Sujets d'Arithmétique

Vadim Schechtman

Table de matières

Zeittafel

Pierre de FERMAT (1601 - 1665)

Leonard EULER (1707 - 1783)

Adrien Marie LEGENDRE (1752 - 1833)

Carl Friedrich GAUSS (1777 - 1855)

Niels Henrik ABEL (1802 - 1829)

Carl Gustav Jacob JACOBI (1804 - 1851)

Eduard KUMMER (1810 - 1893)

Évariste GALOIS (1811 - 1832)

Pafnuty Lvovich CHEBYSHEV (1821 - 1894)

Gotthold EISENSTEIN (1823 - 1852)

Bernhard RIEMANN (1826 - 1866)

David HILBERT (1862 - 1943)

Introduction

Dans ces notes on presente quelques notions et théorèmes classiques de la Théorie de Nombres du XIX-ième siecle.

Voici les résultats principaux: loi de réciprocité quadratique (§2). Nous en donnons deux démonstrations: une à l'aide de sommes de Gauss, l'autre d'Eisenstein, uitlisant les sinus.

Finitude du groupe de classes d'un corps de nombres algébriques (démonstration de Hurwitz); décomposition unique d'un idéal en un produit d'idéaux premiers (§4).

Théorème de Fermat pour les exposants $n = 3$ et $n = 4$ (§7) et pour p premier regulier (§6.).

Théorème de Jacobi (le nombre de representations d'un nombre comme une somme de quatre carrés, 8.22).

Propriétés fondamentales des fonctions elliptiques (d'après Abel et Eisenstein, §9.)

"Teorema elegantissima" de Gauss, 8.12. Nous en donnons deux démonstrations: une, qui utilise les sommes de Jacobi dans §8, et l'autre, due à Eisenstein, au moyen de la division de lemniscate (§10).

Toulouse, juin 2005

§1. Corps finis

1.1. *Théorème de Bezout.* Deux nombres entiers a, b sont premiers l'un à l'autre si et seulement si il existent des nombres entiers c, d tels que $ac + bd = 1$.

1.2. *Théorème.* Soit $p \in \mathbb{Z}$ un nombre premier. Alors $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps.

Preuve: exercice. Utiliser soit le théorème de Bezout, soit le lemme suivant.

1.3. *Lemme.* Un anneau commutatif fini est un corps ssi il est intègre (c'est-á-dire, ne contient pas de diviseurs de zéro).

(a) *Racines primitives*

1.4. Considérons le groupe multiplicatif $\mathbb{F}_p^*$. Celui-ci est un groupe abélien d'ordre $p-1$, d'où $a^{p-1} = 1$ pour chaque $a \in \mathbb{F}_p^*$.

En d'autres termes, pour chaque $b \in \mathbb{Z}$ premier à p, on a $b^{p-1} \equiv 1(p)$ (le "petit" théorème de Fermat).

Exemples d'applications.

1.4.1. *Exercice.* (a) Montrer que si $2^n - 1$ est premier alors n est premier.

(b) Si un premier p divise $2^{37} - 1$ alors p est de la forme $74k + 1$.

En effet, on cherche un premier p tel que $2^{37} \equiv 1(p)$. D'abord p est impair. D'un autre côté, $2^{p-1} \equiv 1(p)$, d'où $37|(p-1)$. Comme $2|(p-1)$, on a $74|(p-1)$, donc p est de la forme $74k + 1$.

(c) Donner des exemples de nombres premiers de la forme $74k + 1$.

($p = 149, 223$)

(d) Montrer que $223 \mid 2^{37} - 1$. Donc, $2^{37} - 1$ n'est pas premier.

En effet, on calcule: $2^8 \equiv 33 \pmod{223}$; $2^{16} \equiv -26 \pmod{223}$; $2^{32} \equiv 7 \pmod{223}$, d'où $2^{37} \equiv 7 \cdot 32 = 224 \equiv 1 \pmod{223}$.

1.4.2. *Exercice.* Nombres premiers de Fermat. (a) Montrer que si $2^m + 1$ est premier alors $m = 2^n$.

(b) Désignons $p_n = 2^{2^n} + 1$. Montrer que p_n est premier pour $n = 1, 2, 3, 4$.

(c) (Euler) Montrer que si un premier p divise p_5 alors $p = 64k + 1$.

(d) (Euler) Montrer que $641 \mid p_5$, donc p_5 n'est pas premier.

1.5. Considérons le groupe $\mathbb{F}_5^*$. On a Card$(\mathbb{F}_5^*)$, donc a priori ce groupe peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Essayons le nombre 2: les restes 2^a modulo 5 pour $a = 1, 2, 3, 4$ sont $2, 4, 3, 1$, donc $\mathbb{F}_5^*$ est cyclique, avec un générateur $\bar{2} = 2 \bmod(5)$.

Cela est un phénomène général.

1.6. *Théorème* (Euler) Soient F un corps, $A \subset F^*$ un sous-groupe fini. Alors A est cyclique.

1.6.1. *Lemme.* Soient A un groupe abélien, $x, y \in A$ des éléments d'ordres a, b, tels que $(a, b) = 1$. Alors xy a l'ordre ab.

En effet, si B (resp. C) est un sous-groupe engendré par x (resp. y) alors l'ordre de $B \cap C$ divise l'ordres de B et de C, donc $B \cap C = \{1\}$. Si $(xy)^c = 1$ alors $x^c, y^c \in B \cap C$ donc $x^c = y^c = 1$, donc $a|c$ et $b|c$. Il en suit que $(ab)|c$, d'où l'assertion.

1.6.2. *Lemme.* Soient A un groupe abélien, $x, y \in A$ des éléments d'ordres a, b. Alors il existe un $z \in A$ d'ordre $c := \mathrm{ppcm}(a, b)$.

En effet, on peut trouver des décompositions $a = a'a''$, $b = b'b''$ avec $(a', b') = 1$ et $c = a'b'$ (vérifier!). Alors $x^{a''}$ (resp. $y^{b''}$ est de l'ordre a' (resp. b'), donc par le lemme précédent $z = x^{a''}y^{b''}$ est de l'ordre c.

1.6.3. *Corollaire.* Soit A un abélien groupe fini, d le maximal des ordres d'éléments de A. Alors l'ordre de chaque élément de A divise d, donc $x^d = 1$ pour chaque $x \in C$.

Revenons à notre théorème. Soit d le maximal des ordres d'éléments de A. D'après le corollaire précédent, $x^d = 1$ pour chaque $x \in A$. D'autre part, l'équation $t^d - 1 = 0$ ne peut pas avoir plus que d racines dans F, d'où $d = \mathrm{Card}(A)$, donc A est cyclique.

(b)

1.7. *Théorème* (Fermat) Soit F un corps de caractéristique $p > 0$.

Alors $(x + y)^p = x^p + y^p$ pour tous $x, y \in F$.

En effet,

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

Mais

$$\binom{i}{p} \equiv 0(p)$$

pour $1 \leq i \leq p$ (vérifier!), d'où l'assertion.

Il en suit que l'application $\sigma : \ F \longrightarrow F$, $\sigma(x) = x^p$ est un morphisme de corps, necessairement injectif; de même pour ses itérés σ^f, $\sigma^f(x) = x^{p^f}$, $f \geq 1$.

Le sous-corps fixé $F_0 = \{x \in F \mid \sigma(x) = x\} \subset F$ contient $\mathbb{F}_p$ par le petit Fermat. Puisque l'équation $t^p - t = 0$ ne peut avoir plus que p racines dans F, il en suit que $F_0 = \mathbb{F}_p$.

1.8. Soit F un corps fini. Sa caractéristique est necessairement un nombre premier p; on a $\mathbb{F}_p \subset F$. Si le degré $[F : \mathbb{F}_p]$ est égale à f, alors F est un espace vectoriel sur $\mathbb{F}_p$ de dimension f, donc $\mathrm{Card}(F) = p^f$.

Réciproquement, pour chaque $f \in \mathbb{Z},\ f \geq 1$, on peut construire un corps F qui ait $q = p^f$ éléments. Pour le faire, plongeons $\mathbb{F}_p$ dans un corps Ω algébriquement clos. Considérons le morphisme $\sigma^f :\ \Omega \longrightarrow \Omega$, $\sigma^f(x) = x^q$. Il est surjectif car Ω est algébriquement clos, donc σ^f est un automorphisme de Ω.

Considérons son sous-corps fixé $F = \{x \in \Omega \mid x^q = x\} \subset \Omega$; il coïncide avec l'ensemble de racines du polynôme $f(t) = t^q - t$ dans Ω.

1.8.1. *Lemme.* Toutes les racines de $f(t)$ sont distincts.

En effet, si $\alpha \in \Omega$ est une racine multiple de $f(t)$ alors $f'(\alpha) = 0$ (démontrer!). D'autre part,

$$f'(t) = qt^{q-1} - 1 = -1$$

n'a pas de racines, donc $f(t)$ n'a pas de racines multiples, cqfd.

Ce lemme implique que $\mathrm{Card}(F) = q$.

Soit $F' \subset \Omega$ un sous-corps à q éléments. On a $\mathrm{Card}(F'^*) = q - 1$, donc $x^{q-1} = 1$ pour chaque $x \in F'$, $x \neq 0$, donc $x^q = x$ pour chaque $x \in F'$. Il en suit que $F' \subset F$, donc $F' = F$.

Enfin, soit K un corps arbitraire à q éléments. Celui-ci est une extension algébrique de $\mathbb{F}_p$ (de degré f). Par la propriété générale, il existe un plongement $\phi :\ K \hookrightarrow \Omega$ prolongeant l'inclusion $\mathbb{F}_p \subset \Omega$, puisque Ω est algébriquement clos. Son image $\phi(K)$ est un sous-corps à q éléments, donc $\phi(K) = F$. Donc $\phi :\ K \xrightarrow{\sim} F$.

On a prouvé

1.9. *Théorème.* Pour chaque nombre premier p et $f \in \mathbb{Z},\ f \geq 1$ il existe un corps à $q = p^f$ éléments. Ce corps est unique à isomorphisme près.

(c) *Fonctions μ et ϕ*

1.10. Notation: $\mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$. Un nombre $n \in \mathbb{Z},\ n > 1$, est dit *libre de carrés (square free)* si il est un produit de nombres premiers distincts.

On définit la *fonction de Moebius* $\mu :\ \mathbb{Z}_+ \longrightarrow \{-1, 0, 1\}$ par: $\mu(1) = 1$, pour $n > 1$ $\mu(n) = 0$ si n n'est pas libre de carrés et $\mu(n) = (-1)^r$ si $n = p_1 \cdot \ldots \cdot p_r$ avec p_i premiers et distincts.

1.11. *Lemme.* Pour $n > 1$, on a $\sum_{d|n}\ \mu(d) = 0$.

En effet, si $n = \prod_{i=1}^{r}\ p_i^{a_i}$ alors

$$\sum_{d|n}\ \mu(d) = \sum_{(\epsilon_1,\ldots,\epsilon_r)\in\{0,1\}^r} \mu(p_1^{\epsilon_1} \cdot \ldots \cdot p_r^{\epsilon_r}) =$$

$$= \sum_{i=0}^{r} (-1)^i \binom{i}{r} = (1-1)^r = 0$$

1.12. Considérons l'ensemble $\mathbb{Z}_+^{\mathbb{C}} = \{f :\ \mathbb{Z}_+ \longrightarrow \mathbb{C}\}$. Introduisons sur cet ensemble une opération $\circ$ (*multiplication de Dirichlet*) par

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

Elle est associative et commutative, avec l'unité $\mathbf{1}$, où $\mathbf{1}(1) = 1$, $\mathbf{1}(n) = 0$ pour $n > 1$ (vérifier!).

On définit $\nu : \mathbb{Z}_+ \longrightarrow \mathbb{C}$ par $\nu(n) = 1$ pour tous n. Évidemment,

$$f \circ \nu(n) = \sum_{d|n} f(d)$$

1.13. *Lemme.* $\mu \circ \nu = \mathbf{1}$

En effet, $\mu \circ \nu(1) = \mu(1)\nu(1) = 1$. D'autre part, pour $n > 1$

$$\mu \circ \nu(n) = \sum_{d|n} \mu(d) = 0,$$

d'après 1.11.

1.14. *Théorème* (formule d'inversion de Moebius) Pour $f \in \mathbb{Z}_+^{\mathbb{C}}$, soit $F(n) = \sum_{d|n} f(d)$. Alors

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

En effet, $F = f \circ \nu$, d'òu, par 1.13, $f = F \circ \mu$.

1.14.1. *Variante.* Soit $f : \mathbb{Z}_+ \longrightarrow G$ une application à valeurs dans un groupe abélien G, écrit multiplicativement. Si $F(n) = \prod_{d|n} f(d)$ alors

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$$

Preuve: exercice.

1.15. *Rémarque.* Dans tous le précédent, on peut aussi remplacer $\mathbb{Z}_+$ par l'ensemble de tous diviseurs d'un nombre fixé $N \in \mathbb{Z}_+$.

1.16. *Fonction d'Euler.* Pour $n \in \mathbb{Z}_+$, on définit $\Phi(n) = \{a \in \mathbb{Z},\ 1 \leq a \leq n \mid (a, n) = 1\}$; $\phi(n) := \mathrm{Card}(\Phi(n))$.

Par exemple, $\phi(1) = 1$, $\phi(p) = p - 1$ si p est premier.

On peut identifier $\Phi(n)$ avec l'ensemble de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

1.16. *Lemme.* $n = \sum_{d|n} \phi(n)$.

En effet, pour chaque $d|n$ soit Φ_d l'ensemble d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z} =$ l'ensemble de générateurs de $\mathbb{Z}/d\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$. Alors $\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} \Phi_d$.

1.17. *Corollaire.* $\phi(n) = \sum_{d|n} d\mu(n/d)$

1.18. *Exercice.* Montrer, en utilisant 1.17, que si $n = \prod_{i=1}^{r} p_i^{a_i}$ est la décomposition en facteurs premiers (tous p_i étant distincts), alors

$$\phi(n)/n = \prod_{i=1}^{r} (1 - p_i^{-1})$$

Solution. On a

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

$$= n - \sum_i n/p_i + \sum_{i<j} n/p_i p_j - \ldots = n \prod_{i=1}^{r} (1 - p_i^{-1})$$

1.19. *Lemme.* $x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x - i)\ (p)$.

En effet, par le petit Fermat nous savons $p-1$ racines $1, \ldots, p-1$ du polynôme dans $\mathbb{F}_p[x]$.

1.19.1. *Corollaire* (théorème de Wilson) $(p-1)! \equiv -1\ (p)$.

Poser $x = 0$ dans 1.19.

1.19.2. *Corollaire.* Si $d \mid (p-1)$ alors le polynome $x^d - 1$ a d racines dans $\mathbb{F}_p$.

En effet, si $d \mid (p-1)$ alors $(x^d-1)|(x^{p-1}-1)$ dans $\mathbb{F}_p$ (prouver!), i.e. $x^{p-1}-1 = (x^d-1)g(x)$. Nous savons que $x^{p-1}-1$ a $p-1$ racines; mais si x^d-1 avait moins que d racines alors $x^{p-1}-1$ aurait moins que $p-1$ racines car $g(x)$ a au plus $\deg(g(x)) = p-1-d$ racines.

1.20. *Théorème.* Le groupe $\mathbb{F}_p^*$ est cyclique.

Soit $\psi(d)$ le nombre d'éléments d'ordre d dans $\mathbb{F}_p^*$. D'après 1.19.2, on a $d = \sum_{c|d} \psi(c)$. D'apres la formule d'inversion de Moebius,

$$\psi(d) = \sum_{c|d} c\mu(d/c) = \phi(d)$$

(par 1.16). En particulier, $\psi(p-1) = \phi(p-1) > 0$ si $p > 2$. Pour $p = 2$ l'assertion est triviale.

(d)

1.21. *Théorème.* On a l'identité dans $\mathbb{F}_p[x]$

$$x^{p^n} - x = \prod_{d|n} F_d(x)$$

où $F_d(x)$ désigne le produit de tous polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$.

La preuve suivra quelques lemmes.

1.22. *Lemme.* (a) Soit K un corps. Dans $K[x]$, le polynôme $x^n - 1$ divise $x^m - 1$ ssi $n|m$.

(b) Soit $a \in \mathbb{Z},\ a > 1$. Alors $a^n - 1$ divise $a^m - 1$ ssi $n|m$.

Exercice.

1.23. *Lemme.* Dans $\mathbb{F}_p[x]$, si un polynôme $f(x)$ divise $x^{p^n} - x$, alors $f(x)^2$ ne le divise pas.

Car si $x^{p^n} - x = f(x)^2 g(x)$, alors en prénant la dérivée,

$$-1 = 2f'(x)f(x)g(x) + f(x)^2 g'(x),$$

ce qui est impossible.

1.24. *Lemme.* Dans $\mathbb{F}_p[x]$, un polynôme irréductible de degré d divise $x^{p^n} - x$ ssi $d|n$.

Soit $f(x)$ un polynôme irréductible de degré d. Posons $K = \mathbb{F}_p[x]/(f) = \mathbb{F}_p(\alpha)$. On a $[K : \mathbb{F}_p] = d$, d'où $\mathrm{Card}(K) = p^d$, donc $\beta^{p^d} - \beta = 0$ pour tous $\beta \in K$.

Si $f(x)|(x^{p^n} - x)$ alors $\alpha^{p^n} - \alpha = 0$ puisque $f(\alpha) = 0$. Il en suit que $\beta^{p^n} - \beta = 0$ pour tous $\beta \in K$ (pourquoi?). Donc $(x^{p^d} - x)|(x^{p^n} - x)$ dans $K[x]$ (car le reste aura p^d racines). Donc $(x^{p^d-1} - 1)|(x^{p^n-1} - 1)$; par 1.22 (a), $(p^d - 1)|(p^n - 1)$, par 1.19 (b), $d|n$.

Réciproquement, puisque $\alpha^{p^d} = \alpha$, on a $f(x)|(x^{p^d} - x)$, $f(x)$ étant le polynôme irréductible pour α. Si $d|n$, alors $(x^{p^d} - x)|(x^{p^n} - x)$ d'après 1.22, donc $f(x)|(x^{p^n} - x)$, cqfd.

Notre théorème est une conséquence immédiate de 1.24.

1.25. *Corollaire.* Si N_d désigne le nombre des polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[x]$, on a

$$p^n = \sum_{d|n} dN_d$$

En appliquant la formule de Moebius,

$$nN_n = \sum_{d|n} \mu(n/d)p^d$$

Donc

$$N_n = n^{-1} \sum_{d|n} \mu(n/d)p^d = n^{-1}(p^n - \ldots + \mu(n)p)$$

Cette expression est une somme des puissances *différentes* de p avec des coéfficients ± 1, donc $N_n > 0$.

Nous avons prouvé en particulier encore une fois l'existence pour chaque $n \geq 1$ d'un corps fini ayant p^n éléments.

1.26. *Exercice* (Galois, cf. [Ga]) (a) Montrer que le polynôme $f(x) = x^3 - 2$ est irréductible dans $\mathbb{F}_7[x]$.

Donc, si i est une racine de $f(x)$, on a $K = \mathbb{F}_{7^3} = \mathbb{F}_7[x]/(f) = \mathbb{F}_7[i]$. Les éléments de K sont: $a_0 + a_1 i + a_2 i^2$, $a_j \in \mathbb{F}_7$.

(b) Trouver un générateur α de $K^\times$.

(c) Trouver l'équation irréductible de α.

Solution. (b) On cherche un élément d'ordre

$$7^3 - 1 = 2 \cdot 3^2 \cdot 19$$

dans $K^\times$. Un élément d'ordre 2: -1; un élément d'ordre 3^2: i.

Cherchons un élément d'ordre 19 sous une forme $\beta = a + bi,\ a, b \in \mathbb{F}_7$. On a

$$(a + bi)^{19} = 3(a - a^4b^3) + 3(a^5b^2 + a^2b^5)i^2$$

(vérifier!), d'où deux équations

$$3a - 3a^4b^3 = 1,\ a^5b^2 + a^2b^5 = 0,$$

satisfaites pour $a = -1,\ b = 1$; donc $\beta = -1 + i$.

Il en résulte

$$\alpha = -i(-1 + i) = i - i^2$$

(c) En excluant i des équations $i^3 = 2,\ \alpha = i - i^2$, on obtient

$$\alpha^3 - \alpha + 2 = 0$$

Ceci est l'équation cherchée de α. On a $K = \mathbb{F}_7(\alpha) = \mathbb{F}_7[x]/(g)$ où $g(x) = x^3 - x + 2$.

§2. Réciprocité quadratique

2.1. *Définition* (Gauss) Soient $m \in \mathbb{Z}_{>1}$, $a \in \mathbb{Z}$, $(a, m) = 1$. a est appelé *résidu quadratique* modulo m si il existe une solution de la congruence $x^2 \equiv a\ (m)$. Sinon, a est appelé *non-résidu quadratique*.

En d'autres termes, a est résidu quadratique modulo m ssi sa classe $\bar{a} := a\mathrm{mod}(m) \in \mathbb{Z}/m\mathbb{Z}$ appartient à $(\mathbb{Z}/m\mathbb{Z})^{*2}$.

Considérons le cas $m = p$ en nombre premier. Le cas $p = 2$ étant trivial, nous supposerons que $p > 2$. Le groupe $\mathbb{F}_p^*$ est cyclique. Soit $u \in \mathbb{F}_p^*$ un générateur (une racine primitive). Alors $a \in \mathbb{F}_p^{*2}$ ssi $a = u^n$ avec n pair.

Il en suit que $a^{(p-1)/2} \in \{-1, 1\}$ et $a \in \mathbb{F}_p^{*2}$ ssi $a^{(p-1)/2} = 1$.

2.2. *Symbole de Legendre.* Soient p un nombre premier impair, a un nombre entier qui n'est pas divisible par p (ou un élément de $\mathbb{F}_p^*$). On définit $(a/p) := a^{(p-1)/2}\mathrm{mod}(p) = \pm 1$.

Donc on a $(-1/p) = (-1)^{(p-1)/2}$. En d'autres termes, $(-1/p) = 1$ si $p \equiv 1\ (4)$ et $(-1/p) = -1$ si $p \equiv 3\ (4)$.

Pour un entier n impair, définissons

$$\epsilon(n) = \frac{n-1}{2}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Considérons le groupe multiplicatif $(\mathbb{Z}/4\mathbb{Z})^*$; il est cyclique, avec un générateur 3. On peut considérer ϵ comme un homomorphisme $\epsilon :\ (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

On a $(-1/p) = (-1)^{\epsilon(p)}$.

2.3. Considérons le groupe $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$. On a

$$(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{1, 7\} \times \{1, 3\}$$

Pour un nombre entier impair n, posons

$$\omega(n) = \frac{n^2-1}{8}\ (\mathrm{mod}\ 2) \in \mathbb{Z}/2\mathbb{Z}$$

Donc $\omega(n) = 0$ si $n \equiv \pm 1\ (\mathrm{mod}\ 8)$ et $\omega(n) = 1$ si $n \equiv \pm 3\ (\mathrm{mod}\ 8)$.

On peut considérer ω comme un homomorphisme $(\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$.

2.4. *Théorème.* $(2/p) = (-1)^{\omega(p)}$

Démonstration. Soit α une racine primitive 8-ième de l'unité dans une clôture algébrique $\Omega \supset \mathbb{F}_p$, c'est-à-dire, un élément $\alpha \in \Omega$ satisfaisant l'équation $\alpha^4 = -1$. Posons $y = \alpha + \alpha^{-1}$. Alors

$$y^2 = \alpha^2 + 2 + \alpha^{-2} = 2$$

Donc

$$(\frac{2}{p}) = 2^{(p-1)/2} = y^{p-1}$$

D'un autre côté,

$$y^p = \alpha^p + \alpha^{-p}$$

Il en suit que si $p \equiv \pm 1 \pmod 8$, alors $y^p = y$, donc $y^{p-1} = 1$.

Par contre, si $p \equiv \pm 3 \pmod 8$, alors (comme $\alpha^4 = -1$)

$$y^p = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -y,$$

donc $y^{p-1} = -1$, cqfd.

2.4.1. *Exercice.* Déterminer le degré $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

Solution. Considérons la tour $\mathbb{F}_p(\alpha) \supset \mathbb{F}_p(\beta) \supset \mathbb{F}_p$, où $\beta = \alpha^2$. On a $\beta^2 = -1$, $\beta^4 = 1$, donc $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = 1$ ssi $\beta \in \mathbb{F}_p \Leftrightarrow 4|(p-1)$; si $p = 4k+3$, alors $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = 2$.

De même, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 1 \Leftrightarrow p \equiv 1 \pmod 8$.

Supposons que $p = 4k+3$, donc $p \equiv 3$ ou $7 \pmod 8$. On a $8|(p^2-1) = \mathrm{Card}(\mathbb{F}_p(\beta))$, donc dans ce cas $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\beta)$.

Il en suit que $[\mathbb{F}(\alpha) : \mathbb{F}_p] = 1$ si $p \equiv 1 \pmod 8$, sinon, ce degré est égal à 2.

Corollaire. Le polynôme $x^4 + 1$ est toujours réductible sur $\mathbb{F}_p$.

Rémarque. On a $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$, donc si $\sqrt{2} \in \mathbb{F}_p$, i.e. $p \equiv \pm 1 \pmod 8$, la même décomposition est valable dans $\mathbb{F}_p[x]$.

2.5. *Variante de la démonstration.* Soit $\zeta = e^{\pi i/4}$. Alors $\zeta^4 = -1$. On va travailler dans l'anneau $A = \mathbb{Z}[\zeta]$. On rémarque que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subset A/pA$. En effet, $A \cong \mathbb{Z}[x]/(x^4+1)$, d'où $A/pA \cong \mathbb{F}_p[x]/(x^4+1)$.

2.5.1. *Exercice.* Prouver que $A \cong \mathbb{Z}[x]/(x^4+1)$.

Considérons l'élément $\tau = \zeta + \zeta^{-1} \in A$. On a

$$\tau^2 = \zeta^2 + 2 + \zeta^{-2} = 2, \tag{2.5.1}$$

car $\zeta^2 = -\zeta^{-2}$. Plus exactement,

$$\zeta = \cos(\pi/4) + i\sin(\pi/4) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$$

d'où

$$\tau = \zeta + \zeta^{-1} = \sqrt{2} \tag{2.5.2}$$

(pour le moment, on n'aura pas besoin de ce résultat plus précis).

Il découle de (2.5.1) que

$$\tau^{p-1} = \tau^{2(p-1)/2} = 2^{p-1} \equiv (\frac{2}{p}) \pmod{p\mathbb{Z}},$$

d'où

$$\tau^p \equiv (\frac{2}{p})\tau \pmod{pA} \tag{2.5.3}$$

D'un autre côté, $\tau^p \equiv \zeta^p + \zeta^{-p} \pmod{pA}$ et $\zeta^p + \zeta^{-p} = \tau$ si $p \equiv \pm 1 (\mathrm{mod}\ 8)$ et $\zeta^p + \zeta^{-p} = -\tau$ si $p \equiv \pm 3 (\mathrm{mod}\ 8)$, i. e.

$$\tau^p \equiv (-1)^{\omega(p)} \tau \pmod{pA}$$

Donc

$$(\frac{2}{p})\tau \equiv (-1)^{\omega(p)} \tau \pmod{pA};$$

multipliant par τ,

$$2(\frac{2}{p}) \equiv 2(-1)^{\omega(p)} \pmod{pA};$$

Puisque 2 est inversible dans $\mathbb{F}_p \subset A/pA$, on en conclut que

$$(\frac{2}{p}) \equiv (-1)^{\omega(p)} \pmod{p},$$

ce qui entraîne $(2/p) = (-1)^{\omega(p)}$, cqfd.

2.6. *Exercice.* Montrer qu'il existe un nombre infini de nombres premiers p de la forme $8n + 7$.

Solution. Soient $p_1, \ldots, p_m$ des nombres premiers de la forme $8n+7$. Considérons le nombre $a = (4 \prod_{i=1}^m p_i)^2 - 2$. Si p est un nombre premier impair divisant a, alors 2 est résidu quadratique modulo p, donc $p \equiv \pm 1(8)$.

Par contre, $a/2 \equiv -1(8)$. Donc il existe un nombre premier p de la forme $8n + 7$ divisant a; évidemment, $p \notin \{p_1, \ldots, p_m\}$.

2.7. *Théorème* (Gauss) Soient p, q des nombres premiers impairs distincts. Alors

$$(\frac{p}{q}) = (-1)^{\epsilon(p)\epsilon(q)} (\frac{q}{p})$$

Dans la preuve on généralisera l'argument 2.5.

Sommes de Gauss quadratiques

2.8. On pose $\zeta = e^{2\pi i/p}$. On a

$$0 = \zeta^p - 1 = (\zeta - 1)(\zeta^{p-1} + \ldots + 1),$$

d'où

$$S_1 := \sum_{a=0}^{p-1} \zeta^a = 0 \tag{2.8.1}$$

Plus généralement, considérons la somme

$$S_a := \sum_{b=0}^{p-1} \zeta^{ab}$$

Il est clair que si $a \equiv 0(p)$, alors $S_a = p$.

Par contre, si $(a,p) = 1$ alors $\{ab \pmod p \mid 0 \leq b \leq p-1\} = \{0, ..., p-1\}$ d'où $S_a = S_1 = 0$.

On va travailler dans l'anneau $A = \mathbb{Z}[\zeta]$. Posons $f_p(x) = \sum_{i=0}^{p-1} x^i$. D'après (2.8.1) on a l'homomorphisme d'anneaux

$$\phi : \ A' = \mathbb{Z}[x]/(f_p(x)) \longrightarrow A, \ \phi(x) = \zeta$$

2.9. *Théorème.* ϕ est un isomorphisme.

Cela sera prouvé plas tard, cf. 3.9.2.1.

D'ailleurs, on peut considérer (avec Gauss) tous ce qui passe ci-dessous dans l'anneau A'.

2.10. Il est commode à poser $(0/p) = 0$.

2.10.1. *Lemme.* $\sum_{a \in \mathbb{F}_p} (a/p) = 0$.

Exercice.

On définit

$$g_a = \sum_{b \in \mathbb{F}_p} (\frac{b}{p}) \zeta^{ab} \ \in A$$

On désigne $g = g_1$.

2.11. *Lemme.* $g_a = (a/p)g$

Exercice.

