COMPUTING THE MULTIPLICATIVE GROUP OF RESIDUE CLASS RINGS

FLORIAN HESS, SEBASTIAN PAULI, AND MICHAEL E. POHST

ABSTRACT. Let $\mathbf{k}$ be a global field with maximal order $\mathfrak{o}_{\mathbf{k}}$ and let $\mathfrak{m}_0$ be an ideal of $\mathfrak{o}_{\mathbf{k}}$. We present algorithms for the computation of the multiplicative group $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^*$ of the residue class ring $\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0$ and the discrete logarithm therein based on the explicit representation of the group of principal units [Has80]. We show how these algorithms can be combined with other methods [Coh00] in order to obtain more efficient algorithms. They are applied to the computation of the ray class group $\mathbf{Cl}_{\mathbf{k}}^{\mathfrak{m}}$ modulo $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_\infty$ denotes a formal product of real infinite places, and also to the computation of conductors of ideal class groups and of discriminants and genera of class fields.

1. Introduction

Let $\mathbf{k}$ be a number field with ring of integers $\mathfrak{o}_{\mathbf{k}}$ and let $\mathfrak{m}_0$ be an ideal of $\mathfrak{o}_{\mathbf{k}}$. We describe how a basis of the multiplicative group $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^*$ can be computed and how the discrete logarithm problem in $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^*$ can be solved.

Let $\prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{m_\mathfrak{p}}$ be the decomposition of $\mathfrak{m}_0$ into a product of prime ideals. Then the unit group $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^*$ of the residue class ring $\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0$ satisfies

$$(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^* \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^{m_\mathfrak{p}})^*.$$

Hence, the computation of $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{m}_0)^*$ is reduced to the computation of all $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^m)^*$. For non-zero prime ideals $\mathfrak{p}$ of $\mathfrak{o}_{\mathbf{k}}$ the completion of $\mathbf{k}$ with respect to the corresponding non-archimedian exponential valuation $v_\mathfrak{p}$ is denoted by $\mathbf{k}_\mathfrak{p}$. Let $\mathfrak{o}_\mathfrak{p}$ denote the valuation ring of $\mathbf{k}_\mathfrak{p}$ with unique maximal ideal $\mathfrak{b}_\mathfrak{p}$. Then

$$(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^m)^* \cong (\mathfrak{o}_\mathfrak{p}/{\mathfrak{b}_\mathfrak{p}}^m)^* \cong (\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^* \times (1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^m) \cong (\mathfrak{o}_{\mathbf{k}}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m).$$

In order to determine $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^m)^*$ we therefore compute $(\mathfrak{o}/\mathfrak{p})^*$ and $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$. Algorithms for the computation of a primitive element of the residue class field $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p})^*$ are contained in the literature, for instance a method by Gauss in [PZ89]. For a survey of algorithms for the discrete logarithm in the finite field $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p})^*$ we refer the reader to [SWD].

In section 3 we present a method for the computation of a basis of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ [Pau96] which is derived from the explicit representation of the principal units (or one-units) of a local field as described in [Has80, chapter 15].

In section 4 we present an algorithm for the computation of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ by H. Cohen, M. Olivier and F. Diaz y Diaz [CDO96, CDO98, Coh00] that exploits the isomorphism

$$(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l) \cong (\mathfrak{p}^k/\mathfrak{p}^l)^+, \text{ for } k \text{ subject to } k \le l \le 2k.$$

They compute successively generators and relations for the groups $(1+\mathfrak{p}^{k_i})/(1+\mathfrak{p}^{l_i})$ with $k_i = 2^i < m, l_i = \min(2^{i+1}, m)$ and combine these.

In section 5 we describe how the $\mathfrak{p}$-adic logarithm and the Artin-Hasse logarithm can be used to solve the discrete logarithm problem. This is described in detail in [Coh00, chapter 4].

In section 6 we present an efficient algorithms for the computation of a basis of the group of principal units and for the discrete logarithm combining methods from sections 3, 4, and 5.

Applications of these algorithms to the computation of ray class groups, their conductors, and the discriminants and signatures of the respective ray class fields are presented in sections 7 and 8. They are also an important tool in the computation of ray class fields [Fie00, Coh00].

