule des résidus. Donc C_L et C_Ω sont orthogonaux. Dans le cas $2g-2 < \deg G < n$, pour des raisons de dimension, C_Ω *est* l'orthogonal de C_L.

DÉFINITION. — *C_L et C_Ω sont les codes géométriques définis par le couple de diviseurs (D, G).*

Remarques.

1. La dualité entre C_L et C_Ω est une traduction de la dualité de Serre sur X.
2. Actuellement, on étudie plutôt les codes C_L. Historiquement, les codes C_Ω ont été construits d'abord, sans doute parce que Goppa, qui les a inventés, n'est pas à l'origine un géomètre, ni un algébriste. La définition de C_Ω pose moins de problèmes que celle de C_L, car le résidu d'une forme différentielle existe toujours, alors qu'il n'en est pas de même de la valeur d'une fonction rationnelle, et il faut des outils algébriques pour contrôler les domaines de définition des fonctions rationnelles.

3. Applications

On dispose maintenant d'une nouvelle famille très vaste de codes linéaires. Les problèmes qui les concernent se ramènent à des problèmes d'arithmétique et de géométrie algébrique (arithmétique en ce qui concerne les points rationnels d'une courbe sur un corps fini, géométrique pour la construction des systèmes linéaires de diviseurs).

Nous allons montrer que la famille des codes géométriques a de bonnes propriétés asymptotiques.

Soit X une courbe projective et lisse de genre g sur $\mathbf{F}_q$, C_L un code obtenu en considérant un couple (D, G) tel que D contienne tous les points rationnels de $X(\mathbf{F}_q)$, $[n, k, d]$ son type. On a :

- $k \geq \deg G + 1 - g$,
- $d \geq n - \deg G$,

d'où

$$\frac{k}{n} + \frac{d}{n} \geq 1 + \frac{1-g}{n}$$

avec $n = \#X(\mathbf{F}_q) = N_q(x)$.

On pose alors

$$\begin{aligned} N_q(g) &= \max\{N_q(X) \mid X \text{ proj. lisse, genre } g \text{ sur } \mathbf{F}_q\} \\ A(q) &= \limsup \frac{N_q(g)}{g}. \end{aligned}$$

On veut borner $A(q)$. Pour cela, on peut utiliser la borne de Weil :

$$|N_q(x) - (q+1)| \leq 2g\sqrt{q}$$

et on obtient $A(q) \leq 2\sqrt{q}$.

Mais cette borne peut être améliorée :

THÉORÈME. — *On a $A(q) \leq \sqrt{q} - 1$. De plus, si q est un carré, on a $A(q) = \sqrt{q} - 1$.*

L'inégalité a été montrée par Drinfeld et Vladut. L'égalité a été prouvée par Ihara, puis indépendamment par Tsfasman, Vladut et Zink, qui en ont aussi déduit, en utilisant des courbes modulaires, qu'il existe une famille de codes géométriques sur $\mathbf{F}_q$ ayant une complexité polynomiale de construction et dépassant la borne de Varshamov-Gilbert, si q est un carré ≥ 49.

4. Généralisation

Cette construction peut être étendue à des variétés algébriques de dimension supérieure. Pour le moment, ces techniques n'ont pas permis de construire de "meilleurs" codes que sur les courbes, mais on a pu dans certains cas, donner ainsi une interprétation géométrique de codes déjà connus. C'est le cas des codes de Reed-Muller :

Codes de Reed-Muller projectifs. — Soit $X = \mathbf{P}^r$ l'espace projectif de dimension r sur $\mathbf{F}_q$. Soient V l'ensemble des points rationnels de X, et N son cardinal. On note U_i l'ouvert de X défini par $X_i \neq 0$. On obtient ainsi un recouvrement ouvert de X : $X = \bigcup_{i=0}^{r} U_i$. On a :

$$\begin{aligned} N &= \#X = \#U_0 + \#(U_1 - U_0) + \cdots + \#\left(U_r - \bigcup_{i=0}^{r-1} U_i\right) \\ &= q^r + q^{r-1} + \cdots + 1 \\ &= \frac{q^{r+1} - 1}{q - 1}. \end{aligned}$$

Soit $\mathcal{L} = \mathcal{O}_P(1)$ le faisceau inversible correspondant aux diviseurs hyperplans.

Pour $m \geq 1$, les sections globales de $\mathcal{L}^m$ s'identifient aux polynômes homogènes de degré m en $X_0, \ldots, X_r$.

Pour tout point x de V, on peut définir une application linéaire d'évaluation en x $\varphi_x : H^0(X, \mathcal{L}^m) \to \mathbf{F}_q$ de la manière suivante :

Si $x \in U_0$, $\varphi_x(f) = f(x)/x_0^m$

Si $x \in U_1 - U_0$, $\varphi_x(f) = f(x)/x_1^m$

Si $x \in U_2 - (U_1 \cup U_0)$, $\varphi_x(f) = f(x)/x_2^m$

...

On a alors une application linéaire d'évaluation :

$$\begin{aligned} H^0(X, \mathcal{L}^m) &\xrightarrow{\psi} \mathbf{F}_q^N \\ f &\longmapsto (\varphi_{x_1}(f), \ldots, \varphi_{x_N}(f)) \end{aligned}$$

dont l'image est un code de Reed-Muller projectif.

On montre par récurrence sur r, que φ est une injection si $m < q$. Dans ce cas, puisqu'un polynôme homogène a au plus $m(q^r - 1)/(q - 1)$ zéros dans $\mathbf{P}^r(\mathbf{F}_q)$, les paramètres du code sont les suivants :

$$\begin{cases} n = \dfrac{q^{r+1} - 1}{q - 1} \\ k = \dbinom{r + m}{r} \\ d \geq \dfrac{q^{r+1} - 1 - m(q^r - 1)}{q - 1} \quad \text{avec égalité quand } m = 1. \end{cases}$$

URA 762 du C.N.R.S.
Département de Mathématiques et Informatique
Ecole Normale Supérieure
45, rue d'Ulm
75005 Paris
FRANCE

Algebraic Curves and Sphere Packings

Michael A. Tsfasman

This talk is mostly devoted to problems which resemble greatly questions about codes, namely to quite a classical problem of dense packing of equal non-overlapping spheres in $\mathbf{R}^N$. It comes out that both direct application of algebraic-geometric codes and use of intuition developped while studying them are quite useful. Moreover, here one can see even better the marvelous integrity of mathematics, two more parts of which — number theory and that of packings — being added to coding theory and algebraic geometry.

In the first chapter we give necessary definitions and produce some beautiful examples. This chapter is quite classical and has nothing to do with either algebraic geometry or number theory.

The relations with the latter are discussed in the second chapter devoted to algebraic geometry and number theory constructions of lattices and packings.

Chapter I
Definitions and examples

How can one pack equal non-overlapping spheres in $\mathbf{R}^N$? What is the density of such packing and how the density behaves for small values of N? For large values of N? How to put the asymptotic problem for $N \to \infty$?

In § 1 we give some basic definitions and introduce different parameters of sphere packings. Then we show how to put the problem rigorously. In § 2 we give some examples of dense packings. Then, in § 3 we discuss the asymptotic setting. The striking similarity between codes and packings is briefly discussed in § 4.

1. Parameters

Packings. — Let us consider the classical problem of *packing* equal non-overlapping spheres in $\mathbf{R}^N$. Let P be the set of centers and let

$$d = d(P) = \inf_{v,u \in L, v \neq u} |u - v|,$$

d is the *minimum distance* of the packing, which equals the maximum possible diameter of non-overlapping spheres centered in P.

The *density* of P is the part of $\mathbf{R}^N$ covered by spheres; to be precise, it can be defined as

$$\Delta(P) = \limsup_{u\to\infty} v(S \cap B_u)/v(B_u),$$

where

$$S = \left\{ x \in \mathbf{R}^N \,\middle|\, \exists y \in P,\ |x-y| < \frac{d}{2} \right\}$$

$$B_u = \left\{ x \in \mathbf{R}^N \,\middle|\, |x| \le u \right\}$$

and $v(\cdot)$ is the standard volume in $\mathbf{R}^N$.

Lattices. — If P is an additive subgroup of $\mathbf{R}^N$, we call the packing P a *lattice packing* (or just a *lattice*; in this case we use the letter L rather than P). Further on we suppose that the rank of L equals N since otherwise $\Delta(L) = 0$. If L is a lattice then any choice of a basis $e_1, \dots, e_N$ in L defines a map $\mathbf{Z}^N \to \mathbf{R}^N$; its matrix is called a *generator matrix* of the lattice.

For lattices the definition of $\Delta(L)$ does not depend on the choice of origin and does not change if we replace the ball B_u by a cube (or by any homotetically increasing solid containing a neighbourhood of the origin).

The volume of the fundamental domain

$$F = \left\{ \sum_{i=1}^{N} x_i e_i \,\middle|\, 0 \le x_i < 1 \right\} \subset \mathbf{R}^N$$

equals the absolute value of the determinant of the generator matrix. This volume is called the *determinant* of the lattice and is denoted by $\det(L)$; we define the discriminant $\operatorname{discr}(L)$ of L as the determinant of the matrix of inner products $||(e_i, e_j)||$, $i, j = 1, \dots, N$. It is easy to check that

$$\operatorname{discr} L = (\det L)^2.$$

Let $V_N = \pi^{N/2}/\Gamma(N/2+1)$ be the volume of unit ball in $\mathbf{R}^N$.

For a lattice there is exactly one sphere in each fundamental domain, or — to be more precise — the pieces of spheres in the fundamental domain, being shifted, form just one sphere. Therefore

$$\Delta(L) = \frac{d(L)^N V_N}{2^N \det L}.$$

Note that by the Stirling formula we have

$$\log_2 V_N = \frac{N}{2} \cdot \log_2 \left(\frac{2\pi e}{N} \right) - \log_2 \sqrt{\pi \cdot N} + o(1);$$

we write this as

$$\frac{1}{N}\cdot\log_2 V_N \sim \frac{1}{2}\cdot\log_2\left(\frac{2\pi e}{N}\right).$$

Thus for $N\to\infty$ we get

$$-\frac{1}{N}\cdot\log_2\Delta(L) \sim -\log_2\sqrt{\frac{\pi\cdot e}{2}} + \log_2\sqrt{N} - \log_2 d(L) + \frac{1}{N}\cdot\log_2(\det L).$$

Other parameters. — Let us define some other parameters of packings (which are often more convenient than Δ) setting

$$\begin{aligned}\delta(P) &= \Delta(P)/V_N,\\ \lambda(P) &= -(\log_2\Delta(P))/N,\\ \nu(P) &= \log_2\delta(P);\end{aligned}$$

we call $\delta(P)$ the *centre density*, and $\lambda(P)$ the *density exponent*. Clearly,

$$\Delta(P) = 2^{-\lambda(P)\cdot N}.$$

For root lattices it is convenient to use $\delta(P)$; $\nu(P)$ is useful to compute the density of lattices obtained by some specific constructions. The density exponent $\lambda(P)$ is especially important for asymptotic problems.

Densest packings. — Set

$$\lambda(N) = \inf_{P\subset\mathbf{R}^N}\lambda(P), \quad \Delta(N) = \sup_{P\subset\mathbf{R}^N}\Delta(P), \ldots$$

A natural problem of finding the densest possible packing in a given dimension can be decomposed into two problems:

(A) Find the precise value of $\lambda(N)$ (or, what is the same, of $\Delta(N)$ or of $\delta(N),\ldots$).

(B) Find a packing P with $\lambda(P)=\lambda(N)$.

These problems are completely solved only for $N=1$ and $N=2$.

Since $\Delta(P)\le 1$, we get

$$\lambda(P)\ge 0$$

for any packing.

For $N=1$ the answer is obvious: equal segments cover the whole line, and hence for this packing L_1 one has $\Delta(L_1)=1$, i.e.

$$\Delta(1)=1, \quad \lambda(1)=0.$$

For $N = 2$ the problem is not so simple but one can prove that

$$\Delta(2) = \pi/2\sqrt{3}.$$

It is easy to check that for the lattice $L_2 \subset \mathbf{R}^2 = \mathbf{C}$ generated by 1 and $\frac{1+\sqrt{-3}}{2}$ we have $\Delta(L_2) = \Delta(2); L_2$ is called the *hexagonal* lattice.

Strangely enough, $\lambda(N)$ is unknown for any $N \geq 3$.

The figures 1, 2, 3 show the densest known packings in dimensions 1, 2, and 3.

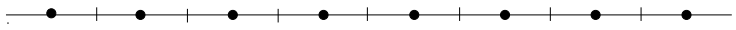

Figure 1: dim = 1, $\Delta = 1$

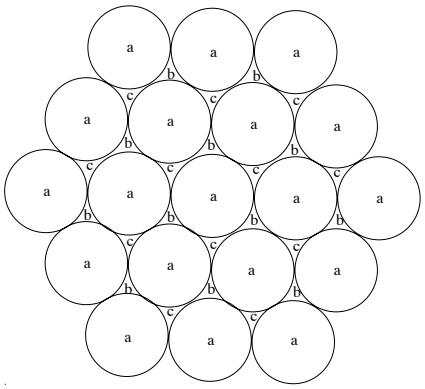

Figure 2 : dim = 2, $\Delta = \dfrac{\pi}{\sqrt{12}} = 0.9069\cdots$

In fact, the packing in dimension 2 is obtained by taking a line, putting spheres of dimension two at the centers of the best packing in dimension one along this line, then taking a similar row next to it as close as possible, then another row, and so on. It can be shown that it is essentially unique.

We can do the same in dimension three. Take a plane, put three-dimensional spheres at the centres "a" of the best two-dimensional packing. Then we have to choose the next layer. It can be centered either over "b" points, or over "c"

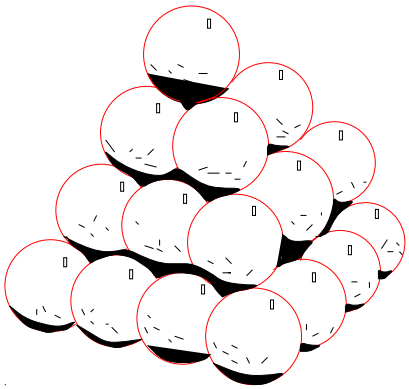

Figure 3 : $\dim = 3$, $\Delta = \dfrac{\pi}{\sqrt{18}} = 0.7405\cdots$

points. Continuing like this we have continually many choices corresponding to binary sequences, the density being the same. One of these choices gives the lattice packing you see on the figure.

It is conjectured that this packing is the densest possible. Recently a proof has been annonced, but as yet the mathematical community does not believe in it.

Densest lattices. — For lattice packings we know slightly more. Let

$$\lambda_\ell(N) = \inf_{L\subset\mathbf{R}^N} \lambda(L), \quad \Delta_\ell(N) = \sup_{L\subset\mathbf{R}^N} \Delta(L), \ldots$$

Clearly

$$\lambda_\ell(N) \geq \lambda(N), \quad \Delta_\ell(N) \leq \Delta(N), \ldots$$

A lattice L is called *unimodular* iff $\det L = 1$. The *dual lattice*

$$L^\perp = \left\{ x \in \mathbf{R}^N \,\middle|\, (x,\ell) \in \mathbf{Z} \quad \text{for any} \quad \ell \in L \right\}$$

is in this case also unimodular.

The inner product in $\mathbf{R}^N$ induces on L a positively definite bilinear form.

In fact, any integral positively definite bilinear form can be obtained from a lattice.

Let now $\varphi(x,y)$ be a positively definite bilinear form in N integral variables, and let $f(x) = \varphi(x,x)$ be the corresponding quadratic form. Suppose that φ is unimodular, i.e. $\operatorname{discr}\varphi = 1$. Such forms are in bijection with unimodular lattices L in $\mathbf{R}^N$. Set

$$\gamma(L) = \gamma(\varphi) = \min_{x\in\mathbf{Z}^N-\{0\}} f(x).$$

In lattice terms it is the squared length of the shortest non-zero vector. It is easy to check that

$$\Delta(L) = V_N \cdot \left(\frac{\gamma(L)}{4}\right)^{N/2};$$

$$\gamma(L) = 4 \cdot \left(\frac{\Delta(L)}{V_N}\right)^{2/N} = 4 \cdot (\delta(L))^{2/N}.$$

One can naturally extend the definition of $\gamma(\varphi)$ to non-unimodular case:

$$\gamma(L) = \gamma(\varphi) = \min_{x \in \mathbf{Z}^N - \{0\}} \left(\frac{f(x)}{\operatorname{discr}\varphi}\right)^{1/N}.$$

Now let us put

$$\gamma(N) = \max_{\varphi} \gamma(\varphi),$$

where maximum is taken over all positively definite bilinear forms in N variables; $\gamma(N)$ and $\Delta_\ell(N)$ are related by formulae similar to those given above.

Note that for $N \to \infty$ we obtain

$$\lambda(N) \sim \log_2 \sqrt{\frac{2N}{\pi \cdot e \cdot \gamma(N)}},$$

$$\log_2(\gamma(N)) \sim \log_2 \left(\frac{2N}{\pi e} \cdot \Delta^{2/N}\right) = -2 \cdot \lambda(N) + \log_2 \left(\frac{2N}{\pi e}\right).$$

Precise values of $\Delta_\ell(N)$ are known for $1 \le N \le 8$; see the table where we have collected the values of all the above parameters for these N.

N	1	2	3	4	5	6	7	8
$\Delta_\ell(N)$	1	0.907	0.740	0.617	0.465	0.373	0.295	0.254
$\delta_\ell(N)$	0.5	0.229	0.177	0.125	0.088	0.072	0.063	0.063
$\lambda_\ell(N)$	0	0.070	0.144	0.174	0.221	0.237	0.251	0.247
$\nu_\ell(N)$	-1	-1.792	-2.5	-3	-3.5	3.792	-4	-4
$\gamma_\ell(N)$	1	1.155	1.260	1.414	1.516	1.665	1.811	2
$\delta_\ell(N)^{-2}$	4	12	32	64	128	192	256	256

Note that within the table $\Delta_\ell(N)$ increases and $\gamma_\ell(N)$ decreases. It is interesting to know whether it is the case for any N.

In the table the integrality of $\delta_\ell(N)^{-2}$ attracts attention. We do not know whether $\delta_\ell(N)^{-2}$ is integral for any N; note however that the densest lattice of a given rank can be generated by a matrix with rational entries and the rationality of $\delta_\ell(N)^{-2}$ follows.

2. Examples

Now we describe the densest lattices for $N \leq 8$ and introduce some interesting lattice families.

We construct families $L \subset \mathbf{R}^N$ and give the values of $d(L)$ and $\det(L)$. Other density parameters for these families are given in the table above.

The simplest family is

$$\mathbf{Z}^N \subset \mathbf{R}^N;$$

for these lattices

$$d(\mathbf{Z}^N) = 1, \quad \det(\mathbf{Z}^N) = 1.$$

Root lattices. — Let us consider in $\mathbf{R}^{N+1}$ the following lattice A_N of rank N:

$$A_N = \left\{ \sum_{i=1}^{N+1} a_i e_i \;\middle|\; a_i \in \mathbf{Z}, \sum a_i = 0 \right\},$$

$\{e_i\}$ being the standard basis in $\mathbf{R}^{N+1}$.

The lattice A_N is generated by vectors

$$\alpha_1 = e_1 - e_2,\ \alpha_2 = e_2 - e_3, \ldots,\ \alpha_N = e_N - e_{N+1};$$

its parameters are

$$d(A_N) = \sqrt{2}, \det(A_N) = \sqrt{N+1}.$$

The family $D_N \subset \mathbf{R}^N$ is defined by

$$D_N = \left\{ \sum_{i=1}^{N} a_i e_i \;\middle|\; a_i \in \mathbf{Z},\ \sum a_i \equiv 0 \bmod 2 \right\}.$$

The lattice D_N is generated by $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3, \ldots$, $\alpha_{N-1} = e_{N-1} - e_N$, and $\alpha_N = e_{N-1} + e_N$; its parameters are

$$d(D_N) = \sqrt{2}, \quad \det(D_N) = 2.$$

The following important family does exist only for $N = 4, 5, 6, 7, 8$. For such N define the lattice E_N in $\mathbf{R}^8$ by its basis:

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(e_1 + e_8) - \frac{1}{2} \cdot (e_2 + \cdots + e_7), \\ \alpha_2 &= e_1 + e_2, \\ \alpha_i &= e_i - e_{i-1} \qquad \text{for} \quad i = 3, \ldots, N. \end{aligned}$$

The lattice E_8 can be given by

$$E_8 = \left\{ \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; 2 \cdot a_i \in \mathbf{Z},\ a_i - a_j \in \mathbf{Z},\ \sum_{i=1}^{8} a_i \in 2 \cdot \mathbf{Z} \right\};$$

and the rest E_N are intersections of E_8 with planes of codimension $(8 - N)$. In particular,

$$\begin{aligned} E_7 &= \left\{ x = \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; x \in E_8,\ a_7 = -a_8 \right\}, \\ E_6 &= \left\{ x = \sum_{i=1}^{8} a_i \cdot e_i \;\middle|\; x \in E_7,\ a_6 = -a_7 \right\}. \end{aligned}$$

The parameters are $d(E_N) = \sqrt{2}$ and $\det(E_N) = 9 - N$.

