Solutions to Exercise Sheet 6
Algebraic Number Theory

November 18, 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.

Solution. 1. We refer to Appendix A.4.1.

2. We refer to Appendix A.4.1.

3. Recall that for any $\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})$ we have $\sigma(\alpha)$ is a roof of P and for any root $\beta \in \overline{K}$ of P there is a $\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})$ so that $\sigma(\alpha) = \beta$. Then we have
$$P(X) = \prod_{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})} (X - \sigma(\alpha)) \in \overline{K}[X].$$
We compute
$$\begin{aligned} P'(X) &= \left(\prod_{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})} (X - \sigma(\alpha)) \right)' \\ &= \sum_{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K})} \prod_{\substack{\tau \in \mathrm{Hom}_K(K(\alpha), \overline{K}) \\ \sigma \neq \tau}} (X - \tau(\alpha)). \end{aligned}$$

[1] Typo in the exercise sheet. Missing the power of 2.

Hence $P'(\alpha) = \prod_{\substack{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K}) \\ \sigma \neq id}} (\alpha - \sigma(\alpha))$. Since the norm is multiplicative we have

$$\begin{aligned} N_{K(\alpha)/K}(P'(\alpha)) &= \prod_{\substack{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K}) \\ \sigma \neq id}} N_{K(\alpha)/K}(\alpha - \sigma(\alpha)) \\ &= \prod_{\substack{\sigma \in \mathrm{Hom}_K(K(\alpha), \overline{K}) \\ \sigma \neq id}} \prod_{\tau \in \mathrm{Hom}_K(K(\alpha), \overline{K})} (\tau(\alpha - \sigma(\alpha))) \\ &= \prod_{\sigma \neq \tau \in \mathrm{Hom}_K(K(\alpha), \overline{K})} (\sigma(\alpha) - \tau(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2. \end{aligned}$$

Hence, the desired result.

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]

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 $S^{-1}(M/N) \simeq (S^{-1}M)/(S^{-1}N)$.

[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.

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 $\mathfrak{p}$.

Solution. 1. Suppose $0 \in S$. Then $(a, s) \sim (0, s)$ for every $a \in A$ and $s \in S$ and so $S^{-1}A = \{0\}$. Suppose $0 \notin S$ (in particular, $0 \neq 1$ in A). Then $(1, 1)$ is not equivalent to $(0, 1)$.

The second claim is clear from the classical construction of the fraction field.

2. ψ_S is clearly a group homomorphism. For the second claim suppose that A is an integral domain and $\psi_S(a) = \psi_S(b)$. Then there exists $s \in S$ so that

$$s(a - b) = 0,$$

since A is a domain and $0 \notin S$ it follows that $a - b = 0$.

3. We define $\tilde{\phi}\colon S^{-1}A \to B$ by $\tilde{\phi}\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1}$.

Well-defined: suppose $\frac{a}{s} = \frac{a'}{s'}$. Then there exists $s'' \in S$ so that $s''(as' - a's) = 0$. Then $\phi(s''(as' - a's)) = 0$ and so $\phi(s'')\left(\phi(a)\phi(s') - \phi(a')\phi(s)\right) = 0$. Since $\phi(s''), \phi(s)$ and $\phi(s')$ are units we multiply by $(\phi(s'')\phi(s)\phi(s'))^{-1}$ and get

$$\phi(a)\phi(s)^{-1} - \phi(a')\phi(s') = 0.$$

Hence $\tilde{\phi}$ is well-defined.

It is clear that $\phi = \tilde{\phi} \circ \psi_S$.

Suppose f is another such a map. Then for any $s \in S$ we have $f(s) = \phi(s)$ and $1 = f(1) = f(s)f\left(\frac{1}{s}\right)$. Hence $f\left(\frac{1}{s}\right) = f(s)^{-1}$. Hence, $f\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$.

4. Consider the map

$$S^{-1}(M/N) \to S^{-1}M/S^{-1}N,\ \frac{1}{s}(x + N) \mapsto \frac{x}{s} + S^{-1}N.$$

I skip the details about well-definiteness and linearity. Let us check that the map is injective: suppose $\frac{1}{s}(x + N)$ is mapped to 0, then $\frac{x}{s} \in S^{-1}N$, that is there exist $n \in N$ and $s' \in S$ so that $\frac{x}{s} = \frac{n}{s'}$. Hence, by definition, there is $t \in S$ so that

$$0 = t(s'x - sn) = ts'x - tsn.$$

That is, $ts'x \in N$, which is equivalent to $\frac{1}{s}(x + N) = (0 + N) \in S^{-1}(M/N)$.

