Homework 2 - Number Theory

Exercise 1. Let $F = \mathbb{Q}(\alpha)$ where α is the unique positive fourth root of 3 in $\mathbb{R}$.

a) Find the matrix φ_β of the multiplication by $\beta = \alpha^2 - 2\alpha - 1$ map on F. Compute $N_{F/\mathbb{Q}}(\beta)$ and $Tr_{F/\mathbb{Q}}(\beta)$.

b) Find the zeros of the minimal polynomial $p_{\alpha,\mathbb{Q}}(X)$ of α in $\mathbb{C}$ and the images of β under the four embeddings of F into $\mathbb{C}$.

c) Determine the characteristic polynomials $\chi_{\alpha,\mathbb{Q}}(X)$, $\chi_{\alpha^2,\mathbb{Q}}(X)$ and $\chi_{\alpha-1,\mathbb{Q}}(X)$.

d) Compute $Tr(\alpha^i)$ for $0 \leq i \leq 3$, the 4×4-matrix with entries $Tr(\alpha^{i-1}\alpha^{j-1})$ and the discriminant $\Delta_{F/\mathbb{Q}}(1, \alpha, \alpha^2, \alpha^3)$.

Exercise 2. **a**) Show that $\overline{\mathbb{Q}}$ is not a number field.

b) Let F be a number field. Its multiplicative group of roots of unity is defined by

$$\mu(F) = \{\alpha \in F | \alpha^n = 1 \text{ for some } n \in \mathbb{N}\}.$$

Show that $\mu(F)$ is a finite group. (It follows that $\mu(F)$ is cyclic.)

c) Show that the ring $\overline{\mathbb{Z}}$ of all algebraic integers is not Noetherian.

d) Let $\overline{\mathbb{Z}}_d^M$ be the set of algebraic integers α of degree at most d over $\mathbb{Q}$ such that α has absolute value bounded by M. Is it true that $\#\overline{\mathbb{Z}}_d^M < \infty$?

Exercise 3. Let F be a number field and $L = F(\alpha)$ with minimal polynomial $p_\alpha(X)$ of degree m.

a) Verify the formula $\Delta_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{m-1}) = (-1)^{\frac{m(m-1)}{2}} N_{L/K}(p'_\alpha(\alpha))$.

b) Compute $\Delta_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})$ when $p_\alpha(X) = X^m + aX + b$.

(Answer: $(-1)^{\frac{m(m-1)}{2}}(m^m b^{m-1} + (-1)^{m-1}(m-1)^{m-1}a^m)$).

c) Let $L = \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha = 1$. Show that $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Exercise 4. **a**) Read the statement and proof of Proposition 2.11 in the textbook.

b) Identify $\mathcal{O}_F$ for $F = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

c) Prove Proposition 2.12 in the textbook.

d) If $\alpha^3 = \alpha + 4$, show that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}\{1\} \oplus \mathbb{Z}\{\alpha\} \oplus \mathbb{Z}\{\frac{\alpha^2+\alpha}{2}\}$ as abelian groups.

Exercise 5. Let F be a number field.

a) Prove Stickelberger's theorem (1897): The discriminant $\Delta_F \equiv 0, 1 \bmod 4$.

b) Prove Kronecker's theorem (1882): The sign of Δ_F equals $(-1)^c$ where c is the number of pairs of complex embeddings of F ($\sigma\colon F \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$).

Exercise 6. **a**) If L/K is inseparable, show that $Tr_{L/K} = 0$.

b) Explicate the proof in **a**) for your favorable inseparable field extension.