MM120 Théorie des nombres — Loïc Merel
Année 2013-2014 — Dominique Bernardi, Pierre Charollois

Feuille 5

Théorème de Чеботарёв (Tchebotariov, Chebotaryov, Chebotarev, etc.)

Exercice 1 Soit $f \in \mathbb{Z}[X] \setminus \{0\}$ un polynôme non nul à coefficients entiers. Pour tout nombre premier p, on note $n_p(f) = |\{a \in \mathbb{F}_p;\ f(a) = 0\}|$ le nombre de racines distinctes de f modulo p. Montrer que le nombre moyen de racines modulo p, c'est-à-dire

$$\lim_{X \to \infty} \frac{\sum_{p<X} n_p(f)}{\sum_{p<X} 1}$$

est égal au nombre de facteurs irréductibles distincts de f dans $\mathbb{Q}[X]$. Si f est produit de facteurs linéaires pour presque tout p, montrer que f est produit de facteurs linéaires dans $Q[X]$

Exercice 2

a) Soit X un ensemble de cardinal $n > 1$, et G un groupe agissant transitivement sur X. Montrer qu'il existe $\sigma \in G$ tel que $\forall x \in X, \sigma(x) \neq x$.

b) Montrer que si $f \in \mathbb{Z}[X]$ est irréductible et a un zéro modulo p pour presque tout p, alors f est de degré 1.

c) Trouver un polynôme unitaire $f \in \mathbb{Z}[X]$ de degré minimal tel que f n'ait pas de racine dans $\mathbb{Z}$ mais que f ait une racine modulo p pour tout p premier.

Exercice 3 Montrer que le nombre w_K des racines de l'unité dans un corps de nombres K est le pgcd des $N\mathfrak{p} - 1$, où $\mathfrak{p}$ parcourt les idéaux premiers de caractéristique $\geq 1 + [K : \mathbb{Q}]$.

Exercice 4 Montrer que l'anneau $\prod_p \mathbb{F}_p$ admet un idéal maximal $\mathfrak{m}$ et un sous-anneau $B \supset \mathfrak{m}$ tels que $B/\mathfrak{m}$ soit une clôture algébrique de $\mathbb{Q}$.

Exercice 5

a) Soit $(X_n)_{n \in \mathbb{N}}$ une suite d'ensembles de nombres premiers disjoints. On suppose que chaque X_n a une densité d_n. Peut-on en conclure que $X = \cup_n X_n$ a pour densité $\sum_n d_n$?

b) Soit $(Y_n)_{n \in \mathbb{N}}$ une autre suite d'ensembles de nombres premiers disjoints entre eux et des X_n de densité e_n telle que $\sum_n d_n + \sum_n e_n = 1$. Montrer que X a pour densité $\sum_n d_n$.

Exercice 6 Pour tout nombre premier $p \neq 2, 5$, notons d_p la période du développement décimal de $1/p$. Montrer que l'ensemble des p tels que d_p est impair a une densité et calculer cette densité. On pourra montrer que la condition sur p équivaut à l'existence d'un entier $r \geq 1$ tel que p est totalement décomposé dans $\mathbb{Q}(\zeta_{2^r}, \sqrt[2^r]{10})$ mais pas dans $\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^r]{10})$.

Corps de classes de Hilbert

Exercice 7 Soient p et q deux nombres premiers distincts congrus à 1 $\pmod 4$. Montrer que le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{pq})$ contient $\sqrt{p}$ et $\sqrt{q}$. En déduire que h_K est pair.

Exercice 8

a) Montrer que le corps de classes de Hibert de $K = \mathbb{Q}(\sqrt{-5})$ est $K(i)$. Montrer qu'un nombre premier p s'écrit sous la forme $x^2 + 5y^2$ si et seulement si il est congru à 1 ou 9 $\pmod{20}$.

b) Montrer que si α est une racine du polynôme $f = X^4 + 2X^2 - 7$, le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{-14})$ est $K(\alpha)$. Montrer qu'un nombre premier p s'écrit $x^2 + 14y^2$ si et seulement si il vérifie "f a une racine modulo p et $p \equiv 1, 9, 15, 23, 25$ ou $39 \pmod{56}$".

c) On rappelle que le discriminant de $X^3 + aX + b$ est $-(4a^3 + 27b^2)$. Expliciter les corps de classes de Hilbert de $\mathbb{Q}(\sqrt{-23})$ et $\mathbb{Q}(\sqrt{-31})$.

Exercice 9 On rappelle (voir feuille 1) que si a et b sont deux entiers sans facteurs carrés premiers entre eux et tels que $a \not\equiv \pm b \pmod 9$, le corps $\mathbb{Q}(\sqrt[3]{ab})$ a pour discriminant $-27a^2b^2$. Trouver une unité de $K = \mathbb{Q}(\sqrt[3]{6})$ et montrer que $h_K = 1$.