In section 9 we describe the respective algorithms in the case where $\mathbf{k}$ is a global function field.

2. Notation

Throughout the paper a finite 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 $M \in \mathbb{Z}^{m\times n}$ of rank m, such that $v^T g = 0$ for $v \in \mathbb{Z}^m$ if and only if v 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 $a = v^{\mathrm{T}} g$. If $g_1, \ldots, g_m$ is a basis of G, M is usually a diagonal matrix. Algorithms for calculations with finite abelian groups can be found in [Coh00] and [Sim94]. If G is a multiplicative abelian group, then $v^{\mathrm{T}} g$ is an abbreviation for $g_1^{v_1} \cdots g_m^{v_m}$.

We denote the degree of $\mathbf{k}$ over $\mathbb{Q}$ by n. We denote an integral basis of the ring of integers $\mathfrak{o}_{\mathbf{k}}$ of $\mathbf{k}$ by a vector $w \in \mathfrak{o}_{\mathbf{k}}{}^n$. A matrix representation of an ideal $\mathfrak{a} \subset \mathfrak{o}_{\mathbf{k}}$ is a matrix $A \in \mathbb{Z}^{n\times n}$ such that Aw is a $\mathbb{Z}$ basis of $\mathfrak{a}$. If $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}$ is a prime ideal we write e for the ramification index and f for the inertia degree of $\mathfrak{p}$.

For the complexity considerations we fix the following notations. Let R be a ring and $\mathfrak{a}$ an ideal of R.

- We denote by $\mathsf{M}_{\mathfrak{a}}$ the number of bit operations needed for multiplying two elements in R modulo $\mathfrak{a}$.
- Let $a, b \in R$. The number of bit operations needed for finding an element $q \in R$ with $a \equiv q \cdot b \bmod \mathfrak{a}$ is denoted by $\mathsf{D}_{\mathfrak{a}}$.
- The number of bit operations for multiplying a $k \times l$-matrix with a $l \times m$-matrix over a ring R is denoted by $\mathsf{M}_R(k, l, m)$.
- Denote by $\mathsf{T}_R(n)$ the number of bit operations required for triangularizing a $n \times n$ matrix over the ring R.
- Let A be a matrix in $\mathbb{Z}^{n\times n}$ whose coefficients are bounded by a. We denote by S_a the number of bit operations needed to compute the Smith Normal Form S of A and transformation matrices T_L and T_R such that $S = T_L A T_R$.

3. Principal Units

In the sequel we present several results about principal units (also called one-units), for details we refer to [Has80, chapter 15], and apply these to the computation of the multiplicative group of residue class rings [Pau96]. We assume that p is the unique rational prime contained in $\mathfrak{p}$. An element $\eta_\nu \in 1 + \mathfrak{b}_{\mathfrak{p}}$ is called a principal unit of level ν, iff $\eta_\nu \equiv 1 \bmod {\mathfrak{b}_\mathfrak{p}}^\nu$. Every principal unit $\eta \in 1+\mathfrak{b}_\mathfrak{p}$ has a unique representation $\eta = \prod_{\nu=1}^{\infty}(1+a_\nu\pi^\nu)$, where the a_ν are from a fixed set of representatives of $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ and $\pi \in \mathfrak{p}\setminus\mathfrak{p}^2$. The groups $(1+{\mathfrak{b}_\mathfrak{p}}^m)/(1+{\mathfrak{b}_\mathfrak{p}}^{m+1})$ are isomorphic to $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+$.

The p-th power rule yields that the p-th powers of principal units generators of a level are generators for principal units of further levels.