Note that $A_1 = \mathbf{Z}, D_3 = A_3, E_4 = A_4, E_5 = D_5$. The lattice families A, D, and E are root lattices which arise in many questions: in the theory of Lie groups and algebras, in the singularity theory, in the theory of rational surfaces, etc.

Lattices Γ. — Let now $N \geq 8, N \equiv 0 \bmod 4$. Set

$$\Gamma_N = \left\{ \sum_{i=1}^{N} a_i \cdot e_i \;\middle|\; 2 \cdot a_i \in \mathbf{Z},\ a_i - a_j \in \mathbf{Z},\ \sum_{i=1}^{N} a_i \in 2\mathbf{Z} \right\}.$$

The lattice Γ_N is generated by vectors $e_i + e_j$ and the vector $\frac{1}{2} \sum\limits_{i=1}^{N} e_i$; its parameters are

$$d(\Gamma_N) \geq \sqrt{2}, \quad \det(\Gamma_N) = 1.$$

Note that $\Gamma_8 = E_8$.

The lattices $A_1 = \mathbf{Z}, A_2, A_3 = D_3, D_4, D_5, E_6, E_7, E_8 = \Gamma_8$ have the density coinciding with that from the table. They are the densest lattices in their dimensions. A proof of this fact can be obtained by the reduction theory of quadratic forms.

Note that for all the described families

$$\lambda(L_N) \sim \log_2 \sqrt{N} \to \infty \quad \text{for} \quad N \to \infty.$$

We shall see that there are lattices which asymptotically behave significantly better.

For $N \geq 9$ we do not know the precise value of $\lambda_\ell(N)$ and only some bounds are known. As in the case of codes it is natural to call upper bounds for $\Delta(N)$ and $\Delta_\ell(N)$ *possibility bounds* and lower ones *existence bounds* (note however that for $\lambda(N)$ possibility bounds are lower ones, and existence bounds are upper ones).

We do not describe here various methods of constructing dense packings in dimensions from 9 up to 100000. We need here only the Leech lattice which is a very beautiful object arising in many questions.

Leech lattice. — There exists a unique integral even unimodular lattice of dimension 24 which has no vector of length $\sqrt{2}$ (recall that a lattice is called *even* iff the scalar square of any of its vectors is even). This lattice is called *Leech lattice* and is denoted by Λ_{24}; it is closely connected with Golay $[24, 12, 8]_2$-code C_{24}. It can be constructed in many ways. Here is one of the simplest.

The lattice Λ_{24} is generated by vectors

$$V_{i,c} = \frac{1}{\sqrt{8}} \cdot u_{i,c}, \quad 1 \leq i \leq 24,\ c \in C_{24},$$

where $u_{i,c}$ has ∓ 3 in i-th position and ± 1 in all other positions, and the upper sign is chosen for a position where the codeword c has 1.

The parameters of the Leech lattice are

$$\det(\Lambda_{24}) = 1, \quad d(\Lambda_{24}) = 2;$$

therefore,

$$\delta(\Lambda_{24}) = 1,\ \nu(\Lambda_{24}) = 0,\ \gamma(\Lambda_{24}) = 4,$$

$$\Delta(\Lambda_{24}) \approx 0.00193 \quad \text{and} \quad \lambda(\Lambda_{24}) \approx 0.376.$$

The covering radius of the Leech lattice equals $2\sqrt{2}$, i.e. balls of radius $2\sqrt{2}$ centered at lattice points cover the whole space $\mathbf{R}^{24}$. One can describe "deep holes" of the Leech lattice, i.e. points with distance $2\sqrt{2}$ from the nearest lattice point.

The automorphism group Co_0 of the Leech lattice is enormous:

$$|Co_0| = 8315553613086720000.$$

The maximal sporadic simple group, the Fischer-Gries group (the Monster), can be realised as the automorphism group of an algebra closely connected to the Leech lattice.

Kissing number. — There is another nice problem concerning sphere packings, of slightly a different nature (local). How many spheres can touch the given sphere in an N-dimensional space (all spheres being equal)? This number is called the *kissing number*.

The answer is known only in dimensions 1, 2, 3, 8, and 24, the kissing numbers being respectively 2, 6, 12, 240, and 196560. The examples are given by local arangements in the lattices A_1, A_2, A_3, D_4, E_8, and Λ_{24}.

3. Asymptotic problems

For asymptotic problems it is convenient to consider

$$\widetilde{\lambda} = \liminf_{N\to\infty} \lambda(N).$$

To compute $\widetilde{\lambda}$, i.e. to understand what is the maximum asymptotic density $\widetilde{\Delta} = 2^{-\widetilde{\lambda}N}$ of a high-dimensional packing, is most likely a very hard problem. We are interested in bounds for this value. The situation here is similar to that in coding theory, and $\widetilde{\lambda}$ is an analogue of $\alpha_q(\delta)$.

A *family* of packings is a set $\{P_N\}$ of packings, $P^N \subset \mathbf{R}^N$ where N runs over an infinite subset of $\mathbf{N}$.

Let

$$\lambda(\{P_N\}) = \liminf \lambda(P_N).$$

We call families with $\lambda(\{P_N\}) < \infty$ *good families* (they are analogues of good families of codes, i.e. those with $k/n \to R > 0$ and $d/n \to \delta > 0$).

One can show that $\inf\limits_{\{P_N\}} \lambda(\{P_N\}) = \widetilde{\lambda}$.

Similarly for lattices we set

$$\widetilde{\lambda}_\ell = \liminf_{N\to\infty} \lambda_\ell(N) = \inf_{\{L_N\}} \lambda(\{L_N\}).$$

Bounds. — Here are the best known estimates of $\widetilde{\lambda}$:

THEOREM. — $1 \geq \widetilde{\lambda}_\ell \geq \lambda \geq 0.599$.

The upper bound which is an existence bound is called the Minkowski bound, the lower one (a possibility bound) the Kabatyansky-Levenstein bound.

The Kabatyansky-Levenstein bound can be obtained by technique similar to that of the Mc Eliece-Rodemich-Ramsey-Welch bound in coding theory. The proof of the former consists of two parts : the first is the linear programing bound for packing of spheres on $S^N \subset \mathbf{R}^{N+1}$ and the second provides a way to pass from S^N to $\mathbf{R}^N$, which is based on the following simple construction. Let Λ_N be a packing in $\mathbf{R}^N$

and let us embed $\mathbf{R}^N$ into $\mathbf{R}^{N+1}$ in the natural way (i.e. assuming that vectors from $\mathbf{R}^N$ have zero for the last coordinate). Thus $\mathbf{R}^N \cap S^N = S^{N-1}$; let us consider those balls from Λ_N which are contained in the unit $(N-1)$-ball. Lifting their centers to S^N we obtain a packing of S^N and its parameters can be estimated through the parameters of Λ_N.

Here is another bound (Rogers):

PROPOSITION.

$$\Delta(N) \leq \sigma_N,$$

where σ_N *is the ratio of the volume of the intersection* $\left(\bigcup_{i=1}^{N+1} B_i \cap \Sigma_N\right)$ *to the volume of* Σ_N, *where* Σ_N *is the perfect simplex of edge length* 2 *and* $B_1, \ldots, B_{N+1}$ *are unit balls centered at the vertices of* Σ_N.

The Rogers bound gives $\widetilde{\lambda} \geq 0.5$ but it is quite useful for moderate values of N.

The Minkowski bound (which is an analogue of the Gilbert-Varshamov bound) can be obtained by a technique similar to the code-theoretic one. As in the case of codes almost all linear codes asymptotically lie on the Gilbert-Varshamov bound, here almost all lattice families have $\lambda(\{L_N\}) = 1$.

Thus it is known that there exists lattices of density $\Delta \sim 2^{-N}$ but we do not know how to construct them explicitly. The problem of explicit construction of dense packings naturally arises.

4. Codes and packings

Between codes and packings there exists a system of beautiful analogies. Indeed, one can consider an $[n,k,d]_q$-code $C \subseteq \mathbf{F}_q^n$ as the set of centers of a sphere packing (of radius $t = \left[\frac{d-1}{2}\right]$) in the Hamming metric. Minimum distance of a code corresponds to the diameter $d(L)$ of a sphere packing.

Linear codes correspond to lattice packings. Indeed, a linear code is a subset in $\mathbf{F}_q^n$ which is closed under addition and under multiplication by elements of $\mathbf{F}_q$, and lattice is closed under addition and multiplication by integers. Strictly speaking, we can consider "quasi-linear" codes, i.e. subsets which are closed under addition and under multiplication by elements of $\mathbf{F}_p$ (rather than $\mathbf{F}_q$) as an analogue of lattices, but we do not pursue this idea here.

Let C be a linear $[n,k,d]_q$-code. Then the volume (the cardinality) of the factor-space $\mathbf{F}_q^n/C$ equals q^{n-k}. For a lattice $L \subset \mathbf{R}^N$ the volume of the factor-space $\mathbf{R}^N/L$ equals $\det(L)$, i.e. $\log(\det L)$ is an analogue of the code codimension $(n-k)$. To be definite we shall assume that in the expression $\log(\det L)$ the log symbol corresponds to the binary logarithm.

There are two possible analogues of the dimension N of a lattice (which equals its rank): the length n and the dimension k of a code. We use the first one; nevertheless we think that the second can be also of some use.

The density of a packing corresponds to the density of a packing in the Hamming metric. Note that the density of a lattice packing equals the volume of the ball of radius d divided by $\det L$. For the density of a packing in the Hamming metric the analoguous statement is also true if we assume the ball volume to be normalized:

$$\text{the ball volume} = (\text{number of points in the ball})/q^n.$$

An analogy between code and lattice parameters is not complete. Indeed, the density of packing does not change under a homothety $L \mapsto a \cdot L$. Hence one can assume that $d(L) = 1$ (or $\det L = 1$) and thus a packing has two essential parameters N and Δ, whence a code has three essential parameters n, k, and d. Thus the unique asymptotic parameter λ is an analogue of the pair of code asymptotic parameters (δ, R).

An asymptotic by good packing family (i.e. with $\lambda < \infty$ for $N \to \infty$) is an analogue of an asymptotically good code family (i.e. with $R \cdot \delta > 0$ for $n \to \infty$).

The Gilbert-Varshamov bound corresponds to the Minkowski bound; and the Hamming bound to the condition $\lambda \geq 0$. It is no clear which is a reasonable analogue of the Plotkin bound in coding theory (this is an interesting question). The Kabatyansky-Levenstein bound corresponds to the Mc Elice-Rodemich-Ramsey-Welch bound.

Packings on a sphere correspond to constant-weight codes.

An interresting question about analogies between concrete code families and lattice families is mostly open. For instance, parity check codes correspond either to lattices A_N, or to D_N.

The θ-function of a lattice corresponds to the code enumerator; this analogy is quite useful.

Unimodular lattices correspond to self-dual codes.

We are interested in analogues of algebraic-geometric codes. Below we shall describe some of them. These analogies are closely connected to a very deep analogy between algebraic curves over finite fields and algebraic number fields.

Chapter II
Curves, number fields and packings

To construct sphere packing starting from curves over finite fields or from algebraic number fields one should first recall the main notions of these two domains. That of curves was already recalled in the previous talks, § 1 is devoted to algebraic number theory. We also stress the parallelism between number fields and curves over finite fields.

Then we can give some sphere packing constructions, choosing only those that look both simple, natural and beautiful. Each of then can be used to produce many interesting examples of lattice packing. To show that they are really good we study these packing for N tending to infinity.

1. Algebraic number fields

A finite extension k of $\mathbf{Q}$ is called an algebraic number field. Its degree $n = [k : \mathbf{Q}]$ equals the dimension of k as a $\mathbf{Q}$-vector space.

Algebraic integers. — If $x \in k$ satisfies the relation

$$x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_1 \cdot x + a_0 = 0, \quad a_i \in \mathbf{Z}$$

then x is called an algebraic integer or an integral element of k.

PROPOSITION. — *The sum and the product of algebraic integers are also algebraic integers.*

COROLLARY. — *The subset of integers of k is a ring.*

This ring O_k is called the ring of integers of k or its maximal order. Any subring $O \subseteq O_k$ of finite index $[O_k : O]$ is called an order.

PROPOSITION. — *For any $z \in k$ there exists $c \in \mathbf{Z}$ such that $c \cdot z$ is an algebraic integer.*

Therefore we have

$$O_k = \mathbf{Z}w_1 + \cdots + \mathbf{Z}w_n$$

for some basis $\{w_1, \ldots, w_n\}$ of k over $\mathbf{Q}$: such a basis is called a *fundamental basis* of k.

Trace and norm. — Let now $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ be the set of distinct embeddings of k into $\mathbf{C}$. Since for any embedding σ_i such that $\sigma_i(k)$ does not lie in $\mathbf{R}$ the embedding $\bar{\sigma}_i$ does not coincide with σ_i, these embeddings are present in the set Σ in pairs $(\sigma_i, \bar{\sigma}_i)$. Thus if s is the number of embeddings $\sigma_i : k \hookrightarrow \mathbf{C}$ with $\sigma_i(k) \subset \mathbf{R}$ (such embeddings are called real) and t is the number of pairs $(\sigma_i, \bar{\sigma}_i)$ where $\sigma_i \neq \bar{\sigma}_i$ (such embeddings are called complex) then $s + 2t = n$.

Let us set

$$\begin{aligned} \mathrm{Tr}(x) &= \mathrm{Tr}_{k/\mathbf{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x), \\ N(x) &= N_{k/\mathbf{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x). \end{aligned}$$

$\mathrm{Tr}(x)$ is called the $(k/\mathbf{Q})$-*trace* of x, and $N(x)$ the $(k/\mathbf{Q})$-*norm* of x.

If $a_m \cdot x^m + \cdots + a_0 = 0$ is the minimal equation of x over $\mathbf{Q}$ then $m|n$, moreover

$$\mathrm{Tr}(x) = -na_{m-1}/(ma_m) \quad \text{and} \quad N(x) = (-1)^n (a_0/a_m)^{n/m}.$$

The bilinear form $\mathrm{Tr}(x \cdot y)$ is non-degenerate; $N(x) \in \mathbf{Z}$ if and only if $x \in O_k$.

Discriminant. — Let k be an algebraic number field of degree n and let $\{w_1, \ldots, w_n\}$ be its fundamental basis. The integer $D_k = \det(\mathrm{Tr}(w_i \cdot w_j))$ is called the (absolute) *discriminant* of k.

It can be checked that this definition does not depend on the choice of $\{w_1, \ldots, w_n\}$.

THEOREM. — *If $n > 1$, i.e. $k \neq \mathbf{Q}$, then $|D_k| > 1$.*

One can give another definition of D_k which follows. Let s be the number of real embeddings σ_i and t be the number of conjugate pairs $(\sigma_j, \bar{\sigma}_j)$ of complex embeddings of k. Let $A = \mathbf{R}^s \times \mathbf{C}^t$ be a commutative $\mathbf{R}$-algebra of rank $n = s + 2t$, and let σ be the following ring embedding

$$\begin{aligned} k &\xrightarrow{\sigma} \mathbf{R}^s \times \mathbf{C}^t, \\ a &\longmapsto (\sigma_1(a), \ldots, \sigma_s(a); \sigma_{s+1}(a), \ldots, \sigma_{s+t}(a)). \end{aligned}$$

The image $\sigma(k)$ generates A (over $\mathbf{R}$); check also that $\sigma(O_k)$ is a lattice in $A \simeq \mathbf{R}^n$.

The following proposition will be used later.

PROPOSITION.

$$|\det \sigma(O_k)| = 2^{-t} \cdot \sqrt{|D_k|}.$$

Proof. — Let $\{w_1, \ldots w_n\}$ be a fundamental basis of k, let $\sigma_j(w_i) = x_{ji} \in \mathbf{R}$ for any $i, j = 1, \ldots, s$, and let $\sigma_{s+j}(w_i) = y_{ji} + \sqrt{-1} \cdot z_{ji}$ for any $i, j = 1, \ldots, t$, where y_{ji} and $z_{ji} \in \mathbf{R}$. Then

$$d = \det \sigma(O_k) = \det \begin{bmatrix} x_{11} & \cdots & x_{s1} & y_{11} & z_{11} & \cdots & y_{t1} & z_{t1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ x_{1n} & \cdots & x_{sn} & y_{1n} & z_{1n} & \cdots & y_{tn} & z_{tn} \end{bmatrix}$$

It is clear that $d = d^*/(-2\sqrt{-1})^t$ where

$$d^* = \det \begin{bmatrix} x_{11} & \cdots & x_{s1} & y_{11} + \sqrt{-1} \cdot z_{11} & y_{11} - \sqrt{-1} \cdot z_{11} & \cdots \\ \vdots & & \vdots & \vdots & & \\ x_{1n} & \cdots & x_{sn} & y_{1n} + \sqrt{-1} \cdot z_{1n} & y_{1n} - \sqrt{-1} \cdot z_{1n} & \cdots \end{bmatrix}$$

i.e. $D^* = \det(\sigma_i(w_j))$, where $\{\sigma_1, \ldots, \sigma_n\}$ is the full set of embeddings of k into $\mathbf{C}$. Since by the definition of the trace

$$\mathrm{Tr}(w_i \cdot w_j) = \sum_{\ell=1}^{n} \sigma_\ell(w_i) \cdot \sigma_\ell(w_j)$$

for $1 \leq i, j \leq n$, one has a matrix equality

$$(\mathrm{Tr}(w_i \cdot w_j)) = {}^{\mathrm{trans}}(\sigma_\ell(w_i)) \cdot (\sigma_\ell(w_j))$$

where *trans* denotes transposition, whence

$$D_k = \det(\mathrm{Tr}(w_i \cdot w_j)) = (d^*)^2$$

and we are done.

Units. — An element $a \in O_k$ is called a *unit* if and only if $a^{-1} \in O_k$. Clearly all the units form a group which is denoted O_k^*. Torsion elements of O_k^* are roots of unity.

One easily checks that $a \in O_k^*$ if and only if $N_{k/\mathbf{Q}}(a) = \pm 1$.

The structure of the group O_k^* is rather simple, it is described by the famous Dirichlet theorem:

THEOREM. — *O_k^* is the product of its finite torsion subgroup by a free abelian group of rank $r = s + t - 1$.*

Sketch of proof. — Let us consider the map

$$\begin{array}{ccc} O_k^* & \xrightarrow{\log} & \mathbf{R}^{s+t} \\ a & \longmapsto & (\log|\sigma_1(a)|, \ldots, \log|\sigma_s(a)| \; ; \; \log|\sigma_{s+1}(a)|^2, \ldots) \end{array}$$

Its kernel is the torsion subgroup of O_k^*, and its image $\log(O_k^*)$ is contained in the hyperplane $H \subset \mathbf{R}^{s+t}$ defined by $x_1 + \cdots + x_{s+t} = 0$. Indeed,

$$|\sigma_1(a)| \cdots |\sigma_s(a)| \cdot |\sigma_{s+1}(a)|^2 \cdots |\sigma_{s+t}(a)|^2 = |N(a)| = 1.$$

One can show that $\log(O_k^*)$ is a lattice in H (of full rank) which gives the theorem.

