Exercise Sheet 5
Algebraic Number Theory

October 14, 2025

Exercise 1 (Computing discriminant for quadratic extensions)**.** Let K be a number field. Recall that given an element $x \in K$, we denote by $[\times x]_{K/\mathbb{Q}} \in \mathrm{End}_{\mathbb{Q}}(K)$ the map $K \ni y \mapsto yx$ and we defined the *trace of* $x \in K$ by

$$\mathrm{tr}_{K/\mathbb{Q}}(x) = \mathrm{tr}([\times x]_{K/\mathbb{Q}}).$$

This induces the so-called *trace bilinear form* which is the $\mathbb{Q}$-bilinear form on K given by

$$(x, y) \in K \times K \mapsto \mathrm{tr}_{K/\mathbb{Q}}(xy)$$

Let $\alpha_1, ..., \alpha_n$ be an ordered $\mathbb{Q}$-basis of K, we define the discriminant wrt this basis by

$$\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det(\mathrm{tr}(\alpha_i \alpha_j)_{ij})$$

1. Show that the discriminant is the indipendet of the choice of $\mathbb{Z}$-basis of O_K. We call this quantity the discriminant of K, denoted $\mathrm{disc}(K)$.
2. Compute $\mathrm{disc}(K)$ for $K = \mathbb{Q}(\sqrt{D})$. You may need to consider different cases depending on D.
3. Compare the prime divisors of $\mathrm{disc}(K)$ with the result of Exercise 3, Exercise Sheet 3.

Exercise 2 (Orders in quadratic extensions)**.** Let $K/\mathbb{Q}$ be a finite extension. Recall we constructed O_K, the ring of integers of K, which is a (unital) ring and a finitely generated $\mathbb{Z}$-module and it generates K as $\mathbb{Q}$-vector space. We say that a subring $O \subset K$ is an *order* if O is a finitely generated $\mathbb{Z}$-module and generates K as $\mathbb{Q}$-vector space.

1. Show that O_K is the unique maximal order of K.

Suppose now that $K = \mathbb{Q}(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}$ (with D square-free integer). From Exercise Sheet 3 we know that $O_K = \mathbb{Z} + \mathbb{Z}\alpha_D$, for some integral element α_D.

2. Show that for any order $O \subset \mathbb{Q}(\sqrt{D})$ there exists a unique positive integer f so that $O = \mathbb{Z} + fO_K$.
3. Let (α, β) be a $\mathbb{Z}$ basis of an order $O \subset \mathbb{Q}(\sqrt{D})$. We define $\mathrm{disc}(O) = \mathrm{disc}(\alpha, \beta)$ the discriminant of O. Show that $\mathrm{disc}(O)$ is well-defined (independent of the chosen basis) and compute $\mathrm{disc}(O)$ in terms of D and f as above.

Exercise 3 (Separable algebras over fields)**.** Let Q be a field and K be a commutative algebra over Q, which is finitely generated as Q-module.

1. An algebra A over Q is said to be *reduced* if every $a \neq 0$ in A is *not nilpotent*, meaning that $a^n \neq 0$ for all $n \in \mathbb{Z}_{\geq 0}$. Suppose in addition that K is separable, show then that K is reduced over Q.

2. Show that a finitely generated (as Q-vector space) commutative Q-algebra A has only finitely many maximal ideals.

   Hint: Realize that ideals are Q vector subspaces of A. In particular, first prove that if

   $$\mathcal{B} \supset I_1 \supset \cdots \supset I_m \supset \cdots (0),$$

   is a descending chain of ideals, then there exists $m \in \mathbb{Z}_{\geq 1}$ so that $I_m = I_{m+1}$.

3. Let A be a finitely generated (as K-vector space) commutative reduced K-algebra and $\mathcal{M}$ its finite family of maximal ideals. Show that

   $$A \to \prod_{M \in \mathcal{M}} A/M;\ \beta \mapsto (\beta + M)$$

   is an isomorphism.

   Hint: To show that $J = \bigcap_{M \in \mathcal{M}} M = \{0\}$, show first that there exists $n \geq 1$ so that $J^n = J^{n+1}$. With this try to show that $J^n = \{0\}$ (or assume Nakayama's Lemma).

4. Deduce that if K is as above and moreover it is separable, then there exist finitely many finite separable extensions $K_1, \ldots, K_n$ of Q so that

   $$K \simeq \prod_{i=1}^{n} K_i.$$

5. State and show the converse of the last statement.

Exercise 4 (Quadratic reciprocity law, again and again)**.** We again prove quadratic reciprocity law.[1] Let p, q be distinct odd primes. For any integer n and any $a \in \mathbb{Z}$ define

$$S_n(a;p) = \{(x_1, \ldots, x_n) \in \mathbb{F}_p^n \ | x_1^2 + \cdots x_n^2 = a\}.$$

The goal is to compute the cardinality $|S_q(1;p)| \pmod q$ in two different ways.

1. Notice that $\mathbb{F}_p$ acts on $S_q(a;p)$ by shifting the coordinates :

   $$u \cdot (x_1, \ldots, x_q) = (x_{1+u}, \ldots, x_{q+u}), \qquad u \in \mathbb{F}_q,\ (x_1, \ldots, x_q) \in S_q(a;p).$$

   Show that $S_q(1;p) \equiv 1 + \left(\frac{p}{q}\right) \pmod q$

   Hint: count the number of fixed points.

Next, we find a recursive formula for $S_n(a;p)$:

2. Observe that $|S_n(a;p)| = \sum_{c,d \in \mathbb{F}_p} |S_{n-2}(a - c^2 - d^2; p)|$

3. Show that $|S_1(a;p)| = 1 + \left(\frac{a}{p}\right)$.

4. Show that $|S_2(a;p)| = p - (-1)^{\frac{p-1}{2}}$ if $a \neq 0$ and $|S_2(0;p)| = p + (p-1)(-1)^{\frac{p-1}{2}}$.

   Hint: For the first assertion consider the finitely generated $\mathbb{F}_p$ algebra $\mathbb{F}_p[X]/(X^2+1)$ and consider the norm map.

5. For an integer $n > 2$ show that

   $$|S_n(a;p)| = (p - (-1)^{\frac{p-1}{2}}) \sum_{b \in \mathbb{F}_p} |S_{n-2}(b;p)| + p(-1)^{\frac{p-1}{2}} |S_n(a;p)|$$

   and deduce

   $$|S_n(a;p)| = p^{n-1} + p^{n-2}(-1)^{\frac{p-1}{2}} + p(-1)^{\frac{p-1}{2}} |S_{n-2}(a;p)|$$

   .

6. Deduce that for $n = 2k+1$, $k \in \mathbb{Z}$, one has

   $$|S_n(1;p)| = p^{2k} + p^k (-1)^{k\frac{p-1}{2}}.$$

7. Consider the two expressions of $|S_q(1;p)| \pmod q$ and conclude.

[1] With the solution, I will also provide the reference where I found this proof.