Theorem 3.1 (p-th power rule)**.** *Let e be the ramification index of $\mathfrak{b}_\mathfrak{p}$ and $\eta_\nu \equiv 1+a\pi^\nu \bmod {\mathfrak{b}_\mathfrak{p}}^{\nu+1}$, where a is in $\mathfrak{o}_\mathfrak{p}$. Let $p=-\pi^e\varepsilon$ be the factorisation of p where ε is a unit. Then the p–th power of η_ν satisfies*

$$\eta_\nu^p \equiv \begin{cases} 1 & + \quad a^p\pi^{p\nu} & \bmod^* & {\mathfrak{b}_\mathfrak{p}}^{p\nu+1} & \text{if} & \nu < \frac{e}{p-1}\ , \\ 1 & + \quad (a^p-\varepsilon a)\pi^{p\nu} & \bmod^* & {\mathfrak{b}_\mathfrak{p}}^{p\nu+1} & \text{if} & \nu = \frac{e}{p-1}\ , \\ 1 & - \quad \varepsilon a\pi^{\nu+e} & \bmod^* & {\mathfrak{b}_\mathfrak{p}}^{\nu+e+1} & \text{if} & \nu > \frac{e}{p-1}\ . \end{cases}$$

The maps $h_1 : a+\mathfrak{b}_\mathfrak{p} \longmapsto a^p+\mathfrak{b}_\mathfrak{p}$ and $h_3 : a+\mathfrak{b}_\mathfrak{p} \longmapsto -\varepsilon a+\mathfrak{b}_\mathfrak{p}$ are automorphisms of $(\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p})^+$, whereas $h_2 : a+\mathfrak{b}_\mathfrak{p} \longmapsto a^p-\varepsilon a+\mathfrak{b}_\mathfrak{p}$ is in general only a homomorphism.

This has the following consequence. If $\eta_{1\nu},\ldots,\eta_{f\nu}$ is a system of generators for the level $\nu < \frac{e}{p-1}$ (for the level $\nu > \frac{e}{p-1}$), then $\eta_{1\nu}^p,\ldots,\eta_{f\nu}^p$ is a system of generators for the level $p\nu$ (for the level $\nu+e$). Levels based on the level $\nu = \frac{e}{p-1}$ need to be discussed separately.

Lemma 3.2. *The kernel of h_2 is of order 1 or p.*

The systems of generators for the levels $\nu \geq \frac{e}{p-1}+e = \frac{pe}{p-1}$ are obtained from the systems of generators for the levels $\nu' < \frac{pe}{p-1}$. The systems of generators for the levels ν with $p \mid \nu$ are obtained from systems of generators for lower levels. We define the set of fundamental levels F_e of $\mathfrak{b}_\mathfrak{p}$ by

$$F_e := \left\{\nu \mid 0<\nu<\tfrac{pe}{p-1}, p\nmid\nu\right\}.$$

All levels can be obtained from the fundamental levels via the substitutions presented above. Note that the cardinality of F_e is e.

The next statement is deduced from the basis representation of the principal units in Hasse's book [Has80, p. 238]. The proof also gives an algorithm for solving the discrete logarithm problem in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$.

Theorem 3.3 (Basis Representation, case I)**.** *If*

i.) $(p-1)$ *does not divide e or*
ii.) h_2 *is an isomorphism or*
iii.) $m < \frac{e}{p-1}$ *holds,*

then the class $[\eta] \in (1+\mathfrak{b}_\mathfrak{p})/(1+{\mathfrak{b}_\mathfrak{p}}^m)$ has the basis representation

$$[\eta] = \prod_{\nu\in F_e}\prod_{i=1}^{f}[\eta_{i\nu}]^{a_{i\nu}} \quad (0 \leq a_{i\nu} < \operatorname{ord}([\eta_{i\nu}]))\ .$$

The $\eta_{i\nu}$ are given in the form $\eta_{i\nu} = 1 + \omega_i\pi^\nu$ for a fixed set of representatives of a $\mathbb{Z}/p\mathbb{Z}$ - basis $\omega_1, \dots, \omega_f$ of $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$. The order of $\eta_{i\nu}$ is $\operatorname{ord}([\eta_{i\nu}]) = p^{s_\nu}$ with

$$\begin{aligned}
s_\nu &= \begin{cases} 0, & \nu \geq m \\ s_{1\nu} + s_{2\nu} + 1, & \nu < m \end{cases} \\
s_{1\nu} &= \begin{cases} \lfloor \log_p \frac{m-1}{\nu} \rfloor, & m \leq \frac{pe}{p-1} \\ \lfloor \log_p \frac{pe}{\nu(p-1)} \rfloor, & m > \frac{pe}{p-1} \end{cases} \\
s_{2\nu} &= \begin{cases} 0, & m \leq \frac{pe}{p-1} \\ \lfloor \frac{m-1-\nu^{s_{1\nu}}}{e} \rfloor, & m > \frac{pe}{p-1}. \end{cases}
\end{aligned}$$

Proof. We begin by computing the orders of the $\eta_{i\nu}$ and show that we have a basis representation afterwards.