The determinant of this lattice

$$R = R_k = \det \begin{bmatrix} \log|\sigma_1(u_1)| & \cdots & \log|\sigma_1(u_{s+t-1})| \\ \vdots & & \vdots \\ \log|\sigma_{s+t-1}(u_1)| & \cdots & \log|\sigma_{s+t-1}(u_{s+t-1})| \end{bmatrix}$$

where $\{u_1, \dots, u_{s+t-1}\}$ is a basis of O_k^* modulo torsion, is called the *regulator* of k.

Places. — A map $||\cdot|| : k \to \mathbf{R}$ is called an *absolute value* if the following conditions hold :

- $||0|| = 0$, $||x|| > 0$ if $x \neq 0$;
- there exist $x, y \in k^*$ such that $||x|| \neq ||y||$;
- $||x \cdot y|| = ||x|| \cdot ||y||$;
- there exists a positive real λ such that $||x + y|| \leq \lambda \cdot (||x|| + ||y||)$.

Two absolute values $||\cdot||_1$ and $||\cdot||_2$ are *equivalent* if there exists a positive real θ such that $||\cdot||_1 = ||\cdot||_2^\theta$. An equivalence class of absolute values is called a *place* of k.

There is a beautiful description of all places of a number field.

Let $\sigma : k \hookrightarrow \mathbf{C}$ be an embedding of fields. Let us put $||x||_\sigma = |\sigma(x)|$ if σ is a real embedding (i.e. $\mathrm{Im}\sigma \subset \mathbf{R}$), and $||x||_\sigma = |\sigma(x)|^2$ if σ is a complex embedding. These are absolute values. One can check that two such absolute values $||\cdot||_\sigma$ and $||\cdot||_{\sigma'}$ are equivalent if and only if either $\sigma' = \sigma$, or $\sigma' = \bar{\sigma}$. Thus we obtain s *real* and t *complex* places of k. These places are called *infinite* or *archimedean*, the set of infinite places is denoted by S_∞.

Let then $\mathfrak{p}$ be a maximal ideal of O_k. For $x \in k^*$ let

$$\mathrm{ord}_\mathfrak{p}(x) = \max\{n |\ x \in \mathfrak{p}^n\}.$$

One easily checks that

$$\mathrm{ord}_\mathfrak{p}(x \cdot y) = \mathrm{ord}_\mathfrak{p}(x) + \mathrm{ord}_\mathfrak{p}(y)$$

for any $x, y \in k^*$, and if also $x + y \in k^*$ then

$$\mathrm{ord}_\mathfrak{p}(x + y) \geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(y)\}.$$

Let us define the corresponding absolute value: for $x \in k^*$ let

$$||x||_\mathfrak{p} = N(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(x)},$$

where $N(\mathfrak{p}) = |O_k/\mathfrak{p}|$. For such an absolute value (and for any one equivalent to it) a stronger condition holds:

$$||x + y|| \leq \lambda \cdot \max\{||x||, ||y||\}$$

(which is wrong for archimedean absolute values). Such absolute values are called *non-archimedean*. If $\mathfrak{p} \neq \mathfrak{p}'$ then the corresponding absolute values are not equivalent, i.e. each maximal ideal (each closed point of $\operatorname{Spec} O_k$) corresponds to a place of k. Such places are called *finite* or *non-archimedean*.

It comes out that each place of a number field is either infinite or finite. If v is a place of k then the absolute values defined above are called *normalized* and denoted $||\cdot||_v$.

Let us recall that if there are no complex places, the number field is called *totally real*, if there are no real places, it is called *totally complex*.

Class group. — Let $\mathfrak{a}$ be an ideal of O_k, and let $a \in k^*$. The set $\mathfrak{c} = a^{-1}\mathfrak{a}$ is called a *fractional ideal*. The set of non-zero fractional ideals is a group with the composition defined by

$$\mathfrak{a} \cdot \mathfrak{b} = \{x \cdot y |\, x \in \mathfrak{a}, y \in \mathfrak{b}\}.$$

Note that the inverse element is given by

$$\mathfrak{a}^{-1} = \{x |\, x^{-1} \in \mathfrak{a} - \{0\}\} \cup \{0\}.$$

We call fractional ideals $\mathfrak{c}$ and $\mathfrak{c}_1$ *equivalent* if $\mathfrak{c}_1 = a\mathfrak{c}$ for some $a \in k^*$. Equivalence classes of non-zero fractional ideals form a group Cl_k which is called the (ideal) *class group* of k.

THEOREM. — *The group* Cl_k *is finite for any algebraic number field* k.

The order of the class group $h = h_k = |\,\mathrm{Cl}_k\,|$ is called the *class number* of k.

Extensions. — Sometimes it is necessary to consider field extensions K/k, K and k being algebraic number fields. Let $[K : k] = \dim_k K = n$ and let O_K and O_k be the rings of integers in K and k, respectively. Any $x \in K$ is a root of an irreducible over k equation of the form

$$a_m \cdot x^m + \cdots + a_0 = 0$$

where $a_i \in O_k$ for $i = 0, \ldots, m$.

Let us define the (*relative*) *trace* and *norm* as

$$\begin{aligned} \mathrm{Tr}_{K/k}(x) &= -a_{m-1}/a_m, \\ N_{K/k}(x) &= (-1)^m a_0/a_m. \end{aligned}$$

Different. — Let us consider the following subset in k:

$$\mathfrak{B}_{K/k} = \{x \in K |\ \mathrm{Tr}_{K/k}(x \cdot y) \in O_k \text{ for any } y \in O_k\}.$$

One can easily check that $\mathfrak{B}_{K/k}$ is a O_K-submodule in K which contains O_K. Hence there exist a unique ideal $\mathfrak{D}_{K/k}$ in O_k such that $\mathfrak{D}_{K/k} \cdot \mathfrak{B}_{K/k} = O_K$. The ideal $\mathfrak{D}_{K/k}$ is called the *different* of the extensions K/k. The ideal

$$D_{K/k} = \{N_{K/k}(x) |\ x \in \mathfrak{D}_{K/k}\}$$

in O_k is called the (relative) *discriminant* of the extension K/k.

The relative discriminant $D_{K/\mathbf{Q}}$ equals the ideal in $\mathbf{Z}$ generated by the absolute discriminant D_k. Thus D_k is defined by $D_{k/\mathbf{Q}}$ up to a sign.

Let $L \supset K \supset k$ be algebraic number fields. Then $\mathfrak{D}_{L/k} = \mathfrak{D}_{L/k} \cdot \mathfrak{D}_{K/k}$.

Proposition. — *Let the degree of the extension L/K be equal to m. Then*

$$D_{L/k} = D_{K/k}^m \cdot N_{K/k}(D_{L/K}).$$

Unramified extensions. — An algebraic field extension is called *unramified* if $D_{K/k} = (1)$. We have just seen that $\mathbf{Q}$ has no unramified extensions.

The rule $\mathfrak{a} \mapsto \mathfrak{a} \cdot O_K$ defines a group homomorphism $\mathrm{Cl}_k \to \mathrm{Cl}_K$; the norm map defines a homorphism $\mathrm{Cl}_K \to \mathrm{Cl}_k$. If an extension K/k is unramified and abelian (i.e. normal with an abelian Galois group $\mathrm{Gal}(K/k)$) then the (global) class field theory gives

Theorem. — $\mathrm{Gal}(K/k)$ *is isomorphic to the factor-group* $\mathrm{Cl}_k / N_{K/k}(\mathrm{Cl}_k)$.

Moreover there exists a maximal unramified abelian extension K_1 which is called the *Hilbert* or *absolute class-field* of k; $\mathrm{Gal}(K_1/k)$ is isomorphic to Cl_k.

Theorem. — *Let K_1 be the absolute class field of an algebraic number field k. Then the canonical homomorphism $\mathrm{Cl}_k \to \mathrm{Cl}_{K_1}$ is trivial, i.e. all the ideals of O_k become principal in O_{K_1}.*

Class field towers. — As we have seen above $\mathbf{Q}$ has no unramified extensions. There exist many algebraic number fields k with $h_k > 1$; for these fields the absolute class field K_1 is an unramified extension of degree h_K. If $h_{k_1} > 1$ we get the field $K_2 = (K_1)_1$ which is an unramified extension K_2/k (note that the extension K_2/k cannot be abelian). Iterating this construction we get either

(a) $h_{K_n} = 1$ for some n; hence we cannot obtain a larger unramified extension of k by our construction; or

(b) $h_{K_n} > 1$ for any n and hence we obtain an infinite unramified tower $k \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots$.

An algebraic number field which satisfies the last condition is called a field with an *infinite class field tower.*

THEOREM. — *There exists a function $f : \mathbf{N} \to \mathbf{N}$ such that if k is an algebraic number field of degree n and D_k has at least $f(n)$ distinct prime divisors then k has an infinite class field tower.*

On can give a precise formula for $f(n)$ but we do not need it here.

The discriminant D_k of a field satisfying the conditions of this theorem cannot be small. One can ask how to construct fields with infinite class field towers and small discriminants. To compare fields of various degrees one should use the parameter $|D_k|^{1/n}$ (note that it is constant in unramified towers). Here are the best examples discovered by J. Martinet.

THEOREM. — *The field*

$$k = \mathbf{Q}\left(\cos\frac{2\pi}{11}, \sqrt{-46}\right)$$

of degree 10 *over* $\mathbf{Q}$ *has an infinite class field tower;*

$$|D_k| = 2^{15} \cdot 11^8 \cdot 23^5 \quad \textit{and} \quad |D_k|^{1/n} \approx 92.37.$$

The field

$$k = \mathbf{Q}\left(\sqrt{2}, \sqrt{3 \cdot 5 \cdot 7 \cdot 23 \cdot 29}\right)$$

of degree 4 *has an infinite class field tower of totally real fields;*

$$|D_k| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 23^2 \cdot 29^2 \quad \textit{and} \quad |D_k|^{1/n} \approx 1058.57.$$

On the other hand using so-called "explicit formulae" one can obtain a lower bound for $|D_k|^{1/n}$:

THEOREM. — *let k_i be algebraic number fields and let $n_i = [k_i : \mathbf{Q}] \to \infty$. Let s_i be the number of real embeddings and t_i the number of pairs of complex embeddings of k_i. Suppose that the limits $\sigma = \lim s_i/n_i$ and $\tau = \lim t_i/n_i$ do exist. Then*

$$\liminf |D_{k_i}|^{1/n_i} \geq (4\pi e^{\gamma+1})^{\sigma} \cdot (4\pi e^{\gamma})^{2\tau}$$

γ being the Euler constant. If the generalized Riemann hypothesis is valid then

$$\liminf |D_{k_i}|^{1/n_i} \geq (8\pi e^{\gamma+\pi/2})^{\sigma} \cdot (8\pi e^{\gamma})^{2\tau}.$$

Curves and number fields. — Algebraic number fields and fields of rational functions on curves over finite fields are called *global fields*. They have many features in common. Here we briefly describe some of them.

Let k be an algebraic number field and let O_k be its ring of integers. Let X be a curve over $\mathbf{F}_q$, $K = \mathbf{F}_q(X)$, let F be a finite set of closed points of X, $U = X - F$, and let $O_F = \mathbf{F}_q[U]$ be the ring of rational functions which are regular on U.

For both rings O_k and O_F any factor over a maximal ideal is a finite field.

For O_F all these fields contain $\mathbf{F}_q$ (the so-called "case of equal characteristics"), in the number field case among these fields there is an extension of $\mathbf{F}_p$ for any prime p (the "case of different characteristics").

The notion of a place is in fact good for any global field. One can show that any place of $K = \mathbf{F}_q(X)$ is finite and corresponds to a closed point of X.

We can choose various finite sets F and get various rings O_F. In the number case we can choose a finite set S of maximal ideals of O_k and consider the ring O_S which is obtained from O_k by inverting non-zero elements of ideals from S; note that $\operatorname{Spec} O_S = \operatorname{Spec} O_k - S$ and $O_\phi = O_k$. Rings of the form O_S or O_F can be characterized as those having one-dimensional irreducible regular spectra of finite type over $\mathbf{Z}$.

The number field case is mostly more difficult than the function field case. Indeed, $\operatorname{Spec} O_F$ can be embedded into a proper scheme X and $\operatorname{Spec} O_k$ has no "good" embedding into a proper scheme. The last fact makes it indispensable to study infinite places of $\operatorname{Spec} O_k$.

The field $\mathbf{F}_q(T)$, T being a variable, is an analogue of $\mathbf{Q}$ since $k = \mathbf{F}_q(X)$ (where X is a curve over $\mathbf{F}_q$) is a finite extension of $\mathbf{F}_q(T)$; the ring $\mathbf{F}_q[T]$ is an analogue of $\mathbf{Z}$. Note however, that there is no canonical embedding of $\mathbf{F}_q(T)$ into $\mathbf{F}_q(X)$ and hence we cannot say that $[\mathbf{F}_q(X) : \mathbf{F}_q(T)]$ is an analogue of the degree of an algebraic number field.

One can suggest another analogue of the degree, namely, the number of $\mathbf{F}_q$-points of X. Indeed, if $|X(\mathbf{F}_q)| = N$, then the degree of a map $f : X \to \mathbf{P}^1$ (i.e. the degree of an extension $[\mathbf{F}(X) : \mathbf{F}_q(T)]$) can not be too small: $\deg f \geq N/(q+1)$, since any $\mathbf{F}_q$-point of X is mapped to an $\mathbf{F}_q$-point of $\mathbf{P}^1$ and any fiber of f contains at most $\deg f$ $\mathbf{F}_q$-rational points.

Let a map $f : X \to \mathbf{P}^1$ be fixed, and let us fix an $\mathbf{F}_q$-point ∞ on $\mathbf{P}^1$. Then we have $\mathbf{P}^1 - \{\infty\} = \mathbf{A}^1$, $\mathbf{F}_q[\mathbf{A}^1] = \mathbf{F}_q[T]$ and we can regard the integral closure of $\mathbf{F}_q[T]$ in $\mathbf{F}_q(X)$ as an analogue of O_k. Note that this closure coincides with $O_{F_\infty} = \mathbf{F}_q[X - F_\infty]$ where $F_\infty = f^{-1}(\infty)$.

The ramification divisor B_f of the map f is an analogue of the different. The discriminant corresponds to the divisor $D = \sum e_p p$ where e_p is the ramification index of $P \in \mathbf{P}^1$. The value $\log \sqrt{|D_k|}$ is an analogue of the genus of a curve.

A fractional ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$, where $\mathfrak{p}$ runs over prime ideals of O_k, corresponds to a divisor on X, $\mathfrak{a}^{-1}$ corresponds to $L(D)$ and the group $\operatorname{Pic} X$ is an analogue of Cl_k.

Note also that $\mathbf{F}_q(T)$ has no unramified extensions (just as $\mathbf{Q}$).

The value $\liminf(g/N)$ is an analogue of $\liminf \log |D_k|/n$. The "explicit formulae" technique gives estimates for both these values.

The question about an adequate analogue of the number of rational points on the Jacobian is rather delicate. One can suggest that its "genuine" analogue is the product $h_k R_k$ rather than h_k.

Units O_S^* of the ring O_S correspond to units O_F^* of O_F; the group μ_k is an analogue of $\mathbf{F}_\mathbf{q}^*$. Moreover, just as in the number field case, $O_F^*/\mathbf{F}_q^*$ is a free abelian group of rank $|F| - 1$ (note that $O_S^*/\mu_k \simeq \mathbf{Z}^{s+t+|S|-1}$).

There are some other analogies which are less clear but also useful, and we use them in the next section.

2. Number field and function field lattices

We are ready to present several constructions of lattices in the context of number theory and algebraic geometry and to calculate or estimate their parameters.

These results are quite recent and their discovery was stimulated by the theory of algebraic-geometric codes.

Additive lattices

Let k an be algebraic number field, of degree $N = s + 2t$, let O_k be its ring of integers, and let

$$\sigma : k \hookrightarrow \mathbf{R}^s \times \mathbf{C}^t$$

be the standard embedding. The image $L = \sigma(O_k)$ is a lattice of rank N.

Parameters. — Let us compute the density of L. We have already seen above that

$$\det L = 2^{-t}\sqrt{|D_k|}.$$

PROPOSITION.

$$\sqrt{s+t} \geq d(L) \geq \sqrt{s/2+t}$$

and if $t = 0$ *then*

$$d(L) = \sqrt{N}.$$

Proof. — Let

$$x = \sigma(f) = (x_1, \ldots, x_s; y_1 + \sqrt{-1}\cdot z_1, \ldots, y_t + \sqrt{-1}\cdot z_t).$$

We have

$$|\sigma(f)| = \sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t}(y_j^2 + z_j^2)}.$$

For $f = 1$, $|\sigma(1)| = \sqrt{s+t}$.

The arithmetic mean geometric mean inequality yields

$$\begin{aligned}
\sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t}(y_j^2 + z_j^2)} &\geq \frac{1}{\sqrt{2}}\cdot\sqrt{\sum_{j=1}^{s} x_j^2 + 2\cdot\sum_{j=1}^{t}(y_j^2 + z_j^2)} \\
&\geq \sqrt{\frac{s+2t}{2}}\cdot\left[\prod_{j=1}^{s} x_j^2 \cdot \prod_{j=1}^{t}(y_j^2 + z_j^2)^2\right]^{1/2N} \\
&= \sqrt{\frac{s}{2}+t}\cdot|N_{K/\mathbf{Q}}(f)|^{1/N} \\
&\geq \sqrt{\frac{s}{2}+t},
\end{aligned}$$

since $N_{K/\mathbf{Q}}(f) \in \mathbf{Z}$. In the totally real case

$$\sqrt{\sum_{j=1}^{N} x_j^2} \geq \sqrt{N}\cdot\left[\prod_{j=1}^{N} x_j^2\right]^{1/2N} = \sqrt{N}\cdot|N_{K/\mathbf{Q}}(f)|^{1/N} \geq \sqrt{N},$$

and we get the required result.

Unramified towers. — Now let the field K vary so that $N \to \infty$, and K is either totally real, or totally complex. Then

$$\lambda(L) \sim -\log_2\sqrt{\frac{\pi e}{2}} + \frac{1}{N}\cdot\log_2\sqrt{|D_K|}.$$

If we want to construct good lattices the last term should be bounded. It is definitely so if K runs over an unramified tower of fields over some K_0, in which case it is just constant. We get

THEOREM. — *If a number field K_0 of degree N_0 has an infinite unramified tower of fields $K \supset K_0$ which are either totally real, or totally complex, then it yields an asymptocally good family of lattices $\{L_N \subset \mathbf{R}^N\}$ with*

$$\lambda(\{L_N\}) \sim -\log_2 \sqrt{\frac{\pi e}{2}} + \frac{1}{N_0} \cdot \log_2 \sqrt{|D_{K_0}|}.$$

For $K_0 = \mathbf{Q}\left(\cos\frac{2\pi}{11}, \sqrt{-46}\right)$ we get $\lambda \sim 2.2218$ (recall that K_0 has an infinite class field tower).

On the other hand, the above "explicit formulae" theorem shows that for any family of fields K we cannot get asymptotically less than $1.193\cdots$ (and $1.694\cdots$ assuming the generalized Riemann hypothesis).

Multiplicative number field lattices

Up to this moment we have used the additive groups of global fields. Now we are going to exploit their multiplicative structure.

Construction. — We start with a number field K of degree $N = s + 2t$ and a finite number of its places $S = S_\infty \cup S_f$ which includes all archimedean ones, let $n = |S|$. Let O_S^* be the set of S-units, i.e. $a \in O_S^*$ if and only if all the prime divisors of its numerator and denominator belong to S_f.

There is a natural map

$$\begin{array}{ccc} O_S^* & \xrightarrow{\varphi_S} & \mathbf{R}^n, \\ f & \longmapsto & \{\log ||f||_v\}, \end{array}$$

where $v \in S$, and $||\cdot||_v$ is the normalized absolute value, i.e. $||f||_v = |\sigma_v(f)|$ for real places, $||f||_v = |\sigma_v(f)|^2$ for complex ones, and $||f||_v = N(v)^{-ord_v(f)}$ for $v \in S_f$. It is clear that

$$\mathrm{Ker}\varphi_S = \mu_K$$

is the group of roots of 1 in K, and that

$$\mathrm{Im}\,\varphi_S \subset H = \left\{x \in \mathbf{R}^n \middle| \sum x_i = 0\right\}$$

because of the product formula.

