SUJETS D'ARITHMÉTIQUE

Cours Maitrise Printemps 2007

Vadim Schechtman

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)

Pafnuty Lvovich CHEBYSHEV (1821 - 1894)

Évariste GALOIS (1811 - 1832)

Gotthold EISENSTEIN (1823 - 1852)

Bernhard RIEMANN (1826 - 1866)

§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 s'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 s'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 s'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 s'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.

1.9.1. *Exercice.* Montrer que $\mathbb{F}_q \subset \mathbb{F}_{q'}$ ssi $q = p^f,\ q' = p^{f'}$ et $f | f'$ (cf. 1.22 (b)).

(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

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

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

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

En effet, par le petit Fermat on connaît $p-1$ 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 s'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 1.22 (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.

(d) Calculer le nombre de polynômes irréductibles de degré 3 sur $\mathbb{F}_7$.

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

$$(a + bi)^7 = a^7 + b^7 i^7 = a + 4bi,$$

$$(a + bi)^{14} = a^2 + 8abi + 16b^2 i^2 = a^2 + abi + 2b^2 i^2,$$

ensuite,

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

(vérifier!), d'où deux équations

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

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 s'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 s'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, α est un élément d'ordre 8, donc $\alpha \in \mathbb{F}_q$ ssi $\mathbb{F}_q^*$ contient en élément d'ordre 8, donc $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$ où n est minimal tel que $8|(p^n - 1)$.

Il s'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

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

d'où

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

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 $A = \mathbb{Z}[\zeta]$. Considérons le polynôme

$$f_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$$

D'après (2.8.1) on a l'homomorphisme surjectif d'anneaux

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

2.9. *Théorème.* ϕ est un isomorphisme.

Pour une preuve voir 3.9.

D'ailleurs, on peut considérer (avec Gauss) tous ce qui se 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 $g_R + g_N = -1$ (pourquoi?). 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 s'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 s'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* (Gauss, Eisenstein) (a) Montrer que $f_m(t)$ satisfait à l'équation différentielle

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

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

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

(c) En déduire que

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

$$= \sum_{j=0}^{(m-1)/2} (-1)^j \cdot \frac{m(m^2-1^2)(m^2-3^2)\ldots(m^2-(2j-1)^2)}{(2j+1)!} \cdot t^{2j+1}$$

[En effet, soit

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$$

une solution de (b). Alors:

$$0 = (1-t^2) \sum_{i=2}^{\infty} i(i-1) a_i t^{i-2} - t \sum_{i=1}^{\infty} i a_i t^{i-1} + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= \sum_{i=0}^{\infty} (i+2)(i+1) a_{i+2} t^i - \sum_{i=2}^{\infty} i(i-1) a_i t^i +$$

$$- \sum_{i=1}^{\infty} i a_i t^i + m^2 \sum_{i=0}^{\infty} a_i t^i =$$

$$= 2a_2 + m^2 a_0 + (6a_3 - a_1 + m^2 a_1) \cdot t +$$

$$+\sum_{i=2}^{\infty}\Big\{(i+2)(i+1)a_{i+2}-i(i-1)a_i-ia_i+m^2a_i\Big\}\cdot t^i,$$

d'où:

$$2a_2+m^2a_0=0,\ \text{i.e. } a_2=-m^2a_0/2;$$

$$6a_3+(m^2-1)a_1=0,\ \text{i.e. } a_3=-(m^2-1)a_1/6$$

et

$$(i+2)(i+1)a_{i+2}+\big(m^2-i^2\big)\big)a_i=0,$$

i.e.

$$a_{i+2}=-\frac{m^2-i^2}{(i+2)(i+1)}\cdot a_i,\ i\geq 2$$

Maintenant on rémarque que chez $f(t)=f_m(t)$, $a_0=f_m(0)=0$ et $a_1=f'_m(0)=m$, d'où la formule (c) est immédiate.]

(d) On note que si $m\in\mathbb{C}-\{0,\pm1,\pm3,\dots\}$ alors on obtient comme $f_m(t)$ une série infinie:

$$f_m(t)==\sum_{j=0}^{\infty}(-1)^j\cdot\frac{m(m^2-1^2)(m^2-3^2)\dots(m^2-(2j-1)^2)}{(2j+1)!}\cdot t^{2j+1}$$

Montrer que cette série converge absolument si $|t|<1$, uniformément sur chaque disque fermé $|t|\leq r<1$.

[Ceci est une conséquence immédiate du

Critère de d'Alembert. Si $\sum_{n=0}^{\infty}\ b_n$ est une série telle qu'il existent $r<1$ et n_0 tels que

$$\frac{|b_n|}{|b_{n+1}|}\leq r$$

pour $n\geq n_0$, alors cette série converge absolument.]

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

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

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

(b) Soit $f(t)=e^{2\pi it}-e^{-2\pi it}$. 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,

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

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.

Un théorème de Fermat

2.27. *Exercice.* (a) Montrer que l'anneau de nombres gaussiens $A = \mathbb{Z}[i]$ est euclidien par rapport à la norme $N(a+bi) = a^2 + b^2$.

(b) Montrer que $x \in A$ est inversible ssi $N(x) = 1$. En conclure que $A^* = \{\pm 1, \pm i\}$.

(c) Un nombre $x \in A$ est dit *premier* si $x = yz$ implique que soit y, soit z est inversible. Si x est premier et $x \not| y$ alors $(x, y) = A$ ("théorème de Bezout"). Si x est premier et $x|(yz)$ alors $x|y$ ou $x|z$.

Soit p un nombre premier dans $\mathbb{Z}$ de la forme $4k+1$.

(d) Il existe $a \in \mathbb{Z}$ tel que $a^2 + 1 \equiv 0 (\mathrm{mod} p)$.

(e) p est n'est pas premier dans A.

En effet, si a est comme dans (d), alors $p|(a^2+1) = (a+i)(a-i)$. Si p etait premier alors il diviserait soit $a+i$, soit $a-i$. Par exemple, si $p|(a+i)$ alors $a + i = p(a' + b'i)$ ce qui est évidemment impossible.

(f) Il existent $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

En effet, d'après (e), $p = xy$ avec x, y non-inversibles. En prenant la norme, $p^2 = N(x)N(y)$ avec $N(x), N(y) > 1$, d'où $p = N(x) = N(y)$.

§3. Critère d'Eisenstein

Lemme de Gauss

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 $(a_0, \ldots, a_n) = A$.

Chaque $f(t) \in K[t]$ peut s'écrire sous une forme

$$f(t) = cf_p(t),\ c \in K,\ f_p(t) \in A[t],\ f_p(t) \text{ primitif} \tag{3.1.1}$$

3.2. *Théorème.* Soit $f(t) \in K[t]$ écrit en deux manières

$$f(t) = cf_p(t) = c' f'_p(t)$$

où $c, c' \in K$ et $f_p(t),\ f'_p(t)$ sont primitifs. Alors il existe une unité de A, $u \in A^*$ telle que $c' = uc$.

Démosntration. Écrivons $c = a/b,\ c' = a'/b'$ où $a, b, a', b' \in A$ et les fractions sont irréductibles; soient

$$f_p(t) = d_0 + \ldots + d_n t^n,\ f'_p(t) = d'_0 + \ldots + d'_n t^n$$

Donc

$$\frac{a}{b}\{d_0 + \ldots + d_n t^n\} = \frac{a'}{b'}\{d'_0 + \ldots + d'_n t^n\} \tag{3.2.1}$$

d'où

$$ab' d_i = a' b d' i,\ i = 0, \ldots, n$$

Soit p en diviseur premier de a; alors $p \not| b$. Si p ne divisait pas a' alors p diviserais tous d'_i ce qui est impossible puisque $f_p(t)$ est primitif par hypothèse. Donc $p|a'$. De même, si $p|b$ alors $p|b'$. En divisant (3.2.1) par p et en répétant, on arrive à la conclusion.

3.3. On peut exprimer cela en disant que pour un $f(t) \in K[t]$, dans l'écriture (3.1.1) l'élément c est défini à multiplication par une unité dans A près.

Donc le A-module $c(f) = (c) := cA \subset K$ ne depend que de f; il est appelé *le contenu* de f.

Évidemment, $f(t) \in A[t]$ ssi $c(f) \subset A$.

3.4. *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.

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

En effet, si $f = cf_p$ et $g = c'd_p$ alors $fg = cc'f_pg_p$. Puisque f_pg_p est primitif, $c(fg) = (cc') = (c)(c') = c(f)c(g)$.

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

Démonstration. En effet, supposons que $f(t) = g(t)h(t)$, avec $g, h \in K[t]$ de degrés > 0. Nous avons $g(t) = cg_p(t),\ h(t) = c'h_p(t)$, d'où $f(t) = cc'g_p(t)h_p(t)$. Le produit $g_p(t)h_p(t)$ est primitif par 3.4 et $f(t) \in A[t]$ donc $cc' \in A$ d'après théorème d'unicité 3.2. Donc $f = (cc'g_p) \cdot h_p$ est réductible dans $A[t]$.