If $\nu \geq m$, then $\operatorname{ord}([\eta_{i\nu}]) = 1$ holds. For $\nu < m \leq \frac{pe}{p-1}$ the generators of the fundamental level $\nu \in F_e$ are generators of the levels $p^{s_1}\nu$, where $s_1 \in \mathbb{Z}^{>0}$ with $p^{s_1}\nu < m$.

We now look for the maximal $s_{1\nu}$ fulfilling the last inequality. With $p^{s_{1\nu}}\nu \leq m-1$ we get $s_{1\nu} = \lfloor \log_p(\frac{m-1}{\nu}) \rfloor$. Hence $p^{s_{1\nu}}\nu$ is the maximal level $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$ for which $\eta_{i\nu}$ is a system of generators. With the p-th power rule and the choice of $s_{1\nu}$ we get $\eta_{i\nu}^{p^{s_{1\nu}+1}} \equiv 1 \bmod {\mathfrak{b}_\mathfrak{p}}^m$. Hence the order of the class $[\eta_{i\nu}]$ in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^m)$ is $p^{s_{1\nu}+1}$.

For $m > \frac{pe}{p-1}$ the $\eta_{i\nu}$ are the generators of the levels $p^{s_1}\nu + s_2 e$ where $s_1, s_2 \in \mathbb{Z}^{>0}$ satisfy $p^{s_1}\nu + s_2 e < m$ and $p^{s_1}\nu < \frac{pe}{p-1}$. We are looking for the maximal level, whose generators are p-th powers of $\eta_{i\nu}$. As above $s_{1\nu}$ is calculated for $m = \frac{pe}{p-1}$. Then $p^{s_{1\nu}}\nu + s_2 e \leq m - 1$ holds and we get $s_{2\nu} = \lfloor \frac{m-1-p^{s_{1\nu}}\nu}{e} \rfloor$ for the maximal $s_{2\nu}$ for which the inequality holds. As above the order of $[\eta_{i\nu}]$ is increased by a power of p and we obtain $s_\nu = s_{1\nu} + s_{2\nu} + 1$.

We show by induction on m that we indeed have a basis representation. Let $\omega_1, \dots, \omega_f$ be fixed representatives $\mathbb{Z}/p\mathbb{Z}$-basis of $\mathfrak{o}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$ and $\eta \in 1 + \mathfrak{b}_\mathfrak{p}$. We denote the class of η in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^k)$ by $[\eta]_k$.

We start with the case $(p-1) \nmid e$. The class of η in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^2)$ has the basis representation

$$\eta \equiv \prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i\pi^\nu)^{a_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^2 \quad \left(0 \leq a_{i\nu} < \operatorname{ord}([1 + \omega_i\pi^\nu]_1) = \begin{cases} 1, & \nu \neq 1 \\ p, & \nu = 1 \end{cases}\right).$$

Next we assume that the basis representation of $[\eta]_k$ in $(1 + \mathfrak{b}_\mathfrak{p})/(1 + {\mathfrak{b}_\mathfrak{p}}^k)$ is known for $k < m$:

$$\eta \equiv \prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i\pi^\nu)^{a_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^k \;\; (0 \leq a_{i\nu} < \operatorname{ord}([1 + \omega_i\pi^\nu]_k)).$$

We construct $b_{11}, \dots, b_{fe}$ satisfying

$$\eta \equiv \prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i\pi^\nu)^{b_{i\nu}} \bmod {\mathfrak{b}_\mathfrak{p}}^{k+1} \;\; (0 \leq b_{i\nu} < \operatorname{ord}([1 + \omega_i\pi^\nu]_{k+1})).$$