Parameters. — Let R be the regulator of K and let $h = h_K$ be its class number. Set $h(f) = \sum_v |\log ||f||_v|$ for $f \in K^*$, this is the *height function* (sorry that it is denoted by the same letter as the class number); $h(f) = 0$ if and only if $f \in \mu_K$. We set

$$h(K) = \min_{f \in K^* - \mu_K} h(a)$$

and call it the *height of the field* K.

PROPOSITION. — *Let $L_S = \varphi_S(O_S^*)$. Then*

(a) $$d(L_S) \geq \tfrac{1}{\sqrt{n}} \cdot h(K),$$

(b) $$\operatorname{rk} L_S = n-1 \quad \textit{and} \quad \det L_S \leq \sqrt{n} \cdot R \cdot h \cdot \prod_{v \in S_f} \log N(v).$$

We do not prove it here because the function field case that follows is much simpler and gives better results.

Asymptotic behaviour. — To obtain asymptotically good families of lattices we are going to consider unramified towers of fileds. In such towers $\frac{1}{N} \cdot \log \sqrt{|D_K|}$ is constant. Let us for simplicity assume that all the fields in the tower are totally real.

THEOREM. — *If a number field K_0 of degree n_0 has an infinite unramified tower of totally real fields then the above construction with $S = S_\infty$ yields a family of asymptotically good multiplicative lattices $\{L_N = L_S \subset \mathbf{R}^N\}$ with $N \to \infty$ and*

$$\lambda(\{L_N\}) \leq -\log_2 \sqrt{\pi^3 e/2} - \log_2 \log_e \left[\frac{1+\sqrt{5}}{2}\right] + \frac{1}{n_0} \cdot \log_2 |D_{K_0}|.$$

For $K_0 = \mathbf{Q}\left(\sqrt{2}, \sqrt{3 \cdot 5 \cdot 7 \cdot 23 \cdot 29}\right)$ we get $\lambda \lesssim 8.41$.

Function field lattices

Here is a direct function field analogue of the previous construction.

Construction. — Let

$$O_{\mathcal{P}}^* = \{f \in K^* \mid \operatorname{Supp}(f) \subseteq \mathcal{P}\}.$$

Recall that $\mathcal{P} \subseteq X(\mathbf{F}_q)$ for a curve X over $\mathbf{F}_q$ and $K = \mathbf{F}_q(X)$. Let $\operatorname{Div}_{\mathcal{P}}(X)$ denote the group of divisors supported in $\mathcal{P}$, $\operatorname{Div}^0(X)$ of those of degree 0, $P_{\mathcal{P}}(X)$ the subgroup of principal divisors. Let $J_X = \operatorname{Div}^0(X)/P(X)$ be the Jacobian of X.

There is a natural map

$$\begin{array}{rcl} O_{\mathcal{P}}^* & \xrightarrow{\varphi_{\mathcal{P}}} & \operatorname{Div}_{\mathcal{P}}(X) \simeq \mathbf{Z}^n, \\ f & \longmapsto & (f). \end{array}$$

It is clear that $\operatorname{Ker} \varphi_{\mathcal{P}} = \mathbf{F}_q^*$ is again the group of roots of 1 in K, and that

$$\operatorname{Im} \varphi_{\mathcal{P}} \subseteq \operatorname{Div}_{\mathcal{P}}^0(X) \simeq A_{n-1} = \left\{x \in \mathbf{Z}^n \mid \sum x_i = 0\right\}.$$

We set

$$L_{\mathcal{P}} = \varphi_{\mathcal{P}}(O_{\mathcal{P}}^*) \subseteq A_{n-1} \otimes \mathbf{R} \simeq \mathbf{R}^{n-1}.$$

Parameters. — Let us estimate the parameters of $L_{\mathcal{P}}$.

THEOREM. — *Let* $L_{\mathcal{P}} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P}})$. *Then*

(a) $$d(L_{\mathcal{P}}) \geq \min_{f \in O^*_{\mathcal{P}} - \mathbf{F}^*_q} \sqrt{2 \cdot \deg f} \geq \sqrt{\frac{2 \cdot |X(\mathbf{F}_q)|}{q+1}},$$

(b) $$\operatorname{rk} L_{\mathcal{P}} = n - 1 \quad \textit{and}$$
$$\det L_{\mathcal{P}} \leq \sqrt{n} \cdot |J_X(\mathbf{F}_q)| \leq \sqrt{n} \cdot \left[1 + q + \frac{|X(\mathbf{F}_q)| - q - 1}{g}\right]^g.$$

Proof.

(a) Let $f \in O^*_{\mathcal{P}}$, $f \notin \mathbf{F}^*_q$,

$$\varphi_{\mathcal{P}}(f) = (x_1, \ldots, x_n) \in \mathbf{Z}^n.$$

Then

$$|\varphi_{\mathcal{P}}(f)| = \sqrt{\sum x_i^2} \geq \sqrt{\sum |x_i|} = \sqrt{2 \cdot \deg f},$$

since $x_i \in \mathbf{Z}$, $\sum x_i = 0$, $\deg f = \sum_{x_i > 0} x_i$. Any $f \in K$ maps $\mathbf{F}_q$-points to $\mathbf{F}_q$-points of $\mathbf{P}^1$. Therefore

$$|X(\mathbf{F}_q)| \leq (q+1) \cdot \deg f$$

and we get the second inequality.

(b) We know that $\det A_{n-1} = \sqrt{n}$ and

$$\det L_{\mathcal{P}} = [A_{n-1} : L_{\mathcal{P}}] \cdot \det A_{n-1}.$$

Then

$$A_{n-1} \simeq \operatorname{Div}^0_{\mathcal{P}}(X) \subset \operatorname{Div}^0(X),$$

and

$$L_{\mathcal{P}} \simeq P_{\mathcal{P}}(X) = P(X) \cap \operatorname{Div}^0_{\mathcal{P}}(X).$$

Therefore

$$[A_{n-1} : L_{\mathcal{P}}] \leq [\operatorname{Div}^0(X) : P(X)] = |J_X(\mathbf{F}_q)|.$$

To prove the second inequality it is sufficient to establish the following bound for the number of points on the Jacobian:

$$|J_X(\mathbf{F}_q)| \leq \left[1 + q + \frac{|X(\mathbf{F}_q)| - q - q}{g}\right]^g.$$

Indeed, $|J_X(\mathbf{F}_q)| = \prod_{i=1}^{2g} (1 - \omega_i)$, ω_i being the Frobenius roots, $|\omega_i| = \sqrt{q}$, $\omega_{g+i} = \bar{\omega}_i$. The arithmetic mean geometric mean inequality yields

$$\prod_{i=1}^{2g} (1 - \omega_i) = \prod_{i=1}^{g} (q + 1 - \omega_i - \bar{\omega}_i) \leq \left[\frac{\sum_{i=1}^g (q + 1 - \omega_i - \bar{\omega}_i)}{g}\right]^g,$$

and the estimate for $|J_X(\mathbf{F}_q)|$ follows from

$$-\sum_{i=1}^{g} (\omega_i + \bar{\omega}_i) = |X(\mathbf{F}_q)| - q - 1.$$

Asymptotic behaviour. — We consider families of curves of growing genus with

$$\frac{|X(\mathbf{F}_q)|}{g} \to A,$$

and set $\mathcal{P} = X(\mathbf{F}_q)$. We get

THEOREM. — *A family of curves X over $\mathbf{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbf{F}_q)|}{g} \to A > 0$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbf{R}^N\}$ with

$$\lambda(\{L_N\}) \le -\log_2 \sqrt{\pi e} + \log_2 \sqrt{q+1} + A^{-1} \log_2(1+q+A).$$

We are again interested to take the largest possible A. Let $q = p^{2m}$, then we can consider curves with $A = \sqrt{q} - 1$. For such curves we can in fact do better than for an arbitrary family.

PROPOSITION. — *For a family of curves X over $\mathbf{F}_q$ with*

$$\frac{|X(\mathbf{F}_q)|}{g} \to \sqrt{q} - 1$$

there is an asymptotic equality

$$\frac{1}{g} \cdot \log_2 |J_X(\mathbf{F}_q)| \sim \log_2 q + (\sqrt{q} - 1) \cdot \log_2 \left(\frac{q}{q-1} \right).$$

Using this result we get

THEOREM. — *A family of curves X over $\mathbf{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbf{F}_q)|}{g} \to \sqrt{q} - 1$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbf{R}^N\}$ with

$$\lambda(\{L_N\}) \le -\log_2 \sqrt{\pi e} + \log_2 \frac{\sqrt{q+1}}{q-1} + \frac{\sqrt{q}}{\sqrt{q}-1} \cdot \log_2 q.$$

For $q = 9$ we get $\lambda \lesssim 1.8687\cdots$.

Congruence constructions

Now we shall discuss some constructions depending on a divisor.

Multiplicative congruence sublattices. — The construction of multiplicative lattices can be slightly elaborated. We consider some specific sublattices of $L_{\mathcal{P}}$.

Let D be a positive divisor on X, $D = \sum a_i P_i$, $r_i = \deg P_i$, $N(P_i) = q^{r_i}$,

$$a = \deg D = \sum a_i r_i.$$

We write $f \equiv 1 \bmod D$ if $\operatorname{ord}_{P_i}(f-1) \geq a_i$ for any $P_i \in \operatorname{Supp} D$. Suppose that $\mathcal{P} \cap \operatorname{Supp} D = \varnothing$. Let

$$O^*_{\mathcal{P},D} = \{f \in O^*_{\mathcal{P}} |\ f \equiv 1 \bmod D\},$$

and consider the lattice $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P},D}) \subseteq L_{\mathcal{P}}$.

Parameters. — Here are the estimates.

PROPOSITION. *Let $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(O^*_{\mathcal{P},D})$. Then*

(a) $d(L_{\mathcal{P},D}) \geq \sqrt{2a}$,

(b) $\operatorname{rk} L_{\mathcal{P},D} = n-1$ *and*

$$\det L_{\mathcal{P},D} \leq \sqrt{n} \cdot |J_X(\mathbf{F}_q)| \cdot \frac{q^a}{q-1} \cdot \prod \left(1 - q^{-r_i}\right).$$

Proof.

(a) As above we have

$$d(L_{\mathcal{P},D}) \geq \min_{f \in O^*_{\mathcal{P},D} - \{1\}} \sqrt{2 \cdot \deg f},$$

and we notice that $\deg f = \deg(f-1) \geq \deg D = a$.

(b) We have already estimated $\det L_{\mathcal{P}}$, and we only need to estimate $[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. Look at the embedding $O^*_{\mathcal{P}} \hookrightarrow \prod \hat{O}^*_{P_i}$ is the group of units in the completion of the local ring at P_i. Let

$$\hat{O}^*_{P_i,a_i} = \{x \in \hat{O}^*_{P_i} |\ x \equiv 1 \bmod a_i P_i\}.$$

We have $O^*_{\mathcal{P},D} = O^*_{\mathcal{P}} \cap (\prod \hat{O}^*_{P_i,a_i})$ and

$$[O^*_{\mathcal{P}} : O^*_{\mathcal{P},D}] \leq \left[\prod \hat{O}^*_{P_i} : \prod \hat{O}^*_{P_i,a_i}\right] = \prod \left[(q^{r_i}-1)^{r_i(a_i-1)}\right].$$

Then $\operatorname{Ker} \varphi_{\mathcal{P}} = \mathbf{F}^*_q$ and $0^*_{\mathcal{P},D} \cap \operatorname{Ker} \varphi_{\mathcal{P}} = \{1\}$, therefore

$$[O^*_{\mathcal{P}} : O^*_{\mathcal{P},D}] = (q-1) \cdot [L_{\mathcal{P}} : L_{\mathcal{P},D}].$$

Asymptotic behaviour. — Consider the same family of curves as above, let $\mathcal{P} = X(\mathbf{F}_q)$ and let D be such that

$$\lim \frac{\deg D}{|X(\mathbf{F}_q)|} = (2 \cdot \log_e q)^{-1}$$

(this choice appears to be optimal). We get

THEOREM. — *A family of curves X over $\mathbf{F}_q$ of growing genus g such that*

$$\frac{|X(\mathbf{F}_q)|}{g} \to \sqrt{q} - 1$$

with the appropriate choice of divisors yields an asymptotically good family of lattices $\{L_N \subset \mathbf{R}^N\}$ with

$$\lambda(\{L_N\}) \le -\log_2 \sqrt{\frac{\pi}{2}} + \frac{1}{2} \cdot \log_2(\log_e q) + \frac{\sqrt{q}}{\sqrt{q}-1} \cdot \log_2 q - \log_2(q-1).$$

For $q = 2209 = 47^2$ we get $\lambda \lesssim 1.3888\cdots$.

Number field case. — We can now return to number fields and give a parallel theory, which is as usual more difficult.

For the totally complex field $\mathbf{Q}\left(\cos\frac{2\pi}{11}, \sqrt{-46}\right)$ and $S_0 = S_\infty$ we get $\lambda \lesssim 11.1512\cdots$ For the totally real field $\mathbf{Q}(\sqrt{2}, \sqrt{3\cdot 5\cdot 7\cdot 23\cdot 29})$ and $S_0 = S_\infty$ we get $\lambda \lesssim 8.80$. These are not best choices but what we get is always much worse than for the function field case.

Another approach

Algebraic curves can also be used to construct lattices indirectly, that is we construct lattices using algebraic geometric codes. The construction is less elegant and we come to families of lattices with $\lambda \lesssim 2.30\cdots$ and families of non-lattice packings with $\lambda \lesssim 1.31\cdots$.

Bibliography

[1] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups, 2nd edition*, Springer-Verlag, New-York, 1992.

[2] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht/Boston/London, 1991.

[3] M.A. Tsfasman, *Global Fields, Codes and Sphere Packings*, in *Journées Arithmétiques de Luminy 17-21 juillet 1989*, Astérisque **198-199-200** (1991).

Institute for Information
Transmission Problems
19 Ermolovoi Street
GSP-4 Moscow 101447
Russia

e-mail: tsfasman@ippi.msk.su

et

Laboratoire de
Mathématiques Discrètes
Luminy - Case 930
13288 Marseille cedex 9
France

e-mail: tsfasman@lmd.univ-mrs.fr

Courbes algébriques

Michel Raynaud

Sur le corps des complexes $\mathbf{C}$, une surface de Riemann X est définie par un atlas de cartes à valeurs dans des ouverts de $\mathbf{C}$, avec des changements de cartes holomorphes. Lorsque X est compacte, X est algébrique, c'est à dire peut être définie par des équations polynomiales homogènes, dans un espace projectif convenable. Le passage des équations polynomiales à un atlas résulte alors du théorème des fonctions implicites. Il utilise la topologie de $\mathbf{C}$ et les fonctions analytiques. Nous allons voir comment on peut contourner cette difficulté sur un corps commutatif k quelconque.

Désormais k désigne un corps commutatif, de caractéristique $p \geq 0$. Notons d'abord que le calcul différentiel algébrique garde un sens : un polynôme à coefficients dans k, en les variables $x_1, \ldots, x_n$, admet des dérivées partielles par rapport aux x_j, de définition purement algébrique. Si A est une k-algèbre de type fini, quotient de $k[x_1, \cdots, x_n]$ par un idéal I, le A-module des k-différentielles $\Omega^1_{A/k}$ de A est le quotient du A-module libre de base les dx_j, par les relations $df = 0$, où f parcourt un système de générateurs de I. Notons que si $p > 0$ et si g est une puissance p-ème d'un élément de A, on a automatiquement $dg = 0$.

1. Courbes lisses, affines ou projectives

Carte étale. — Considérons une variété algébrique affine X, de k-algèbre $A = k[x_1, \ldots, x_n]/I$. Les points rationnels de X correspondent aux n-uples $a = (a_1, \ldots, a_n)$ dans k^n qui annulent les polynômes de I. En un tel point, l'évaluation des fonctions en a définit un morphisme de k-algèbre $A \to k$. Son noyau est donc un idéal maximal m. On obtient ainsi une bijection entre les points de X dans k^n et les idéaux maximaux m de A, tels que A/m soit k-isomorphe à k. Mais il y a lieu d'élargir la notion de point de X, en considérant tous les **idéaux maximaux** de A. Si m est un tel idéal maximal, le quotient A/m est un corps extension de k. Comme c'est aussi une k-algèbre de type fini, cette extension est automatiquement de degré fini sur k. Ainsi un point a de X correspond à un idéal maximal m_a de A et admet un corps résiduel $k(a) = A/m_a$, de degré fini sur k. Un tel point devient rationnel si on étend le corps de définition de k à $k(a)$.

Supposons que l'idéal I soit engendré par $f_1, \ldots, f_{n-1}$ et que le mineur Δ des dérivées partielles des f_j par rapport à $x_1, \ldots, x_{n-1}$ soit inversible dans A. Lorsque $k = \mathbf{C}$, le théorème des **fonctions implicites** nous dit alors que x_n est une coordonnée locale sur X, vue comme surface de Riemann. Sur un corps k général, il n'y a plus

de théorème des fonctions implicites. Notons toutefois qu'avec les hypothèses faites, dx_n est une base du A-module $\Omega^1_{A/k}$. La projection $X \to \mathcal{A}$ sur la droite affine, qui envoie $(x_1, \ldots, x_n)$ sur x_n est appelée un **morphisme étale**. Ainsi un morphisme étale correspond à un isomorphisme local sur les complexes.

Sous les hypothèses ci-dessus, nous dirons que X est **une courbe affine lisse**, de coordonnée étale x_n. Une coordonnée étale ne correspond plus en général à un morphisme injectif dans la droite affine, mais du point de vue du calcul différentiel, elle conduit au même confort qu'une carte holomorphe sur les complexes.

Courbe affine. — Une variété affine X d'anneau $A = k[x_1, \ldots, x_n]/I$ est une courbe lisse, si localement pour la topologie de Zariski, elle admet une coordonnée étale au sens précédent. De façon précise, si a est un point de X, on demande qu'il existe un polynôme g dans $k[x_1, \ldots, x_n]$, non nul en a, tel que dans le localisé $k[x_1, \ldots, x_n][g^{-1}]$, l'image de I soit engendrée par $n-1$ éléments $f_1, \ldots, f_{n-1}$ de $k[x_1, \ldots, x_n]$, avec un mineur d'ordre $n-1$ de la matrice jacobienne inversible en a.

Courbe projective. — On définit de même une courbe lisse projective, dans l'espace projectif $\mathbf{P}^n$, de coordonnées homogènes $U_0, \ldots, U_n$, en considérant cette fois un idéal I d'équations homogènes, qui localement est engendré par $n-1$ équations, dont la matrice jacobienne admet un mineur d'ordre $n-1$ inversible.

Exemple. — Considérons l'application de la droite projective $\mathbf{P}$, de coordonnées homogènes (λ, μ), dans l'espace projectif $\mathbf{P}^3$, de coordonnées homogènes (U, V, W, T), donnée par les formules :

$$U = \lambda^3, \quad V = \lambda^2\mu, \quad W = \lambda\mu^2, \quad T = \mu^3.$$

Alors, l'image est une courbe lisse définie comme l'intersection des trois quadriques :

$$UT - VW = UW - V^2 = VT - W^2 = 0.$$

Corps des fractions et anneaux locaux. — On considère désormais une courbe lisse X, affine ou projective, et on suppose qu'elle est connexe, c'est à dire qu'il n'y a pas sur X de fonction algébrique idempotente non triviale. Alors X admet un corps des fractions rationnelles $F = F(X)$ qui est une extension de type fini de k, de degré de transcendance 1. Dans le cas affine, d'anneau $A = k[x_1, \ldots, x_n]/I$, A est alors intègre et F n'est autre que le corps des fractions de A. Dans le cas projectif, de coordonnées homogènes U_j et lorsque la courbe X n'est pas contenue dans un hyperplan de coordonnées, F est engendré par les fonctions induites sur la courbe par les U_i/U_j.