Par exemple, puisque $\bar{\zeta} = \zeta^{-1}$, on trouve pour la conjuguée complexe

$$\bar{g} = g_{-1} = (-1/p)g = (-1)^{\epsilon(p)} g \tag{2.11.1}$$

2.11.1. *Exercice.* Montrer que

$$g = \sum_{a=0}^{p-1} e^{2\pi i a^2/p} \tag{2.11.2}$$

Solution. Soient $R, N \subset \{1, \ldots, p-1\}$ les sous-ensembles de résidus (resp. non-résidus) quadratiques,

$$g_R = \sum_{a \in R} \zeta^a, \ g_N = \sum_{a \in N} \zeta^a$$

On a $g_R + g_N = -1$ (pourquois?). Donc

$$g = g_R - g_N = 1 + 2g_R = 1 + \sum_{a=1}^{p-1} e^{2\pi i a^2/p}$$

2.12. *Théorème* (Gauss)

$$|g|^2 = g\bar{g} = p \tag{2.12.1}$$

D'après (2.11.1), cela est équivalent à

$$g^2 = (-1)^{\epsilon(p)}p \tag{2.12.2}$$

Rémarquons que $g_a^2 = g^2$ pour tous $a,\ (a,p) = 1$.

Démonstration. Considérons le nombre $\sum_{a\in\mathbb{F}_p}\ g_a g_{-a} = \sum_{a\in\mathbb{F}_p^*}\ g_a g_{-a}$. D'un côté, on a pour $a \in \mathbb{F}_p^*$

$$g_a g_{-a} = (a/p)(-a/p)g^2 = (-1/p)g^2,$$

d'où

$$\sum_a\ g_a g_{-a} = (p-1)(-1/p)g^2$$

D'un autre côté,

$$g_a g_{-a} = \sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\zeta^{a(b-c)},$$

d'où

$$\sum_a\ g_a g_{-a} = \sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\sum_a\ \zeta^{a(b-c)} =$$

(cf. 2.8)

$$= p\sum_{b,c}\ (\frac{b}{p})(\frac{c}{p})\ \delta(b,c) = p\sum_b\ (\frac{b^2}{p}) = p(p-1),$$

ce qui entraîne (2.12.2).

2.13. Maintenant on peut prouver la loi de réciprocité quadratique 2.7. La preuve est pareille à 2.5, avec τ remplacée par g. On va utiliser des congruences dans A (ou dans A'). On pose

$$p^* := (-1)^{\epsilon(p)}p$$

Rappelons que q est un nombre premier impair distinct de p. On a

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv (\frac{p^*}{q})\ (\mathrm{mod}\ qA),$$

d'où

$$g^q \equiv (\frac{p^*}{q})g\ (\mathrm{mod}\ qA)$$

D'autre part,

$$g^q \equiv \sum_b\ (\frac{b}{p})^q\zeta^{bq}\ (\mathrm{mod}\ qA),$$

avec

$$\sum_b\ (\frac{b}{p})^q\zeta^{bq} = g_q = (\frac{q}{p})g$$

(q étant impair). Donc

$$(\frac{p^*}{q})g \equiv (\frac{q}{p})g \pmod{qA}$$

En multipliant par g,

$$(\frac{p^*}{q})p^* \equiv (\frac{q}{p})p^* \pmod{qA}$$

Mais p^* est inversible dans A/qA, donc

$$(\frac{p^*}{q}) \equiv (\frac{q}{p}) \pmod{qA},$$

d'où

$$(\frac{p^*}{q}) = (\frac{q}{p})$$

Cela est 2.7, car

$$(\frac{p^*}{q}) = (\frac{-1}{q})^{\epsilon(p)}(\frac{p}{q}) = (-1)^{\epsilon(p)\epsilon(q)}(\frac{p}{q})$$

2.13.1. *Exercice.* Calculer (13/17).

Sommes de Gauss à valeurs dans un corps fini

2.14. Soient p et ℓ deux nombres premiers distincts impairs. Dans une clôture algébrique $\Omega \supset \mathbb{F}_p$, choisissons une racine primitive ℓ-ième de l'unité, w. On définit la "somme de Gauss"

$$y = \sum_{a \in \mathbb{F}_\ell} (\frac{a}{\ell})w^a$$

2.15. *Théorème.* $y^2 = (-1)^{\epsilon(\ell)}\ell$.

Cf. 2.12.

En effet:

$$y^2 = \sum_{a,b} (\frac{ab}{\ell})w^{a+b} = \sum_{c \in \mathbb{F}_\ell} w^c \sum_{a \in \mathbb{F}_\ell} (\frac{a(c-a)}{\ell})$$

Or si $a \neq 0$:

$$(\frac{a(c-a)}{\ell}) = (\frac{-a^2}{\ell})(\frac{1-ca^{-1}}{\ell}) = (-1)^{\epsilon(\ell)}(\frac{1-ca^{-1}}{\ell}),$$

d'où

$$(-1)^{\epsilon(\ell)}y^2 = \sum_{c \in \mathbb{F}_\ell} A_c w^c,$$

où

$$A_c = \sum_{a \in \mathbb{F}_\ell^*} (\frac{1-ca^{-1}}{\ell})$$

Si $c = 0$, $A_0 = \ell - 1$. D'un autre côté, si $c \neq 0$, l'application $a \mapsto 1 - ca^{-1}$ est une bijection $\mathbb{F}_\ell^* \xrightarrow{\sim} \mathbb{F}_\ell - \{1\}$. Donc

$$A_c = \sum_{d \in \mathbb{F}_\ell} (\frac{d}{\ell}) - (\frac{1}{\ell}) = -1$$

Il en suit:

$$\sum_{c \in \mathbb{F}_\ell} A_c w^c = \ell - 1 - \sum_{c \in \mathbb{F}_\ell^*} w^c = \ell,$$

ce qui démontre le théorème.

2.15.1. $y \in \Omega^*$.

2.16. *Lemme.* $y^{p-1} = (p/\ell)$.

En effet, puisque $\mathrm{char}(\Omega) = p$,

$$y^p = \sum_{a \in \mathbb{F}_\ell} (\frac{a}{\ell}) w^{ap} = (\frac{p}{\ell}) y,$$

ce qui entraîne le lemme, vu 2.15.1.

2.17. Maintenant on peut prouver 2.7, encore une fois. On a

$$y^{p-1} = (y^2)^{(p-1)/2} = ((-1)^{\epsilon(\ell)}\ell)^{(p-1)/2} = (\frac{(-1)^{\epsilon(\ell)}\ell}{p})$$

En combinant avec 2.16, cela implique le théorème.

Une démonstration d'Eisenstein

2.18. Soit p un nombre premier impair. Soit $S \subset \mathbb{F}_p^*$ un sous-ensemble tel que $\mathbb{F}_p^* = S \coprod (-S)$, par exemple, $S = \{1, \ldots, (p-1)/2\}$.

Pour $a \in \mathbb{F}_p^*,\ s \in S$, posons

$$as = e_s(a) s_a,\ e_s(a) = \pm 1,\ s_a \in S$$

On remarque que si $s \neq s'$ alors $s_a \neq s'_a$, car sinon, on aurait $s' = \pm s$, ce qui est impossible par hypothèse sur S. Donc $s \mapsto s_a$ est une bijection de S sur lui-même.

2.19. *Lemme* (Gauss) $(a/p) = \prod_{s \in S}\ e_s(a)$

En effet,

$$a^{(p-1)/2} \prod_{s \in S}\ s = \prod_{s \in S}\ (as) = \prod_{s \in S}\ e_s(a) s_a = \prod_{s \in S}\ e_s(a) \prod_{s \in S}\ s,$$

d'où

$$a^{(p-1)/2} = \prod_{s \in S}\ e_s(a),$$

ce qui entraîne le lemme.

2.20. *Exercice.* En déduire théorème 2.4.

Solution. Prenons $a = 2$, $S = \{1, \dots, (p-1)/2\}$. On a $e_s(2) = 1$ si $2s \leq (p-1)/2$ et $e_s(2) = -1$ si $2s > (p-1)/2$. Donc $(2/p) = (-1)^{n(p)}$ où $n(p)$ est le nombre d'entiers s tels que $(p-1)/4 < s \leq (p-1)/2$. Il reste à montrer que $n(p) \equiv \omega(p) \pmod 2$.

En effet, si $p = 4k+1$, la condition est $k < s \leq 2k$, d'où $n(p) = k$. De même, si $p = 4k-1$, $n(p) = k$ (vérifier!) Donc si $k = 2n$, c'est-à-dire, $p = 8n \pm 1$, alors $(2/p) = 1$.

Par contre, si $k = 2n+1$, i.e. $p = 8n + 4 \pm 1 = 8m \pm 3$, on a $(2/p) = -1$, cqfd.

Polynômes de Tchebycheff

2.21. *Lemme.* Soit m un nombre entier impair, $m \geq 1$. On a $\sin(mx) = f_m(\sin(x))$, où $f_m(t) \in \mathbb{Z}[t]$ est un polynôme de degré m, divisible par t, avec le terme supérieur égale à $(-4)^{(m-1)/2}$.

Démonstration par récurrence sur m. Le cas $m = 1$ est évident. Supposons que l'assertion est prouvée pour m. Nous avons

$$\sin(mx) = f_m(\sin(x)),$$

d'où, en faisant la dérivée,

$$m\cos(mx) = f'_m(\sin(x))\cos(x)$$

Donc

$$\sin((m+2)x) = \sin(mx)\cos(2x) + \cos(mx)\sin(2x) =$$

$$= f_m(\sin(x))(1 - 2\sin^2 x)) + 2m^{-1} f'_m(\sin(x))(1 - \sin^2 x)\sin(x) = f_{m+2}(\sin(x)),$$

où

$$f_{m+2}(t) = f_m(t)(1 - 2t^2) + 2m^{-1} f'_m(t)t(1 - t^2) \tag{2.21.1}$$

Il en suit que $f_{m+2}(t) \in t\mathbb{Z}[t]$ et si $f_m(t) = a_m t^m + \dots$, alors $f_{m+2}(t) = -4a_m t^{m+2} + \dots$, ce qui implique le lemme.

Variante. On a

$$\sin((m-2)x) = \sin(mx)\cos(2x) - \cos(mx)\sin(2x),$$

donc

$$\sin((m+2)x) + \sin((m-2)x) = 2\sin(mx)(1 - 2\sin^2(x)),$$

d'où l'équation de récurrence

$$f_{m+2}(t) = 2f_m(t)(1 - 2t^2) - f_{m-2}(t) \tag{2.21.2}$$

(On a $f_1(t) = t,\ f_{-1}(t) = -t$.)

2.22. *Lemme.* Soit m en entier impair ≥ 1. Alors

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} (\sin^2 x - \sin^2(2\pi a/m))$$

En effet, d'après le lemme précédent,

$$(-4)^{-(m-1)/2} \frac{\sin(mx)}{\sin(x)} = g_m(\sin(x)),$$

où $g(t)$ est un polynôme unitaire de degré pair $m-1$. Or, il est très facile d'exhiber les $m-1$ racines distinctes de $g_m(t)$: ils sont $\pm\sin(2\pi a/m)$, $a = 1, \ldots, (m-1)/2$ (on remarque que les nombres $\{\pm 2a \mid a = 1, \ldots, (m-1)/2\}$ décrivent tous les résidus possibles mod m sauf 0), d'où la formule désirée.

2.23. *Exercice* (Eisenstein) Montrer que $f_m(t)$ satisfait à l'équation différentielle

$$\frac{df_m(t)}{dt} = \frac{m\sqrt{1 - f_m(t)^2}}{\sqrt{1-t^2}}$$

(a) En déduire que

$$f_m(t) = mt - \frac{m(m^2-1)}{3!}t^3 + \frac{m(m^2-1)(m^2-3^2)}{5!}t^5 - \ldots + (-1)^{(m-1)/2} 2^{m-1} t^m$$

(b) En déduire que $f_m(t)$ satisfait à l'équation différentielle

$$(1-t^2)f_m''(t) - tf_m'(t) + m^2 f_m(t) = 0$$

2.24. *Exercice.* Soit toujours m un entier impair, $m \geq 1$.

(a) Soit $\zeta = e^{2\pi i/m}$. Montrer que

$$u^m - v^m = \prod_{b=0}^{m-1} (\zeta^b u - \zeta^{-b} v)$$

(b) Soit $f(t) = e^{2\pi i t} - e^{-2\pi i t}$. Montrer que

$$f(mt) = f(t) \prod_{a=1}^{(m-1)/2} f(t - a/m) f(t + a/m)$$

(c) En déduire le lemme 2.22.

2.25. *Lemme.* Sous les hypothèses 2.18,

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \frac{\sin(2\pi as/p)}{\sin(2\pi s/p)}$$

En effet, pour chaque $s \in S$, $as = e_s(a)s_a$, d'où

$$\sin(2\pi as/p) = e_s(a)\sin(2\pi s_a/p)$$

En faisant le produit sur $s \in S$, on a, par le lemme de Gauss,

$$(\frac{a}{p}) = \prod_{s\in S} e_s(a) = \prod_{s\in S} \frac{\sin(2\pi as/p)}{\sin(2\pi s/p)},$$

en tenant compte de ce que $s \mapsto s_a$ est une bijection, cqfd.

2.26. *Une démonstration de 2.7.* Soient ℓ, p deux nombres premiers distincts impairs. Prenons $S = \{1, \dots, (p-1)/2\}$, $T = \{1, \dots, (\ell-1)/2\}$. On a

$$(\frac{\ell}{p}) = \prod_{s\in S} \frac{\sin(2\pi \ell s/p)}{\sin(2\pi s/p)} =$$

$$= \prod_{s\in S} (-4)^{(\ell-1)/2} \prod_{t\in T} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell)) =$$

$$= (-4)^{(\ell-1)(p-1)/4} \prod_{s,t} (\sin^2(2\pi s/p) - \sin^2(2\pi t/\ell))$$

En permutant les rôles de ℓ et p, on obtient

$$(\frac{\ell}{p}) = (-1)^{(\ell-1)(p-1)/4} (\frac{p}{\ell}),$$

cqfd.

§3. Nombres algébriques

Critère d'Eisenstein

3.1. Soit A un anneau principal, K son corps de fractions. Par exemple, $A = \mathbb{Z}$, $K = \mathbb{Q}$. Un polynôme $f(t) = a_0 + \ldots + a_n t^n \in A[t]$ est dit *primitif* si $(a_0, \ldots, a_n) = A$.

Pour chaque $f(t) \in K[t]$, $f(t) = c(f) f_p(t)$, où $c(f) \in K$ et $f_p(t) \in A[t]$ est primitif. L'èlément $c(f)$ est défini à multiplication par une unité dans A près (et parfois appelé le contenu de f).

On a $f(t) \in A[t]$ ssi $c(f) \in A$.

3.2. *Lemme* (Gauss) Si $f, g \in A[t]$ sont primitifs, il en est de même de leurs produit.

En effet, il suffit de prouver que si un premier $p \in A$ ne divise pas ni f ni g, alors il ne divise pas fg. Considérons la projection canonique $\pi : A[t] \longrightarrow A/(p)[t]$. On remarque que $A/(p)$ étant intègre, $A/(p)[t]$ est intègre. Donc si $\pi(f) \neq 0$ et $\pi(g) \neq 0$, alors $\pi(fg) \neq 0$, cqfd.

3.3. *Corollaire.* Pour $f, g \in K[t]$, on a $c(fg) = c(f)c(g)$.

Exercice (cf. la preuve du corollaire suivant).

3.4. *Corollaire.* Si $f \in A[t]$ est réductible dans $K[t]$, alors il est réductible dans $A[t]$.

En effet, supposons que $f(t) = g(t)h(t)$, avec $g, h \in K[t]$ de degrés > 0. Nous avons $g(t) = c(g)g_p(t)$, $h(t) = c(h)h_p(t)$, d'où $f(t) = c(g)c(h)g_p(t)h_p(t)$. Le produit $g_p(t)h_p(t)$ est primitif, donc $c(g)c(h) = c(f) \in A$, puisque $f(t) \in A[t]$. Donc $f(t)$ est réductible dans $A[t]$.

3.5. *Théorème.* Soient $f(t) = a_0 + \ldots + a_n t^n \in A[t]$, $n > 0$, $p \in A$ un premier tel que: $p \not| \, a_n$, $p | \, a_i$ pour $i < n$ et $p^2 \not| \, a_0$. Alors $f(t)$ est irréductible dans $K[t]$.

En effet, d'après 3.4 il suffit de prouver que f est irréductible dans $A[t]$. Supposons au contraire que $f(t) = g(t)h(t)$, avec

$$g(t) = b_0 + \ldots + b_m t^m, \; h(t) = c_0 + \ldots + c_k t^k \in A[t], \; m, k > 0$$

On a $p^2 \not| \, b_0 c_0 = a_0$, donc $p \not| \, b_0$ ou $p \not| \, c_0$, disons $p \not| \, b_0$; alors $p \mid c_0$. D'autre part $p \not| \, a_n = b_m c_k$ entraîne $p \not| \, c_k$. Soit r l'indice minimal tel que $p \not| \, c_r$. On a $r \leq k < k + m = n$. Considérons

$$a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0$$

On a $p \not| \, b_0 c_r$ mais $p \mid b_i c_{r-i}$ pour $i > 0$, donc $p \not| \, a_r$, contrairement à l'hypothèse.

3.6. *Exemple.* Soit p un nombre premier. Alors $f(t) = 1 + t + \ldots + t^{p-1}$ est irréductible dans $\mathbb{Q}[t]$.

En effet, considérons

$$g(t) = f(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{i=1}^{p} \binom{i}{p} t^{i-1}$$

Ce polynôme satisfait au critère d'Eisenstein, donc il est irréductible, donc $f(t)$ l'est.

3.6.1. *Exercice.* Soit $p > 2$ premier. Prouver que le polynôme $f_p(t) \in \mathbb{Z}[t]$ défini par $f_p(\sin(x)) = \sin(px)/\sin x$ (cf. 2.21, 2.23) est un polynôme d'Eisenstein.

Solution. On a $f_p(t) = a_0 + a_2 t^2 + \ldots + a_{p-1} t^{p-1}$. On sait déjà que $a_{p-1} = \pm 2^{p-1}$, donc $p \not| a_{p-1}$.

Ensuite,

$$a_0 = f_p(0) = \lim_{x \to 0} \frac{\sin(px)}{\sin x} = p$$

Soit $g(t) = tf(t)$. Grace à (2.21.1),

$$\frac{2}{p} t(t^2 - 1) g_p'(t) = g_{p+2}(t) - g_p(t)(1 - 2t^2) \in \mathbb{Z}[t],$$

et on conclut facilement par récurrence sur k que $p | a_k$ pour $k < p - 1$.

(b) *Éléments entiers*

3.7. Dans tous ce qui suit "anneau commutatif" signifie un anneau commutatif associatif unitaire.

Soient $A \subset B$ des anneaux commutatifs. Un element $b \in B$ est dit *entier* sur A s'il satisfait à l'équation

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

avec $a_i \in A$.

3.8. *Théorème.* Si b, b' sont entiers sur A alors $b + b'$ et bb' sont entiers sur A.

Donc le sous-ensemble $A^c \subset B$ d'éléments entiers sur A est un sous-anneau, $A \subset A^c \subset B$. Il est appelé la *fermeture intégrale* de A dans B. Si $A = A^c$, on dit que A est intégralement clos dans B.

Si $A^c = B$, on dit que B est entier sur A, ou que $A \subset B$ est une extension entiere.

Un anneau A intègre est dit intégralement clos s'il est intégralement clos dans son corps de fractions.

3.9. *Exemples.*

3.9.1. *Exercice.* $\mathbb{Z}$ est intégralement clos.

3.9.2. Considérons le corps $\mathbb{Q}(\zeta)$ où $\zeta = e^{2\pi i/m}$. Cet élément est entier sur $\mathbb{Z}$, donc $\mathbb{Z} \subset \mathbb{Z}[\zeta]$ est une extension entiere. On peut prouver que $\mathbb{Z}[\zeta]$ est la ferméture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(\zeta)$.

3.9.2.1. *Exercice.* Supposons que $m = p$ est premier. On a $f_p(\zeta) = 0$, où

$$f_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + \ldots + 1$$

Montrer que l'homomorphisme $\phi : \mathbb{Z}[t]/(f_p(t)) \longrightarrow \mathbb{Z}[\zeta]$, $\phi(t) = \zeta$, est un isomorphisme.

(Utiliser 3.6 et l'argument du "contenu", cf. preuve de 3.4.)

3.9.3. *Exercice.* Soient $\mathbb{Z} \subset R$ une extension entiere, $n \in \mathbb{Z} - \{\pm 1\}$. Montrer que $nR \neq R$ (cf. 3.15).

3.10. *Lemme.* Soient A un anneau commutatif, M un A-module de type fini, $\phi : M \longrightarrow M$ un endomorphisme. Supposons que $\phi(M) = \mathfrak{a}M$, où $\mathfrak{a} \subset A$ est un idéal.

Alors ϕ satisfait à une équation

$$\phi^n + a_1\phi^{n-1} + \ldots + a_n = 0$$

avec $a_i \in \mathfrak{a}$.

En effet, soient $x_1, \ldots, x_n \in M$ des générateurs. On a $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$, $a_{ij} \in \mathfrak{a}$. On peut récrire cela sous une forme matricielle

$$(\phi I_n - A)x = 0,\ x = (x_1, \ldots, x_n)^t, A = (a_{ij})$$

En multipliant cela par la matrice des cofacteurs de $\phi I_n - A$, on obtient l'équation cherchée

$$f(\phi) := \det(\phi I_n - A) = 0$$

3.11. *Exercice* (lemme de Nakayama) Soient A un anneau local avec l'idéal maximal $\mathfrak{m}$, M un A-module de type fini. Supposons que $M = \mathfrak{m}M$. Alors $M = 0$.

Solution. En prenant $\phi = \mathrm{Id}$, $\mathfrak{a} = \mathfrak{m}$ dans 3.10, on obtient $(1 + \sum a_i)x = 0$ pour chaque $x \in M$. Or $1 + \sum a_i \in A^*$, d'où l'assertion.

3.12. *Lemme.* Sous les hypothèses de 3.7, b est entier sur A ssi $A[b] \subset B$ est un A-module de type fini.

Exercice.

3.13. Maintenant on peut prouver théorème 3.8. Par hypothèse, $A[b]$ est de type fini sur A; ensuite, b' est entier sur A donc sur $A[b]$, donc $M = A[b, b'] = A[b][b']$ est de type fini sur $A[b]$, donc M est de type fini sur A.

Définissons $\phi : M \longrightarrow M$ par $\phi(x) = (b + b')x$ et prenons $\mathfrak{a} = A$. Alors 3.10 nous dit que $b + b'$ est entier sur A. De même pour bb'.

3.14. *Corollaire.* Si $A \subset B \subset C$, B est entier sur A et C est entier sur B alors C est entier sur A.

Exercice.

3.15. *Lemme.* Soient $A \subset B$ des anneaux intègres, B entier sur A. Alors A est un corps ssi B l'est.

Supposons que A est un corps, $b \in B,\ b \neq 0$. Soit

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

une équation du degré minimal, donc $a_n \neq 0$. Alors

$$b(b^{n-1} + \ldots + a_{n-1}) = -a_n,$$

d'où

$$b \cdot\ [-a_n^{-1}(b^{n-1} + \ldots + a_{n-1})] = 1,$$

donc $b \in B^*$.

Par contre, si B est un corps, $a \in A,\ a \neq 0$, considérons $a^{-1} \in B$. Il est entier sur A, donc satisfait à une équation

$$a^{-n} + a_1 a^{-n+1} + \ldots a_n = 0,$$

donc

$$0 = 1 + a_1 a + \ldots + a_n a^n = 1 + a(a_1 + \ldots + a_n a^{n-1}),$$

donc

$$a^{-1} = -(a_1 + \ldots + a_n a^{n-1}) \in A,$$

cqfd.

3.16. *Corollaire.* Soient $A \subset B$ une extension entiere, $\mathfrak{p} \subset B$ un idéal premier, $\mathfrak{q} = A \cap \mathfrak{p}$. Alors $\mathfrak{p}$ est maximal ssi $\mathfrak{q}$ est maximal.

Exercice.

3.17. *Corollaire.* Soit $A \subset B$ une extension entiere. Soient $\mathfrak{q} \subset \mathfrak{q}' \subset B$ deux idéaux premiers tels que $\mathfrak{p} := \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Alors $\mathfrak{q} = \mathfrak{q}'$.

En effet, $A_\mathfrak{p} \subset B_\mathfrak{p}$ est une extension entiere, $\mathfrak{p}_\mathfrak{p} \subset A_\mathfrak{p}$ est maximal et $\mathfrak{p}_\mathfrak{p} = \mathfrak{q}_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{q}'_\mathfrak{p} \cap A_\mathfrak{p}$. Donc $\mathfrak{q}_\mathfrak{p} = \mathfrak{q}'_\mathfrak{p}$, d'où $\mathfrak{q} = \mathfrak{q}'$.

3.18. *Théorème.* Soient $A \subset B$ une extension entiere, $\mathfrak{p} \subset A$ un idéal premier. Alors il existe $\mathfrak{q} \subset B$ premier tel que $\mathfrak{p} = \mathfrak{q} \cap A$.

En effet, considérons l'extension entiere $A_\mathfrak{p} \subset B_\mathfrak{p}$. Soit $\mathfrak{m} \subset B_\mathfrak{p}$ un idéal maximal. D'après 3.16, $\mathfrak{m} \cap A_\mathfrak{p}$ est maximal, donc $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$.

Soient $\phi_A :\ A \longrightarrow A_\mathfrak{p},\ \phi_B :\ B \longrightarrow B_\mathfrak{p}$ les morphismes canoniques. Il en suit que $\mathfrak{p} = \phi_A^{-1}(\mathfrak{p}_\mathfrak{p}) = A \cap \phi_B^{-1}(\mathfrak{m}) := \mathfrak{q}$, cqfd.

3.19. Soit $F \supset \mathbb{Q}$ une extension finie. On appele *l'anneau des entiers dans* F la clôture intégrale de $\mathbb{Z}$ dans F.

(c) *Corps quadratiques*

3.20. Soit $F \supset \mathbb{Q}$ une extension de degré 2. Alors $F = \mathbb{Q}(\sqrt{d})$, où $d \in \mathbb{Z}$ est sans facteurs carrés (prouver!) Donc $F = \mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$.

Cette extension est galoisienne: le groupe de Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ contient deux éléments, $G = \{1, \sigma\}$, où $\sigma(\sqrt{d}) = -\sqrt{d}$.

Pour $\alpha = r+s\sqrt{d}$, on désigne par $t(\alpha) = \alpha+\sigma(\alpha) = 2r$, $N(\alpha) = \alpha\sigma(\alpha) = r^2-s^2d$ sa trace et sa norme.

Soit $R \subset F$ l'anneau des entiers.

3.21. *Lemme.* $\alpha \in R$ ssi $t(\alpha), N(\alpha) \in \mathbb{Z}$.

En effet, si $\alpha \in R$, $\sigma(\alpha) \in R$, donc $t(\alpha) \in \mathbb{Q}$ et est entier sur $\mathbb{Z}$, donc $t(\alpha) \in \mathbb{Z}$ d'après 3.9.1. Le même pour la norme.

Réciproquement, chaque $\alpha \in F$ satisfait à l'équation

$$(x - \alpha)(x - \sigma(\alpha)) = x^2 - t(\alpha)x + N(\alpha) = 0$$

Donc si $t(\alpha), N(\alpha) \in \mathbb{Z}$, α est entier sur $\mathbb{Z}$.

3.22. *Théorème.* Si $d \equiv 2, 3 \pmod 4$, $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Si $d \equiv 1 \pmod 4$, $R = \mathbb{Z} + \mathbb{Z}\gamma$, où

$$\gamma = \frac{-1 + \sqrt{d}}{2}$$

En effet, si $\alpha = r + s\sqrt{d} \in R$ alors $t(\alpha) = 2r = m \in \mathbb{Z}$ et $N(\alpha) = r^2 - s^2d \in \mathbb{Z}$. Il en suit que $4s^2d \in \mathbb{Z}$. Puisque d est sans facteurs carrés, $2s = n \in \mathbb{Z}$. Donc

$$m^2 - n^2d = 4(r^2 - s^2d) \equiv 0 \pmod 4$$

Si $d \equiv 3 \pmod 4$, il en suit que $m^2 + n^2 \equiv 0 \pmod 4$. Cela implique que m, n sont pairs, donc $r, s \in \mathbb{Z}$, donc $R \subset \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Puisque l'inclusion réciproque est évidente, $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Le même argument avec $d \equiv 2 \pmod 4$.

Maintenant supposons que $d \equiv 1 \pmod 4$. Alors

$$m^2 - n^2d \equiv m^2 - n^2 \equiv 0 \pmod 4,$$

d'où $m \equiv n \pmod 2$, donc

$$\alpha = \frac{m + n\sqrt{d}}{2} = \frac{m + n}{2} + n\frac{-1 + \sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\gamma$$

De l'autre côté, $t(\gamma) = -1$ et $N(\gamma) = (1 - d)/4 \in \mathbb{Z}$, donc $\gamma \in R$ et $R = \mathbb{Z} + \mathbb{Z}\gamma$.

3.23. *Analogie géométrique.*

(A) (arithmétique): $S = \mathbb{Z} \subset R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[y]/(y^2-d)$; $\sigma : R \xrightarrow{\sim} R$, $\sigma(\sqrt{d}) = -\sqrt{d}$;

(G) (géométrie): $S = \mathbb{C}[x] \subset R = S[y](y^2 - f(x)) = \mathbb{C}[x, y]/(y^2 - f(x))$, où $f(x) \in \mathbb{C}[x]$; $\sigma : R \xrightarrow{\sim} R$, $\sigma(y) = -y$.

(A): Un nombre premier $p \in \mathbb{Z}$, l'idéal premier $(p) \subset \mathbb{Z}$, $\pi :\ \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$;

(G): Un polynôme irréductible $x - \lambda \in \mathbb{C}[x]$ ($\lambda \in \mathbb{C}$); l'idéal premier $(x - \lambda) \subset \mathbb{C}[x]$; $\pi :\ \mathbb{C}[x] \longrightarrow \mathbb{C}[x]/(x - \lambda) \cong \mathbb{C},\ \pi(g(x)) = g(\lambda)$.

Décomposition d'un idéal en idéaux premiers

(G): $\mathbb{C} = \mathbb{C}[x]/(x - \lambda) \subset R/(x - \lambda)R$. Ici

$$R/(x - \lambda)R = \mathbb{C}[x, y]/(x - \lambda, y^2 - f(x)) \stackrel{\pi}{\sim} \mathbb{C}[y]/(y^2 - f(\lambda)),\ \pi(x) = \lambda$$

Donc on voit deux possibilités.