Let $\nu' \in F_e$ be the fundamental level for k. There exist s_1, s_3 with $s_1 = \max\{s \in \mathbb{Z} \mid \nu' p^s < \min(k, \frac{pe}{p-1})\}$ and $k = \nu' p^{s_1} + s_3 e$. Then

$$\eta' = \frac{\eta}{\prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i \pi^{\nu})^{a_{i\nu}}}$$

is a principal unit of level k. Let $\omega'_1, \ldots, \omega'_f$ subject to $\omega'_i = h_3^{s_3}(h_1^{s_1}(\omega_i))$. There exist $c_1, \ldots, c_f$ with $0 \le c_i < p$ with

$$\eta' \equiv \prod_{i=1}^{f} (1 + \omega'_i \pi^k)^{c_i} \bmod \mathfrak{b}_{\mathfrak{p}}{}^{k+1} \quad .$$

Hence, we obtain

$$\eta \equiv \prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i \pi^{\nu})^{a_{i\nu}} \prod_{i=1}^{f} (1 + \omega'_i \pi^k)^{c_i} \bmod \mathfrak{b}_{\mathfrak{p}}{}^{k+1} \quad .$$

The ω_i were chosen to satisfy $(1 + \omega_i \pi^{\nu'})^{p^{s_1+s_2}} \equiv (1 + \omega'_i \pi^k) \bmod \mathfrak{b}_{\mathfrak{p}}{}^{k+1}$, and we conclude

$$\prod_{i=1}^{f} (1 + \omega'_i \pi^k)^{c_i} \equiv \prod_{i=1}^{f} (1 + \omega'_i \pi^{\nu'})^{c_i p^{s_1+s_2}} \bmod \mathfrak{b}_{\mathfrak{p}}{}^{k+1}.$$

With $b_{i\nu} := \begin{cases} a_{i\nu}, & \nu \neq \nu' \\ a_{i\nu} + c_i p^{s_1+s_2}, & \nu = \nu' \end{cases}$ we finally get the representation

$$\eta \equiv \prod_{\nu \in F_e} \prod_{i=1}^{f} (1 + \omega_i \pi^{\nu})^{b_{i\nu}} \bmod \mathfrak{b}_{\mathfrak{p}}{}^{k+1} \quad \left(0 \le b_{i\nu} < \begin{cases} \operatorname{ord}([1 + \omega_i \pi^{\nu}]_k), & \nu \neq \nu' \\ p \operatorname{ord}([1 + \omega_i \pi^{\nu}]_k), & \nu = \nu' \end{cases} \right).$$

The generators of the level ν' are the generators of the new level k. It follows from the p-th power rule that the order of $(1 + \omega_i \pi^{\nu'})$ increases by the factor p and that the orders of the other generators do not change.

In case $(p-1) \mid e$ the proof is analogous, we just need to use a different isomorphism, $h_2 : \omega \mapsto p\omega - \varepsilon\omega$, to proceed from level $\frac{e}{p-1}$ to level $\frac{pe}{p-1}$. □

Proposition 3.4. *In case I (see theorem 3.3) a basis of* $(1 + \mathfrak{p})/(1 + \mathfrak{p})^m$ *can be computed in* $O\big(ef \log \frac{pe}{p-1} \mathsf{M}_{\mathfrak{p}^m}\big)$ *bit operations.*

The multiplicative groups $(1 + \mathfrak{b}_{\mathfrak{p}})/(1 + \mathfrak{b}_{\mathfrak{p}}{}^m)$ and $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$ are isomorphic and since we chose π and $\omega_1, \ldots, \omega_f$ in $\mathfrak{o}_{\mathbf{k}}$, the generators of $(1 + \mathfrak{b}_{\mathfrak{p}})/(1 + \mathfrak{b}_{\mathfrak{p}}{}^m)$ are generators of $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$.

Hence a basis of the group $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$ can be computed easily if $(p-1)$ does not divide e or h_2 is an isomorphism or $m < \frac{e}{p-1}$ holds. The proof of theorem 3.3 above yields an algorithm for solving the discrete logarithm problem in $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$.