Considérons, dans l'espace affine de coordonnées $x_1, \ldots, x_n$, une courbe affine X, passant par l'origine o et admettant x_n pour coordonnée étale. Si on complète $k[x_1, \ldots, x_n]$ pour la topologie définie par l'idéal maximal $(x_1, \ldots, x_n)$, on obtient l'anneau de séries formelles $k[\![x_1, \ldots, x_n]\!]$ et dans ce contexte formel, on dispose à nouveau d'un théorème des fonctions implicites : les x_i s'expriment comme séries formelles en x_n sans terme constant. En particulier le complété de l'anneau local de X en o est $k[\![x_n]\!]$, donc est un anneau de valuation discrète. Rappelons qu'un **anneau de valuation discrète** R est un anneau local principal intègre qui n'est pas un corps. Son unique idéal maximal m est alors engendré par un élément non nul et R/m est le corps résiduel. Les idéaux non nuls de R sont les puissances de m. Par exemple, l'anneau des germes de fonctions holomorphes au voisinage de 0 dans $\mathbf{C}$ est un anneau de valuation discrète. Il en est de même des localisés en les idéaux maximaux d'un anneau d'entiers de corps de nombres.

Revenons à notre courbe X passant par l'origine o. L'anneau local de X en o est un anneau de valuation discrète, puisqu'il en est ainsi de son complété. Plus généralement, en tout point z d'une courbe lisse X, l'anneau local des germes de fonctions algébriques en z est un anneau de valuation discrète $\mathcal{O}_{X,z}$, de corps des fractions $F = F(X)$, de corps résiduel $k(z)$, extension finie de k. Si X est affine d'algèbre A et si z correspond à l'idéal maximal m de A, l'anneau local $\mathcal{O}_{X,z}$ se déduit de A par localisation par les éléments de $A - m$.

Rappelons qu'un corps est **parfait** s'il est de caractéristique zéro ou bien s'il est de caractéristique $p > 0$ et si tout élément est une puissance p-ème. En particulier les corps finis et les corps algébriquement clos sont parfaits.

Lorsque le corps de base est parfait, le corps résiduel $k(z)$ au point z d'une courbe lisse X se relève canoniquement dans le complété de l'anneau local en z, qui se trouve donc être isomorphe à l'anneau de séries formelles $k(z)[\![t]\!]$.

Ainsi lorsque X est une courbe lisse affine connexe, son anneau A est un anneau noethérien intègre dont les localisés aux divers idéaux maximaux sont des anneaux de valuation discrète. Un tel anneau est un **anneau de Dedekind**. A côté des anneaux des courbes affines lisses, les anneaux de Dedekind les plus utiles sont les anneaux d'entiers d'un corps de nombres. Un tel anneau est presqu'aussi confortable qu'un annau principal : tout idéal est localement principal et tout idéal I non nul s'écrit de manière unique comme produit d'un nombre fini d'idéaux maximaux.

Soit X une k-courbe lisse connexe de corps des fractions F et soit k' la fermeture intégrale de k dans F. Alors k' est une extension finie séparable de k et X est en fait une courbe sur k'. Il y a intérêt à remplacer le corps des constantes k par k', ce qui assure que la courbe X reste connexe après toute extension de corps. On dit alors que X est **géométriquement connexe**.

Une courbe X est munie de la **topologie de Zariski** pour laquelle les ouverts non vides sont les complémentaires des ensembles finis de points. Cette toplogie n'est pas séparée mais elle assure que si $f \in F(X)$, f est définie sur un ouvert de X et l'ensemble des zéros et des pôles de f sont des fermés.

Courbes projectives et places. — Sur le corps des complexes une courbe projective, munie de la topologie héritée de celle de $\mathbf{C}$, est **compacte**. Nous allons donner une caractérisation des courbes projectives sur un corps quelconque.

Soit X une k-courbe lisse, connexe, de corps des fractions F.

DÉFINITION. — *Une k-**place** de F est un anneau de valuation discrète V contenant k, et de corps des fractions F.*

Nous avons vu qu'à tout point z de X, correspond une k-place de F : l'anneau local $\mathcal{O}_{X,z}$.

PROPOSITION. — *Si X est une courbe lisse projective, connexe, les k-places de $F(X)$ sont en bijection avec les points de X.*

Ainsi, on obtient une caractérisation des points d'une courbe projective et lisse en terme du corps des fractions $F(X)$ et du corps des constantes k. Elle est indépendante du plongement projectif. On dit qu'une courbe projective est **complète**, par opposition aux courbes affines pour lesquelles il manque un nombre fini de points qui apparaitront "à l'infini", si l'on plonge l'espace affine dans l'espace projectif.

PROPOSITION. — *Supposons le corps k **parfait**. L'application $X \mapsto F(X)$, réalise une bijection entre les courbes lisses, complètes, connexes et les corps F, extension de type fini de k, de degré de transcendance 1.*

Pour construire la courbe X à partir de F, on procède comme suit. On choisit un élément x de F transcendant sur k. Alors $[F : k(x)] = d$ est fini. Soit A_1 (*resp.* A_2) la clôture intégrale de $k[x]$ (*resp.* $k[x^{-1}]$) dans F. C'est une k-algèbre de type fini, qui est l'algèbre d'une courbe affine lisse X_1 (*resp.* X_2) (c'est ici que sert k parfait). Par recollement de X_1 et X_2 au-dessus de $k[x, x^{-1}]$, on obtient une courbe complète X, lisse, de corps des fractions F, réalisée comme revêtement (ramifié) de degré d, de la droite projective de coordonnée x.

Remarque. — Une courbe lisse complète se réalise de multiples façons comme courbe projective. Si de plus k est infini, on peut toujours la réaliser comme courbe gauche dans $\mathbf{P}^3$. Les plus accessibles de ces courbes gauches sont celles qui sont intersection complète de deux surfaces de degrés d_1 et d_2. En dehors de ce cas très exceptionnel, et de celui encore plus exceptionnel des courbes planes, les équations explicites de la courbe plongée sont difficiles à utiliser. On va plutôt s'intéresser à des propriétés intrinsèques de la courbe, indépendantes de tout plongement projectif.

2. Diviseurs et faisceaux inversibles

Soit X une courbe lisse, connexe, définie sur le corps k et de corps des fractions F. On note $\mathrm{Div}(X)$ le groupe libre commutatif, de base les points de X. Un diviseur est donc donné par une combinaison formelle $D = \sum_z n_z z$, où z parcourt les points de X et où les n_z sont des entiers presque tous nuls. Le diviseur D est dit ≥ 0 si $n_z \geq 0$, pour tout z. Si f est un élément non nul de F, on lui associe son diviseur $(f) = \sum_z v_z(f)z$, où v_z est la valuation de l'anneau local $\mathcal{O}_{X,z}$, qui vaut 1 sur un générateur de l'idéal maximal. Les diviseurs de la forme (f) sont les diviseurs principaux. Deux diviseurs sont linéairement équivalents s'ils différent par un diviseur principal.

Un faisceau inversible $\mathcal{L}$ sur X est un faisceau localement isomorphe au faisceau structural $\mathcal{O}_X$, pour la topologie de Zariski. On peut toujours recouvrir X par deux ouverts affines U et U', tels que $\mathcal{L}_{|U}$ (*resp.* $\mathcal{L}_{|U'}$) soit engendré par une base s (*resp.* s'). Alors sur $U \cap U'$, on a $s' = us$, où u est une fonction inversible. Le faisceau des 1-formes différentielles $\omega = \Omega^1_X$ est un faisceau inversible localement engendré par la différentielle dx d'une coordonnée étale; on l'appelle le **faisceau canonique**.

A tout diviseur D, on associe classiquement un faisceau inversible noté $\mathcal{O}_X(D)$ qui est un sous-faisceau du faisceau constant $\underline{F}$ des fonctions rationnelles sur X. Pour tout ouvert U de X, les sections de $\mathcal{O}_X(D)$ sur U, sont les fonctions rationnelles f sur U, telle que $[(f) + D]_{|U} \geq 0$. Pour U assez petit, un générateur de $\mathcal{O}_X(D)_{|U}$ est une fonction f de F telle que $[(f) + D]_{|U} = 0$. En particulier, les sections globales de $\mathcal{O}_X(D)$ sont les fonctions rationnelles f telles que $(f) + D \geq 0$.

Réciproquement, si on part d'un faisceau inversible $\mathcal{L}$ sur X, le faisceau $\mathcal{L} \otimes_{\mathcal{O}_X} \underline{F}$ est isomorphe à $\underline{F}$. Le choix d'une section non nulle de $\mathcal{L} \otimes_{\mathcal{O}_X} \underline{F}$ permet d'identifier $\mathcal{L}$ à un sous-faisceau de $\underline{F}$, de la forme $\mathcal{O}_X(D)$, pour un diviseur D convenable. Changer de section, revient à remplacer D par un diviseur linéairement équivalent. On obtient ainsi un dictionnaire entre classes d'isomorphismes de faisceaux inversibles et classes de diviseurs.

Supposons de plus la courbe X **complète**. On définit alors le degré d'un diviseur $D = \sum_z n_z z$, par la formule : degré $(D) = \sum_z n_z [k(z) : k]$, où $[k(z) : k]$ désigne le degré sur k de l'extension résiduelle $k(z)$. Alors tout diviseur principal (f) est de degré 0 (i.e. le degré du diviseur des zéros est égal à celui des pôles). En particulier, on peut parler du degré d'une classe de diviseurs, et si $\mathcal{L}$ est un faisceau inversible, isomorphe à $\mathcal{O}_X(D)$, on définit le degré de $\mathcal{L}$ comme étant celui de D. Toujours dans le cas où X est complète, le k-espace vectoriel $H^0(X, \mathcal{L})$, des sections globales de $\mathcal{L}$, est de dimension finie. Chaque section non nulle s de $\mathcal{L} \approx \mathcal{O}_X(D)$ admet un ensemble de zéros qui est un diviseur $\Delta \geq 0$, linéairement équivalent à D. Si X est géométriquement connexe, les seuls éléments non nuls de F, de diviseur nul, sont les éléments non nuls de k. On obtient ainsi une bijection entre l'espace projectif des

droites du k-vectoriel $H^0(X,\mathcal{L})$, où $\mathcal{L}=\mathcal{O}_X(D)$, et l'ensemble des diviseurs $\Delta\geq 0$, linéairement équivalents à D. En particulier, si $\mathcal{L}$ est degré $<0, H^0(X,\mathcal{L})=0$.

3. Le genre

Sur les complexes, une surface de Riemann X compacte connexe a un genre g, défini par sa topologie : comme espace topologique X est un tore à g trous. Mais g est aussi la dimension sur $\mathbf{C}$ de l'espace des formes différentielles holomorphes sur X. C'est cette dernière définition qui va pouvoir s'adapter au cas d'un corps quelconque.

DÉFINITION. — *Soit X une k-courbe lisse complète géométriquement connexe. Le genre g de X est la dimension sur k du k-espace vectoriel $H^0(X,\omega)$, espace des formes différentielles algébriques sur X.*

Remarque. — On peut aussi déterminer le genre g de X, à partir du degré de ω qui est $2g-2$.

Exemple. — Rappelons que sur l'espace projectif $Q=\mathbf{P}^n$ et pour tout entier m, on note $\mathcal{O}_Q(m)$ le faisceau inversible des "fonctions" homogènes de degré m. Si X est une courbe plane, lisse de degré d, dans le plan projectif $Q=\mathbf{P}^2$, le faisceau ω_X est isomorphe à $\mathcal{O}_Q(d-3)_{|X}$ et le genre de X est $(d-1)(d-2)/2$.

Soit $\pi : Y\to X$ un morphisme fini de degré d entre courbes lisses, complètes géométriquement connexes. Supposons que le corps des fractions $F(Y)$ de Y soit une extension séparable de $F(X)$. Alors ω_Y contient $\pi^*(\omega_X)$, l'image réciproque par π du faisceau ω_X, de sorte qu'il existe un faisceau d'idéaux $\mathcal{V}_{Y/X}$ sur Y, tel que $\omega_Y=\pi^*(\omega_X)[\mathcal{V}_{Y/X}]^{-1}$. Le faisceau $\mathcal{V}_{Y/X}$ est la **différente** de Y par rapport à X et correspond à un diviseur ≥ 0 sur Y : $\sum_y n_y y$, avec $n_y\geq 0$. De plus, $n_y>0$ si et seulement si π est ramifié en y. En comparant les degrés on trouve la **formule de Hurwitz** :

$$2\text{genre}(Y)-2=d\,[2\text{genre}(X)-2]+\deg\mathcal{V}_{Y/X}.$$

L'avantage de cette formule est que le calcul du degré de la différente se ramène à un calcul local en chacun des points de ramification de π : si y est un point de Y au-dessus du point x de X et si t (*resp.* τ) sont des coordonnées étales centrées en x (*resp.* y), on a $dt=u\tau^{n_y}d\tau$, où u est une unité en y.

- En un point y de Y où l'indice de ramification e_y de π est d'ordre premier à p (on dit alors que la ramification est modérée), l'exposant n_y de y dans la différente est e_y-1, comme dans le cas complexe.

- Par contre, en un point y où l'indice de ramification géométrique est multiple de p (on dit qu'il y a ramification sauvage), l'exposant n_y de y peut être arbritrairement élévé, indépendamment du degré d.

Exemple. — Plaçons nous en caractéristique $p > 0$. Considérons la droite affine de coordonnée x et le revêtement galoisien de groupe $\mathbf{Z}/p\mathbf{Z}$, d'équation :

$$U^p - U = H(x),$$

où $H(x)$ est un polynôme en x, de degré $m > 0$ premier à p. Ce revêtement de la droite affine est non ramifié et s'étend en un revêtement Y de la droite projective $\mathbf{P}$, totalement ramifié au-dessus de l'infini. Notons ∞' l'unique point de Y au-dessus du point ∞ de $\mathbf{P}$ et calculons l'exposant de ∞' dans la différente $\mathcal{V}_{Y/\mathbf{P}}$.

Soit τ une coordonnée étale centrée en ∞' et $t = 1/x$ la coordonnée sur $\mathbf{P}$ centrée en ∞. La fonction rationnelle U admet en ∞' un pôle d'ordre m et donc, puisque $(m, p) = 1$, dU admet en ∞' un pôle d'ordre $m + 1$. D'où, à des unités locales près, : $d\tau/\tau^{m+1} \approx dU = -dH \approx dt/t^{m+1}$. Donc $dt \approx (t/\tau)^{m+1} d\tau$. L'exposant dans la différente au point ∞' est donc $(p-1)(m+1)$, et par suite le genre de Y est $g = (m-1)(p-1)/2$.

4. Courbes de petit genre

Soit X une courbe complète lisse sur k, géométriquement connexe, de genre g.

— Si $g = 0$, X est canoniquement une **conique** dans le plan projectif. Si de plus elle possède un point rationnel, (en particulier si k est fini), X est isomorphe à la droite projective. Par contre sur $\mathbf{R}$, la conique "imaginaire" d'équation $U^2 + V^2 + W^2 = 0$, n'a pas de points rationnels. Sur un corps algébriquement clos de caractéristique 2, une conique projective lisse admet pour équation $UV + W^2 = 0$. Le fait que la dérivée par rapport à W soit nulle, entraîne que toutes les tangentes à la conique passent par le point $(0, 0, 1)$.

— Lorsque $g = 1$, X est une courbe **elliptique**. Si X possède un point rationnel (ce qui est le cas en particulier si k est fini), X se réalise comme cubique dans le plan projectif. En coordonnées homogènes U, V, W, l'équation de la cubique peut être mise sous le forme :

$$V^2W + a_1UVW + a_3VW^2 = U^3 + a_2U^2W + a_4UW^2 + a_6W^3,$$

avec un discriminant $\Delta \neq 0$.

Lorsque la caractéristique p est différente de 2 et 3, on se ramène, par translations, à la forme de Weierstrass habituelle :

$$V^2W = U^3 + a_4UW^2 + a_6W^3,$$

avec $\Delta = -(4a_4^3 + 27a_6^2)$.

— Lorsque $g = 2$, X ne se réalise pas comme courbe plane ou comme courbe gauche intersection complète. Par contre, X est hyperelliptique, c'est-à-dire est canoniquement un revêtement séparable de degré 2 de la droite projective $\mathbf{P}$.

Pour $p \neq 2$, ce revêtement est ramifié en 6 points géométriques et X est la complétion projective d'une courbe affine d'équation $y^2 = P_6(x)$, où P_6 est un polynôme de degré 6, sans racines multiples. Si l'un des points de ramification est rationnel et choisi à l'infini, X est la complétion d'une courbe affine d'équation $y^2 = H(x)$, où H est polynôme unitaire en x de degré 5, sans racines multiples.

Si $p = 2$, le revêtement de la droite projective peut être ramifié en 3, 2, ou 1 point géométrique et X est la complétion projective d'une courbe affine d'équation du type : $y^2 + P_3(x)y + P_6(x) = 0$, où P_i est un polynôme de degré $\leq i$. Par exemple, l'équation $y^2 - y = x^5$, conduit à une courbe de genre 2, ramifiée uniquement au-dessus de $x = \infty$.

— Une courbe de genre 3, se réalise canoniquement comme quartique dans le plan projectif, sauf si elle est hyperelliptique. Parmi les quartiques, on trouve celle de Klein d'équation : $U^3V + V^3W + W^3U = 0$. Sur les complexes, cette courbe admet un groupe G d'automorphismes qui est le deuxième groupe fini simple : $G \approx PSL(\mathbf{F}_7)$ à 168 éléments. En caractéristique 3, le groupe d'automorphismes gonfle jusqu'à devenir le groupe projectif $PU(3,3)$ à 6048 éléments.

5. Formule de Riemann-Roch et dualité

Soit toujours X une k-courbe lisse, complète, géométriquement connexe de genre g.

Si $\mathcal{F}$ est un faisceau en groupes commutatifs sur X pour la topologie de Zariski, on dispose de ses groupes de cohomologie $H^i(X, \mathcal{F})$, qui sont nuls pour $i \neq 0, 1$. Si $\mathcal{F}$ est un faisceau inversible $\mathcal{L}$, les groupes $H^i(X, \mathcal{L})$ sont des k-vectoriels de dimension finie. On note $H^i(\mathcal{L})$ la dimension sur k de $H^i(X, \mathcal{L})$. Si $\mathcal{L}$ est un faisceau inversible, $\mathcal{L}^*$ désigne le faisceau inversible dual. Lorsque $\mathcal{L} = \mathcal{O}_X(D)$, $\mathcal{L}^* = \mathcal{O}_X(-D)$.

La compréhension de la cohomologie des faisceaux inversibles est régie par celle du faisceau dualisant ω.

THÉORÈME.

1. *$H^1(X, \omega)$ est canoniquement isomorphe au corps k.*
2. *Pour tout faisceau inversible $\mathcal{L}$ sur X, et tout entier i, l'accouplement*

$$H^i(X, \mathcal{L}) \times H^{1-i}(X, \omega \otimes \mathcal{L}^*) \to H^1(X, \omega) = k,$$

donné par le cup-produit, est une dualité parfaite.

Rappelons que pour calculer la cohomologie d'un faisceau $\mathcal{F}$ sur X, on considère une résolution de $\mathcal{F}$:

$$0 \to \mathcal{F} \to \mathcal{F}^1 \to \mathcal{F}^2 \to \cdots,$$

où les $\mathcal{F}^i$ sont acycliques, c'est-à-dire ont des groupes de cohomologie $H^i(X, \mathcal{F}^i)$ nuls pour $j > 0$. Le groupe $H^j(X, \mathcal{F})$ est alors le j-ème groupe de cohomologie du complexe :

$$H^0(X, \mathcal{F}^1) \to H^0(X, \mathcal{F}^2) \to \cdots$$

Parmi les faisceaux acycliques, on trouve les faisceaux flasques $\mathcal{G}$, c'est-à-dire ceux pour lesquels, pour tout couple d'ouverts U, V avec $V \supset U$, toute section de $\mathcal{G}$ sur U s'étend en une section de $\mathcal{G}$ sur V.

