Algebraic Number Theory
Manuel Luethi
Federico Viola

Exercise Sheet 4
Spring 2024

---

1. 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 and let $\mathcal{O}_K$ be the maximal order in K and let $p \in \mathbb{Z} - \{0\}$ prime. You can assume throughout that every ideal in $\mathcal{O}_K$ admits a unique factorization into prime ideals. Moreover, letting $\mathrm{Nr}(I) = [\mathcal{O}_K \colon I]$ for any ideal $\{0\} \neq I \lhd \mathcal{O}_K$, we have that $\mathrm{Nr}(I.J) = \mathrm{Nr}(I)\mathrm{Nr}(J)$.
   a) Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$. Deduce that the minimal polynomial $\mu_\alpha(X)$ of α is a monic polynomial in $\mathbb{Z}[X]$.
   b) Prove that
   $$\mathcal{O}_K / p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(\mu_\alpha(X))$$
   .
   c) Show that one of the following is true:
      (i) The ideal (p) is prime in $\mathcal{O}_K$. (In this case we say (p) is *inert*.)
      (ii) The ideal (p) splits into two distinct prime ideals in $\mathcal{O}_K$. (In this case we say (p) is *totally split*.)
      (iii) The ideal (p) is a square of a prime ideal in $\mathcal{O}_K$. (In this case we say (p) is *ramified*.)
   d) Use the above statement to first find the inert primes in terms of D.
   e) Prove that p is a ramified prime if and only if $\mathcal{O}_K/p\mathcal{O}_K$ has nilpotents. Find the ramified and split primes in terms of $\Delta(\mathcal{O}_K)$.
2. Let K be a number field and let $f \colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ denote the geometric embedding of K.
   a) Show that for any two lattices $M, N \subseteq K$, the product
   $$M.N = \left\{ \sum_{i=1}^{r} m_i n_i \colon r \in \mathbb{N} \cup \{0\}, m_i \in M, n_i \in N \right\}$$
   is a lattice in K.
   b) Given a lattice $\Lambda \subseteq K$ and a $\mathbb{Z}$-basis $\mathcal{B} = (\omega_1, \ldots, \omega_d)$ of Λ, we defined the discriminant of $\mathcal{B}$ by
   $$\Delta(\mathcal{B}) = \big(\det(\sigma_i \omega_j)\big)^2$$
   Show that $\Delta(\mathcal{B})$ only depends on Λ, i.e., is independent of the choice of $\mathcal{B}$ and the choice of the type $(\sigma_1, \ldots, \sigma_{r_1+r_2})$.
   c) Show that
   $$\Delta(\mathcal{B}) = (-4)^{r_2} \mathrm{covol}\big(f(\Lambda)\big)^2.$$
   d) Let $P(X) = X^2 + bX + c \in \mathbb{Q}[X]$ irreducible and let $\alpha \in \mathbb{C}$ be a solution to P, i.e., $P(\alpha) = 0$. Show that $(1, \alpha)$ is a basis of $\mathbb{Q}(\alpha)$ and
   $$\Delta(1, \alpha) = b^2 - 4c.$$
3. Given a lattice $L \leqslant K$, define
   $$\mathcal{O}_L := \{x \in K \colon xL \subseteq L\}.$$
   Show that $\mathcal{O}_L$ is an order.

4. Using `SageMATH`, write a function that takes as input a non-square $D \in \mathbb{Z}$ and a natural number N and returns the proportion of primes up to N which are ramified, inert, and split in $K = \mathbb{Q}(\sqrt{D})$ respectively.

   Make a conjecture about the asymptotic proportions as $N \to \infty$.

   Hint: Choose $N > |\Delta(1, \alpha)|^2$ for large $|\Delta(1, \alpha)|$, where $\alpha \in K$ is chosen such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Note that $\Delta(1, \alpha)$ is the *discriminant* of the maximal order in K, which is called the discriminant of K. In `SageMATH`, the discriminant of the number field K can be obtained by invoking `K.discriminant()`. For example, in case of the Gaussian integers ($D = -1$), running

```
K.<i> = NumberField(x^2 + 1)
Delta = K.discriminant()
```

   will assign the value $-4 = \Delta(1, \mathrm{i})$ to Δ. Other commands you might find useful are

```
# construct the maximal order in the number field K
O = K.ring_of_integers()
# construct the ideal (n) in O
I = O.ideal(n)
# return the prime factorization of I in O
I.factor()
```