Critère d'Eisenstein

3.7. *Théorème.* Soient $f(t) = a_0 + \ldots + a_nt^n \in A[t]$, $n > 0$, $p \in A$ un premier tel que: $p \nmid a_n,\ p| a_i$ pour $i < n$ et $p^2 \nmid a_0$. 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

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

On a $p^2 \nmid b_0c_0 = a_0$, donc $p \nmid b_0$ ou $p \nmid c_0$, disons $p \nmid b_0$; alors $p \mid c_0$. D'autre part $p \nmid a_n = b_mc_k$ entraîne $p \nmid c_k$. Soit r l'indice minimal tel que $p \nmid c_r$. On a $r \leq k < k + m = n$. Considérons

$$a_r = b_0c_r + b_1c_{r-1} + \ldots + b_rc_0$$

On a $p \nmid b_0c_r$ mais $p \mid b_ic_{r-i}$ pour $i > 0$, donc $p \nmid a_r$, contrairement à l'hypothèse.

3.8. *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.

3.9. *Corollaire.* Soit $\zeta = e^{2\pi i/p}$. Considérons l'homomorphisme

$$\phi :\ \mathbb{Z}[t]/(f) \longrightarrow \mathbb{Z}[\zeta],\ \phi(x) = \zeta$$

Alors ϕ est un isomorphisme.

Il est clair que ϕ est surjectif. Soit $g(t) \in \mathbb{Z}[t]$ tel que $g(\zeta) = 0$. Puisque $f(t)$ est irréductible dans $\mathbb{Q}[t]$, c'est le polynôme minimal de ζ, donc il existe $h(t) \in \mathbb{Q}[t]$ tel que $g(t) = h(t)f(t)$. Donc $c(g) = c(f)c(h) \subset A$; or, $c(f) = A$, d'où $c(h) = c(g) \subset A$; donc $g \in A[t]$. Il s'en suit que $g \in (f)$, i.e. ϕ est injectif.

3.10. *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 $g_p(t) = t f_p(t)$. 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 $k < p - 1$.

Variante: si $f_1(t), f_2(t) \in \mathbb{Z}[t]$ et $p \not| f_i,\ i = 1, 2$ alors $p \not| f_1 f_2$ (pourquoi?). Donc $p | g_p'(t)$, d'où $p | a_k$ pour $k < p - 1$.

§4. Formule de produit de Gauss

4.1. Cf. [G], (d). On pose

$$(m,\mu) = \frac{(1-x^m)(1-x^{m-1})\cdot\ldots\cdot(1-x^{m-\mu+1})}{(1-x)(1-xx)\cdot\ldots(1-x^\mu)}$$

("les coéfficients x-binomiaux"). Ici $\mu \in \mathbb{N}$.

Exemples: $(m,0) = 1$;

$$(-1,\mu) = \prod_{i=1}^{\mu} \frac{1-x^{-i}}{1-x^i} = (-1)^\mu x^{-\mu(\mu+1)/2}$$

Si $|x| < 1$, on peut définir

$$(-\infty,\mu) := \lim_{m\to\infty}(-m,\mu) = \frac{1}{(1-x)(1-xx)\cdot\ldots\cdot(1-x^\mu)}$$

Si $m \in \mathbb{N}$, $(m,\mu) = 0$ si $\mu > m$, et

$$(m,\mu) = (m, m-\mu)$$

4.2. On a

$$(m,\mu) = (m-1,\mu) + x^{m-\mu}(m-1,\mu-1) \tag{4.2.1}$$

Il s'en suit que si $m \in \mathbb{N},\ m > \mu+1$, alors

$$(m,\mu+1) = \sum_{i=0}^{m-\mu-1} (\mu+i,\mu)x^i$$

On en déduit par recurrence sur μ que (m,μ) est un polynôme en x si $m \in \mathbb{N}$.

4.3. On pose

$$f(x,m) = 1 - \frac{1-x^m}{1-x} + \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)} - \ldots = \sum_{\mu=0}^{\infty} (-1)^\mu (m,\mu)$$

Si $m \in \mathbb{N}$, la somme est finie:

$$f(x,m) = \sum_{\mu=0}^{m} (-1)^\mu (m,\mu)$$

On a $f(x,0) = 1,\ f(x,1) = (1,0) - (1,1) = 0$.

4.4. Il découle de (4.2.1):

$$(m,0) = 1$$

$$-(m,1) = -(m-1,1) - x^{m-1}$$

$$(m,2) = (m-1,2) + x^{m-2}(m-1,1), \text{ etc.},$$

d'où

$$f(x,m) = \sum_{i=0}^{\infty} (-1)^i (1-x^{m-1-i})(m-1,i)$$

Par contre,

$$(1-x^{m-1-i})(m-1,i) = (1-x^{m-1})(m-2,i),$$

d'où

$$f(x,m) = (1-x^{m-1}) f(x,m-2) \tag{4.4.1}$$

4.4. Supposons que $m \in \mathbb{N}$. Alors si m est pair (4.4.1) implique que

$$f(x,m) = (1-x)(1-x^3)\cdot\ldots\cdot(1-x^{m-1}) = \prod_{j=0}^{(m-2)/2} (1-x^{2j+1}) \tag{4.4.1}$$

Par contre, si m est impair, $f(x,m) = 0$ car $f(x,1) = 0$.

4.6. Si $m = -2k,\ k \in \mathbb{Z}, k > 0$, on obtient

$$f(x,-2k) = \frac{1}{(1-x^{-1})(1-x^{-3})\cdot\ldots\cdot(1-x^{-2k+1})}$$

(ici on considère $f(x,-2k)$ comme une série en x^{-1} convergeant si $|x| > 1$).

En faisant $k \to \infty$, on aura

$$f(x,-\infty) = \sum_{i=0}^{\infty} \frac{1}{(x-1)(xx-1)\cdot\ldots\cdot(x^i-1)} = \frac{1}{\prod_{n=0}^{\infty}(1-x^{-2n-1})},$$

où $|x| > 1$.

Pour tous $m \in \mathbb{Z}$, on obtient

$$f(x,m) = f(x,-\infty)(1-x^{m-1})(1-x^{m-3})\cdot\ldots = \frac{(1-x^{m-1})(1-x^{m-3})\cdot\ldots}{(1-x^{-1})(1-x^{-3})\cdot\ldots}$$

On posant $m = -1$:

$$f(x,-1) = 1 + x^{-1} + x^{-3} + x^{-6} + \ldots = \frac{(1-x^{-2})(1-x^{-4})\cdot\ldots}{(1-x^{-1})(1-x^{-3})\cdot\ldots}, \quad |x| > 1,$$

ou bien

$$\sum_{n=0}^{\infty} x^{n(n+1)/2} = 1 + x + x^3 + x^6 + \ldots = \frac{(1-xx)(1-x^4)\cdot\ldots}{(1-x)(1-x^3)\cdot\ldots}, \quad |x| < 1 \tag{4.6.1}$$

On peut récrire

$$\sum_{n=0}^{\infty} x^{n(n+1)/2} = \frac{1}{2} \sum_{n=-\infty}^{\infty} x^{n(n+1)/2}$$

et

$$\frac{\prod_{i=1}^{\infty}(1-x^{2i})}{\prod_{i=1}^{\infty}(1-x^{2i-1})}=\frac{\prod_{i=1}^{\infty}(1-x^{2i})^2}{\prod_{i=1}^{\infty}(1-x^i)}=$$

$$=\frac{\prod_{i=1}^{\infty}(1+x^i)^2(1-x^i)^2}{\prod_{i=1}^{\infty}(1-x^i)}=\prod_{i=1}^{\infty}(1+x^i)^2(1-x^i),$$

donc

$$\frac{1}{2}\sum_{n=-\infty}^{\infty}x^{n(n+1)/2}=\prod_{i=1}^{\infty}(1+x^i)^2(1-x^i),$$

ce qui est une formule standarte de la théorie des fonctions theta, cf. Jacobi, Fund., no. 66, (4); [W] (d), p. I, ch. IV, §9, (28).

4.7. Maintenant soit n un entier positif impair; posons $m=n-1$, et soit r une racine primitive de l'équation $x^n=1$; posons $x=r$. On a

$$(n-1,\mu)=\frac{(1-r^{n-1})(1-r^{n-2})\cdot\ldots\cdot(1-r^{n-\mu})}{(1-r)(1-rr)\cdot\ldots\cdot(1-r^{\mu})}$$

Or:

$$\frac{1-r^{n-i}}{1-r^i}=\frac{1-r^{-i}}{1-r^i}=-r^{-i},$$

d'où

$$(n-1,\mu)=(-1)^{\mu}r^{-\mu(\mu+1)/2}$$

Donc

$$f(r,n-1)=1+r^{-1}+r^{-3}+r^{-6}+\ldots r^{-n(n-1)/2}=(1-r)(1-r^3)\cdot\ldots\cdot(1-r^{n-2}),\tag{4.7.1}$$

par (4.4.1).

