COMPUTING RESIDUE CLASS RINGS AND PICARD GROUPS OF ORDERS

JÜRGEN KLÜNERS AND SEBASTIAN PAULI

ABSTRACT. Let K be a a global field and $\mathcal{O}$ be an order of K. We develop algorithms for the computation of the unit group of residue class rings for ideals in $\mathcal{O}$. As an application we show how to compute the unit group and the Picard group of $\mathcal{O}$ provided that we are able to compute the unit group and class group of the maximal order $\widetilde{\mathcal{O}}$ of K.

1. INTRODUCTION

Let $\mathcal{O}$ be an order of a global field and $\mathfrak{a}$ be an ideal of $\mathcal{O}$. We develop algorithms to determine the multiplicative structure $(\mathcal{O}/\mathfrak{a})^*$ of the residue class ring $\mathcal{O}/\mathfrak{a}$. As applications we give algorithms to compute the unit group $\mathcal{O}^*$ and the Picard group $\mathrm{Pic}(\mathcal{O})$ which is the group of invertible fractional ideals of $\mathcal{O}$ modulo its subgroup of principal fractional ideals. For the case where $\mathcal{O}$ is a maximal order there are algorithms for the computation of $(\mathcal{O}/\mathfrak{a})^*$ (see [Coh00, section 4.2] for number fields and [HPP02] for number fields and function fields). If $\mathcal{O}$ is a maximal order (and therefore a Dedekind domain) the Picard group coincides with the ordinary ideal class group in the number field case and an S-class group in the function field case. For maximal orders there are well known algorithms for the computation of the unit group and the class group.

In general the order $\mathcal{O}$ is not a Dedekind domain. Since not all ideals of $\mathcal{O}$ are a product of prime ideals the ideal arithmetic is more difficult than in a Dedekind domain. Furthermore the localization of $\mathcal{O}$ at a non-regular prime ideal is not a principal ideal domain. We show how these difficulties can be overcome.

In the computer algebra systems KASH [Po$^+$00] and Magma [Ca$^+$03] there are functions for computing the unit group of non-maximal orders of number fields. Examples show that our approach is much more efficient especially when the index of the order in its maximal order is large. Furthermore there is an implementation of an algorithm for determining Picard groups of orders of quadratic number fields in Magma. To our best knowledge there were no algorithms known for field extension of higher degrees or for the function field case.

In the following we present an overview over the main ideas and the structure of this paper. Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals of $\mathcal{O}$ containing $\mathfrak{a}$. Using standard results from primary decomposition we get:

$$(\mathcal{O}/\mathfrak{a})^* \cong (\mathcal{O}_{\mathfrak{p}_1}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_1})^* \times \ldots \times (\mathcal{O}_{\mathfrak{p}_r}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_r})^*,$$

1991 *Mathematics Subject Classification.* Primary 11R65; 11Y40.

where $\mathcal{O}_{\mathfrak{p}_i}$ denotes the localization of $\mathcal{O}$ at $\mathfrak{p}_i$. Thus it is sufficient to compute the groups $(\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_i})^*$ $(1 \le i \le r)$. We prove in section 4 for $\mathfrak{p}^m \subseteq \mathfrak{a} \subseteq \mathcal{O}$:

$$(\mathcal{O}_{\mathfrak{p}}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}})^* \cong \big(\mathcal{O}/(\mathfrak{a}+\mathfrak{p}^m)\big)^* \cong (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{a}+\mathfrak{p}^m), \tag{1}$$

where $\mathfrak{p} \supseteq \mathfrak{a}$ is a prime ideal of $\mathcal{O}$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}$. In section 3 we show how to find all prime ideals in $\mathcal{O}$ which contain a given ideal $\mathfrak{a}$. Furthermore we give algorithms for the computation of the residue class field $\mathcal{O}/\mathfrak{p}$ including the canonical epimorphism $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$. In section 4 we develop a first method for the computation of the multiplicative group of residue class rings in arbitrary orders. It is based on the isomorphism (1) and the canonical isomorphism $\psi : (1+\mathfrak{a})/(1+\mathfrak{b}) \to \mathfrak{a}/\mathfrak{b}$ which holds for ideals satisfying $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a}^2$. In section 5 we recall some properties of Picard groups. Most important for our purposes is the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \widetilde{\mathcal{O}}^* \longrightarrow \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\widetilde{\mathcal{O}}) \longrightarrow 1,$$

where $\widetilde{\mathcal{O}}$ is the integral closure of $\mathcal{O}$ in its field of fractions, the direct sum runs through all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, and $\mathcal{O}_{\mathfrak{p}}$ (respectively $\widetilde{\mathcal{O}}_{\mathfrak{p}}$) denotes the localization of $\mathcal{O}$ at $\mathfrak{p}$ (respectively $\widetilde{\mathcal{O}}$ at $\mathfrak{p}\widetilde{\mathcal{O}}$). We assume that $\widetilde{\mathcal{O}}^*$ and $\mathrm{Pic}(\widetilde{\mathcal{O}})$ are already computed. We show in proposition 6.2 that

$$\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \cong \bigoplus_{\mathfrak{p}} (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathcal{F}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathcal{F}\mathcal{O}_{\mathfrak{p}})^*,$$

where $\mathcal{F}$ is the conductor of $\mathcal{O}$, i.e. the largest subset of $\mathcal{O}$ which is an ideal of $\mathcal{O}$ as well as $\widetilde{\mathcal{O}}$. This reduces the computation of $\mathcal{O}^*$ and $\mathrm{Pic}(\mathcal{O})$ to residue class ring computations. If all maps of the above sequence are known we obtain $\mathcal{O}^*$ and $\mathrm{Pic}(\mathcal{O})$ using methods for computations with finitely generated abelian groups. The computation of the conductor $\mathcal{F}$ is described in section 6. In section 7 we define a canonical homomorphism $(\mathcal{O}/\mathfrak{a})^* \to (\widetilde{\mathcal{O}}/\mathfrak{a}\widetilde{\mathcal{O}})^*$ and show in which cases this homomorphism is injective. Using this information we give a second algorithm to compute $(\mathcal{O}/\mathfrak{a})^*$ which is especially useful for the case when $\mathfrak{a}$ is the conductor of $\mathcal{O}$. In section 8 we explicitly describe how the unit group $\mathcal{O}^*$ and the Picard group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$ can be computed. This is followed by some examples in section 9.

2. Notations

In this section we introduce some notations which we use throughout this paper. Let $\widetilde{\mathcal{O}}$ be a Dedekind ring and let $\mathfrak{p}$ be a prime ideal of $\widetilde{\mathcal{O}}$. For $a \in \widetilde{\mathcal{O}}$ we denote by $v_{\mathfrak{p}}(a)$ the $\mathfrak{p}$-adic exponential valuation of a.

Abelian groups. An additive abelian group G is presented by a column vector $g \in G^m$, whose entries form a system of generators for G, and by a matrix of relations $M \in \mathbb{Z}^{n\times m}$ of rank m, such that $v^{\mathrm{tr}}g = 0$ for $v \in \mathbb{Z}^m$ if and only if v^{tr} is an integral linear combination of the rows of M. We note that for every $a \in G$ there is a $v \in \mathbb{Z}^m$ satisfying $a = v^{\mathrm{tr}}g$. If $g_1, \ldots, g_m$ is a basis of G, M will usually be a diagonal matrix. Algorithms for calculations with finite abelian groups can be found in [Coh00, section 4.1] and [Sim94] for example. If G is a multiplicative abelian group, then $v^{\mathrm{tr}}g$ is an abbreviation for $g_1^{v_1} \cdots g_m^{v_m}$. If G is a quotient group (*i.e.* $G = H/S$ for some subgroup S of a group H) we often represent the generators of G by elements of H.

Orders. Let $R = \mathbb{Z}$ or $R = \mathbb{F}_q[t]$ and Q be its field of fractions. Let K/Q be a finite algebraic extension of degree n. A free R-module $\mathcal{O} \subseteq K$ of rank n, which is a ring, is called an R-order of K.

Example 2.1. Let K be an algebraic number field of degree n. A $\mathbb{Z}$-order $\mathcal{O}$ of K is a ring which is a free $\mathbb{Z}$-module of rank n. Therefore we get $\mathcal{O} = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, where $\omega_1, \ldots, \omega_n \in K$ are integral over $\mathbb{Z}$ and form a basis of the $\mathbb{Q}$-vector space K.

An order is said to be the maximal R-order of K if it is maximal among the R-orders of K. We denote the maximal R-order of K by $\widetilde{\mathcal{O}}$. Note that $\widetilde{\mathcal{O}}$ is a Dedekind domain and therefore integrally closed.

Example 2.2. Let $R = \mathbb{F}_q[t]$ be the ring of polynomials over the finite field with q elements. Let $f \in \mathbb{F}_q[t][x]$ be monic and irreducible. The $\mathbb{F}_q[t]$-order $\mathcal{O} := \mathbb{F}_q[t][x]/(f)$ is called the equation order of f. Let K be the field of fractions of $\mathcal{O}$. The integral closure

$$\widetilde{\mathcal{O}} := \{\alpha \in K \mid \text{ there exists a monic } h \in \mathbb{F}_q[t][x] \text{ with } h(\alpha) = 0\}$$

is the maximal $\mathbb{F}_q[t]$-order of K. It is also called the finite maximal order of K.

