Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 9, 6 avril 2021

— Un idéal de K est, par abus de terminologie, un idéal de $\mathfrak{O}_K$.
— On dira qu'un idéal $\mathfrak{a}$ de K divise un $x \in \mathfrak{O}_K$ quand $x \in \mathfrak{a}$.
— On dira que deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de K sont premiers entre eux quand aucun idéal premier de K divise simultanément $\mathfrak{a}$ et $\mathfrak{b}$.
— Si $\mathfrak{a}$ est un idéal fractionnaire de K, sa classe dans Cl_K sera notée $[\mathfrak{a}]$.
— Une fonction $f : \mathbb{Z} \to \mathbb{C}$ est totalement multiplicative si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{Z}$.

D'autres propriétés du groupe de classes

Exercice 1 (Des groupes de classe très grands)**.** Soit $m > 1$ un entier $\equiv 5\ (12)$ et sans facteur carré, α la racine $\sqrt{-m}$, et $K = \mathbb{Q}(\alpha)$. On souhaite montrer l'existence d'un élément d'ordre $> \log_3 m$ dans Cl_K.

1/ Prouver que $3\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}'$ où $\mathfrak{p} \neq \mathfrak{p}'$ sont des premiers de K. De plus, montrer que $\mathfrak{p}'$ est l'image de $\mathfrak{p}$ par l'automorphisme $\sigma : K \to K$ définit par $\sigma(\alpha) = -\alpha$.

Correction. On sait que $m \equiv 1\ (4) \Rightarrow -m \equiv 3\ (4)$. Donc, $\mathfrak{O}_K = \mathbb{Z}[\alpha]$. Ensuite, $X^2 + m \equiv X^2 + 2\ (3)$ et donc $(3) = (3, 1-\alpha)(3, 1+\alpha)$. En prenant $\mathfrak{p} = (3, 1-\alpha)$ on obtient le résultat souhaité. □

2/ Si $d = \mathrm{ord}([\mathfrak{p}])$, soit $x + y\alpha$ un générateur de $\mathfrak{p}^d$. Justifier l'égalité $3^d = x^2 + my^2$.

Correction. Soit $x + y\alpha$ un générateur de $\mathfrak{p}^d$. Il suit que $\sigma(x + y\alpha) = x - y\alpha$ est un générateur de $\sigma(\mathfrak{p})^d$. On déduit que $3^d = u(x^2 + my^2)$ avec $u \in \mathfrak{O}_K^\times$. Or, $u \in \mathfrak{O}_K \cap \mathbb{Q}$ montre que $u \in \mathbb{Z}$. Comme $u \in \mathfrak{O}_K^\times$, on déduit que $u \in \mathbb{Z}^\times = \{\pm 1\}$. Il est facile de voir que l'unique possibilité est $u = 1$. □

3/ En déduire que $d > \log_3 m$. Indication : Supposer le contraire pour montrer que d est pair et que $(3^{d/2})$ s'écrit de deux façons différentes comme produit d'idéaux premiers.

Correction. Si $3^d \leqslant m$ alors $x^2 + my^2 \leqslant m$, ce qui implique que $y = 0$. De $3^d = x^2$ on tire que d est pair et $x = \pm 3^{d/2}$. Dans ce cas, $\mathfrak{p}^d = (x) = (3^{d/2}) = \mathfrak{p}^{d/2}\mathfrak{q}^{d/2}$. Or, cette égalité contredit l'unicité de la décomposition de $(3^{d/2})$ en idéaux premiers. □

Exercice 2. Soit $m \geqslant 2$ un entier. On souhaite étudier l'équation de Bachet–Fermat

$$Y^3 = X^2 + m \tag{BF}$$

en faisant des hypothèses suivantes sur m :

P1. il ne possède pas de facteurs carrés,

P2. il est $\equiv 1\ (4)$ ou $\equiv 2\ (4)$,

P3. Si $\varrho = \sqrt{-m}$, alors le nombre de classes du corps $K = \mathbb{Q}(\varrho)$ n'est pas divisible par 3.