(NR) (cas non-ramifié): $f(\lambda) \neq 0$. Alors

$$\mathbb{C}[y]/(y^2 - f(\lambda)) \stackrel{\sim}{\longrightarrow} \mathbb{C}[y]/(y - \sqrt{f(\lambda)}) \oplus \mathbb{C}[y]/(y + \sqrt{f(\lambda)}) = \mathbb{C} \oplus \mathbb{C}$$

et

$$(x - \lambda)R = \mathfrak{P}\mathfrak{P}',$$

où

$$\mathfrak{P} = (x - \lambda, y - \sqrt{f(\lambda)})/(y^2 - f(x)) \subset R = \mathbb{C}[x, y]/(y^2 - f(x))$$

(on remarque que

$$y^2 - f(x) = y^2 - f(\lambda) - f(x) + f(\lambda) = (y - \sqrt{f(\lambda)})(y + \sqrt{f(\lambda)}) + (x - \lambda)g(x) \in (x - \lambda, y - \sqrt{f(\lambda)})),$$

et

$$\mathfrak{P}' = (x - \lambda, y + \sqrt{f(\lambda)})/(y^2 - f(x)) = \sigma(\mathfrak{P})$$

(R) (cas ramifié): $f(\lambda) = 0$. Alors

$$(x - \lambda)R = \mathfrak{P}^2,$$

où

$$\mathfrak{P} = (x - \lambda, y^2)/(y^2 - f(x)) \subset R$$

3.23.1. *Exercice.* Montrer que R coïncide avec la clôture intégrale de S dans $F = K(\sqrt{f}),\ K = \mathbb{C}(x)$. En conclure que R est intégralement clos.

(A): $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subset R/pR = \mathbb{Z}[y]/(p, y^2 - d)$. On a

$$\mathbb{Z}[y]/(p, y^2 - d) \stackrel{\sim}{\longrightarrow} \mathbb{F}_p[y]/(y^2 - \bar{d}),\ \bar{d} := d \pmod p$$

On a trois possibilités.

(a): $p \not| d$ et $p \neq 2$

(a1) = (NR) (cas non-ramifié): d est un résidu quadratique modulo p. Soit $a \in \mathbb{Z},\ a^2 \equiv d \pmod p$. Alors

$$\mathbb{F}_p[y]/(y^2 - \bar{d}) \stackrel{\sim}{\longrightarrow} \mathbb{F}_p[y]/(y - \bar{a}) \oplus \mathbb{F}_p[y]/(y + \bar{a}) \cong \mathbb{F}_p \oplus \mathbb{F}_p$$

et

$$pR = \mathfrak{P}\mathfrak{P}',$$

où

$$\mathfrak{P} = (p, \sqrt{d} - a) = (p, y - a)/(y^2 - d) \subset R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[y]/(y^2 - d)$$

et

$$\mathfrak{P}' = (p, \sqrt{d} + a) = (p, y + a)/(y^2 - d) = \sigma(\mathfrak{P})$$

(a2) (cas inert): d est non-résidu quadratique mod p, i.e. $\bar{d} \in \mathbb{F}_p^* - \mathbb{F}_p^{*2}$. Dans ce cas le polynôme $y^2 - \bar{d}$ est irréductible sur $\mathbb{F}_p$, on a

$$\mathbb{F}_p[y]/(y^2 - \bar{d}) \cong \mathbb{F}_{p^2}$$

et l'idéal

$$\mathfrak{P} = pR = (p, y^2 - d)/(y^2 - d) \subset R$$

est premier.

(b) = (R) (cas ramifié): $p \mid d$ ou $p = 2$. Si $p \mid d$,

$$R/pR \cong \mathbb{F}_p[y]/(y^2)$$

et

$$pR = \mathfrak{P}^2,$$

où

$$\mathfrak{P} = (p, \sqrt{d}) \subset R$$

Si $p = 2$ et $2 \not| \, d$, alors $\bar{d} \in \mathbb{F}_p^* = \mathbb{F}_p^{*2}$. Soit a comme dans (a1). Alors

$$pR = \mathfrak{P}^2,$$

où

$$\mathfrak{P} = (p, \sqrt{d} - a)$$

3.24. *Exercice* ("les nombres idéaux"). Considérons l'anneau des entiers $R = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{Q}[\sqrt{-5}]$. Il n'est pas factoriel. En effet,

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

dans R. Par contre, trouver des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_4 \subset R$ tels que

$$(3) = \mathfrak{p}_1\mathfrak{p}_2, \ (7) = \mathfrak{p}_3\mathfrak{p}_4$$

et

$$(1 + 2\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, \ (1 - 2\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$$

Solution. On a $R/(3) = \mathbb{F}_3[y]/(y^2 + \bar{5})$; $y^2 + \bar{5} = y^2 - 1 = (y - 1)(y + 1) \in \mathbb{F}_3[y]$, d'où

$$(3) = (3, \sqrt{-5} - 1)(3, \sqrt{-5} + 1) = \mathfrak{p}_1\mathfrak{p}_2$$

De même, $y^2+\bar{5}=(y-\bar{3})(y+\bar{3})\in\mathbb{F}_7[y]$, d'où

$$(7)=(7,\sqrt{-5}-3)(7,\sqrt{-5}+3)=\mathfrak{p}_3\mathfrak{p}_4$$

Après, on vérifie que $1+2\sqrt{-5}\in\mathfrak{p}_1\cap\mathfrak{p}_3$ et $1-2\sqrt{-5}\in\mathfrak{p}_2\cap\mathfrak{p}_4$, d'où

$$(1+2\sqrt{-5})=\mathfrak{p}_1\mathfrak{p}_3,\ (1-2\sqrt{-5})=\mathfrak{p}_2\mathfrak{p}_4$$

3.25. *Exercice.* Montrer que $R=\mathbb{Z}[\sqrt{5}]$ n'est pas intégrablement clos et n'est pas factoriel. Quelle est sa clôture intégrale R^c?

Idée:

$$4=2\cdot 2=(\sqrt{5}-1)(\sqrt{5}+1)$$

Qu'est-ce que c'est passe dans R^c?

Appendice. Encore un petit peu d'algèbre commutative

3.26. *Lemme.* Soit $A\subset B$ une extension entière, B étant intègre, $\mathfrak{b}\subset B$ une idéal. Si $\mathfrak{b}\neq 0$, alors $\mathfrak{a}:=\mathfrak{b}\cap A\neq 0$.

On peut supposer que $\mathfrak{b}\neq B$. Si $\mathfrak{b}\cap A=0$, soit $S:=A-\{0\}$; considérons la localisation $K:=A_S\subset B_S$. Ceci est une extension entière, K est un corps, donc B_S est un corps, c'est qui est impossible, car il contient un idéal propre $\mathfrak{b}_S$.

Variante. Soit $b\in\mathfrak{b}$ un élément nonnul,

$$b^n+a_1b^{n-1}+\ldots+a_{n-1}b+a_n=0$$

une équation de dependance intégrale de degré minimal sur A. Alors $a_n\neq 0$, et $a_n\in\mathfrak{a}$.

3.27. *Lemme.* Soit $A\subset B$ une extension entière, $\mathfrak{a}\subset A$ un idéal propre. Alors $\mathfrak{a}B\neq B$.

En effet, supposons au contraire que $\mathfrak{a}B=B$, donc $1=\sum_{i=1}^n a_ib_i$. En remplaçant B par $A[b_1,\ldots,b_n]$, on peut supposer que B est une A-module de type fini. Soit $\mathfrak{p}\supset\mathfrak{a}$ un idéal premier de A. Considérons l'extension $A_\mathfrak{p}\subset B_\mathfrak{p}$. On a $B_\mathfrak{p}=\mathfrak{p}B_\mathfrak{p}$, donc $B_\mathfrak{p}=0$ par Nakayama: impossible.

3.28. *Théorème* (Nullstellensatz de Hilbert en dimension 2). Chaque idéal maximal $\mathfrak{m}\subset A:=\mathbb{C}[x,y]$ est de la forme $\mathfrak{m}=(x-\lambda,y-\mu),\ (\lambda,\mu)\in\mathbb{C}^2$.

Démonstration. Chosissons un élément nonnul $f(x,y)\in\mathfrak{m}$. Écrivons f comme un polynôme en y:

$$f(x,y)=g(x)y^n+g_1(x)y^{n-1}+\ldots+g_n(x),\ g(x)\neq 0$$

On a deux possibilités. Si $g(x)\in\mathfrak{m}$, et λ est une racine de $g(x)$, alors $x-\lambda\in\mathfrak{m}$. Passons aux quotients $\bar{\mathfrak{m}}=\mathfrak{m}/(x-\lambda)\subset\bar{A}=A/(x-\lambda)\xrightarrow{\sim}\mathbb{C}[y]$. Alors $\bar{\mathfrak{m}}$ est un idéal maximal de $\bar{A}$, donc $\mathfrak{m}=(y-\mu)$, d'où $\mathfrak{m}=(x-\lambda,y-\mu)$.

Par contre, si $g\notin\mathfrak{m}$, considérons l'anneau $C=(A/(f))_g$ avec l'idéal maximal $\bar{\mathfrak{m}}_g:=(\mathfrak{m}/(f))_g$. Alors C est une extension entière de $B_g:=\mathbb{C}[x]_g$ donc $\mathfrak{m}_g\cap B_g$, étant un idéal maximal de B_g, est égale à $(x-\lambda)$ (o'u $\lambda\in\mathbb{C},\ g(\lambda)\neq 0$). Il en suit que $x-\lambda\in\mathfrak{m}$, et on finit l'argument comme dans le cas précédent.

§4. Ramification

Norme et trace

4.1. Soit $E \subset F$ une extension finie de corps de degré n. Pour $\alpha \in F$ considérons le morphisme de multiplication par α, $\mu_\alpha : F \longrightarrow F$, $\mu_\alpha(a) = \alpha a$. Ceci est un opérateur linéaire sur E considéré comme un espace linéaire sur F.

On définit

$$f_\alpha(x) := \det(xI_n - \mu_\alpha) \in F[x]$$

(le polynôme caractéristique de α);

$$N(\alpha) = N_{F/E}(\alpha) := \det(\mu_\alpha)$$

$$t(\alpha) = t_{F/E}(\alpha) = \mathrm{tr}(\mu_\alpha)$$

Donc

$$f_\alpha(x) = x^n - t(\alpha)x^{n-1} + \ldots + (-1)^n N(\alpha)$$

La norme est un homomorphisme de groupes $N : F^* \longrightarrow E^*$; la trace est un homomorphisme de groupes additifs $t : F \longrightarrow E$.

Transitivité. Si $F \subset K$ est une extension finie,

$$N_{K/E} = N_{F/E} \circ N_{K/F};\ t_{K/E} = t_{F/E} \circ t_{K/F}$$

4.2. *Exercice* (théorème de Hamilton - Cayley) $f_\alpha(\alpha) = 0$.

Utiliser la méthode de 3.10.

4.3. *Exercice.* Soit $g(x)$ le polynôme minimal unitaire de α. On a la tour $E \subset E(\alpha) \subset F$, d'où $n = me,\ m = [E(\alpha) : E] = \deg(g(x)),\ e = [F : E(\alpha)]$.

Montrer que $f_\alpha(x) = g(x)^e$.

4.4. *Extensions separables* (rappels) Soient $F \subset K$ une extension de corps de degré fini n, $F \subset C$ une extension de corps avec C algébriquement clos. Il existe $\leq n$ prolongements du plongement $F \subset C$ à un plongement $\sigma : K \hookrightarrow C$. S'il en existe n, l'extension $F \subset K$ est appelée separable.

Si $K \subset E$ est une extensions finie, E/F est separable ssi E/K et K/F le sont.

Un élément $\alpha \in K$ est dit separable (sur F) si son polynôme minimal $f(x)$ n'a pas de racines multiples (dans $\bar{F}$, ou dans n'importe quel corps C algébriquement clos contenant F). K est separable sur F ssi chaque $\alpha \in K$ est separable sur F.

Si K/F est separable, alors il existe $\alpha \in F$ tel que $K = F(\alpha)$.

Les conditions suivantes sont équivalentes:

(i) K/F est separable;

(ii) la fonction trace $t : K \longrightarrow F$ n'est pas identiquement 0;

(iii) la forme bilinéaire $K \otimes_F K \longrightarrow F$,

$$a \otimes b \mapsto t(ab) \tag{4.4.1}$$

est non-degenerée.

D'après (ii), si $\mathrm{char}(F) = 0$ alors K/F est separable, car $t(1) = n$.

4.5. Soit $K \subset L$ une extension separable de degré fini n. Soit $\bar{L}$ une clôture algébrique de L. Soient $\sigma_i : \ L \hookrightarrow \bar{L}, \ i = 1, \ldots, n$ les plongements distincts prolongeants le plongement $K \subset \bar{L}$; nous supposerons que σ_1 est égale au plongement donné $L \subset \bar{L}$.

Pour $\alpha \in L$ on désigne parfois $\alpha^{(i)} := \sigma_i(\alpha)$, donc $\sigma_1(\alpha) = \alpha$. Le séléments $\alpha^{(i)}$ sont appelés *les conjugués* de α.

Considérons le polynôme

$$f(x) = \prod_{i=1}^{n} (x - \alpha^{(i)})$$

Il appartient à $K[x]$ et coïncide avec le polynôme caractéristique de α. Il en suit que

$$N(\alpha) = \prod_i \ \alpha^{(i)} \text{ et } t(\alpha) = \sum_i \ \alpha^{(i)}$$

Par exemple, tous les $\alpha^{(i)}$ sont distincts ssi $L = K(\alpha)$ ssi $f(\alpha)$ est le polynôme minimal unitaire de α.

Le discriminant

4.6. Soit $K \subset L$ une extension de corps de degré n. Soient $\alpha_1, \ldots, \alpha_n \in L$. On pose

$$\Delta(\alpha_1, \ldots, \alpha_n) := \det(t(\alpha_i \alpha_j))$$

4.7. *Lemme.* (i) Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ alors $\alpha_1, \ldots, \alpha_n$ forment une base de L/K (c'est-à-dire, une base de L comme un K-espace vectoriel).

(ii) Réciproquement, si L/K est separable et $\alpha_1, \ldots, \alpha_n$ est une base de L/K, alors $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

En effet, si $\sum_i \ a_i \alpha_i = 0$ est une relation nontriviale, alors pour chaque j $\sum_i \ a_i t(\alpha_i \alpha_j) = 0$, donc $\det(t(\alpha_i \alpha_j) = 0$, ce qui prouve (i).

Réciproquement, si $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Alors il existent $a_1, \ldots, a_n \in K$, pas tous égaux à 0, tels que pour chaque j

$$\sum_i \ a_i t(\alpha_i \alpha_j) = 0$$

Supposons $\alpha_1, \ldots, \alpha_n$ est une base de L/K, et posons $\beta = \sum_i \ a_i \alpha_i \neq 0$. Alors $t(\beta \alpha_j) = 0$ pour chaque j, donc $t(\beta\gamma) = 0$ pour chaque γ, donc $t \equiv 0$. (À propos,

cela démontre que la forme bilinéaire $t(\alpha\beta)$ et dégénérée ssi $t \cong 0$, i.e. l'équivalence (ii) $\Leftrightarrow$ (iii) de 4.4.) Donc L/K ne peut être separable, ce qui prouve (ii).

4.8. *Lemme.* Soient $\alpha_1, \dots, \alpha_n$; $\beta_1, \dots, \beta_n$ deux bases de L/K, avec $\alpha_i = \sum_j a_{ij}\beta_j$. Alors

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \dots, \beta_n)$$

Exercice.

4.9. *Lemme.* Supposons que L/K est separable. Alors

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(\alpha_i^{(j)})^2$$

En effet, on a $t(\alpha_i\alpha_j) = \sum_p \alpha_i^{(p)}\alpha_j^{(p)}$. Posons $A = (t(\alpha_i\alpha_j))$, $B = (\alpha_i^{(j)})$. Alors $A = BB^t$.

4.10. *Lemme.* Soit L/K separable de degré n, $L = K(\beta)$. Alors $1, \beta, \dots, \beta^{n-1}$ est une base de L/K. Soit $f(x)$ le polynôme minimal unitaire de β. Alors

$$\Delta(1, \beta, \dots, \beta^{n-1}) = (-1)^{n(n-1)/2} N(f'(\beta))$$

En effet,

$$\det(\beta^{(i)j}) = \prod_{i<j} (\beta^{(j)} - \beta^{(i)})$$

(Vandermonde). Il en suit que

$$\Delta(1, \beta, \dots, \beta^{n-1}) = \prod_{i<j} (\beta^{(j)} - \beta^{(i)})^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\beta^{(j)} - \beta^{(i)})$$

D'un autre côté, $f(x) = \prod_i (x - \beta^{(i)})$, d'où $f'(\beta^{(j)} = \prod_{i \neq j} (\beta^{(j)} - \beta^{(i)})$, et $N(f'(\beta)) = \prod_j f'(\beta^{(j)})$.

Idéaux

4.11. Fixons un sous-corps $F \subset \mathbb{C}$ de degré fini n sur $\mathbb{Q}$. On remarque que l'extension $F/\mathbb{Q}$ est separable. Soit $R \subset F$ l'anneau des entiers.

Pour chaque $\alpha \in R$, tous ces conjugués $\alpha^{(i)}$ sont entiers sur $\mathbb{Z}$. Donc leur produit $N(\alpha) = \prod_i \alpha^{(i)}$ est entier sur $\mathbb{Z}$ et appartient à $\mathbb{Q}$, d'où $N(\alpha) \in \mathbb{Z}$. De même, $t(\alpha) \in \mathbb{Z}$.

Si $\alpha_1, \dots, \alpha_n \in F$, alors $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$; si $\alpha_1, \dots, \alpha_n \in R$, alors $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

Dans ce qui suit, "idéal" = idéal nonnul de R.

Exercice. Pour chaque $\beta \in F$ il existe $a \in \mathbb{Z}$, $a \neq 0$, tel que $a\beta \in R$.

4.12. *Lemme.* Chaque idéal $\mathfrak{a}$ contient une base de $F/\mathbb{Q}$.

En effet, soit $\alpha_1, \dots, \alpha_n$ une base arbitraire de $F/\mathbb{Q}$. Il existe $a \in \mathbb{Z},\ a \neq 0$, tel que tous $a\alpha_i \in R$. Choisissons un $b \in \mathfrak{a},\ b \neq 0$. Alors $\{ab\alpha_i\}$ est une base de $F/\mathbb{Q}$ contenue dans $\mathfrak{a}$.

4.13. *Lemme.* Soient $\mathfrak{a}$ un idéal, $\alpha_1, \dots, \alpha_n$ une base de $F/\mathbb{Q}$ contenue dans $\mathfrak{a}$ avec $|\Delta(\alpha_1, \dots, \alpha_n)|$ minimal.

Alors $\{\alpha_i\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}$, c'est-à-dire, $\mathfrak{a} = \oplus_i\ \mathbb{Z}\alpha_i$.

Remarquons que pour chaque base $\beta_1, \dots, \beta_n$ de $F/\mathbb{Q}$ contenue dans $\mathfrak{a}$, le nombre $|\Delta(\beta_1, \dots, \beta_n)|$ est un entier rationel > 0, donc une base avec ce nombre minimal bien existe.

Pour démontrer le lemme, considérons un élément arbitraire $\alpha \in \mathfrak{a}$. Alors $\alpha = \sum_i\ c_i\alpha_i,\ c_i \in \mathbb{Q}$, et il faut montrer tous $\gamma_i \in \mathbb{Z}$. Si ce n'est pas le cas, il existe $c_i \in \mathbb{Q} - \mathbb{Z}$. On peut supposer que $i = 1$.

On a $c_1 = m + \theta$, avec $m \in \mathbb{Z}$ et $0 < \theta < 1$. Posons

$$\beta_1 = \alpha - m\alpha_1 = \theta\alpha_1 + \sum_{i \geq 2}\ c_i\alpha_i,$$

$\beta_i = \alpha_i,\ i \geq 2$. Alors $\beta_1, \dots, \beta_n$ est aussi une base de $F/\mathbb{Q}$ contenue dans $\mathfrak{a}$ et

$$\Delta(\beta_1, \dots, \beta_n) = \theta^2\ \Delta(\alpha_1, \dots, \alpha_n)$$

(pourquoi?). Donc $|\Delta(\beta_1, \dots, \beta_n)| < |\Delta(\alpha_1, \dots, \alpha_n)|$, contrairement à l'hypothèse.

D'après ce lemme, chaque idéal $\mathfrak{a}$ contient une $\mathbb{Z}$-base $\alpha_1, \dots, \alpha_n$. Le nombre $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ ne depend pas du choix de la base, par 4.8; on le désigne $\Delta(\mathfrak{a})$ et appele *le discriminant* de $\mathfrak{a}$. Le discriminant de F est par définition $\delta_F := \Delta(R)$.

4.14. *Exercice.* Pour chaque idéal $\mathfrak{a}$, $\mathfrak{a} \cap \mathbb{Z} \neq 0$.

Solution. Choisissons $\beta \in \mathfrak{a},\ \beta \neq 0$. Il satisfait à une equation

$$\beta^k + a_1\beta^{k-1} + \ldots + a_k = 0,\ a_i \in \mathbb{Z}$$

On peut supposer que $a_k \neq 0$. Or, $a_k \in \mathfrak{a} \cap \mathbb{Z}$.

4.15. *Lemme.* Pour chaque idéal $\mathfrak{a}$ l'anneau quotient $R/\mathfrak{a}$ est fini.

En effet, il existe $a \in \mathbb{Z} \cap \mathfrak{a},\ a \neq 0$. Il suffit de montrer que $R/(a)$ est fini. Or, d'après 4.13, $R \cong \mathbb{Z}^n$ comme un groupe abéilien, donc $R/(a) \cong (\mathbb{Z}/a\mathbb{Z})^n$.

4.15.1. *Corollaire.* R est noetherien.

4.15.2. *Corollaire.* Chaque idéal premier nonnul $\mathfrak{p} \subset R$ est maximal.

En effet, $R/\mathfrak{p}$ est un anneau intègre fini, donc un corps.

Classes d'idéaux

4.16. *Lemme.* (i) Si $\mathfrak{a}$ est un idéal et $\beta \in F$, $\beta\mathfrak{a} \subset \mathfrak{a}$, alors $\beta \in R$.

(ii) Si $\mathfrak{a}, \mathfrak{b}$ sont des idéaux tels que $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ alors $\mathfrak{b} = R$.

En effet, $\mathfrak{a}$ est un $\mathbb{Z}$-module de type fini, donc β est entier sur $\mathbb{Z}$ d'après lemme 3.10, d'où (i).

Soit $a_1, \dots, a_n$ une base entiere de $\mathfrak{a}$. Si $\mathfrak{a} = \mathfrak{ab}$ alors $a_i = \sum_j \ b_{ij}a_j, \ b_{ij} \in B$. Il en suit que $\det(I_n - (b_{ij})) = 0$, d'où, en faisant le determinant, $1 \in \mathfrak{b}$, i.e. $\mathfrak{b} = R$.

4.17. Deux idéaux $\mathfrak{a}, \mathfrak{b}$ sont appelés équivalents, $\mathfrak{a} \sim \mathfrak{b}$, s'il existent $\alpha, \beta \in R$ nonnuls tels que $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Ceci est une relation d'équivalence (vérifier!). Les classes d'équivalence sont appelées les classes d'idéaux. L'ensemble de classes d'équivalence sera noté $Cl(F)$.

La multiplication d'idéaux $\mathfrak{a}, \mathfrak{b} \mapsto \mathfrak{ab}$ fournit sur $Cl(F)$ une structure d'un monoîde avec l'unité = la classe de R.

Les deux faits fondamentaux sont: (a) $Cl(F)$ est fini. (b) $Cl(F)$ est un groupe, appelé *le groupe de classes d'idéaux de* F. Cela sera prouvé plus tard. On désigne $h_F := \mathrm{Card}(Cl(F))$.

Exercice. $h_F = 1$ ssi R est principal.

4.18. *Lemme* (Hurwitz) Il existe $M \in \mathbb{Z}_{>0}$ ayant la proprieté suivante:

(P) pour chaque $\gamma \in F$ il existent un entier t, $1 \leq t \leq M$ et $\alpha \in R$ tels que $|N(t\gamma - \alpha)| < 1$.

Démonstration. Choisissons une $\mathbb{Z}$-base $\beta_1, \dots, \beta_n$ dans R. Alors elle est une $\mathbb{Q}$-base de F. Donc pour chaque $\gamma \in F$, $\gamma = \sum_i \ c_i\beta_i, \ c_i \in \mathbb{Q}$.

On a

$$N(\gamma) = \prod_j \ (\sum_i \ c_i\beta_i^{(j)})$$

Prenons la valeur absolue (tout est plongé dans $\mathbb{C}$): pour chaque j

$$|\sum_i \ c_i\beta_i^{(j)}| \leq (\max_i |c_i|) \ \sum_i \ |\beta_i^{(j)}|,$$

d'où

$$|N(\gamma)| \leq C \ (\max_i |c_i|)^n \tag{4.18.1}$$

où $C = \prod_j \ (\sum_i \ |\beta_i^{(j)}|)$. Choisissons un entier $m > C^{1/n}$ et posons $M = m^n$.

Écrivons $\gamma = \sum_i \ c_i\beta_i = \sum_i \ a_i\beta_i + \sum_i \ \theta_i\beta_i = [\gamma] + \{\gamma\}$, où $a_i \in \mathbb{Z}$ et $0 \leq \theta_i < 1$. Donc $[\gamma] \in R$.

Plongeons $\phi : \ F \hookrightarrow \mathbb{Q}^n \subset \mathbb{R}^n$, $\phi(\gamma) = (c_1, \dots, c_n)$. Alors $\phi(\{\gamma\})$ est contenu dans le cube unitaire $K = \{(c_1, \dots, c_n) \mid 0 \leq c_i \leq 1\}$. Découpons K en m^n petits cubes K_j de côté $1/m$.

Considérons les points $\phi(\{k\gamma\}, \ 1 \leq k \leq m^n + 1$. Alors, par le principe de Dirichlet, il existent $h, l, \ \ 1 \leq h, l \leq m^n + 1$ tels que $h > l$, et $\phi(\{h\gamma\})$ et $\phi(\{l\gamma\})$ appartiennent au même petit cube.

Écrivons $h\gamma = [h\gamma] + \{h\gamma\}, \ l\gamma = [h\gamma] + \{h\gamma\}$, et faisons la soustraction:

$$(h - l)\gamma = [h\gamma] - [l\gamma] + \{h\gamma\} - \{l\gamma\}$$

Posons $t = h - l,\ \alpha = [h\gamma] - [l\gamma],\ \delta = \{h\gamma\} - \{l\gamma\}$.

Alors $1 \leq t \leq m^n = M$, $\alpha \in R$ et $|N(\delta)| \leq C(1/m)^n < 1$, d'après (4.18.1), ce qui fournit l'assertion de lemme.

Corollaire. Pour chaques $a, b \in R,\ b \neq 0$, il existent un entier t, $1 \leq t \leq M$ et $c \in R$ tels que $|N(ta - bc)| < |N(b)|$.

En effet, on applique le lemme précédent à a/b.

4.19. *Théorème.* $Cl(F)$ est fini.

Soit $\mathfrak{a}$ un idéal. Pour chaque $a \in \mathfrak{a},\ a \neq 0$, $|N(a)|$ est un entier > 0. Choisissons un élément $b \in \mathfrak{a}$ nonnul tel que $|N(b)|$ est minimal.

Pour chaque $a \in \mathfrak{a}$ il existe un entier t, $1 \leq t \leq M$ tel que $|N(ta - bc)| < |N(b)|$ avec $c \in R$. Or, $ta - bc \in \mathfrak{a}$, d'où $ta - bc = 0$. Donc $M!\mathfrak{a} \subset (b)$. Posons $\mathfrak{b} := b^{-1}M!\mathfrak{a} \subset R$; ceci est un idéal, et $M!\mathfrak{a} = b\mathfrak{b}$.

Puisque $b \in \mathfrak{a}$, $M!b \in b\mathfrak{b}$, donc $M! \in \mathfrak{b}$. Or $(M!)$ est contenu dans un nombre fini d'idéaux, donc $\mathfrak{a}$ est équivalent à un idéal contenu dans un ensemble fini, cqfd.

4.20. *Lemme.* Si $\mathfrak{a}, \mathfrak{b}$ sont des idéaux, $a \in R$, $a\mathfrak{a} = \mathfrak{b}\mathfrak{a}$, alors $(a) = \mathfrak{b}$.

En effet, si $b \in \mathfrak{b}$ alors $ba^{-1}\mathfrak{a} \subset \mathfrak{a}$, donc $ba^{-1} \in R$. Donc $\mathfrak{b} \subset (b)$, d'où $a^{-1}\mathfrak{b} \subset R$ est un idéal.

Par hypothèse $\mathfrak{a} = a^{-1}\mathfrak{b}\mathfrak{a}$, donc $a^{-1}\mathfrak{b} = R$ d'après 4.16 (ii), d'où le lemme.

4.21. *Lemme.* Pour chaque idéal $\mathfrak{a}$ il existe un entier h, $1 \leq h \leq h_F$, tel que l'idéal $\mathfrak{a}^h$ est principal.

En effet, considérons les puissances $\mathfrak{a}^i,\ 1 \leq i \leq h_F + 1$. Parmi eux il existent des idéaux équivalents, i.e. il existent $i < j$ tels que $\mathfrak{a}^i \sim \mathfrak{a}^j$. Donc $(a)\mathfrak{a}^i = (b)\mathfrak{a}^j$, $a, b \in R$ nonnuls.

Posons $h = j - i$, $\mathfrak{b} = \mathfrak{a}^h$. On a $(a)\mathfrak{a}^i = (b)\mathfrak{b}\mathfrak{a}^i$, donc $ab^{-1}\mathfrak{a}^i \subset \mathfrak{a}^i$, donc $c := ab^{-1} \in R$. On a $c\mathfrak{a}^i = \mathfrak{b}\mathfrak{a}^i$, d'où $\mathfrak{b} = (c)$ par 4.20, cqfd.

4.22. *Théorème.* $Cl(F)$ est un groupe.

Exercice.

En particulier, pour chaque idéal $\mathfrak{a}$, l'idéal $\mathfrak{a}^{h_F}$ est principal.

Décomposition en idéaux premiers

4.23. *Lemme.* Si $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ alors $\mathfrak{b} = \mathfrak{b}$.

En effet, si $\mathfrak{a}^h = (a)$, alors, en multipliant l'hypothèse par $\mathfrak{a}^{h-1}$, on obtient $(a)\mathfrak{b} = (a)\mathfrak{c}$, d'où $\mathfrak{b} = \mathfrak{c}$.

4.24. *Lemme.* Si $\mathfrak{a} \subset \mathfrak{b}$ alors il existe $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

En effet, soit $\mathfrak{b}^h = (b)$. Alors $\mathfrak{b}^{h-1}\mathfrak{a} \subset (b)$, donc $\mathfrak{c} := b^{-1}\mathfrak{b}^{h-1}\mathfrak{a} \subset R$ est un idéal, et $\mathfrak{b}\mathfrak{c} = b^{-1}\mathfrak{b}^h\mathfrak{a} = \mathfrak{a}$.

4.24. *Lemme.* Chaque idéal $\mathfrak{a} \neq R$ est un produit d'idéaux premiers.

En effet, $\mathfrak{a}$ est contenu dans un idéal premier, $\mathfrak{a} \subset \mathfrak{p}$, donc $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$, $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{a} \neq \mathfrak{b}$. Si $\mathfrak{b} = R$, on a fini. Sinon, en procédant, on obtient une chaîne $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{c} \subset \ldots$; elle doit être finie car R est noetherien.

