Algebraic Number Theory | Exercise Sheet 1
Manuel Luethi | Spring 2024
Federico Viola

---

1. For what follows, let $f \in \mathbb{Q}[X]$ be an irreducible polynomial. Our goal is to produce a realization of the field $K \cong \mathbb{Q}[X]/(f)$ suitable for computations. We assume that
$$f = X^d + a_{d-1}X^{d-1} + \cdots + a_0$$
for $(a_0, \ldots, a_{d-1}) \in \mathbb{Q}^d$.
   a) Recall that K is a finite-dimensional vector space over $\mathbb{Q}$. Given $a \in K$, we denote by $\times a \colon K \to K$ the map given by
   $$\forall b \in K \quad \times a(b) = ba.$$
   Show that $\iota \colon a \mapsto \times a$ defines a monomorphism $\iota \colon K \longrightarrow \mathrm{End}_{\mathbb{Q}}(K)$ of $\mathbb{Q}$-algebras.
   b) Give an explicit embedding of K in $\mathrm{Mat}_d(\mathbb{Q})$.
   Hint: Show that for any root ζ of f, the companion matrix of f is a matrix representation of $\times\zeta$.
   c) Let $\iota \colon K \longrightarrow \mathrm{Mat}_d(\mathbb{Q})$ be a field embedding and let ζ be a root of f. Show that for all non-zero $v \in \mathbb{Q}^d$ the tuple
   $$\big(v, v\iota(\zeta), \ldots, v\iota(\zeta)^{d-1}\big)$$
   is a basis of $\mathbb{Q}^d$.
   d) Show that any two embeddings $\iota_1, \iota_2 \colon K \longrightarrow \mathrm{Mat}_d(\mathbb{Q})$ are conjugate, i.e., there exists $g \in \mathrm{GL}_d(\mathbb{Q})$ such that
   $$\forall a \in K \quad \iota_2(a) = g\iota_1(a)g^{-1}.$$
   Hint: Use the preceding subexercise.
   e) Using SageMATH, write a function which takes as input irreducible polynomial $f \in \mathbb{Q}[X]$ and returns K as a subfield of $\mathrm{Mat}_d(\mathbb{Q})$ by specifying a $\mathbb{Q}$-basis.
   Remark: This implementation is very precise but not very efficient, as the complexity of multiplication in K is the complexity of multiplication in the much larger ambient $\mathbb{Q}$-algebra $\mathrm{Mat}_d(\mathbb{Q})$. SageMATH offers several implementations of number fields.
2. Let $d \geqslant 2$ be a squarefree integer. Let $K = \mathbb{Q}(\sqrt{d})$ and $A = \mathbb{Z}[\sqrt{d}]$. Given an element $z = a + b\sqrt{d} \in A$, we let $\overline{z} = a - b\sqrt{d}$ and $\mathrm{N}(z) = z\overline{z}$.
   We also define the Pell equation
   $$x^2 - dy^2 = 1.$$
   a) Prove that $\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1)\,\mathrm{N}(z_2)$
   b) Prove that
   $$A^\times = \{x + y\sqrt{d} \in A | x^2 - dy^2 = \pm 1\}$$
   and that the set of solutions of the Pell equation
   $$A_1^\times = \{x + y\sqrt{d} \in A | x^2 - dy^2 = 1\}$$
   forms a subgroup of $A^\times$ of index at most 2.
   c) Show that $\phi : A_1^\times \to (\mathbb{R}, +)$, $a + b\sqrt{d} \mapsto \log|a + b\sqrt{d}|$ is a group homomorphism with kernel ± 1.

d) Show that $\phi(A_1^\times)$ is a cyclic subgroup of $(\mathbb{R}, +)$.
Hint: Prove that for every compact subset $B \subset \mathbb{R}$, $\phi^{-1}(B)$ is finite. Deduce that $\phi(A_1^\times)$ is discrete and thus cyclic.

e) Conclude that if the Pell equation admits a non-trivial solution ($\neq \pm 1$), then all solutions are of the form $\pm z_0^n$ for some $z_0 \in A_1^\times$, where $z_0 \neq \pm 1$ and n runs over $\mathbb{Z}$.

f) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $n \geqslant 1$. Prove that there exists $a \in \mathbb{Z}$ and $b \in \{1, ..., n\}$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{(n+1)b}.$$

Hint: Use the pigeonhole principle with $0, \{\alpha\}, \{2\alpha\}, ..., \{n\alpha\}, 1$ where $\{\alpha\}$ denotes the fractional part of α.

g) Deduce from the previous part that there exist infinitely many pairs (a, b) with $\gcd(a, b) = 1$ and

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

h) Using the pigeonhole principle once again, show that there exists $n \in \mathbb{Z}$ satisfying $1 \leqslant |n| \leqslant 2\sqrt{d} + 1$ and such that $x^2 - dy^2 = n$ has infinitely many solutions (x, y) with x, y positive. Conclude that there exist two distinct solutions $(x_1, y_1), (x_2, y_2)$ with $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$.

i) Set $z_1 = x_1 + y_1\sqrt{d}$, $z_2 = x_2 + y_2\sqrt{d}$ and $z_0 = z_1/z_2$. Prove that z_0 is a non-trivial solution of the Pell equation.

3. Let $f = X^2 + BX + C \in \mathbb{Z}[X]$ irreducible and assume that $B^2 - 4C < 0$. Let ζ be a root of f and consider the ring $\mathbb{Z}[\zeta] \subset \mathbb{C}$.

a) Show that

$$\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta.$$

Deduce that $\mathbb{Z}[\zeta]$ is a *lattice* in $\mathbb{C}$, i.e., $\mathbb{Z}[\zeta] \subset \mathbb{C}$ is a discrete subgroup containing an $\mathbb{R}$-basis of $\mathbb{C}$.

b) Let $\vartheta : \mathbb{Z}[\zeta] \to \mathbb{Z}^2$ denote the $\mathbb{Z}$-module isomorphism $\vartheta(a + b\zeta) = (a, b)$ and define $\iota : \mathbb{Z}[\zeta] \to \mathrm{Mat}_2(\mathbb{Z})$ by

$$\forall s, x \in \mathbb{Z}[\zeta] \quad \vartheta(xs) = \vartheta(x)\iota(s).$$

Show that ι is well-defined and an injective homomorphism of rings.

c) Given $s \in \mathbb{Z}[\zeta]$, let $(s) \lhd \mathbb{Z}[\zeta]$ be the ideal generated by s. Let $M_s = \mathbb{Z}^2\iota(s)$. Show that as $\mathbb{Z}$-modules

$$\mathbb{Z}[\zeta]/(s) \cong \mathbb{Z}^2/M_s.$$