Dans la suite, on *admet l'existence* d'une solution $(x, y) \in \mathbb{Z}^2$ de (BF).

1/ Montrer que y est impair et que $x \wedge y = 1$.

Correction. Si $y \equiv 0\ (2)$ alors $x^2 + m \equiv 0\ (4)$ et donc $x^2 \equiv 2, 3\ (4)$, ce qui est impossible. Ensuite, si $p \mid x \wedge y$, alors $p^2 \mid m$, ce qui est exclu. □

2/ Montrer que les idéaux $(x - \varrho)$ et $(x + \varrho)$ sont premiers entre eux.

Correction. Soit $\mathfrak{p}$ un diviseur commun de $(x-\varrho)$ et $(x+\varrho)$. Il suit que $\mathfrak{p} \mid (x-\varrho)(x+\varrho) = (y^3) \Rightarrow \mathfrak{p} \mid y$. Or, $\mathfrak{p} \mid x - \varrho + x + \varrho$ et donc $\mathfrak{p} \mid 2x$. Dans ce cas, soit $\mathfrak{p} \mid 2$, soit $\mathfrak{p} \mid x$. Si $\mathfrak{p} \mid x$ et $\mathfrak{p} \mid y$, alors un générateur premier de $\mathfrak{p} \cap \mathbb{Z}$ divise x et y parce que $x, y \in \mathfrak{p} \cap \mathbb{Z}$. Ceci étant impossible, on déduit que $\mathfrak{p} \mid 2$. Or, mais comme y est impair, $\mathfrak{p} \mid (2, y) = (1)$, ce qui est aussi impossible. □

3/ En employant l'hypothèse sur le nombre de classes, déduire l'existence d'un couple d'entiers (u, v) et d'une unité $\varepsilon \in \mathfrak{O}_K^\times$ tels que

$$x + \varrho = \varepsilon(u + v\varrho)^3.$$

Correction. On écrit $(x + \varrho) = \prod_i \mathfrak{p}_i^{a_i}$ et $(x - \varrho) = \prod_j \mathfrak{q}_j^{b_j}$. Donc, $(y^3) = \prod_i \mathfrak{p}_i^{a_i} \prod \mathfrak{q}_j^{b_j}$. Il suit que chaque a_i et chaque b_j est multiple de 3. En particulier, $(x + \varrho) = \mathfrak{a}^3$ et $(x - \varrho) = \mathfrak{b}^3$. Or, mais si $\mathfrak{a}^3$ est principal, resp. $\mathfrak{b}^3$, on déduit que $\mathfrak{a}$ est principal, resp. $\mathfrak{b}$, car la multiplication par 3 dans le groupe abélien Cl_K est injective. L'équation en découle. □

4/ Montrer $\mathfrak{O}_K^\times = \{\pm 1\}$ et en déduire que $x + \varrho$ est le cube d'un *unique* élément de $\mathfrak{O}_K$.

Correction. Si $\varepsilon = r + s\varrho \in \mathfrak{O}_K^\times$, alors $r^2 + s^2 m = \pm 1$. Or, comme $m \geqslant 2$, on déduit que $s = 0$ et $r = \pm 1$, c'est-à-dire, $\varepsilon = \pm 1$. En remplaçant (u, v) par $(-u, -v)$ si nécessaire, on déduit que $(u + v\varrho)^3 = x + \varrho$. Ceci montre que $x + \varrho$ est un cube.

Ensuite, on suppose que $x + \varrho = \alpha^3 = \beta^3$. On déduit que $(\alpha/\beta) \in K$ est une racine de l'unité et appartient ainsi à $\mathfrak{O}_K$. De même, $(\beta/\alpha) \in \mathfrak{O}_K$ et $\alpha/\beta = \pm 1$. Comme $\beta = -\alpha$ est exclue, on déduit que α est *unique*. □

5/ En déduire que *uniquement* un des cas suivants a lieu :

Cas 1 : Le réel $U = \sqrt{(m+1)/3}$ est entier et les *seules* solutions de (BF) sont (X, Y) et $(-X, Y)$, où

$$X = U \cdot \left(U^2 - 3m\right) \quad \text{et} \quad Y = U^2 + m.$$

Cas 2 : Le réel $U = \sqrt{(m-1)/3}$ est entier et les *seules* solutions de (BF) sont (X, Y) et $(-X, Y)$, où

$$X = U \cdot \left(U^2 - 3m\right) \quad \text{et} \quad Y = U^2 + m.$$

Cas 3 : L'équation (BF) ne possède aucune solution en entiers.