4.25. Soit $\mathfrak{p}$ un idéal premier. Considérons la chaîne $\mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots$. Pour chaque i, $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$. En effet, si $\mathfrak{p}^i = \mathfrak{p}^{i+1}$ alors $\mathfrak{p} = R$ d'après 4.23.

Soit $\mathfrak{a}$ un idéal arbitraire. Si $\mathfrak{a} \notin \mathfrak{p}$, on pose $\mathrm{ord}_{\mathfrak{p}}\mathfrak{a} = 0$. Sinon, il existe (car $R/\mathfrak{a}$ est fini par exemple) un entier $i \geq 1$ tel que $\mathfrak{a} \subset \mathfrak{p}^i$ mais $\mathfrak{a} \not\subset \mathfrak{p}^{i+1}$. Ceci définit une fonction dite "d'ordre"

$$\mathrm{ord}_{\mathfrak{p}} : \{\text{Idéaux de } R\} \longrightarrow \mathbb{N}$$

On peut dire que

$$\mathrm{ord}_{\mathfrak{p}}\mathfrak{a} = i \Leftrightarrow \mathfrak{a} = \mathfrak{p}^i\mathfrak{b},\ \mathfrak{b} \not\subset \mathfrak{p}$$

4.26. *Lemme.* (i) $\mathrm{ord}_{\mathfrak{p}}\mathfrak{p} = 1$

(ii) Si $\mathfrak{p}'$ est premier différent de $\mathfrak{p}$, $\mathrm{ord}_{\mathfrak{p}}\mathfrak{p}' = 0$

(iii) $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$

Exercice (pour (iii), utiliser $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \supset \mathfrak{a}$ ou $\mathfrak{p} \supset \mathfrak{b}$).

4.27. *Théorème* (Kummer, Dedekind) Pour chaque idéal $\mathfrak{a}$, on a une décomposition unique

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\mathfrak{a}}$$

Exercice.

Ramification

4.28. Soit $\mathfrak{p} \subset R$ un idéal premier. On a $\mathfrak{p} \cap \mathbb{Z} \neq 0$, donc $\mathfrak{p} \cap \mathbb{Z} = (p)$, où p est un nombre premier.

Le nombre $e = \mathrm{ord}_{\mathfrak{p}}\ (p)$ est appelé l'index de ramification de $\mathfrak{p}$.

L'anneau quotient $R/\mathfrak{p}$ est un corps fini, une extension de $\mathbb{F}_p$ de degré f, i.e. $\mathrm{Card}(R/\mathfrak{p}) = p^f$. Le nombre f est appelé le degré de $\mathfrak{p}$.

4.29. *Lemme.* Pour chaque e on a un isomorphisme (non canonique) de groupes abéliens $R/\mathfrak{p} \cong \mathfrak{p}^{e-1}/\mathfrak{p}^e$.

Il en suit que $\mathrm{Card}(\mathfrak{p}^{e-1}/\mathfrak{p}^e) = p^f$ et $\mathrm{Card}(R/\mathfrak{p}^e) = p^{ef}$.

En effet, $\mathfrak{p}^{e-1} \neq \mathfrak{p}^e$; choisissons $a \in \mathfrak{p}^e - \mathfrak{p}^{e-1}$. On affirme que $\mathfrak{p}^e = \mathfrak{p}^{e-1} + (a)$. En effet, $\mathfrak{p}^{e-1} + (a) \subset \mathfrak{p}^e$, donc le seul idéal premier contenant $\mathfrak{p}^{e-1} + (a)$ est $\mathfrak{p}$, d'où $\mathfrak{p}^{e-1} + (a) = \mathfrak{p}^{e'}$. Puisque $\mathfrak{p}^{e-1} + (a) \subset \mathfrak{p}^e$, $e' = e$.

Définissons un morphisme $\phi :\ R \longrightarrow \mathfrak{p}^{e-1}/\mathfrak{p}^e$, $\phi(b) = ab$. On a vu que ϕ est un epimorphisme. D'autre part, $b \in \mathrm{Ker}(\phi) \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(ab) \geq e \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(b) \geq 1$ (car $\mathrm{ord}_{\mathfrak{p}}(a) = e-1$). Donc $\mathrm{Ker}(\phi) = \mathfrak{p}$, i.e. $\mathfrak{p}$ induit un isomorphisme $R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^{e-1}/\mathfrak{p}^e$.

4.30. *Théorème.* Considérons la décomposition

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

Alors $\sum_{i=1}^{g} e_i f_i = n$. (Rappelons que $n = [F : \mathbb{Q}]$.)

4.31. *Lemme* (théorème des restes chinois) Soit A un anneau commutatif; soient $\mathfrak{a}_i,\ i = 1, \ldots, m$ des idéaux de A deux à deux premiers, c'est-à-dire, $\mathfrak{a}_i + \mathfrak{a}_j = A$ pour tous $i \neq j$. Posons $\mathfrak{a} := \prod_i \mathfrak{a}_i$.

Alors

$$A/\mathfrak{a} \cong \oplus_{i=1}^{m} A/\mathfrak{a}_i$$

Soit

$$\phi :\ A/\mathfrak{a} \longrightarrow \oplus_{i=1}^{m} A/\mathfrak{a}_i$$

le morphisme évident.

(a) ϕ est surjectif.

En effet, $\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = A$ (prouver!), donc il existent $a_1 \in \mathfrak{a}_1,\ b_1 \in \prod_{i=2}^{n} \mathfrak{a}_i$ tels que $a_1 + b_1 = 1$. On a $b_1 \equiv 1 \pmod{\mathfrak{a}_1}$ et $b_1 \equiv 0 \pmod{\mathfrak{a}_i}$ pour $i \geq 2$.

De même, pour chaque i il existe b_i tel que $b_i \equiv 1 \pmod{\mathfrak{a}_i}$ et $b_i \equiv 0 \pmod{\mathfrak{a}_j}$ pour $j \neq i$, ce qui entraîne l'assertion.

(a) Ker $\phi = \mathfrak{a}$.

Évidemment, Ker $\phi = \cap_{i=1}^{n} \mathfrak{a}_i$, donc il faut démontrer que $\cap_{i=1}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i$. Il est clair que $\cap_{i=1}^{n} \mathfrak{a}_i \supset \prod_{i=1}^{n} \mathfrak{a}_i$.

Maintenant faisons la recurrence par n. $n = 2$. Soit $a_1 + a_2 = 1,\ a_i \in \mathfrak{a}_i$. Pour $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2,\ a = aa_1 + aa_2 \in \mathfrak{a}_1\mathfrak{a}_2$.

Cas général. Par hypothèse de recurrence, $\cap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{a}_1 \cap \prod_{i=2}^{n} \mathfrak{a}_i$. Or, les idéaux $\mathfrak{a}_1$ et $\prod_{i=2}^{n} \mathfrak{a}_i$ sont premiers entre eux, donc, par le cas $n = 2$, $\mathfrak{a}_1 \cap \prod_{i=2}^{n} \mathfrak{a}_i = \prod_{i=1}^{n} \mathfrak{a}_i$.

Ceci entraîne le lemme.

4.32. *Preuve de 4.30.* Puisque $R \cong \mathbb{Z}^n$ comme un $\mathbb{Z}$-module, $\mathrm{Card}(R/(p)) = p^n$.

D'un autre côté, les idéaux $\mathfrak{p}_i^{e_i}$ sont deux à deux premiers (démontrer!), donc

$$R/(p) \cong \oplus_{i=1}^{g} R/\mathfrak{p}^{e_i},$$

d'où $\mathrm{Card}(R/(p)) = p^{\sum e_i f_i}$, cqfd.

Cas galoisien

4.33. Maintenant supposons que l'extension $F/\mathbb{Q}$ est normale, donc galoisienne. Soit $G = \mathrm{Gal}(F/\mathbb{Q})$. Considérons la décomposition

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \tag{4.33.1}$$

Donc $\{\mathfrak{p}_1, \dots, \mathfrak{p}_g\}$ est l'ensemble des idéaux premiers contenants p.

4.34. *Lemme.* G agit transitivement sur l'ensemble $\{\mathfrak{p}_1, \dots, \mathfrak{p}_g\}$, c'est-à-dire, pour chaques i, j il existe $\sigma \in G$ tel que $\mathfrak{p}_j = \sigma\mathfrak{p}_i$.

Supposons au contraire qu'il existe un idéal premier $\mathfrak{p} \ni p$, $\mathfrak{p} \notin \{\sigma\mathfrak{p}_i \mid \sigma \in G\}$. D'après le théorème des restes chinois il existe $a \in R$, $a \equiv 0 \pmod{\mathfrak{p}}$, $a \equiv 1 \pmod{\sigma\mathfrak{p}_i}$ pour chaque $\sigma \in G$.

La norme

$$N(a) = \prod_{\sigma \in G} \sigma a \in \mathfrak{p} \cap \mathbb{Z} = (p) \subset \mathfrak{p}_i,$$

donc il existe $\sigma \in G$ tel que $\sigma a \in \mathfrak{p}_i$, d'où $a \in \sigma^{-1}\mathfrak{p}_i$, contrairement à l'hypothèse sur a.

4.35. *Théorème.* Dans la décomposition (4.33.1) tous e_i sont égaux, disons à e, et tous f_i sont égaux, disons à f. Donc $efg = n$, et la décomposition (4.33.1) devient

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i^e \tag{4.35.1}$$

En effet, pour chaque i, j, $\mathfrak{p}_i = \sigma\mathfrak{p}_j$, donc σ établit un isomorphisme des corps des restes $R/\mathfrak{p}_i \xrightarrow{\sim} R/\mathfrak{p}_j$, d'où $f_i = f_j$.

De plus, agissons sur (4.33.1) par σ:

$$(p) = \prod_k (\sigma\mathfrak{p}_k)^{e_k},$$

d'où $e_i = e_j$ par l'unicité de la décomposition en idéaux premiers.

4.36. Pour un idéal premier $\mathfrak{p}$, le sous-groupe stabilisateur $G_\mathfrak{p} = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\}$ est appelé *le groupe de décomposition* de $\mathfrak{p}$.

D'après 4.34 et 4.35, les sous-groupes $G_{\mathfrak{p}_i}$ sont tous conjugués, et $\mathrm{Card}(G_{\mathfrak{p}_i}) = n/g = ef$.

On a le morphisme évident

$$\pi_\mathfrak{p} : \ G_\mathfrak{p} \longrightarrow \mathrm{Gal}((R/\mathfrak{p})/\mathbb{F}_p)$$

(où $\mathfrak{p} \cap \mathbb{Z} = (p)$).

Le noyau $I_\mathfrak{p} = \mathrm{Ker}\ \pi_\mathfrak{p} \subset G_\mathfrak{p}$ est appelé *le groupe d'inertie* de $\mathfrak{p}$.

4.37. *Théorème.* Le morphisme $\pi_\mathfrak{p}$ est surjectif.

Il en suit que $e = \mathrm{Card}(I_{\mathfrak{p}_i})$ (pour n'importe quel i), et

$$\mathrm{Gal}((R/\mathfrak{p})/\mathbb{F}_p) \cong G_\mathfrak{p}/I_\mathfrak{p} \tag{4.37.1}$$

Si $e = 1$, le nombre premier p est appelé *non-ramifié* dans F.

Si c'est le cas, la décomposition (4.35.1) est particulierement simple:

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i,\ g = n/f \tag{4.37.2}$$

Plus généralement, soient $K/\mathbb{Q}$ une extension finie, $A \subset K$ l'anneau des entiers, L/K une extension finie galoisienne, $B \subset L$ la clôture intégrale de A dans L, $G = \mathrm{Gal}(L/K)$.

Soient $\mathfrak{p} \subset A$ un idéal premier (sous-entendu: nonnul), $\mathfrak{q} \subset B$ un idéal premier au-dessus de $\mathfrak{p}$, $G_\mathfrak{q} = \{\sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q}\}$ le groupe de décomposition.

On utilisera une notation $k(\mathfrak{p}) := A/\mathfrak{p}$; donc $k(\mathfrak{q}) = B/\mathfrak{q}$.

On veut démontrer 4.37 sous une forme plus générale:

4.38. *Théorème.* Le morphisme canonique

$$\pi_\mathfrak{q} = \pi_{L/K;\mathfrak{q}} :\ G_\mathfrak{q} \longrightarrow \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$$

est surjectif.

On remarque d'abord que toute la théorie *précédante* 4.37 reste valable avec l'extension $\mathbb{Q} \subset F$ remplacée par $K \subset L$.

Posons $L' = L^{G_\mathfrak{q}}$, donc $G_\mathfrak{q} = \mathrm{Gal}(L/L')$,

$$B' = \text{la clôture intégrale de } A \text{ dans } L' = B \cap L',$$

$\mathfrak{q}' = \mathfrak{q} \cap B'$. Alors $\mathfrak{q}'$ est un *unique* idéal premier de B au-dessus de $\mathfrak{q}$ d'après une généralisation de 4.34.

4.39. *Lemme.* L'injection canonique $i :\ k(\mathfrak{p}) \hookrightarrow k(\mathfrak{q}')$ est l'égalite.

Soit $\sigma \in G - G_\mathfrak{q}$; alors $\mathfrak{q} \neq \sigma\mathfrak{q}$, donc $\sigma^{-1}\mathfrak{q} \neq \mathfrak{q}$. Il en suit que

$$\mathfrak{q}'_\sigma := \sigma^{-1}\mathfrak{q} \cap B' \neq \mathfrak{q}',$$

puisque $\mathfrak{q}$ est l'unique idéal premier au-dessus de $\mathfrak{q}'$.

Soient $\bar{x} \in k(\mathfrak{q}')$ un élément arbitraire, $x \in B'$, $x \pmod{\mathfrak{q}'} = \bar{x}$.

Par le théorème des restes chinois il existe $y \in B'$ tel que $y \equiv x \pmod{\mathfrak{q}'}$ et $y \equiv 1 \pmod{\mathfrak{q}'_\sigma}$ pour tous $\sigma \in G - G_\mathfrak{q}$. Donc $\sigma y \equiv 1 \pmod{\mathfrak{q}'}$ pour tous $\sigma \in G - G_\mathfrak{q}$.

Il en suit que sa norme

$$z := N_{L'/K}(y) = \prod_{\tau \in G/G_\mathfrak{q}} \tau y \equiv x \pmod{\mathfrak{q}};$$

Or $z \in A$, donc $\bar{x} = i(z \bmod \mathfrak{p})$, cqfd.

Nous aurons besoin d'un fait standard de la théorie de Galois:

4.40. *Lemme.* Soient L/K une extension normale, $\bar{L} \supset L$ une clôture algébrique; $x \in L$, $f(t) \in K[t]$ le polynôme irréductible de x. Donc toutes les racines de $f(t)$ dans $\bar{L}$ appartiennent à L.

Alors $G := \mathrm{Aut}(L/K)$ agit transitivement sur l'ensemble de racines de $f(t)$.

En effet, si y, y' sont deux racines de f, il existe un unique isomorphisme $h : K(y) \xrightarrow{\sim} K(y')$ au-dessus de K tel que $h(y) = y'$. On peut prolonger h en un plongement $g : L \longrightarrow \bar{L}$; puisque L/K est normale, $g(L) = L$.

4.41. Revenons au théorème 4.38. Le lemme 4.39 montre qu'il suffit de supposer que $G = G_{\mathfrak{q}}$.

L'extension $k(\mathfrak{p}) \subset k(\mathfrak{q})$ est une extension de corps finis, donc $k(\mathfrak{q}) = k(\mathfrak{p})(\bar{x})$ (il suffit de prendre pour $\bar{x}$ un générateur du groupe cyclique $k(\mathfrak{q})^*$).

Soit $x \in B$, $x \pmod{\mathfrak{q}} = \bar{x}$. Soit $f(t)$ le polynôme irréductible unitaire de x sur K. f se décompose en facteurs linéaires sur L; toutes les racines de f sont conjuguées à x, donc ils sont entiers sur A, donc ils appartiennent à B. Il en suit que $f(t) \in (B \cap K)[t] = A[t]$.

Soit $\bar{f}(t) \in k(\mathfrak{p})$ sa réduction; elle se décompose en facteurs linéaires dans $k(\mathfrak{q})$: les racines de $\bar{f}(t)$ sont les réductions modulo $\mathfrak{q}$ des racines de f.

Soit $g(t)$ le polynôme irréductible unitaire de $\bar{x}$ sur $k(\mathfrak{p})$; g divise $\bar{f}$, donc $g(t)$ se décompose en facteurs linéaires dans $k(\mathfrak{q})[t]$ (ce que nous savons déjà, l'extension $k(\mathfrak{q})/k(\mathfrak{p})$ étant galoisienne). Il en suit que chaque racine de g dans $k(\mathfrak{q})$ est la réduction modulo $\mathfrak{q}$ d'une racine de f.

Maintenant, si $\sigma \in \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$, $\sigma(\bar{x}) = \bar{y}$ où $\bar{y}$ est une racine de g. Si y est une racine de f dont la réduction est $\bar{x}$, il existe $\tau \in G$ tel que $\tau x = y$. Alors $\pi_{\mathfrak{q}}(\tau) = \sigma$, ce qui prouve le théorème.

§5. Corps cyclotomiques

Cas $\mathbb{Q}(\zeta_p)$

5.1. Soit p un nombre premier, $\zeta = e^{2\pi i/p}$ une racine primitive p-ième de l'unité. Elle satisfait à l'équation $f_p(\zeta) = 0$, où

$$f(t) = f_p(t) = 1 + t + \ldots + t^{p-1}$$

Considérons le corps $L = \mathbb{Q}(\zeta)$.

Nous savons déjà (cf. 3.6) que $f_p(t)$ est irrédictible sur $\mathbb{Q}$, donc $L = \mathbb{Q}[t]/(f_p)$, $[L : \mathbb{Q}] = p - 1$.

Dans $L[t]$ le polynôme $f(t)$ se décompose en facteurs linéaires

$$f(t) = \prod_{i=1}^{p-1} (t - \zeta^i) \tag{5.1.1}$$

Il en suit que $L/\mathbb{Q}$ est normale, i.e. galoisienne.

Le groupe de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ est isomorphe à $\mathbb{F}_p^*$, donc cyclique. En effet, l'automorphisme $\sigma_a \in G$ correspondant à $a \in \mathbb{F}_p^*$ envoie ζ en ζ^a.

5.2. Soit R l'anneau des entiers dans L; il est clair que $R \supset \mathbb{Z}[\zeta]$. Nous verrons plus tard que $R = \mathbb{Z}[t]$.

Le lemme suivant est facile mais important.

Lemme. Pour chaques $i, j,\ 1 \leq i, j \leq p - 1$,

$$\epsilon_{ij} := \frac{1 - \zeta^i}{1 - \zeta^j} \ \in R^*$$

En effet, il existe $a \in \mathbb{Z}, 1 \leq a \leq p - 1$ tel que $i \equiv aj \pmod{p}$, d'où

$$\epsilon_{ij} = 1 + \zeta^j + \ldots + \zeta^{(a-1)j}$$

5.3. En substituant $t = 1$ dans (5.1.1), on obtient

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i),$$

d'où

$$p = \epsilon\ (1 - \zeta)^{p-1},\ \epsilon \in R^* \tag{5.3.1}$$

Par contre, $1 - \zeta \notin R^*$, parce que sinon, p serait inversible dans R, donc dans $\mathbb{Z}$ (cf. 3.9.3, 3.15), ce qui n'est pas le cas.

Considérons l'idéal $\mathfrak{p} = (1-\zeta) \subset R$; (5.3.1) implique

$$(p) = \mathfrak{p}^{p-1} \tag{5.3.2}$$

Puisque (p) est un produit de $\leq [L:\mathbb{Q}]$ idéaux premiers dans R, on en conclut que $\mathfrak{p}$ est premier.

(À propos, on a prouvé encore une fois que $[L:\mathbb{Q}] = p-1$, car dans l'argument précédent on n'a utilisé que l'algébricité de L sur $\mathbb{Q}$.)

Dans l'égalite $efg = p-1$ on a $g = p-1$; on en conclut que $e = 1,\ f = 1$, i.e. $k(\mathfrak{p}) = R/\mathfrak{p} = \mathbb{F}_p$.

5.4. *Théorème.* $R = \mathbb{Z}[\zeta]$.

Rémarquons que

$$\mathbb{Z}[\zeta]/(\zeta-1) = \mathbb{Z}[t]/(t-1, f(t)) = \mathbb{Z}/(f(1)) = \mathbb{Z}/(p)$$

On peut déjà conclure que l'inclusion $\mathbb{Z}[\zeta] \hookrightarrow R$ induit un isomorphisme

$$\mathbb{Z}[\zeta]/(\zeta-1) \xrightarrow{\sim} R/(\zeta-1) = R/\mathfrak{p}$$

Donc pour chaque $x \in R$ il existent $\alpha \in \mathbb{Z}[\zeta]$ et $y \in R$ tels que $x = \alpha + (\zeta-1)y$. En faisant la même chose avec y, etc., on voit qu'il existe $\beta \in \mathbb{Z}[\zeta]$ tel que $x \equiv \beta \pmod{\mathfrak{p}^{p-1}}$. Or $\mathfrak{p}^{p-1} = pR$, donc

$$x \equiv \beta \pmod{pR}$$

Il reste à montrer que $pR \subset \mathbb{Z}[\zeta]$.

Considérons la fonction trace $tr = tr_{L/\mathbb{Q}}$. Remarquons que

$$tr(\zeta^i) = \sum_{a=1}^{p-1} \zeta^{ai} = -1 \text{ si } i \not\equiv 0 \pmod{p};\ p-1 \text{ si } i \equiv 0 \pmod{p}$$

Soit $x = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2} \in R,\ a_i \in \mathbb{Q}$. Alors

$$tr(x\zeta) = -\sum_{j=0}^{p-2} a_j \in \mathbb{Z}$$

et pour chaque i, $0 \leq i \leq p-2$,

$$tr(x\zeta^{-i}) = -\sum_{j=0}^{p-2} a_j + (p-1)a_i \in \mathbb{Z}$$

d'où $pa_i \in \mathbb{Z}$, i.e. $px \in \mathbb{Z}[\zeta]$, cqfd.

Cas $\mathbb{Q}(\zeta_m)$

5.5. Soient m un entier, $m \geq 1$. Dorénavant on fixe les notations suivantes: $\zeta = \zeta_m = e^{2\pi i/m}$, $L = \mathbb{Q}(\zeta)$, $R \subset L$ l'anneau des entiers.

Le corps L est le corps de décomposition du polynôme

$$t^m - 1 = \prod_{i=0}^{m-1} (t - \zeta^i), \tag{5.5.1}$$

donc l'extension $L/\mathbb{Q}$ est normale. Soit $G = \mathrm{Gal}(L/\mathbb{Q})$.

Si $g \in G$, $g(\zeta) = \zeta^{\theta(g)}$, $\theta(g) \in (\mathbb{Z}/m\mathbb{Z})^*$. Ceci définit un homomorphisme

$$\theta : \ G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \tag{5.5.2}$$

Il est clair que θ est un monomorphisme.

Suivant l'usage, on définit la fonction d'Euler $\phi(m) := \mathrm{Card}(\mathbb{Z}/m\mathbb{Z})^*$.

Corollaire. $[L : \mathbb{Q}] \mid \phi(m)$.

On verra plus tard que θ est un isomorphisme.

5.6. *Polynômes cyclotomiques.* On définit

$$\Phi_m(t) = \prod_{(a,m)=1,\ 1\leq a<m} (t - \zeta_m^a)$$

Lemme.

$$t^m - 1 = \prod_{d|m} \Phi_d(t)$$

En effet,

$$t^m - 1 = \prod_{i=0}^{m-1} (t - \zeta_m^i) = \prod_{d|m} \prod_{(i,m)=d} (t - \zeta_m^i)$$

Si $(i, m) = d$, $j = i/d$, alors $(j, m) = 1$, donc $\zeta_m^i = \zeta_m^{dj} = \zeta_{m/d}^j$, d'où

$$\prod_{(i,m)=d} (t - \zeta_m^i) = \prod_{(j,m)=1} (t - \zeta_{m/d}^j) = \Phi_{m/d}(t),$$

d'où l'assertion.

Corollaire. $\Phi_m(t) \in \mathbb{Z}[t]$.

Prouvons cela par récurrence sur m. Le cas $m = 1$ est trivial. Par contre, $\Phi_m(t) = (t^m - 1)/f(t)$, où $f(t) \in \mathbb{Z}[t]$ est un polynôme unitaire, par hypothèse de recurrence, d'où $\Phi_m(t) \in \mathbb{Z}[t]$.

Autre preuve: les coéfficients sont entiers sur $\mathbb{Z}$. D'un autre côté, ses racines sont permutées par G, donc ses coéfficients sont invariants par G, donc ils appartiennent à $\mathbb{Q}$, donc ils habitent dans $\mathbb{Z}$.

5.7. *Lemme.* Soit p un nombre premier ne divisant pas m. Soit $\mathfrak{p} \subset R$ un idéal premier contenant p.

Alors les classes des éléments $\zeta^i,\ 0 \leq i \leq m-1$, dans $k(\mathfrak{p}) = R/\mathfrak{p}$ sont toutes distinctes.

Si f est le degré de $\mathfrak{p}$ (i.e. $f = [k(\mathfrak{p}) : \mathbb{F}_p]$) alors $p^f \equiv 1 \pmod{m}$.

En effet, (5.5.1) implique

$$m = \prod_{i=0}^{m-1} (1 - \zeta^i)$$

Or $m \not\equiv 0 \pmod{p}$, d'où $\zeta^i \not\equiv 1 \pmod{\mathfrak{p}}$ pour chaque $i, 0 \leq i \leq m-1$. Ceci entraine la première assertion.

Il en suit que les puissances $\zeta^i,\ 0 \leq i \leq m-1$ forment un sous-groupe de $k(\mathfrak{p})^*$ d'ordre m, donc $m \mid \mathrm{Card}(k(\mathfrak{p})^*) = p^f - 1$.

5.8. *Théorème.* $\Phi_m(t)$ est irréductible.

Démonstration (van der Waerden) Rappelons que le polynôme irréductible unitaire $g(t)$ (sur $\mathbb{Q}$) d'un nombre entier algébrique α appartient à $\mathbb{Z}[t]$ (en effet, toutes ces racines, étant conjuguées à α, sont entiers sur $\mathbb{Z}$, donc ces coéfficients sont entiers est appartient à $\mathbb{Q}$, donc à $\mathbb{Z}$).

Soit $f(t) \in \mathbb{Z}[t]$ le polynôme irréductible unitaire de ζ sur $\mathbb{Q}$. Puisque $\Phi_m(\zeta) = 0$, $f(t) \mid \Phi_m(t)$.

(a) Pour chaque $p \not| m$, $f(\zeta^p) = 0$.

En effet, $x^m - 1 = f(t)g(t) \in \mathbb{Z}[t]$. Supposons que $f(\zeta^p) \neq 0$. Alors $g(\zeta^p) = 0$.

Soit $\mathfrak{p}$ un idéal premier de R au-dessus de p, donc $k(\mathfrak{p}) = R/\mathfrak{p} \supset \mathbb{Z}/(p) = \mathbb{F}_p$. Considérons sa réduction $\bar{f}(t) \in \mathbb{F}_p[t]$. On a

$$t^m - 1 = \bar{f}(t)\bar{g}(t) \in \mathbb{F}_p[t]$$

Par hypothèse, $\bar{g}(\zeta^p) = 0$. Or $\bar{g}(\zeta^p) = \bar{g}(\zeta)^p$, d'où $\bar{g}(\zeta) = 0$.

D'après 5.7, toutes les racines de $t^m - 1$ dans $k(\mathfrak{p})$ sont distinctes, donc $\bar{f}(t) \neq 0$: contradiction.

(b) Pour chaque a premier à m, $f(\zeta^a) = 0$.

En effet, choisissons un premier p divisant a. D'après (a), $f(\zeta^p) = 0$. Il en suit que le polynôme irréductible $g(t)$ de ζ^p divise $f(t)$. Maintenant repeter l'argument (a) avec un premier q divisant $b = a/p$, etc.

Finalement, (b) implique que $\Phi_m(t) \mid f(t)$, donc ces deux polynômes sont égaux.

Corollaire. $[L : \mathbb{Q}] = \phi(m)$ et $\theta :\ G \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^*$.

5.9. *Lemme.* Soient $K/\mathbb{Q}$ une extension de degré fini n, $S \subset K$ l'anneau des entiers, $a_1, \ldots, a_n$ une $\mathbb{Q}$-base de K appartenant à S. Notons par Δ le discriminant $\Delta(a_1, \ldots, a_n)$.

Alors $\Delta S \subset \oplus_{i=1}^n \mathbb{Z}a_i$.

En effet, soit $x = \sum_i b_i a_i \in S,\ b_i \in \mathbb{Q}$. On a $t(xa_j) = \sum_i b_i t(a_i a_j)$ (ici $t = tr_{K/\mathbb{Q}}$. Or $t(xa_j), t(a_i a_j) \in \mathbb{Z}$, d'où $\Delta b_i = \det(t(a_p a_q))b_i \in \mathbb{Z}$ (expliquer!) Donc $\Delta x \in \oplus_{i=1}^n \mathbb{Z}a_i$.

5.10. *Lemme.* Posons $\Delta := \Delta(1, \zeta, \dots, \zeta^{\phi(m)-1})$. On a $\Delta \mid m^{\phi(m)}$.

On a $t^m - 1 = \Phi_m(t)g(t)$, d'où

$$mt^{m-1} = \Phi'_m(t)g(t) + \Phi_m(t)g'(t),$$

donc

$$m\zeta^{m-1} = \Phi'(\zeta)g(\zeta)$$

Prenons la norme: on a $N(\zeta) = \pm 1,\ N(\Phi'(\zeta)) = \pm\Delta$ (voir 4.10). Donc $\Delta N(g(\zeta)) = \pm m^{\phi(m)}$.

5.11. *Lemme.* Soit p un premier ne divisant pas m. Pour chaque $x \in R$ il existe $\alpha \in \mathbb{Z}[\zeta]$ tel que $x \equiv \alpha \pmod{pR}$.

D'après le lemme précédent, $p \not\mid \Delta$. Donc il existe $\Delta' \in \mathbb{Z}$ tel que $\Delta\Delta' \equiv 1 \pmod{p}$. Donc $x \equiv \Delta'\Delta x \pmod{pR}$, avec $\Delta x \in \mathbb{Z}[\zeta]$.

5.12. *Corollaire.* Si $p \not\mid m$ et $p^n \equiv 1 \pmod{m}$ alors pour chaque $x \in R$, $x^{p^n} \equiv x \pmod{pR}$.

On a $x \equiv \alpha \pmod{pR}$ où $\alpha = \sum_i a_i\zeta^i,\ a_i \in \mathbb{Z}$; donc

$$x^p \equiv (\sum_i a_i\zeta^i)^p \equiv \sum_i a_i^p\zeta^{pi} \equiv \sum_i a_i\zeta^{pi} \pmod{pR}$$

En itérant n fois, en tenant compte que $\zeta^{p^n} = \zeta$, on obtient l'assertion.

