Solutions to Exercise Sheet 5
Algebraic Number Theory

November 3, 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 indipendent 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.

Solution. 1. Let $(b_1, \ldots, b_n)$ and $(c_1, \ldots, c_n)$ be $\mathbb{Z}$-basis of O_K. Then we can write

$$c_j = \sum_{1 \le i \le n} a_{ij} b_i, \qquad 1 \le j \le n.$$

The matrix $A = (a_{ij})_{1 \le i,j \le n} \in \mathrm{Mat}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$ and its inverse also lies in $\mathrm{Mat}_n(\mathbb{Z})$. That is, $A \in \mathrm{GL}_n(\mathbb{Z})$ and so $\det(A) \in \{\pm 1\}$. Since tr is linear we have

$$\mathrm{tr}(c_i c_j) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ki} a_{lj} \,\mathrm{tr}(b_l b_k),$$

that is

$$(\mathrm{tr}(c_i c_j))_{1 \le i,j \le n} = A^t \; (\mathrm{tr}(b_i b_j))_{1 \le i,j \le n} A.$$

Therefore

$$\mathrm{disc}(c_1, \ldots, c_n) = \det(A)^2 \,\mathrm{disc}(b_1, \ldots, b_n) = \mathrm{disc}(b_1, \ldots, b_n).$$

2. Recall, from previous Exercise Sheets, we know that $O_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\alpha_D]$ with $\alpha_D = \sqrt{D}$ if $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$ or $\alpha_D = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \,(\mathrm{mod}\, 4)$. Suppose first $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$, then

$$\mathrm{disc}(1, \sqrt{D}) = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{D}) \\ \mathrm{tr}(\sqrt{D}) & \mathrm{tr}(D) \end{pmatrix}.$$

We compute

$$\mathrm{tr}(\sqrt{D}) = \mathrm{tr}([\times \sqrt{D}]) = \mathrm{tr} \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix} = 0$$

and $\mathrm{tr}(D) = 2D$. Therefore we have

$$\mathrm{disc}(K) = \mathrm{disc}(1, \sqrt{D}) = 4D.$$

Now suppose $D \equiv 1 \pmod 4$. Then

$$\mathrm{disc}(K) = \mathrm{disc}(1, \frac{1+\sqrt{D}}{2}) = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\frac{1+\sqrt{D}}{2}) \\ \mathrm{tr}(\frac{1+\sqrt{D}}{2}) & \mathrm{tr}(\frac{D+1+2\sqrt{D}}{4}) \end{pmatrix}.$$

Using $\mathrm{tr}(1) = 2, \mathrm{tr}(\sqrt{D}) = 0$ we deduce that

$$\mathrm{disc}(K) = 2 \cdot \frac{D+1}{2} - 1 = D.$$

3. The ramified primes are the one dividing the discriminant.

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.

Solution. 1. We show that any order is contained in O_K. Suppose that $O \subset K$ is an order. Since O is a finitely generated $\mathbb{Z}$-module we see that O is in fact integral over $\mathbb{Z}$. Hence, it is contained in the integral closure O_K.

2. Since O is a free $\mathbb{Z}$-module of the same rank as O_K we see that $f = [O_K : O] < \infty$. Now we claim that $O = \mathbb{Z} + fO_K$. Since $fO_K \subset O$ we see that the right-hand side is contained in the left-hand side. On the other hand we have $O_K : \mathbb{Z} + fO_K] = f$ and so we deduce $O = \mathbb{Z} + fO_K$.

3. The independence of the chosen bases is similar as in the first exercise. We choose the basis $(1, f\alpha_D)$ of O, where $\alpha_D = \sqrt{D}$, if $D \equiv 2, 3 \pmod 4$, and $\alpha_D = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \pmod 4$. We get then

$$\mathrm{disc}(O) = \det \begin{pmatrix} \mathrm{tr}(1) & f\,\mathrm{tr}(\alpha_D) \\ f\,\mathrm{tr}(\alpha_D) & f^2\,\mathrm{tr}(\alpha_D) \end{pmatrix} = f^2\,\mathrm{disc}(O_K).$$

4.

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.