For an ideal $\mathfrak{a}$ of $\mathcal{O}$ we denote by $[\mathcal{O} : \mathfrak{a}]$ the index of the additive groups.

3. Prime Ideals and Residue Class Fields

Prime Ideals. In this section we describe how to compute the prime ideals $\mathfrak{p}$ containing a given ideal $\mathfrak{a} \subseteq \mathcal{O}$ for an arbitrary order $\mathcal{O}$.

If $\mathcal{O}$ is a Dedekind domain this task can be solved using well known factorization algorithms.

If $\mathcal{O}$ is an equation order we can use the following proposition for the computation of the generators of the prime ideals over a prime element in R (see [PZ89, section 6.2]).

Proposition 3.1. *Let $f \in R[x]$ be monic and irreducible. Let $\mathcal{O} = R[\alpha] = R[x]/(f(x))$. Let q be a prime element of R. Denote the irreducible factors of f over the residue class field $R/(q)$ by $\overline{f}_1, \ldots, \overline{f}_g$. Then the prime ideals of $\mathcal{O}$ that contain q are $\mathfrak{p}_i = q\mathcal{O} + f_i(\alpha)\mathcal{O}$.*

In general it is not that easy to describe the prime ideals in an R-order $\mathcal{O}$. We use the factorization of ideals in the maximal order $\widetilde{\mathcal{O}}$ of $\mathcal{O}$ to obtain them. If $\mathfrak{q}$ is a prime ideal of the maximal order $\widetilde{\mathcal{O}}$ then $\mathfrak{q} \cap \mathcal{O}$ is a prime ideal of $\mathcal{O}$. Thus we can find all prime ideals in $\mathcal{O}$ as intersections of prime ideals in $\widetilde{\mathcal{O}}$ with $\mathcal{O}$. If the basis of an ideal in $\widetilde{\mathcal{O}}$ as an R-module is known, we compute a basis of its intersection with $\mathcal{O}$ as follows:

Let M, M_1, M_2 be R-modules of rank n, where M_1, M_2 are submodules of M. Let B_i be the column vectors consisting of the basis elements of M_i $(i = 1\,, 2)$. Let $C \in R^{2n \times 2n}$ be a matrix of maximal rank such that $C\binom{B_1}{B_2} = 0$. Denote the matrix consisting of the first n columns of the upper row Hermite Normal Form of C by C'. Then $C'B_1$ is a basis of $M_1 \cap M_2$.

The next question is how to compute all prime ideals of $\mathcal{O}$ which contain a given ideal $\mathfrak{a}$. In case we have computed the maximal order $\widetilde{\mathcal{O}}$ we simply compute the intersection of $\mathcal{O}$ with all prime ideals which occur in the factorization of $\mathfrak{a}\widetilde{\mathcal{O}}$. If we

have another algorithm to compute prime ideals (e.g. in equation orders) we factor the norm $\mathrm{N}(\mathfrak{a})$ of $\mathfrak{a}$. A prime ideal $\mathfrak{p}$ with $\mathfrak{p} \supseteq \mathfrak{a}$ has the property that $\mathrm{N}(\mathfrak{p}) \mid \mathrm{N}(\mathfrak{a})$. Now we test the finitely many prime ideals lying over prime divisors of $\mathrm{N}(\mathfrak{a})$.

Residue Class Fields. For a prime ideal $\mathfrak{p}$ of an order $\mathcal{O}$ we describe the computation of the residue class field $\mathcal{O}/\mathfrak{p}$. If $\mathcal{O}$ is an equation order, *i.e.*, there exists $f \in R[x]$ such that $\mathcal{O} \cong R[x]/(f)$, the description of the residue class fields follows directly from proposition 3.1. Namely, if P is a prime ideal of R and $f \equiv f_1^{e_1} \cdots f_s^{e_s} \bmod P$ with f_i $(1 \le i \le s)$ irreducible over R/P then the residue class fields of the ideals of $\mathcal{O}$ over P are $(R/P)[x]/(\overline{f_i})$. The corresponding epimorphism $\mathcal{O} \to (R/P)[x]/(\overline{f_i})$ is given via $\alpha \mapsto \bar{\alpha}_i$, where $f(\alpha) = 0$ and $f_i(\bar{\alpha}_i) = 0$.

If $\mathcal{O}$ is not an equation order the algorithm is more complicated. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Let $P = R \cap \mathfrak{p}$ and $\omega = (\omega_1, \ldots, \omega_n)^{\mathrm{tr}}$ be an R-basis of $\mathcal{O}$. Let $M \in R^{n \times n}$ be a matrix such that $(\tau_1, \ldots, \tau_n)^{\mathrm{tr}} = M\omega$ is a basis of the R-module $\mathfrak{p}$. The quotient ring $\mathcal{O}/\mathfrak{p}$ can be described by the generators $\omega_1, \ldots, \omega_n$ and the relation matrix M. We assume that $M = (m_{i,j})_{1 \le i \le n, 1 \le j \le n}$ is given in Hermite normal form (which can always be obtained). We denote by $[a]$ the class of a modulo $\mathfrak{p}$. Then the coefficients a_i of an element $[a] = \sum_{i=1}^{n} a_i[\omega_i] \in \mathcal{O}/\mathfrak{p}$ can be bounded by the diagonal entries $m_{i,i}$ of the matrix M $(1 \le i \le n)$, either in absolute value if $\mathcal{O}$ is a $\mathbb{Z}$-order or in degree if $\mathcal{O}$ is an $\mathbb{F}_q[t]$-order. Unfortunately, we have to distinguish between the number field and the function field case. The following two examples describe how to get representatives for the residue class fields in these cases.

Example 3.2. Let $R = \mathbb{Z}$ and $p \in \mathfrak{p} \cap \mathbb{P}$. In this case the determinant of M is the number of elements of $\mathcal{O}/\mathfrak{p}$. The diagonal of M consists of 1's and p's since $p\omega_i \in \mathfrak{p}$ for $1 \le i \le n$. Let $I := \{i \mid a_{i,i} = p\}$. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Then canonical representatives for $\mathcal{O}/\mathfrak{p}$ are given by $\sum_{i \in I} c_i\omega_i$, where $c_i \in \{0, \ldots, p-1\}$.

Example 3.3. Let $R = \mathbb{F}_q[t]$ and b be a generator of degree k of the principal ideal $P := \mathfrak{p} \cap \mathbb{F}_q[t]$. The diagonal entries of $M = (m_{i,j})$ consist of polynomials with degree bounded by $k-1$. Let $d_j := \max_{1 \le i \le n}\{\deg(m_{i,j})\} \le k-1$. For $1 \le j \le n$ let

$$w_j : \mathbb{F}_q[t]_{\le d_j} \to \mathbb{F}_q^{d_j+1}, a_{d_j}t^{d_j} + \cdots + a_1 t + a_0 \mapsto (a_{d_j}, \ldots, a_1, a_0),$$

where $\mathbb{F}_q[t]_{\le d_j} = \{f' \in \mathbb{F}_q[t] \mid \deg(f) \le d_j\}$. Then

$$N := \begin{pmatrix} w_1(m_{1,1}) & \ldots & w_n(m_{1,n}) \\ \vdots & \ddots & \vdots \\ w_1(m_{n,1}) & \ldots & w_n(m_{n,n}) \end{pmatrix}$$

is an $\mathbb{F}_q$-relation matrix for the generators

$$(\omega_1, \omega_1 \cdot t, \ldots, \omega_1 \cdot t^{d_1}, \ldots, \omega_n, \ldots, \omega_n \cdot t^{d_n})$$

of the quotient ring $\mathcal{O}/\mathfrak{p}$.

Now we know representatives for the residue class field. Using a probabilistic approach one quickly finds a primitive element β for $(\mathcal{O}/\mathfrak{p})/(R/P)$:

Lemma 3.4. *Let F be an extension of $\mathbb{F}_q$ of degree m. Let $\beta \in F$. The probability that $F = \mathbb{F}_q(\beta)$ is at least $1/2$.*

Proof. The number of elements of $\mathbb{F}_{q^m}$ generating a proper subfield of $\mathbb{F}_{q^m}$ is at most

$$\sum_{\substack{l \text{ prime} \\ l<m,\, l|m}} q^{m/l} \leq (\log_2 m) q^{m/2}.$$

Therefore the probability that a randomly chosen element of $\mathbb{F}_{q^m}$ belongs to a proper subfield of $\mathbb{F}_{q^m}$ is at most

$$\frac{(\log_2 m) q^{m/2}}{q^m} = \frac{\log_2 m}{q^{m/2}} \leq \frac{\log_2 m}{2^{m/2}} \leq \frac{m}{2m} = \frac{1}{2} \quad \text{for } m \geq 8.$$

The result is verified easily for $1 < m < 8$. □

Let χ_β be the minimal polynomial of β over R/P. Now $\mathcal{O}/\mathfrak{p} = (R/P)[x]/(\chi_\beta)$. The epimorphism $\mathcal{O} \to (R/P)[x]/(\chi_\beta)$ can be constructed using linear algebra.