5.13. *Corollaire.* Si $p \not\mid m$, chaque idéal premier $\mathfrak{p} \subset R$ au-dessus de (p) est nonramifié.

Supposons le contraire, donc $p \in \mathfrak{p}^2$. Soit $x \in \mathfrak{p} - \mathfrak{p}^2$. On a

$$x^{p^n} \equiv x \pmod{pR} \equiv x \pmod{\mathfrak{p}^2}$$

puisque $p^n \geq 2$, $x \in \mathfrak{p}^2$: contrairement à l'hypothèse.

5.14. Pour un nombre premier p, $p \not\mid m$, on designe par $\sigma_p \in G$ l'élément $\sigma_p(\zeta) = \zeta$.

Lemme. Pout tous $x \in R$, $\sigma_p(x) \equiv x^p \pmod{pR}$.

En effet, $x \equiv \alpha \pmod{pR}$ où $\alpha = \sum_i a_i\zeta^i,\ a_i \in \mathbb{Z}$, d'où

$$\sigma^p(x) \equiv \sigma_p(\alpha) = \sum_i a_i\zeta^{pi} \equiv (\sum_i a_i\zeta^i)^p \equiv x^p \pmod{pR}$$

Corollaire. Si $\mathfrak{p} \subset R$ est un idéal premier au-dessus de (p), alors $\sigma_p(\mathfrak{p}) = \mathfrak{p}$.

En effet, pour $x \in \mathfrak{p}$,

$$\sigma_p(x) \equiv x^p \pmod{pR} \equiv\equiv x^p \pmod{\mathfrak{p}} \equiv 0 \pmod{\mathfrak{p}},$$

d'où $\sigma_p(\mathfrak{p}) \subset \mathfrak{p}$. Il en suit que $\sigma_p(\mathfrak{p}) = \mathfrak{p}$ car $\sigma_p(\mathfrak{p})$ est maximal.

5.15. *Théorème.* Soient $p \not| m$, f un entier positif minimal tel que $p^f \equiv 1 \pmod{m}$. Alors la décomposition de (p) en idéaux premiers dans R est de la forme

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i$$

où chaque $\mathfrak{p}_i$ a le degré f, donc $g = \phi(m)/f$.

On sait déjà que les $\mathfrak{p}_i$ sont nonramifiés, donc $e = 1$. Soit $\mathfrak{p} = \mathfrak{p}_i$. Il nous ne reste qu'à montrer que $f' := [k(\mathfrak{p}) : \mathbb{F}_p]$ est égal à f.

On a $p^{f'} = \mathrm{Card}(k(\mathfrak{p}))$, et f' est un nombre positif minimal tel que pour chaque $x \in R$, $x^{p^{f'}} \equiv x \pmod{\mathfrak{p}}$ (en tenant compte que $k(\mathfrak{p})^*$ est cyclique).

D'un autre côté, $\sigma_p^f = 1$, est de plus f est égale à l'ordre de σ_p.

Pour chaque $x \in R$ on a

$$x = \sigma_p^f(x) \equiv x^{p^f} \pmod{\mathfrak{p}},$$

d'où $f' \leq f$. D'autre part, $\zeta^{p^{f'}} \equiv \zeta \pmod{\mathfrak{p}}$, donc $\zeta^{p^{f'}} = \zeta$ vu lemme 5.7. Il en suit que $\sigma_p^{f'} = 1$, donc $f \leq f'$. On conclut que $f' = f$, cqfd.

Corollaire. Le groupe de décomposition $G_{\mathfrak{p}}$ coïncide avec le groupe cyclique d'ordre f engendré par σ_p.

En effet, on sait que $\sigma_p \in G_{\mathfrak{p}}$ (cf. corollaire 5.14), et les deux groupes en question ont le même ordre f.

Réciprocité quadratique

5.16. Soient $p > 2$ un nombre premier, $L = \mathbb{Q}(\zeta)$, $\zeta = \zeta_p$, R l'anneau des entiers dans L. On pose $p^* = (-1)^{(p-1)/2}$.

Lemme. p^* est le carré dans R, c'est-à-dire, il existe $\tau \in R$ tel que $\tau^2 = p^*$.

En effet, on le sait déjà, grace aux sommes de Gauss (cf. 2.12). On va donner ici, avec Kronecker, une preuve independante.

On a

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i)$$

$$(1 - \zeta^i)(1 - \zeta^{-i}) = -\zeta^{-i}(1 - \zeta^i)^2,$$

d'où

$$p = (-1)^{\frac{p-1}{2}} \zeta^a \prod_{i=1}^{(p-1)/2} (1 - \zeta^i)^2,$$

où

$$a = -\sum_{j=1}^{(p-1)/2} j$$

Donc $p^* = \tau^2$, où

$$\tau = \zeta^{a/2} \prod_{i=1}^{(p-1)/2} (1 - \zeta^i)$$

(on remarque que $1/2 \in \mathbb{F}_p$ puisque p est impair).

5.17. Soit q un autre nombre premier impair, différent de p. Considérons l'automorphisme de Frobenius $\sigma_q \in G = \mathrm{Gal}(L/\mathbb{Q})$; par définition, $\sigma_q(\zeta) = \zeta^q$. σ_q est un générateur du groupe cyclique G d'ordre $p-1$.

Soit $K = \mathbb{Q}(\tau)$, donc $L \supset K \supset \mathbb{Q}$, $[L : K] = (p-1)/2$, $[K : \mathbb{Q}] = 2$. On a $\sigma_q(\tau) = \epsilon\tau$, où $\epsilon = 1$ si $\sigma_q \in G^2$ et $\epsilon = -1$ sinon. Il en suit que

$$\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau$$

5.18. Soit $\mathfrak{q} \subset R$ un idéal premier au-dessus de q. Alors on a d'après 5.14

$$\sigma_q(\tau) \equiv \tau^q \pmod{\mathfrak{q}},$$

donc

$$\left(\frac{q}{p}\right)\tau \equiv \tau^q \pmod{\mathfrak{q}},$$

d'où

$$\left(\frac{q}{p}\right) \equiv \tau^{q-1} \pmod{\mathfrak{q}}$$

(car τ est inversible modulo $\mathfrak{q}$).

Il en suit que

$$\left(\frac{p^*}{q}\right) \equiv p^{*(q-1)/2} = \tau^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{\mathfrak{q}}$$

d'où la loi de réciprocité, encore une fois:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

6. Théorème de Kummer

Théorème de Kronecker

6.1. Terminologie: "un corps de nombres algébriques" = une extension finie $L \subset \mathbb{Q}$. Soit R est l'anneau des entiers dans L. "Unité de L = un élément inversible de R.

Soit L un corps de nombres algébriques de degré n sur $\mathbb{Q}$; on a $L = \mathbb{Q}(\alpha)$. Soit $f(t) \in \mathbb{Q}[t]$ le polynôme irréductible unitaite de α; si l'on choisit un plongement $\mathbb{Q} \hookrightarrow \mathbb{C}$, on a $f(t) = \prod_{i=1}^{n} (t - \alpha^{(i)})$. Les racines $\alpha^{(i)}$ correspondent biuniquement aux plongements différents $f_i : \ L \hookrightarrow \mathbb{C}, \ f_i(\alpha) = \alpha^{(i)}$.

Parmis les α_i on a s nombres réels et $2t$ nombres qui ne sont pas réels (parce que pour chaque racine complexe β on a necessairement la racine cojuguée $\bar{\beta}$. Donc on a l'égalite importante:

$$s + 2t = n \tag{6.1.1}$$

Les plongements f_i correspondants aux racines reèls sont appelés *les plongements réels*, les autres sont appelés *les plongements complexes.*

On dit que L est totalement réel si $t = 0$. Exemple: $\mathbb{Q}(\sqrt{d}), \ d > 0$. On dit que L est totalement complexe si $s = 0$. Exemples: $\mathbb{Q}(\sqrt{d}), d < 0; \mathbb{Q}(\zeta_n), \ n > 2$.

Rénumerons $\alpha^{(j)}$ d'une manière suivante:

$$\alpha_1, \ldots, \alpha_s; \alpha_{s+1}, \bar{\alpha}_{s+1}, \ldots \alpha_{s+t}, \bar{\alpha}_{s+t}$$

où $\alpha_i \in \mathbb{R} \ (1 \leq i \leq s), \ \alpha_{s+j} \notin \mathbb{R} \ (1 \leq j \leq t)$, donc les plongements f_i sorrespondants sont:

$$f_1, \ldots, f_s; f_{s+1}, \bar{f}_{s+1}, \ldots, f_{s+t}, \bar{f}_{s+t} \tag{6.1.2}$$

Cette numération sera supposée dorénavant.

Introduisons l'application

$$f = (f_1, \ldots, f_{s+t}) : \ L \longrightarrow \mathbb{R}^s \oplus \mathbb{C}^t$$

Celle ci est un morphisme d'anneaux, évidemment injectif. Soit

$$g = (q_1, \ldots, g_n) : \ L \longrightarrow \mathbb{R}^n$$

le composé de f avec l'isomorphisme (de $\mathbb{R}$-espaces vectoriels) $\mathbb{R}^s \oplus \mathbb{C}^t \xrightarrow{\sim} \mathbb{R}^n$ qui est défini par la règle:

$$(a_1, \ldots, a_{s+t}) \mapsto (a_1, \ldots, a_s, \Re(a_{s+1}), \Im(a_{s+1}), \ldots, \Re(a_{s+1}), \Im(a_{s+1}))$$

6.2. *Lemme.* Soit $\alpha_1, \ldots, \alpha_n$ une base de L sur $\mathbb{Q}$. Alors les vecteurs $g(\alpha_1), \ldots, g(\alpha_n)$ sont linéairement independants, donc forment une $\mathbb{R}$-base de $\mathbb{R}^n$.

Il faut montrer que la matrice $G = (g_i(\alpha_j))$ $n \times n$ réelle est nondégénerée. Désignerons la suite (6.1.2) de plongements par $(h_1, \dots, h_n)$, donc $h_i(x) = x^{(i)}$ dans les notations 4.5.

Au lieu de G, considérons la matrice complexe $G' = (h_i(\alpha_j)) = (\alpha_j^{(i)})$. Alors on voit aisement que

$$\det(G') = (-2i)^t \det(G)$$

(pourquoi?). Or, d'après lemme 4.9 $\det(G')^2 = \Delta(\alpha_1, \dots, \alpha_n) \neq 0$.

6.3. Soit V un $\mathbb{R}$-espace vectoriel de dimension n. *Un réseau* $A \subset V$ est un sous-groupe abélien isomorphe à $\mathbb{Z}^n$, tel qu'il existe une $\mathbb{Z}$-base $a_1, \dots, a_n$ de A qui est une $\mathbb{R}$-base de V.

Lemme. Un sous-groupe abélien $A \subset V$ est un réseau ssi il est discret est *cocompact*, c'est-à-dire, le quotient V/A est compact.

Exercice.

6.4. *Corollaire.* $g(R) \subset \mathbb{R}^n$ est un réseau.

En effet, d'après 4.13 il existe une $\mathbb{Z}$-base $\alpha_1, \dots, \alpha_n$ de R, donc $\{g(\alpha_i)\}$ sera une $\mathbb{Z}$-base de $g(R)$.

6.5. *Théorème* (Kronecker) Le sous-groupe $S \subset R^*$ se composant des éléments $x \in L$ tels que $|g_i(x)| = 1$ pour chaque i, coïncide avec le groupe de toutes racines de l'unité dans L.

Il est un groupe fini, cyclique, de l'ordre pair.

Il est clair que si $\zeta \in L$ est une racine de l'unité alors $g_i(\zeta) = 1$ pour tous i.

Réciproquement, $g(S) \subset R$ est un sous-ensemble borné par hypothèse, est discret, car il est contenu dans le réseau $g(S)$, donc fini, donc S est fini. Il en suit que chaque élément de S est une racine de l'unité.

S est cyclique comme un sous-groupe fini de L^*; il est de l'ordre pair puisqu'il contient le sous-groupe $\{\pm 1\}$.

Remarque. Il est essentiel que $S \subset R$. En effet, pour $x = (3 + 4i)/5 \in L = \mathbb{Q}(i)$ on a $|\sigma(x)| = |\bar{\sigma}(x)| = 1$ (où $\sigma, \bar{\sigma}$ sont deux plongements $L \hookrightarrow \mathbb{C}$), mais $x \notin R = \mathbb{Z}[i]$, donc il n'est pas une racine de l'unité.

Lemme de Kummer

6.6. Soient $p > 2$ un nombre premier, $\zeta = e^{2\pi i/p}$, $L = \mathbb{Q}(\zeta)$, $R \subset L$ l'anneau des entiers.

Considérons le sous-corps $K = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos(2\pi i/p) \subset L$; ceci est un sous-corps (maximal) réel de L. On a $[L : K] = 2$; K est le sous-corps fixé de la conjugaison complexe. Donc $[K : \mathbb{Q}] = (p - 1)/2$.

Les unités de K sont appelés *réelles*. Une unité ϵ de L est réelle ssi $\epsilon = \bar{\epsilon}$.

6.7. *Lemme* (lui aussi, de Kummer) Le sous-groupe de racines de l'unité $S \subset R^*$ est égal au groupe cyclique de l'ordre $2p$, $S' \subset R$, engendré par $-\zeta$.

En effet, il est clair que $S' \subset S$, donc $2p \mid m := \mathrm{Card}(S)$.

Le groupe S est cyclique; soit η un générateur de S. Soit $F = \mathbb{Q}(\eta) \subset L$. η est une racine primitive de l'unité d'ordre m, donc $[F : \mathbb{Q}] = \phi(m)$.

Or

$$[F : \mathbb{Q}] = \phi(m) \mid [L : \mathbb{Q}] = p - 1$$

Posons $m = p^r a,\ (a, p) = 1$; remarquons que $2 \mid a$ car $2p \mid m$. Alors

$$\phi(m) = \phi(p^r)\phi(a) = p^{r-1}(p-1)\phi(a) \mid (p-1),$$

d'où $r = 1,\ \phi(a) = 1$, donc $a = 2$. On en conclut que $m = 2p$, cqfd.

6.8. *Lemme* (Kummer) Chaque unité de L est un produit d'une unité réelle par une puissance de ζ.

Soit

$$\epsilon = r(\zeta) = \sum_{i=0}^{p-2} a_i \zeta^i \in R^*;\ a_i \in \mathbb{Z}$$

On a $\bar{\epsilon} = r(\zeta^{-1}) = r(\zeta^{p-1}) \in R^*$. Soit $\mu = \epsilon\bar{\epsilon}^{-1} \in R^*$. Les conjuguées de μ sont

$$\sigma_j(\mu) = r(\zeta^j)r(\zeta^{-j}) = \sigma_j(\epsilon)\bar{\sigma_j(\epsilon)},\ j = 1, \ldots, p-1,$$

donc $|\sigma_j(\mu)| = 1$ pour tous j. D'après 6.5 et 6.7, $\mu = \pm\zeta^s$. Montrons que le signe est $+$.

En effet, sinon, $\epsilon = -\zeta^s\bar{\epsilon}$.

Sous-lemme. Soit $\lambda = 1 - \zeta \in R$. Si $a \in \mathbb{Z} \subset R$ et $\lambda \mid a$ dans R, alors $p \mid a$ dans $\mathbb{Z}$.

En effet, l'égalite $p = \prod_{i=1}^{p-1}(1 - \zeta^i)$ signifie que

$$N(\lambda) = p \tag{6.8.1}$$

Ici $N = N_{L/\mathbb{Q}}$. Donc, en prenant la norme de $a = \lambda\alpha$ dans R, on obtient $a^n = pN(\alpha)$ dans $\mathbb{Z}$, d'où l'assertion.

Revenons à notre preuve. On a $\zeta^i \equiv 1 \pmod{\lambda}$ pour tous i, d'où

$$\epsilon \equiv \bar{\epsilon}\sum_{i=0}^{p-2} a_i = A \pmod{\lambda}$$

Mais si $\epsilon = -\zeta^s\bar{\epsilon}$ alors $A \equiv -A \pmod{\lambda}$, donc $2A \equiv 0 \pmod{\lambda}$, d'où, vu le sous-lemme, $p \mid 2A$, donc $p \mid A$ car p est impair. Il en suit que $A \equiv 0 \pmod{\lambda}$, donc $\epsilon \in (\lambda)$, ce qui est absurde, car ϵ est une unité.

On en conclut que $\epsilon = \zeta^s\bar{\epsilon}$. Soit $b \in \mathbb{Z},\ 2b \equiv s \pmod{p}$. Alors $\epsilon = \zeta^{2b}\bar{\epsilon}$.

Posons $\eta = \epsilon/\zeta^b$. Alors η est réelle (vérifier!), et $\epsilon = \zeta^b\ \eta$.

Théorème de Kummer

6.9. Un nombre premier $p > 2$ est appelé *regulier* s'il ne divise pas $h_L = \mathrm{Card}(Cl(L))$, $L = \mathbb{Q}(\zeta_p)$.

6.10. *Théorème* (Kummer) Si p est régulier, alors léquation de Fermat $x^p + y^p = z^p$ n'a pas de solutions entiers tels que $p \not| (xyz)$.

Le théorème de Fermat sous l'hypothèse $p \not| (xyz)$ est appelé le premier cas du théorème de Fermat.

Tout d'abord, l'assertion est vraie pour $p = 3$: exercice (considerez les congruences modulo 9). Donc on peut supposer que $p \geq 5$.

Soit (x, y, z) une solution entière de l'équation $x^p + y^p = z^p$, telle que $p \not| (xyz)$. On peut supposer que $\mathrm{pgcd}(x, y, z) = 1$. Cela implique que x, y, z sont premier deux à deux (sic!)

Si $x \equiv y \equiv -z \pmod{p}$ alors $p \mid 3x$ ce qui est impossible par hypothèse. Donc, en remplaçant si necessaire (x, y, z) par $(x, -z, -y)$, on peut supposer que $x \not\equiv y \pmod{p}$.

On désigne comme toujours $\zeta = \zeta_p$, $L = \mathbb{Q}(\zeta_p)$, $R = \mathbb{Z}[\zeta_p]$ l'anneau des entiers de L.

6.11. *Lemme.* Les idéaux $(x + \zeta^i y) \subset R$, $0 \leq i \leq p - 1$, sont premiers deux à deux.

Supposons que $\mathfrak{p} \mid (x + \zeta^i y)$ et $\mathfrak{p} \mid (x + \zeta^j y)$ pour $i \neq j$. Alors $\mathfrak{p} \mid (\zeta^i - \zeta^j)y = (\text{unité})(1 - \zeta)y$. Donc, soit $\mathfrak{p} = (1 - \zeta)$, soit $\mathfrak{p} \mid y$.

De même, $\mathfrak{p} \mid (\zeta^i(x + \zeta^j y) - \zeta^j(x + \zeta^i y) = (\text{unité})(1 - \zeta)x$, donc soit $\mathfrak{p} = (1 - \zeta)$, soit $\mathfrak{p} \mid x$.

Si $\mathfrak{p} \neq (1 - \zeta)$ alors $\mathfrak{p} \mid x$ et $\mathfrak{p} \mid y$ ce qui est impossible car $(x, y) = 1$. Donc $\mathfrak{p} = (1-\zeta)$. Mais alors $(x+y) \equiv (x+\zeta^i y) \pmod{\mathfrak{p}}$, et par hypothèse $\mathfrak{p} \mid (x+\zeta^i y)$, donc $x+y \equiv 0 (\mathrm{mod}\ (1-\zeta)$. D'après le sous-lemme 6.8 ceci implique que $x+y \equiv 0 \pmod{p}$, d'où $z^p = x^p + y^p \equiv (x + y)^p \equiv 0 \pmod{p}$, contrairement à l'hypothèse.

6.12. *Lemme.* Soit $\alpha \in R$. Alors $\alpha^p \equiv a \pmod{p}$, $a \in \mathbb{Z}$.

En effet, $\alpha = \sum_i a_i \zeta^i$, $a_i \in \mathbb{Z}$, d'où $\alpha^p \equiv \sum_i a_i^p \pmod{p}$.

6.13. *Lemme.* Soit $\alpha = \sum_{i=0}^{p-1} a_i \zeta^i \in R$, $a_i \in \mathbb{Z}$. Si $n \in \mathbb{Z}$, $n \mid \alpha$, et il existe i tel que $a_i = 0$, alors $n \mid a_j$ pour tous j.

En effet, $1 + \zeta + \ldots + \zeta^{p-1} = 0$, et l'on peut prendre comme une $\mathbb{Z}$-base de R toutes les puissances de ζ, sauf ζ^i.

6.14. *Fin de la preuve de* 6.10. Nous avons dans R

$$z^p = x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y)$$

(expliquer!) D'après lemme 6.11, chaque idéal $(x + \zeta^i y)$ est une p-ième puissance,

$$(x + \zeta^i y) = \mathfrak{a}_i^p$$

Donc l'idéal $\mathfrak{a}_i^p$ est principal. Puisque p est régulier, cela implique que $\mathfrak{a}_i$ est principal, disons $\mathfrak{a}_i = (\alpha_i)$.

Prenons $i = 1$, donc $x+\zeta y = \epsilon\alpha^p,\ \epsilon \in R^*, \alpha \in R$. D'après le lemme de Kummer, $\epsilon = \zeta^r\eta$ où $\eta = \bar{\eta}$. Par contre $\alpha^p \equiv a \pmod p$ où $a \in \mathbb{Z}$. Il en suit que

$$x + \zeta y = \zeta^r\eta\alpha^p \equiv \zeta^r\eta a \pmod p$$

En prenant les conjuguées,

$$x + \zeta^{-1}y \equiv \zeta^{-r}\eta a \pmod p,$$

d'où

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1}y) \pmod p$$

ou

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0 \pmod p \tag{6.14.1}$$

Si tous le nombres $1, \zeta, \zeta^{2r}$ et ζ^{2r-1} sont distincts, alors le lemme 6.13 implique que $p \mid x$, contrairement à l'hypothèse (ici on a utilisé que $p \geq 5$).

Il nous restent les possibilités suivantes.

(a) $1 = \zeta^{2r}$. Alors (6.14.1) devient $\zeta y - \zeta^{2r-1}y \equiv 0 \pmod p$; en appliquant 6.13 de nouveau, on obtient $p \mid y$: contradiction.

(b) $1 = \zeta^{2r-1}$. Alors $x-y-(x-y)\zeta \equiv 0 \pmod p$, d'où $p \mid (x-y)$: contradiction.

(c) $\zeta = \zeta^{2r-1}$. Alors $x - \zeta^2 x \equiv 0 \pmod p$, d'où $p \mid x$: contradiction.

La preuve est finie.

§7. Descente de Fermat

Triples pythagoréens

7.1. *Théorème.* Soit (a, b, c) un triple d'entiers, $a, b, c > 0$, satisfaisants à l'équation

$$a^2 + b^2 = c^2$$

Supposons que $\mathrm{pgcd}(a, b, c) = 1$.

Alors, après peut-être la permutation de a et b,

$$a = 2pq,\ b = p^2 - q^2,\ c = p^2 + q^2,$$

où $p, q \in \mathbb{Z}_{>0},\ (p, q) = 1,\ p > q$ et $p - q$ est impair.

Première démonstration.

Un nombre premier divisant deux de nombres a, b, c necessairement divise le troisième, donc a, b, c sont deux-à-deux premiers.

Il en suit que parmi a, b, c deux nombres sont impairs et un nombre est pair. Le cas a, b impairs c pair est impossible (expliquer!) Donc, après la permutation de a, b si necessaire, on peut supposer que $a = 2u$ est pair, b, c sont impairs.

On a

$$4u^2 = c^2 - b^2 = (c - b)(c + b)$$

Posons $c - b = 2v,\ c + b = 2w$. Alors $c = v + w,\ b = w - v$; il en suit que v, w sont premiers entre eux.

On a $u^2 = vw$; donc $v = q^2,\ w = p^2$. $p - q$ est impair parce que sinon, b serait pair.

Deuxième démonstration. Comme ci-dessus, a, b, c sont deux à deux premiers, et c est impair.

On va utiliser l'anneau de nombres gaussiens $R = \mathbb{Z}[i]$, qui est l'anneau des entiers dans $L = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$.

7.1.1. *Lemme.* R est euclidien, donc principal.

Exercice.

7.1.2. *Lemme.* Les idéaux $(a + bi), (a - bi) \subset R$ sont premiers entre eux, cf. lemme 6.11.

Soit $\pi \in R$ un élément premier divisant $a + bi$ et $a - bi$. Alors π divise $2a$.

On affirme que π ne divise pas 2. Parce que sinon, $N(\pi)\ |N(2) = 4$ (rappelons que $N(\alpha+\beta i) = \alpha^2+\beta^2$. On a $N(\pi) > 1$ (car π n'est pas une unité), donc $N(\pi) = 2$ ou 4. Mais π divise c, donc $N(\pi)$ divise $N(c) = c^2$, ce qui contredit au fait que c est impair.

Question: quelle est la décomposition de 2 en produit de nombres premiers dans R?

Il en suit que $\pi \mid b$. De même, $\pi \mid b$ (expliquer!). Mais alors $N(\pi)$ divise $N(a) = a^2$ et $N(b) = b^2$: contradiction, car a et b sont supposés premiers entre eux.

On a la décomposition dans R

$$(a + bi)(a - bi) = c^2,$$

cf. 6.14. Le lemme précédent implique que $(a + bi) = (\alpha)^2,\ \alpha \in R$, donc

$$a + bi = \epsilon\alpha^2$$

Les seuls unités dans R sont $\pm 1,\ \pm i$ (expliquer!).

Supposon que $\epsilon = 1$. Écrivons $\alpha = u + iv$, alors $\alpha^2 = u^2 - v^2 + 2uv\ i$, d'où l'assertion du théorème dans ce cas.

Les cas $\epsilon = -1$ ou $\pm i$ sont pareils est laissés comme un exercice.

Théorème de Fermat: exposante 4

7.2. *Théorème* (Fermat) (a) Soient $a, b, c \in \mathbb{Z}_{>0}$ les côtés d'un triangle pythagorien, $a^2 + b^2 = c^2$. Alors son aire n'est pas un carré.

(b) Il n'existe pas de solutions $(x, y, z) \in \mathbb{Z}^3_{>0}$ de l'équation

$$x^4 - y^4 = z^2$$

On va démontrer (a) et (b) simultanément. Étant donnés a, b, c comme dans (a), on peut supposer, vu le théorème précédent, que $(a, b, c) = (2pq, p^2 - q^2, p^2 + q^2)$, où p, q sont premiers entre eux, $p > q$ et $p - q$ est impair. L'aire de ce triangle sera $S = (ab)/2 = pq(p + q)(p - q)$. Ici les nombres $p, q, p + q, p - q$ sont deux à deux premiers.

Il en suit que si S est un carré, alors ces facteurs le sont: $p = x^2,\ q = y^2,\ p+q = u^2,\ p - q = v^2$. Ici u, v sont impairs et premiers entre eux. Si l'on pose $z = uv$, alors $x^4 - y^4 = z^2$. (Il en suit déjà que (b) $\Rightarrow$ (a).)

Nous avons $u^2 = v^2+2y^2$, donc $2y^2 = (u-v)(u+v)$. On a $\gcd(u+v, u-v) = 2$, donc $u+v = 2k,\ u-v = 2l$ avec k et l premiers entre eux. D'ici $2y^2 = 4kl$, $y^2 = 2kl$. Il en suit que $y = 2y'$, donc $2y'^2 = kl$. Donc, soit

(1) $k = 2s^2,\ l = r^2$, $u + v = 4s^2,\ u - v = 2r^2$, $u = r^2 + 2s^2,\ v = 2s^2 - r^2$, soit

(2) $k = r^2,\ l = 2s^2$, $u - v = 4s^2,\ u + v = 2r^2$, $u = r^2 + 2s^2,\ v = -2s^2 + r^2$.

Dans les deux cas,

$$x^2 = \frac{1}{2}(u^2 + v^2) = r^4 + 4s^4, \tag{7.2.1}$$

i.e. $(r^2, 2s^2, x)$ sont les côtés d'un triangle pythagorien dont l'aire est $S' = (rs)^2$. Sa hypoténuse est $x < x^4 + y^4 =$ l'hypoténuse du triangle original. On conclut que (a) est vrai par la descente.

On remarque que

$$y^2 = 2kl,\ x^2 = k^2 + l^2,\ z = k^2 - l^2 \tag{7.2.2}$$

Réciproquement, soient x, y, z sont comme dans (b). On peut les supposer deux à deux premiers. Alors, vu 7.1, ils sont de la forme (7.2.2), avec $(k, l) = 1$.

Le même raisonnement nous fournit le triangle $r^2, 2s^2, x$ dont l'aire $S' = (rs)^2$, donc (a) $\Rightarrow$ (b).

7.2.1. *Exercice.* Montrez qu'il n'existe pas d'un triangle rectangluaire de côtés rationels, dont l'aire est égale à 1.

Solution. Le problème est de chercher $a, c \in \mathbb{Q}$ avec $a^2+(2/a)^2 = c^2$, i.e. $a, b \in \mathbb{Q}$ tels que $a^4 + 4 = b^2$. Donc il suffit de montrer que l'équation $r^4 + 4s^4 = x^2$ n'a pas de solutions entiers.

On reconnaît l'équation (7.2.1). Donc essayons d'aller en sens opposé. Soient $x, r, s \in \mathbb{Z}$ une solution de (7.2.1). On peut supposer que $(r, 2s) = 1$ (expliquer!).

Donc il existent $p, q \in \mathbb{Z},\ (p, q) = 1$, tels que $s^2 = pq,\ r^2 = p^2 - q^2$. La première égalité donne $p = y^2,\ q = z^2$, d'où $r^2 = x^4 - y^4$, ce qui est impossible.

Le théorème suivant se demontre de la manière complétement analogue.

7.3. *Théorème* (Fermat) (a) Soient $a, b, c \in \mathbb{Z}_{>0}$ les côtés d'un triangle pythagorien, $a^2 + b^2 = c^2$. Alors son aire n'est pas un double carré.

(b) Il n'existe pas de solutions $(x, y, z) \in \mathbb{Z}^3_{>0}$ de l'équation

$$x^4 + y^4 = z^2$$

Étant donnés a, b, c comme dans (a), on peut supposer qu'il sont premiers entre eux, donc comme ci-dessus que $(a, b, c) = (2pq, p^2-q^2, p^2+q^2)$, où p, q sont premiers entre eux, $p > q$ et $p - q$ est impair. L'aire de ce triangle sera $S = (ab)/2 = pq(p + q)(p - q)$. Ici les nombres $p, q, p + q, p - q$ sont deux à deux premiers.

Supposons que $S = 2R^2$. Alors $p + q = u^2,\ p - q = v^2$ et soit $p = 2x^2,\ q = y^2$, soit $p = x^2,\ q = 2y^2$. Mais u, v sont impairs et $2p^2 = u^2 + v^2$, d'où p est impair. Donc $p = x^2,\ q = 2y^2$.

