Exercise Sheet 6
Algebraic Number Theory

November 13, 2025

Exercise 1. Let K be a field. Fix $\overline{K}$ an algebraic closure of K and let $\alpha \in \overline{K}$ be separable and consider the field extension $K(\alpha)/K$ in $\overline{K}$. Also, let $P \in K[X]$ be the minimal polynomial of α and $n = \deg(P)$

1. Show that for any $x \in K(\alpha)$ it holds that
$$N_{K(\alpha)/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})} \sigma(x)$$
and
$$\mathrm{Tr}_{K(\alpha)/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})} \sigma(x).$$
Hint: Give a look at the Appendix A.4.1

2. Enumerate $\mathrm{Hom}_K(K(\alpha), \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Show that
$$\mathrm{disc}_{K(\alpha)/K}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$ [1]
Hint: Give a look at the Appendix A.4.1

3. Show that
$$\mathrm{disc}_{K(\alpha)/K}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(P'(\alpha)),$$
where $P' \in K[X]$ is the formal derivative of P.

Exercise 2 (Localisation)**.** Let A be a commutative ring and $S \subseteq A$ be non-empty a multiplicative subset[2] containing 1. We define a the equivalence (check it) relation on $A \times S$, $\sim$ by
$$(a, s) \sim (b, t) \iff \exists u \in S : u(at - bs) = 0.$$

We call $A \times S/\sim$ the localization of A by S and denote it by $S^{-1}A$. The equivalence class of (a, s) in $S^{-1}A$ is often denoted $\frac{a}{s}$.

The set $S^{-1}A$ with the binary operations $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + s_1 a_2}{s_1 s_2}$ and $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$ is a commutative ring.

1. Show that $S^{-1}A = \{0\}$ if and only if $0 \in S$. Also show that if A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A = \mathrm{Frac}(A)$.

From now on we assume that $0 \notin S$.

2. Show that the map
$$\psi_S : A \to S^{-1}A;\ a \mapsto \frac{a}{1}$$
is a ring homomorphism. If A is an integral domain and $0 \notin S$, show that it is injective.[3]

[1] Typo in the exercise sheet. Missing the power of 2.
[2] If $s_1, s_2 \in S$, then $s_1 \cdot s_2 \in S$.
[3] In the Exercise Sheet the $0 \notin S$ assumption was missing.

3. Prove the universal property of localisation: given a morphism of rings
$$\phi : A \to B$$
s.t. $\phi(S) \subseteq B^\times$ there is a unique morphism of rings
$$\tilde{\phi} : S^{-1}A \to B$$
s.t.
$$\phi = \tilde{\phi} \circ \psi_S.$$

We can also localise modules: Let M be an A-module. We define a relation on $M \times S$, $\sim$ by
$$(m, s) \sim (n, t) \iff \exists u \in S : u(tm - sn) = 0.$$
This is also an equivalence relation. We call $M \times S/\sim$ the localization of M by S and denote it by $S^{-1}M$. The equivalence class of (m, s) in $S^{-1}M$ is often denoted $\frac{m}{s}$. The set $S^{-1}M$ has a natural $S^{-1}A$-module structure which extends the A-module structure on M.

4. Prove that for given A-modules $N \subseteq M$ we have $S^{-1}(M/N) \simeq (S^{-1}M)/(S^{-1}N)$.
5. Prove that any submodule $N' \subseteq S^{-1}M$ is of the form $S^{-1}N$ for some submodule $N \subseteq M$. Conclude that all ideals of $S^{-1}A$ are of the form $S^{-1}I$ for some ideal $I \subset A$.
6. Show that for an integral domain A the map
$$\{P \subset S^{-1}A \mid P \text{ prime ideal}\} \to \{Q \subset A \mid Q \text{ prime ideal}, Q \cap S = \varnothing\}; P \mapsto \psi_S^{-1}(P)$$
is a bijection.
7. Let $\mathfrak{p} \subset A$ be a maximal ideal. For the multiplicative subset $S = A \setminus \mathfrak{p}$ we denote $S^{-1}A$ by $A_\mathfrak{p}$, called the localisation of A at $\mathfrak{p}$. Show that $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$ and
$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq (A/\mathfrak{p}),$$
i.e., the fraction field of A at $\mathfrak{p}$.

Exercise 3. In class we have shown that if A is a Dedekind ring, then for any prime ideal $\mathfrak{p} \subset A$ the localization $A_\mathfrak{p}$ is a PID. Show the converse, in particular show that if A is a noetherian domain and $A_\mathfrak{p}$ is a PID for every prime ideal $\mathfrak{p} \subset A$, then A is a Dedekind domain.

Exercise 4. Let $K/\mathbb{Q}$ be a finite extension. We know that K is monogeneous, that is $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Fix such an α and *suppose* that $\alpha \in O_K$.

1. Show that $\operatorname{disc}_{K/\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}) \in \mathbb{Z}$.
2. Show that if $\operatorname{disc}_{K/\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1})$ is square-free in $\mathbb{Z}$, then $O_K = \mathbb{Z}[\alpha]$.

Exercise 5. Fix $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$

1. Let $f = X^2 + bX + c \in \mathbb{Q}[X]$ be an irreducible polynomial. Let $\alpha \in \overline{\mathbb{Q}}$ be a root of f. Show that
$$\operatorname{disc}(1, \alpha) = b^2 - 4c.$$
2. Let $\alpha \in \overline{\mathbb{Q}}$ be a root of $X^3 + X + 1 \in \mathbb{Z}[X]$. Compute $\operatorname{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \alpha^2)$ and deduce that $O_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$
3. Compute $\operatorname{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha)$, where $\alpha \in \overline{\mathbb{Q}}$ is a root of $X^2 - b$, and $b \in \mathbb{Z}$ not a cube.
4. Compute $\operatorname{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \alpha^2)$, where $\alpha \in \overline{\mathbb{Q}}$ is a root of $X^3 - 3X + 1$.