Correction. On suppose que (BF) possède une solution $(x, y) \in \mathbb{Z}^2$: on est dans l'un des deux premiers cas. Il suit que $x + \varrho = (u + v\varrho)^3$ pour $u, v \in \mathbb{Z}$. Donc,

$$\begin{aligned} x &= u^3 - 3v^2mu \\ 1 &= 3u^2v - v^3m. \end{aligned}$$

Dans ces cas, $v \mid 1$ et donc $v = \pm 1$. *Si* $v = 1$, alors $u^2 = (m+1)/3$. *Si* $v = -1$, alors $u^2 = (m-1)/3$. Par contre, en tout cas,

$$x = u(u^2 - 3m).$$

En conclusion, si (BF) possède une solution en entiers, alors l'un des deux réels $\sqrt{(m+1)/3}$ ou $\sqrt{(m-1)/3}$ est entier.

Si $(m+1)/3$ est *un entier*, alors $(m-1)/3 = (m+1)/3 - 2/3$ ne l'est pas. De même, si $(m-1)/3$ est un *entier*, $(m+1)/3$ ne l'est pas. Donc, *Cas 1 et Cas 2 sont mutuellement exclusifs.*

Ensuite, si le cas 1 a lieu, alors (BF) possède (X, Y) et $(-X, Y)$ comme solutions parce que

$$\begin{aligned} X^2 + m &= \frac{m+1}{3}\left(\frac{1-8m}{3}\right)^2 + m \\ &= \frac{(m+1)(1-8m)^2 + 27m}{27} \\ &= \frac{64m^3 + 48m^2 + 12m + 1}{27} \\ &= \frac{(4m+1)^3}{27}. \end{aligned}$$

De plus, elles sont *les uniques solutions*, comme montre l'argument suivant. Si (x', y') est une autre solution, la question 4 dit que $x' + \varrho = (u' + v'\varrho)^3$ pour un certain couple d'entiers u' et v'. À nouveau :

$$\begin{aligned} x' &= u'^3 - 3v'^2 m u' \\ 1 &= 3u'^2 v' - v'^3 m. \end{aligned}$$

Si $v' = 1$, alors $u'^2 = (m+1)/3$, et si $v' = -1$, alors $u'^2 = (m-1)/3$. Comme remarqué avant, $(m+1)/3$ et $(m-1)/3$ ne peuvent pas être simultanément des entiers et on déduit que $v' = 1$, que $u' = \pm\sqrt{(m+1)/3}$ et que

$$x' = u'(u'^2 - 3m).$$

Donc $x' = \pm X$. Clairement y' sera uniquement déterminée.

Le fait que dans le cas 2 les solutions (X, Y) et $(-X, Y)$ sont des solutions, et de plus sont les seules, se vérifie de façon analogue. □

6/ Quels sont les solutions en entiers des équations $Y^3 = X^2+2$, $Y^3 = X^2+5$, $Y^3 = X^2+6$, $Y^3 = X^2+10$, $Y^3 = X^2+13$ et $Y^3 = X^2+14$? (Pour rappel, si $h(-m)$ note le nombre de classes du corps $\mathbb{Q}(\sqrt{-m})$, alors $h(-2) = 1$, $h(-5) = h(-6) = h(-10) = h(-13) = 2$ et $h(-14) = 4$, comme a été vu lors des séances précédentes.)

Correction. Si $m = 6, 10, 14$: (BF) ne possède pas des solutions car m satisfait P1.–P3 et ni $(m+1)/3$, ni $(m-1)/3$ est carré.