Alors $4y^2 = (u+v)(u-v)$. On a $\operatorname{pgcd}(u+v, u-v) = 2$, donc $u+v = 2k,\ u-v = 2l,\ (k, l) = 1$; $y^2 = kl$, donc $k = r^2,\ l = s^2$, d'où $u = r^2 + s^2,\ v = r^2 - s^2$, donc

$$x^2 = \frac{1}{2}(u^2 + v^2) = r^4 + s^4$$

(Il en suit que (b) $\Rightarrow$ (a).)

Le triangle (r^2, s^2, x) a l'aire $S' = (rs)^2/2$. Remarquons que $u = r^2 + s^2$, donc l'un de s, r doit être pair; donc rs est pair, et $S' = 2(rs/2)^2$. L'hypoténuse de ce triangle $x <$ l'hypoténuse du triangle $(a, b, c) = p^2 + q^2 = x^4 + 4y^4$, d'où (a) par la descente.

Réciproquement, si $x^2 = r^4 + s^4$, posons $y = rs,\ p = x^2,\ q = 2y^2$. Alors le triangle $(2pq, p-q, p+q)$ a l'aire $S = pq(p+q)(p-q) = 2x^2y^2(r^2+s^2)^2(r^2-s^2)^2$, donc (a) $\Rightarrow$ (b), ce qui démontre le théorème.

Théorème de Fermat: exposante 3

7.4. Posons $L = \mathbb{Q}(\zeta),\ \zeta = e^{2\pi i/3}$. ζ est une racine de l'équation $t^2 + t + 1 = 0$, donc $L = \mathbb{Q}(\sqrt{-3})$. L'anneau des entiers dans L est $R = \mathbb{Z}[\zeta]$.

7.4.1. *Lemme.* R est un anneau euclidien, donc principal.

Preuve???

Les unités dans R sont: $\pm\zeta^i,\ i = 0, 1, 2$: démontrer!

Posons $\lambda = 1 - \zeta$. On a $t^2 + t + 1 = (t - \zeta)(t - \zeta^2)$, d'où

$$3 = (1 - \zeta)(1 - \zeta^2) = \lambda^2(1 + \zeta) = -\zeta^2\lambda^2 \tag{7.4.2}$$

Le corps résiduel

$$R/(\lambda) \cong \mathbb{Z}[t]/(t^2 + t + 1, t - 1) \cong \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3 \tag{7.4.3}$$

En particulier, λ est un élément premier. Il en suit que pour chaque n

$$R/(\lambda^n) \cong \ \oplus_{i=0}^{n-1}\ \mathbb{F}_3\ \lambda^i \tag{7.4.4}$$

(pourquoi?).

On désigne par $v:\ R \longrightarrow \mathbb{N}$ la valuation λ-adique: c'est-à-dire, $v(\alpha) = n$ signifie que $\alpha = \beta\lambda^n$, avec $\lambda \not| \beta$.

7.5. *Théorème.* Soit $u \in R^*$. L'équation

$$x^3 + y^3 = uz^3 \tag{7.5.1}$$

n'a pas de solutions $(x, y, z) \in R^3,\ xyz \neq 0$.

7.6. *Lemme.* Si $x \in R,\ x \equiv 1 \pmod{\lambda}$, alors $x^3 \equiv\ 1 \pmod{\lambda^4}$.

En effet, si $x = 1 + y\lambda$, on a

$$x^3 - 1 = (x - 1)(x - \zeta)(x - \zeta^2) = \lambda y(1 + \lambda y - \zeta)(1 + \lambda y - \zeta^2) =$$

$$= \lambda y(\lambda + \lambda y)(\lambda(1 + \zeta) + \lambda y) = \lambda^3 y(1 + y)(y - \zeta^2)$$

Or, $y - \zeta^2 \equiv y - 1 \pmod{\lambda}$ et $y \equiv 0, \pm 1 \pmod{\lambda}$, d'où

$$y(1 + y)(y - \zeta^2) \equiv 0 \pmod{\lambda}$$

7.7. *Lemme.* Le théorème est vrai sous l'hypothèse $\lambda \not| (xyz)$.

En effet, sinon, prenons la réduction de (7.5.1) modulo λ^4:

$$\pm 1 \pm 1 \equiv \pm u \pmod{\lambda^4} \tag{7.7.1}$$

Ceci est impossible. En effet, chaque élément de $R/(\lambda^4)$ s'écrit de la façon unique sous une forme $\sum_{i=0}^{3}\ a_i\lambda^i,\ a_i = 0, \pm 1$.

Maintenant l'impossibolité de (7.7.1) se vérifie cas par cas.

Par exemple:

$$3 = -\zeta^2\lambda^2 \equiv\ -\lambda^2 \pmod{\lambda^3}, \tag{7.7.2}$$

car $\zeta \equiv 1 \pmod{\lambda}$, d'où $3 \not\equiv 0 \pmod{\lambda^4}$.

Les autres cas sont laissés comme un exercice.

7.8. *Lemme.* Si x, y, z satisfont à (7.5.1), $\lambda \not| (xy)$ et $\lambda \mid z$, alors $v(z) \geq 2$.

En effet,

$$\pm 1 \pm 1 \equiv uz^3 \pmod{\lambda^4}$$

On a $\pm 1 \pm 1 = \pm 2$ ou 0.

Si $0 \equiv uz^3 \pmod{\lambda^4}$ alors $v(z) \geq 2$.

Si $\pm 2 \equiv uz^3 \pmod{\lambda^4}$ alors $\lambda \mid 2$, puisque $\lambda \mid z$, ce qui est impossible (expliquer!).

7.9. *Lemme principal* (descente) Soient x, y, z une solution de (7.5.1) avec $(x, y) = 1$, $\lambda \not| (xy)$, $v(z) = n \geq 2$.

Alors il existent $x', y', z' \in R$, $u' \in R^*$ tels que

$$x'^3 + y'^3 = u'z'^3,$$

$v(z') = n - 1$, $\lambda \not| (x'y')$, $(x', y') = 1$.

On a

$$(x + y)(x + \zeta y)(x + \zeta^2 y) = uz^3,$$

$v(uz^3) = 3n \geq 6$, donc parmi les facteurs du côté gauche il existe un de valuation ≥ 2; en remplacant si necessairement y par ζy ou par $\zeta^2 y$, on peut supposer que $v(x + y) \geq 2$.

Rappelons que

$$v(\alpha + \beta) = \min(v(\alpha), v(\beta)) \text{ si } v(\alpha) \neq v(\beta)$$

Il en suit que

$$v(x + \zeta y) = v(x + y + (\zeta - 1)y) = 1$$

puisque $v((\zeta - 1)y) = v(-\lambda y) = 1$. De même, $v(x + \zeta^2 y) = 1$ (expliquer!). Cela implique que $v(x + y) = 3n - 2$.

On a $\text{pgcd}(x + y, x + \zeta y) = \lambda$. En effet, si π est premier, $(\pi) \neq (\lambda)$, et $\pi \,|(x + y)$ et $\pi \,|(x + \zeta y)$, alors $\pi \mid (1 - \zeta)y = \lambda y$, donc $\pi \mid y$ et $\pi \mid x$ ce qui est impossible par hypothèse $(x, y) = 1$.

De même, $\text{pgcd}(x + y, x + \zeta^2 y) = \text{pgcd}(x + \zeta y, x + \zeta^2 y) = \lambda$ (vérifier!).

Il en suit que

$$x + y = v\alpha^3\lambda^{3n-2},\ x + \zeta y = v'\beta^3\lambda,\ x + \zeta^2 y = v''\gamma^3\lambda,$$

avec $v, v', v'' \in R^*$, α, β, γ deux à deux premiers.

Multitplions la deuxième identité par ζ et la troisième par ζ^2 et ajoutons-les:

$$v\alpha^3\lambda^{3n-2} + \zeta v'\beta^3\lambda + \zeta^2 v''\gamma^3\lambda = 0,$$

en divisant par λ (sic!):

$$v\alpha^3\lambda^{3n-3} + \zeta v'\beta^3 + \zeta^2 v''\gamma^3 = 0$$

Posons $z' = \alpha\lambda^{n-1},\ x' = \beta,\ y' = \gamma$:

$$x'^3 + \epsilon y'^3 = \epsilon' z'^3 \tag{7.9.1}$$

avec $\epsilon, \epsilon' \in R^*$. Modulo λ^2 cela devient:

$$\pm 1 + \epsilon \equiv 0 \pmod{\lambda^2} \tag{7.9.2}$$

7.9.1. *Sous-lemme.* La congruence (7.9.2) entraîne $\epsilon = \pm 1$.

En effet, sinon, $\epsilon = \pm\zeta$ ou $\pm\zeta^2$. Si par exemple $\epsilon = \zeta$, alors $\zeta - 1 = -\lambda \not\equiv 0 \pmod{\lambda^2}$.

De même, $\zeta + 1 = -\lambda + 2$. On a $2 = 3 - 1$, $3 \equiv 0 \pmod{\lambda^2}$, donc

$$-\lambda + 2 \equiv -\lambda - 1 \not\equiv 0 \pmod{\lambda^2}$$

Les autres cas sont traités de la même manière; on les laisse au lecteur.

Donc (7.9.1) se récrit

$$x'^3 \pm y'^3 = \epsilon' z'^3$$

En remplaçant ici y' par $-y'$ si necessairement, on obtient 7.9.

7.10. *Fin de la preuve de* 7.5. On peut supposer que x, y, z soient premiers deux à deux. Le cas $\lambda \not| (xyz)$ est traité dans 7.7.

Si $\lambda \not| (xy)$ et $\lambda \mid z$, alors $v(z) \geq 2$ vu 7.8, et on conclut par la descente 7.9.

Supposons par contre que $\lambda \mid x$ et $\lambda \not| (yz)$. Alors

$$\pm 1 \equiv \pm u \pmod{\lambda^3}$$

D'après 7.9.1, ceci implique $u = \pm 1$, d'où $x^3 + y^3 = \pm z^3$, donc $(\pm z)^3 + (-y)^3 = x^3$, et on est dans le cas précédent.

Ceci achève la preuve.

§8. Théorème de Jacobi

Sommes de Gauss et de Jacobi

8.1. *Caractères.* Soit p un nombre premier. Un caractère (multiplicatif) de $\mathbb{F}_p$ est un homomorphisme $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$. Pour chaque $x \in \mathbb{F}_p$, $\chi(x)^{p-1} = \chi(x^{p-1}) = \chi(1) = 1$, donc $\chi(x)$ est une racine $(p-1)$-ième de l'unité. Il en suit que

$$\chi(x)^{-1} = \chi(\bar{x})$$

On désigne par e le caractère trivial, $e(x) = 1$ pour chaque $x \in \mathbb{F}_p^*$.

On pose $\chi(0) = 0$ si $\chi \neq e$ et $e(0) = 1$.

Le groupe $\mathbb{F}_p^*$ étant cyclique d'ordre $p-1$, les caractères forment un groupe cyclique $X(\mathbb{F}_p^*)$ d'ordre $p-1$ (expliquer!).

Suivant l'usage, on dit que χ et d'ordre a si $\chi^a = e$ et $\chi^b \neq e$ pour $1 < b < a$. On a $a \mid (p-1)$.

8.1.1. *Exemple.* Le symbole de Legendre

$$\left(\frac{?}{p}\right) : \mathbb{F}_p^* \longrightarrow \{\pm 1\}$$

est un caractère d'ordre 2 ($p > 2$).

8.1.2. *Exercices.* (a) Pour chaque $x \in \mathbb{F}_p^*$, $x \neq 1$ il existe $\chi \in \mathbb{F}_p^*$ tel que $\chi(x) \neq 1$.

(b) $\sum_{x \in \mathbb{F}_p} \chi(x) = 0$ si $\chi \neq e$ et p si $\chi = e$.

(c) $\sum_{\chi \in X(\mathbb{F}_p^*)} \chi(x) = 0$ si $x \neq \mathbb{F}_p^* - \{1\}$ et $p-1$ si $x = 1$.

8.2. *Sommes de Gauss.* Soient $\zeta = e^{2\pi i/p}$, $a \in \mathbb{F}_p$, $\chi \in X(\mathbb{F}_p^*)$. On définit

$$g_a(\chi) := \sum_{x \in \mathbb{F}_p} \chi(x)\zeta^{ax}$$

Par définition, $g_a(\chi) \in \mathbb{Q}(\zeta_p, \zeta_{p-1})$.

8.2.1. *Exercice.* $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$ si $\chi \neq e$ et $a \neq 0$. Si $a = 0$ et $\chi \neq e$ ou $a \neq 0$ et $\chi = e$, alors $g_a(\chi) = 0$. Enfin, $g_0(e) = p$.

On désignera $g(\chi) := g_1(\chi)$.

8.3. *Théorème.* Si $\chi \neq e$, alors $|g(\chi)| = \sqrt{p}$.

Considérons la somme $S = \sum_a |g_a(\chi)|^2$. Il est clair que $|g_a(\chi)|^2 = |g(\chi)|^2$ si $a \neq 0$; puisque $g_0(\chi) = 0$, on a $S = (p-1)|g(\chi)|^2$.

Par contre,

$$|g_a(\chi)|^2 = g_a(\chi)g_a(\bar{\chi}) = \sum_{x,y} \chi(x)\chi(\bar{y})\ \zeta^{a(x-y)},$$

donc

$$S = \sum_{x,y} \chi(x)\bar{\chi}(y) \sum_a \zeta^{a(x-y)} = p \sum_{x,y} \chi(x)\bar{\chi}(y)\, \delta(x,y) = p \sum_x |\chi(x)|^2 = p(p-1),$$

d'où le théorème.

8.3.1. *Enoncé équivalente.* On a

$$g(\bar{\chi}) = \chi(-1)g(\bar{\chi})$$

(exercice). Donc le théorème nous dit que

$$g(\chi)g(\bar{\chi}) = \chi(-1)p$$

Par exemple, si χ est d'ordre 2, alors $\bar{\chi} = \chi$, donc $g(\chi)^2 = \chi(-1)p$; on a déjà vu cela.

8.4. *Sommes de Jacobi.* Soient $\chi, \chi' \in X(\mathbb{F}_p^*)$. On définit

$$J(\chi, \chi') = \sum_{a \in \mathbb{F}_p} \chi(a)\chi'(1-a) \in \mathbb{Q}(\zeta_{p-1})$$

Il est clair que $J(\chi, \chi') = J(\chi', \chi)$.

8.5. *Théorème.* (a) $J(e, e) = p$

(b) $J(e, \chi) = 0$ si $\chi \neq e$

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$ si $\chi \neq e$

(d) Si $\chi, \chi', \chi\chi' \neq e$, alors

$$J(\chi, \chi') = \frac{g(\chi)g(\chi')}{g(\chi\chi')}$$

En particulier, $|J(\chi, \chi')| = \sqrt{p}$.

(a) est trivial; (b): exercice.

(c):

$$J(\chi, \chi^{-1}) = \sum_{a \neq 1} \chi(a(1-a)^{-1})$$

Quand a parcourt $\mathbb{F}_p - \{1\}$, $c = a(1-a)^{-1}$ parcourt $\mathbb{F}_p - \{-1\}$. Donc

$$J(\chi, \chi^{-1}) = \sum_{c \in \mathbb{F}_p - \{-1\}} \chi(c) = -\chi(-1)$$

(d): Calculons le produit

$$g(\chi)g(\chi') = (\sum_a \chi(a)\zeta^a)(\sum_b \chi'(b)\zeta^b) = \sum_c (\sum_{a+b=c} \chi(a)\chi'(b))\, \zeta^c$$

On a

$$\sum_{a+b=0} \chi(a)\chi'(b) = \sum_a \chi(a)\chi'(-a) = \chi'(-1) \sum_a (\chi\chi')(a) = 0$$

D'autre part, si $c \neq 0$,

$$\sum_{a+b=c} \chi(a)\chi'(b) = (\chi\chi')(c)\ J(\chi,\chi')$$

Il en suit que

$$g(\chi)g(\chi') = \sum_c (\chi\chi')(c)\ J(\chi,\chi')\ \zeta^c = g(\chi\chi')J(\chi,\chi'),$$

cqfd.

8.5.1. *Fonctions* Γ *et* B *de Euler.* On définit

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt = \int_0^\infty e^{-t}t^s\frac{dt}{t}, \quad \Re(s) > 0$$

Montrer que $\Gamma(s+1) = s\Gamma(s)$ et $\Gamma(n) = (n-1)!$ si $n \in \mathbb{N}$.

Posons

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx, \quad \Re(s), \Re(t) > 0$$

8.5.1.1. *Théorème.*

$$B(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$$

Exercice. Démontrer cette formule pour $p, q \in \mathbb{N}$.

Démontrons le théorème. Supposons que $\Re(s), \Re(t) > 1/2$. On a

$$\Gamma(s)\Gamma(t) = \int_0^\infty e^{-x}x^{s-1}dx \int_0^\infty e^{-y}y^{s-1}dy =$$

$$= 4 \lim_{R\to\infty} \int_0^\infty \int_0^\infty e^{-x^2-y^2}x^{2s-1}y^{2s-1}dxdy =$$

$$= 4 \lim_{R\to\infty} \int\int_{Q_R} e^{-x^2-y^2}x^{2s-1}y^{2s-1}dxdy,$$

où $Q_R = \{(x,y)|\ x^2+y^2 = R^2,\ x,y \geq 0\}$. Passons aux coordonnées polaires, $x = r\cos\theta, y = r\sin\theta$:

$$\int\int_{Q_R} e^{-x^2-y^2}x^{2s-1}y^{2s-1}dxdy = \int_0^R \int_0^{\pi/2} e^{-r^2}(r\cos\theta)^{2s-1}(r\sin\theta)^{2t-1}rdrd\theta,$$

d'où

$$\Gamma(s)\Gamma(t) = 4\int_0^\infty e^{-r^2}r^{2(s+t)-1}dr \int_0^{\pi/2} (\cos\theta)^{2s-1}(\sin\theta)^{2t-1}d\theta$$

Or:

$$2\int_0^\infty e^{-r^2} r^{2(s+t)-1} dr = \Gamma(s+t)$$

et

$$2\int_0^{\pi/2} (\cos\theta)^{2s-1} (\sin\theta)^{2t-1} d\theta =$$

$(u = \cos^2\theta)$

$$= \int_0^1 u^{s-1}(1-u)^{t-1} du = B(s,t),$$

cqfd.

8.5.1.2. *Exercice.* Rémarquons que

$$e^{-t} = \lim_{n\to\infty} \big(1 - \frac{t}{n}\big)^n,$$

d'où

$$\Gamma(s) = \lim_{n\to\infty} \int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1} dt$$

(expliquer). En déduire $\Gamma(s)$ comme une valeur limite de B.

En effet,

$$\int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1} dt =$$

$(u = t/n)$

$$= n^s \int_0^1 \big(1-u\big)^n u^{s-1} du$$

Pour $n \in \mathbb{N}$ on a

$$B(n+1,t) = \int_0^1 (1-v)^n v^{t-1} dv = \frac{n!}{t(t+1)\cdot\ldots\cdot(t+n)}$$

et cela est vrai pour tous $t \neq 0, -1, \ldots - n$ (prouver!)

Il en suit que

$$\Gamma(s) = \lim_{n\to\infty} n^s B(n+1,s) = \lim_{n\to\infty} n^s \frac{n!}{s(s+1)\cdot\ldots\cdot(s+n)} \qquad (8.5.1.2.1)$$

(*formule d'Euler - Gauss*).

Exercice. Calculer $\Gamma(1/2)$.

Solution. On a

$$\Gamma(1/2)^2 = \frac{\Gamma(1/2)\Gamma(1/2)}{\Gamma(1)} = B(1/2,1/2)$$

Par définition,

$$B(1/2,1/2) = \int_0^1 x^{-1/2}(1-x)^{-1/2} dx =$$

$(x = u^2)$

$$= 2\int_0^1 \frac{du}{\sqrt{1-u^2}} = 2 \arcsin\ 1 = \pi,$$

d'où

$$\Gamma(1/2) = \int_0^\infty e^{-x}x^{-1/2}dx = \sqrt{\pi}$$

On rémarque que

$$\int_0^\infty e^{-x}x^{-1/2}dx = 2\int_0^\infty e^{-u^2}du = \int_{-\infty}^\infty e^{-u^2}du,$$

donc

$$\int_{-\infty}^\infty e^{-u^2}du = \sqrt{\pi}$$

(l'intégrale de Poisson).

Sommes de deux carrés

8.6. On va travailler dans l'anneau de nombres gaussiens $R = \mathbb{Z}[i]$ qui est l'anneau d'entiers dans $L = \mathbb{Q}(i)$. La norme $N:\ L^* \longrightarrow \mathbb{Q}^*$ s'ecrit

$$N(a+bi) = |a+bi|^2 = a^2 + b^2$$

On a $N(x) \neq 0 \Leftrightarrow x \neq 0$.

8.6.1. *Lemme.* R est euclidien par rapport à N, donc principal.

En effet, on doit démontrer que, étant donnés $\alpha, \beta \in R,\ \beta \neq 0$, il existent $\gamma, r \in R$ tels que $\alpha = \gamma\beta + r$, avec $N(r) < N(\beta)$.

En divisant par y, il suffit de démontrer que, étant donné $x \in L$, il existe $\alpha \in R$ tel que $N(x-\alpha) < 1$. Or, il existe même un $\alpha \in R$ avec $N(x-\alpha) \leq 1/2$, ce qu'on voit tout de suite géométriquement.

8.6.1.1. *Exercice.* Montrer que les anneaux des entiers dans les corps suivants sont euclidiens par rapport à la norme: $\mathbb{Q}(\sqrt{d})$ où $d = -1, -2, -3, -7, -11$.

8.6.2. *Exercice.* Les unités dans R sont $\pm 1, \pm i$, autrement dit,

$$R^* = \mu_4 := \{x \in \mathbb{C}^* \mid x^4 = 1\} \tag{8.6.1}$$

En effet, un $\alpha \in R$ est inversible ssi $N(\alpha) = 1$.

8.7. *Théorème* (Fermat) Soit $p > 2$ premier.

(a) Si $p \mid (a^2 + b^2)$ avec $a, b \in \mathbb{Z},\ p \not| a$, alors $p \equiv 1 \pmod 4$.

(b) Chaque p premier de la forme $4k+1$ est représentable de la façon essentiellement unique sous une forme $p = a^2 + b^2$, $a, b \in \mathbb{Z}$.

"Essentiellement unique" signifie qu'on peut changer les signes de a et de b et permuter a avec b, ce qui donne 8 solutions.

Remarquons que $2 = (\pm 1)^2 + (\pm 1)^2$ (4 possibilités).

8.8. *Démonstration de* (a). Si $p \nmid a$ alors $p \mid b$. On a $a^2 \equiv -b^2 \pmod{p}$, donc $(a/b)^2 = -1$ dans $\mathbb{F}_p$, donc $(-1/p) = 1$, d'où $p \equiv 1 \pmod 4$.

8.10. *Démonstration de* (b). Montrons que chaque p premier de la forme $4k+1$ est égale à $a^2 + b^2,\ a, b \in \mathbb{Z}$.

Choisissons un générateur $\lambda \in \mathbb{F}_p^*$. Alors

$$\chi(\lambda^a) = e^{2\pi i a k/(p-1)} = e^{\pi i a/2} \in \mu_4$$

est un caractére de $\mathbb{F}_p^*$ d'ordre 4. Il en suit que la somme de Jacobi $J(\chi, \chi) \in R = \mathbb{Z}[i]$, soit $J(\chi, \chi) = a + bi$.

Théorème 8.5 (d) montre alors que

$$a^2 + b^2 = |J(\chi, \chi)|^2 = p$$

Unicité. Posons $\pi = J(\chi, \chi)$, donc $p = \pi\bar{\pi}$.

Si $p = c^2 + d^2$ est une autre représentation, $\pi' = c + di$, alors $p = \pi'\bar{\pi}'$. Alors π' est necessairement premier dans R (prouver!).

L'anneau R étant principal, il en suit que soit $\pi' = \epsilon\pi$, soit $\pi' = \epsilon\bar{\pi}$, avec $\epsilon \in R^*$. Ceci donne exactement 8 possibilités mentionnées ci-dessus.

8.11. *Une autre démonstration de* (b). On utilise 3.23 (pour $d = -1$), cf. *loc. cit.* (a1).

Puisque $p \equiv 1 \pmod 4$, il existe $a \in \mathbb{Z},\ a^2 \equiv -1 \pmod p$. Alors

$$(p) = \mathfrak{p}\bar{\mathfrak{p}},\ \text{où } \mathfrak{p} = (p, i - a) \subset R$$

C'est ce qu'on veut: R étant principal, $\mathfrak{p} = (\pi)$; si $\pi = a + bi$ alors $p = a^2 + b^2$. On finit comme ci-dessus.

8.11.1. *Exercice.* (a) Prouver que

$$(13) = (13, 5 - i)(13, 5 + i)$$

dans R.

(b) En faisant la division euclidienne dans R, prouver que $\operatorname{pgcd}(13, 5-i) = 3-2i$, donc $(13, 5 - i) = (3 - 2i)$.

8.12. *Theorema elegantissima* (Gauss) Soit p un nombre premier, $p = 4\nu + 1$.

Alors parmis 8 représentations $p = a^2 + b^2,\ a, b \in \mathbb{Z}$ il existe une, telle que

$$2a \equiv \binom{2\nu}{\nu} \pmod p \tag{8.12.1}$$

Cf. [G] (b), p. 90.

Ceci permet de trouver aisement a et b.

8.13. *Lemme clef.* Soit $p = \pi\bar{\pi}$ une décomposition dans R. Il existe une autre décomposition $p = J\bar{J}$,telle que

$$J \equiv 0 \pmod{\pi} \tag{8.13.1}$$

et

$$J \equiv \binom{2\nu}{\nu} \pmod{\bar{\pi}} \tag{8.13.2}$$

Ce lemme implique le théorème immédiatement: si $J = a + bi$, on a par (8.13.2):

$$a^2 - b^2 + 2ab\ i = J^2 \equiv \binom{2\nu}{\nu} J = \binom{2\nu}{\nu}(a + bi) \pmod{J\bar{\pi}}$$

Or, $J\bar{\pi} \equiv 0 \pmod{p}$ grace à (8.13.1), d'où

$$2ab \equiv \binom{2\nu}{\nu} b \pmod{p},$$

d'où (8.12.1) car b est premier à p.

8.14. Eisenstein prouve le lemme à l'aide de la division de lemniscate; on peut trouver la preuve très jolie dans [E], §3, p. 551.

Nous prouvons 8.13 en utilisant les sommes de Jacobi, comme dans [W] (b), pp. 317 - 318.

Soit $p = \pi\bar{\pi}$ une décomposition arbitraire dans R. L'inclusion $\mathbb{Z} \subset R$ induit un isomorphisme canonique $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong R/(\pi)$. Autrement dit, pour chaque $x \in R$ il existe un unique $\bar{a} \in \mathbb{F}_p$ tel que

$$x \equiv \bar{a} \pmod{\pi}$$

Considérons le composé

$$\mu_4 \subset R \longrightarrow R/(\pi) \cong \mathbb{F}_p$$

Elle induit un isomorphisme

$$\phi_\pi :\ \mu_4 \xrightarrow{\sim} \mathbb{F}^*_{p(4)} := \{x \in \mathbb{F}^*_p \mid x^4 = 1\}$$

Définissons un caractère $\chi = \chi_\pi$ de $\mathbb{F}^*_p$ d'ordre 4 par $\chi(x) = \phi_\pi^{-1}(x^\nu)$.

Explicitement, étant donné un $x \in \mathbb{F}_p$, choisissons un $a \in \mathbb{Z}$ tel que $x = \bar{a} = a \pmod{p}$. Alors il existe un unique $\zeta \in \mu_4 \subset R^\times$ tel que

$$a^\nu \equiv \zeta \pmod{\pi}$$

Par définition, $\chi(x) = \zeta$. Autrement dit,

$$\chi(\bar{a}) \equiv a^\nu \pmod{\pi} \tag{8.14.1}$$

Posons $J = -J(\chi, \chi)$; on veut calculer les restes de J modulo π et $\bar{\pi}$. Il découle de (8.14.1) que

$$J \equiv -\sum_{a=1}^{p-1} a^{\nu}(1-a)^{\nu} = -\sum_{a=1}^{p-1} \sum_{k=0}^{\nu} \binom{\nu}{k} (-1)^k a^{\nu+k} \pmod{\pi}$$

8.14.1. *Sous-lemme.* Si $(p-1) \not| \, k$ alors $\sum_{a=1}^{p-1} a^k \equiv 0 \pmod{p}$. Si $(p-1) \mid k$ alors la somme est $\equiv -1$ modulo p.

Exercice. Solution: supposons que $(p-1) \not| \, k$. Notre assertion est équivalente à: $\sum_{x \in \mathbb{F}_p} x^k = 0$. Soit y un générateur de $\mathbb{F}_p^*$. Alors $y^k \neq 1$; on a

$$\sum_{x \in \mathbb{F}_p} x^k = \sum_{i=0}^{p-2} y^{ki} = \frac{y^{(p-1)k} - 1}{y^k - 1} = 0$$

Ceci entraîne (8.13.1).

Maintenant prenons le conjugué complexe de (8.14.1):

$$\chi(\bar{a}^{-1}) = \bar{\chi}(\bar{a}) \equiv a^{\nu} \pmod{\bar{\pi}},$$

d'où

$$\chi(\bar{a}) \equiv a^{p-1-\nu} \pmod{\bar{\pi}} \tag{8.14.2}$$

(expliquer pourquoi). On a $p - 1 - \nu = 3\nu$, donc

$$J \equiv -\sum_{a=1}^{p-1} a^{3\nu}(1-a)^{3\nu} = -\sum_{a=1}^{p-1} \sum_{k=0}^{\nu} \binom{3\nu}{k} (-1)^k a^{3\nu+k} \pmod{\bar{\pi}}$$

Vu le sous-lemme,

$$J \equiv (-1)^{\nu+1} \binom{3\nu}{\nu} \pmod{\bar{\pi}}$$

Il semble qu'on est arrivé à une erreur; mais on conclut grace à une congruence un peu surprenante mais élémentaire:

8.14.2. *Sous-lemme.* On a

$$(-1)^{\nu} \binom{3\nu}{\nu} \equiv \binom{2\nu}{\nu} \pmod{p}$$

Exercice.