4. Residue Class Rings I

For an ideal $\mathfrak{b}$ of a maximal order $\widetilde{\mathcal{O}}$ of K the structure of the multiplicative group $(\widetilde{\mathcal{O}}/\mathfrak{b})^*$ is well known. Generators for it are given explicitly by Hasse [Has80, chapter 15]. Algorithms for the computation of generators and relations and the discrete logarithm are described in [Coh00, section 4.2] for the number field case and in [HPP02] for number fields and global function fields. We apply similar techniques to the computation of generators of $(\mathcal{O}/\mathfrak{a})^*$ where $\mathcal{O}$ is an arbitrary order and $\mathfrak{a}$ is an ideal of $\mathcal{O}$. In the following we denote by $\mathcal{O}_\mathfrak{p}$ the localization of $\mathcal{O}$ at a prime ideal $\mathfrak{p}$ and use the fact that there is a canonical embedding $\mathcal{O} \hookrightarrow \mathcal{O}_\mathfrak{p}$. We need the following result from commutative algebra.

Theorem 4.1. *Let $\mathcal{O}$ be a Noetherian domain of dimension 1 and $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$. Then*

(i) *If $\mathfrak{a}$ is contained in exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}$, i.e. $\mathfrak{a}$ is $\mathfrak{p}$-primary, then $\mathcal{O}/\mathfrak{a} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}$.*

(ii) *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals containing $\mathfrak{a}$. Then*

$$\mathcal{O}/\mathfrak{a} \cong \mathcal{O}_{\mathfrak{p}_1}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_1} \times \ldots \times \mathcal{O}_{\mathfrak{p}_r}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_r}.$$

(iii) *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Then*

$$\mathcal{O}/\mathfrak{p}^m \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p}.$$

Proof. The first assertion is stated in [AMcD69] just before proposition 4.1 on page 50. The second assertion follows immediately from the first part and propositions 4.6 and 4.9 in [AMcD69]. The last assertion is a special case of the first one. □

As it is not easy to conduct calculations in the localization $\mathcal{O}_\mathfrak{p}$ we carry out our calculations in $\mathcal{O}$ modulo a suitable power of $\mathfrak{p}$. If $\mathfrak{a} \subseteq \mathfrak{p}$ there always exists an integer m such that $\mathfrak{p}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$ (e.g. see [Eis95, theorem 2.13]). Using theorem 4.1 and the fact that $\mathfrak{a} + \mathfrak{p}^m$ is $\mathfrak{p}$-primary we get

$$\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/(\mathfrak{a} + \mathfrak{p}^m)\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/(\mathfrak{a} + \mathfrak{p}^m) \cong (\mathcal{O}/\mathfrak{p}^m)/\big((\mathfrak{a} + \mathfrak{p}^m)/\mathfrak{p}^m\big). \tag{2}$$

This allows us to first compute $\mathcal{O}/\mathfrak{p}^m$ and then to factor out the ideal $(\mathfrak{a} + \mathfrak{p}^m)/\mathfrak{p}^m$ of $\mathcal{O}/\mathfrak{p}^m$. The following proposition gives an estimate for the needed size of m.

Proposition 4.2. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ with $\mathfrak{p} \supseteq \mathfrak{a}$. Let $p = \operatorname{char}(\mathcal{O}/\mathfrak{p}\mathcal{O})$. Then*

(i) $v_p([\mathcal{O}_\mathfrak{p} : \mathfrak{a}\mathcal{O}_\mathfrak{p}]) \leq v_p([\mathcal{O} : \mathfrak{a}])$.
(ii) *For* $m \geq \frac{v_p([\mathcal{O}_\mathfrak{p} : \mathfrak{a}\mathcal{O}_\mathfrak{p}])}{v_p([\mathcal{O}_\mathfrak{p} : \mathfrak{p}\mathcal{O}_\mathfrak{p}])}$ *we get* $\mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$.

Proof. Let $m \in \mathbb{Z}$ with $\mathfrak{p}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$.
(i) Using (2) we have $\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/(\mathfrak{a}+\mathfrak{p}^m)$. As additive groups this is isomorphic to $(\mathcal{O}/\mathfrak{a})/((\mathfrak{a}+\mathfrak{p}^m)/\mathfrak{a})$ and we get $[\mathcal{O} : \mathfrak{a}] = [\mathcal{O}_\mathfrak{p} : \mathfrak{a}\mathcal{O}_\mathfrak{p}][\mathfrak{a}+\mathfrak{p}^m : \mathfrak{a}]$.
(ii) $\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}$ is an Artinian ring. We consider the decomposition series

$$\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq (\mathfrak{a}\mathcal{O}_\mathfrak{p} + \mathfrak{p}\mathcal{O}_\mathfrak{p})/\mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq \cdots \supseteq (\mathfrak{a}\mathcal{O}_\mathfrak{p} + \mathfrak{p}^m\mathcal{O}_\mathfrak{p})/\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}.$$

Since $\mathcal{O}_\mathfrak{p}$ is a local ring each quotient $((\mathfrak{a}\mathcal{O}_\mathfrak{p} + \mathfrak{p}^i\mathcal{O}_\mathfrak{p})/\mathfrak{a}\mathcal{O}_\mathfrak{p})/((\mathfrak{a}\mathcal{O}_\mathfrak{p} + \mathfrak{p}^{i+1}\mathcal{O}_\mathfrak{p})/\mathfrak{a}\mathcal{O}_\mathfrak{p})$ is isomorphic to $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Therefore $[\mathcal{O}_\mathfrak{p} : \mathfrak{p}\mathcal{O}_\mathfrak{p}]^m \mid [\mathcal{O}_\mathfrak{p} : \mathfrak{a}\mathcal{O}_\mathfrak{p}]$. Since the series stabilizes if and only if $\mathfrak{p}^m\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}$ we get the desired result. □

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals of $\mathcal{O}$ for which $\mathfrak{a} \subseteq \mathfrak{p}_i$ $(1 \leq i \leq r)$. We have described in section 3 how to compute $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Let $m_1, \ldots, m_r$ be integers such that $\mathfrak{p}_i\mathcal{O}_{\mathfrak{p}_i} \supseteq \mathfrak{a}\mathcal{O}_{\mathfrak{p}_i} \supseteq \mathfrak{p}_i^{m_i}\mathcal{O}_{\mathfrak{p}_i}$. With (2) we obtain for $1 \leq i \leq r$:

$$\left(\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_i}\right)^* \cong \left(\mathcal{O}/(\mathfrak{a}+\mathfrak{p}_i^{m_i})\right)^*.$$

Assume that (g_i, M_i) with $g_i = (g_{i,1}, \ldots, g_{i,n_i})^{\mathrm{tr}}$, $g_{i,j} \in \mathcal{O}$, and $M_i \in \mathbb{Z}^{n_i \times n_i}$ are generators and relations of the multiplicative group $(\mathcal{O}/(\mathfrak{a}+\mathfrak{p}_i^{m_i}))^*$. We use the Chinese remainder theorem to obtain generators $h_i = (h_{i,1}, \ldots, h_{i,n_i})^{\mathrm{tr}}$ such that for all $1 \leq j \leq n_i$:

$$\begin{aligned} h_{i,j} &\equiv g_{i,j} \bmod \mathfrak{p}_i^{m_i} \\ h_{i,j} &\equiv 1 \bmod \mathfrak{p}_k^{m_k} \text{ for all } k \neq i. \end{aligned}$$

This yields generators and relations (h, M) of $(\mathcal{O}/\mathfrak{a})^*$:

$$(h, M) = \left(\begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix}, \begin{pmatrix} M_1 & & 0 \\ & \ddots & \\ 0 & & M_r \end{pmatrix} \right).$$

Lemma 4.3. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathcal{O}$. *Then for every* $m \in \mathbb{N}$ *we have*

$$(\mathcal{O}/\mathfrak{p}^m)^* \cong (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m).$$

Proof. Let $\overline{\zeta}$ be a generator of $(\mathcal{O}/\mathfrak{p})^*$. Hensel lifting gives us a root of unity $\zeta \in \mathcal{O}/\mathfrak{p}^m$ with $\zeta \equiv \overline{\zeta} \bmod \mathfrak{p}$. Let

$$\psi : (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m) \longrightarrow (\mathcal{O}/\mathfrak{p}^m)^*$$

with $\psi((\overline{\zeta}^s, \eta)) := \zeta^s \cdot \eta$. It is clear that ψ is a homomorphism. Let $\gamma \in (\mathcal{O}/\mathfrak{p}^m)^*$. Let $s \in \mathbb{N}$ such that $\zeta^s \equiv \gamma \bmod \mathfrak{p}$. Now $\gamma/\zeta^s \equiv 1 \bmod \mathfrak{p}$, *i.e.*, $\gamma/\zeta^s \in 1+\mathfrak{p}^m$. As this decomposition is unique the map ψ is bijective. □

Let $\mathfrak{b}$ be an ideal in $\mathcal{O}$ with $\mathfrak{p} \supseteq \mathfrak{b} \supseteq \mathfrak{p}^m$ for some $m \in \mathbb{N}$. The more general result

$$(\mathcal{O}/\mathfrak{b})^* \cong (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{b}).$$

can be proven in the same way as the preceding lemma. One replaces $\mathfrak{p}^m$ by $\mathfrak{b}$ in the second part of the proof. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ and let $m \in \mathbb{N}$ such that

$\mathfrak{p}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{a}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$. Using (2) it follows that

$$\begin{aligned}(\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p})^* &\cong \big(\mathcal{O}/(\mathfrak{a}+\mathfrak{p}^m)\big)^* \\ &\cong (\mathcal{O}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{a}+\mathfrak{p}^m) \\ &\cong (\mathcal{O}/\mathfrak{p})^* \times \big((1+\mathfrak{p})/(1+\mathfrak{p}^m)\big)\big/\big((1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)\big).\end{aligned}$$

The computation of residue class fields is described in section 3. Algorithms for the computation of a primitive element of the multiplicative group $(\mathcal{O}/\mathfrak{p})^*$ of the residue class field $\mathcal{O}/\mathfrak{p}$ are contained in the literature, see [PZ89, section 2.5] for instance. Let ζ be as in the proof of lemma 4.3. Then

$$(\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p})^* \cong \langle\zeta\rangle \times \big((1+\mathfrak{p})/(1+\mathfrak{p}^m)\big)\big/\big((1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)\big).$$

Thus the problem of computing $(\mathcal{O}/\mathfrak{a})^*$ is reduced to the computation of the group $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ and the discrete logarithm therein, i.e., expressing elements of $(1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)$ in the generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$.