Solution. 1. Suppose $\alpha \in K \smallsetminus \{0\}$ satisfies $\alpha^n = 0$ for some $n \in \mathbb{Z}_{\geq 1}$. Then the minimal polynomial of α if of the form T^m for some $1 \leq m \leq n$, which is not separable.

2. Notice that the statement in the Hint follows from the fact that A is finite dimensional as Q vector space. Let $\mathcal{M}$ be the collection of maximal ideals of A and let $\{M_1, \ldots, M_n, \ldots\} \subset \mathcal{M}$. We have the following descending chain of ideals

$$A \supset M_1 \supset M_1 M_2 \supset M_1 \cdots M_n \supset \cdots \supset \{0\}.$$

The sequence stabilizes, that is there is a n so that $M_1 \cdots M_n = M_1 \cdots M_n \cdots M_k$ for every $k > n$. In particular, $M_1 \cap \cdots M_n \subset M_k$. We show by induction on n that one $M_i \subset M_k$ and so $M_k = M_i$. If $n = 1$ is clear. Suppose $n > 1$. Suppose that $M_n \nsubseteq M_k$. Let $b \in M_n \smallsetminus M_k$. Then $bM_1 \cdots M_{n-1} \subset M_k$. Since M_k is maximal and in particular prime, we see that $M_1 \cdots M_{n-1} \subset M_k$ and by the induction hypothesis there exists $1 \leq i \leq n-1$ so that $M_i \subset M_k$. Hence we see that $\{M_1, \ldots, M_n, \cdots\} = \{M_1, \ldots, M_n\}$ is finite and so we deduce $\mathcal{M}$ is finite.

3. By the Chinese remainder theorem we have

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

We just need to show that $J = \bigcap_{M \in \mathcal{M}} M$ is 0. We have

$$A \supset J \supset J^2 \supset \cdots J^n \supset \cdots \{0\}.$$

In particular, there exists an integer n so that $J^n = J^{n+1}$. We claim that $J^n = 0$ and $J = \{0\}$, since A is reduced. Suppose $J^n \neq 0$. Then we define $\mathcal{I} = \{I \subset J^n \text{ ideal } | IJ^n \neq 0\}$. Then $J^n \in \mathcal{I}$ since $J^n \cdot J^n = J^{n-1}J^{n+1} = J^{n-1}J^n = \cdots = J^n \neq 0$. Hence $\mathcal{I}$ has a minimal element,[1] say I. Let $x \in I$ and $a \in J^n$ be so that $xa \neq 0$. Hence $xJ^n \neq 0$ an by minimality $I = (x)$. We claim that $(x) = (xc)$ for some $c \in J^n$. In fact, since $a \in J^n = J^{2n}$ we can write $a = \sum_i c_i d_i$ for $c_i, d_i \in J^n$. Then since $xa \neq 0$ it must be that $xc_i d_i \neq 0$ for at least one of the $c_i d_i$. Hence we can choose $c = c_i$ and we see that $xc \in I$ and $xcJ^n \neq 0$. By minimality we deduce $(x) = (xc)$. Hence, after eventually multiply c by a unit, we have $x = xc$. This implies $x(1-c) = 0$.

We claim that $1 - c$ is a unit. In fact suppose it is not, then $1 - c \in M$ for some maximal ideal M. However $c \in J^n \subset M$ and so $1 \in M$ which is a contradiction. In particular we deduce that $x = 0$ but this is a contradiction.

In particular, we have shown that $J^n = 0$, and so, since A is reduced, that $J = 0$.

[1] Or maximal with respect to reverse inclusion

4. The Q-linear isomorphism above identifies the trace linear forms

$$\mathrm{tr}_{K/Q} = \prod_{M\in\mathcal{M}} \mathrm{tr}_{(K/M)/Q}$$

and we see that, if K/Q is separable, then the bilinear form induced by $\mathrm{tr}_{K/Q}$ is non degenerate. This implies that the bilinear form induced by $\mathrm{tr}_{(K/M)/Q}$ is non degenerate for every $M \in \mathcal{M}$. This implies that K/M is a separable finite extension of Q for every $M \in \mathcal{M}$. The argument is to find in the Appendix, precisely Theorem A.7, of the lecture notes.

5. Let $K_1, \ldots, K_n$ be finite separable field extensions of Q and let $K = \prod_{i=1}^n K_i$. Then K is a finitely generated separable Q-algebra.