Pour calculer $H^1(X, \omega)$, on dispose d'une résolution acyclique naturelle de ω. En effet, ω se plonge dans le faisceau constant $\omega \otimes_{\mathcal{O}_X} \underline{F}$ des formes différentielles rationnelles. Le conoyau est le faisceau M des parties polaires de différentielles. On obtient ainsi une résolution flasque canonique de ω, qui permet de calculer la cohomologie. En particulier, on a :

$$H^1(X, \omega) = \operatorname{coker}[H^0(X, \omega \otimes_{\mathcal{O}_X} \underline{F}) \to H^0(X, M)].$$

Notons qu'en chaque point x de X, une section μ de M admet un **résidu** $\operatorname{Res}_X(\mu)$ qui est un élément du corps résiduel $k(x)$. Si x est un point rationnel et si t est une coordonnée étale centrée en x, μ s'écrit $(\sum_{-1}^{-n} a_i t^i)dt$ et le résidu est le coefficient a_{-1}. On doit bien sûr vérifier qu'il est indépendant du choix de t. Si μ est une section de M, on peut, grâce à l'opération de trace, définir la "somme" des résidus $\sum_x \operatorname{Tr}_{k(x)/k} \operatorname{Res}_x(\mu)$, qui est un élément de k. L'assertion (1) du théorème équivaut alors à la conjonction des deux propriétés suivantes :

1. Pour toute forme différentielle rationnelle τ, on a $\sum_x \operatorname{Tr}_{k(x)/k} \operatorname{Res}_x(\tau) = 0$.
2. Toute section μ de M, telle $\sum_x \operatorname{Tr}_{k(x)/k} \operatorname{Res}_x(\mu) = 0$, est la partie polaire d'une différentielle rationnelle τ sur X.

On trouvera dans [3] une démonstration accessible du théorème ci-dessus, du moins lorsque le corps k est algébriquement clos.

COROLLAIRE. — *On a* $g = h^1(\mathcal{O}_X)$.

Pour tout faisceau inversible $\mathcal{L}$ sur X, on définit la caractéristique d'Euler-Poincaré de $\mathcal{L}$, par $\chi(\mathcal{L}) = h^0(\mathcal{L}) - h^1(\mathcal{L})$.

On connait $\chi(\omega) = g - 1$. On en déduit facilement le corollaire suivant :

COROLLAIRE. — *Pour tout faisceau inversible* $\mathcal{L}$ *sur* X, *on a :*

$$\chi(\mathcal{L}) = 1 - g + \text{degré}(\mathcal{L}).$$

Ainsi la caractéristique d'Euler-Poincaré se calcule au moyen d'invariants numériques, par contre les dimensions des espaces de cohomologie $h^i(\mathcal{L})$ peuvent être plus difficiles à déterminer.

En combinant avec la formule de dualité on obtient :

COROLLAIRE (théorème de Riemann-Roch). — *Pour tout faisceau inversible* $\mathcal{L}$ *sur* X, *on a*

$$h^0(\mathcal{L}) - h^0(\omega \otimes (\mathcal{L}^*)) = 1 - g + \text{degré}(\mathcal{L}).$$

Cet énoncé a l'avantage de ne plus faire intervenir que des espaces de cohomologie en degré zéro. Si l'on choisit un diviseur K dans la classe canonique, il se reformule :

$$h^0(\mathcal{O}_X(D)) - h^0(\mathcal{O}_X(K - D)) = 1 - g + \text{degré}(D).$$

COROLLAIRE. — *Pour* $\text{degré}(\mathcal{L}) < 0$, *on a* $h^0(\mathcal{L}) = 0$. *Pour* $\text{degré}(\mathcal{L}) > 2g-2$, *on a* $h^1(\mathcal{L}) = 0$ *et* $h^0(\mathcal{L}) = 1 - g + \text{degré}(\mathcal{L})$.

Remarque. — Sur la droite projective, le théorème de décomposition des fractions rationnelles en éléments simples, nous dit qu'étant donnée une partie polaire arbitraire, on peut trouver une fonction rationnelle globale, définie à l'addition près d'une constante, qui admet précisément la donnée comme partie polaire. Il n'en va plus de même en genre $g > 0$. Ainsi le corollaire précédent nous dit que si on se donne un diviseur positif D de degré $> 2g - 2$, $h^0(\mathcal{O}_X(D))$ a pour dimension seulement $1 - g + \text{degré}(D)$, qui est strictement plus petit que $1 + \text{degré}(D)$ pour $g > 0$.

6. Courbes sur les corps finis

Désormais k désigne un corps fini $\mathbf{F}_q$, à q éléments. On choisit une clôture algébrique $\bar{k}$ de k. Pour tout entier $m \geq 1$, k_m désigne l'extension de degré m de k contenue dans $\bar{k}$. On note $X \otimes_k k_m$ la courbe déduite de X par extension du corps de base k à k_m et $\bar{X}$ la courbe $X \otimes_k \bar{k}$. Pour tout entier $m > 0$, $X(k_m)$ est l'ensemble fini des points rationnels de $X \otimes_k k_m$.

On note :

A_m le nombre de diviseurs ≥ 0 sur X, de degré m,

M_m le nombre de points de X de corps résiduel k_m,

N_m le nombre de points rationnels de $X \otimes_k k_m$.

Rappelons que pour s complexe avec $\text{Re}(s) > 1$, on définit la fonction zêta de Riemann par la formule :

$$\zeta(s) = \sum \frac{1}{n^s} = \prod \frac{1}{(1 - 1/p^s)},$$

où p parcourt l'ensemble des nombres premiers, c'est à dire encore le spectre maximal de $\mathbf{Z}$. Cette expression admet un analogue pour la courbe X, qui est la fonction zêta de la courbe X :

$$\zeta_X(s) = \prod_X \frac{1}{(1 - 1/(\#k(x))^s)},$$

où $\#k(x)$ désigne le cardinal du corps résiduel $k(x)$. Or, en un point x où $[k(x) : k] = m$, on a $\#k(x) = q^m$. Par suite, si on pose $T = 1/q^s$ et

$$(*) \qquad Z_X(T) = \prod_{x \in X} \frac{1}{(1 - T^{\deg(x)})},$$

On a $\zeta_X(s) = Z_X(q^{-s})$.

PROPOSITION. — *Les trois séries formelles suivantes sont égales, et coïncident avec $Z_X(T)$:*

(a) $\sum_0^\infty A_m T^m$,

(b) $\prod_1^\infty (1 - T^m)^{-M_m}$,

(c) $\exp(\sum_1^\infty N_m T^m/m)$.

L'expression (b) résulte de $(*)$ en regroupant les termes qui correspondent à un degré m donné.

L'égalité de (a) et (b) provient du fait que tout diviseur positif s'écrit de manière unique comme somme de points de X à coefficients entiers ≥ 0.

L'égalité de (b) et (c), résulte, en prenant les dérivées logarithmiques, de la relation $N_m = \sum_{d|m} dM_d$.

COROLLAIRE. — *On a $TZ'_X/Z_X = \sum_1^\infty N_m T^m$.*

Faisons l'observation suivante. Supposons avoir écrit Z_X sous la forme P/Q, où P et Q sont des polynômes en T de terme constant 1. Ecrivons dans $\mathbf{C}[T]$:

$$P = \prod_i (1 - \alpha_i T), \quad Q = \prod_j (1 - \beta_j T).$$

Alors

$$TZ'_X/Z_X = -\sum_i \alpha_i T/(1 - \alpha_i T) + \sum_j \beta_j T/(1 - \beta_j T).$$

Par suite on a :

$$N_m = \sum_j \beta_j^m - \sum_i \alpha_i^m.$$

THÉORÈME (André Weil).

1. *Il existe un polynôme de $\mathbf{Z}[T]$ de degré $2g$: $P_1 = 1 + \cdots + q^g T^{2g}$, tel que $Z_X(T) = P_1(T)/(1-T)(1-qT)$, en particulier Z_X est une fraction rationnelle en T.*
2. *On a $P_1(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$, où les α_i sont des entiers algébriques, qui, dans tout plongement dans $\mathbf{C}$ ont pour module $\sqrt{q}$. De plus l'application $\alpha \mapsto q/\alpha$ induit une permutation des α_i.*

Notons que toutes les propriétés ci-dessus, à l'exception du module des α_i, se déduisent formellement du théorème de Riemann-Roch. Quant au fait que les α_i

aient pour module $\sqrt{q}$, il équivaut au fait que les zéros de la fonction $\zeta_X(s)$ ont pour partie réelle $1/2$, un analogue de l'hypothèse de Riemann.

COROLLAIRE. — *Pour tout entier $m > 0$ on a $N_m = 1 + q^m - \sum_{i=1}^{2g} \alpha_i^m$. En particulier,*

$$|N_m - (1 + q^m)| \leq 2gq^{m/2}.$$

COROLLAIRE. — *Le nombre h de classes de diviseurs de degré 0 sur X est fini, égal $P_1(1)$.*

Cela résulte du fait que pour un degré $m > 2g - 2$, chaque classe de diviseurs compte $(q^{m+1-g} - 1)/(q - 1)$ éléments, et par suite $A_m = h(q^{m+1-g} - 1)/(q - 1)$.

Remarques.

(1) On note que $1 + q^m$ est le nombre de points rationnels de la droite projective sur k_m. En particulier, quand m tend vers l'infini, N_m est équivalent à $1 + q^m$.

(2) On retrouve que pour $g = 0$ ou 1, X a toujours un point rationnel. Sur le corps $k = \mathbf{F}_4$, la courbe elliptique d'équation $y^2 - y = x^3 + j$, où j est une racine primitive troisième de l'unité, a pour seul point rationnel le point à l'infini, et la borne inférieure de Weil est atteinte.

(3) Considérons sur le corps $\mathbf{F}_3$, la courbe de genre 2 d'équation : $y^2 = P_6(x)$, avec $P_6 = x^6 + x^4 + x^2 + 1$. Elle admet le maximum de points rationnels possible pour une courbe hyperelliptique, à savoir 8. Par contre la courbe $y^2 = -P_6(x)$ n'a pas de points rationnels. C'est aussi le cas de la courbe $U^{p-1} + V^{p-1} + W^{p-1} = 0$ sur le corps à p éléments pour $p \geq 5$.

COROLLAIRE. — *Pour connaître $Z_X(T)$, et donc tous les N_m, il suffit de connaître les g premiers. En particulier, pour connaître la fonction zêta d'une courbe elliptique, il suffit de connaître N_1.*

La démonstration de Weil [4] utilise les propriétés d'intersection du morphisme de Frobenius sur la jacobienne de X. On trouvera dans [2] une démonstration liée à la théorie des intersections sur les surfaces. Une démonstration élémentaire, à partir de Riemann-Roch a été donnée ultérieurement par Stépanov [1].

La justification la plus conceptuelle de l'expression de la fonction zêta vaut en fait pour une variété algébrique lisse projective quelconque et a été pressentie par Weil, lorsqu'il a formulé ses célèbres conjectures sur les corps finis.

On commence par définir l'endomorphisme de Frobenius Φ sur X, qui consiste à élever les fonctions à la puissance q. Soit $\bar{\Phi}$ l'extension de Φ à $\bar{X}$. Alors les N_m points rationnels de X dans k_m sont les N_m points fixes de $\bar{\Phi}^m$.

Si l'on était sur les complexes, on pourrait utiliser la cohomologie transcendante $H^i(X_{\text{top}}, \mathbf{Q})$ et la formule de Lefschetz, qui exprime le nombre de points fixes d'un endomorphisme, et plus généralement d'une correspondance, comme somme alternée de ses traces sur la cohomologie. Weil a suggéré qu'il devait exister une cohomologie de $\bar{X}$ à valeur dans un corps (?) de caractéristique zéro, qui conduise à une formule des traces de Lefschetz :

$$N_m = \sum (-1)^i \mathrm{Tr}(\bar{\Phi}^m, H^i(\bar{X}, ?)).$$

Dans les années 60, Grothendieck a défini la cohomologie en question, puis Grothendieck et Deligne ont démontré les conjectures de Weil en toute dimension.

Choisissons un nombre premier ℓ, distinct de la caractéristique p. A l'aide de la **topologie étale**, on définit pour chaque entier $n > 0$, les groupes de cohomologie $H^i(\bar{X}, \mathbf{Z}/\ell^n\mathbf{Z})$ qui sont des $\mathbf{Z}/\ell^n\mathbf{Z}$-modules de type fini. Pour n variable, ces cohomologies forment un système projectif, et par définition, on pose :

$$H^i(\bar{X}, \mathbf{Z}_\ell) = \varprojlim_n H^i(\bar{X}, \mathbf{Z}/\ell^n\mathbf{Z})$$

qui est un $\mathbf{Z}$-module de type fini, et $H^i(\bar{X}, \mathbf{Q}_\ell) = H^i(\bar{X}, \mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, qui est un $\mathbf{Q}_\ell$-espace vectoriel.

Lorsque $k = \mathbf{C}$, les espaces de cohomologie $H^i(\bar{X}, \mathbf{Q}_\ell)$ sont canoniquement isomorphes aux espaces de cohomologie $H^i(X_{\text{top}}, \mathbf{Q}_\ell)$ associés à la variété topologique X_{top} sous-jacente à X.

Pour une courbe propre et lisse, de genre g, sur un corps k algébriquement clos, $H^0(X, \mathbf{Q}_\ell) = \mathbf{Q}_\ell$, $H^1(X, \mathbf{Q}_\ell)$ est de dimension $2g$, $H^2(X, \mathbf{Q}_\ell)$ est de dimension 1.

Pour une variété algébrique propre et lisse, de dimension d, sur un corps k fini, le Frobenius $\bar{\Phi}$ agit par fonctorialité sur les espaces $H^i(\bar{X}, \mathbf{Q}_\ell)$, et

$$P_i(T) = \det(1 - T\bar{\Phi} | H^i(\bar{X}, \mathbf{Q}_\ell))$$

est un polynôme à coefficients entiers, indépendant de ℓ, qui dans $\mathbf{C}[T]$, s'écrit $\prod(1 - \alpha_j T)$, où les α_j sont des nombres complexes de module $q^{i/2}$. L'expression de la fonction zêta de X, par rapport à la variable $T = q^{-s}$, est alors :

$$Z_X(T) = \frac{P_1(T) \cdots P_{2d-1}(T)}{P_0(T) \cdots P_{2d}(T)}.$$

Bibliographie

[1] E. Bombieri, *Counting points on curves over finite fields (d'après S.A. Stepanov)*, in *Séminaire Bourbaki*, Springer Lecture Notes in Math. **383** (1972).

[2] P. Monsky, *p-Adic analysis and zeta functions*, Lectures in mathematics, dept. of mathematics, Kyoto University, Kinokuniya Book-Store, Tokyo, 1970.

[3] J.-P. Serre, *groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[4] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

Département de Mathématiques
Université de Paris XI
91405 Orsay Cedex
France

Nombre de points d'une variété algébrique sur un corps fini

Christian Houzel

En 1949, A. Weil a associé à toute variété algébrique sur un corps fini k une *fonction zêta* liée au nombre de points de la variété dans les diverses extensions finies de k et il a formulé des conjectures célèbres au sujet de cette fonction. Les conjectures de Weil ont été un des principaux stimulants pour le développement de la géométrie algébrique abstraite, en particulier dans l'œuvre d'A. Grothendieck ; elles ont été finalement démontrées par P. Deligne en 1973 en utilisant les outils élaborés par Grothendieck.

Dans cet exposé, nous allons essayer d'expliquer l'histoire qui précède la formulation des conjectures de Weil et de montrer comment on a pu arriver à les concevoir.

La fonction zêta classique, celle de Riemann, donne des informations sur la distribution des *nombres premiers* dans l'anneau $\mathbf{Z}$ des entiers. Sa définition a été étendue par Dedekind au cas d'un *corps de nombres algébriques* K (extension finie de $\mathbf{Q}$) ; la fonction zêta de Dedekind est liée à la distribution des *idéaux premiers* dans l'anneau des entiers de K et elle informe aussi sur le nombre des classes d'idéaux de K.

1. E. Artin

Dans sa thèse (1921, publiée en 1924), E. Artin a développé, sur le modèle de la théorie des corps quadratiques, une théorie arithmétique des extensions quadratiques $\Omega = K(\sqrt{D})$ du corps des fractions rationnelles $K = \mathbf{F}_p(t)$ à coefficients dans un corps fini $\mathbf{F}_p$ (p nombre premier impair) ; une telle extension est engendrée par la racine carrée d'un polynôme D (sans facteur carré) à coefficients dans $\mathbf{F}_p$. Artin y définit l'anneau des entiers, les idéaux de cet anneau, qui se décomposent d'une manière unique en produits d'idéaux *premiers* et se partagent en un nombre fini de *classes modulo* les idéaux principaux ; le nombre h de ces classes est 1 si D est de degré 0 ou 1 et 2 si D est de degré 2. En vue d'évaluer h dans les autres cas, Artin associe une fonction zêta au corps Ω sur le modèle de celle de Dedekind en théorie des nombres :

$$Z(s) = Z_D(s) = \sum_{\mathfrak{a}} \frac{1}{|N\mathfrak{a}|^s};$$

dans cette formule $\mathfrak{a}$ parcourt l'ensemble des idéaux non nuls, $N\mathfrak{a}$ est la *norme* de l'idéal $\mathfrak{a}$, c'est à dire le polynôme unitaire qui engendre le produit $\mathfrak{a}\mathfrak{a}'$ de $\mathfrak{a}$ par son

conjugué $\mathfrak{a}'$ (obtenu par l'automorphisme de Ω qui change $\sqrt{D}$ en $-\sqrt{D}$; le produit est automatiquement un idéal principal) et, pour chaque polynôme $F \in \mathbf{F}_p[t]$ de degré n on pose $|F| = p^n$ (on notera que $|N\mathfrak{a}|$ est le nombre d'éléments de l'anneau résiduel mod $\mathfrak{a}$). La variable s est complexe et la série converge pour $\mathrm{Re}(s) > 1$; comme dans le cas des corps de nombres, on peut écrire $\boldsymbol{Z}(s)$ sous forme d'un produit étendu à tous les *idéaux premiers* :

$$\boldsymbol{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |N\mathfrak{p}|^{-s}}.$$

Artin regroupe dans ce produit les $\mathfrak{p}$ qui divisent un même polynôme irréductible $P \in \mathbf{F}_p[t]$, puis en transformant à nouveau le produit en série il trouve

$$\boldsymbol{Z}(s) = \frac{1}{1 - p^{-(s-1)}} \sum_F \left[\frac{D}{F}\right] \frac{1}{|F|^s}$$

où F parcourt l'ensemble des polynômes unitaires à coefficients dans $\mathbf{F}_p$ et où $\left[\dfrac{D}{F}\right] = \pm 1$ est un symbole analogue à celui de Jacobi en théorie des nombres. Ce symbole fait l'objet d'une *loi de réciprocité*, établie par Artin, qui permet de montrer que la somme

$$\sigma_\nu = \sum_{|F| = p^\nu} \left[\frac{D}{F}\right]$$

est nulle pour $\nu \geq n = \deg D$ lorsque $n \geq 1$; ainsi, pour D non constant,

$$\boldsymbol{Z}_D(s) = \frac{1}{1 - p^{-(s-1)}} \sum_{\nu=0}^{n-1} \frac{\sigma_\nu}{p^{\nu s}}.$$

Lorsque D est constant, on peut supposer que c'est une racine primitive g mod p et on trouve que

$$\boldsymbol{Z}_g(s) = \frac{1}{1 - p^{-(s-1)}} \cdot \frac{1}{1 + p^{-(s-1)}};$$

dans tous les cas $\boldsymbol{Z}(s)$ est rationnelle en p^{-s}.