Computing $(1+\mathfrak{a})/(1+\mathfrak{b})$ for $\mathfrak{a}^2 \subseteq \mathfrak{b}$.

Lemma 4.4. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of an order $\mathcal{O}$ such that $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a}^2$. Then the map $\psi : (1+\mathfrak{a})/(1+\mathfrak{b}) \to \mathfrak{a}/\mathfrak{b}$, $[1+\gamma] \mapsto [\gamma]$ is a group-isomorphism, where $[1+\gamma]$ and $[\gamma]$ denote the class modulo $[1+\mathfrak{b}]$ and $[\mathfrak{b}]$, respectively.*

Proof. Let $[1+\gamma] \in (1+\mathfrak{a})/(1+\mathfrak{b})$. The image of $[1+\gamma]$ in $\mathfrak{a}/\mathfrak{b}$ is $[0]$ if and only if $\gamma \in \mathfrak{b}$. Thus the map is well defined and bijective. Let $[1+\gamma]$ and $[1+\delta]$ be elements of $(1+\mathfrak{a})/(1+\mathfrak{b})$. As $\gamma\delta \in \mathfrak{a}^2 \subseteq \mathfrak{b}$ we have $\psi([1+\gamma]\cdot[1+\delta]) = \psi([1+\gamma+\delta+\gamma\delta]) = \psi([1+\gamma+\delta]) = [\gamma+\delta] = \psi([1+\gamma]) + \psi([1+\delta])$. Hence ψ is an isomorphism. □

In order to apply lemma 4.4 let $\mathfrak{a} = R\tau_{\mathfrak{a},1} + \ldots + R\tau_{\mathfrak{a},n}$ and $\mathfrak{b} = R\tau_{\mathfrak{b},1} + \ldots + R\tau_{\mathfrak{b},n}$ be ideals of $\mathcal{O}$ with $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a}^2$. A basis of the additive group $\mathfrak{a}/\mathfrak{b}$ can be computed as follows:

Let $\omega = (\omega_1, \ldots, \omega_n)^{\mathrm{tr}}$ be an R-basis of $\mathcal{O}$. Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are given by the matrices $A, B \in R^{n\times n}$, via $\tau_\mathfrak{a} = (\tau_{\mathfrak{a},1}, \ldots, \tau_{\mathfrak{a},n})^{\mathrm{tr}} = A\omega$ and $\tau_\mathfrak{b} = (\tau_{\mathfrak{b},1}, \ldots, \tau_{\mathfrak{b},n})^{\mathrm{tr}} = B\omega$, respectively. The matrix BA^{-1} represents the elements of $\mathfrak{b}$ by the elements of $\mathfrak{a}$, as $\tau_\mathfrak{b} = BA^{-1}A\omega = BA^{-1}\tau_\mathfrak{a}$. The elements $\tau_{\mathfrak{a},1}, \ldots, \tau_{\mathfrak{a},n}$ are generators for the group $\mathfrak{a}/\mathfrak{b}$ and the matrix BA^{-1} describes the relations, as follows:

In the number field case $BA^{-1} \in \mathbb{Z}^{n\times n}$. Therefore the additive abelian group $\mathfrak{a}/\mathfrak{b}$ can be described by

$$(g, M) := \left(\begin{pmatrix} \tau_{\mathfrak{a},1} \\ \vdots \\ \tau_{\mathfrak{a},n} \end{pmatrix}, BA^{-1} \right)$$

The Smith normal form of M yields a basis of the group.

In the function field case we have $C = (c_{i,j})_{i,j} := BA^{-1} \in \mathbb{F}_q[t]^{n\times n}$. The goal is to find a relation matrix with coefficients in $\mathbb{Z}$. Let $d_j := \max_{1\le i\le n}\{\deg(c_{i,j})\}$. For $1 \le j \le n$ let

$$w_j : \mathbb{F}_q[t]_{\le d_j} \to \mathbb{F}_q{}^{d_j+1}, a_{d_j}t^{d_j} + \cdots + a_1 t + a_0 \mapsto (a_{d_j}, \ldots, a_1, a_0).$$

We define

$$D = (d_{i,j}) := \begin{pmatrix} w_1(c_{1,1}) & \ldots & w_n(c_{1,n}) \\ \vdots & \ddots & \vdots \\ w_1(c_{n,1}) & \ldots & w_n(c_{n,n}) \end{pmatrix}$$

which is an $\mathbb{F}_q$-relation matrix of the group generated by

$$h = (h_1, \ldots, h_s) := (\tau_{\mathfrak{a},1}, \tau_{\mathfrak{a},1} \cdot t, \ldots, \tau_{\mathfrak{a},1} \cdot t^{d_1}, \ldots, \tau_{\mathfrak{a},n}, \ldots, \tau_{\mathfrak{a},n} \cdot t^{d_n})^{\mathrm{tr}}.$$

Now we are in the situation that we have generators $(h_1, \ldots, h_s)$ and a matrix of relations $D \in {\mathbb{F}_q}^{n \times s}$. Let $q = p^f$ and $\rho_1, \ldots, \rho_f$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. We consider the map

$$u : \mathbb{F}_q \to {\mathbb{F}_p}^f,\ a = \sum_{i=1}^{f} a_i \rho_i \mapsto (a_1, \ldots, a_f)$$

and obtain generators and relations over $\mathbb{F}_p$:

$$(g, N) := \left((h_1\rho_1, \ldots, h_1\rho_f, \ldots, h_s\rho_f)^{\mathrm{tr}}, \begin{pmatrix} u(d_{1,1}) & \ldots & u(d_{1,s}) \\ \vdots & \ddots & \vdots \\ u(d_{n,1}) & \ldots & u(d_{n,s}) \end{pmatrix} \right).$$

The result are generators and an $\mathbb{F}_p$-relation matrix. Let I be the identity matrix of dimension fs. The matrix $M := \binom{pI}{N}$ is a relation matrix of the additive group $\mathfrak{a}/\mathfrak{b}$ generated by the components of the vector g.

Assume that $g = (g_1, \ldots, g_r)^{\mathrm{tr}}$. By lemma 4.4 the multiplicative group $(1 + \mathfrak{a})/(1 + \mathfrak{b})$ is represented by

$$\big((1 + g_1, \ldots, 1 + g_r)^{\mathrm{tr}}, M\big).$$

The discrete logarithm in $(1 + \mathfrak{a})/(1 + \mathfrak{b})$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathcal{O}$ with $\mathfrak{a}^2 \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. We use the notations of the discussion after lemma 4.4. Let $b \in 1 + \mathfrak{a}$. Therefore we can write:

$$b - 1 = \sum_{k=1}^{n} \alpha_k \tau_{\mathfrak{a},k} = \alpha A \omega,$$

where the $\alpha_k \in R$ can be computed using linear algebra.

If $\mathcal{O}$ is an order of a number field lemma 4.4 yields a representation $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ by the generators g of the group $(1 + \mathfrak{a})/(1 + \mathfrak{b})$.

If $\mathcal{O}$ is an order of a function field then $\alpha \in \mathbb{F}_q[t]^n$. Reducing the components α_i of α modulo $\tau_{\mathfrak{a},i}$ and applying the maps w_j gives a representation of b with respect to the generators g.

Computing $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$. Let $k, l \in \mathbb{Z}$ with $k < l \leq 2k$. Denote the class of $1 + a$ modulo $(1 + \mathfrak{p}^i)$ by $[1 + a]_i$. By the isomorphism theorem the sequence

$$\begin{array}{ccccccccc} 1 & \to & (1 + \mathfrak{p}^k)/(1 + \mathfrak{p}^l) & \stackrel{\Psi}{\to} & (1 + \mathfrak{p})/(1 + \mathfrak{p}^l) & \stackrel{\Phi}{\to} & (1 + \mathfrak{p})/(1 + \mathfrak{p}^k) & \to & 1 \\ & & [1 + a]_l & \mapsto & [1 + a]_l & \mapsto & [1 + a]_k & & \end{array}$$

is exact. Assume that generators and relations (g_k, M_k) of $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$ are known. Then we have $M_k g_k \in 1 + \mathfrak{p}^k$. Denote by (h_l, N_l) generators and relations of $(1 + \mathfrak{p}^k)/(1+\mathfrak{p}^l)$. Using the method for computing the representation of elements in $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$ described above we determine a matrix $P \in R^{n \times n}$ with $[\Psi^{-1}(M_k g_k)]_l = [P h_l]_l$ and obtain the representation

$$(g_l, M_l) := \left(\begin{pmatrix} g_k \\ h_l \end{pmatrix}, \begin{pmatrix} M_k & -P \\ 0 & N_l \end{pmatrix} \right).$$

for $(1 + \mathfrak{p})/(1 + \mathfrak{p}^l)$.

