April 19th, 2016

Number Theory II

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

Exercise sheet 1[1]

Exercise 1. An integer d is called *square-free*, if $a^2|d$ implies $a = \pm 1$. Let $K = \mathbb{Q}(\sqrt{d})$. This is a number field of degree 2. In this exercise we compute the ring of integers $\mathcal{O}_K$. Recall that every element of K is of the form $a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$.

(i) If $a, b \in \mathbb{Q}$, then $a + b\sqrt{d} \in \mathcal{O}_K$ if and only if $2a \in \mathbb{Z}$, $2b \in \mathbb{Z}$ and $(2a)^2 - d(2b)^2 \equiv 0 \mod 4$.

(ii) We have

$$\mathcal{O}_K = \begin{cases} \left\{ a + b\sqrt{d} \,\middle|\, a, b, \in \mathbb{Z} \right\} \subset K & \text{if } d \equiv 2 \mod 4 \text{ or } d \equiv 3 \mod 4 \\ \left\{ \frac{a+b\sqrt{d}}{2} \,\middle|\, a, b \in \mathbb{Z}, a - b \text{ even} \right\} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

(iii) $\mathcal{O}_K$ is a free abelian group of rank 2 with a basis given by

$$\begin{cases} \{1, \sqrt{d}\} & \text{if } d \equiv 2, 3 \mod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Exercise 2. We consider the ring $\mathbb{Z}[i]$ of algebraic integers of $\mathbb{Q}(i)$.

(a) Show that $\mathbb{Z}[i]$ is an Euclidean domain, so in particular it is PID and UFD. (Hint: Consider the function $\varphi : \mathbb{Z}[i] \to \mathbb{N}$ which sends $\alpha \in \mathbb{Z}[i]$ to $\alpha\overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate of α. Prove that for every α and $\beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r$$

and $\varphi(r) < \varphi(\beta)$.)

(b) Show that the function φ in (a) is multiplicative.

(c) Use (b) to show that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\alpha = \pm 1, \pm i$.

Exercise 3. Let ζ_5 be the 5th root of unity $\exp(\frac{2\pi i}{5})$ and let $x = \cos(\frac{2\pi}{5})$.

(i) Prove that $2x$ is integral over $\mathbb{Z}$ and belongs to $\mathbb{Z}[\zeta_5]$.

(ii) Prove that x is algebraic over $\mathbb{Q}$, but not integral over $\mathbb{Z}$.

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on April 29th.

(iii) Prove that $2x$ is in fact an element of the ring of integers of $\mathbb{Q}(\sqrt{5})$, and hence $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$. Is this inclusion an equality?

Exercise 4. *This exercise is not part of the assignment, you can skip it. It is here only to complement the first part of the lecture.*

The goal of this exercise is to prove Fermat's last theorem for $n = 4$, using the description of the Pythagorean triples we saw in class.

If $x^4 + y^4 = z^4$ has a solution in positive integers, then so does $x^4 + y^4 = w^2$. Let x, y, w be a solution with smallest possible w. Then x^2, y^2, w is a primitive Pythagorean triple. Assuming (without loss of generality) that x is odd, we can write $x^2 = m^2 - n^2$, $y^2 = 2mn$, $w = m^2 + n^2$ with m and n relatively prime positive integers, not both odd.

(i) Show that $x = r^2 - s^2$, $n = 2rs$, $m = r^2 + s^2$, with r, s relatively prime positive integers, not both odd.

(ii) Show that r, s, m are pairwise relativey prime. Using $y^2 = 4rsm$, conclude that r, s and m are all squares, say a^2, b^2 and c^2.

(iii) Show that $a^4 + b^4 = c^2$, and that this contradicts minimality of w.