8.15. *Variante du calcul.* La classe $a \pmod{\bar{\pi}}$, $a \in \mathbb{Z}$, ne depend que de $\bar{a} \in \mathbb{F}_p$, donc on peut récrire (8.14.2) sous une forme

$$\chi(x) \equiv x^{-\nu} \pmod{\bar{\pi}}, \ x \in \mathbb{F}_p$$

Il en suit (maintenant on fait la sommation dans $\mathbb{F}_p$):

$$J \equiv -\sum_{x \neq 0,1} x^{-\nu}(1-x)^{-\nu} = -\sum_{x \neq 0,1} x^{-2\nu}(x^{-1}-1)^{-\nu} = -\sum_{y \neq 0,1} y^{2\nu}(y-1)^{-\nu} =$$

$(z = y - 1)$

$$= -\sum_{z \neq -1,0} (z+1)^{2\nu} z^{-\nu} = -\sum_{z} (z+1)^{2\nu} z^{-\nu} \equiv \binom{2\nu}{\nu} \pmod{\bar{\pi}},$$

la dernière congruence grace à 8.14.1.

8.16. *Exemple.* $p = 13 = 4 \cdot 3 + 1$,

$$\binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{6} = 20 \equiv -6 \pmod{13},$$

$13 = (-3)^2 + 2^2$.

Exercice. Faire le cas $p = 29$.

8.17. *Nombres primaires* (exercice). Cf. [G] (c), pp. 106, 107.

Remarquer que $2 = (1+i)(1-i) = i(1+i)^2$. Décrire le sous-réseau $L = (1+i)R \subset R$. Disons, avec Gauss, qu'un nombre $x \in R$ est impair s'il n'est pas divisible par $1 + i$. $a + bi$ est impair $\Leftrightarrow$ $a + b$ est impair.

Considérons l'anneau quotient $S = R/(2 + 2i)$. Décrire tous ses éléments. Il y en a combien? S est un anneau local avec l'idéal maximal $\mathfrak{m} = (1 + i)S$. Eléments de $\mathfrak{m}$: les classses modulo $(2 + 2i)$ de $0, 1 + i, 1 - i, 2, 2i$. Eléments de $S^* = S - \mathfrak{m}$: les classes de $1, -1, i$ et $-i$.

Donc l'inclusion $\mu_4 \subset R$ induit un isomorphisme $\mu_4 \xrightarrow{\sim} S^*$. $x \in R$ est impair $\Leftrightarrow$ sa classe modulo $2 + 2i$ appartient à S^*.

Il en suit que pour chaque x impair il existe un unique $\zeta = i^\nu \in \mu_4$ tel que $x \equiv \zeta \pmod{2 + 2i}$. x est appelé *primaire* si $x \equiv 1 \pmod{2 + 2i}$.

8.18. Pour un nombre entier $n > 0$ désignons pas $N_2(n)$ le nombre de couples $a, b \in \mathbb{Z},\ a > 0,\ b \geq 0$, tels que $a^2 + b^2 = n$.

Alors le théorème de Fermat calcule $N_2(p)$ pour p premier: $N_2(2) = 1,\ N_2(p) = 2$ si $p \equiv 1 \pmod 4$ et $N_2(p) = 0$ si $p \equiv 3 \pmod 4$.

Posons $\chi(p) = (-1/p)$ si p est premier impair, $\chi(2) = 0$. Alors on obtient

$$N_2(p) = 1 + \chi(p),\ p \text{ premier}$$

8.19. Plus généralement, définissons $\chi : \mathbb{Z} \longrightarrow \{0, \pm 1\}$ par $\chi(n) = \pm 1$ si $n \equiv \pm 1 \pmod 4$, et $\chi(n) = 0$ si n est pair.

Autrement dit, si n est impair, alors

$$\chi(n) = (-1)^{\frac{n-1}{2}} \tag{8.19.1}$$

En d'autres termes, considérons l'anneau $S = \mathbb{Z}/4\mathbb{Z}$. On a un isomorphisme évident $\phi :\ \mu_2 := \{\pm 1\} \xrightarrow{\sim} S^*$. Alors $\chi(n) = \phi^{-1}(x \bmod 4)$ si $(x \bmod 4) \in S^*$ et 0 sinon.

8.20. *Théorème.* Pour chaque $n \in \mathbb{Z}_{>0}$,

$$N_2(n) = \sum_{d|n} \chi(d)$$

Pour un idéal $\mathfrak{a} = (x) \subset R = \mathbb{Z}[i]$, posons $N(\mathfrak{a}) = N(x)$. Alors $N_2(n) =$ le nombre des idéaux $\mathfrak{a}$ avec $N(\mathfrak{a}) = n$.

8.20.1. *Exercice.* Montrer que $N_2(nm) = N_2(n)N_2(m)$ si n, m sont premiers entre eux.

8.20.2. *Exercice.* Prouver un cas particulier de 8.20: si p est premier, alors

$$N_2(p^k) = \sum_{i=0}^{k} \chi(p^i)$$

En déduire le théorème.

8.20.3. *Corollaire.* Soit $n \in \mathbb{Z}_{>0},\ n \equiv 2 \pmod 4$. Alors le nombre de couples $a, b \in \mathbb{Z}_{>0}$ tels que $a^2 + b^2 = n$ est égale à

$$\sum_{d \mid (n/2)} \chi(d)$$

Exercice.

8.21. *Fonctions ζ et L* (exercice). Montrer que

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

(le produit sur les nombres permiers). De même, introduisons les fonctions

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

et

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})} = \sum_{n=1}^{\infty} \frac{N_2(n)}{n^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

où $K = \mathbb{Q}(i)$, la sommation sur tous les idéaux de R, le produit sur les idéaux premiers.

Alors 8.20 est équivalent à l'identité

$$\zeta_K(s) = \zeta(s)L(\chi, s)$$

Sommes de quatre carrés

8.22. *Théorème.* Soit $n \in \mathbb{Z}_{>0},\ n \equiv 4 \pmod 8$. Désignons par $N_4(n)$ le nombre de quadruples $a, b, c, d \in \mathbb{Z}_{>0}$, avec a, b, c, d impairs, tels que $a^2 + b^2 + c^2 + d^2 = n$. Alors

$$N_4(n) = \sum_{d \mid n,\ d>0,\ d \text{ impair}} d \tag{8.22.1}$$

Tous d'abord, $N_4(n)$ est égale au nombre de x, y, z, w, u, v positifs impairs tels que

$$x^2 + y^2 = 2u,\ z^2 + w^2 = 2v,\ u + v = m := n/2$$

Donc, vu 8.20.3,

$$N_4(n) = \sum_{u+v=m,\ u,v>0,\ u,v \text{ impairs}} \ \sum_{d|u,\ e|v} \chi(d)\chi(e) =$$

$$= \sum_{ds+et=m} \chi(de) = \sum_{ds+et=m} (-1)^{(d-e)/2}$$

où d, e, s, t sont positifs impairs.

Désignons par N_0 (resp. N') la partie de cette somme avec $d = e$ (resp. $d \neq e$).

8.22.1. *Exercice.* N_0 est égale au membre de droite de (8.22.1), i.e. au nombre de diviseurs positifs impairs de n.

Soit S l'ensemble de d, e, s, t positifs impairs tels que $ds + et = m$ et $d > e$.

8.22.2. *Exercice.* $N' = 2\ \sum_S\ \chi(de)$.

8.23. Considérons une matrice

$$A_n = \begin{pmatrix} n+1 & n+2 \\ n & n+1 \end{pmatrix}$$

Définissons d', e', s', t' par

$$A_n \begin{pmatrix} t & d \\ s & -e \end{pmatrix} = \begin{pmatrix} d' & t' \\ e' & -s' \end{pmatrix},$$

i.e.

$$d' = (n+1)t + (n+2)s;\ e' = nt + (n+1)s$$

$$t' = (n+1)d - (n+2)e;\ s' = -nd + (n+1)e$$

Evidemment, $d' > e',\ d' > 0$ et $e' > 0$. Par contre,

$$s' > 0 \Leftrightarrow (n+1)e > nd$$

et

$$t' > 0 \Leftrightarrow (n+1)d > (n+2)e$$

Posons $x = e/d, 0 < x < 1$. Alors il existe un unique $n \in \mathbb{Z}_{>0}$ tel que

$$(n+1)/(n+2) > x > n/(n+1)$$

donc $s' > 0$ et $t' > 0$. On a défini une application $\Phi : \ S \longrightarrow S$.

8.23.1. Φ est bijective.

Exercice.

Remarquons que $d'-e' = s+t$. Soient $d = 2a+1$, $s = 2b+1$, $e = 2c+1$, $t = 2u+1$. Par hypothèse, $ds + et \equiv 2 \pmod 4$, d'où $a + b + c + u \equiv 0 \pmod 2$.

Il en suit que:

$$\frac{d-e}{2} = a - c \text{ est pair } \Leftrightarrow \ \frac{s+t}{2} = b + u + 1 \text{ est impair,}$$

i.e. $\chi(de) = -\chi(d'e')$. Donc

$$\frac{N'}{2} = \sum_S \ \chi(de) = -\sum_S \ \chi(d'e') = -\frac{N'}{2},$$

d'où $N' = 0$.

Ceci prouve le théorème.

§9. Fonctions elliptiques

Fonctions trigonométriques

9.1. Dans notre traitement de fonctions elliptiques nous suivons Abel et Eisenstein (voir [E] (b) et [A]). On débute, avec Eisenstein, par les fonctions trigonométriques.

Définissons le *sinus* comme une fonction $s(t)$ telle que $s(0) = 0$ et qui satisfait à l'équation différentielle

$$s'(t) = \sqrt{1 - s(t)^2} := c(t) \tag{9.1.1}$$

La fonction $c(t)$ sera appelée *cosinus*. Ici t est une variable reélle, et on prend la branche positive de racine, donc $c(0) = 1$.

Autrement dit, introduisons une fonction $a(s)$ (arcsinus) par

$$a(s) = \int_0^s \frac{dx}{\sqrt{1 - x^2}} \tag{9.1.2}$$

On voit que $a(s)$ est une fonction bien définie est monotone sur l'intervale $0 \leq s \leq 1$, et $0 \leq a(s) \leq \pi/2$, où le nombre reél π est défini par

$$\frac{\pi}{2} = \int_0^1 \frac{dx}{\sqrt{1 - x^2}} \tag{9.1.3}$$

(noter que l'integral converge en $x = 1$!).

Donc, $a : \ [0, 1] \longrightarrow [0, \pi/2]$. On définit s comme la fonction inverse $s = a^{-1} : [0, \pi/2] \longrightarrow [0, 1]$, elle est aussi monotone.

Par contre, (9.1.1) (avec la condition initiale) entraine que $s(-t) = -s(t)$, donc notre fonction est définie comme une fonction impair et monotone $s : \ [-\pi/2, \pi(2)] \longrightarrow [-1, 1]$.

On rémarque que (9.1.1) implique:

$$s''(t) = -s(t), \ s'''(t) = -c(t), \tag{9.1.4}$$

etc.

Le *théorème d'addition* ci-dessous est fondamental:

9.2. *Théorème.*

$$s(t + u) = s(t)c(u) + c(t)s(u) \tag{9.2.1}$$

Considérons le développement de Taylor

$$s(t + u) = s(u) + s'(u)t + \frac{1}{2}s''(u)t^2 + \ldots =$$

(d'après (9.1.4))

$$= A(t)s(u) + B(t)c(u)$$

En substituant $u = 0$, on obtient $B(t) = s(t)$.

En dérivant par u:

$$c(t+u) = A(t)c(u) - B(t)s(u)$$

Le substitution $u = 0$ fournit $A(t) = c(t)$, cqfd.

9.3. *Corollaires.*

$$s(t+\pi/2) = s(\pi/2 - t) = c(t)$$

$$s(t) = c(t-\pi/2) = c(\pi/2 - t);\ c(t+\pi/2) = -s(t)$$

$$c(t+u) = c(t)c(u) - s(t)s(u)$$

De là, on peut prolonger s, c en des fonctions $\mathbb{R} \longrightarrow [-1, 1]$ telles que

$$s(t+\pi) = -s(t);\ c(t+\pi) = -c(t)$$

$$s(t+2\pi) = s(t);\ c(t+2\pi) = c(t)$$

9.4. *Point de vue formel.* On définit

$$(1+t)^{1/2} = \sum_{i=0}^{\infty} \binom{1/2}{i} t^i \in \mathbb{Q}[[t]]$$

où

$$\binom{1/2}{i} = \frac{1/2 \cdot (1/2-1) \cdot \ldots \cdot (1/2-i+1)}{i!}$$

Exercices.

9.4.1. Montrer que $\binom{1/2}{i} = 2^{-a}b,\ a, b \in \mathbb{N}$.

9.4.2. Déduire de (9.1.1) les développements de Taylor usuels pour sinus et cosinus.

Fonctions elliptiques

9.5. Considérons une fonction

$$a(x) = \int_0^x \frac{dt}{\sqrt{(1-c^2t^2)(1+e^2t^2)}}, \tag{9.5.1}$$

$e, c \in \mathbb{R}_{>0}$. Elle est bien définie et monotone sur l'interval $[0, c^{-1}]$. On pose

$$\frac{\omega}{4} = \int_0^{c^{-1}} \frac{dt}{\sqrt{(1-c^2t^2)(1+e^2t^2)}} \tag{9.5.2}$$

(NB: l'integral converge.) Donc $a:\ [0, c^{-1}] \longrightarrow [0, \omega/4]$.

On définit *le sinus elliptique* $\phi(t)$ comme l'inverse $\phi = a^{-1}:\ [0, \omega/4] \longrightarrow [0, c^{-1}]$.

On a $a(\phi(t)) = t$, d'où $a'(\phi(t))\phi'(t) = 1$, i.e. $\phi'(t) = a'(\phi(t))^{-1}$.

Donc $\phi(t)$ est une unique fonction satisfaisant à l'équation différentielle

$$\phi'(t) = \sqrt{(1 - c^2\phi(t)^2)(1 + e^2\phi(t)^2)} =: \Delta(t) \tag{9.5.3}$$

avec la condition initiale $\phi(0) = 0$.

Telle $\phi(t)$ existe dans une voisinage de 0, et $\phi(-t) = -\phi(t)$, donc on prolonge ϕ en une fonction monotone impaire $\phi:\ [-\omega/4, \omega/4] \longrightarrow [-c^{-1}, c^{-1}]$.

9.6. *Prolongement à l'argument imaginaire.* Faisons dans l'intégral (9.5.1) une substitution $u = it$, donc $t = -iu$ (où $i = \sqrt{-1}$). L'intégral ne changera pas; donc on aura

$$a(x) = \int_0^{ix} \frac{-idu}{\sqrt{(1 + c^2u^2)(1 - e^2u^2)}} = -i\tilde{a}(ix),$$

où

$$\tilde{a}(x) = \int_0^{x} \frac{du}{\sqrt{(1 + c^2u^2)(1 - e^2u^2)}} \tag{9.6.1}$$

Donc

$$ia(x) = \tilde{a}(ix);\ a(x) = \frac{\tilde{a}(ix)}{i}$$

On pose

$$\frac{\tilde{\omega}}{4} = \int_0^{e^{-1}} \frac{du}{\sqrt{(1 + c^2u^2)(1 - e^2u^2)}} \tag{9.6.2}$$

Alors la fonction $\tilde{\phi} = \tilde{a}^{-1}$ monotone est définie, $\tilde{\phi}:\ [0, \tilde{\omega}/4] \longrightarrow [0, e^{-1}]$.

Il en suit:

$$\tilde{\phi}(ia(x)) = ix,$$

en substituant $a(x) = t,\ x = \phi(t)$, on obtient

$$\tilde{\phi}(it) = i\phi(t)$$

Puisque $\tilde{\tilde{\phi}} = \phi$,

$$\phi(it) = i\tilde{\phi}(t) \tag{9.6.3}$$

Ceci est notre formule principale; elle définit $\phi(x)$ pour $x \in i\mathbb{R}$.

9.7. *Variation.* Faisons dans (9.5.3) un changement de variables $t = iu$, et remarquons que $d/dt = -id/du$:

$$-i\frac{d\phi(iu)}{du} = \sqrt{(1 - c^2\phi(iu)^2)(1 + e^2\phi(iu)^2)}$$

Donc, $\tilde{\phi}(u) := -i\phi(iu)$ est une seule fonction qui satisfait à l'équation différentielle

$$\tilde{\phi}'(u) = \sqrt{(1 + c^2\tilde{\phi}(u)^2)(1 - e^2\tilde{\phi}(u)^2)}$$

et à condition initiale $\tilde{\phi}(u) = 0$.

Théorème d'addition

9.8. Revenons à (9.5.2). Remarquons que

$$\phi''(t) = \Delta'(t) =$$

$$= \frac{1}{2}\phi'(t)\{(1-c^2\phi(t)^2)(1+e^2\phi(t)^2)\}^{-1/2} \cdot (2(e^2-c^2)\phi(t) - 4e^2c^2\phi(t)^3) =$$

$$= (e^2-c^2)\phi(t) - 2e^2c^2\phi(t)^3 \tag{9.8.1}$$

Posons pour briévité $x := \phi(t)$. Il en suit que

$$\frac{d^{2\nu+1}x}{dt^{2\nu+1}} = q_\nu(x)\Delta(x);\ \frac{d^{2\nu}x}{dt^{2\nu}} = p_\nu(x),$$

où p_ν, q_ν sont des polynômes (à coéfficients entiers), et $p_\nu(-x) = -p_\nu(x),\ q_\nu(-x) = q_\nu(x)$.

Maintenant considérons le développement de Taylor de la fonction $\phi(t+u)$ (où l'on pose $y := \phi(u)$):

$$\phi(t+u) = y + ty' + \frac{1}{2}t^2y'' + \ldots =$$

$$= u(t,y) + v(t,y)\Delta(y),$$

où $u(t,-y) = -u(t,y),\ v(t,-y) = v(t,y)$. Donc

$$\phi(t-u) = -u(t,y) + v(t,y)\Delta(y)$$

$$\phi(t+u) + \phi(t-u) = 2v(t,y)\Delta(y) := 2w(t,y), \tag{9.8.2}$$

où

$$w(t,y) = \sum_{\nu=0}^{\infty} a_\nu(t)\ y^{2\nu}\ \Delta(y)$$

Notre but sera trouver les coéfficients $a_\nu(t)$.

9.9. En dérivant par rapport à u:

$$\frac{\partial w}{\partial u} =$$

(cf. (9.8.1))

$$= \sum_\nu a_\nu\ \{2\nu y^{2\nu-1}\ (1-c^2y^2)(1+e^2y^2) + y^{2\nu}\ ((e^2-c^2)y - 2e^2c^2y^3)\} =$$

$$= \sum_\nu a_\nu\ \{2\nu\ y^{2\nu-1} + (2\nu+1)(e^2-c^2)\ y^{2\nu+1} - (2\nu+2)e^2c^2\ y^{2\nu+3}\} =$$

$$= \sum_\nu \{-2\nu e^2c^2a_{\nu-1} + (2\nu+1)(e^2-c^2)a_\nu + 2(\nu+1)a_{\nu+1}\}\ y^{2\nu+1}$$

Donc (en rappelant que $y' = \Delta(y)$)

$$\frac{\partial^2 w}{\partial u^2} =$$

$$= \sum_\nu (2\nu+1)\{-2\nu e^2c^2a_{\nu-1} + (2\nu+1)(e^2-c^2)a_\nu + 2(\nu+1)a_{\nu+1}\}\ y^{2\nu}\Delta(y)$$

D'autre part, (9.8.2) implique que

$$\frac{\partial^2 w}{\partial^2 u} = \frac{\partial^2 w}{\partial^2 t} = \sum_\nu \frac{\partial^2 a_\nu(t)}{\partial^2 t}\ y^{2\nu}\ \Delta(y)$$

Il en suit que

$$(2\nu+1)\{-2\nu e^2c^2a_{\nu-1} + (2\nu+1)(e^2-c^2)a_\nu + 2(\nu+1)a_{\nu+1}\} = \frac{\partial^2 a_\nu(t)}{\partial^2 t} \quad (9.9.1)$$

Ceci est une relation de recursion. En substituant $u = 0$ dans (9.8.2), on obtient (en tenant compte que $\Delta(y(0)) = 1$):

$$a_0 = x \quad (9.9.2)$$

9.10. Pour résoudre (9.9.1), (9.9.2), rémarquons que pour chaque fonction $f(x) = f(x(t))$,

$$\frac{\partial^2 f}{\partial t^2} = \frac{\partial^2 f}{\partial x^2}\left(\frac{\partial x}{\partial t}\right)^2 + \frac{\partial f}{\partial x}\frac{\partial^2 x}{\partial t^2}$$

Prenons $f = x^{2\nu+1}$:

$$\frac{\partial^2 (x^{2\nu+1})}{\partial t^2} =$$

$$= (2\nu+1)2\nu x^{2\nu-1}(1 + (e^2-c^2)x^2 - e^2c^2x^4) + (2\nu+1)x^{2\nu}((e^2-c^2)x - 2e^2c^2x^3) =$$

$$= (2\nu+1)2\nu x^{2\nu-1} + (2\nu+1)^2(e^2-c^2)x^{2\nu+1} - (2\nu+1)(2\nu+2)e^2c^2x^{2\nu+3}$$

Multiplions cela par $(-1)^\nu e^{2\nu}c^{2\nu}$:

$$\frac{\partial^2((-e^2c^2)^\nu x^{2\nu+1})}{\partial t^2} =$$

$$= -e^2c^2(2\nu+1)2\nu(-e^2c^2)^{\nu-1}x^{2\nu-1} + (2\nu+1)^2(e^2-c^2)(-e^2c^2)^\nu x^{2\nu+1} +$$

$$+(2\nu+1)(2\nu+2)(-e^2c^2)^{\nu+1}x^{2\nu+3}$$

En comparant avec (9.9.1), (9.9.2), on trouve

$$a_\nu = (-e^2c^2)^\nu x^{2\nu+1} = x\cdot(-e^2c^2x^2)^\nu \quad (9.10.1)$$

De là,

$$w(t,y) = \sum_\nu a_\nu(t)y^{2\nu}\Delta(y) = \frac{x\Delta(y)}{1+e^2c^2x^2y^2}$$

Donc

$$\phi(t+u)+\phi(t-u)=\frac{2x\Delta(y)}{1+e^2c^2x^2y^2}$$

En échangeant t avec u,

$$\phi(t+u)-\phi(t-u)=\frac{2y\Delta(x)}{1+e^2c^2x^2y^2},$$

d'où

$$\phi(t+u)=\frac{x\Delta(y)+y\Delta(x)}{1+e^2c^2x^2y^2}$$

On a établit le résultat fondamental

9.11. *Théorème* (Euler)

$$\phi(t+u)=\frac{\phi(t)\Delta(u)+\phi(u)\Delta(t)}{1+e^2c^2\phi(t)^2\phi(u)^2}$$

où

$$\Delta(t)=\sqrt{(1-c^2\phi(t)^2)(1+e^2\phi(t)^2)}$$

9.11.1. *Exercice.* En déduire que:

$$\psi(t+u)=\frac{\psi(t)\psi(u)-c^2\phi(t)\phi(u)\tilde{\psi}(t)\tilde{\psi}(u)}{1+e^2c^2\phi(t)^2\phi(u)^2}$$

et

$$\tilde{\psi}(t+u)=\frac{\tilde{\psi}(t)\tilde{\psi}(u)+c^2\phi(t)\phi(u)\psi(t)\psi(u)}{1+e^2c^2\phi(t)^2\phi(u)^2}$$

Conséquences

9.12. On utilisera les notations

$$\psi(t)=\sqrt{1-c^2\phi(t)^2},\ \tilde{\psi}(t)=\sqrt{1+e^2\phi(t)^2}, \tag{9.12.1}$$

donc $\Delta(t)=\psi(t)\tilde{\psi}(t)$. Les deux fonctions $\psi,\tilde{\psi}$ sont pairs.

Par définition,

$$\phi(\pm\omega/4)=\pm c^{-1},\ \tilde{\phi}(\pm\tilde{\omega}/4)=\pm e^{-1} \tag{9.12.2}$$

$$\phi(\pm i\tilde{\omega}/4)=\pm i\tilde{\phi}(\tilde{\omega}/4)=\pm ie^{-1}, \tag{9.12.3}$$

d'où

$$\psi(\pm\omega/4)=\Delta(\pm\omega/4)=0,\ \tilde{\psi}(\pm\omega/4)=\sqrt{1+e^2/c^2} \tag{9.12.4}$$

$$\tilde{\psi}(\pm i\tilde{\omega}/4)=\Delta(\pm i\tilde{\omega}/2)=0,\ \psi(\pm i\omega/4)=\sqrt{1+c^2/e^2} \tag{9.12.5}$$

Le théorème d'addition nous donne

$$\phi(t\pm\omega/4)=\pm c^{-1}\ \psi(t)/\tilde{\psi}(t) \tag{9.12.6}$$

$$\phi(t \pm i\tilde{\omega}/4) = \pm ie^{-1}\ \tilde{\psi}(t)/\psi(t) \tag{9.12.7}$$

Il en suit que

$$\phi(\omega/4 + t) = \phi(\omega/4 - t),\ \phi(i\tilde{\omega}/4 + t) = \phi(i\tilde{\omega}/4 - t) \tag{9.12.8}$$

En faisant $u = t + \omega/4$ (resp. $u = t + i\tilde{\omega}/4$) on obtient

$$\phi(u + \omega/2) = -\phi(u),\ \phi(u + it\omega/2) = -\phi(u), \tag{9.12.9}$$

d'où

$$\phi(u + n\omega/2 + mi\tilde{\omega}/2) = (-1)^{m+n}\phi(u)\ (m, n \in \mathbb{Z}) \tag{9.12.10}$$

En particulier, $\phi(t)$ est périodique, avec deux périodes, ω et $i\tilde{\omega}$.

9.13. *Zéros et poles.* Dans le rectangle (dit "fondamental")

$$F = \{z = a + bi\ |0 \leq a < \omega,\ 0 \leq b < \tilde{\omega}\}$$

(rappelons que e, c sont supposés réels positifs), la fonction $\phi(t)$ a quatre zéros $0, \omega/2, i\tilde{\omega}/2, (\omega + i\tilde{\omega})/2$.

D'autre part, (9.12.6) implique que $\alpha := \omega/4 + i\tilde{\omega}/4$ est un pole de $\phi(t)$, donc on a quatre poles dans F: $\alpha, \alpha + \omega/2, \alpha + \tilde{\omega}/2$ et $\alpha + (\omega + i\tilde{\omega})/2$.

9.14. *Exercice.* Montrer que ce sont *tous* les zéros (resp. poles) dans F.

9.15. *Courbes elliptiques.* Considérons un sous-groupe abélien

$$L' = \mathbb{Z} \cdot \omega \oplus \mathbb{Z} \cdot i\tilde{\omega} \subset \mathbb{C}$$

Ceci est un réseau. Soit

$$E' = \{(x, y) \in \mathbb{C}^2 \mid y^2 = (1 - c^2x^2)(1 + e^2x^2)\} \cup \{(\infty, \infty)\}$$

Alors les fonctions $\phi(z), \phi'(z)$ fournissent un morphisme ("uniformisation")

$$(\phi, \phi') :\ \mathbb{C}/L' \longrightarrow E'$$

Ce morphisme est surjectif, mais un point de E' a normalement deux images inverses.

Pour améliorer cela, considérons une fonction $\rho(z) = \phi(z)^2$. On a

$$\rho'(z) = 2\phi(z)\phi'(z) = 2\phi(z)\sqrt{(1 - c^2\phi(z)^2)(1 + e^2\phi(z)^2)}$$

Donc $\rho(z)$ satisfait à l'équation différentielle

$$\rho'(z)^2 = 2\rho(z)(1 - c^2\rho(z))(1 + e^2\rho(z))$$

Soient

$$L = \mathbb{Z} \cdot \omega/2 + \mathbb{Z} \cdot i\tilde{\omega}/2 \subset \mathbb{C}$$

$$E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 2x(1 - c^2x)(1 + e^2x)\} \cup \{(\infty, \infty)\}$$

Alors on aura un morphisme

$$(\rho, \rho') : \ \mathbb{C}/L \longrightarrow E$$

qui est une bijection.

Fonctions elliptiques de Jacobi

9.16. On commence par l'intégrale

$$u = \int_0^{\phi} \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}} = \int_0^{\sin \phi} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$$

$(t = \sin\theta);\ 0 < k < 1.$

Le *sinus elliptique de Jacobi* $y = \mathrm{sn}(u) = \mathrm{sn}(u;k)$ est la fonction inverse à

$$u(y) = \int_0^{y} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} \tag{9.16.1}$$

Donc

$$u = \int_0^{\mathrm{sn}u} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}};\ \mathrm{sn}(0) = 0$$

Période:

$$K = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}} = \int_0^{1} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}},$$

donc $\mathrm{sn}(K;k) = 1$.

Module complémentaire $k',\ 0 < k' < 1$, est défini de l'équation $k^2 + k'^2 = 1$. On pose

$$K' = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - k'^2 \sin^2 \theta}}$$

9.17. Les fonctions $\mathrm{cn}(u) = \mathrm{cn}(u;k)$ et $\mathrm{dn}(u) = \mathrm{dn}(u;k)$ sont définies par équations

$$\mathrm{sn}^2(u) + \mathrm{cn}^2(u) = 1$$

$$k^2\mathrm{sn}^2(u) + \mathrm{dn}^2(u) = 1$$

On a $\mathrm{cn}(0) = \mathrm{dn}(0) = 1$.

Faisons dans l'intégrale (9.16.1) un changement de variables $u = \sqrt{1-t^2}$. On a $t^2 = 1 - u^2$, donc $2tdt = -2udu$, i.e.

$$dt = -\frac{udu}{\sqrt{1-u}}$$

Il en suit:

$$\int_0^{y} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int_{\sqrt{1-y^2}}^{1} \frac{du}{\sqrt{(1-u^2)(k'^2+k^2u^2)}},$$

i.e.

$$u = \int_{\mathrm{cn}(u)}^{1} \frac{du}{\sqrt{(1-u^2)(k'^2+k^2u^2)}} = k'^{-1} \int_{\mathrm{cn}(u)}^{1} \frac{du}{\sqrt{(1-u^2)(1+(k/k')^2u^2}}$$

9.18. De même, en faisant le changement

$$u = \frac{t}{\sqrt{1-k^2t^2}},$$

donc

$$dt = \frac{du}{(1+k^2u^2)^{3/2}},$$

on obtient

$$\int_0^y \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = \int_0^{y/\sqrt{1-k^2y^2}} \frac{du}{\sqrt{(1-k'^2u^2)(1+k^2u^2)}},$$

d'où

$$u = \int_0^{\mathrm{sn}(u)/\mathrm{dn}(u)} \frac{du}{\sqrt{(1-k'^2u^2)(1+k^2u^2)}}$$

Cela détermine le passage des fonctions elliptiques de Jacobi aux celles d'Abel.

10. Lemniscate

10.1. *Lemniscate* est une courbe C définie par la condition

$$C = \{\mathfrak{h} \in \mathbb{R}^2 \mid d(\mathfrak{h}, \mathfrak{h}_1)d(\mathfrak{h}, \mathfrak{h}^2) = c^2\}$$

Ici $\mathfrak{h}_1, \mathfrak{h}_2$ sont deux points fixés $d(?, ?)$ est la distance, c est fixé.

