ENS Cachan
M1 mathématiques Arithmétique - 2014-2015

Exercices - Feuille 2

I. Extensions quadratiques

Soit d un entier qui n'est pas un carré. On fixe $\sqrt{d}$ une racine carrée de d dans $\mathbb{C}$. Posons $\mathbb{Q}(\sqrt{d}) = \{u + v\sqrt{d} : u, v \in \mathbb{Q}\}$. Un *corps quadratique* est une extension de $\mathbb{Q}$ de degré 2.
1. Montrer que $\mathbb{Q}(\sqrt{d})$ est un corps quadratique. Montrer que tout corps quadratique est de cette forme. Est-ce que l'extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est galoisienne ? Quel est son groupe de Galois, et comment il agir sur les éléments de $\mathbb{Q}(\sqrt{d})$?
2. Soient d et d' des entiers non carrés. Montrer que $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{d'})$ sont égaux si et seulement si d/d' est un carré dans $\mathbb{Q}$. En déduire que tout corps quadratique est isomorphe à $\mathbb{Q}(\sqrt{d})$ avec un entier $d \neq 0, 1$ sans facteur carré et uniquement déterminé.
3. Soit $Q(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ irréductible sur $\mathbb{Q}$. Posons $\Delta = b^2 - 4ac$. Montrer que le corps de décomposition de Q est $\mathbb{Q}(\sqrt{\Delta})$. Quelles sont les valeurs possibles de $\Delta \pmod 4$?
4. Réciproquement, étant donné $d \neq 1$ un entier sans facteur carré, donner un polynôme quadratique Q dont son corps de décomposition est $\mathbb{Q}(\sqrt{d})$. Montrer que tout tel polynôme est de discriminant divisible par d, de plus si $d \equiv 1 \pmod 4$ (resp. $d \equiv 2, 3 \pmod 4$) on peut choisir Q monique et de discriminant d (resp. $4d$), notons Q_d un tel polynôme.

II. Entiers quadratiques

1. Soit α une racine de Q_d. Posons $\mathcal{O}_d = \mathbb{Z}[\alpha] = \{x_1 + x_2\alpha : x_1, x_2 \in \mathbb{Z}\}$. Montrer que c'est un anneau de corps de fraction égal à $\mathbb{Q}(\sqrt{d})$.
2. Pour tout polynôme unitaire à coefficients entiers qui a une racine $\gamma \in \mathbb{Q}(\sqrt{d})$, montrer que $\gamma \in \mathcal{O}_d$. En déduire que toute racine $x \in \mathbb{Q}(\sqrt{d})$ d'un polynôme unitaire à coefficients dans $\mathcal{O}_d$ vérifie $x \in \mathcal{O}_d$. (On dit que $\mathcal{O}_d$ est *intégralement clos*). Cette dernière propriété est-elle vérifiée si on remplace $\mathcal{O}_d$ par $\mathbb{Z}[\sqrt{d}]$? (indication : Soit $A_1/A_2/A_3$ une extension d'anneaux intègres, si A_2 est intègre sur A_3 et si $\gamma \in A_1$ est intègre sur A_2 alors γ est intègre sur A_3)
3. Considérons $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ défini par $N(x_1 + x_2\sqrt{d}) = x_1^2 - dx_2^2$. Montrer que $N(x)N(y) = N(xy)$ et $N(\mathcal{O}_d) \subset \mathbb{Z}$.
4. Montrer que $N(x) = \pm 1$ si x est inversible dans $\mathcal{O}_d$. Déterminer $\mathcal{O}_d^\times$ lorsque $d < 0$. (Le cas $d > 0$ est beaucoup plus difficile, voir le cours.)
5. Montrer que $\mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$. Dans cet anneau, déterminer les diviseurs de $2, 3, 1 + \sqrt{-5}$ et $1 - \sqrt{-5}$. Montrer que ces nombres sont des éléments irréductibles dans $\mathcal{O}_{-5}$, mais ils ne sont pas des éléments premiers. Cet anneau est-il principal ? Est-il factoriel ?

III. Réduction modulo p

1. Soit p un nombre premier. Notons $\bar{Q}_d \in \mathbb{F}_p[X]$ la réduction de Q_d modulo p. Notons k_p le corps de décomposition de $\bar{Q}_d$, montrer que $k_p/\mathbb{F}_p$ est de degré $f_p = 1$ ou 2. Quel est son groupe de Galois G_p ? Montrer que $f_p = 1$ si et seulement si $x \mapsto x^p$ est l'identité sur k_p ou encore, pour $p \neq 2$, si et seulement si d est un carré modulo p. Pour $p = 2$, donner un contre-exemple pour la dernière équivalence.