Seventh exercise sheet "Algebra II" winter term 2024/5. The following can be derived from Proposition 2.5.3 of the lecture.

Problem 1 (3 points). *Let $A \in \mathrm{Mat}(m,m;\mathbb{Z})$ be a matrix with non-vanishing determinant. Show that $\#(\mathbb{Z}^m/A\mathbb{Z}^m) = |\det A|$.*

Let K be an algebraic number field, $S \subseteq K$ a subring with field of quotients K for which the additive group $(S,+)$ is finitely generated. Such subrings are called *orders* in K. If $\vec{s} = (s_i)_{i=1}^m$ is a base for this free abelian group we put

$$\mathbf{d}_S = \det\bigl(\mathrm{Tr}_{K/\mathbb{Q}}(s_i s_j)\bigr)_{i,j=1}^m. \tag{1}$$

If $\vec{t}$ is another base then $\vec{t} = A\vec{s}$ and $\vec{s} = B\vec{t}$ for integer matrices A and B which are inverse to each other. As $\det(A)\det(B) = 1$ we have $\det A = \det B \in \{\pm 1\}$. As (1) gets multiplied by the square of this determinant when the base is replaced by $\vec{t}$, (1) is independent of the choice of the base.

As in the lecture let $S^* = \bigl\{k \in K \bigm| \mathrm{Tr}_{K/\mathbb{Q}}(kS) \subseteq \mathbb{Z}\bigr\}$.

Problem 2 (2 points). *Show that $[S^* : S] = \mathbf{d}_S$.*

Remark 1. *We have $S \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^* \subseteq S^*$ and it is not hard to show that $[\mathcal{O}_K : S] = [S^* : \mathcal{O}_K^*]$ which we denote by f. Then $\mathbf{d}_S = f^2 \mathbf{d}_{\mathcal{O}_K}$. This has the interesting consequence that $S = \mathcal{O}_K$ when $\mathbf{d}_S$ is square free.*

Problem 3 (3 points). *If $I \subseteq \mathcal{O}_K$ is a non-zero ideal, show that $n = [\mathcal{O}_K : I]$ is finite and $\mathrm{N}_{\mathcal{O}_K/\mathbb{Z}} I = n\mathbb{Z}$.*

Problem 4 (3 points). *If $S = \mathcal{O}_K$, show that $\mathfrak{d}_{S/\mathbb{Z}} = \mathbf{d}_S \mathbb{Z}$.*

This equalitiy of ideals in $\mathbb{Z}$ determines $\mathbf{d}_S$ from $\mathfrak{d}_{S/\mathbb{Z}}$ up to sign, and the sign is determined by the fact that $\mathbf{d}_S$ is positive if and only if the number of field homomorphisms $K \to \mathbb{C}$ with image not contained in $\mathbb{R}$ (which is even) is divisible by four.

Problem 5 (2 point). *Let R be a Dedekind domain with field of quotients K, L a finite field extension of K and $S \subseteq L$ a subring which is integral over R, where we assume $R \neq K$ and that L is the field of quotients of S. Show that S is the integral closure of R in K if and only if $S_\mathfrak{m}$ is a discrete valuation ring for all $\mathfrak{m} \in \mathrm{mSpec} S$.*

With $\mathfrak{m}$ as before, let $S^{(\mathfrak{m})} = \bigl\{l \in L \bigm| l\mathfrak{m} \subseteq \mathfrak{m}\bigr\}$.

Problem 6 (3 points). *In the situation of the previous problem, show that S is the integral closure of R in L if and only if $S^{(\mathfrak{m})} = S$ for all $\mathfrak{m} \in \mathrm{mSpec} S$.*

General methods for determining $\mathcal{O}_K$ for an algebraic number field K usually start with an order S for K. One method for finding $\mathcal{O}_K$ uses the criterion from the previous problem, which is automatically satisfied at all $\mathfrak{m}$ not containing $\mathbf{d}_S$, which only leaves finitely many remaining $\mathfrak{m}$. For these it is easy to see that $S^{(\mathfrak{m})}$ is integral over $\mathbb{Z}$, hence an order for K. If it is larger than S one can replace S by $S^{(\mathfrak{m})}$ and start a new iteration of the method. If there is no $\mathfrak{m}$ for which $S^{(\mathfrak{m})}$ is larger than S, we terminate with $\mathcal{O}_K = S$. In this it is sufficient to consider $S^{(\mathfrak{m})}$ with $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$ where p^2 divides $\mathbf{d}_S$.

Of course this requires a number of algorithms which are beyond the scope of this lecture module. For instance, it is necessary to decompose $\mathbf{d}_S$ into prime factors. From the point of view of algorithmic complexity this is the hardest step. Finding the $\mathfrak{m}$ containing p with $p^2|\mathbf{d}_S$ then uses algorithms for polynomials over finite fields to determine the structure of S/pS. A detailed algorithm can be found in the basic text books of H. Cohen (Algorithm 6.1.8) or of Pohst and Zassenhaus (Section 4.6) on basic algorithmic algebraic number theory.

The following is often attributed to Gotthold Eisenstein, although it was found a few years earlier by Theodor Schönemann.

Problem 7 (4 points). *Let A be a factorial domain with field of quotients K, π a prime element of A and $P = \sum_{k=0}^{d} p_k T^k \in A[T]$ with $p_d = 1$, all other p_k divisible by π and p_0 not divisible by π^2. Show that P is irreducible.*

Here the fact that $A[T]$ is factorial can be used without proof, and the same holds for the fact that such P are irreducible in $A[T]$ if and only if this holds in $K[T]$.

Solutions should be submitted to the tutor by e-mail before Friday November 29 24:00.