Soient $\mathfrak{h}_1 = (-a, 0),\ \mathfrak{h}_2 = (a, 0),\ a > 0;\ \mathfrak{h} = (x, y);\ r = d(\mathfrak{h}, O),\ O = (0, 0);\ r_i = d(\mathfrak{h}, \mathfrak{h}_i)$. Alors

$$r^2 = x^2 + y^2;$$

$$r_1^2 = (x + a)^2 + y^2 = r^2 + a^2 + 2ax$$

$$r_2^2 = (x - a)^2 + y^2 = r^2 + a^2 - 2ax$$

Donc la condition $r_1 r_2 = c^2$ se récrit

$$r^4 + 2a^2r^2 + a^4 - 4a^2x^2 = c^4$$

Supposons que $a = c$ et $2a^2 = 1$. Alors

$$2x^2 = r^2 + r^4$$

et

$$2y^2 = r^2 - r^4$$

Nous considérons x, y comme des fonctions en r; donc

$$2xx' = r + 2r^3$$

$$2yy' = r - 2r^3$$

Soit $s(r)$ la longeur de la lemniscate du point O jusqu'au point $(x(r), y(r))$, $0 \leq r \leq 1$. Alors

$$s'(r)^2 = x'(r)^2 + y'(r)^2$$

Donc

$$(2xy)^2 s'^2 = (2xy)^2(x'^2 + y'^2) =$$

$$= y^2(r + 2r^3)^2 + x^2(r - 2r^3)^2 =$$

$$= \frac{r^2 - r^4}{2}(r^2 + 4r^4 + 4r^6) + \frac{r^2 + r^4}{2}(r^2 - 4r^4 + 4r^6) = r^4$$

D'un autre côté,

$$(2xy)^2 = (r^2 + r^4)(r^2 - r^4) = r^4(1 - r^4),$$

d'où

$$(1 - r^4)s'^2 = 1, \quad \frac{ds}{dr} = \frac{1}{\sqrt{1 - r^4}}$$

10.2. Considérons une fonction

$$a(x) = \int_0^x \frac{dt}{\sqrt{1-t^4}}, \tag{10.2.1}$$

Elle est bien définie et monotone sur l'interval $[0,1]$. On pose

$$\frac{\omega}{4} = \int_0^1 \frac{dt}{\sqrt{1-t^4}} \tag{10.2.2}$$

(ceci est l'analogue de $\pi/2$; donc ω est l'analogue de 2π). (NB: l'integral converge.) On peut, suivant Legendre, exprimer cette valeur en termes de la fonction Γ. En effet,

$$\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 4\int_0^1 u^{-3/4}(1-u)^{-1/2}du =$$

$$= 4B(1/4,1/2) = 4\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)} = 4\sqrt{\pi}\frac{\Gamma(1/4)}{\Gamma(3/4)}$$

En utilisant la relation

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin\ \pi x},$$

(cf. 10.2.1 ci-dessous), on déduit

$$\Gamma(1/4)\Gamma(3/4) = \frac{\pi}{\sin\ \pi/4} = \sqrt{2}\ \pi,$$

d'où

$$\omega/4 = 2\sqrt{2/\pi}\ \Gamma(1/4)^2$$

Donc $a : [0,1] \longrightarrow [0,\omega/4]$. On définit *le sinus lemniscatique* $\phi(t)$ comme l'inverse $\phi = a^{-1} : [0,\omega/4] \longrightarrow [0,1]$.

On a $a(\phi(t)) = t$, d'où $a'(\phi(t))\phi'(t) = 1$, i.e. $\phi'(t) = a'(\phi(t))^{-1}$.

Donc $\phi(t)$ est une unique fonction satisfaisant à l'équation différentielle

$$\phi'(t) = \sqrt{1-\phi(t)^4} =: \Delta(t) \tag{10.2.3}$$

avec la condition initiale $\phi(0) = 0$.

On pose

$$\psi(t) = \sqrt{1-\phi(t)^2},\ \tilde{\psi}(t) = \sqrt{1+\phi(t)^2}$$

donc

$$\Delta(t) = \psi(t)\tilde{\psi}(t)$$

10.2.1. *Lemme.* On a

$$\Gamma(a)\Gamma(1-a) = \frac{\pi}{\sin\ \pi a}$$

Preuve. Par la formule d'Euler

$$\Gamma(a)\Gamma(1-a) = B(a,1-a) = \int_0^1 x^{a-1}(1-x)^{-a}dx =$$

$(x = u/(u+1))$

$$= \int_0^\infty \frac{u^{a-1}}{u+1} du = I$$

Nous calculons la dernière intégrale par la formule de Cauchy, cf. [WW], 6.24, Example 1. En effet, considérons intégrale

$$I(r,R) = \int_{C(r,R)} \frac{(-z)^{a-1}}{z+1} dz,$$

où $C(r,R)$ est le contour

$$C(r,R) = \{r \le z \le R\} \cup \{z = Re^{i\theta},\ 0 \le \theta \le 2\pi\} \cup$$

$$\cup \{R \ge z \ge r\} \cup \{z = re^{i\theta},\ 2\pi \ge \theta \ge 0\}$$

Alors

$$I(r,R) = 2i\sin(a\pi) \int_r^R \frac{u^{a-1}}{u+1} du = 2\pi i \ \mathrm{Res}_{z=-1} \frac{(-z)^{a-1}}{z+1} = 2\pi i,$$

d'où

$$I = \lim_{r\to 0,\ R\to\infty} (2i\sin(a\pi)^{-1} I(r,R) = \frac{\pi}{\sin(a\pi)}$$

10.3. *Prolongement à l'argument imaginaire.* Faisons dans (10.2.3) un changement de variables $t = iu$, et remarquons que $d/dt = -id/du$:

$$-i\frac{d\phi(iu)}{du} = \sqrt{1 - \phi(iu)^4}$$

Donc, $\tilde{\phi}(u) := -i\phi(iu)$ est une seule fonction qui satisfait à l'équation différentielle

$$\tilde{\phi}'(u) = \sqrt{1 - \tilde{\phi}(u)^4}$$

et à condition initiale $\tilde{\phi}(u) = 0$. Il en suit que

$$\tilde{\phi}(u) = \phi(t),$$

i.e.

$$\phi(it) = i\phi(t)$$

Donc

$$\psi(it) = \tilde{\psi}(t),\ \tilde{\psi}(it) = \psi(t),\ \Delta(it) = \Delta(t)$$

10.3. *Théorème d'addition.*

$$\phi(t+u) = \frac{\phi(t)\Delta(u) + \phi(u)\Delta(t)}{1 + \phi(t)^2\phi(u)^2}$$

10.4. *Démonstration.* Par définition,

$$\phi'(t) = (1 - \phi(t)^4)^{1/2} = \Delta(t) \tag{10.4.1}$$

d'où

$$\phi''(t) = -2\phi(t)^3 \tag{10.4.2}$$

Posons pour briévité $x := \phi(t)$. Il en suit que

$$\frac{d^{2\nu+1}x}{dt^{2\nu+1}} = q_\nu(x)\Delta(x);\ \frac{d^{2\nu}x}{dt^{2\nu}} = p_\nu(x),$$

où p_ν, q_ν sont des polynômes (à coéfficients entiers), et $p_\nu(-x) = -p_\nu(x),\ q_\nu(-x) = q_\nu(x)$.

Maintenant considérons le développement de Taylor de la fonction $\phi(t+u)$ (où l'on pose $y := \phi(u)$):

$$\phi(t+u) = y + ty' + \frac{1}{2}t^2y'' + \ldots =$$

$$= u(t,y) + v(t,y)\Delta(y),$$

où $u(t,-y) = -u(t,y),\ v(t,-y) = v(t,y)$. Donc

$$\phi(t-u) = -u(t,y) + v(t,y)\Delta(y)$$

$$\phi(t+u) + \phi(t-u) = 2v(t,y)\Delta(y) := 2w(t,y), \tag{10.4.3}$$

où

$$w(t,y) = \sum_{\nu=0}^{\infty} a_\nu(t)\ y^{2\nu}\ \Delta(y) \tag{10.4.4}$$

Notre but sera trouver les coéfficients $a_\nu(t)$.

10.5. On a

$$y' = \Delta(y);\ y'' = \Delta'(y) = -2y^3;\ \Delta(y)^2 = 1 - y^4$$

Il en suit:

$$\frac{\partial w}{\partial u} = \sum_\nu\ a_\nu\{2\nu y^{2\nu-1}(1-y^4) - 2y^{2\nu}y^3\} =$$

$$= \sum_\nu\ a_\nu\{2\nu y^{2\nu-1} - 2(\nu+1)y^{2\nu+3}\} =$$

$$= \sum_\nu\ 2\{-\nu a_{\nu-1} + (\nu+1)a_{\nu+1}\}y^{2\nu+1}$$

D'ici:

$$\frac{\partial^2 w}{\partial u^2} = \sum_\nu\ 2(2\nu+1)\{-\nu a_{\nu-1} + (\nu+1)a_{\nu+1}\}y^{2\nu}\Delta(y)$$

D'un autre côté, (10.4.3) implique que

$$\frac{\partial^2 w}{\partial^2 u} = \frac{\partial^2 w}{\partial^2 t} = \sum_\nu \frac{\partial^2 a_\nu(t)}{\partial^2 t}\, y^{2\nu}\, \Delta(y)$$

Il en suit que

$$\frac{\partial^2 a_\nu(t)}{\partial^2 t} = 2(2\nu+1)\{-\nu a_{\nu-1} + (\nu+1)a_{\nu+1}\} \tag{10.5.1}$$

Ceci est une relation de recursion. En substituant $u = 0$ dans (10.4.3), on obtient (en tenant compte que $\Delta(y(0)) = 1$):

$$a_0 = x;\ a_{-1} = 0 \tag{10.5.2}$$

10.6. Pour résoudre (10.5.1), (10.5.2), rémarquons que pour chaque fonction $f(x) = f(x(t))$,

$$\frac{\partial^2 f}{\partial t^2} = \frac{\partial^2 f}{\partial x^2}\left(\frac{\partial x}{\partial t}\right)^2 + \frac{\partial f}{\partial x}\frac{\partial^2 x}{\partial t^2}$$

Prenons $f = x^{2\nu+1}$:

$$\frac{\partial^2 (x^{2\nu+1})}{\partial t^2} =$$

$$= (2\nu+1)2\nu x^{2\nu-1}(1-x^4) + (2\nu+1)x^{2\nu}(-2x^3) =$$

$$= (2\nu+1)2\nu x^{2\nu-1} - (2\nu+1)(2\nu+2)x^{2\nu+3}$$

En comparant avec (9.9.1), (9.9.2), on trouve

$$a_\nu = (-1)^\nu x^{2\nu+1} = x\cdot(-x^2)^\nu \tag{10.6.1}$$

De là,

$$w(t,y) = \sum_\nu a_\nu(t) y^{2\nu}\Delta(y) = \frac{x\Delta(y)}{1+x^2y^2}$$

Donc

$$\phi(t+u) + \phi(t-u) = \frac{2x\Delta(y)}{1+x^2y^2}$$

En échangeant t avec u,

$$\phi(t+u) - \phi(t-u) = \frac{2y\Delta(x)}{1+x^2y^2},$$

d'où

$$\phi(t+u) = \frac{x\Delta(y) + y\Delta(x)}{1+x^2y^2}$$

Ceci prouve le théorème d'addition.

10.7. *Exercice.* En déduire que:

$$\psi(t+u) = \frac{\psi(t)\psi(u) - \phi(t)\phi(u)\tilde{\psi}(t)\tilde{\psi}(u)}{1+\phi(t)^2\phi(u)^2}$$

$$\tilde{\psi}(t+u) = \frac{\tilde{\psi}(t)\tilde{\psi}(u) + \phi(t)\phi(u)\psi(t)\psi(u)}{1+\phi(t)^2\phi(u)^2}$$

Démontrons par exemple la première formule. On a

$$\psi(t+u)^2 = 1 - \phi(t+u)^2 =$$

$$= 1 - \frac{(\phi(t)\Delta(u) + \phi(u)\Delta(t))^2}{(1+\phi(t)^2\phi(u)^2)^2} = (1+\phi(t)^2\phi(u)^2)^{-2}\times$$

$$\times \{1 + 2\phi(t)^2\phi(u)^2 + \phi(t)^4\phi(u)^4 -$$

$$-\phi(t)^2(1-\phi(u)^4) - \phi(u)^2(1-\phi(t)^4) - 2\phi(t)\psi(u)\tilde{\psi}(u)\phi(u)\psi(t)\tilde{\psi}(t)\}$$

D'un autre côté, le carré du membre droit sera

$$(1+\phi(t)^2\phi(u)^2)^{-2} \times \{(1-\phi(t)^2)(1-\phi(u)^2) +$$

$$+\phi(t)^2\phi(u)^2(1+\phi(t)^2)(1+\phi(u)^2) - 2\phi(t)\psi(u)\tilde{\psi}(u)\phi(u)\psi(t)\tilde{\psi}(t)\}$$

Il est aisé à voir que les numérateurs sont égaux, d'où l'assertion.

10.8. *Périodes.* Par définition,

$$\phi(\pm\omega/4) = \pm 1;\ \phi(\pm i\omega/4) = \pm i \tag{10.8.1}$$

d'où

$$\psi(\pm\omega/4) = \Delta(\pm\omega/4) = 0,\ \tilde{\psi}(\pm\omega/4) = \sqrt{2} \tag{10.8.2}$$

$$\tilde{\psi}(\pm i\omega/4) = \Delta(\pm i\omega/2) = 0,\ \psi(\pm i\omega/4) = \sqrt{2} \tag{10.8.3}$$

Le théorème d'addition nous fournit

$$\phi(t \pm \omega/4) = \pm\ \psi(t)/\tilde{\psi}(t) \tag{10.8.4}$$

$$\phi(t \pm i\omega/4) = \pm i\tilde{\psi}(t)/\psi(t) \tag{10.8.5}$$

Il en suit que

$$\phi(\omega/4 + t) = \phi(\omega/4 - t),\ \phi(i\omega/4 + t) = \phi(i\omega/4 - t) \tag{10.8.6}$$

En faisant $u = t + \omega/4$ (resp. $u = t + i\omega/4$) on obtient

$$\phi(u + \omega/2) = -\phi(u),\ \phi(u + it\omega/2) = -\phi(u), \tag{10.8.7}$$

d'où

$$\phi(u + n\omega/2 + mi\omega/2) = (-1)^{m+n}\phi(u)\ (m, n \in \mathbb{Z}) \tag{10.8.8}$$

En particulier, $\phi(t)$ est périodique, avec deux périodes, ω et $i\omega$.

10.9. *Exemple.*

$$\phi(2t) = \frac{2\phi(t)\Delta(t)}{1+\phi(t)^4}$$

$$\psi(2t) = \frac{\psi(t)^2 - \phi(t)^2\tilde{\psi}(t)^2}{1+\phi(t)^4} =$$

$$= \frac{1-\phi(t)^2 - \phi(t)^2(1+\phi(t)^2)}{1+\phi(t)^4} =$$

$$= \frac{1-2\phi(t)^2 - \phi(t)^4}{1+\phi(t)^4}$$

De même,

$$\tilde{\psi}(2t) = \frac{\tilde{\psi}(t)^2 + \phi(t)^2\psi(t)^2}{1+\phi(t)^4} =$$

$$= \frac{1+2\phi(t)^2 - \phi(t)^4}{1+\phi(t)^4},$$

d'où

$$\Delta(2t) = \frac{(1-\phi(t)^4)^2 - 4\phi(t)^4}{(1+\phi(t)^4)^2} =$$

$$= \frac{1-6\phi(t)^4 + \phi(t)^8}{(1+\phi(t)^4)^2}$$

Ensuite,

$$\phi((2+i)t) = \phi(2t+it) = \frac{\phi(2t)\Delta(t) + i\phi(t)\Delta(2t)}{1-\phi(2t)^2\phi(t)^2}$$

Posons $x := \phi(t)$. On aura:

$$\phi(2t)\Delta(t) = \frac{2x(1-x^4)}{1+x^4}$$

$$i\phi(t)\Delta(2t) = i\ \frac{x(1-6x^4+x^8)}{(1+x^4)^2},$$

donc le numérateur:

$$\phi(2t)\Delta(t) + i\phi(t)\Delta(2t) =$$

$$= x\frac{2(1-x^8) + i(1-6x^4+x^8)}{(1+x^4)^2} = x\frac{2+i-6ix^4+(-2+i)x^8}{(1+x^4)^2}$$

Le dénominateur:

$$1-\phi(2t)^2\phi(t)^2 = 1-x^2\frac{4x^2(1-x^4)}{(1+x^4)^2} = \frac{1-2x^4+5x^8}{(1+x^4)^2}$$

Donc

$$\phi((2+i)t) = x\frac{2+i-6ix^4+(-2+i)x^8}{1-2x^4+5x^8}$$

On a

$$1-2a+5a^2 = 5(a+\frac{-1-2i}{5})(a+\frac{-1+2i}{5})$$

Par contre, les racines de l'équation $2+i-6ia+(-2+i)a^2=0$ sont:

$$a_{1,2}=\frac{3i\pm\sqrt{-9-(2+i)(-2+i)}}{-2+i}=$$

$$=\frac{3i\pm\sqrt{-4}}{-2+i}=-\frac{i+2}{5}(3i\pm 2i),\ a_1=-\frac{i(i+2)}{5}=\frac{1-2i}{5};\ a_2=1-2i$$

D'où

$$2+i-6ia+(-2+i)a^2=(i-2)(a-1+2i)(a-\frac{1-2i}{5})$$

Il en suit que

$$\phi((2+i)t)=-ix\frac{1-2i-x^4}{-1+(1-2i)x^4}$$

10.9.1. *Exercice.* Montrer que

$$\phi(3x)=-\phi(x)\frac{3-6\phi(x)-\phi(x)^4}{-1-6\phi(x)^4+3\phi(x)^8}$$

10.10. Rappelons qu'un nombre $m=a+bi\in\mathbb{Z}[i]$ est appelé *impair* s'il satisfait aux conditions équivalentes ci-dessous:

(i) m est premier à 2;

(ii) $1+i$ ne divise pas m;

(iii) $a+b$ est impair

(Exercice: montrer l'équivalence.)

Chaque nombre impair est congru à l'unique $i^\nu,\ 0\le\nu\le 3$ modulo $(2+2i)$. m est appelé *primaire* si $m\equiv 1\pmod{2+2i}$.

10.10.1. *Exercice.* $m=a+bi$ est primaire ssi $a=2a'+1,\ b=2b',\ a,',b'\in\mathbb{Z}$ et $a'+b'$ est pair.

Le théorème suivant généralise l'exemple 10.3.

10.11. *Théorème.* Soit $m=a+bi$ impair, $p=N(m)=a^2+b^2=4k+1$. Alors

$$\phi(mt)=\phi(t)\frac{P(\phi(t)^4)}{Q(\phi(t)^4)} \tag{10.11.1}$$

où $P(z),Q(z)\in\mathbb{Z}[i][z]$ sont des polynômes de degré k, $Q(0)=1$.

10.11.1. *Exercice.* Vérifier le théorème pour $p=13=3^2+2^2$, $m=3+2i$.

Reponse:

$$\frac{P(z)}{Q(z)}=\frac{3+2i+(7-4i)z+(-11+10i)z^2+z^3}{1+(-11+10i)z+(7-4i)z^2+(3+2i)z^3} \tag{10.11.2}$$

10.12. Posons $x := \phi(t),\ y = \phi(mt)$. Alors $dx = \phi'(t)dt = \sqrt{1-x^4}dt,\ dy = m\sqrt{1-y^4}dt$, d'où

$$\frac{dy}{\sqrt{1-y^4}} = m\frac{dx}{\sqrt{1-x^4}},$$

ou

$$\frac{dy}{dx} = m\frac{\sqrt{1-y^4}}{\sqrt{1-x^4}}$$

10.12.1. *Exercice.* Montrer que $y(x)$ satisfait à l'équation différentielle

$$(1-x^4)y'' - 2x^3y' + 2m^2y^3 = 0$$

(comparer avec 2.23).

On a $y_{x=0} = y_{t=0} = 0$, donc $(dy/dx)_{x=0} = m$. Il en suit que

$$y = x\frac{m + A_1x^4 + \ldots + A_kx^{4k}}{1 + B_1x^4 + \ldots + B_kx^{4k}} = x\frac{P(x^4)}{Q(x^4)} \tag{10.12.1}$$

10.13. Faisons une substitution $u = y^{-1},\ v = x^{-1}$. Alors $du/dv = -(x^2/y^2)\cdot(dy/dx)$, d'où

$$\left(\frac{du}{dv}\right)^2 = m^2\frac{x^4}{y^4}\frac{1-y^4}{1-x^4} = m^2\frac{1-u^4}{1-v^4}$$

donc

$$\frac{du}{dv} = (-1)^\mu m\frac{\sqrt{1-u^4}}{\sqrt{1-v^4}},$$

où le signe $(-1)^\mu$ sera déterminé plus tard. Posons $w = (-1)^\mu u$. Alors la fonction $w(v)$ satisfait à léquation différentielle

$$\frac{dw}{dv} = m\frac{\sqrt{1-w^4}}{\sqrt{1-v^4}};\ w(0) = 0,$$

et

$$w(v) = (-1)^\mu v\frac{Q(v^{-1})}{P(v^{-1})},$$

Il en suit que $w(v) = vP(v)/Q(v)$, donc

$$(-1)^\mu\frac{Q(v^{-1})}{P(v^{-1})} = \frac{P(v)}{Q(v)}$$

D'ici

$$B_j = (-1)^\mu A_{k-j},\ j = 0, \ldots, k \tag{10.13.1}$$

Pour déterminer le signe, on utilise

10.14. *Exercice.* Si $a, b \in \mathbb{Z}$,

$$\phi((1+2a+2bi)\frac{\omega}{4}) = (-1)^{a+b}$$

Maintenant si $m = 1 + 2a + 2bi$, substituons dans (10.12.1) $t = \omega/4$, donc $x = \phi(\omega/4) = 1$, $y = \phi(m\omega/4) = (-1)^{a+b}$; en tenant compte de (10.13.1), on obtient

$$(-1)^{a+b} = \frac{\sum A_j}{\sum B_j} = (-1)^{\mu}$$

10.16. *Corollaire.* Soit $m = a + bi$ primaire, donc (cf. 10.10.1) $a = 2a' + 1$, $b = 2b'$, $a', b' \in \mathbb{Z}$ et $a' + b'$ est pair. Alors dans l'expression (10.12.1)

$$y = \phi(mt) = x\frac{m + A_1x^4 + \ldots + A_{k-1}x^{4k-4} + x^{4k}}{1 + A_{k-1}x + \ldots + A_1x^{4k-4} + mx^{4k}} = x\frac{P(x^4)}{Q(x^4)} \qquad (10.16.1)$$

où $x = \phi(t)$.

10.17. *Théorème* (Eisenstein) Dans les notations 10.11, 10.12, supposons que m est premier dans $\mathbb{Z}[i]$. Alors tous les coefficients A_j sauf A_k sont divisibles par m.

Démonstration. Par hypothèse, m est impair. On a $N(m) = a^2 + b^2 = p = 4k+1$ où $p > 2$ est premier. Introduisons la notation

$$y = x\frac{P(x^4)}{Q(x^4)} = \frac{U(x)}{V(x)}$$

Donc

$$U(x) = A_0x + A_1x^5 + \ldots + A_{k-1}x^{p-4} + A_kx^p,\ A_0 = m$$
$$V(x) = 1 + B_1x^4 + \ldots + B_kx^{p-1}$$

Par hypothèse

$$\frac{dy}{dx} = V^{-2}(U'V - UV') = m\frac{\sqrt{1 - U^4/V^4}}{\sqrt{1 - x^4}},$$

d'où

$$U'V - UV' = m\frac{\sqrt{V^4 - U^4}}{\sqrt{1 - x^4}} =: mT(x) \qquad (10.17.1)$$

D'une part, le membre gauche de cette égalité appartient à $\mathbb{Z}[i][x]$, donc $T(x) \in \mathbb{Q}(i)[x]$.

D'autre part, $V^4 - U^4 \in \mathbb{Z}[i][x]$ est un polynôme avec $(V^4 - U^4)(0) = 1$ tel que $(V^4 - U^4)(x) = 0$ si $x^4 = 1$ (cf. la fin de 10.15), donc il est divisible par $1 - x^4$ dans $\mathbb{Z}[i][x]$. Autrement dit, $T^2 \in \mathbb{Z}[i][x]$ et $T(0) = 1$.

10.17.1. *Lemme.* Soit R un anneau principal, K son corps des fractions, $T(x) \in K[x]$ un polynôme tel que $T(x)^2 \in R[x]$ et $T(0) = 1$. Alors $T(x) \in R[x]$.

Exemple. $T(x) = 1 + ax$, $T(x)^2 = 1 + 2ax + a^2x^2$, donc $a^2 \in R$, d'où $a \in R$.

Exercice. (a) Vérifier le lemme pour $\deg(T) = 2, 3, 4$. (b) Prouver le cas général.

Donc $T(x) \in \mathbb{Z}[i][x]$. Donc d'après (10.17.1) tous le coefficients de $U'V - UV'$ sont divisibles par m. Or:

$$U'(x) = A_0 + 5A_1x^4 + \ldots + (p-4)A_{k-1}x^{p-5} + pA_kx^{p-1}$$

et

$$V'(x) = B_1 + 4B_1x^3 + \dots ,$$

d'où

$$U'V - V'U = \sum_j C_j x^{4j} = A_0 + (5A_1 - 3A_0B_1)x^4 + \dots$$

On a $C_j = (4j+1)A_j + \dots$. Donc par récurrence $m \mid (4j+1)A_j$ pour $j < k$. Or m est premier à $4j+1$ pour $j < k$ (expliquer!), donc $m \mid A_j$, cqfd.

10.18. *Corollaire.* Sous les hypothèses 10.17, le polynôme $P(x^4) \in \mathbb{Z}[i][x]$ est irréductible.

Grace à critère d'Eisenstein 3.5.

10.19. *Théorème* (Gauss, Eisenstein) Soit $m = a + bi$ premier et primaire, $p = m\bar{m} = (a+bi)(a-bi) = 4k+1$. Alors

$$m \equiv (-1)^k \binom{2k}{k} \pmod{\bar{m}} \tag{10.19.1}$$

Démonstration. Posons pour briévité

$$\Gamma := (-1)^k \binom{2k}{k} \tag{10.19.2}$$

Nous utilisons corollaire 10.16. Considérons y dans (10.16.1) comme une série formelle en x:

$$y = \frac{U(x)}{V(x)} = c_1x + c_5x^5 + c_9x^9 + \dots = R(x) \in \mathbb{Z}[i][[x]]$$

Donc on aura $U = RV$. D'après 10.17, $U \equiv x^p \pmod{m}$, $V \equiv 1 \pmod{m}$, d'où

$$R(x) \equiv x^p \pmod{m} \tag{10.19.3}$$

Il en suit que $dR/dx \equiv 0 \pmod{m}$.

Considérons la série $m^{-1}dy/dx = m^{-1}dR/dx \in \mathbb{Z}[i][[x]]$. On a

$$\frac{1}{m}\frac{dy}{dx} = \sqrt{\frac{1-R(x)^4}{1-x^4}}$$

La congruence (10.19.3) entraîne:

$$\frac{1-R(x)^4}{1-x^4} \equiv \frac{1-x^{4p}}{1-x^4} \equiv \frac{(1-x^4)^p}{1-x^4} = (1-x^4)^{p-1} \pmod{m}$$

De là, on déduit que

$$\sqrt{\frac{1-R(x)^4}{1-x^4}} \equiv (1-x^4)^{(p-1)/2} = (1-x^4)^{2k} \pmod{m}$$

(utiliser 9.4.1). Autrement dit,

$$\frac{1}{m}\frac{dR}{dx} \equiv (1-x^4)^{2k} \pmod{m}$$

Le coefficient à $x^{4k} = x^{p-1}$ à gauche est $m^{-1}pc_p = \bar{m}c_p \equiv \bar{m} \pmod{m}$.

D'un autre côté, le coefficient à x^{4k} à droite est $(-1)^k\binom{2k}{k} = \Gamma$. Il en suit que

$$\bar{m} \equiv \Gamma \pmod{m}$$

La congruence cherchée (10.19.1) est sa conjuguée complexe.

10.20. *Corollaire* (Gauss) Sous les hypothèses 10.19,

$$2a \equiv \Gamma \pmod{p}$$

Exercice.

Bibliographie

[A] N.H.Abel, Recherches sur les fonctions elliptiques, Crelles J., Bd. 2,3 (1827, 1828) = Œuvres Complètes, t. I, Deuxième édition, Éditions Jacques Gabay, pp. 263 - 388.

[BS] Z.Borevič et I.Šafarevič, Théorie de nombres (traduit de russe), Gauthiers-Villars, 1967.

[E] G.Eisenstein (a) Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, Crelles J. 39 (1850), 160 - 179 = Werke, Bd. II, Chelsea, pp. 536 - 555. (b) Neuer Beweis der Summationformeln, Crelle's J. 30 (1846), 211 - 214 = Werke, Bd. I, pp. 325 - 328. (c) Ableitung des biquadratischen Fondamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsformeln, Crelles J. 30 (1846), 185 - 210 = Werke, Bd. I, pp. 299 - 324.

[Ga] E.Galois, Sur la théorie des nombres, Bulletin des Sciences (de Férrusac), tome XIII (1830), p. 428 = Œvres mathématiques, Éditions Jacques Gabay, pp. 398 - 407.

[G] C.F.Gauss (a) Disquisitiones arithmeticae, 1801, Werke, Bd. I. Traduction française: Recherches arithmétiques, Jacques Gabay, 1989. (b) Theoria residuorum biquadraticorum, Commentatio prima, Comm. soc. reg. sci. Gott. 6(1828) = Werke, Bd. II, pp. 65 - 92. (c) Theoria residuorum biquadraticorum, Commentatio secunda, Comm. soc. reg. sci. Gott. 7(1832) = Werke, Bd. II, pp. 93 - 148.

[IR] K.Ireland, M.Rosen, A classical introduction to modern number theory, Springer, GTM **87**.

[L] F.Lemmermeyer, Reciprocity laws from Euler to Eisenstein, Springer-Verlag, 2000.

[S] J.-P.Serre, Cours d'arithmétique, PUF, 1995.

[Wa] L.Washington, Introduction to cyclotomic fields, Springer, 1982.

[W] A.Weil (a) Number theory. An approach through history, from Hammurapi to Legendre, Birkhäuser, 1984. (b) La cyclotomie jadis et naguère, Sem. Bourbaki, Juin 1974 = Œuvres scientifiques, tome III, pp. 311 - 327. (c) Sur les sommes de trois et quatre carrés, Enseign. Math. XX (1974), 215 - 222 = Œuvres scientifiques, tome III, pp. 303 - 310.

[WW] E.T.Whittaker, G.N.Watson, A course of modern analysis, Cambridge University Press, 1927.