Université Paris Diderot — Arithmétique – Année 2011-12
ENS Cachan
M1 mathématiques

Feuille d'exercices 1

Corps quadratiques

Soit d un entier qui n'est pas un carré dans $\mathbf{Q}$. Soit $\sqrt{d}$ une racine carrée de d dans $\mathbf{C}$. Posons $\mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d}/a, b \in \mathbf{Q}\}$.

Un *corps quadratique* est une extension de corps de $\mathbf{Q}$ de degré 2.

I

1. Montrer que $\mathbf{Q}(\sqrt{d})$ est un corps quadratique. Montrer que tout corps quadratique est isomorphe à $\mathbf{Q}(\sqrt{d})$ pour d bien choisi. L'extension $\mathbf{Q}(\sqrt{d})|\mathbf{Q}$ est-elle galoisienne ? Quel est le groupe de Galois ? Indiquer explicitement les éléments du groupe de Galois.

2. Soient d et d' des entiers non carrés. Montrer que les corps $\mathbf{Q}(\sqrt{d})$ et $\mathbf{Q}(\sqrt{d'})$ sont égaux si et seulement si d/d' est un carré dans $\mathbf{Q}$. En déduire que tout corps quadratique est isomorphe à $\mathbf{Q}(\sqrt{d})$ avec $d \neq 0, 1$ entier sans facteur facteur carré et uniquement déterminé.

3. Soit $Q(X) = aX^2 + bX + c \in \mathbf{Z}[X]$, irréductible sur $\mathbf{Q}$. Posons $\Delta = b^2 - 4ac$. Montrer qu'un corps de décomposition de Q est $\mathbf{Q}(\sqrt{\Delta})$. Quelles sont les valeurs possibles de Δ modulo 4 ?

4. Réciproquement, étant donné d sans facteur carré, donner un polynôme quadratique Q dont un corps de décomposition est $\mathbf{Q}(\sqrt{d})$. Montrer que si $d \equiv 1 \pmod 4$ (resp. $d \equiv 3 \pmod 4$ ou $d \equiv 2 \pmod 4$) tout tel polynôme est de discriminant divisible par d et qu'on peut choisir Q unitaire et de discriminant d (resp. $4d$). Notons Q_d un polynôme ainsi choisi.

II

5. Soit α une racine de Q_d. Posons $\mathcal{O}_d = \mathbf{Z}[\alpha] = \{a + b\alpha/a, b \in \mathbf{Z}\}$. Montrer que c'est un anneau de corps de fraction égal à $\mathbf{Q}(\sqrt{d})$.

6. Montrer que tout polynôme unitaire à coefficients entiers qui a une racine dans $\mathbf{Q}(\sqrt{d})$ a une racine dans $\mathcal{O}_d$. En déduire que toute racine $x \in \mathbf{Q}(\sqrt{d})$ d'un polynôme unitaire à coefficient dans $\mathcal{O}_d$ vérifie $x \in \mathcal{O}_d$ (autrement dit $\mathcal{O}_d$ est *intégralement clos*). Cette propriété est-elle vérifiée si on remplace $\mathcal{O}_d$ par $\mathbf{Z}[\sqrt{d}]$?

7. Considérons $N : \mathbf{Q}(\sqrt{d}) \to \mathbf{Q}$ défini par $N(a + b\sqrt{d}) = a^2 - db^2$ (a, $b \in \mathbf{Z}$). Montrer que $N(O_d)$ est contenu dans $\mathbf{Z}$ et qu'on a $N(xy) = N(x)N(y)$ (x, $y \in \mathbf{Q}(\sqrt{d})$).

8. Montrer que tout élément inversible x de $\mathcal{O}_d$ vérifie $N(x) = 1$ ou $N(x) = -1$.(On dit que x est une *unité* de $\mathbf{Q}(\sqrt{d})$.) Déterminer $\mathcal{O}_d^*$ lorsque $d < 0$. (Si $d > 0$, c'est possible, mais c'est plus difficile.)

9. Montrer que $\mathcal{O}_{-5} = \mathbf{Z}[\sqrt{-5}]$. Dans l'anneau $\mathcal{O}_{-5}$, déterminer les diviseurs de 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$. Montrer que ces nombres sont premiers dans $\mathcal{O}_{-5}$. L'anneau $\mathcal{O}_{-5}$ est-il principal ? Est-il factoriel ?

III

10. Soit p un nombre premier. Notons $\bar{Q}_d \in \mathbf{F}_p[X]$ la réduction de Q_d modulo p. Notons k_p un corps de décomposition de $\bar{Q}_d$ sur $\mathbf{F}_p$. Montrer que c'est un corps à p ou à p^2 éléments. Notons f_p le degré de l'extension $k_p|\mathbf{F}_p$. C'est le *degré résiduel*. Cette extension est-elle galoisienne ? Quel est le groupe de Galois G_p ? Indiquer explicitement les éléments du groupe de Galois (on rappellera ce qu'est la substitution de Frobenius). Montrer que k_p possède p éléments si et seulement si l'application $x \mapsto x^p$ est l'identité sur k_p ou encore si et seulement si d est un carré modulo p.

11. Le corps résiduel k_p change-t-il si on remplace Q_d par un polynôme quadratique $Q \in \mathbf{Z}[X]$ de corps de décomposition $\mathbf{Q}(\sqrt{d})$? Pour combien de nombres premiers p ce corps change-t-il ?

12. Y a-t-il nécessairement des nombres premier p tels que le degré résiduel soit égal à 1 (resp. à 2) ? Y en a-t-il une infinité ? Peut-on dire que l'une des valeurs du degré résiduel est plus probable que l'autre lorsque p varie ?