Surjectivity is clear.

5. Let $N' \subset S^{-1}M$ be any submodule. Consider the A-linear map

$$\psi_S\colon M \to S^{-1}M;\ m \mapsto \frac{m}{1}.$$

Let $N = \psi_S^{-1}(N')$. Then N is an A-submodule of M. We claim that $N' = \{\frac{n}{s} \mid n \in N, s \in S\} = S^{-1}N$. Let $\frac{m}{s} \in N'$. Then $\frac{m}{1} = s \cdot \frac{m}{s} \in N'$ and so $m \in N$ and $\frac{m}{s} \in S^{-1}N$. Let $\frac{n}{s} \in S^{-1}N$, with $n \in N$. That is, $\psi_S(n) = \frac{n}{1} \in N'$ and so $\frac{1}{s} \cdot \frac{n}{1} = \frac{n}{s} \in N'$.

The conclusion about ideals is a trivial consequence (the pre-image of an ideal is still an ideal and it is a straightforward computation to show that $S^{-1}I$ is an ideal of $S^{-1}A$, for any ideal $I \subset A$).

6. First we show that the map is well-defined. Let $P \subset S^{-1}A$ a prime ideal. Then $P' = \phi_S^{-1}(P) \subset A$ is a prime ideal. Also suppose $x \in P' \cap S$, then $\frac{x}{1} \in S^{-1}P' = P$ is a unit, which is impossible since $P \subsetneq S^{-1}A$.

   The pre-image under a non-trivial ring homomorphism of a prime ideal is a prime ideal. The inverse map is again given by $\{P \in \operatorname{spec} A \mid P \cap S = \varnothing\} \ni P \mapsto S^{-1}P \in \operatorname{spec}(S^{-1}A)$. We show that this is well-defined: let $\frac{x}{s_1}, \frac{y}{s_1} \in S^{-1}A$ so that $\frac{xy}{s_1 s_2} \in S^{-1}P$. Then there is $t \in S$ so that $txy \in P$. Since $t \notin P$, we deduce $xy \in P$, that is $x \in P$ or $y \in P$ and so we deduce $\frac{x}{s_1}$ or $\frac{y}{s_1}$ lies in P.

7. Let $\frac{x}{s} \in A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p}$, then, in particular, $x \notin P$ and so $x \in S$ and so $\frac{x}{s}$ is a unit ($\frac{x}{s} \cdot \frac{s}{x} = 1$). This shows that $A_\mathfrak{p}$ is local with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$.[4]

   Consider the ring homomorphism

$$A \xrightarrow{\psi_S} A_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

   We claim that this map is surjective. Let $\frac{x}{s} + \mathfrak{p}A_\mathfrak{p} \in A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. We want to find $y \in A$ so that $\frac{x}{s} - \frac{y}{1} \in \mathfrak{p}A_\mathfrak{p}$. The latter happens if and only if $x - sy \in \mathfrak{p}$. Since $s \notin \mathfrak{p}$ there exists $\overline{s} \in A$ so that $s\overline{s} \equiv 1 \pmod{\mathfrak{p}}$. We choose $y = \overline{s}x$ and we see that $x - sy \in \mathfrak{p}$. Hence the map is surjective.

   It is now sufficient to show that ker of the above morphism is $\mathfrak{p}$. But this is clear, since $\frac{x}{1} \in \mathfrak{p}A_\mathfrak{p}$ if and only if there are $y \in \mathfrak{p}$, $s, t \in S$ so that $t(sx - y) \in \mathfrak{p}$ and the latter happens if and only if $x \in \mathfrak{p}$ (since s, t are not in $\mathfrak{p}$ and the ideal is prime).

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.

Solution. First, an observation: let $\mathfrak{p}$ be a prime ideal and consider $A_\mathfrak{p}$, which is a local PID. If $A_\mathfrak{p}$ *is not* a field, we define, for $a \in A$, $v_\mathfrak{p}(a)$ to be the unique integer so that $aA_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(a)}$. Notice that $A_\mathfrak{p}$ is a field if and only if $\mathfrak{p} = (0)$. For each prime $\mathfrak{p}$ we see $A_\mathfrak{p} \subset Q$ (see Exercise 2.3), more precisely for $\mathfrak{p} \neq (0)$ we have

$$A_\mathfrak{p} = \left\{ \frac{a}{b} \in Q \mid a \in A,\ b \notin \mathfrak{p} \right\}.$$

Next, we show that A is integrally closed. Let $Q = \operatorname{Frac}(A)$ and let $x \in Q$ be integral over A. Trivially, x is integral over $A_\mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{spec} A$, so since $A_\mathfrak{p} \subset Q$ is a PID and so integrally closed, $x \in \bigcap_{\mathfrak{p} \in \operatorname{spec} A} A_\mathfrak{p} \subset \bigcap_\mathfrak{m} A_\mathfrak{m}$, where the second intersection is taken over all maximal ideals of A. We conclude by using the following claim.