4.8. On peut remplacer dans (4.7.1) r par n'importe quel r^{λ} où $(\lambda,n)=1$; par exemple par r^{-2}:

$$\sum_{i=0}^{n-1}r^{i(i+1)}=1+r^2+r^6+r^{12}+\ldots+r^{n(n-1)}=$$

$$=(1-r^{-2\cdot1})(1-r^{-2\cdot3})\cdot\ldots\cdot(1-r^{-2(n-2)})\tag{4.8.1}$$

Soit $n=2k+1$; on a

$$1+3+5+\ldots+(2k-1)=k^2,$$

i.e.

$$1+3+\ldots+(n-2)=\frac{(n-1)^2}{4}$$

Multiplions les deux côtés de (4.8.1) par

$$1\cdot r\cdot r^3\cdot\ldots\cdot r^{n-2}=r^{(n-1)^2/4}=r^{k^2}$$

Rémarquons que

$$i(i+1)+k^2 \equiv (k-i)^2 (\text{mod } n),$$

donc à gauche on obtient

$$\sum_{i=0}^{2k} r^{(k-i)^2} = \sum_{i=0}^{n-1} r^{i^2}$$

car $i^2 \equiv (n-i)^2 \pmod{n}$. Il s'en suit que

$$1+r+r^2+\ldots+r^{(n-1)^2} = (r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\cdot\ldots\cdot(r^{n-2}-r^{-n+2}) \quad (4.8.2)$$

4.9. Soit p un nombre premier impair, $p = 2k+1$, $\zeta = e^{2\pi i/p}$. Considérons la somme de Gauss

$$g(\zeta) = \sum_{a=1}^{p-1} (\frac{a}{p})\zeta^a = \sum_{\rho\in R} \zeta^\rho - \sum_{\nu\in N} \zeta^\nu,$$

où R (resp. N) est l'ensemble des résidus (resp. des non-résidus) quadratiques. Puisque

$$1 + \sum_{\rho\in R} \zeta^\rho + \sum_{\nu\in N} \zeta^\nu = \sum_{a=0}^{p-1} \zeta^a = 0,$$

on a

$$g(\zeta) = 1 + 2\sum_{\rho\in R} \zeta^\rho = \sum_{n=0}^{p-1} \zeta^{a^2}$$

Donc

$$g(\zeta) = \prod_{s\in S} (\zeta^s - \zeta^{-s}) = (2i)^k \prod_{s\in S} \sin\ 2\pi s/p$$

où

$$S = \{1,3,5,\ldots,2k-1\}, \quad \text{Card}(S) = k = (p-1)/2$$

Supposons que k est impair, $k = 2j+1$, i.e. $p = 4j+3$. On a

$$S = \{1,3,5,\ldots,2j+1\} \coprod \{k+2, k+4, \ldots, k+2j\},$$

où $k+2 = p-k+1 \equiv -(k-1) \pmod{p}$, etc., d'où

$$\prod_{s\in S} \sin\ 2\pi s/p = (-1)^j \prod_{a=1}^{k} \sin\ 2\pi a/p,$$

donc

$$g(\zeta) = (2i)^{2j+1}(-1)^j \prod_{a=1}^{k} \sin\ 2\pi a/p = i2^{(p-1)/2} \prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$$

De même, si $k = 2j$, i.e. $p = 4j+1$,

$$g(\zeta) = 2^{(p-1)/2} \prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$$

4.9. Dans le produit $\prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p$, on a $0 < a < p/2$, donc $0 < 2\pi a/p < \pi$, d'où

$$\prod_{a=1}^{(p-1)/2} \sin\ 2\pi a/p > 0$$

D'autre part il est bien connu que $|g(\zeta)|^2 = p$. Il s'en suit que

$$g(\zeta) = \sqrt{p} \quad \text{si } p \equiv 1 \pmod 4$$

et

$$g(\zeta) = i\sqrt{p} \quad \text{si } p \equiv 3 \pmod 4$$

§5. Sommes de Gauss et de Jacobi

5.1. *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 s'en suit que

$$\chi(x)^{-1} = \bar{\chi}(x)$$

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 $a \mid (p-1)$.

5.1.1. *Exemple.* Le symbole de Legendre

$$\left(\frac{?}{p}\right) : \mathbb{F}_p^* \longrightarrow \{\pm 1\}$$

est un caractère d'ordre 2 ($p > 2$).

5.1.2. *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 $x = 1$.

5.2. *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, $g_a(\chi) \in \mathbb{Q}(\zeta_p, \zeta_{p-1})$.

5.2.1. *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 $g(\chi) := g_1(\chi)$.

5.3. *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,

$$|g_a(\chi)|^2 = g_a(\chi)\bar{g_a}(\chi) = \sum_{x,y} \chi(x)\bar{\chi}(y)\ \zeta^{a(x-y)},$$

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.

5.3.1. *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.

5.4. *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 $J(\chi, \chi') = J(\chi', \chi)$.

5.5. *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 s'en suit que

$$g(\chi)g(\chi') = \sum_c (\chi\chi')(c)\ J(\chi,\chi')\ \zeta^c = g(\chi\chi')J(\chi,\chi'),$$

cqfd.

Fonctions Γ *et* B *d'Euler.*

5.6. 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

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx, \quad \Re(s), \Re(t) > 0$$

5.7. *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.

Une autre démonstration (Jacobi, cf. [J]). On a

$$\Gamma(a)\Gamma(b) = \int_0^\infty \int_0^\infty e^{-x-y} x^{a-1} y^{b-1} dx dy$$

On fait le changement de variables $x + y = r,\ x = rw$, donc $0 \le r < \infty$, $0 \le w \le 1$ et $dxdy = rdwdr$, d'où

$$\Gamma(a)\Gamma(b) = \int_0^1 w^{a-1}(1-w)^{b-1} dw \int_0^\infty e^{-r} x^{a+b-1} dr = B(a,b)\Gamma(a+b)$$

5.8. *Exercice.* Rémarquons que

$$e^{-t} = \lim_{n\to\infty} \big(1 - \frac{t}{n}\big)^n,$$

d'où

$$\Gamma(s) = \lim_{n\to\infty} \int_0^n \big(1 - \frac{t}{n}\big)^n t^{s-1} dt \tag{5.8.1}$$

(pour une preuve, cf. 5.8.1 ci-dessous).

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 découle que

$$\Gamma(s) = \lim_{n\to\infty} n^s B(n+1, s) = \lim_{n\to\infty} n^s \frac{n!}{s(s+1)\cdot\ldots\cdot(s+n)} \tag{5.8.2}$$

(*formule d'Euler - Gauss*).

5.8.1. *Exercice.* Preuve de (5.8.1), cf. [WW], 12.2.

(a) Pour tous $0 \leq y < 1$,

$$1 + y \leq e^y \leq (1-y)^{-1}$$

(b) Pour tous $0 \leq \alpha \leq 1$,

$$(1-\alpha)^n \geq 1 - n\alpha$$

(c) Déduire de (a) et (b) que

$$0 \leq e^{-t} - \left(1 - \frac{t}{n}\right)^n \leq n^{-1} t^2 e^{-t}$$

pour tous $0 \leq t < n$.

[En effet, en faisant $y = t/n$ dans (a), on obtient:

$$1 + t/n \leq e^{t/n} \leq (1 - t/n)^{-1},$$

d'où

$$(1 + t/n)^n \leq e^t \leq (1 - t/n)^{-n},$$

et

$$(1 + t/n)^{-n} \geq e^{-t} \geq (1 - t/n)^n,$$

Il s'en suit:

$$0 \leq e^{-t} - (1 - t/n)^n = e^{-t} \cdot \left(1 - e^t \cdot (1 - t/n)^n\right) \leq$$

$$\leq e^{-t} \cdot \left(1 - (1 - t^2/n^2)^n\right)$$

D'un autre part, d'après (b) avec $\alpha = t^2/n^2$, on aura

$$1 - (1 - t^2/n^2)^n \leq t^2/n,$$

d'où le résultat.]

(d) En déduire que

$$\left| \int_0^n \left\{ e^{-t} - \left(1 - \frac{t}{n}\right)^n \right\} \cdot t^{s-1} dt \right| \to 0$$

quand $n \to \infty$.

[En effet, d'après (c),

$$\left| \int_0^n \left\{ e^{-t} - \left(1 - \frac{t}{n}\right)^n \right\} \cdot t^{s-1} dt \right| \leq n^{-1} \int_0^n e^{-t} t^{s+1} dt <\leq n^{-1} \int_0^\infty e^{-t} t^{s+1} dt,$$

ce qui $\to 0$, puisque la dernière intégrale converge.]

(e) En déduire (5.8.1).

5.8.2. *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

5.9. 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 $N(x) \neq 0 \Leftrightarrow x \neq 0$.

5.10. *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.

5.11. *Exercice.* Montrer que les anneaux des entiers dans les corps suivants sont euclidiens par rapport à la norme: $\mathbb{Q}(\sqrt{d})$ où $d = -1, -2, -3, -7, -11$.

5.12. *Exercice.* Les unités dans R sont $\pm 1, \pm i$, autrement dit,

$$R^* = \mu_4 := \{x \in \mathbb{C}^* \mid x^4 = 1\} \tag{5.12.1}$$

En effet, un $\alpha \in R$ est inversible ssi $N(\alpha) = 1$.

5.13. *Théorème* (Fermat) Soit $p > 2$ premier.

(a) Si $p \mid (a^2 + b^2)$ avec $a, b \in \mathbb{Z},\ p \not\mid a$, 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).

5.14. *Démonstration de* (a). Si $p \not\mid a$ 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 $p \equiv 1 \pmod 4$.

5.15. *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 s'en suit que la somme de Jacobi $J(\chi, \chi) \in R = \mathbb{Z}[i]$, soit $J(\chi, \chi) = a + bi$.