In order to compute generators and relations of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ we successively compute generators and relations of the groups

$$(1+\mathfrak{p})/(1+\mathfrak{p}^2),\ (1+\mathfrak{p})/(1+\mathfrak{p}^4),\ldots,\ (1+\mathfrak{p})/(1+\mathfrak{p}^m)$$

using the methods described above. As the algorithms are almost identical to the ones in [HPP02] for the quadratic case we do not present them here.

Computing $(\mathcal{O}/\mathfrak{a})^*$. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ and let $\mathfrak{p}\subseteq\mathcal{O}$ be a prime ideal with $\mathfrak{a}\subseteq\mathfrak{p}$. As we have seen above

$$(1+\mathfrak{p})/(1+\mathfrak{a}+\mathfrak{p}^m)\cong\big((1+\mathfrak{p})/(1+\mathfrak{p}^m)\big)\big/\big((1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)\big).$$

We remark that images of the generators of the group $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ are generators of the group $(1+\mathfrak{p})/(1+\mathfrak{a}+\mathfrak{p}^m)$, too. We need to compute generators of the group $(1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)$ in order to get the relations.

Denote by N a relation matrix of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ and let A be the matrix whose rows contain the representation of generators of $(1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)$ by the generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$. Then $\binom{N}{A}$ is a relation matrix of

$$\big((1+\mathfrak{p})/(1+\mathfrak{p}^m)\big)\big/\big((1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)\big).$$

We already described how to compute N. In order to compute A we do the following. As $\mathfrak{a}+\mathfrak{p}^m\subseteq\mathfrak{p}$ we have $(\mathfrak{a}+\mathfrak{p}^m)^m\subseteq\mathfrak{p}^m$. Lemma 4.4 yields sets of generators a_j for the groups $\big(1+(\mathfrak{a}+\mathfrak{p}^m)^{2^j}\big)\big/\big(1+(\mathfrak{a}+\mathfrak{p}^m)^{2^{j+1}}\big)$ for $0\le j<\log_2(m)$. The group $(1+\mathfrak{a}+\mathfrak{p}^m)/(1+\mathfrak{p}^m)$ is generated by the images of $a_0\cup\cdots\cup a_{\lfloor\log_2(m)\rfloor}$.

The following algorithm is the result of the discussion in this section.

Algorithm 4.5.
Input: An ideal $\mathfrak{a}$ of an order $\mathcal{O}$
Output: Generators and relations (g,M) of $(\mathcal{O}/\mathfrak{a})^*$

- Set $P=\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}\leftarrow\{\mathfrak{p}\subseteq\mathcal{O}\text{ prime}\mid\mathfrak{a}\subseteq\mathfrak{p}\}$.
- For all $\mathfrak{p}_i\in P$:
  - Determine m_i such that $\mathfrak{p}_i^{m_i}\subseteq\mathfrak{a}\mathcal{O}_{\mathfrak{p}_i}$.
  - Compute generators and relations (g_i,N_i) of $(\mathcal{O}/\mathfrak{p}_i^{m_i})^*$.
  - Compute generators $a_{i,0}\cup\cdots\cup a_{i,\lfloor\log_2(m_i)\rfloor}$ of $(1+\mathfrak{a}+\mathfrak{p}_i^{m_i})/(1+\mathfrak{p}_i^{m_i})$.
  - Let A_i be the matrix containing representations of the elements in $a_{i,0}\cup\cdots\cup a_{i,\lfloor\log_2(m_i)\rfloor}$ by the generators g_i of $(\mathcal{O}/\mathfrak{p}_i^{m_i})^*$.
  - $(g_i,M_i)\leftarrow\left(g_i,\binom{N_i}{A_i}\right)$ are generators and relations of $(\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}_i})^*$.
- For all i obtain generators $h_i=(h_{i,1},\ldots,h_{i,n_i})^{\mathrm{tr}}$ using the Chinese remainder theorem such that for all $1\le j\le n_i$:

$$\begin{aligned}h_{i,j}&\equiv g_{i,j}\bmod\mathfrak{p}_i^{m_i}\\ h_{i,j}&\equiv 1\bmod\mathfrak{p}_k^{m_k}\text{ for all }k\neq i.\end{aligned}$$

- Return

$$\left(\begin{pmatrix}h_1\\ \vdots\\ h_r\end{pmatrix},\begin{pmatrix}M_1&&0\\ &\ddots&\\ 0&&M_r\end{pmatrix}\right).$$

5. Picard Groups

We give an overview of some properties of the Picard group of an order $\mathcal{O}$. For a more detailed exposition of these results including proofs see [Neu92, Kapitel I, §12].

A fractional ideal of an order $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule of the field of fractions K. A fractional ideal $\mathfrak{a}$ is called invertible, if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.

Definition 5.1 (Picard Group)**.** Let $\mathcal{O}$ be an order. Denote by $J(\mathcal{O})$ the group of invertible fractional ideals of $\mathcal{O}$. This group contains the group $P(\mathcal{O})$ of fractional principal ideals $a\mathcal{O}$ where $a \in K^*$. The group $\mathrm{Pic}(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$ is called the Picard group of $\mathcal{O}$.

Example 5.2. $\mathrm{Pic}(\widetilde{\mathcal{O}})$ is the ideal class group of the maximal order $\widetilde{\mathcal{O}}$. Let K be a number field with maximal order $\widetilde{\mathcal{O}}$. Then $\mathrm{Cl}_K = \mathrm{Pic}(\widetilde{\mathcal{O}})$ is the class group of K.

Example 5.3. Let T be a non-empty subset of the set of places of a rational function field $\mathbb{F}_q(t)$. Let $R := \{a \in \mathbb{F}_q(t) \mid v_{\mathfrak{p}}(a) \geq 0,\ \mathfrak{p} \notin T\}$. Let $\mathcal{O}$ be an R-order with field of fractions K. Let S be the set of all places of K that lie over the places contained in T and set $\widetilde{\mathcal{O}} := \{b \in K \mid v_{\mathfrak{q}}(b) \geq 0,\ \mathfrak{q} \notin S\}$. $\widetilde{\mathcal{O}}$ is called the S-maximal order of K (also see [Ros02, chapter 14]). The ideal class group $\mathrm{Pic}(\widetilde{\mathcal{O}})$ of $\widetilde{\mathcal{O}}$ is called the S-class group of K.

Localization yields a useful criterion for the invertibility of a fractional ideal. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. We denote by $\mathcal{O}_{\mathfrak{p}}$ the localization of $\mathcal{O}$ at $\mathfrak{p}$.

Lemma 5.4. *A fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is invertible if and only if for every prime ideal $\mathfrak{p} \neq 0$ the ideal $\mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ of the localization of $\mathcal{O}$ at $\mathfrak{p}$ is a fractional principal ideal.*

Consider the map $J(\mathcal{O}) \to \bigoplus_{\mathfrak{p}} P(\mathcal{O}_{\mathfrak{p}})$, $\mathfrak{a} \mapsto (\mathfrak{a}\mathcal{O}_{\mathfrak{p}})_{\mathfrak{p}}$. In [Neu92, Kapitel I, §12] it is proved that this is a homomorphism and that $(a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \bigcap a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ is its inverse. Hence we obtain:

Lemma 5.5.

$$J(\mathcal{O}) \cong \bigoplus_{\mathfrak{p}} P(\mathcal{O}_{\mathfrak{p}}).$$

Thus $\mathrm{Pic}(\mathcal{O}) = \bigoplus_{\mathfrak{p}} P(\mathcal{O}_{\mathfrak{p}})/P(\mathcal{O})$. For any order $\mathcal{O}$ of K we have $P(\mathcal{O}) \cong K^*/\mathcal{O}^*$. This gives the exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^*/\mathcal{O}^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{\mathfrak{p}}^* & \longrightarrow & \mathrm{Pic}(\mathcal{O}) & \longrightarrow & 1 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 1 & \longrightarrow & K^*/\widetilde{\mathcal{O}}^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\widetilde{\mathcal{O}}_{\mathfrak{p}}^* & \longrightarrow & \mathrm{Pic}(\widetilde{\mathcal{O}}) & \longrightarrow & 1 \end{array}$$

The maps α and β are induced by the embeddings $\mathcal{O} \to \widetilde{\mathcal{O}}$ and $\mathcal{O}_{\mathfrak{p}} \to \widetilde{\mathcal{O}}_{\mathfrak{p}}$, respectively. The map γ is induced by $J(\mathcal{O}) \to J(\widetilde{\mathcal{O}}), \mathfrak{a} \mapsto \mathfrak{a}\widetilde{\mathcal{O}}$. Obviously α and β are surjective with $\ker(\alpha) = \widetilde{\mathcal{O}}^*/\mathcal{O}^*$ and $\ker(\beta) = \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$. It follows that γ is surjective. Application of the snake lemma yields:

Theorem 5.6. *Let $\mathcal{O}$ be an order and $\widetilde{\mathcal{O}}$ be its maximal order. Then there is a natural exact sequence*

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \widetilde{\mathcal{O}}^* \longrightarrow \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\widetilde{\mathcal{O}}) \longrightarrow 1.$$

6. The Conductor of an Order

We want to compute $\mathrm{Pic}(\mathcal{O})$ using theorem 5.6. For this we need to know $\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ including the homomorphisms in the exact sequence. The conductor of an order is an useful tool for this computation.