   Let $z = (z_1, \ldots, z_n) \in K$. Since K_i/Q is separable the map Q-linear map $[\times z_i]\colon K_i \to K_i$ is diagonalizable. The Q-linear map $[\times z]\colon K \to K$ is then diagonalizable and so z is separable over Q. Hence K/Q is a separable algebra.

Exercise 4 (Quadratic reciprocity law, again and again)**.** We again prove quadratic reciprocity law.[2] 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 $S_q(1;p) \equiv 1 + \left(\frac{q}{p}\right) \pmod q$[3]

   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.

[2] I found the details of this proof in [Yua]

[3] In the exercise Sheet this was misstyped $\left(\frac{p}{q}\right)$ instead of $\left(\frac{q}{p}\right)$

Solution. 1. We have

$$S_q(1;p) = \{(x_1, \dots, x_q) \in \mathbb{F}_p^q \mid x_1^2 + \cdots + x_q^2 = 1\}.$$

Consider the action of $\mathbb{Z}/q$, then the orbits define a partition of $S_q(1;p)$ and we have

$$|S_q(1;p)| = |\{\text{fixed points}\}| + \sum_{\substack{O \\ |O| \geq 2}} |O|,$$

where the sum runs over the orbit with at least two elements. By the orbit stabilizer theorem every orbit with at least two elements has cardinality divisible by q. Hence

$$|S_q(1;p)| \equiv |\{\text{fixed points}\}| \,(\mathrm{mod}\, q).$$

Notice that the set of fixed points is empty if and only if q^{-1} (and hence, if and only if q) is not a square $(\mathrm{mod}\, p)$- Moreover, if it is non empty it has exactly 2 elements. In particular, we see that $|\{\text{fixed points}\}| = 1 + \left(\frac{q}{p}\right)$.

2. Observe that $x_1^2 + \cdots + x_n^2 = a$ if and only if $x_1^2 + \cdots x_{n-2}^2 = a - x_n^2 - x_{n-1}^2$. Hence the desired claim.

3. $S_1(a;p) = \{x \in \mathbb{F}_p \mid x^2 = a\}$ and its cardinality is $|S_1(a;p)| = 1 + \left(\frac{a}{p}\right)$.

4. Consider, as the hint suggests, the finitely generated $\mathbb{F}_p$-algebra $A = \mathbb{F}_p[X]/(X^2+1)$ and the norm map $N_{A/\mathbb{F}_p}$. We compute first the norm. Let $[f] \in A$. By euclidean division we may assume that $f = uX + v$ for some $u, v \in \mathbb{F}_p$. Consider the basis $(1, X)$ of A as $\mathbb{F}_p$- vector space. Then with respect to this basis, we have

$$[\times[f]] = \begin{pmatrix} v & -u \\ u & v \end{pmatrix}$$

and so $N_{A/\mathbb{F}_p}([f]) = u^2 + v^2$.

The norm map $N_{A/\mathbb{F}_p}$ is surjective. The argument is very similar to one in Exercise Sheet 1. The two subsets $\{x^2 \mid x \in \mathbb{F}_p\}$ and $\{a - y^2 \mid y \in \mathbb{F}_p\}$ they have both cardinality $\frac{p+1}{2}$ (using p is odd) and so they must intersect, that is there exist $x, y \in \mathbb{F}_p$ so that $x^2 = a - y^2$

Since $N_{A/\mathbb{F}_p}$ is multiplicative it induces a group homomorphism

$$N_{A/\mathbb{F}_p} \colon A^\times \to \mathbb{F}_p^\times.$$

Suppose so $a \neq 0$. Since $|S_2(a;p)| = |N_{A/\mathbb{F}_p}^{-1}(\{a\})| = |N_{A/\mathbb{F}_p}^{-1}(\{1\})|$ we get just need to compute the size of the kernel of $N_{A/\mathbb{F}_p}$ and since it is surjective we get that

$$|S_2(a;p)| = \frac{|A^\times|}{p-1}.$$

If $p \equiv 1 \,(\mathrm{mod}\, 4)$, then the $A \simeq \mathbb{F}_p^2$ and so $A^\times \sim (\mathbb{F}_p^\times)^2$ and we deduce

$$|S_2(a;p)| = \frac{(p-1)^2}{p-1} = p - 1.$$

If $p \equiv 3 \,(\mathrm{mod}\, 4)$, then $A \simeq \mathbb{F}_{p^2}$ and $A^\times \simeq \mathbb{F}_{p^2}^\times$ and so

$$|S_2(a;p)| = \frac{p^2-1}{p-1} = p + 1.$$

This conclude the case $a \neq 0$.