Théorème 5.5 (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 s'en suit que soit $\pi' = \epsilon\pi$, soit $\pi' = \epsilon\bar{\pi}$, avec $\epsilon \in R^*$. Ceci donne exactement 8 possibilités mentionnées ci-dessus.

5.16. *Exercice.* (a) Prouver que

$$(13) = (13, 5 - i)(13, 5 + i)$$

dans R.

(b) En faisant la division euclidienne dans R, prouver que $\text{pgcd}(13, 5-i) = 3-2i$, donc $(13, 5-i) = (3-2i)$.

5.17. *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

$$2a \equiv \binom{2\nu}{\nu} \pmod{p} \tag{5.17.1}$$

Cf. [G] (b), p. 90.

Ceci permet de trouver aisement a et b.

5.18. *Lemme clef.* Soit $p = \pi\bar{\pi}$ une décomposition dans R. Il existe une autre décomposition $p = J\bar{J}$,telle que

$$J \equiv 0 \pmod{\pi} \tag{5.18.1}$$

et

$$J \equiv \binom{2\nu}{\nu} \pmod{\bar{\pi}} \tag{5.18.2}$$

Ce lemme implique le théorème immédiatement: si $J = a + bi$, on a par (5.18.2):

$$a^2 - b^2 + 2ab\ i = J^2 \equiv \binom{2\nu}{\nu} J = \binom{2\nu}{\nu}(a + bi) \pmod{J\bar{\pi}}$$

Or, $J\bar{\pi} \equiv 0 \pmod{p}$ grace à (5.13.1), d'où

$$2ab \equiv \binom{2\nu}{\nu} b \pmod{p},$$

d'où (5.12.1) car b est premier à p.

5.19. 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 prouverons 5.18 en utilisant les sommes de Jacobi, comme dans [W] (b), pp. 317 - 315.

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,

$$\chi(\bar{a}) \equiv a^\nu \pmod \pi \tag{5.19.1}$$

Posons $J = -J(\chi, \chi)$; on veut calculer les restes de J modulo π et $\bar{\pi}$. Il découle de (5.19.1) que

$$J \equiv -\sum_{a=1}^{p-1} a^\nu (1-a)^\nu \pmod \pi$$

Or,

$$-\sum_{a=1}^{p-1} a^\nu (1-a)^\nu = -\sum_{a=1}^{p-1} \sum_{k=0}^{\nu} \binom{\nu}{k} (-1)^k a^{\nu+k}$$

5.20. *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 (5.18.1).

Maintenant prenons le conjugué complexe de (5.19.1):

$$\chi(\bar{a}^{-1}) = \bar{\chi}(\bar{a}) \equiv a^\nu \pmod{\bar{\pi}},$$

d'où

$$\chi(\bar{a}) \equiv a^{p-1-\nu} \pmod{\bar{\pi}} \tag{5.20.1}$$

(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 en conclut grace à une congruence un peu surprenante mais élémentaire:

5.21. *Sous-lemme.* On a

$$(-1)^\nu \binom{3\nu}{\nu} \equiv \binom{2\nu}{\nu} \pmod{p}$$

Exercice.

5.22. *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 reécrire (5.20.1) sous une forme

$$\chi(x) \equiv x^{-\nu} \pmod{\bar{\pi}},\ x \in \mathbb{F}_p$$

Il s'en suit:

$$J \equiv -\sum_{x \neq 0,1} x^{-\nu}(1-x)^{-\nu} (\mathrm{mod}\ \bar{\pi})$$

Maintenant on fait la sommation dans $\mathbb{F}_p$:

$$-\sum_{x\neq 0,1} x^{-\nu}(1-x)^{-\nu} = -\sum_{x\neq 0,1} x^{-2\nu}(x^{-1}-1)^{-\nu} = -\sum_{y\neq 0,1} y^{2\nu}(y-1)^{-\nu} =$$

$(z = y-1)$

$$= -\sum_{z\neq -1,0} (z+1)^{2\nu} z^{-\nu} = -\sum_{z\neq 0} (z+1)^{2\nu} z^{-\nu} = \binom{2\nu}{\nu},$$

la dernière égalité grace à 5.20.1.

5.23. *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 $p = 29$.

5.24. *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 s'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 $x \equiv 1 \pmod{2+2i}$.

6. Lemniscate

Fonctions trigonométriques

6.1. Définissons le *sinus* comme une fonction $s(t)$ telle que $s(0) = 0$ et qui satisfait à l'équation différentielle

$$s'(t) = \sqrt{1 - s(t)^2} := c(t) \tag{6.1.1}$$

La fonction $c(t)$ sera appelée le *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

$$a(s) = \int_0^s \frac{dx}{\sqrt{1 - x^2}} \tag{6.1.2}$$

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

$$\frac{\pi}{2} = \int_0^1 \frac{dx}{\sqrt{1 - x^2}} \tag{6.1.3}$$

(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, (6.1.1) (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 (6.1.1) implique:

$$s''(t) = -s(t), \ s'''(t) = -c(t), \tag{6.1.4}$$

etc.

Le *théorème d'addition* ci-dessous est fondamental:

6.2. *Théorème.*

$$s(t + u) = s(t)c(u) + c(t)s(u) \tag{6.2.1}$$

Démonstration. Soit $f(t, u) = s(t)c(u) + c(t)s(u)$; alors

$$\partial f/\partial t = c(t)c(u) - s(t)s(u) = \partial f/\partial u,$$

donc il existe une fonction $r(x)$ telle que $f(t, u) = r(t + u)$. En posant $u = 0$, on obtient $r(t) = s(t)$.

6.3. *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

$$s(t + \pi) = -s(t);\ c(t + \pi) = -c(t)$$

$$s(t + 2\pi) = s(t);\ c(t + 2\pi) = c(t)$$

6.4. *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.

6.4.1. Montrer que $\binom{1/2}{i} = 2^{-a}b,\ a, b \in \mathbb{N}$.

6.4.2. Déduire de (6.1.1) les développements de Taylor usuels pour sinus et cosinus.

Fonctions lemniscatiques

6.5. *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

$$(1 - r^4)s'^2 = 1, \quad \frac{ds}{dr} = \frac{1}{\sqrt{1 - r^4}}$$

6.6. Considérons une fonction

$$a(x) = \int_0^x \frac{dt}{\sqrt{1 - t^4}}, \tag{6.6.1}$$

Elle est bien définie et monotone sur l'interval $[0, 1]$. On pose

$$\frac{\omega}{4} = \int_0^1 \frac{dt}{\sqrt{1 - t^4}} \tag{6.6.2}$$

(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,

$$\int_0^1 \frac{dt}{\sqrt{1 - t^4}} = \frac{1}{4}\int_0^1 u^{-3/4}(1 - u)^{-1/2} du =$$

$$= \frac{1}{4}B(1/4, 1/2) = \frac{1}{4}\frac{\Gamma(1/4)\Gamma(1/2)}{\Gamma(3/4)} = \frac{\sqrt{\pi}}{4}\frac{\Gamma(1/4)}{\Gamma(3/4)}$$

En utilisant la relation

$$\Gamma(x)\Gamma(1 - x) = \frac{\pi}{\sin\ \pi x},$$

(cf. 7.3 ci-dessous), on en déduit

$$\Gamma(1/4)\Gamma(3/4) = \frac{\pi}{\sin\ \pi/4} = \sqrt{2}\ \pi,$$

d'où

$$\omega = \frac{\Gamma(1/4)^2}{\sqrt{2\pi}}$$

6.7. *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

$$C(r,R) = \{r \le z \le R\} \cup \{z = Re^{i\theta},\ 0 \le \theta \le 2\pi\} \cup$$

$$\cup \{R \ge z \ge r\} \cup \{z = re^{i\theta},\ 2\pi \ge \theta \ge 0\} =$$

$$= C_1 \cup C_2 \cup C_3 \cup C_4$$

Alors

$$I(R,r) = \int_{C_2} + \int_{C_4} + (1-e^{2\pi i(a-1)})\cdot\int_r^R \frac{u^{a-1}}{u+1}du = 2\pi i\,\mathrm{Res}_{z=-1}\frac{z^{a-1}}{z+1} = 2\pi i\cdot e^{\pi i(a-1)}$$

À la limite

$$\lim_{r\to 0,\ R\to\infty} \int_{C_2} = \lim_{r\to 0,\ R\to\infty} \int_{C_4} = 0,$$

d'où

$$I = 2\pi i \cdot \frac{e^{\pi i(a-1)}}{1-e^{2\pi i(a-1)}} = \frac{2\pi i}{e^{-\pi i(a-1)} - e^{\pi i(a-1)}} =$$

$$= \frac{2\pi i}{e^{\pi i a} - e^{-\pi i a}} = \frac{\pi}{\sin(\pi a)}$$

6.8. 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

$$\phi'(t) = \sqrt{1-\phi(t)^4} =: \Delta(t) \qquad (6.8.1)$$

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

$$\Delta(t) = \psi(t)\tilde{\psi}(t)$$

et

$$\phi'(t) = \psi(t)\tilde{\psi}(t) \tag{6.8.2}$$

Ensuite,

$$\psi'(t) = -\frac{2\phi(t)\phi'(t)}{2\sqrt{1 - \phi(t)^2}} = -\phi(t)\tilde{\psi}(t) \tag{6.8.3}$$

