Algebraic Number Theory
Manuel Luethi
Federico Viola

Exercise Sheet 4 (Solutions)
Spring 2024

---

1. a) Recall that $\mathcal{O}_K$ is the maximal order in K. In particular, it is a lattice in K. Suppose that $\frac{1}{n} \in \mathcal{O}_K$, where $n \in \mathbb{Z} - \{0\}$. Then $\frac{1}{n} \in \mathcal{O}_K$ and, thus, $\frac{1}{n}\mathcal{O}_K \subseteq \mathcal{O}_K$. In particular, letting $x \in \mathcal{O}_K$ be a primitive vector in the lattice $\mathcal{O}_K$, we find that $\frac{x}{n} \in \mathcal{O}_K$, i.e., $n \in \{\pm 1\}$. In particular, 1 is primitive in $\mathcal{O}_K$. Therefore, $\mathcal{O}_K$ admits a $\mathbb{Z}$-basis of the form $(1, \alpha)$ for some $\alpha \in \mathcal{O}_K$. Since $\alpha^k \in \mathcal{O}_K$ for all $k \in \mathbb{N}$, it follows that $\mathcal{O}_K \subseteq \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ as desired.

   b) Similar to exercise 1c in Exercise Sheet 3. Consider the composition

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X] \twoheadrightarrow \mathbb{F}_p[X]/(\mu_\alpha(X)),$$

   where the first map is the reduction of the coefficients modulo p and the second is the quotient map. The kernel of this map is $(p, \mu_\alpha(X))$, so have

$$\mathbb{Z}[X]/(p, \mu_\alpha(X)) \cong \mathbb{F}_p[X]/(\mu_\alpha(X)).$$

   On the other hand, we have another surjective morphism

$$\mathbb{Z}[X] \overset{\mathrm{ev}_\alpha}{\twoheadrightarrow} \mathbb{Z}[\alpha] \twoheadrightarrow \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha],$$

   where the first map is given by the evaluation of a polynomial at α. The kernel of the evaluation is $(\mu_\alpha(X))$: it is clear that $(\mu_\alpha(X)) \subset \ker \mathrm{ev}_\alpha$ and, on the other hand, if $P(\alpha) = 0$ then $\mu_\alpha(X) | P$ in $\mathbb{Q}[X]$ and by Gauss's Lemma $\mu_\alpha(X) | P$ in $\mathbb{Z}[X]$. Therefore the kernel of the composition is $(p, X^2 + X + 1)$ and this gives the desired isomorphism.

   c) Let

$$(p) = \pi_1^{\alpha_1} \pi_2^{\alpha_2} \cdots \pi_k^{\alpha_k}$$

   be the factorization of (p) as product of prime ideals. Since the norm of the ideal (p) is p^2, we get

$$p^2 = \mathrm{Nr}(\pi_1)^{\alpha_1} \mathrm{Nr}(\pi_2)^{\alpha_2} \cdots \mathrm{Nr}(\pi_k)^{\alpha_k}$$

   and therefore $\sum_{i=1}^k \alpha_i \leqslant 2$. We have three cases: either $(p) = \pi_1$ is prime with $\mathrm{Nr}(\pi_1) = p^2$ (inert case), or $(p) = \pi_1 \pi_2$ with π_1, π_2 distinct prime ideals of norm p (totally split case), or $(p) = \pi_1^2$ with π_1 prime ideal of norm p (ramified case).

   d) By definition p is inert if and only if the ideal (p) is prime, which is true if and only if $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(\mu_\alpha(X))$ is a domain. This is true if and only if the polynomial $\mu_\alpha(X)$ is irreducible in $\mathbb{F}_p[X]$, so if and only if the discriminant is not a square modulo p.

   e) If $(p) = \pi_1^2$ then for all $x \in \pi_1$ we have $p | x^2$ in $\mathcal{O}_K$. The projection of x in $\mathcal{O}_K/p\mathcal{O}_K$ is nilpotent, since its square is zero in $\mathcal{O}_K/p\mathcal{O}_K$. Conversely, if $z \in \mathcal{O}_K/p\mathcal{O}_K$ is nilpotent and x is a preimage of z in $\mathcal{O}_K$, we have $(x, p)^n \subseteq (p)$ for some $n \in \mathbb{N}$. It holds $(1) \subset (x, p) \subset (p)$ with strict inclusions. Therefore (p) cannot be prime. If $(p) = \pi_1 \pi_2$ is totally split it must be either $(x, p) = \pi_1$ or $(x, p) = \pi_2$, but (p) does not contain π_1^n or π_2^n for any n. Therefore p must be ramified.

   Now recall that $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(\mu_\alpha(X))$ and assume that p is not inert, so $\mu_\alpha(X)$ is not irreducible in $\mathbb{F}_p[X]$. Since its degree is two it must be $\mu_\alpha(X) = (X - a_1)(X - a_2)$ for some $a_1, a_2 \in \mathbb{F}_p$. If $a_1 = a_2$ then $X - a_1$ is nilpotent

in $\mathbb{F}_p[X]/(\mu_\alpha(X))$, while if $a_1 \neq a_2$ there are no nilpotents in $\mathbb{F}_p[X]/(\mu_\alpha(X))$. Therefore p is ramified if and only if $\mu_\alpha(X)$ has two coincident roots in $\mathbb{F}_p$, so if and only if the discriminant is zero modulo p.

