Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Make Up Exam

Question 1.

1. Give an example of a number field $F \neq \mathbb{Q}$ such that 3 and 5 are ramified in $F/\mathbb{Q}$.
2. Give an example of a number field $F \neq \mathbb{Q}$ such that 3 and 5 are inert in $F/\mathbb{Q}$.
3. Give an example of a number field $F \neq \mathbb{Q}$ such that 3 and 5 are unramified, but not inert in $F/\mathbb{Q}$.

Question 2.

1. Let $\alpha = \sqrt[3]{2}$, $K = \mathbb{Q}(\alpha)$. Let $a, b, c \in \mathbb{Q}$. Express the trace
$$\mathrm{Tr}_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2)$$
in terms of a, b, and c.
2. Give an example of an algebraic number $\beta \in \mathbb{C}$ which is not integral over $\mathbb{Z}$, but such that $\mathrm{N}_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta) \in \mathbb{Z}$.

Question 3. Let $\alpha \in \mathbb{C}$ with $\alpha^2 - \alpha + 9 = 0$, and let $K = \mathbb{Q}(\alpha)$.

1. Determine the class group of K.
2. Determine all prime numbers p which are ramified in $K/\mathbb{Q}$.

Question 4. Let $\alpha \in \mathbb{C}$ be a zero of $f(X) = X^3 + 2X - 1$. Let $K = \mathbb{Q}(\alpha)$.

1. Prove that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
2. Prove that α is a unit in the ring of integers $\mathcal{O}_K$ of K.
3. Prove that the rank of $\mathcal{O}_K^\times$ as a $\mathbb{Z}$-module is 1.

Question 5. Let L/K be a finite Galois extension of number fields, let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of integers of K and L, respectively, and let $\mathfrak{P} \subset \mathcal{O}_L$ be a maximal ideal.

1. State the definition of the *decomposition group* of $\mathfrak{P}$.
2. Let $E := L^{I_{\mathfrak{P}}}$ be the fix field of the inertia subgroup $I_{\mathfrak{P}}$ of $\mathfrak{P}$. Let $\mathfrak{P}' := \mathfrak{P} \cap \mathcal{O}_E$. Prove that $\mathfrak{P}'$ is unramified in the extension E/K. (*Hint.* You may use that the ramification index is multiplicative in a tower of field extensions.)

Question 6. Let $\zeta \in \mathbb{C}$ be a primitive 8-th root of unity, let $K = \mathbb{Q}(\zeta)$, and let $\mathcal{O}_K = \mathbb{Z}[\zeta]$ be the ring of integers of K.

1. Show that the minimal polynomial of ζ over $\mathbb{Q}$ is $X^4 + 1$.
2. Show that for every prime number p, the polynomial $X^4 + 1$ is reducible in $\mathbb{F}_p[X]$.

Question 7.

1. Compute the p-adic absolute value $\left|\frac{4}{5}\right|_p$ for all prime numbers p.
2. Show that the series
$$\sum_{i=0}^{\infty} 15^i$$
converges in $\mathbb{Q}_5$ and compute its limit.

Cheat sheet

Quadratic number fields. Let $d \neq 0, 1$ be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$.

- If $d \equiv 1 \mod 4$, then the absolute discriminant of K is d, and its ring of integers is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.
- If $d \not\equiv 1 \mod 4$, then the absolute discriminant of K is $4d$, and its ring of integers is $\mathbb{Z}[\sqrt{d}]$.

Discriminant. Let L/K be a separable field extension of degree 3, and assume that $x \in L$ such that $L = K(x)$ and $x^3 + ax + b = 0$, $a, b \in K$. Then the discriminant $D(1, x, x^2)$ is equal to $-4a^3 - 27b^2$.

Minkowski bound.

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}_K|}$$

Prime ideals in an extension of number fields. Let L/K be an extension of number fields and let $\mathcal{O}_L$, $\mathcal{O}_K$ denote the rings of integers of L and K, respectively. A non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is called

- *inert in* L/K, if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal in $\mathcal{O}_L$,
- *split in* L/K, if $\mathfrak{p}\mathcal{O}_L$ is a product of $[L : K]$ pairwise different prime ideals of $\mathcal{O}_L$,
- *ramified in* L/K, if there exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ with $\mathfrak{p} \subseteq \mathfrak{P}^2$.