Enfin,

$$\tilde{\psi}'(t) = \phi(t)\psi(t) \tag{6.8.4}$$

6.9. *Prolongement à l'argument imaginaire.* Faisons dans (6.8.1) 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 s'en suit que

$$\tilde{\phi}(u) = \phi(t),$$

i.e.

$$\phi(it) = i\phi(t)$$

Donc

$$\psi(it) = \tilde{\psi}(t),\ \tilde{\psi}(it) = \psi(t),\ \Delta(it) = \Delta(t)$$

6.10. *Théorème d'addition.*

$$\phi(t + u) = \frac{\phi(t)\Delta(u) + \phi(u)\Delta(t)}{1 + \phi(t)^2\phi(u)^2}$$

Démonstration (Abel). On désigne le second membre par $\chi(t, u)$. On a

$$\frac{\partial\chi}{\partial t} = \frac{\partial}{\partial t}\left[\frac{\phi(t)\psi(u)\tilde{\psi}(u) + \phi(u)\psi(t)\tilde{\psi}(t)}{1 + \phi(t)^2\phi(u)^2}\right] =$$

$$= \frac{\phi'(t)\psi(u)\tilde{\psi}(u) + \phi(u)\psi'(t)\tilde{\psi}(t) + \phi(u)\psi(t)\tilde{\psi}'(t)}{1 + \phi(t)^2\phi(u)^2} -$$

$$-\frac{2[\phi(t)\psi(u)\tilde{\psi}(u)+\phi(u)\psi(t)\tilde{\psi}(t)]\cdot\phi(t)\phi'(t)\phi(u)^2}{(1+\phi(t)^2\phi(u)^2)^2}=$$

$$=\frac{\psi(t)\tilde{\psi}(t)\psi(u)\tilde{\psi}(u)-\phi(u)\phi(t)\tilde{\psi}(t)^2+\phi(u)\psi(t)^2\phi(t)}{1+\phi(t)^2\phi(u)^2}-$$

$$-\frac{2[\phi(t)\psi(u)\tilde{\psi}(u)+\phi(u)\psi(t)\tilde{\psi}(t)]\cdot\phi(t)\psi(t)\tilde{\psi}(t)\phi(u)^2}{(1+\phi(t)^2\phi(u)^2)^2}=$$

$$=\frac{\psi(t)\tilde{\psi}(t)\psi(u)\tilde{\psi}(u)-\phi(u)\phi(t)\tilde{\psi}(t)^2+\phi(u)\psi(t)^2\phi(t)}{1+\phi(t)^2\phi(u)^2}-$$

$$-\frac{2[\phi(t)\psi(u)\tilde{\psi}(u)+\phi(u)\psi(t)\tilde{\psi}(t)]\cdot\phi(t)\psi(t)\tilde{\psi}(t)\phi(u)^2}{(1+\phi(t)^2\phi(u)^2)^2}=$$

$$=(1+\phi(t)^2\phi(u)^2)^{-2}\cdot\Big\{(1+\phi(t)^2\phi(u)^2)[\psi(t)\tilde{\psi}(t)\psi(u)\tilde{\psi}(u)+\phi(u)\phi(t)(-\tilde{\psi}(t)^2+\psi(t)^2)]-$$

$$-2[\phi(t)^2\phi(u)^2\psi(t)\tilde{\psi}(t)\psi(u)\tilde{\psi}(u)+\phi(t)\phi(u)^3\psi(t)^2\tilde{\psi}(t)^2]\Big\}$$

Or,

$$A:=(1+\phi(t)^2\phi(u)^2)\phi(u)\phi(t)(-\tilde{\psi}(t)^2+\psi(t)^2)]=-2(1+\phi(t)^2\phi(u)^2)\phi(u)\phi(t)^3$$

et

$$B:=-2\phi(t)\phi(u)^3\psi(t)^2\tilde{\psi}(t)^2=-2\phi(t)\phi(u)^3(1-\phi(t)^4),$$

d'où

$$A+B=2(\phi(t)^5\phi(u)^3+\phi(u)^5\phi(t)^3)$$

Il s'en suit que

$$\frac{\partial\chi}{\partial t}(t,u)=\frac{\partial\chi}{\partial t}(u,t),$$

d'où

$$\frac{\partial\chi}{\partial t}=\frac{\partial\chi}{\partial u}$$

Comme une conséquence

$$\chi(t,u)=r(t+u)$$

pour quelque fonction r. En posant $u=0$, on obtient $r=\phi$.

Ceci prouve le théorème d'addition.

6.10.1. *Corollaire.*

$$\phi(u+v)-\phi(u-v)=\frac{2\phi(v)\Delta(u)}{1+\phi(u)^2\phi(v)^2} \qquad (a)$$

$$\phi(\alpha)-\phi(\beta)=\frac{2\phi((\alpha-\beta)/2)\Delta((\alpha+\beta)/2)}{1+\phi((\alpha-\beta)/2)^2\phi((\alpha+\beta)/2)^2} \qquad (b)$$

6.11. *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.

6.12. *Périodes.* Par définition,

$$\phi(\pm\omega/4) = \pm 1;\ \phi(\pm i\omega/4) = \pm i \tag{6.12.1}$$

d'où

$$\psi(\pm\omega/4) = \Delta(\pm\omega/4) = 0,\ \tilde{\psi}(\pm\omega/4) = \sqrt{2} \tag{6.12.2}$$

$$\tilde{\psi}(\pm i\omega/4) = \Delta(\pm i\omega/2) = 0,\ \psi(\pm i\omega/4) = \sqrt{2} \tag{6.12.3}$$

Le théorème d'addition nous fournit

$$\phi(t \pm \omega/4) = \pm\ \psi(t)/\tilde{\psi}(t) \tag{6.12.4}$$

$$\phi(t \pm i\omega/4) = \pm i\tilde{\psi}(t)/\psi(t) \tag{6.12.5}$$

Il s'en suit que

$$\phi(\omega/4 + t) = \phi(\omega/4 - t),\ \phi(i\omega/4 + t) = \phi(i\omega/4 - t) \tag{6.12.6}$$

En faisant $u = t + \omega/4$ (resp. $u = t + i\omega/4$) on obtient

$$\phi(u + \omega/2) = -\phi(u),\ \phi(u + i\omega/2) = -\phi(u), \tag{6.12.7}$$

d'où

$$\phi(u + n\omega/2 + mi\omega/2) = (-1)^{m+n}\phi(u)\ (m, n \in \mathbb{Z}) \tag{6.12.8}$$

En particulier, $\phi(t)$ est périodique, avec deux périodes, ω et $i\omega$.

6.13. *Exercice.* Prouver que $(1+i)\omega/2$ et $(1-i)\omega/2$ sont deux périodes de $\phi(t)$.

6.14. *Zéros et pôles.* Par définition, $\phi(0) = 0$ et $\phi'(0) = \Delta(0) = 1$, donc 0 est un zéro simple de $\phi(t)$. Il découle que tous points du réseau

$$Z = \mathbb{Z} \cdot (\omega/2) \oplus \mathbb{Z} \cdot (i\omega/2)$$

sont des zéros simples de $\phi(t)$.

Par contre, d'après (6.12.2 - 4), le point $\omega/4 + i\omega/4$ est un pôle de $\phi(t)$, et il est facile à voir que c'est un pôle simple. Donc tous points du réseau

$$P = \omega/4 + i\omega/4 + Z = \{(n+1/2) \cdot \omega/2 + (m+1/2)i\omega/2 |\ m, n \in \mathbb{Z}\}$$

sont des pôles simples de $\phi(t)$.

Théorème. Ce sont tous zéros et pôles de $\phi(t)$.

Preuve (Abel). Le comportement réel des fonctions $\phi(t)$, $\psi(t)$ et $\tilde{\psi}(t)$ est clair de 6.12: pour $t \in \mathbb{R}$ on a:

$-1 \leq \phi(t) \leq 1$ les zéros sont $n\omega/2,\ n \in \mathbb{Z}$, il n'y a pas de pôles;

$-1 \leq \psi(t) \leq 1$ les zéros sont $\omega/4 + n\omega/2,\ n \in \mathbb{Z}$, il n'y a pas de pôles;

$1 \leq \tilde{\psi}(t) \leq \sqrt{2}$ il n'y a pas ni de zéros, ni de pôles;

Dans le domaine complexe, on utilise le théorème d'addition:

$$\phi(\alpha + i\beta) = \frac{\phi(\alpha)\Delta(i\beta) + \Delta(\alpha)\phi(i\beta)}{1 + \phi(\alpha)^2\phi(i\beta)^2} = \frac{\phi(\alpha)\Delta(\beta) + i\Delta(\alpha)\phi(\beta)}{1 - \phi(\alpha)^2\phi(\beta)^2}$$

Zéros: si $z = \alpha + i\beta$ est un zéro de $\phi(t)$ alors

$$\phi(\alpha)\Delta(\beta) = 0 \text{ et } \Delta(\alpha)\phi(\beta) = 0$$

Si $\phi(\alpha) = 0$ alors $\Delta(\alpha) \neq 0$ donc $\phi(\beta) = 0$, donc $z \in Z$.