Pour relier la fonction zêta au nombre h des classes d'idéaux, Artin étudie, pour chaque classe d'idéaux $\boldsymbol{K}$ la somme partielle $\boldsymbol{Z}(s, \boldsymbol{K})$ de la série obtenue en prenant $\mathfrak{a} \in \boldsymbol{K}$. Dans le "cas imaginaire" (D de degré impair ou bien de degré pair avec un coefficient dominant non carré dans $\mathbf{F}_p$), ils trouve que $\boldsymbol{Z}(0, \boldsymbol{K}) = 1/w$ indépendamment de la classe $\boldsymbol{K}$, où w est le nombre des *unités* de Ω (éléments inversibles de l'anneau des entiers) ; ainsi

$$h = \begin{cases} -w\boldsymbol{Z}(0) = 1 & \text{si } D = g, \\ \\ \sigma_0 + \sigma_1 + \cdots + \sigma_{n-1} & \text{si } \deg D = n \geq 1. \end{cases}$$

Le cas "réel" (D de degré pair avec un coefficient dominant carré) est un peu plus compliqué : on a $\sigma_0+\sigma_1+\cdots+\sigma_{n-1}=0$ comme conséquence de la loi de réciprocité et on n'atteint pas h en considérant $\boldsymbol{Z}$ en 0 ; mais on a, indépendamment de $\boldsymbol{K}$,

$$\lim_{s\to 1}(s-1)\boldsymbol{Z}(s,\boldsymbol{K})=\frac{(p-1)R}{|\sqrt{D}|\log p}$$

où le nombre R est défini de manière que $|\varepsilon_0|=p^R$, ε_0 étant une "unité fondamentale" de Ω. Ainsi

$$h=\frac{|\sqrt{D}|}{(p-1)R}\sum_{\nu-0}^{n-1}\frac{\sigma_\nu}{p^\nu}$$

et le résidu de $\boldsymbol{Z}(s)$ en son pôle $s=1$ est $\dfrac{h}{\kappa\log p}$ où $\kappa=\dfrac{|\sqrt{D}|}{(p-1)R}$. On trouve une forme analogue pour ce résidu dans le cas imaginaire grâce à l'*équation fonctionnelle* de la fonction zêta, qui se démontre sur les fonctions partielles $\boldsymbol{Z}(s,\boldsymbol{K})$:

$$\boldsymbol{Z}(1-s)=\begin{cases}\dfrac{1-p^{-(s-1)}}{1-p^s}\left(\sqrt{\dfrac{|D|}{p}}\right)^{2s-1}\cdot\boldsymbol{Z}(s) & \text{pour } n \text{ impair}\\[2ex] \dfrac{1-p^{-(s-1)}}{1-p^{2s}}\left(\sqrt{|D|}\right)^{2s-1}\cdot\boldsymbol{Z}(s) & \text{pour } n \text{ pair}\end{cases}$$

et D de coefficient dominant g ; les valeurs κ correspondantes sont respectivement $\sqrt{\frac{|D|}{p}}$ et $\frac{2\sqrt{|D|}}{p+1}$. Il y a aussi une équation fonctionnelle dans le cas réel ; Artin l'obtient à partir des précédentes grâce à l'identité facile

$$(*)\qquad \boldsymbol{Z}_D(s+\frac{\pi i}{\log p})=\frac{1-p^{-(s-1)}}{1+p^{-(s-1)}}\cdot\boldsymbol{Z}_{gD}(s)$$

et elle s'écrit

$$\boldsymbol{Z}(1-s)=\left(\frac{1-p^{-(s-1)}}{1+p^s}\right)^2\left(\sqrt{|D|}\right)^{2s-1}\boldsymbol{Z}(s).$$

L'équation fonctionnelle se traduit par des relations entre les coefficients σ_ν :

$$\sigma_{2m-\nu}=p^{m-\nu}\sigma_\nu \qquad \text{si } \deg D=2m+1 \text{ est impair}$$

et

$$\sigma_{2m-\nu}\pm p\sigma_{m\nu-1}=p^{m-\nu}(\sigma_\nu\pm p\sigma_{\nu-1}) \quad \text{si } \deg D=2m \text{ est pair}$$

($\pm=+$ dans le cas imaginaire et $-$ dans le cas réel). A l'aide de ces relations, le calcul des σ_ν et de h devient facile pour les petites valeurs de p et de m et Artin donne des tables de ces nombres pour $\deg D=3, p=3,5$ et 7 et pour $\deg D=4, p=3$.

Par ailleurs $(*)$ montre que $\boldsymbol{Z}_D(1+\frac{\pi i}{\log p})$ n'est pas nul puisque le résidu de $\boldsymbol{Z}_{gD}$ en $s=1$ n'est pas nul ; comme $\boldsymbol{Z}$ est une fonction périodique de s (de période $\frac{2\pi i}{\log p}$), elle ne s'annule en aucun des points $1+\frac{(2n+1)\pi i}{\log p}$ et Artin en déduit qu'elle ne s'annule pas sur la droite $\mathrm{Re}(s)=1$.

Dans les cas correspondant à ses tables numériques, Artin va plus loin en établissant l'analogue de l'*hypothèse de Riemann*; les zéros (non triviaux) de $\boldsymbol{Z}$ sont sur la droite $\mathrm{Re}(s) = 1/2$. Ceci signifie encore que les racines $z = \beta_\nu \neq \pm 1$ de l'équation algébrique $z^{n-1} + \sigma_1 z^{n-2} + \cdots + \sigma_{n-1} = 0$ sont toutes de valeur absolue $p^{1/2}$. Pour $n = 3$, cette équation se réduit à $z^2 + \sigma_1 z + p = 0$ et l'hypothèse de Riemann signifie donc que les racines de cette équation sont imaginaires conjuguées ou encore que $|\sigma_1| < 2\sqrt{p}$; les tables donnent $|\sigma_1| \leq 3$ pour $p = 3, |\sigma_1| \leq 4$ pour $p = 5$ et $|\sigma_1| \leq 5$ pour $p = 7$, d'où l'hypothèse de Riemann. Pour $n = 4$ l'équation $z^3 + \sigma_1 z^2 + \sigma_2 z + p = 0$ avec $\sigma_2 = p - 1 + \sigma_1$ (racine triviale -1); ses racines non triviales sont celles de l'équation $z^2 + (\sigma_1 - 1)z + p = 0$ et l'hypothèse de Riemann s'écrit dans ce cas $|\sigma_1 - 1| < 2\sqrt{p}$ qu'Artin vérifie pour $p = 3$ ou 5.

Le nombre h de classes d'idéaux s'exprime au moyen de $\boldsymbol{Z}(0)$ (cas imaginaire) ou de $\boldsymbol{Z}'(0)$ (cas réel) et par conséquent au moyen des racines β_ν :

$$h = \begin{cases} \displaystyle\prod_{\nu=1}^{n-1} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ impair,} \\ \displaystyle 2\prod_{\nu=1}^{n-1} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ pair dans le cas imaginaire,} \\ \displaystyle \frac{1}{R}\prod_{v=1}^{n-2} (\beta_\nu - 1) & \text{pour } n = \deg D \text{ pair dans le cas réel.} \end{cases}$$

En utilisant l'hypothèse de Riemann, Artin en déduit des encadrements pour h et il trouve ainsi qu'il n'y a qu'un nombre fini de corps $K(\sqrt{D})$ avec un nombre de classes h donné; par exemple, si $p > 5$ et $n > 3$, le nombre de classes est ≥ 2.

La fonction $\boldsymbol{Z}$ donne aussi une estimation asymptotique du nombre $\pi(x)$ d'idéaux premiers $\mathfrak{p}$ tels que $|N\mathfrak{p}| = x$; on a

$$\pi(p^\nu) = \frac{p^\nu}{\nu} + O\left(\frac{p^{\theta\nu}}{\nu}\right)$$

en notant θ la borne supérieure des parties réelles des zéros de $\boldsymbol{Z}$ (si l'hypothèse de Riemann est vraie, $\theta = 1/2$).

2. F.K. Schmidt

La théorie d'Artin a été étendue par F.K. Schmidt (1925, 1931) au cas des extensions finies K (non nécessairement quadratiques) d'un corps de fonctions rationnelles $k(z)$ à coefficients dans un corps fini k. Pour définir et étudier la fonction zêta dans ce cas plus général, Schmidt a été amené à changer de point de vue et à remplacer le modèle des corps de nombres algébriques par celui des corps de fonctions algébriques d'une variable. Dedekind et Weber (1882) avaient en effet développé, en s'inspirant de la théorie des nombres algébriques, une théorie purement algébrique des extensions finies K du corps $\mathbf{C}(z)$ des fonctions rationnelles à coefficients complexes ; une

telle extension est formée des fonctions rationnelles en deux variables z et u liées par une relation algébrique $F(z,u)=0$. Le but de Dedekind et Weber était d'obtenir une définition générale et rigoureuse des points de la surface de Riemann associée à la fonction algébrique u de z. Un point correspond à une *place* P de K, sous-anneau de valuation de K formé des fonctions régulières au point considéré; un tel anneau possède un unique idéal maximal $\mathfrak{p}$, formé des fonctions nulles au point et l'homomorphisme $\mathrm{P}\to \mathrm{P}/\mathfrak{p}\cong \mathbf{C}$ correspond à l'évaluation d'une fonction au point.

Dans le cas de Schmidt, $\mathbf{C}$ est remplacé par un corps fini k (de caractéristique p_0), mais on peut encore définir les places P de K (ce sont les sous-anneaux intégralement clos de K admettant K comme corps des fractions) et ceci d'une manière indépendante du choix de la variable z; si $z\in \mathrm{P}$ cette place contient la fermeture entière $\mathfrak{I}$ de $k[z]$ dans K, $\mathfrak{I}\cap\mathfrak{p}=\tilde{\mathfrak{p}}$ est un idéal *premier* de $\mathfrak{I}$ et P est le localisé correspondant. Les places qui ne contiennent pas z s'interprètent comme des points à l'infini relativement à la variable z et on obtient toutes les places en localisant les fermetures intégrales des deux anneaux $k[z]$ et $k[1/z]$. Au lieu de travailler, comme Artin, avec un anneau d'entiers $\mathfrak{I}$ et ses idéaux, Schmidt travaille avec les *diviseurs* de K, qui sont des expressions formelles $\mathfrak{c}=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où les $\mathfrak{p}_i$ sont des idéaux maximaux de places P_i et les exposants e_i sont des entiers (non nécessairement positifs); ces diviseurs forment un groupe multiplicatif (commutatif) $\boldsymbol{D}$ engendré librement par les diviseurs *premiers* $\mathfrak{c}=\mathfrak{p}$. Un diviseur est dit *entier* si tous ses exposants sont ≥ 0 et un diviseur $\mathfrak{c}'$ est *multiple* de $\mathfrak{c}''$ si $\mathfrak{c}'/\mathfrak{c}''$ est entier. A un élément z non nul de K on associe le diviseur $(z)=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où les $\mathfrak{p}_i$ sont tels que $\mathrm{P}_i z\neq \mathrm{P}_i$ et les e_i sont déterminés par $\mathrm{P}_i z=\mathfrak{p}_i^{e_i}$; si $\tilde{\mathfrak{c}}=\tilde{\mathfrak{p}}_1^{e_1}\tilde{\mathfrak{p}}_2^{e_2}\cdots\tilde{\mathfrak{p}}_s^{e_s}$ est un idéal d'un sous-anneau de Dedekind R de K avec sa décomposition en produit d'idéaux premiers, on lui associe le diviseur $\mathfrak{c}=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}$ où, pour chaque i, $\mathfrak{p}_i$ est l'idéal maximal de la place $R_{\tilde{\mathfrak{p}}_i}$.

L'*ordre* est un homomorphisme du groupe $\boldsymbol{D}$ dans le groupe $\mathbf{Z}$ des entiers; pour un diviseur premier $\mathfrak{p}$, c'est le degré de l'extension résiduelle $\mathrm{P}/\mathfrak{p}$ relativement à $(\mathrm{P}\cap k[z])/(\mathfrak{p}\cap k[z])$; les diviseurs d'éléments de K sont d'ordre 0, donc tous les diviseurs d'une même classe *modulo* le sous-groupe $\boldsymbol{H}$ des diviseurs d'éléments de K ont le même ordre. Si z appartient à K mais pas à k et que K est séparable sur $k(z)$, Schmidt asssocie à l'extension $K/k(z)$ un diviseur *différente* ∂_z dont l'ordre est l'indice de *ramification* w_z de K sur $k(z)$; le *genre* de K est défini par

$$g=\frac{w_z}{2}-m_z+1$$

où $m_z=[K:k(z)]$ et il est indépendant du choix de z.

Le point central de la théorie de Schmidt est l'analogue du théorème de *Riemann-Roch* dans le théorie classique des fonctions algébriques d'une variable, il permet d'évaluer le nombre des diviseurs entiers qui appartiennent à une classe donnée de diviseurs $\boldsymbol{C}\in \boldsymbol{D}/\boldsymbol{H}$. Si $\mathfrak{c}$ est un diviseur donné, les diviseurs entiers équivalents

sont de la forme $(\alpha)\mathfrak{c}$ où $\alpha \in K$ est choisi tel que (α) soit multiple de $\mathfrak{e}/\mathfrak{c}$ ($\mathfrak{e}$ note le diviseur neutre). Un premier résultat (difficile) est que les $\alpha \in K$ tels que (α) soit multiple d'un diviseur donné forment un sous-k-espace vectoriel de rang fini ; Schmidt établit ensuite que ce rang r ne dépend que de la classe $\boldsymbol{C}$ de $\mathfrak{c}$ dans le cas où le diviseur donné est $\mathfrak{e}/\mathfrak{c}$ et il l'appelle la *dimension* $\{\boldsymbol{C}\} = r$ de $\boldsymbol{C}$. Si k a p éléments, le nombre de diviseurs entiers dans $\boldsymbol{C}$ est $(p^r - 1)/(p - 1)$. Le théorème de Riemann-Roch s'énonce par la relation

$$\{\boldsymbol{C}\} = \left\{\frac{\boldsymbol{W}}{\boldsymbol{C}}\right\} + q - g + 1$$

où q est l'ordre de la classe $\boldsymbol{C}$ et $\boldsymbol{W}$ est la *classe différentielle* de K, c'est-à-dire celle des diviseurs ∂_z/n_z^2 où z est un élément de K non dans k, de dénominateur n_z ; on en tire (en faisant successivement $\boldsymbol{C} = \boldsymbol{H}$ et $\boldsymbol{C} = \boldsymbol{W}$) que $\boldsymbol{W}$ est d'ordre $2g - 2$, donc la classe *complémentaire* $\boldsymbol{C}' = \boldsymbol{W}/\boldsymbol{C}$ de $\boldsymbol{C}$ est d'ordre $q' = 2g - 2 - q$. Ceci permet de donner au théorème une forme symétrique

$$\{\boldsymbol{C}\} - \frac{q}{2} = \{\boldsymbol{C}'\} - \frac{q'}{2};$$

lorsque $q \geq 2g - 2, q' \leq 0$ donc

$$\{\boldsymbol{C}'\} = 0 \quad \text{et} \quad \{\boldsymbol{C}\} = q - g + 1 \ (> 0 \text{ si } q > 0).$$

La fonction zêta associée par Schmidt au corps K est définie par le produit infini

$$\boldsymbol{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |\mathfrak{p}|^{-s}}$$

étendu à tous les diviseurs premiers de K et dans lequel $|\mathfrak{p}| = p^f$ si $\mathfrak{p}$ est d'ordre f ; le produit converge pour $\mathrm{Re}(s) > 1$ et il est égal à la somme de la série $\sum_{\mathfrak{c}} 1/|\mathfrak{c}|^s$ (où $\mathfrak{c}$ parcourt l'ensemble des diviseurs entiers). Schmidt somme cette série réunissant les $\mathfrak{c}$ d'une même classe ; il n'y a qu'un nombre fini de $\mathfrak{c}$ avec un ordre $< q_0 = 2g - 2$ et, pour les autres, le nombre d'éléments de la classe est donné explicitement par le théorème de Riemann-Roch ; il démontre en même temps que le p.g.c.d. des ordres des diviseurs premiers est 1 et il trouve finalement

$$\boldsymbol{Z}(s) = \frac{1}{p-1} \sum_{q=1}^{q_0-1} \sum_{i=1}^{h} \frac{p^{\left\{C_q^{(i)}\right\}}}{p^{qs}} + \frac{hp^{-(g-1)}}{p-1} \cdot \frac{p^{(2g-2)(1-s)}}{1 - p^{1-s}} + \frac{h}{p-1} \cdot \frac{1}{1-p^s}$$

où h est le nombre (fini) des classes de diviseurs d'ordre 0. Cette formule et le théorème de Riemann-Roch donnent l'équation fonctionnelle

$$\boldsymbol{Z}(1-s) = p^{(g-1)(2s-1)} \boldsymbol{Z}(s).$$

Schmidt compare sa fonction zêta à celle qu'on obtiendrait en considérant les idéaux d'un anneau $\mathfrak{I}$ à la manière d'Artin et il retrouve les résultats d'Artin dans le cas particulier des extensions quadratiques.

3. H. Hasse

H. Hasse a pu démontrer l'hypothèse de Riemann pour la fonction zêta de Schmidt dans le cas où le genre g est 1 ; il a exposé ce résultat au Congrès international d'Oslo en 1936. Partant d'un polynôme irréductible à deux variables $f(X,Y) \in \mathbf{F}_p[X,Y]$ (p premier), il considère un facteur irréductible f_0 de f sur la clôture algébrique k de $\mathbf{F}_p$ et le corps k_0 engendré par les coefficients de f_0 ; le corps K_0 est alors l'extension de k_0 engendrée par X et Y liés par $f_0(X,Y)=0$. Si $q=p^f$ est le nombre d'éléments de k_0, la fonction zêta s'écrit

$$\boldsymbol{Z}(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}} = \prod_{n\geq 1} \left(\frac{1}{1-q^{-ns}}\right)^{N_n} = 1 + \frac{N_1}{q^s} + \cdots$$

où N_n est le nombre de diviseurs premiers de *degré* n (on dit désormais *degré* au lieu d'*ordre* comme Schmidt) ; Hasse la décompose en $\boldsymbol{Z}_0(s)L(s)$ avec

$$\boldsymbol{Z}_0(s) = \frac{1}{1-\dfrac{1}{q^s}} \cdot \frac{1}{1-\dfrac{q}{q^s}} = 1 + \frac{q+1}{q^s} + \cdots$$

(fonction zêta de $k_0(X)$) et

$$L(s) = 1 + \frac{N_1-(q+1)}{q^s} + \cdots + \frac{q^s}{q^{2gs}} = \prod_{i=1}^{g}\left(1-\frac{\omega_i}{q^s}\right)$$

où g est le genre de K_0.

Avec ces notations

$$N_1 - (q+1) = \sum_{i=1}^{2g} \omega_i$$

et l'hypothèse de Riemann, qui s'écrit $|\omega_i| = q^{1/2}$ pour $1 \leq i \leq 2g$, implique l'inégalité

$$|N_1 - (q+1)| \leq 2g\sqrt{q}.$$

Dans le cas où $g=1$, on a

$$L(s) = 1 + \frac{N_1-(q+1)}{q^s} + \frac{q}{q^{2s}}$$

et l'hypothèse de Riemann siginifie que les racines ω_1 et ω_2 sont imaginaires conjuguées c'est à dire que

$$|N_1 - (q+1)| \leq 2\sqrt{q};$$

des inégalités moins précises avaient été obtenues par Davenport et par Mordell dans le cas d'une équation

$$Y^2 = f(X),$$

f polynôme de degré 3 à coefficients dans $\mathbf{F}_p$ (avec des exposants 3/4 ou 2/3 au lieu de 1/2).

Pour démontrer l'hypothèse de Riemann, Hasse étudie la structure de l'ensemble $\boldsymbol{A}$ des "points" de $K = k(X, Y)$ (ce sont, par définition, les diviseurs premiers de degré 1); parmi ces points, les N_1 diviseurs premiers de degré 1 de K_0 sont caractérisés par leur invariance relativement à l'opération de *Frobenius* π, qui provient de l'élévation à la puissance q de X et de Y. D'une manière précise, $\pi : \varphi(X, Y) \mapsto \varphi(X^q, Y^q)$ est un isomorphisme de K sur un sous-corps $K\pi = k(X^q, Y^q)$ et on pose, pour tout diviseur premier $\mathfrak{p}$ de K,

$$\pi\mathfrak{p} = (N_{K/K\pi}\mathfrak{p})^{\pi^{-1}}.$$

Hasse dit qu'un isomorphisme μ de K sur un sous-corps $K\mu$ est un *méromorphisme* de K et il le fait opérer sur $\boldsymbol{A}$ en posant

$$\mu\mathfrak{p} = (N_{K/K\mu}\mathfrak{p})^{\mu^{-1}}.$$

Lorsqu'on choisit une origine $\mathfrak{o}$ dans $\boldsymbol{A}$ on établit une correspondance bijective $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{o}$ de $\boldsymbol{A}$ sur le groupe $\boldsymbol{D}_0/\boldsymbol{H}$ des classes de diviseurs de degré 0, d'où une loi de groupe commutatif sur $\boldsymbol{A}$; l'ensemble M des méromorphismes de $\boldsymbol{A}$ qui laissent $\mathfrak{o}$ invariant a alors une structure d'*anneau* (non nécessairement commutatif) qui contient $\mathbf{Z}$. La *norme*

$$\mu \mapsto N(\mu) = [K : K\mu] \quad (\mu \in M)$$

est multiplicative et c'est une fonction quadratique de μ, d'où on déduit l'inégalité (de Cauchy-Schwarz)

$$(N(\mu \pm \nu) - N(\mu) - N(\nu))^2 \leq 4N(\mu)N(\nu)$$

et le fait que tout méromorphisme μ vérifie une équation du second degré $\mu^2 + \ell\mu + m = 0$ avec

$$\ell = N(\mu - 1) - N(\mu) - 1 = \mu + \bar{\mu} \quad \text{et} \quad m = N(\mu) = \mu\bar{\mu}$$

($\bar{\mu}$ "conjugué" de μ); l'inégalité précédente montre que $\ell^2 \leq 4m$. Dans le cas du méromorphisme π de Frobenius, $m = N(\pi) = q$ et $N(\pi - 1) = N_1$ (nombre de points fixe par π) donc

$$\ell = N(\pi - 1) - N(\pi) - 1 = N_1 - (q + 1);$$

l'inégalité trouvée est précisément celle qui exprime l'hypothèse de Riemann.