2. a) Let S be a finite set of generators of M and T a finite set of generators of N (over $\mathbb{Z}$). These exist since M and N are assumed to be lattices. Then $\{st\colon s \in S, t \in T\}$ is a set of generators of $M.N$, i.e., $M.N$ is a finitely generated subgroup of K. Therefore it suffices to show that $M.N$ contains a basis of K. Since N is a lattice, N contains a $\mathbb{Q}$-basis $\mathcal{B} = (n_1, \dots, n_{[K\colon \mathbb{Q}]}) \in K^{[K\colon \mathbb{Q}]}$ of K. Let $m \in M \smallsetminus 0$, which exists since M spans K over $\mathbb{Q}$. Then $(mn_1, \dots, mn_{[K\colon \mathbb{Q}]}) \in (M.N)^{[K\colon \mathbb{Q}]}$ is a $\mathbb{Q}$-basis of K and, hence, $M.N$ is a lattice.

   b) Since $\sigma_{r_1+i} = \overline{\sigma}_{r_1+r_2+i}$ for $1 \leqslant i \leqslant r_2$, the choice of a different type only changes the order of the elements in the d-tuple $(\sigma_1, \dots, \sigma_{r_1+2r_2})$. Therefore it only changes the order of the rows in the matrix $(\sigma_i\omega_j)$, multiplying its determinant by ± 1. Given another basis $\mathcal{B}$, every element in $\mathcal{B}$ is a $\mathbb{Z}$-linear combination of the elements in $(\omega_1, \dots, \omega_d)$ and vice versa. In particular, a change of basis corresponds to multiplying the vector $(\omega_1, \dots, \omega_d)$ by a matrix $g \in \mathrm{GL}_n(\mathbb{Z})$. Since g has determinant ± 1, therefore $\det(\sigma_i\omega_j)$ is again multiplied by ± 1. The claim follows.

   c) For $1 \leqslant i \leqslant r_2$ and for $1 \leq j \leqslant d$, set $\sigma_{r_1+i}\omega_j = x_{i,j} + iy_{i,j}$. We have

$$(\sigma_{r_1+i}\omega_j, \sigma_{r_1+r_2+i}\omega_j) = (x_{i,j}, y_{i,j}) \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

   Setting $f_{i,j} = \sigma_i\omega_j$ for $1 \leqslant i \leqslant r_1$, $f_{i,j} = x_{i,j}$ for $r_1 + 1 \leqslant i \leqslant r_1 + r_2$, and $f_{i,j} = y_{i,j}$ for $r_1 + r_2 + 1 \leqslant i \leqslant r_1 + 2r_2$, we have

$$\Delta(\mathcal{B}) = (\det(\sigma_i\omega_j))^2 = \left(\det(f_{i,j}) \det \begin{pmatrix} 1 & -1 \\ i & -i \end{pmatrix}^{r_2}\right)^2 = (-4)^{r_2}\mathrm{covol}(f(\Lambda))^2.$$

   d) Since $P(X)$ is irreducible 1 and α are linearly independent, and since the extension is quadratic they span all of $\mathbb{Q}(\alpha)$.
   Using the definition for $\Delta(\mathcal{B})$ with $\mathcal{B} = (1, \alpha)$ we get:

$$\Delta(1, \alpha) = \det \begin{pmatrix} 1 & \alpha \\ 1 & \alpha' \end{pmatrix}^2$$

   where α' is the other root of $P(X)$. Therefore

$$\Delta(1, \alpha) = (\alpha' - \alpha)^2 = \left(\sqrt{b^2 - 4c}\right)^2 = b^2 - 4c.$$

3. We leave to you the formal check that $\mathcal{O}_L$ is a subring of K and only mention that one needs to show $1 \in \mathcal{O}_L$ and for $x, y \in \mathcal{O}_L$ we have that $x + y, x.y \in \mathcal{O}_L$. As L and the maximal order $\mathcal{O}_K$ are lattices, there is a natural number $M \in \mathbb{N}$ such that $ML \subseteq \mathcal{O}_K$. Note that $\mathcal{O}_L = \mathcal{O}_{ML}$. Hence, from now on, we will assume without loss of generality that L is contained in $\mathcal{O}_K$. We let $D = [\mathcal{O}_K\colon L]$ and note that $D\mathcal{O}_K \subseteq L$.

   It follows that, for every $a \in \mathcal{O}_L$ we have $Da\mathcal{O}_K \subseteq \mathcal{O}_K$. In particular, $D\mathcal{O}_L \subseteq \mathcal{O}_K$ since $1 \in \mathcal{O}_K$. In particular, $D\mathcal{O}_L$ is a subgroup of the finitely generated $\mathbb{Z}$-module $\mathcal{O}_K$ and, hence, finitely generated.

   It remains to show that $\mathcal{O}_L$ contains a $\mathbb{Q}$-basis of K. Let $(\lambda_1, \dots, \lambda_n)$ be a $\mathbb{Z}$-basis of L and let $(\omega_1, \dots, \omega_n)$ be a $\mathbb{Z}$-basis of $\mathbb{O}_K$. For every pair $1 \leqslant i, j \leqslant n$

there is $s_{ij} \in \mathbb{N}$ such that

$$s_{ij}\omega_i\lambda_j \in \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_n = L.$$

This is obtained by expressing $\omega_i\lambda_j$ as a $\mathbb{Q}$-linear combination of the λ_i and clearing denominators. Let $s = \prod_{i,j} s_{ij}$, then $s\mathcal{O}_K \subseteq \mathcal{O}_L$ and, since $s\mathcal{O}_K$ contains a $\mathbb{Q}$-basis of K, the claim follows.