Definition 6.1. Let $\mathcal{O}$ be an order of K, and $\widetilde{\mathcal{O}}$ be the integral closure of $\mathcal{O}$ in K. Then

$$\mathcal{F} := \{\beta \in K \mid \beta\widetilde{\mathcal{O}} \subseteq \mathcal{O}\}$$

is called the conductor of $\mathcal{O}$.

It can easily be seen that $\mathcal{F}$ is an ideal of $\mathcal{O}$ and of $\widetilde{\mathcal{O}}$. A prime ideal $0 \neq \mathfrak{p}$ of $\mathcal{O}$ is called regular if the localization $\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}$ at $\mathfrak{p}$ is a discrete valuation ring. The prime ideals of $\mathcal{O}$ containing the conductor $\mathcal{F}$ are exactly the non-regular prime ideals. Thus $\widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ is trivial for all $\mathfrak{p}$ not containing $\mathcal{F}$. We obtain:

Proposition 6.2.

$$\widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \cong (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathcal{F}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathcal{F}\mathcal{O}_{\mathfrak{p}})^*$$

We will apply this isomorphism in the computation of $\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$.

Computing $\mathcal{F}$. It is well known how to compute the conductor of an order, but we have not found a reference in the literature. Since the presentation is short and the computation is an important step of our algorithm we explain it here. We assume that an R-basis of the maximal R-order $\widetilde{\mathcal{O}}$ is known. Let Q be the field of fractions of R. Let $\omega_1, \ldots, \omega_n$ be an R-basis of $\widetilde{\mathcal{O}}$ and $\tau_1, \ldots, \tau_n$ be an R-basis of $\mathcal{O}$. Then we define $b_{i,j,k} \in Q$ by the following equations:

$$\omega_i\omega_j = \sum_{k=1}^{n} b_{i,j,k}\tau_k.$$

We have $\beta \in \mathcal{F}$ if and only if $\beta\omega_j \in \mathcal{F}$ for $1 \leq j \leq n$. For $\beta := \sum_{i=1}^{n} a_i\omega_i$ we obtain

$$\beta\omega_j = \sum_{i=1}^{n} a_i\omega_i\omega_j = \sum_{i=1}^{n} a_i\Big(\sum_{k=1}^{n} b_{i,j,k}\tau_k\Big) = \sum_{k=1}^{n}\left(\sum_{i=1}^{n} a_i b_{i,j,k}\right)\tau_k.$$

Therefore $\beta \in \mathcal{F}$ if and only if

$$\sum_{i=1}^{n} a_i b_{i,j,k} \in R \text{ for all } 1 \leq j,k \leq n.$$

For $1 \leq j \leq n$ define the matrices

$$M_j := \begin{pmatrix} b_{1,j,1} & \cdots & b_{n,j,1} \\ \vdots & \ddots & \vdots \\ b_{1,j,n} & \cdots & b_{n,j,n} \end{pmatrix}.$$

Hence $\beta \in \mathcal{O}$ if and only if $M_j(a_1, \ldots, a_n)^{\mathrm{tr}} \in R^n$ for $1 \leq j \leq n$. Set

$$M := \begin{pmatrix} M_1 \\ \vdots \\ M_n \end{pmatrix}.$$

Let d be the greatest common divisor of all $\widetilde{d} \in R$ with $\widetilde{d}M \in R^{n^2 \times n}$. Thus $\beta \in \mathcal{F}$ if and only if $M(a_1, \ldots, a_n)^{\mathrm{tr}} \in dR^{n^2}$. Let $H \in R^{n \times n}$ be the row Hermite normal form of dM. Hence $\beta \in \mathcal{F}$ if and only if $H(a_1, \ldots, a_n)^{\mathrm{tr}} \in dR^n$. Since the ideal $\mathcal{F}$ is integral $dH^{-1} \in R^{n \times n}$ and we have that $\mathcal{F} = R\beta_1 + \ldots R\beta_n$, where $(\beta_1, \ldots, \beta_n) = (\omega_1, \ldots, \omega_n)dH^{-1}$.

7. Residue Class Rings II

For ideals $\mathfrak{a} \subseteq \mathcal{O}_\mathfrak{p}$ we examine how the multiplicative group $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$ can be described as a subgroup of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*$. The next proposition describes the cases where this is possible.

Proposition 7.1. *Let $\mathfrak{a} \subseteq \mathcal{O}_\mathfrak{p}$ be an ideal. Then there is a canonical homomorphism*

$$\Psi : (\mathcal{O}_\mathfrak{p}/\mathfrak{a})^* \to (\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*, a + \mathfrak{a} \mapsto a + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}.$$

If furthermore $\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{a}$ then Ψ is injective.

Proof. Let $a+\mathfrak{a} = b+\mathfrak{a}$. This implies $a-b \in \mathfrak{a} \subseteq \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$. Therefore $a+\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} = b+\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$. $a + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$ is invertible in $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*$ since it is invertible in $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$ and $\mathfrak{a} \subseteq \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$. Therefore the map Ψ is well defined. Since Ψ is well defined it follows from its definition that it is a homomorphism.

Suppose $a + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} = 1 + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$ for some $a \in \mathcal{O}_\mathfrak{p}$. This implies $a - 1 \in \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}$. Together with the assumption that $\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{a}$ this proves the injectivity. □

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_\mathfrak{p}$ with $\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{a}$. Let $h_1 + \mathfrak{a}, \ldots, h_u + \mathfrak{a}$ be generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$. Using the above proposition we get

$$(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^* = \langle h_1 + \mathfrak{a}, \ldots, h_u + \mathfrak{a}\rangle \cong \langle h_1 + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u + \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}\rangle \subseteq (\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*.$$

In general we only have $\mathfrak{a} \subseteq \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$. The following corollary is useful in this case.

Corollary 7.2. *Let $\mathfrak{b}$ be an ideal of $\mathcal{O}_\mathfrak{p}$ with $\mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{b}$. Let $h_1 + \mathfrak{a}, \ldots, h_u + \mathfrak{a}$ be generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$. Then $\langle h_1 + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}\rangle$ is a subgroup of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p})^*$. The homomorphism*

$$\Phi : \langle h_1 + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}\rangle \to (\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*,\ h_i + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p} \mapsto h_i + \mathfrak{a}\ \ (1 \le i \le u)$$

is surjective and

$$\langle h_1 + \mathfrak{a}, \ldots, h_u + \mathfrak{a}\rangle \cong \langle h_1 + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}\rangle / \ker(\Phi).$$

We use the conductor to determine such an ideal $\mathfrak{b}$ for a given ideal $\mathfrak{a}$.

Lemma 7.3. *Let $\mathcal{F}$ be the conductor of an order $\mathcal{O}$. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. Then*

$$\mathfrak{a} \supseteq (\mathcal{F}\mathfrak{a})\widetilde{\mathcal{O}} \cap \mathcal{O} = \mathcal{F}\mathfrak{a}.$$

Proof. $\mathcal{F}\mathfrak{a}\widetilde{\mathcal{O}} = \mathcal{F}\widetilde{\mathcal{O}}\mathfrak{a} = \mathcal{F}\mathfrak{a} \subseteq \mathfrak{a}$. □

In the proof of the next lemma we construct a minimal m such that $\mathfrak{a} \supseteq \mathfrak{p}^m$.

Lemma 7.4. *Let $\mathfrak{a} \subseteq \mathfrak{p}$ be an ideal in $\mathcal{O}_\mathfrak{p}$ with $\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{a}$. Then there exists an m such that $\mathfrak{p} \supseteq \mathfrak{a} \supseteq \mathfrak{p}^m$.*

Proof. We remark that $\widetilde{\mathcal{O}}_\mathfrak{p}$ is a Dedekind domain with finitely many maximal ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. In a Dedekind domain the product and the intersection of coprime ideals coincide. Let

$$\mathfrak{p}\widetilde{\mathcal{O}}_\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \quad \text{and} \quad \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{m_i}$$

be the factorization of $\mathfrak{p}\widetilde{\mathcal{O}}_\mathfrak{p}$ and $\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p}$ respectively. We obtain

$$\mathfrak{a} = \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{m_i} \cap \mathcal{O}_\mathfrak{p} = \bigcap_{i=1}^{r} (\mathfrak{P}_i^{m_i} \cap \mathcal{O}_\mathfrak{p}) \supseteq \bigcap_{i=1}^{r} \mathfrak{p}^{\lceil m_i/e_i \rceil} = \mathfrak{p}^m,$$

where $m = \max\{\lceil m_i/e_i \rceil \mid 1 \le i \le r\}$. For $1 \le i \le r$ equality holds in the inclusion

$$\mathfrak{P}_i^{m_i} \cap \mathcal{O}_\mathfrak{p} \subseteq \mathfrak{P}^{\lfloor \frac{m_i}{e_i} \rfloor e_i} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{p}^{\lfloor \frac{m_i}{e_i} \rfloor}$$

if and only if $e_i \mid m_i$. Thus m is minimal with $\mathfrak{p} \supseteq \mathfrak{a} \supseteq \mathfrak{p}^m$. □

