M2R Université de Paris-Sud
2006-2007 séance 5 du 13 novembre 2006

Feuille 4 : Ramification, Chebotarev

Exercice 1 (Une famille infinie de corps cubiques K tels que $\forall x \in \mathcal{O}_K$, $\mathcal{O}_K \neq \mathbb{Z}[x]$)
Soient p un premier vérifiant $p = 1 \mod 3$ et ζ_p une racine primitive p-ième de l'unité.

1. Montrer que $\mathbb{Q}(\zeta_p)$ admet un unique sous-corps cubique F_p de degré 3 sur $\mathbb{Q}$. Montrer que $F_p/\mathbb{Q}$ est galoisien.
2. Soit $q \neq p$ premier. Montrer que q est totalement décomposé dans F_p si et seulement si q est un cube modulo p.
3. **(Hensel)** Montrer que si 2 est un cube modulo p, alors
$$\forall x \in \mathcal{O}_{F_p}, \quad \mathcal{O}_{F_p} \neq \mathbb{Z}[x].$$
4. Montrer que l'ensemble des $p = 1 \mod 3$ tels que 2 est un cube modulo p est infini.
5. Soit $p \geq 5$. Montrer que $p = 1 \mod 3$ si et seulement si $\exists x \in \mathbb{Z}/p\mathbb{Z}\backslash\{1\}$ tel que $x^3 = 1$. En déduire que la densité analytique des $p = 1 \mod 3$ tels que 2 est un cube modulo p est $\frac{1}{6}$.

Exercice 2 Soit $n \in \mathbb{Z}$.

1. Montrer que n est un carré dans $\mathbb{Z}$ si et seulement si pour tout p premier suffisamment grand, n est un carré modulo p.
2. Plus généralement soit ℓ un nombre premier. Montrer que n est une puissance ℓ-ème dans $\mathbb{Z}$ si et seulement si pour tout p premier suffisamment grand, n est une puissance ℓ-ème modulo p.

Exercice 3 Soit L/K une extension galoisienne de corps de nombres. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$. Montrer que $\mathfrak{p}\mathcal{O}_L$ est maximal si et seulement si $\mathfrak{p}$ est non ramifié et le groupe $\mathrm{Gal}(L/K)$ est cyclique engendré par $\mathrm{Frob}_{\mathfrak{p}}(L/K)$.

Exercice 4 Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible et soit K_f un corps de décomposition de f sur $\mathbb{Q}$. On note $\mathrm{Spl}(f) = \{p \in \mathbb{Z} \,|\, f \text{ est scindé modulo } p\}$.

1. Soit p et q deux nombres premiers impairs distincts avec $p \equiv 1 \mod 4$. Montrer l'équivalence des propriétés suivantes :
   i. $\left(\frac{p}{q}\right) = 1$
   ii. $X^2 - X + \frac{1-p}{4} \equiv 0 \mod q$
   iii. q se décompose dans $\mathbb{Q}(\sqrt{p})$
   iv. $\mathrm{Frob}_q\Big(\mathbb{Q}(\sqrt{p})/\mathbb{Q}\Big) = 1$
   v. $\left(\frac{q}{p}\right) = 1$.

2. Soit p un nombre premier $p \equiv 1 \mod 4$, $f(X) = X^2 - p$ et $g(X) = X^p - 1$. Montrer que $K_f \subset K_g$.

3. Montrer que $q \in \mathrm{Spl}(g)$ si et seulement si $q \equiv 1 \mod p$. Montrer que $\mathrm{Spl}(g) \subset \mathrm{Spl}(f)$.
4. Soient f et g des polynômes irréductibles de $\mathbb{Z}[X]$ de corps de décomposition respectif K_f et K_g. Montrer que $K_g \subset K_f$ si et seulement si $\mathrm{Spl}(f) \subset^* \mathrm{Spl}(g)$, où $\subset^*$ signifie inclusion à un ensemble fini près (l'équivalence restant vrai avec $\subset^\times$ qui signifie à un ensemble de densité nulle près).