Si $m = 2$, alors (BF) possède les solutions $X = \pm 5$ et $Y = 3$. Si $m = 13$, alors $(70, 17)$ et $(-70, 17)$ sont les uniques solutions. □

Remarque historique : Voici comment Fermat exprima son intérêt pour cette équation : "Peut-on trouver en nombres entiers un carré autre que 25 qui, augmenté de 2, fasse un cube ? A la première vue cela paraît d'une recherche difficile ; en fractions une infinité de nombres se déduisent de la méthode de Bachet ; mais la doctrine des nombres entiers, qui est assurément très belle et très subtile, n'a été cultivée ni par Bachet, ni par aucun autre dans les écrits venus jusqu'à moi." Le fait que (BF) possède, dans le cas $m = 2$, une infinité de solutions rationnelles a été observé par Bachet en employant, dit en langage moderne !, la structure de groupe de la courbe elliptique $y^3 = x^2 + 2$.

Caractères de Dirichlet

Exercice 3. Soit $t > 0$ un entier.

1/ On écrit

$$X_t = \left\{ \chi : \mathbb{Z} \to \mathbb{C} \ : \begin{array}{l} \chi \text{ est } t\text{-périodique,} \\ \chi \text{ est totalement multiplicative et} \\ \chi(m) \text{ s'annule uniquement si } m \wedge t \neq 1. \end{array} \right\}.$$

Quel est le lien entre X_t est les caractères de Dirichlet modulo t ?

Correction. Soit $\chi : (\mathbb{Z}/t)^\times \to \mathbb{C}^\times$ un caractère linéaire ; le caractère de Dirichlet associé est

$$\widetilde{\chi}(m) = \begin{cases} 0, & \text{si } m \wedge t \neq 1, \\ \chi(m + t\mathbb{Z}) & \text{si } t \wedge m = 1. \end{cases}$$

Il suit que $\widetilde{\chi}$ appartient à X_t. De même, si $\widetilde{\chi} \in X_t$ alors $\chi : n + t\mathbb{Z} \mapsto \widetilde{\chi}(n)$ induit un morphisme de groupes $(\mathbb{Z}/t)^\times \to \mathbb{C}^\times$. Dit autrement, X_t est l'ensemble des caractères de Dirichlet modulo t. □

2/ Déterminer explicitement X_2, X_4 et X_8.

Correction. On décrit X_4. Soit $\psi : (\mathbb{Z}/4)^\times \to \mathbb{C}^\times$ définit par $\psi(-1) = -1$; c'est l'unique caractère linéaire non-trivial. Donc, X_4 possède deux éléments, $\mathbb{1}_4 : \mathbb{Z} \to \mathbb{C}$, et $\widetilde{\psi}$.

Ensuite, $(\mathbb{Z}/8)^\times$ est un groupe d'ordre 4 où chaque élément différent du élément neutre a ordre 2, d'où $\mathrm{Hom}((\mathbb{Z}/8)^\times, \mathbb{C}^\times) = \{1, \lambda, \mu, \nu\}$ où

$$\lambda : \left| \begin{array}{ll} 1 & \mapsto 1 \\ 3 & \mapsto -1 \\ 5 & \mapsto 1 \\ 7 & \mapsto -1 \end{array} \right. \qquad \mu : \left| \begin{array}{ll} 1 & \mapsto 1 \\ 3 & \mapsto 1 \\ 5 & \mapsto -1 \\ 7 & \mapsto -1 \end{array} \right. \qquad \nu : \left| \begin{array}{ll} 1 & \mapsto 1 \\ 3 & \mapsto -1 \\ 5 & \mapsto -1 \\ 7 & \mapsto 1 \end{array} \right.$$

On observe

$$(\mathbb{Z}/8)^\times \xrightarrow{\lambda} \mathbb{C}^\times \quad = \quad (\mathbb{Z}/8)^\times \longrightarrow (\mathbb{Z}/4)^\times \xrightarrow{\psi} \mathbb{C}^\times$$

□