Hasse termine son travail en indiquant une voie, suggérée par Deuring, pour étendre cette théorie aux corps du genre g quelconque. Pour $g \geq 2$ il n'y a plus de loi de groupe sur $\boldsymbol{A}$ ni d'anneau des méromorphismes, mais on peut construire un anneau des *correspondances* sur le modèle de la théorie développée par Hurwitz en 1886 pour les surfaces de Riemann (une correspondance (m, n) associe un n-uple de points à un m-uple de points).

3. A. Weil

C'est cette voie qu'A. Weil (1940) a suivie pour démontrer l'hypothèse de Riemann dans le cas d'un genre g quelconque. Mais pour développer sa méthode, Weil a de nouveau déplacé le cadre théorique : au lieu de la théorie des fonctions algébriques d'une variable, il prend pour modèle celui de la *géométrie* des courbes algébriques. Ceci l'a amené à développer la géométrie algébrique sur un corps de base (commutatif) arbitraire (Weil 1946) ou géométrie algébrique abstraite. Sur un corps de base k parfait (par exemple fini ou algébriquement clos ou de caractéristique 0), un corps K de fonctions algébriques d'une variable peut s'interpréter comme le corps Ω_k des fonctions sur une courbe algébrique complète Γ sans point multiple qui admettent k comme corps de définition ; les diviseurs de K correspondent aux *diviseurs* sur Γ rationnels par rapport à k, qui sont des combinaisons linéaires de points de Γ à coefficients entiers. En géométrie, on note additivement la loi du groupe des diviseurs. Si le corps de base k est fini, à q éléments, on définit la fonction zêta de Γ par

$$Z(u) = \sum_{\mathfrak{a}} u^{\deg(\mathfrak{a})} = \prod_{\mathfrak{p}} \left(1 - u^{\deg(\mathfrak{p})}\right)^{-1}$$

où la somme est étendue à tous les diviseurs positifs rationnels par rapport à k et le produit à tous les diviseurs premiers rationnels par rapport à k ; la variable u remplace q^{-s} et la convergence a lieu pour $|u| < 1/q$. Weil établit que Z est une fonction *rationnelle*, de la forme

$$\frac{P(u)}{(1-u)(1-qu)}$$

où P est un polynôme de degré $2g$ où g est le *genre* de la courbe Γ et que l'on a une équation fonctionnelle

$$Z\left(\frac{1}{qu}\right) = q^{1-g}u^{2-2g}Z(u);$$

ceci résulte, comme dans la théorie de Schmidt, du théorème de Riemann-Roch qui permet d'évaluer le rang $\ell(\mathfrak{a})$ (sur le corps des constantes) de l'espace vectoriel des diviseurs positifs équivalents à un diviseur $\mathfrak{a}$ donné : $\ell(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1 + r(\mathfrak{a})$ où le genre g est défini comme la valeur maximum de $\deg(\mathfrak{a}) - \ell(\mathfrak{a}) + 1$ lorsque $\mathfrak{a}$ varie et $r(\mathfrak{a}) = \ell(\mathfrak{k} - \mathfrak{a})$ en notant $\mathfrak{k}$ (k gothique) un diviseur *canonique*, c'est à dire la projection sur Γ d'un cycle d'intersection $\Delta \cdot [(\theta) - \Delta]$ (Δ désigne la diagonale du produit $\Gamma \times \Gamma$ et θ une fonction sur ce produit s'annulant à l'ordre 1 le long de Δ et admettant k comme corps de définition ; la classe $\omega = \{\theta\}$ de θ *modulo* les θ' qui s'annulent le long de Δ à un ordre > 1 est appelée une *différentielle* et le diviseur $\mathfrak{k} = (\omega)$ ne dépend que de ω). Tous les diviseurs canoniques sont équivalents et de degré $2g - 2$; on a $\ell(\mathfrak{k}) = g$ et $r(\mathfrak{k}) = 1$.

On a

$$d(\log Z(u)) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \deg(\mathfrak{p}) u^{m \deg(\mathfrak{p})} \frac{du}{u} = \sum_{n=1}^{\infty} \nu_n u^n \frac{du}{u}$$

où $\nu_n = \sum_{\deg(\mathfrak{p})|n} \deg(\mathfrak{p})$ s'interprète comme le nombre de points P de Γ dont le corps de définition $k(\mathrm{P})$ est contenu dans l'extension k_n de degré n de k (unique sous-corps à q^n éléments dans la clôture algébrique de k). Ainsi ν_n est le nombre de points fixes de la *correspondance* de Frobenius itérée I_n définie par l'élévation des coordonnées à la puissance q^n-ième.

Une correspondance X sur Γ est, par définition, un diviseur sur le produit $\Gamma \times \Gamma$ (combinaison linéaire formelle à coefficients entiers de courbes). On fait opérer X sur les diviseurs de Γ de la manière suivante; si $X = X_0 + \mathfrak{a} \times \Gamma$ où X_0 n'a pas de composante de la forme A $\times \Gamma$ (A point de Γ) et $\mathfrak{a}$ est un diviseur de Γ, $X(\mathfrak{b})$ est la deuxième projection de l'intersection $X_0(\mathfrak{b} \times \Gamma)$ ($\mathfrak{b}$ diviseur quelconque de Γ). Le groupe additif des correspondances est muni d'une forme bilinéaire $(X, Y) \mapsto I(X, Y)$ (à valeurs entières) telle que $I(X, Y) = \deg(X \cdot Y)$ lorsque le produit d'intersection $X \cdot Y$ est défini et d'une relation d'équivalence $\equiv$ telle que $X \equiv 0$ équivaille au fait que X transforme tout diviseur $\mathfrak{m}$ de degré 0 en le diviseur $X(\mathfrak{m})$ d'une fonction sur Γ. Les correspondances se composent de manière que $X \circ Y$ transforme $\mathfrak{b}$ en $X(Y(\mathfrak{b}))$ et cette loi de composition est compatible avec la relation d'équivalence; l'ensemble des *classes de correspondances* est ainsi muni d'une structure d'*anneau* (non commutatif) dont l'élément unité est la classe δ de la diagonale Δ. Cet anneau A possède une anti-involution $\xi \mapsto \xi'$ qui provient de la symétrie $P \times Q \mapsto Q \times P$ de $\Gamma \times \Gamma$ et une *trace* $\sigma : A \to \mathbf{Z}$ (forme linéaire) telle que $\sigma(\xi') = \sigma(\xi)$ et $\sigma(\xi \cdot \eta) = \sigma(\eta \cdot \xi)$. La trace $\sigma(\xi)$ d'une classe de correspondances ξ est définie comme dans la théorie de Hurwitz : si X est une correspondance de classe ξ, on lui associe des entiers $d(X)$ et $d'(X)$ de manière que les deux projections de X sur Γ soient $d(X)\Gamma$ et $d'(X)\Gamma$, puis on pose $S(X) = d(X) + d'(X) - I(X \cdot \Delta) = \sigma(\xi)$ (cela ne dépend que de ξ). La trace de δ est $2g$ où g est le genre.

La clef de la démonstration de Weil est l'analogue abstrait d'un théorème démontré par Castelnuovo et Severi (1926) pour la géométrie algébrique complexe : pour toute classe de correspondances $\xi \neq 0$, $\sigma(\xi \cdot \xi') > 0$. Si le genre est 1, on a $\xi \cdot \xi' = N\delta$ avec un entier $N > 0$, d'où $\sigma(\xi \cdot \xi') = 2N > 0$; pour les genres supérieurs, Weil le démontre en travaillant dans la variété $\Omega = \Gamma \times \Gamma \times \cdots \times \Gamma$ produit de $d(X)$ facteurs égaux à Γ. On en déduit (Cauchy-Schwarz) que $(\sigma(\xi \cdot \eta'))^2 \leq \sigma(\xi \cdot \xi')\sigma(\eta \cdot \eta')$. Dans le cas de la correspondance de Frobenius itérée I_n, on a

$$I_n \circ I_n' = q^n \Delta, \quad d(I_n) = 1, \quad d'(I_n) = q^n, \quad \deg(I_n \cdot \Delta) = \nu_n$$

donc

$$S(I_n) = 1 + q^n - \nu_n = \sigma(\iota^n)$$

en notant ι la classe de la correspondance de Frobenius I_1 ; l'inégalité de Cauchy-Schwarz appliquée à $\xi = \iota^n$ et $\eta = \delta$ s'écrit donc

$$(**) \qquad |\sigma(\iota^n)| = |1 + q^n - \nu_n| \leq 2gq^{n/2}$$

Le numérateur $P(u) = (1-u)(1-qu)Z(u)$ de la fonction zêta a pour dérivée logarithmique

$$d(\log P(u)) = -\sum_{n=1}^{\infty} \sigma(\iota^n) u^n \frac{du}{u}$$

et l'inégalité $(**)$ montre que cette série converge pour $|u| < q^{-1/2}$; ainsi P n'a ni zéro ni pôle dans ce disque et Z n'y a donc pas de zéro et pas d'autre pôle que $u = 1/q$.

L'équation fonctionnelle permet alors d'en déduire que $Z(u)$ ne s'annule pas non plus pour $|u| > q^{-1/2}$ et que son seul pôle dans ce domaine est $u = 1$; on a ainsi établi l'hypothèse de Riemann selon laquelle les zéros de $Z(u)$ ont tous $q^{-1/2}$ pour valeur absolue.

Weil a poursuivi son travail en interprétant le polynôme P comme un polynôme caractéristique au moyen de la théorie des *jacobiennes* de courbes (1948). A une courbe Γ de genre g est associée une *variété abélienne* J de dimension g, birationnellement équivalente au produit symétrique de g facteurs égaux à Γ, ainsi qu'une fonction $\varphi : \Gamma \to J$ définie à une constante additive près; rappelons qu'une variété abélienne est, par définition, une variété de groupe qui est complète et que sa loi de groupe est automatiquement commutative. Le groupe des points J est isomorphe au groupe des classes de diviseurs de degré 0 sur Γ et l'anneau A des classes de correspondances sur Γ s'identifie à l'anneau des endomorphismes de J. Si ℓ est un nombre premier $\neq p$, le groupe $\mathfrak{g}_\ell(J)$ des points de J dont l'ordre est une puissance de ℓ est isomorphe à $\mathbf{Q}_\ell^{2g}/\mathbf{Z}_\ell^{2g}$; à la classe de Frobenius ι est associé un endomorphisme de J qui opère sur ce groupe et que l'on peut représenter par une matrice carrée $M_\ell(\iota)$ d'ordre $2g$ à coefficients entiers ℓ-adiques. Alors P est le polynôme caractéristique de cette matrice.

Weil a ensuite essayé d'étendre sa théorie à des variétés algébriques X_0 de dimension quelconque définies sur un corps fini k à q éléments : en notant encore ν_n le nombre des points P de X_0 tels que $k(\mathrm{P})$ soit contenu dans le corps k_m à q^m éléments, il définit la fonction zêta de X_0 par les conditions $Z(0) = 1$ et

$$t\frac{d}{dt}\log Z(t) = \sum_{m=1}^{\infty} \nu_m t^m.$$

Pour des exemples simples, il est facile de calculer les ν_m et de déterminer explicitement $Z(t)$; par exemple pour l'espace affine de dimension r on $\nu_m = q^{mr}$ donc

$$t\frac{d}{dt}\log Z(t) = \frac{q^r t}{1-q^r t} \quad \text{et} \quad Z(t) = \frac{1}{1-q^r t}.$$

De même, pour l'espace projectif de dimension r, $\nu_m = 1 + q^m + \cdots + q^{mr}$ donc

$$t\frac{d}{dt}\log Z(t) = \frac{t}{1-t} + \frac{qt}{1-qt} + \cdots + \frac{q^r t}{1-q^r t}$$

ce qui donne

$$Z(t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^r t)}.$$

Le cas de la *grassmannienne* des sous-espaces de dimension r dans $\mathbf{P}_n$ est aussi calculé par Weil : on a

$$\nu_m = \frac{q^{m(n+1)}-1}{q^m-1}\cdots\frac{q^{m(n+1)}-q^{mr}}{q^{m(r+1)}-q^{mr}} = 1 + b_1 q^m + \cdots + b_d q^{dm}$$

où $d = (n-r)(r+1)$ est la dimension de la grassmannienne et les coefficients b_i sont des entiers. Ainsi

$$t\frac{d}{dt}\log Z(t) = \frac{t}{1-t} + b_1\frac{qt}{1-qt} + \cdots + b_d\frac{q^d t}{1-q^d t}$$

ce qui donne

$$Z(t) = \frac{1}{(1-t)(1-qt)^{b_1}\cdots(1-q^d t)^{b_d}};$$

sur le corps des complexes, la grassmannienne correspondante a pour nombre de Betti b_i en dimension $2i$.

Weil formule enfin ses conjectures générales à la fin d'un article de 1949 consacré au cas des *hypersurfaces monomiales*, c'est-à-dire des variétés d'équation

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = b$$

dans l'espace affine de dimension $r+1$. Il fait le décompte des points au moyen d'une méthode déjà mise en œuvre par Hardy et Littlewood (1922) dans leur étude du problème de Waring et reprise par Hasse et Davenport (1935) à propos de l'équation $ax^m + by^n + cz^r = 0$; cette méthode utilise les *sommes de Gauss* bien connues en théorie des nombres et elle permet d'établir, pour le nombre N des points de l'hypersurface avec $b = 0$, l'inégalité

$$|N - q^r| \leq M(q-1)q^{\frac{r-1}{2}}$$

où M est une constante dépendant seulement des exposants n_i. Le calcul peut être mené à terme avec b quelconque en supposant que tous les n_i sont égaux à un même nombre n ; Weil trouve que

$$Z(U) = \frac{P_{r-1}(U)^{(-1)^r}}{(1-U)(1-qU)\cdots(1-q^{r-1}U)}$$

où P_{r-1} est un polynôme de degré M dont tous les zéros sont de valeur absolue $q^{-\frac{r-1}{2}}$. Or une variété algébrique *complexe* définie par une équation du même type a des nombres de Betti $B_{r-1} = M$ et, pour $h < r-1, B_h = 1$ ou 0 selon que h est pair ou impair.

Ces résultats conduisent Weil à formuler les conjectures suivantes :

1. La fonction zêta d'une variété algébrique X_0 de dimension n sur k est *rationnelle.*

2. Elle satisfait une *équation fonctionnelle*

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{\frac{n\chi}{2}} t^\chi Z(t)$$

où $\chi = (\Delta \cdot \Delta)$ joue le rôle de la *caractéristique d'Euler-Poincaré* de X_0.

3. On a

$$Z(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

où $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$ et, pour $1 \leq h \leq 2n-1$, $P_h(t)$ est un polynôme dont les racines sont des entiers algébriques de valeur absolue $q^{-h/2}$.

4. En définissant le *nombre de Betti* B_h de X_0 en dimension h comme le degré de P_h, on a $\chi = \sum_{h=0}^{2n}(-1)^h B_h$. De plus, si X est une variété algébrique sans point multiple sur un corps de nombres algébriques K, les nombres de Betti classiques de X coïncident pour presque tout idéal premier $\mathfrak{p}$ de K avec ceux de la reduction $X_\mathfrak{p}$ de X mod $\mathfrak{p}$.

A. Weil indique de plus un programme pour démontrer ces conjectures : il s'agit de construire, pour les variétés algébriques X (sans point multiple) sur un corps fini k, une théorie cohomologique convenable ; cette théorie doit faire correspondre à chaque X une suite d'espaces vectoriels $H^i(X)$ sur un corps K de *caractéristique* 0 et ceci d'une manière fonctorielle et avec les propriétés suivantes :

(1) *Dualité de Poincaré* : si X est de dimension n, $h^i(X) = 0$ sauf pour $0 \leq i \leq 2n$, $H^{2n}(X) \approx K$ et on a un accouplement bilinéaire $H^i(X) \times H^{2n-i}(X) \to H^{2n}(X)$ permettant d'identifier $H^{2n-i}(X)$ au dual de $H^i(X)$.

(2) *Formule de Künneth* : $H^*(X) \otimes_K H^*(Y) \approx H^*(X \times Y)$.

(3) *Classe d'un cycle* : il y a un homomorphisme γ_X, fonctoriel et compatible avec la multiplication, du groupe $C^i(X)$ des classes de cycles (pour l'équivalence numérique) de codimension i dans $H^{2i}(X)$.

(4) *Théorème de Lefschetz* pour les sections hyperplanes.

Une telle théorie dispose d'une *formule de Lefschetz* qui permet de calculer le nombre de points fixes d'une correspondance $f \in H^0(X \times X)$ sous la forme

$$< f \cdot \Delta >= \sum_{i=0}^{2n}(-1)^i \mathrm{Tr}(f_i)$$

où f_i est l'endomorphisme de $H^i(X)$ induit par f ; cette formule est l'extension, en dimension quelconque, de la formule de Hurwitz pour les courbes (pour lesquelles

la jacobienne jouait d'ailleurs le rôle de H^1). En notant F la correspondance de Frobenius, on a

$$\nu_m = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr} F_i^m$$

d'où

$$t\frac{d}{dt}\log Z(t) = \sum_{i=0}^{2n}(-1)^i \sum_m \mathrm{Tr}(F_i^m)t^m = \sum_{i=0}^{2n}(-1)^{i+1} t\frac{d}{dt}\log \det(1-tF_i)$$

et, finalement

$$Z(t) = \prod_{i=0}^{2n} \det(1-tF_i)^{(-1)^{i+1}}$$

ce qui donne la première conjecture (rationalité) ; la dualité de Poincaré donne l'équation fonctionnelle (conjecture 2) et on déduit l'hypothèse de Riemann (conjecture 3) des théorèmes de Lefschetz sur les sections hyperplanes, qui permettent de raisonner par récurrence sur la dimension.

Weil (1954) a lui-même démontré ses conjectures dans certains cas particuliers autres que ceux déjà indiqués, comme les intersections de deux quadriques ou les surfaces cubiques. La première démonstration de la conjecture 1 est due à Dwork (1959) ; elle n'utilise pas de cohomologie mais une évaluation directe des ν_m à l'aide de sommes de Gauss grâce à une technique de relèvements p-adiques et des développements d'analyse p-adique. La méthode de Dwork a reçu par la suite une interprétation cohomologique. Entre temps A. Grothendieck a pu construire une théorie cohomologique répondant aux exigences de Weil et démontrer une partie des conjectures ; P. Deligne a établi les théorèmes de Lefschetz pour la cohomologie de Grothendieck et il a terminé la démonstration des conjectures.

Cette histoire est exemplaire des rapports entre l'arithmétique, l'algèbre et la géométrie au vingtième siècle. Elle montre la fécondité de la démarche qui consiste à transporter des idées et des méthodes du cadre qui les a suscitées dans un cadre différent. Mais l'hypothèse de Riemann classique, concernant la fonction zêta du corps des rationnels n'est toujours pas démontrée et il est peu probable qu'on l'atteigne par le genre de méthode dont nous avons parlé.

Département de Mathématiques
Université de Paris VII
2, place Jussieu
75230 Paris cedex 05
FRANCE