Exercise Sheet 3
Algebraic Number Theory

September 30, 2025

Exercise 1 (Quadratic reciprocity law)**.** With this exercise we give a first (of many) proof[1] of the quadratic reciprocity law. We define the Legendre symbol.

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$$

by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if it exists } b \in (\mathbb{Z}/p\mathbb{Z})^\times : b^2 = a, \\ -1 & \text{otherwise.} \end{cases}$$

The quadratic reciprocity law says that for all *odd prime numbers* p, q it holds that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

First we prove/recall the Euler's criterion:

1. Show the Euler's criterion, valid for every odd prime p and $a \in \mathbb{Z}$ coprime to p:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Now we are ready to prove the theorem:

2. Consider the group $G = ((\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times)/U$, where $U = \{\pm(1,1)\}$. Show that the following two subsets of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ are both a system of representatives for G:

$$S_1 = \{(i \pmod{p}, j \pmod{q}) \mid 1 \le i \le p-1, 1 \le j \le \frac{q-1}{2}\}$$
$$S_2 = \{(k \pmod{p}, k \pmod{q}) \mid 1 \le k \le \frac{pq-1}{2}, (k, pq) = 1\}.$$

3. Taking the product of all elements of G show that

$$\left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) U = \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) U.$$

4. Conclude.

Exercise 2. Let $K/\mathbb{Q}$ be a quadratic extension, i.e., $\dim_{\mathbb{Q}} K = 2$. Denote by O_K the ring of integers of K. For this exercise, you may use the following criterion without proof. Let $z \in K$, then

$$z \in O_K \iff \mathrm{char}_z(X) \in \mathbb{Z}[X]$$

where $\mathrm{char}_z(X) \in \mathbb{Q}[X]$ is the characteristic polynomial of the $\mathbb{Q}$-linear map

$$[\times z] \colon K \to K$$

defined by $[\times z](k) = zk$, $k \in K$.

[1] This proof is due to G. Rosseau

1. Show that $K = \mathbb{Q}(\sqrt{D})$ for some $D \in \mathbb{Z}$ squarefree.[2]
2. For $z = a + b\sqrt{D}$, compute $\mathrm{char}_z(X)$.
3. Show that $O_K = \mathbb{Z}[\sqrt{D}]$ if $d \equiv 2, 3 \mod 4$ and $O_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $d \equiv 1 \mod 4$.

Recall that the group of units is defined by

$$O_K^\times = \{z \in O_K \mid \exists w \in O_K : zw = 1\}$$

4. Let $K = \mathbb{Q}(\sqrt{D})$ for some $D \in \mathbb{Z}$ squarefree, $D < 0$. We call such a field an *imaginary quadratic field*. Find $O_K^\times$ in this case. In particular show that $O_K^\times$ has 2,4 or 6 elements and characterize when each situation occurs.

Exercise 3. The aim of this exercise is to classify which prime ideals are inert, split and ramified in a quadratic extension. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic extension. We know that $O_K = \mathbb{Z}[\alpha]$, for some $\alpha \in O_K$. Let p be a prime.

1. Since O_K is a Dedekind domain we can factorise $(p) = pO_K$ into prime ideals. Show that exactly one of the following holds,
   - The ideal (p) is prime in O_K. In this case we say (p) is *inert*.
   - The ideal (p) splits into two distinct prime ideals in O_K. In this case we say (p) is *totally split*.
   - The ideal (p) is a square of a prime ideal in O_K. In this case we say (p) is *ramified*.
2. Prove that
$$O_K/pO_K \simeq \mathbb{F}_p[X]/\overline{\mu_\alpha}$$
where $\mu_\alpha \in \mathbb{Z}[X]$ is the minimal polynomial of α and $\overline{\mu_\alpha}$ is its reduction $(\mathrm{mod}\, p)$.
3. Use the above statement to first find the inert primes in terms of D.
4. Prove that p is a ramified prime iff O_K/pO_K has nilpotents. Find the ramified and split primes in terms of D.

Exercise 4 (A PID that is not Euclidean)**.** Let $\alpha \coloneqq \frac{1+i\sqrt{19}}{2}$. The goal of this exercise is to prove that $\mathbb{Z}[\alpha]$ is a Principal Ideals Domain (PID), but not en Euclidean domain.

