Prof. Dr. Y. Tian **WS 2017/18**
Dr. J. Anschütz

Algebraic Number Theory

4. Exercise sheet

Exercise 1 (4 Points):

Let K be a number field of degree $n = [K\colon \mathbb{Q}]$, and $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, and $\alpha = \alpha_1, \cdots, \alpha_n$ be the roots of $f(x)$.

1) Verify the equality
$$\frac{1}{f(x)} = \sum_{i=1}^{n} \frac{1}{f'(\alpha_i)(x-\alpha_i)}.$$
Hint: Prove that the polynomial $f(x)\sum_{i=1}^{n}\frac{1}{f'(\alpha_i)(x-\alpha_i)} - 1$ *is of degree* $n-1$ *and has* n *roots.*

2) Prove that
$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{\alpha^{i-1}}{f'(\alpha)}\right) = \begin{cases} 0 & \text{if } 1 \leq i \leq n-1 \\ 1 & \text{if } i = n-1. \end{cases}$$
Hint: Write the two sides of the equality in 1) into power series of $\frac{1}{x}$*, and compare the coefficients of* $\frac{1}{x^i}$ *for* $1 \leq i \leq n$.

3) Use 2) to show that $\delta_K^{-1} = (\frac{1}{f'(\alpha)})$.

Exercise 2 (4 Points):

Consider the fields $\mathbb{Q}(\zeta_{23})$, and $K = \mathbb{Q}(\sqrt{-23}) \subseteq \mathbb{Q}(\zeta_{23})$. Let $\mathfrak{p}$ be the prime ideal $(2, (1+\sqrt{-23})/2)$ of $\mathcal{O}_K$. Show that there exists a unique prime ideal $\mathcal{P}$ of $\mathbb{Q}(\zeta_{23})$ above $\mathfrak{p}$, and that $\mathcal{P}$ is not a prinicipal ideal.

Exercise 3 (4 Points):

Let $K = \mathbb{Q}(\zeta_{25})$.

1) Prove that K has a unique subfield of degree 5 over $\mathbb{Q}$, and find an explicit $\alpha \in K$ such that $M = \mathbb{Q}(\alpha)$.
2) Find the decompositions of the primes $p = 2, 3, 5$ in $M/\mathbb{Q}$, and their corresponding decomposition subfields.
3) Prove that p splits in M if and only if $p \equiv \pm 1, \pm 7 \bmod 25$.

Exercise 4 (4 Points):

1) Let $f(X) \in \mathbb{Z}[X]$ be a non-constant polynomial. Prove that there exist infinitely many primes p such that the image of $f(X)$ in $\mathbb{F}_p[X]$ has a root in $\mathbb{F}_p$.
Hint: Consider the prime factors of $f(n!a_0)/a_0$ *for some large* n*, where* $a_0 = f(0)$.
2) Show that, given an integer N, there are infinitely many primes p with $p \equiv 1 \bmod N$.
Hint: Apply 1) to the cyclotomic polynomial $f(X) = \Phi_N(X)$.

To be handed in: Monday, 13. November 2017.