May 10th, 2016

Number Theory II

Prof. H. Esnault, Dr. V. Di Proietto

Exercise sheet 4[1]

Exercise 1. Let R be the ring $\mathbb{Z}[\alpha]$, where $\alpha = \sqrt[3]{2}$.

(i) Verify that $5R = (5, \alpha + 2)(5, \alpha^2 + 3\alpha - 1)$.

(ii) Show that there is a ring isomorphism

$$\mathbb{Z}[X]/(5, X^2 + 3X - 1) \longrightarrow \mathbb{F}_5[X]/(X^2 + 3X - 1).$$

(iii) Show that there is a ring homomorphism

$$\mathbb{Z}[X]/(5, X^2 + 3X - 1) \longrightarrow R/(5, \alpha^2 + 3\alpha - 1).$$

(iv) Conclude that either $R/(5, \alpha^2 + 3\alpha - 1)$ is a field of order 25 or else $(5, \alpha^2 + 3\alpha - 1) = R$.

(v) Using (i), show that $(5, \alpha^2 + 3\alpha - 1) \neq R$.

Exercise 2. (i) Let $R = \mathbb{Z}[\alpha]$, where $\alpha^3 = \alpha + 1$. Verify that $23R = (23, \alpha - 10)^2(23, \alpha - 3)$.

(ii) Show that $(23, \alpha - 10, \alpha - 3) = R$; conclude that $(23, \alpha - 10)$ and $(23, \alpha - 3)$ are prime ideals and that they are relatively prime.

Exercise 3. The aim of this exercise is to prove that the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$, where $\alpha = \sqrt[3]{2}$.

(i) We put $\beta = \alpha + 1$. Show that $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = 2$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) = 3$.

(ii) Show that $|\mathrm{disc}(1, \alpha, \alpha^2)| = |\mathrm{disc}(1, \beta, \beta^2)| = 3^3 2^2$

(iii) Using Ex 1 of exercise sheet 3, show that

$$\mathcal{O}_K \subseteq \left\{ \frac{a_0 + a_1\alpha + a_2\alpha^2}{6} | a_i \in \mathbb{Z} \right\}$$

$$\mathcal{O}_K \subseteq \left\{ \frac{b_0 + b_1\beta + b_2\beta^2}{6} | b_i \in \mathbb{Z} \right\}$$

(iv) Let $p \in \{2, 3\}$ and

$$\gamma = \begin{cases} \alpha & \text{if } p = 2 \\ \beta & \text{if } p = 3 \end{cases}$$

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on May 20th.

and $q = \frac{6}{p}$. Show that for all

$$\frac{c_0 + c_1\gamma + c_2\gamma^2}{6} \in \mathcal{O}_K$$

we have that $c_0 \equiv c_1 \equiv c_2 \equiv 0 \pmod{p}$

(v) Using (iii) and (iv) deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$.

Exercise 4. Let K be a field.

(i) Is $K[X]$ a Dedekind domain?
(ii) Is $K[X, Y]$ a Dedekind domain?

Exercise 5. Let ζ be a primitive m-th root of 1.

(i) Show that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(m)$, where ϕ is the Euler's totient function.
(ii) Show that the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the group $(\mathbb{Z}/m\mathbb{Z})^*$ of invertible elements modulo m.