An integral domain A is called Euclidean if there exists a function $f\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ satisfying the following property: for all $a \in A$, $b \in A \setminus \{0\}$, there exist $q, r \in A$ so that $a = qb + r$ and $r = 0$ or $f(r) < f(b)$. If such a f exists, it is called a Euclidean function.

First, we show that $\mathbb{Z}[\alpha]$ is not Euclidean. Aiming to a contradiction, we assume that $\mathbb{Z}[\alpha]$ is Euclidean.

1. Show that $\alpha^2 - \alpha + 5 = 0$
2. Denote by $|\cdot|$ the usual absolute value in $\mathbb{C}$. Show that $|a|^2 \in \mathbb{Z}$ for every $a \in \mathbb{Z}[\alpha]$ and deduce that $\mathbb{Z}[\alpha]^\times = \{z \in \mathbb{Z}[\alpha] \mid \exists w \in \mathbb{Z}[\alpha] : zw = 1\} = \{\pm 1\}$.
3. Let f be a Euclidean function of $\mathbb{Z}[\alpha]$. Let $z_0 \in \mathbb{Z}[\alpha]$ be so that $f(z_0) = \min\{f(z) \mid z \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}[\alpha]^\times\}$. Show that $\mathbb{Z}[\alpha]/(z_0)$ has at most 3 elements.
4. Show that $X^2 - X + 5$ is irreducible in both $\mathbb{F}_2[X]$ and $\mathbb{F}_3[X]$ and deduce the desired contradiction.

Next, we show that $\mathbb{Z}[\alpha]$ is a PID. Consider $\mathbb{Z}[\alpha] \subset \mathbb{C}$ and define

$$U = \{z + a \in \mathbb{C} \mid |z| < 1, a \in \mathbb{Z}[\alpha]\}$$

the union of all open disks of radius 1 with center an element of $\mathbb{Z}[\alpha]$.

[2] Recall we call an integer $n \in \mathbb{Z}$ squarefree if there is no prime p so that $p^2 | n$.

5. Show that if $z \in \mathbb{C} \setminus U$, then $|\mathrm{im}(z) - \frac{n\sqrt{19}}{2}| \geq \frac{\sqrt{3}}{2}$ for all $n \in \mathbb{Z}$.

6. Show that if $z_1, z_2 \in \mathbb{C} \setminus U$, then $z_1 + z_2 \in U$.

We say that a pair $(a, b) \in \mathbb{Z}[\alpha] \times (\mathbb{Z}[\alpha] \setminus \{0\})$ has (DR) property, if there exists $q, r \in \mathbb{Z}[\alpha]$ so that $a = qb + r$ and $|r| < |b|$.

7. Prove the following statements
   - (a, b) has (DR) if and only if $\frac{a}{b} \in U$.
   - If (a, b) does not have (DR), then $(2a, b)$ has (DR).
   - If (a, b) does not have (DR), then $(\alpha a, b)$ or $((1 - \alpha)a, b)$ has (DR).

8. Show that 2 is coprime to α and $1-\alpha$ in $\mathbb{Z}[\alpha]$, that is, there is no irreducible element that divides both 2 and α (resp. 2 and $1 - \alpha$).

9. Conclude that $\mathbb{Z}[\alpha]$ is a PID.

Exercise 5 (A Diophantine equation)**.** In this exercise, we determine the solution $(x, y) \in \mathbb{Z}^2$ to the equation

$$x^2 + 1 = y^3 \tag{1}$$

1. Let A be a PID and $n \geq 2$ and integer. Suppose $u, v \in A$ are coprime elements so that uv is a n'th power in A. Show that, up to multiplication by units, also u and v are n'th powers.

2. Prove that, up to multiplication by units, the only two irreducible elements dividing 2 in $\mathbb{Z}[i]$ are $1 + i$ and $1 - i$

3. Suppose $x \in \mathbb{Z}$ is odd. Show that $x^2 + 1$ can not be a cube.

   Hint: Check it $\pmod 4$

Now suppose $(x, y) \in \mathbb{Z}^2$ is a solution to (1):

4. Show that $x + i, x - i \in \mathbb{Z}[i]$ are coprime.

5. Deduce that there exists $a, b \in \mathbb{Z}$ such that $x + i = (a + ib)^3$.

6. Conclude that the only solution to (1) in $\mathbb{Z}^2$ is $(0, 1)$.