May 4th, 2016

Number Theory II

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

Exercise sheet 3[1]

Exercise 1. Let K be a number field, with ring of integers $\mathcal{O}_K$, let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of K over $\mathbb{Q}$ consisting of algebraic integers and set $D = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. Then every $\alpha \in \mathcal{O}_K$ can be expressed in the form

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{D}$$

with $m_j \in \mathbb{Z}$ and all m_j^2 divisible by D.

Exercise 2. Let $p > 2$ be a prime number and $\zeta \in \mathbb{C}$ a primitive p-th root of unity. This means that $\zeta^p = 1$ and $\zeta^i \neq 1$ for $0 < i < p$.

(i) For an algebraic number α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ we denote $\mathrm{disc}(1, \ldots, \alpha^{n-1})$ by $\mathrm{disc}(\alpha)$. Show that $\mathrm{disc}(1-\zeta) = \mathrm{disc}(\zeta)$ and that this integer number is divisible only by the prime p.

(ii) Show, using ex 1, that

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \{a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1} | a_0, \ldots, a_{p-1} \in \mathbb{Z}\} = \mathbb{Z}[\zeta],$$

where $\mathcal{O}_{\mathbb{Q}(\zeta)}$ is the ring of integers of $\mathbb{Q}(\zeta)$.

Exercise 3. Let α be a root of the polynomial $X^3 + 5X + 1$. Describe the ring of integers of $\mathbb{Q}(\alpha)$.

Exercise 4. Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$, and let α be an algebraic integer in K. The following argument shows that the ring of integers $\mathcal{O}_K$ is not $\mathbb{Z}[\alpha]$.

(i) Consider the following algebraic integers:

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10});$$
$$\alpha_2 = (1+\sqrt{7})(1-\sqrt{10});$$
$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10});$$
$$\alpha_4 = (1-\sqrt{7})(1-\sqrt{10}).$$

Show that all the products $\alpha_i\alpha_j$, $i \neq j$, are divisible by 3 in $\mathcal{O}_K$, but 3 does not divide any power of any α_i.

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on May 13th.

(ii) Assume now that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, we shall derive a contradiction. Let $f(X)$ be the minimum polynomial of α over $\mathbb{Q}$. For $g(X) \in \mathbb{Z}[X]$, let $\overline{g(X)}$ denote the image of g in $\mathbb{F}_3[X]$. Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ if and only if $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{F}_3[X]$.

(iii) For each i, $1 \leq i \leq 4$, let f_i be a polynomial in $\mathbb{Z}[X]$ such that $\alpha_i = f_i(\alpha)$. Show that $\overline{f} \mid \overline{f_i f_j}$ $(i \neq j)$ in $\mathbb{F}_3[X]$, but $\overline{f}$ does not divide $\overline{f_i}^n$ for any n. Conclude that for each i, $\overline{f}$ has an irreducible factor which does not divide $\overline{f_i}$ but does divide all $\overline{f_j}$, $j \neq i$.

(iv) This shows that $\overline{f}$ has at least four distinct irreducible factors over $\mathbb{F}_3$. On the other hand, f has degree at most 4. Why is this a contradiction?

Let A be an integrally closed domain with field of fractions K, and let B be the integral closure of A in a separable extension L of K of degree m. Let $\{\beta_1, \ldots, \beta_m\}$ be a basis of L over K made of integral elements. If $C = \sum A\beta_i \subset B$ we define $C^* = \{\beta \in L | \mathrm{Tr}(\beta\gamma) \in A \, \forall \gamma \in C\}$.

Exercise 5. We suppose that $L = \mathbb{Q}[\beta]$, with $\beta \in B$, and let f be the minimum polynomial of β. Let $C = \mathbb{Z}[\beta]$. We want to find C^*.

(i) Show that

$$\mathrm{Tr}\left(\frac{\beta^i}{f'(\beta)}\right) = \begin{cases} 0 & \text{if } 0 \leq i \leq m-2 \\ 1 & \text{if } i = m-1 \end{cases}$$

(ii) Show that C^* is a free $\mathbb{Z}$-module with basis $\{\frac{1}{f'(\beta)}, \ldots, \frac{\beta^{m-1}}{f'(\beta)}\}$.