Supppose now $a = 0$. Then we are looking for $x, y \in \mathbb{F}_p$ so that $x^2 = -y^2$. If $p \equiv 3 \pmod 4$, then -1 is not a square in $\mathbb{F}_p$ and so we have only the trivial solution $x = y = 0$, that is

$$|S_2(0;p)| = 1.$$

If $p \equiv 1 \pmod 4$, then $-1 = \epsilon^2$ is a square and we get the equality $x^2 = (\epsilon y)^2$ implies $x = \pm \epsilon y$ and we have

$$|S_2(0;p)| = 2(p-1) + 1 = 2p - 1.$$

Hence the claim

5. We have

$$\begin{aligned}
|S_n(a;p)| &= \sum_{b \in \mathbb{F}_p} S_{n-2}(a-b;p) \sum_{\substack{x,y \in \mathbb{F}_p \\ x^2+y^2=b}} 1 \\
&= \sum_{b \in \mathbb{F}_p^\times} |S_{n-2}(a-b;p)| \left(p - (-1)^{\frac{p-1}{2}}\right) + |S_{n-2}(a;p)| \left(p + (p-1)(-1)^{\frac{p-1}{2}}\right) \\
&= \sum_{b \in \mathbb{F}_p} |S_{n-2}(a-b;p)| \left(p - (-1)^{\frac{p-1}{2}}\right) + p(-1)^{\frac{p-1}{2}} |S_{n-2}(a;p)| \\
&= \left(p - (-1)^{\frac{p-1}{2}}\right) \sum_{b \in \mathbb{F}_p} |S_{n-2}(b;p)| + p(-1)^{\frac{p-1}{2}} |S_{n-2}(a;p)|.
\end{aligned}$$

Now, we clearly have $\sum_{b \in \mathbb{F}_p} |S_{n-2}(b;p)| = p^{n-2}$ and so the second claim.

6. We have for any $a \in \mathbb{F}_p$

$$\begin{aligned}
|S_n(a;p)| &= p^{n-1} - p^{n-2}(-1)^{\frac{p-1}{2}} + p(-1)^{\frac{p-1}{2}} |S_{n-2}(a;p)| \\
&= p^{n-1} - p^{n-2}(-1)^{\frac{p-1}{2}} + p(-1)^{\frac{p-1}{2}} \left(p^{n-3} - p^{n-4}(-1)^{\frac{p-1}{2}} + p(-1)^{\frac{p-1}{2}} |S_{n-4}(a;p)|\right) \\
&= p^{n-1} - p^{n-3}(-1)^{2\frac{p-1}{2}} + p^2(-1)^{2\frac{p-1}{2}} |S_{n-4}(a;p)|.
\end{aligned}$$

By induction we have then for every $k \leq n/2$ that

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

and so for $n = 2k+1$

$$\begin{aligned}
|S_n(1;p)| &= p^{2k} - p^k(-1)^{k\frac{p-1}{2}} + p^k(-1)^{k\frac{p-1}{2}} |S_1(1;p)| \\
&= p^{2k} + p^k(-1)^{k\frac{p-1}{2}},
\end{aligned}$$

since $\left(\frac{1}{p}\right) = 1$.

7. We have

$$1 + \left(\frac{q}{p}\right) \equiv |S_q(1;p)| \equiv p^{q-1} + p^{\frac{q-1}{2}}(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \pmod q.$$

Since $p^{q-1} \equiv 1 \pmod q$ and $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod q$ we deduce that $\left(\frac{q}{p}\right) \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod q$ and since both are numbers between 1 and -1 the equality is true already in $\mathbb{Z}$.

References

[Yua] Qiaochu Yuan. The p-group fixed point theorem. URL: https://qchu.wordpress.com/2013/07/09/the-p-group-fixed-point-theorem/.