Claim: $\bigcap_\mathfrak{m} A_\mathfrak{m} = A$. The inclusion of the right-hand side into the left-hand side is already done in Exercise 2. Suppose $x = \frac{a}{b} \in \bigcap_\mathfrak{m} A_\mathfrak{m}$. Suppose $x \notin A$. Then the ideal $J = \{y \in A \mid yx \in A\}$ is the proper ideal of A. Hence J is contained in some maximal ideal $\mathfrak{m}$. Since $\frac{a}{b} \in A_\mathfrak{m}$, there exist a' and $s \notin \mathfrak{m}$, so that $\frac{a'}{s} = \frac{a}{b}$. Then $sx = s \cdot \frac{a'}{s} = a' \in A$, in particular, one deduces that $s \in \mathrm{m}$, which is a contradiction.

We still have to show that every non-zero prime ideal of A is maximal. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. By the correspondence in Exercise 2.6 the ideal $(A \setminus \mathfrak{m})^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{m}$ is prime. Since $A_\mathfrak{m}$ is principal there exists $\varpi \in A_\mathrm{m}$ so that $(\varpi) = \mathfrak{m}A_\mathfrak{m}$ and since $A_\mathfrak{m}$ is local we can write $\mathfrak{p}A_\mathfrak{m} = (\varpi)^n = (\varpi^n)$, for some $n \in \mathbb{Z}_{\geq 1}$ or $\mathfrak{p} = (0)$. In particular, since $\mathfrak{p}A_\mathfrak{m}$ is prime we deduce that $\mathfrak{p}A_\mathfrak{m} = (0)$ or $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$. Again, by the correspondence in Exercise 2.6 we see that $\mathfrak{p} = \mathfrak{p}A_\mathfrak{m} \cap A$, which is equal to (0) or $\mathfrak{m}$.

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

[4] A commutative ring R is local with unique maximal ideal $\mathfrak{m}$ if and only if $R^\times = R \setminus \mathfrak{m}$.

Solution. 1. Since $\alpha^j \in O_K$ for every $j \in \mathbb{Z}_{\geq 0}$, we see that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q} \cap O_K = \mathbb{Z}$. Hence $\mathrm{disc}(1, \alpha, \cdots, \alpha^{n-1}) = \det((\mathrm{tr}_{K/\mathbb{Q}}(\alpha^{i+j-2})_{1 \leq i,j, \leq n}) \in \mathbb{Z}$.

2. Let $(b_1, \ldots, b_n)$ be a $\mathbb{Z}$-basis of O_K. Let M be the basis change matrix, so that $\alpha^{j+1} = \sum_{i=1}^m M_{ij} b_i$. Notice $M \in \mathrm{Mat}_n(\mathbb{Z})$. Then $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \det(M)^2 \,\mathrm{disc}(b_1, \ldots, b_n)$. If we assume that $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$ is square free, then we see that $\det(M) \in \pm 1$ and so $(1, \ldots, \alpha^{n-1})$ is a $\mathbb{Z}$- basis of O_K. That is $O_K = \mathbb{Z}[\alpha]$.

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

Solution. 1. We use exercise 1 and see that
$$\mathrm{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha) = (-1) N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(2\alpha + b).$$
The multiplication by $2\alpha + 1$ is given in the basis of $(1, \alpha)$, by the matrix
$$\begin{pmatrix} b & -2c \\ 2 & -b \end{pmatrix}$$
and is determinant is $-b^2 + 4c$. Hence we get the desired result.

2. Again,
$$\mathrm{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \alpha^2) = (-1)^3 N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(3\alpha^2 + 1).$$
The multiplication by $3\alpha^2 + 1$ is represented in the basis $(1, \alpha, \alpha^2)$ by the matrix
$$\begin{pmatrix} 1 & -3 & 0 \\ 0 & -2 & -3 \\ 3 & 0 & -2 \end{pmatrix},$$
whose determinant is 31, in particular square free. Hence we deduce $O_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$.

3. By the first bullet point we have $\mathrm{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha) = 4b$.

4. Again,
$$\mathrm{disc}(1, \alpha, \alpha^2) = (-1)^3 N(3(\alpha^2 - 1)) = -27 N(\alpha^2 - 1) = 81.$$