Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2020.

Séance 9, 31 mars 2020

— 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 $[\mathfrak{a}]$.

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 $K = \mathbb{Q}(\alpha)$.

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

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

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

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

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 $h(-14) = 4$. Le calcul de $h(-6)$, $h(-10)$ et $h(-13)$ a été fait lors de la séances du 24 mars 2020 et celui de $h(-14)$ lors de la séance du 27 mars 2020.)

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 $y^3 = x^2 + 2$.

Exercice 3. Soit $p \geqslant 5$ un nombre premier, ζ une racine primitive p-ème de l'unité et K le corps de nombres $\mathbb{Q}(\zeta)$. On suppose que p ne divise pas $|\mathrm{Cl}_K|$ (des tels premiers sont dits "réguliers"). Dans cet exercice, on souhaite montrer le théorème suivant, connu comme le premier cas du "Théorème de Fermat pour exposant régulier", dû à Kummer :

Théorème. *Soient $x, y, z \in \mathbb{Z}$ tels que $z^p + y^p = z^p$. Alors $p \mid xyz$.*

La preuve est découpé en plusieurs exercices. Certains sont moins instructifs que d'autres : le plus importants pour l'éducation en théorie des nombres à notre niveau sont les items 3 et 4 et 5.

Pour ne pas exténuer l'étudiant, on se gardera de prouver le resultat suivant (qui n'est pas hors portée) :

Lemme A. *Soit $u \in \mathfrak{O}_K^\times$. Alors $\zeta^s u$ est réel pour un certain $s \in \{0, 1 \ldots, p-1\}$.*

1/ Il est possible de trouver des entiers x', y' et z', deux-à-deux premiers entre eux tels que $x' \mid x$, $y' \mid y$ et $z' \mid z$, et $x'^p + y'^p = z'^p$.

Dans la suite, on change les notations et on suppose que x, y, z sont deux-à-deux premiers entre eux et que $x^p + y^p = z^p$. Ceci suffit pour établir le théorème.

2/ Prouver l'identité de $\mathfrak{O}_K[X, Y]$:

$$X^p + Y^p = \prod_{i=0}^{p-1} (X + \zeta^i Y).$$

3/ ⋆ Soient $i < j$ des entiers de $\{0, \ldots, p-1\}$. Montrer que *si* les idéaux $\mathfrak{A}_i = (x + \zeta^i y)$ et $\mathfrak{A}_j = (x + \zeta^j y)$ *ne sont pas* premiers entre eux, alors $p \mid z$. Indication : Prouver que $(\zeta^i - \zeta^j) = (1 - \zeta)$ et que $(1 - \zeta)$ est un premier de K qui divise p.

Dans la suite, on suppose que les idéaux $\{\mathfrak{A}_i : i = 0, \ldots, p-1\}$ de la question précédente sont deux-à-deux premiers entre eux. Ceci suffit pour établir le théorème.

4/ ⋆ En utilisant que p ne divise pas $|\mathrm{Cl}_K|$, prouver que $x + \zeta y = u\alpha^p$, où $u \in \mathfrak{O}_K^\times$ et $\alpha \in \mathfrak{O}_K$.

5/ ⋆ Utiliser le Lemme A pour prouver que $x + \zeta y \equiv \zeta^s v a \mod p\mathfrak{O}_K$, où $v \in \mathfrak{O}_K^\times$ est *réel* et a est un *nombre entier*. En déduire que

$$\boxed{x + \overline{\zeta} y \equiv \zeta^{-2s}(x + \zeta y) \mod p\mathfrak{O}_K,}$$

et que l'entier algébrique

$$A := x + \zeta y - \zeta^{2s} x - \zeta^{2s-1} y$$

est divisible par p en $\mathfrak{O}_K$.

6/ Soient $a_0, \ldots, a_{p-2}$ des entiers tels que $a_0 + \cdots + a_{p-2}\zeta^{p-2} \equiv 0 \mod p\mathfrak{O}_K$. Prouver que $p \mid a_i$ pour tout i. Conclure que soit $p \mid xy$, soit $p \mid x - y$. Indication : Étudier les cas $2s \equiv -1, 0, 1\ (p)$. (C'est ici que l'hypothèse $p \geqslant 5$ rentre.)

7/ Appliquer les conclusions précédentes à l'équation $x^p + (-z)^p = (-y)^p$ pour conclure.