We return to the computation of $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$ for an ideal $\mathfrak{a}$ of $\mathcal{O}_\mathfrak{p}$. Let $\mathcal{F}$ be the conductor of $\mathcal{O}$. By lemma 7.3 $\mathfrak{b} := \mathcal{F}\mathfrak{a}$ satisfies the assumptions of corollary 7.2. By lemma 7.4 we find $m \in \mathbb{N}$ such that $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{p}^m$. The multiplicative group $(\mathcal{O}_\mathfrak{p}/\mathfrak{a})^*$ is generated by a representative of a generator of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p})^*$ and the generators of the groups

$$(1+\mathfrak{p})/(1+\mathfrak{p}^2), \ldots, (1+\mathfrak{p}^{m-1})/(1+\mathfrak{p}^m),$$

see lemma 4.3 and lemma 4.4. Denote these generators by $h_1+\mathfrak{a}, \ldots, h_u+\mathfrak{a}$. With corollary 7.2 we get

$$\begin{aligned} (\mathcal{O}_\mathfrak{p}/\mathfrak{a})^* &= (\mathcal{O}_\mathfrak{p}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{a}) \\ &\cong \langle h_1 + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u + \mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p} \rangle / \ker(\Phi) \end{aligned}$$

As $\mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$ the kernel $\ker(\Phi)$ is the subgroup of $\langle h_1+\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u+\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p} \rangle$ generated by the generators of $1+\mathfrak{a}$. There exists $n \in \mathbb{N}$ such that $\mathfrak{b} \supseteq \mathfrak{a}^{2^n}$ (*e.g.* $n = \lceil \log_2 m \rceil$). The image of the group $1+\mathfrak{a}$ in $\langle h_1+\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p}, \ldots, h_u+\mathfrak{b}\widetilde{\mathcal{O}}_\mathfrak{p} \rangle$ is generated by the images of the generators of the groups

$$(1+\mathfrak{a})/(1+\mathfrak{a}^2), \ldots, (1+\mathfrak{a}^{2^{n-1}})/(1+\mathfrak{a}^{2^n}).$$

Together with the first part of section 4 this yields a second method for the computation of $(\mathcal{O}/\mathfrak{a})^*$ for an ideal $\mathfrak{a}$ of an order $\mathcal{O}$. The method for the computation of $(\mathcal{O}/\mathfrak{a})^*$ presented in this section is especially interesting when the multiplicative group of the residue class ring of the respective ideal $\mathfrak{a}\widetilde{\mathcal{O}}$ in the maximal order $\widetilde{\mathcal{O}}$ has to be computed anyway and if $\mathfrak{a} = \mathfrak{a}\widetilde{\mathcal{O}} \cap \mathcal{O}$. As we will see this is the case in the computation of the Picard group and the unit group of $\mathcal{O}$. Another advantage is that the implementation of this method is easier since the whole machinery of residue class rings in maximal orders can be used to get the relations via corollary 7.2.

8. Computing Picard Groups

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. For an ideal $\mathfrak{a}$ of $\mathcal{O}_\mathfrak{p}$ the structure of the multiplicative group $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*$ is well known:

$$(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^* \cong \prod_{\mathfrak{q}|\mathfrak{p}} (\widetilde{\mathcal{O}}_\mathfrak{q}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{q})^* \cong \prod_{\mathfrak{q}|\mathfrak{p}} (\widetilde{\mathcal{O}}_\mathfrak{q}/\mathfrak{q}^{m_\mathfrak{q}})^*,$$

where $m_\mathfrak{q}$ is maximal with respect to $\mathfrak{q}^{m_\mathfrak{q}} \mid \mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{q}$. The products are taken over all prime ideals $\mathfrak{q}$ of $\widetilde{\mathcal{O}}_\mathfrak{p}$ containing $\mathfrak{p}\widetilde{\mathcal{O}}_\mathfrak{p}$. We use the isomorphism

$$\widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \cong (\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathcal{F}\mathcal{O}_\mathfrak{p})^*$$

from proposition 6.2 to compute $\widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$ as follows:

Assume that a vector g of generators and a relation matrix M for $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*$ are known. Denote by N the matrix whose rows contain the representation of a set of generators of $(\mathcal{O}_\mathfrak{p}/\mathcal{F}\mathcal{O}_\mathfrak{p})^*$ in the generators of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*$. Then generators and relations of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathcal{F}\mathcal{O}_\mathfrak{p})^*$ are given by $(g, \binom{M}{N})$.

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ with $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{p}^m$. For the computation of

$$(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p})^*$$

it is sufficient to compute $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*$ and a set of representatives $h_1, \ldots, h_t$ of generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})^*$ in $\mathcal{O}_\mathfrak{p}$, as the representatives of generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})^*$ are also representatives of generators of $(\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p})^*$ and as

$$(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p})^* = (\widetilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{a}\widetilde{\mathcal{O}}_\mathfrak{p})^*/\langle h_1, \ldots, h_t\rangle.$$

We compute the group $\bigoplus_{\mathfrak{p}\subseteq\mathcal{O}} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* = \bigoplus_{\mathcal{F}\subseteq\mathfrak{p}\subseteq\mathcal{O}} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$ using the following algorithm.

Algorithm 8.1.

Input: an order $\mathcal{O}$

Output: Generators and relations (g, M) of $\bigoplus_\mathfrak{p} \widetilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$

- Compute the conductor $\mathcal{F}$ of $\mathcal{O}$. [Section 6]
- Derive a factorization $\mathfrak{q}_1^{e_{\mathfrak{q}_1}} \cdot \cdots \cdot \mathfrak{q}_r^{e_{\mathfrak{q}_r}} = \mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p}$.
- Set $P \leftarrow \{\mathfrak{p}_1, \ldots, \mathfrak{p}_u\} = \{\mathfrak{q}_i \cap \mathcal{O} \mid 1 \le i \le r\}$.
- For all $\mathfrak{p} \in P$:
  - Find m with $\mathcal{F}\mathcal{O}_\mathfrak{p} \supseteq \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$.
  - Compute generators and relations $(g_1, \ldots, g_s, R)$ of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*$, such that $g_i \equiv 1 \bmod \prod_{\mathfrak{q}\in P\setminus\{\mathfrak{p}\}} \mathfrak{q}^{e_\mathfrak{q}}\widetilde{\mathcal{O}}$ for $1 \le i \le s$.
  - Compute generators $[h_1], \ldots, [h_t]$ of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p})$ with the property that $h_i \equiv 1 \bmod \prod_{\mathfrak{q}\in P\setminus\{\mathfrak{p}\}} \mathfrak{q}^{e_\mathfrak{q}}$ for $1 \le i \le t$.
  - Compute generators and relations $(g_\mathfrak{p}, M_\mathfrak{p})$ of $(\widetilde{\mathcal{O}}_\mathfrak{p}/\mathcal{F}\widetilde{\mathcal{O}}_\mathfrak{p})^*/\langle h_1, \ldots, h_t\rangle$.
- Return $\left(\begin{pmatrix} g_{\mathfrak{p}_1} \\ \vdots \\ g_{\mathfrak{p}_u} \end{pmatrix}, \begin{pmatrix} M_{\mathfrak{p}_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & M_{\mathfrak{p}_u} \end{pmatrix}\right)$

As we have mentioned before we use the exact sequence from theorem 5.6 to compute $\mathcal{O}^*$ and $\mathrm{Pic}(\mathcal{O})$. There are efficient algorithms for the computation of ideal class groups and unit groups of $\widetilde{\mathcal{O}}$.

Algorithms for the computation of the unit group $\widetilde{\mathcal{O}}^*$ and the class group of a number field K are described in [Coh93, section 4.9] and [PZ89, chapter 5].

An algorithm for the computation of the unit group of the finite maximal order of a global function field is given in [Sch96]. Florian Hess has developed a method for computing divisor class groups of global function fields [Hes99, Hes02]. From

the divisor class group one easily obtains the ideal class group of the S-maximal orders [Hes99, section 6.3].

Now that we have a method for determining generators and relations for the group $\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ the only unknown groups in the exact sequence from theorem 5.6 are $\mathcal{O}^*$ and $\mathrm{Pic}(\mathcal{O})$.

Computing $\mathcal{O}^*$. The group $\mathcal{O}^*$ is the kernel of the map

$$\widetilde{\mathcal{O}}^* \longrightarrow \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \cong (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathcal{F}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathcal{F}\mathcal{O}_{\mathfrak{p}})^*$$

from the exact sequence in theorem 5.6. This kernel can be easily computed using the homomorphism $\widetilde{\mathcal{O}}^* \to (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathcal{F}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*$.

Computing $\mathrm{Pic}(\mathcal{O})$. We can obtain the group $\mathrm{Pic}(\mathcal{O})$ from the exact sequence

$$\widetilde{\mathcal{O}}^* \longrightarrow \bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Pic}(\widetilde{\mathcal{O}}) \longrightarrow 1$$

using algorithms for computations with finitely generated abelian groups [Coh00, section 4.1]. In order to use these algorithms we need to figure out how the residue classes in $\bigoplus_{\mathfrak{p}} \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ are mapped to the ideals in $\mathrm{Pic}(\mathcal{O})$. In section 5 we considered the map

$$\bigoplus_{\mathfrak{p}} P(\mathcal{O}_{\mathfrak{p}}) \to J(\mathcal{O}),\ (a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \bigcap a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}.$$

This induces a map

$$\bigoplus \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \cong (\widetilde{\mathcal{O}}_{\mathfrak{p}}/\mathcal{F}\widetilde{\mathcal{O}}_{\mathfrak{p}})^*/(\mathcal{O}_{\mathfrak{p}}/\mathcal{F}\mathcal{O}_{\mathfrak{p}})^* \to \mathrm{Pic}(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O}).$$

The Chinese remainder theorem yields a representative $a \in \widetilde{\mathcal{O}}_{\mathfrak{p}}^*$ of the class $[(a_{\mathfrak{p}})_{\mathfrak{p}}]$ in $\bigoplus \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$. The representative a is mapped to $\mathfrak{a} = (a\widetilde{\mathcal{O}}) \cap \mathcal{O}$. By the exact sequence in theorem 5.6 $\mathfrak{a}$ is not principal if the class of a is not trivial in $\bigoplus \widetilde{\mathcal{O}}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$.