Exercice 10 Soit L/K une extension quadratique de corps de nombres telle que K soit totalement réel et L totalement complexe. On dit que L est un corps *de type CM* (pour Complex Multiplication).

a) Montrer que $[\mathfrak{O}_L^\times : \mathfrak{O}_K^\times \mu_L] = 1$ ou 2.

b) Montrer que h_K divise h_L.

Classes de rayon

Exercice 11

a) Soit K un corps de nombres, $\mathfrak{f} = \mathfrak{f}_f \mathfrak{f}_\infty$ un module sur K, Cl le groupe des classes d'idéaux de K, $Cl_\mathfrak{f}$ le groupe des classes de rayon $\mathfrak{f}$, $\mathfrak{O}_+^\times$ le groupes des unités de K positives aux places divisant $\mathfrak{f}_\infty$. Montrer qu'il y a une suite exacte naturelle

$$1 \to (\mathfrak{O}/\mathfrak{f}_f)^\times / \varphi(\mathfrak{O}_+^\times) \to Cl_\mathfrak{f} \to Cl \to 1.$$

b) Montrer que pour $n \geq 1$ le corps de classes de $\mathbb{Q}$ de rayon $n\infty$ est $Q(\zeta_n)$. Quel est le corps de classes de rayon n ?

Exercice 12 Posons $K = \mathbb{Q}(\zeta_3)$ et $\mathfrak{m} = (5 + 3\zeta_3)$. On note F le corps de classes de K de rayon $\mathfrak{m}$.

a) Montrer que $Gal(F/K) \simeq \mathbb{Z}/3\mathbb{Z}$. En déduire que F peut s'écrire

$$F = K\left(\sqrt[3]{\zeta_3^k(5 + 3\zeta_3)}\right).$$

b) Déterminer F. (On pourra considérer le Frobenius en $(4 + 3\zeta_3)$).

Corrigé de l'exercice 4

Notons A l'anneau $\prod_p \mathbb{F}_p$. Il contient un sous-anneau premier que nous noterons $\mathbb{Z}$. Notons I le sous-ensemble de A formé des suites à support fini. Il est clair que I est un idéal de A. Soit K une extension galoisienne finie de $\mathbb{Q}$. Nous dirons que $\alpha \in A$ est adapté à K si pour presque tout p premier décomposé dans K on a $\alpha_p = 0$. Posons

$$J = \{\alpha \in A;\ \exists K/\mathbb{Q} \text{ galoisienne finie telle que } \alpha \text{ adapté à } K\}.$$

Montrons que J est un idéal de A. En effet, si K convient pour α et L pour β, le compositum KL convient pour $\alpha+\beta$. On voit que $I \subset J$ en prenant $K = \mathbb{Q}$. Enfin, grâce à une forme très faible du théorème de Chebotarev, on voit que $J \cap \mathbb{Z} = \{0\}$.

Soit $\mathfrak{m}$ un idéal de A qui contient J, vérifie $\mathfrak{m} \cap \mathbb{Z} = \{0\}$ et est maximal pour cette dernière propriété (Le lemme de Zorn implique qu'un tel $\mathfrak{m}$ existe).

Montrons que $\mathfrak{m}$ est un idéal maximal de A. En effet, si $x \notin \mathfrak{m}$, on a

$$(\mathfrak{m} + xA) \cap \mathbb{Z} \neq \{0\}.$$

Soit donc $m \in \mathfrak{m}$, $a \in A$ et $n \in \mathbb{Z}_{\neq 0}$ tels que $n = m + xa$. Posons $y \in A$ dont la p-composante est 0 si $p \mid n$ et $1/n$ sinon. On a $1 - ny \in I \subset \mathfrak{m}$, et la formule

$$1 = (my + (1 - ny)) + x(ay)$$

montre que x est inversible modulo $\mathfrak{m}$.

Le corps $K = A/\mathfrak{m}$ est de caractéristique nulle puisque $\mathfrak{m} \cap \mathbb{Z} = \{0\}$. Soit $f \in \mathbb{Z}[X]$ et $N/\mathbb{Q}$ son corps de décomposition. Pour presque tout p décomposé dans N, le polynôme f a une racine $\alpha_p \in \mathbb{F}_p$. Pour tous les autres p, posons $\alpha_p = 0$ (par exemple). On a $\alpha \in A$ et $f(\alpha) \in J \subset \mathfrak{m}$. L'image de α dans K est donc une racine de f. On en déduit que K contient $\overline{Q}$.