Si $\Delta(\beta) = 0$ alors $\psi(\beta) = 0$ donc $\beta = \omega/4 + n\omega/2$; alors $\phi(\beta) \neq 0$ donc $\Delta(\alpha) = 0$, d'où $z \in P$; mais on sait déjà que dans ce cas z est un pôle.

Pôles: si $z = \alpha + i\beta$ est un pôle, alors $1 = \phi(\alpha)^2\phi(\beta)^2$, d'où $z \in P$, qed.

6.15. *Exercice.* (a) Trouver tous zéros et pôles de $\psi(t)$ et de $\tilde{\psi}(t)$.

(b) À l'aide de 6.10.1 (b), résoudre l'équation $\phi(\alpha) = \phi(\beta)$.

§7. Multiplication complexe

7.1. *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 s'en suit que

$$\phi((2+i)t) = -ix\frac{1-2i-x^4}{-1+(1-2i)x^4}$$

7.2. *Exercice.* Montrer que

$$\phi(3x) = -\phi(x)\frac{3-6\phi(x)^4-\phi(x)^8}{-1-6\phi(x)^4+3\phi(x)^8}$$

7.3. 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 $m \equiv 1 \pmod{2+2i}$.

7.4. *Exercice. Classification "fine" des nombres impairs.* Soit $m = a+bi$ impair. Il y a 4 possibilités. Montrer que:

(1) $m = a+bi$ est primaire ssi $a = 2a'+1,\ b = 2b',\ a,', b' \in \mathbb{Z}$ et $a'+b'$ est pair;

(2) $m \equiv -1 \pmod{2+2i}$ ssi $a = 2a'+1,\ b = 2b',\ a,', b' \in \mathbb{Z}$ et $a'+b'$ est impair;

(3) $m \equiv i \pmod{2+2i}$ ssi $a = 2a',\ b = 2b'+1,\ a,', b' \in \mathbb{Z}$ et $a'+b'$ est pair;

(4) $m \equiv -i \pmod{2+2i}$ ssi $a = 2a',\ b = 2b'+1,\ a,', b' \in \mathbb{Z}$ et $a'+b'$ est impair.

Le théorème suivant généralise l'exemple 7.1.

7.5. *Théorème* (Abel). Soit $m = a + bi$ impair, $p = N(m) = a^2 + b^2 = 4k + 1$. Alors

$$\phi(mt) = \phi(t)\frac{P(\phi(t)^4)}{Q(\phi(t)^4)} \tag{7.5.1}$$

où $P(z), Q(z) \in \mathbb{Z}[i][z]$ sont des polynômes de degré k, $Q(0) = 1$.

Preuve (sketch). Posons

$$s(t) = \phi(\{(1+i)\omega/2\} \cdot t) \tag{7.5.2}$$

Cette fonction a comme réseau de périodes $A := \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z} \cdot i$. Les zéros de $s(t)$ sont $\mathbb{Z}[i]$ et ses pôles sont $1/2 + \mathbb{Z}[i]$. Il suffit de démontrer l'assertion du théorème avec $\phi(t)$ remplacée par $s(t)$.

(a) Tous d'abord, on prouve par récurrence, à l'aide des formules d'addition que

$$s(mt) = s(t)\frac{U(s(t)^4)}{V(s(t)^4)}$$

avec $U(u), V(u) \in \mathbb{Z}[i][u]$ et $V(0) = 1$.

(b) Soit $W(u)$ le pgcd de U et V dans $\mathbb{Q}(i)[u]$, donc $U = WU'$, $V = WV'$. Écrvons $W = c(W)W'$, $V' = c(V')V''$. On a $1 = c(U) = c(W)c(U')$, donc $V = W'V''$ avec $W', V'' \in \mathbb{Z}[i][u], c(W') = c(V'') = 1$.

De plus, $1 = V(0) = W'(0)V''(0)$, donc on peut supposer que $W'(0) = V''(0) = 1$.

On peut supposer que P, Q sont premiers entre eux dans $\mathbb{Q}(i)[u]$. Il s'en suit qu'ils ne peuvent pas avoir une racine commune $\beta \in \mathbb{C}$ (utiliser Bezout).

Les racines de P sont les racines de $\tilde{\phi}(mt)/\phi(t)$ qui sont $\phi(\alpha/m)$ où α parcourt un système de representants de $A/mA - \{0\}$. On a

$$\mathrm{Card}(A/mA) = N(m)$$

(exercice). D'un autre côté, on montre, en utilisant (6.10.1) (b) que toutes valeurs $\tilde{\phi}(\alpha/m)$ sont distincts et que toutes les racines sont simples, d'où $\deg P(u^4) = N(m) - 1$.

De même, les racines de Q = pôles de $\tilde{\phi}(mt)/\phi(t) =$

$$= \{\phi(\beta/m) | \beta \in (1/2 + A + mA)/mA\} := S$$

d'où $\deg Q(u^4) = \mathrm{Card}(S) = N(m) - 1$.

7.6. *Exercice.* Vérifier le théorème pour $p = 13 = 3^2 + 2^2$, $m = 3 + 2i$.

Réponse:

$$\frac{P(z)}{Q(z)} = \frac{3 + 2i + (7 - 4i)z + (-11 + 10i)z^2 + z^3}{1 + (-11 + 10i)z + (7 - 4i)z^2 + (3 + 2i)z^3} \tag{7.6.1}$$

7.7 *Exercice.* Vérifier le théorème pour $m \in \mathbb{Z}$.

7.8. 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

$$\frac{dy}{dx} = m\frac{\sqrt{1-y^4}}{\sqrt{1-x^4}}$$

7.9. *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 s'en suit que

$$y = x\frac{m + A_1x^4 + \ldots + A_kx^{4k}}{1 + B_1x^4 + \ldots + B_kx^{4k}} = x\frac{P(x^4)}{Q(x^4)} \tag{7.9.1}$$

7.10. 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 l'équation différentielle

$$\frac{dw}{dv} = m\frac{\sqrt{1-w^4}}{\sqrt{1-v^4}}$$

De plus la valeur $v = 0$ correspond à $x = \infty$, i.e. par exemple à $t = \omega/4 + i\omega/4$. Dans ce cas

$$y = \phi(m(\omega/4 + i\omega/4)) = \infty$$

(m étant impair), d'où $w(0) = 0$. Il s'en suit que $w(v) = vP(v)/Q(v)$.

Or, par définition,

$$w(v) = (-1)^\mu v\frac{Q(v^{-1})}{P(v^{-1})},$$

d'où

$$(-1)^\mu\frac{Q(v^{-1})}{P(v^{-1})} = \frac{P(v)}{Q(v)}$$

D'ici

$$B_j = (-1)^\mu A_{k-j},\ j = 0, \ldots, k \tag{7.10.1}$$

Pour déterminer le signe, on utilise

7.11. *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 (6.17.1) $t = \omega/4$, donc $x = \phi(\omega/4) = 1,\ y = \phi(m\omega/4) = (-1)^{a+b}$; en tenant compte de (6.18.1), on obtient

$$(-1)^{a+b} = \frac{\sum A_j}{\sum B_j} = (-1)^{\mu}$$

7.12. *Corollaire.* Soit $m = a+bi$ primaire, donc (cf. 7.4) $a = 2a'+1,\ b = 2b',\ a', b' \in \mathbb{Z}$ et $a'+b'$ est pair. Alors dans l'expression (7.5.1)

$$y = \phi(mt) = x\frac{m + A_1x^4 + \ldots + A_{k-1}x^{4k-4} + x^{4k}}{1 + A_{k-1}x + \ldots + A_1x^{4k-4} + mx^{4k}} = x\frac{P(x^4)}{Q(x^4)} \tag{7.12.1}$$

où $x = \phi(t)$.

7.13. *Théorème* (Eisenstein). Soit $m = a+bi$ primaire; supposons que m est premier dans $\mathbb{Z}[i]$ et que $N(m) = p = 4k+1$ premier dans $\mathbb{Z}$. Alors tous les coefficients A_j sauf A_k sont divisibles par m.

Démonstration. 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

$$U'V - UV' = m\frac{\sqrt{V^4-U^4}}{\sqrt{1-x^4}} =: mT(x) \tag{7.13.1}$$

D'un 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. de 7.16), donc il est divisible par $1-x^4$ dans $\mathbb{Z}[i][x]$ (sic!). Autrement dit, $T^2 \in \mathbb{Z}[i][x]$ et $T(0) = 1$.

Donc on a $c(T^2) = c(T)^2 \subset \mathbb{Z}[i]$, d'où $c(T) \subset \mathbb{Z}[i]$, donc $T(x) \in \mathbb{Z}[i][x]$. Donc d'après (6.21.1) tous 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

$$V'(x) = B_1 + 4B_2x^3 + \dots ,$$

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 $j < k$. Car sinon, $4j+1 = mn$; en passant aux normes $(4j+1)^2 = pN(n)$, donc $p = 4k+1|(4j+1)$ - impossible.

Donc $m \mid A_j$, cqfd.

7.14. *Remarque.* La même conclusion reste vraie pour le nombres premiers réels, $m = 4\ell + 3$ (Eisenstein), mais la démonstration précédente ne marche pas (à la fin); il faut une autre.

7.15. *Corollaire.* Sous les hypothèses 7.13, le polynôme $P(x^4) \in \mathbb{Z}[i][x]$ est irréductible.

Grace à critère d'Eisenstein 3.5.

