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 $\sigma(\alpha) = -\alpha$.

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

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.

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 $x \wedge y = 1$.

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

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

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

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

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

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

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

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

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

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.)

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 ?

2/ Déterminer explicitement X_2, X_4 et X_8.