ZAHLENTHEORIE II – ÜBUNGSBLATT 10

PROF. DR. HÉLÈNE ESNAULT AND DR. LEI ZHANG

Exercise 1. Let K, L be number fields. Recall that KL is defined to be $K[L] = L[K]$, i.e. the extension of L generated by the elements of K or vice versa.

Assume that $[K : \mathbb{Q}][L : \mathbb{Q}] = [KL : \mathbb{Q}]$. This exercise proves that if $d = \gcd(d_K, d_L)$ is the greatest common divisor of the discriminants of K, L, then

$$\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L.$$

(a) Fix an embedding $\tau : L \hookrightarrow \mathbb{C}$. Show that every embedding $\sigma : K \hookrightarrow \mathbb{C}$ of K extends uniquely to an embedding $\hat{\sigma} : KL \hookrightarrow \mathbb{C}$ such that $\hat{\sigma}|_L = \tau$.

(b) Let $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ and $\beta_1, \dots, \beta_m$ an integral bases of $\mathcal{O}_L$. Show that $\{\alpha_i\beta_j | i = 1, \dots, n, j = 1, \dots, m\}$ is a $\mathbb{Q}$-basis of KL.

(c) Show that every $\gamma \in \mathcal{O}_{KL}$ can be written as

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r}\alpha_i\beta_j$$

with $a_{ij} \in \mathbb{Z}$ and with $r \in \mathbb{Z} \setminus \{0\}$ such that there exists no prime p with $p|r$ and $p|a_{ij}$ for all i, j.

(d) Define $x_i = \sum_{j=1}^{m} \frac{a_{ij}}{r}\tau(\beta_j) \in \mathbb{C}$ and show that $d_K x_i$ is integral over $\mathbb{Z}$. Conclude that $r|d_K$. Interchanging the roles of K and L, conclude that $r|d_L$ and hence that $r|\gcd(d_K, d_L)$.

(e) Conclude that

$$\mathcal{O}_{KL} \subseteq \frac{1}{\gcd(d_K, d_L)}\mathcal{O}_K\mathcal{O}_L.$$

Exercise 2. Let ζ_n be a primitive n-th root of 1, $n \geq 2$. In the class we have shown that if p ramifies then $p|n$. Is the converse true?

Exercise 3. (a) Recall for $m > 1$ that $\phi(m)$ denotes the order of the group $(\mathbb{Z}/m\mathbb{Z})^*$. Show that if $m, n > 1$ are coprime to each other, then $\phi(mn) = \phi(m)\phi(n)$.

(b) Let $m, n > 1$ be natural numbers. Show that $\phi(mn) \geq \phi(n)$, and the equality holds if and only if $m = 2$ and n is odd.

(c) Let $n > 1$ be an integer. Show that $\mu(\mathbb{Q}(\zeta_n))$ has order n when n is even and has order $2n$ when n is odd.

Exercise 4. Let m, n be mutually coprime natural numbers which are greater than 1. Show that $\mathbb{Q}(\zeta_m) \bigcap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

If you want your solutions to be corrected, please hand them in just before the lecture on June 27, 2017. If you have any questions concerning these exercises you can contact Dr. Lei Zhang via `l.zhang@fu-berlin.de` or come to Arnimallee 3 112A.