7.16. *Théorème* (Gauss) Soit $m = a + bi$ premier et primaire, $p = m\bar{m} = (a+bi)(a-bi) = 4k+1$. Alors

$$m \equiv (-1)^k \binom{2k}{k} \pmod{\bar{m}} \tag{7.16.1}$$

Démonstration (Eisenstein). Posons pour briévité

$$\Gamma := (-1)^k \binom{2k}{k} \tag{7.16.2}$$

Considérons y dans (7.12.1) 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 7.13, $U \equiv x^p \pmod{m}$, $V \equiv 1 \pmod{m}$, d'où

$$R(x) \equiv x^p \pmod{m} \tag{7.16.3}$$

Autrement dit, $c_p \equiv 1 \pmod{m}$ et $c_{4i+1} \equiv 0 \pmod{m}$ pour $i \neq k$.

Il s'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 (7.16.3) 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 6.4.1). 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 s'en suit que

$$\bar{m} \equiv \Gamma \pmod{m}$$

La congruence cherchée (7.16.1) est sa conjuguée complexe.

7.17. *Corollaire* (Gauss) Sous les hypothèses 7.19,

$$2a \equiv \Gamma \pmod{p}$$

Exercice.

§8. Réciprocité biquadratique

8.1. *Exercice.* Soit L un groupe abélien libre de rang 2 avec une base $\{e_1, e_2\}$ (*un réseau*). Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

une matrice avec $a, b, c, d \in \mathbb{Z}$ et $\Delta := \det A \neq 0$. On pose

$$e_1' = ae_1 + be_2,\ e_2' = ce_1 + de_2$$

$$L' = \mathbb{Z} \cdot e_1' \oplus \mathbb{Z} \cdot e_2' \subset L$$

Le but de cet exercice est de montrer que le groupe L/L' est fini et

$$\mathrm{Card}(L/L') = |\Delta| \tag{8.1.1}$$

On utilisera "la méthode de Gauss".

(a) Montrer que les transformations suivantes de la matrice A ne changent pas les deux membres de (8.1.1): la permutation de deux lignes; un remplacement d'une ligne ℓ_i par $\ell_i + k\ell_j$, où $i \neq j$ et $k \in \mathbb{Z}$.

Par contre, si l'on multiplie une ligne par un nombre entier k, les deux membres de (8.1.1) se multiplient par $|k|$.

(b) Montrer qu'on peut obtenir par une suite de trasnformations (a) de la matrice A une matrice triangulaire

$$A' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

(c) Prouver l'assertion en cas de matrices triangulaires, et conclure.

8.2. Prenons pour L l'anneau des gaussiens $R = \mathbb{Z}[i]$ avec la base $\{1, i\}$. Soit $m = a + bi \neq 0$. Alors

$$L' := mR = \mathbb{Z} \cdot (a + bi) \oplus \mathbb{Z} \cdot (-b + ai)$$

Donc

$$\mathrm{Card}(R/mR) = \det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 = N(m)$$

8.3. Supposons maintenant que $m = a+bi$ est premier impair avec a, b différents de 0; donc

$$N(m) = a^2 + b^2 = p = 4k + 1$$

est une nombre entier premier. Donc $F := R/mR$ est un corps dont le groupe multiplicatif $F^* = (R/mR)^*$ est d'ordre $N(m) - 1 = 4k$.

Le composé

$$R^* = \{\pm 1, \pm i\} = \mu_4 \longrightarrow F^* \longrightarrow F^*/F^{*4}$$

est un isomorphisme, et l'on identifie F^*/F^{*4} avec μ_4, d'où le caractère

$$\chi_4 : (R/mR)^* \longrightarrow \mu_4,\ \chi(x) = x^k$$

Maintenant on peut définir *le symbole de Legendre biquadratique.* Étant donné $n \in R$ premier à m, on pose

$$\left(\frac{n}{m}\right)_4 = \chi_4(n \bmod(mR)) = (n \bmod(mR))^{(N(m)-1)/4} \in \mu_4$$

8.4. *Théorème* (loi de réciprocité biquadratique) (Gauss). Soient $\mu, \nu \in R$ premiers primaires. Alors

$$\left(\frac{\nu}{\mu}\right)_4 = (-1)^{(N(\nu)-1)/4\cdot(N(\mu)-1)/4} \cdot \left(\frac{\mu}{\nu}\right)_4$$

Variante d'une preuve de la réciprocité quadratique

8.5. *Exercice. Une formule surprénante.* Montrer que

$$(\sin x + \sin y)(\sin x - \sin y) = \sin(x+y)\sin(x-y)$$

8.6. Rappelons (cf. 2.22) que l'on a:

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

pour $m \in \mathbb{N}$ impair. En remplaçant x par $2\pi x$,

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

$$= (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} \sin\big(2\pi x - 2\pi a/m\big) \cdot \sin\big(2\pi x + 2\pi a/m\big) \qquad (8.6.1)$$

On pose:

$$s(x) := \sin(2\pi x)$$

Donc $s(x) = s(x+1)$. Alors on obtient:

$$\frac{s(mx)}{s(x)} = (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} s(x-a/m)s(x+a/m) = (-4)^{(m-1)/2} \prod_{a=1}^{(m-1)/2} f(x, a/m)$$

où

$$f(x,y) := s(x+y)s(x-y)$$

8.7. Soit p premier entier impair, n premier à p. Rappelons "le lemme de Gauss" (cf. 2.25):

$$\left(\frac{n}{p}\right) = \prod_{a\in M} \frac{s(an/p)}{s(a/p)}$$

où $M \subset \{1, 2, \ldots, (p-1)/2\}$ est un sous-ensemble arbitraire ayant la propriété $M \coprod (-M) = \{1, 2, \ldots, (p-1)/2\}$.

Soit ℓ un deuxième nombre premier impair, différent de p. Alors on aura:

$$\left(\frac{\ell}{p}\right) = \prod_{a=1}^{(p-1)/2} \frac{s(a\ell/p)}{s(a/p)} =$$

$$= (-4)^{(\ell-1)/2\cdot(p-1)/2} \prod_{a=1}^{(p-1)/2} \prod_{b=1}^{(p-1)/2} f(a/p, b/\ell)$$

Maintenant la réciprocité quadratique est une conséquence immédiate de l'identité $f(x, y) = -f(y, x)$.

Encore quelques propriétés des fonctions lemniscatiques

8.8. *Lemme.* $\phi(z)$ est une fonction holomorphe.

Exercice (vérifier les équations de Cauchy - Riemann).

[Solution. On a:

$$\phi(x+iy) = \frac{\phi(x)\Delta(iy) + \Delta(x)\phi(iy)}{1 + \phi(x)^2\phi(iy)^2} =$$

$$= \frac{\phi(x)\Delta(y) + i\Delta(x)\phi(y)}{1 - \phi(x)^2\phi(y)^2} = u(x, y) + iv(x, y)$$

On rémarque que $v(x, y) = u(y, x)$.

Il nous faut vérifier les équations de Cauchy - Riemann:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}; \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

Rappelons (cf. 6.8): $\phi'(x) = \Delta(x)$,

$$\Delta'(x) = (\psi(x)\tilde{\psi}(x))' = -\phi(x)\tilde{\psi}(x)^2 + \phi(x)\psi(x)^2 =$$

$$= \phi(x)(-1 - \phi(x)^2 + 1 - \phi(x)^2) = -2\phi(x)^3$$

De là:

$$\frac{\partial u}{\partial x} = \frac{\Delta(x)\Delta(y)(1 - \phi(x)^2\phi(y)^2) + 2\phi(x)\Delta(y)\Delta(x)\phi(x)\phi(y)^2}{(1 - \phi(x)^2\phi(y)^2)^2} =$$

$$= \Delta(x)\Delta(y) \cdot \frac{1+\phi(x)^2\phi(y)^2}{(1-\phi(x)^2\phi(y)^2)^2}$$

On note que $u'_x(x,y) = u'_x(y,x)$, d'où il vient:

$$v'_y(x,y) = u'_x(y,x) = u'_x(x,y),$$

la première équation de Cauchy - Riemann. De même,

$$\frac{\partial v}{\partial x} = \frac{-2\phi(x)^3\phi(y)(1-\phi(x)^2\phi(y)^2) + 2\Delta(x)\phi(y)\phi(x)\Delta(x)\phi(y)^2}{(1-\phi(x)^2\phi(y)^2))^2} =$$

$$= 2\phi(x)\phi(y) \cdot \frac{-\phi(x)^2 + \phi(x)^4\phi(y)^2 + (1-\phi(x)^4)\phi(y)^2}{(1-\phi(x)^2\phi(y)^2)^2} =$$

$$= 2\phi(x)\phi(y) \cdot \frac{\phi(y)^2 - \phi(x)^2}{(1-\phi(x)^2\phi(y)^2)^2}$$

On voit que $v'_x(x,y) = -v'_x(y,x)$, d'où:

$$u'_y(x,y) = v'_x(y,x) = -v'_x(x,y),$$

qed.]

