Algebraic Number Theory

Problem sheet 4

1. (1+2+2 points) Let $\mathfrak{a}$ be a fractional ideal of K, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ for some $\mathfrak{b}, \mathfrak{c} \subseteq \mathcal{O}_K$ integral ideals, define the norm of $\mathfrak{a}$ as follows:

$$N(\mathfrak{a}) := \tfrac{N(\mathfrak{b})}{N(\mathfrak{c})}$$

   (a) Prove that the norm of fractional ideal is well-defined and $N : J_K \mapsto \mathbb{R}_{>0}$ is a homomorphism.

   (b) Show that $d(\mathfrak{a}) = d_K \cdot N(\mathfrak{a})^2$.

   (c) Define $\delta_K^{-1} := \{x \in K \mid \mathrm{Tr}(xy) \in \mathbb{Z}, \forall y \in \mathcal{O}_K\}$, show that δ_K^{-1} is a fractional ideal. Let δ_K denote its inverse, called **different** of K. Show that $N(\delta_K) = |d_K|$.

2. (3 points)(**Hermite**) For any integer d, prove that there are only finitely many number fields with discriminant d.

   Remark. Let us consider the map $d : \{numberfields\} \to \{n | n \equiv 0, 1(4)\}, K \mapsto d_K$.(Recall that we have seen that, if $d = d_K$, then $d \equiv 0, 1(4)$. Thus this map is well-defined). Now one can ask if the map is surjective? Also, theorem of Hermite tells us every fiber is finite, so one can ask if the fibre is uniformly finite?

3. (2 points)(**Universal Mapping Property**) Let R and R' be commutative rings and $S \subset R$ be a multiplicatively closed subset. Assume further that $\varphi\colon R \to R'$ is a ring homomorphism such that $\varphi(S) \subseteq R'^{\times}$. Show that φ extends uniquely to a ring homomorphism $\tilde{\varphi}\colon RS^{-1} \to R'$.

   Remark. It is easy to see that the result still holds when R' is noncommutative.

4. (3 points) Let R be a commutative ring and $S \subset R$ be a multiplicatively closed subset. Show that RS^{-1} is a flat R-module, ie. $RS^{-1} \otimes_R \cdot$ is an exact functor.

5. (3 points) Let R be a commutative ring and M a module, prove that TFAE:

   (a) $M = 0$;

   (b) $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p} \lhd R$;

   (c) $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \lhd R$.

6. (3 points) Let R be a commutative ring and let $f\colon M \to N$ be an R-module homomorphism between R-modules M, N. Show that TFAE:

   (i) f is injective (resp. surjective);

   (ii) $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp. surjective) for all prime ideals $\mathfrak{p} \lhd R$;

   (iii) $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective) for all maximal ideals $\mathfrak{m} \lhd R$.

   Where $M_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R M$, $M_{\mathfrak{m}} = R_{\mathfrak{m}} \otimes_R M$, $N_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R N$, and $N_{\mathfrak{m}} = R_{\mathfrak{m}} \otimes_R N$.

7. (3 points) Let R be an integral domain and $0 \notin S \subset R$ be a multiplicatively closed subset. Assume RS^{-1} is integral over R. Show that $RS^{-1} = R$.

8. (3 points) (Nakayama's Lemma) Let R be a local ring with maximal ideal $\mathfrak{m} \lhd R$ and let M be a finitely generated R-module. Further let $N \leq M$ be a submodule such that $M = N + \mathfrak{m}M$. Show that $M = N$.

9. (3 points) Let K be a field and $v \colon K^\times \to \mathbb{Z}$ be a surjective group homomorphism and let $v(0) = \infty$. Assume $v(x + y) \geq \min(v(x), v(y))$. Verify that $\mathcal{O} := \{\alpha \in K \mid v(\alpha) \geq 0\}$ is a DVR.

10. (3 points) Prove that a ring R is a DVR if and only if R is Dedekind and local ring.

11. (3 points) Let $\mathcal{O}$ be a Dedekind domain and let k be a positive integer. Let $\mathfrak{p}_i \lhd \mathcal{O}$ be a prime ideal for all $1 \leq i \leq k$, $x_i \in K$ (where K is the field of fractions of $\mathcal{O}$) and $n_i \in \mathbb{Z}$. Show that there exists an element $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ $(i = 1, \ldots, k)$ and $v_{\mathfrak{p}}(x) \geq 0$ for all primes $\mathfrak{p} \neq \mathfrak{p}_i$.

12. Let $K/\mathbb{Q}$ be a number field and S be a finite set of prime ideals in $\mathcal{O}_K$. Put $X = \mathrm{Spec}(\mathcal{O}_K) \setminus S$.

    (a) (6+1 points) Verify that the sequence

    $$1 \to \mathcal{O}^\times \to \mathcal{O}(X)^\times \to \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus X} K^\times/\mathcal{O}_{\mathfrak{p}}^\times \to Cl(\mathcal{O}) \to Cl(\mathcal{O}(X)) \to 1\ .$$

    is exact (construction of the maps is part of the problem). Further show that $K^\times/\mathcal{O}_{\mathfrak{p}}^\times \cong \mathbb{Z}$ for all primes $0 \neq \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$.

    (b) (2 points) Verify that $Cl(\mathcal{O}_K(X))$ is finite and $\mathcal{O}_K(X)^\times \cong \mu(K) \times \mathbb{Z}^{|S|+r+s-1}$ where r (resp. s) is the number of real embeddings (resp. of pairs of complex embeddings) of K.

13. (3 points) (Newton polygon) Let $\mathcal{O}$ be a DVR with field of fractions K and valuation $v \colon K^\times \to \mathbb{Z}$. The Newton polygon of a polynomial $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ of degree n is the lower convex hull of the points $(-i, v(a_i))$ in the plain (ie. a convex broken line connecting $(-n, v(a_n))$ with $(0, v(a_0))$ whose vertices are among the points $(-i, v(a_i))$ such that none of these points are below the broken line). Further denote by $S(f)$ the multiset of slopes of the Newton polygon, ie. $S(f)$ is a multiset with n elements such that the multiplicity of the rational number s in $S(f)$ is the length of the projection of line in the Newton polygon with slope s. Show that $S(fg) = S(f) \cup S(g)$. In particular, if the Newton polygon of the polynomial $f(x) \in K[x]$ consists of a single segment with no lattice points apart from the two endpoints then f is irreducible.