9. Examples

All algorithms described in this paper have been implemented in the computer algebra system Magma [Ca$^+$03]. The Magma package containing the functions is available at the authors homepages. The computations were conducted on a PC with an AMD Athlon XP 1800 processor with 512 MB RAM running Linux.

In the first two examples we compute the Picard group and the unit group of two different orders.

Example 9.1. Let $\mathcal{O} = \mathbb{Z}[\sqrt[3]{2000}]$ be an order and $K = \mathbb{Q}(\sqrt[3]{2})$ its field of fractions. K has unit rank one and class number one. The conductor of $\mathcal{O}$ is $\mathcal{F} = (100)$. We obtain

$$\begin{aligned}
(\widetilde{\mathcal{O}}/\mathcal{F})^* &\cong C_2^2 \times C_{20} \times C_{40} \times C_{120},\\
(\mathcal{O}/\mathcal{F})^* &\cong C_2 \times C_{10} \times C_{20},\\
(\widetilde{\mathcal{O}}/\mathcal{F})^*/(\mathcal{O}/\mathcal{F})^* &\cong C_8 \times C_{120}\\
\mathrm{Pic}(\mathcal{O})/\mathrm{Cl}_K &\cong C_{24}.
\end{aligned}$$

Since the class group of K is trivial we get $\mathrm{Pic}(\mathcal{O}) \cong C_{24}$. The whole computation took 0.4 seconds. The element

$$11519200001 + 22664172850\sqrt[3]{2000} - 1871423004\sqrt[3]{2000}^2$$

is a fundamental unit of $\mathcal{O}$. It has index 40 in $\widetilde{\mathcal{O}}^*$.

Example 9.2. Let $f = x^3 - 12x^2 - 6324x + 459510 \in \mathbb{Z}[x]$. Let α be a root of f and set $\mathcal{O} = \mathbb{Z}[\alpha]$. This order has the same quotient field as in the previous example. We get

$$\begin{aligned}
(\widetilde{\mathcal{O}}/\mathcal{F})^* &\cong C_6^2 \times C_{24} \times C_{504} \times C_{78624},\\
(\mathcal{O}/\mathcal{F})^* &\cong C_2 \times C_4^2 \times C_{4368},\\
(\widetilde{\mathcal{O}}/\mathcal{F})^*/(\mathcal{O}/\mathcal{F})^* &\cong C_6^2 \times C_{18} \times C_{378}\\
\mathrm{Pic}(\mathcal{O})/\mathrm{Cl}_K &\cong C_3 \times C_6^2 \times C_{18}.
\end{aligned}$$

Since the class group of K is trivial we get $\mathrm{Pic}(\mathcal{O}) \cong C_3 \times C_6^2 \times C_{18}$.

We found

$$\begin{aligned}
\mathcal{O}^* = \langle &-1, 72889299677002352500609207007772363 49 - \\
&37518645348677758942690319612626524\alpha - \\
&11243947444258606337244350699191 17\alpha^2\rangle
\end{aligned}$$

with $[\widetilde{\mathcal{O}}^* : \mathcal{O}^*] = 126$. The whole computation took 0.3 seconds.

The following example is interesting because the class group of K is not trivial. Furthermore the group extension by the class group is non-split.

Example 9.3. Let $\mathcal{O} = \mathbb{Z}[x]/(f)$ with $f = x^5 - 1389x^4 + 512066x^3 - 11859166x^2 + 83453925x - 211865821$ and K its field of fractions. We remark that K is isomorphic to $\mathbb{Q}[x]/(x^5 + 2x^4 + 12x^3 + 14x^2 - 12x - 16)$. Let $\widetilde{\mathcal{O}}$ be the integral closure of $\mathcal{O}$ in K. The index of $\mathcal{O}$ in $\widetilde{\mathcal{O}}$ is $5082900972974240768 = 2^{10} \cdot 11 \cdot 451251861947287$. We get

$$\begin{aligned}
(\widetilde{\mathcal{O}}/\mathcal{F})^* &\cong C_2^8 \times C_8 \times C_{36100148955782880}^2,\\
(\mathcal{O}/\mathcal{F})^* &\cong C_2^4 \times C_4 \times C_{36100148955782880},\\
(\widetilde{\mathcal{O}}/\mathcal{F})^*/(\mathcal{O}/\mathcal{F})^* &\cong C_2^5 \times C_{36100148955782880}\\
\mathrm{Pic}(\mathcal{O})/\mathrm{Cl}_K &\cong C_2^4.
\end{aligned}$$

The ideal class group Cl_K of $\widetilde{\mathcal{O}}$ is isomorphic to C_{12}. Finally we obtain $\mathrm{Pic}(\mathcal{O}) \cong C_2^3 \times C_{24}$. The computations were finished within 2 seconds. The unit group of $\mathcal{O}$ is generated by

$$\langle -1, \varepsilon_1^{120975552}\varepsilon_2^{-46343618}, \varepsilon_1^{210255456}\varepsilon_2^{516272076}\rangle,$$

where $\varepsilon_1, \varepsilon_2$ are certain fundamental units of $\widetilde{\mathcal{O}}$.

The last example shows that the algorithm also works for global function fields.

Example 9.4. Let $f = x^2 + 4t^{11} + 2t^9 = x^2 - t^8(t^3 + 3t)) \in \mathbb{F}_5[t][x]$ and $K = \mathbb{F}_5(t)[x]/(f)$. Let $\mathcal{O} = \mathbb{F}_5[t][x]/(f)$ be the equation order of f. Let S be the set of infinite places of K, *i.e.* the set of all places over $\mathfrak{p}_\infty = (1/t)$. The S-maximal order

$$\mathcal{O} = \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0 \text{ for all places } \mathfrak{p} \notin S\}$$

is the finite maximal order of K. The S-class group Cl_S of K is isomorphic to C_{10}. We obtained

$$\begin{aligned}(\widetilde{\mathcal{O}}/\mathcal{F})^* &\cong C_5^5 \times C_{100},\\ (\mathcal{O}/\mathcal{F})^* &\cong C_5 \times C_{20},\\ (\widetilde{\mathcal{O}}/\mathcal{F})^*/(\mathcal{O}/\mathcal{F})^* &\cong C_5^3 \times C_{25},\\ \mathrm{Pic}(\mathcal{O})/\mathrm{Cl}_K &\cong C_5^3 \times C_{25}.\end{aligned}$$

We get $\mathrm{Pic}(\mathcal{O}) \cong C_5^4 \times C_{50}$. The unit groups of the order and its integral closure coincide. The whole computation took 0.4 seconds.

References

[AMcD69] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

[Ca+03] J.J. Canon et al., The computer algebra system Magma, University of Sydney (2003), `http://magma.maths.usyd.edu.au/magma/`.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Springer Verlag, New York, 1993.

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Springer Verlag, New York, 2000.

[CDO01] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier *Algorithmic methods for finitely generated abelian groups* J. Symb. Comp. **31** (2001), 133–147.

[Eis95] David Eisenbud, *Commutative Algebra*, Springer Verlag, New York, 1995.

[Has80] Helmut Hasse, *Number theory*, Springer Verlag, Berlin, 1980.

[Hes99] Florian Heß, *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*, Dissertation, TU - Berlin, 1999, `http://www.math.TU-Berlin.DE/~kant/publications/diss/diss_FH.ps.gz`.

[Hes02] Florian Heß, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comp. **33** (2002): 425–445.

[HPP02] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), 1531-1548.

[Neu92] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.

[Po+00] Michael E. Pohst *et al*, *The computer algebra system KASH/KANT*, TU-Berlin, 2000, `http://www.math.tu-berlin.de/~kant/`.

[PZ89] Michael E. Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[Sch96] Martin Schörnig, *Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern*, Dissertation, TU - Berlin, 1996, `http://www.math.TU-Berlin.DE/~kant/publications/diss/MS_diss.ps.gz`.

[Ros02] Michael Rosen, *Number Theory in Function Fields*, Springer Verlag, New York 2002.

[Sim94] Charles C. Sims, *Computation with finitely presented groups*, Cambridge University Press, 1994.

[Wil93] Klaus Wildanger, *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, Heinrich-Heine-Universität Düsseldorf, 1993, `http://www.math.tu-berlin.de/~kant/publications/diplom/wildanger.ps.gz`

Universität Kassel, Fachbereich Mathematik und Informatik, Heinrich-Plett-Str. 40, 34132 Kassel, Germany.

E-mail address: `klueners@mathematik.uni-kassel.de`

Technische Universität Berlin, Institut für Mathematik, Sekretariat MA 8–1, Strasse des 17. Juni 136, 10623 Berlin, Germany

E-mail address: `pauli@math.tu-berlin.de`