Prof. Dr. Y. Tian
Dr. J. Anschütz

WS 2017/18

Algebraic Number Theory

2. Exercise sheet

Exercise 1 (4 Points):

Prove that $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\mu_8)$ are all the subfields of the 8-th cyclotomic field $\mathbb{Q}(\mu_8)$. For $L = \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$ compute the character

$$(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q}) \cong \{\pm 1\}.$$

Exercise 2 (4 Points):

Let $A \subseteq B$ be an extension of rings and let $C \subseteq B$ be the integral closure of A in B. Let $S \subseteq A$ be a multiplicative subset. Prove that $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Exercise 3 (4 Points):

Let $f(x) = x^3 + ax + b$ be an irreducible polynomial over $\mathbb{Q}$, and let $\alpha \in \mathbb{C}$ be a root of $f(x)$. Set $K = \mathbb{Q}[\alpha]$, and $\mathcal{O}_K$ to be the ring of integers of K.

1) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$ and find an irreducible polynomial for $2a\alpha + 3b$ over $\mathbb{Q}$.
2) Show that $\mathrm{Disc}_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -(4a^3 + 27b^2)$.
3) Prove that $f(x)$ is irreducible when $a = b = -1$, and find an integral basis of K.

Exercise 4 (4 Points):

Consider the number field $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$, and let $\mathcal{O}_K$ be its ring of integers. The aim of this exercise is to show that there exists no algebraic integer such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

1) Consider the elements:
$$\begin{aligned} \alpha_1 &= (1+\sqrt{7})(1+\sqrt{10}) \\ \alpha_2 &= (1+\sqrt{7})(1-\sqrt{10}) \\ \alpha_3 &= (1-\sqrt{7})(1+\sqrt{10}) \\ \alpha_4 &= (1-\sqrt{7})(1-\sqrt{10}) \end{aligned}$$
Show that for any $i \neq j$, the product $\alpha_i\alpha_j$ is divisible by 3 in $\mathcal{O}_K$.
2) Let $i \in \{1,2,3,4\}$ and $n \geq 0$ be an integer. Show that
$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \equiv (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \bmod 3.$$
Deduce that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i) \equiv 1 \bmod 3$ and hence 3 does not divide $\alpha_i \in \mathcal{O}_K$.
3) Let α be an algebraic integer. Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α. For all polynomials $g \in \mathbb{Z}[X]$, we denote by $\overline{g} \in \mathbb{F}_3[X]$ its reduction modulo 3. Show that $g(\alpha)$ is divisible by 3 in $\mathcal{O}_K$ if and only if $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{F}_3[X]$.
4) For $1 \leq i \leq 4$, let $g_i(X) \in \mathbb{Z}[X]$ be such that $\alpha_i = g_i(\alpha)$. Show that there exists an irreducible factor of $\overline{f}$ that divides $\overline{g}_j$ for any $j \neq i$ but does not divide $\overline{g}_i$.
5) Consider the number of irreducible factors of $\overline{f}$ and deduce a contradiction.

To be handed in: Monday, 30. October 2017.