8.9. *Lemme.* On a: (a)

$$\phi(t+\omega/4) = \frac{\psi(t)}{\tilde{\psi}(t)};\ \phi(t+i\omega/4) = i\frac{\Delta(t)}{1-\phi(t)^2}$$

(b)

$$\psi(t+\omega/4) = -\sqrt{2}\frac{\phi(t)\tilde{\psi}(t)}{1+\phi(t)^2};\ \psi(t+i\omega/4) = \sqrt{2}\frac{\psi(t)}{1-\phi(t)^2}$$

(c)

$$\tilde{\psi}(t+\omega/4) = \sqrt{2}\frac{\tilde{\psi}(t)}{1+\phi(t)^2};\ \tilde{\psi}(t+i\omega/4) = i\sqrt{2}\frac{\phi(t)\psi(t)}{1-\phi(t)^2}$$

Exercice.

8.9.1. *Corollaire.*

$$\phi(t)\phi(t+(1\pm i)\omega/4) = \mp i$$

Exercice.

8.10. On pose $s(t) := \phi((1-i)\omega z/2)$.

Lemme. (a) $s(t)$ est une fonction avec le réseau des périodes $L = \mathbb{Z}[i]$ et dont le diviseur est

$$(s) = (0) + ((1+i)/2) - (1/2) - (i/2),$$

c'est-à-dire les points $z \equiv 0$ ou $(1+i)/2$ modulo L sont des zéros simples, les points $z \equiv 1/2$ ou $i/2$ modulo L sont des pôles simples de $\phi(z)$, la valeur de $\phi(z)$ en autres points et finie et différente de 0.

(b) On a:

$$s(iz) = is(z);\ s(z)s(z-1/2) = i;\ s((1+i)/4) = 1$$

Le théorème suivant est l'analogue de (8.6.1):

8.11. *Théorème.* Soit $\nu \in \mathbb{Z}[i]$ impair,

$$\nu \equiv \epsilon_\nu \bmod (2-2i),\ \epsilon_\nu \in \mu_4 = \mathbb{Z}[i]^*$$

Alors

$$s(\nu z) = \epsilon_\nu \prod_{\alpha \in \mathbb{Z}[i]/(\nu)} s(z - \alpha/\nu) \tag{8.11.1}$$

Démonstration. Le diviseur de la fonction $s(\nu z)$ est

$$\sum_{\alpha \in \mathbb{Z}[i]/(\nu)} \Big\{ (\alpha/\nu) + (\alpha/\nu + (1+i)/2) - (\alpha/\nu - 1/2) - (\alpha/\nu + i/2) \Big\}$$

(expliquer pourquoi; on utilise que $(\nu, 1+i) = 1$), tandis que le diviseur de $s(z-\alpha/\nu)$ est

$$(\alpha/\nu) + (\alpha/\nu + (1+i)/2) - (\alpha/\nu - 1/2) - (\alpha/\nu + i/2)$$

Il s'en suit que le quotient de deux membres de (8.11.1) est une constante, par le théorème de Liouville:

$$s(\nu z) = \delta_\nu \prod_{\alpha \in \mathbb{Z}[i]/(\nu)} s(z - \alpha/\nu)$$

Il reste à montrer que $\delta_\nu = \epsilon_\nu$.

Posons $\gamma = (1+i)/4$. Alors:

$$s(\gamma+\alpha/\nu)s(\gamma-i\alpha/\nu) = -is(\gamma+\alpha/\nu)s(i\gamma+\alpha/\nu) = -is(\gamma+\alpha/\nu)s(\gamma+1/2+\alpha/\nu) = 1$$

Il existe un sous-ensemble $M \subset \mathbb{Z}[i]/(\nu) - \{0\}$ tel que $\mathbb{Z}[i]/(\nu) = \{0\} \coprod M \coprod (-iM)$. Puisque $s(\gamma) = 1$, il s'en suit que

$$\prod_\alpha s(\gamma + \alpha/\nu) = 1,$$

d'où $\delta_\nu = s(\nu\gamma)$. Or,

$$s(\nu\gamma) = s(\epsilon_\nu\gamma + (\nu - \epsilon_\nu)\gamma)$$

On a $(\nu - \epsilon_\nu)\gamma \in (2-2i)(1+i)/4 \cdot \mathbb{Z}[i] = \mathbb{Z}[i]$, d'où

$$s(\epsilon_\nu\gamma + (\nu - \epsilon_\nu)\gamma) = s(\epsilon_\nu\gamma) = \epsilon_\nu s(\gamma) = \epsilon_\nu,$$

qed.

Lemme de Gauss

8.12. La discussion ci-dessous est completement analogue à 2.18 - 2.19.

Soit $\nu \in \mathbb{Z}[i]$ premier impair; $F_\nu = \mathbb{Z}[i]/(\nu)$ le corps quotient. Il esxiste un sous-ensemble $N \subset F_\nu^*$ tel que

$$F_\nu^* = \coprod_{a=0}^{3} i^a N$$

Pour $\mu \in F_\nu^*,\ t \in N$, on pose:

$$\mu t = e_t(\mu) t_\mu,\ e_t(\mu) \in \{\pm 1, \pm i\}$$

Si $t \neq t'$ alors $t_\mu = t'_\mu$, car sinon, on aurait $t = i^a t'$, contrairement à l'hypothèse sur N.

Donc pour μ fixé, $t \mapsto t_\mu$ est une bijection $N \xrightarrow{\sim} N$.

8.13. *Lemme.* Pour $\mu \in \mathbb{Z}[i]$ premier à ν,

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{t \in N} e_t(\mu)$$

Démonstration. En effet,

$$\mu^{(N(\nu)-1)/4} \prod_{t \in N} t = \prod_{t \in N} (\mu t) =$$

$$= \prod_{t \in N} e_t(\mu) t_\mu = \prod_{t \in N} e_t(\mu) \prod_{t \in N} t_\mu = \prod_{t \in N} e_t(\mu) \prod_{t \in N} t,$$

d'où

$$\left(\frac{\mu}{\nu}\right)_4 = \mu^{(N(\nu)-1)/4} = \prod_{t \in N} e_t(\mu),$$

cqfd.

Maintenant on peut prouver, avec Eisenstein, la réciprocité biquadratique. On commence par un corollaire à 8.13:

8.14. *Lemme.* Sous les hypothèses de 8.13,

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{t \in N} \frac{s(\mu t/\nu)}{s(t/\nu)}$$

En effet,

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{t \in N} e_t(\mu);$$

or, $\mu t = e_t(\mu) t_\mu$, d'où

$$s(\mu t/\nu) = s(e_t(\mu) t_\mu/\nu) = e_t(\mu) s(t_\mu/\nu)$$

Il s'en suit que

$$\prod_{t\in N} e_t(\mu) = \prod_{t\in N} \frac{s(\mu t/\nu)}{s(t_\mu/\nu)} = \frac{s(\mu t/\nu)}{s(t/\nu)},$$

qed.

8.15. Maintenant supposons que μ, ν sont les deux premiers et primaires, i.e. $\equiv 1 \bmod (2-2i)$, et $\nu \neq \mu$. Alors, en utilisant 8.11,

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{t\in N} \frac{s(\mu t/\nu)}{s(t/\nu)} = \prod_{t\in N} \frac{\prod_{\alpha\in F_\mu} s(t/\nu - \alpha/\mu)}{s(t/\nu)} = \prod_{t\in N} \prod_{\alpha\in F_\mu^*} s(t/\nu - \alpha/\mu)$$

Choisissons un sous-ensemble $N' \subset F_\mu^*$ tel que $F_\mu^* = \coprod_{a=0}^3 i^a N'$, et posons

$$f(x,y) = \prod_{a=0}^{3} s(x - i^a y)$$

Alors:

$$\prod_{\alpha\in F_\mu^*} s(t/\nu - \alpha/\mu) = \prod_{t'\in N'} f(t/\nu - t'/\mu),$$

donc

$$\left(\frac{\mu}{\nu}\right)_4 = \prod_{t\in N} \prod_{\alpha\in F_\mu^*} s(t/\nu - \alpha/\mu) = \prod_{t\in N} \prod_{t'\in N'} f(t/\nu - t'/\mu)$$

Puisque $f(x,y) = -f(y,x)$ (vérifier), si l'on échange dans la dernière expression ν avec μ, on gagne le signe $(-1)^{(N(\mu)-1)/4\cdot(N(\nu)-1)/4}$, ce qui prouve le théorème.

8.16. Énoncer et prouver le théorème pour μ, ν pas necessairement primaires.

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. (d) Summatio quarumdam serierum singularium, Werke, Bd. II, p. 9.

[IR] K.Ireland, M.Rosen, A classical introduction to modern number theory, Springer, GTM **87**.

[J] C.-G.-J. Jacobi, Demonstratio formulae

$$\int_0^1 w^{a-1}(1-w)^{b-1}dw = \frac{\int_0^\infty e^{-x}x^{a-1}dx \int_0^\infty e^{-x}x^{b-1}dx}{\int_0^\infty e^{-x}x^{a+b-1}dx} = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

Crelle J. für die reine und angewandte Mathematik, Bd. 11, p. 307.

[L] F.Lemmermeyer, Reciprocity laws from Euler to Eisenstein, Springer-Verlag, 2000.

[S] J.-P.Serre, Cours d'arithmétique, PUF, 1995.

[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. (d) Elliptic functions according to Eisenstein and Kronecker, Springer, 1976.

[WW] E.T.Whittaker, G.N.Watson, A course of modern analysis, Cambridge University Press, 1927.