Algorithm 3.5 (Discrete logarithm, principal units, case I)**.**

```
Input:   $\eta \in 1 + \mathfrak{p}$, $\mathfrak{o}_{\mathbf{k}}$, $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}$, $e$, $f$, $p$, $m \in \mathbb{Z}^{>0}$, a basis $(\eta_{11}, \ldots, \eta_{fe})$ of
         $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$ and a system of representatives $(\omega_1, \cdots, \omega_n)$ of
         a $\mathbb{Z}/p\mathbb{Z}$-basis of $\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}$ in $\mathfrak{o}_{\mathbf{k}}$ as in theorem 3.3.
Output:  $a \in \mathbb{Z}^{ef}$ such that $[a^T(\eta_{11}, \ldots, \eta_{fe})] = [\eta]$.
    ∘ Set $a \leftarrow 0 \in \mathbb{Z}^{fe}$.
    ∘ For all levels $1 \le \nu < m$ do:
        ∘ Find base level $\nu'$ of $\nu$.
        ∘ Compute the number of substitutions $s_1, s_2, s_3$.
        ∘ Set $\omega_i' \leftarrow h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$ for $i = 1, \dots, f$.
        ∘ Find $c_1, \dots, c_f$, such that $(\eta - 1)/\pi^\nu \equiv \sum_{i=1}^f c_i\omega_i' \bmod \mathfrak{p}$.
        ∘ Replace $a_{1\nu'} \leftarrow a_{1\nu'} + p^{s_1+s_2+s_3}c_1, \dots, a_{f\nu'} \leftarrow a_{f\nu'} + p^{s_1+s_2+s_3}c_f$.
        ∘ Replace $\eta \leftarrow \eta / \prod_{i=1}^f \eta_{i\nu'}^{p^{s_1+s_2+s_3}c_i}$.
    ∘ Return $a$.
```

For each computation of the discrete logarithm with algorithm 3.5 the values $h_3^{s_3}(h_2^{s_2}(h_1^{s_1}(\omega_i)))$ and $\eta_{i\nu}^{p^{s_1+s_2+s_3}}$ have to be computed. This can be done in $O\big(f(mef \log p\mathsf{M}_{\mathfrak{p}^m}\big)$ and $O(m\mathsf{M}_{\mathfrak{p}^m})$ bit operations respectively.

Assuming the data above is known algorithm 3.5 returns the discrete logarithm of $\eta \in (1+\mathfrak{p})/(1+\mathfrak{p})^m$ in $O\big(m(\mathsf{D}_{\mathfrak{o}_\mathbf{k}}^{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{F}_p}(f) + f \log p \cdot \mathsf{M}_{\mathfrak{p}^m})\big)$ bit operations.

If $(p-1)$ divides e and h_2 is not an isomorphism the generators of the level $\frac{e}{p-1}$ are not a complete system of generators for the level $\frac{pe}{p-1}$. In order to obtain the generators of the level $e/(p-1)$ the substitution h_1 is applied p^{μ_0-1} times to the generators of the fundamental step e_0 where $p^{\mu_0-1}(p-1)e_0 = e$ and p does not divide e_0. Since the order of the kernel of h_2 is p in this case, we can find a $\mathbb{Z}/p\mathbb{Z}$ - basis $\omega_1, \dots, \omega_f$ with $\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv 0 \bmod \mathfrak{p}$, so that $\omega_1^{p^{\mu_0}}$ generates the kernel of h_2. To complete the system of generators for the level $\frac{pe}{p-1}$, we introduce an additional generator ω_* of $\mathfrak{o}_\mathbf{k}/\mathfrak{p}$ which is not contained in the image of h_2. If $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ has no solution, then ω_* is not contained in the image of h_2.

Theorem 3.6 (Unique Representation, case II)**.** *Let $(p-1) \mid e$ and h_2 not be an isomorphism. Choose e_0 and μ_0 such that $e = p^{\mu_0-1}(p-1)e_0$ and p does not divide e_0. Let $\omega_1, \dots, \omega_f$ be a $\mathbb{Z}/p\mathbb{Z}$ - basis of $\mathfrak{o}_\mathbf{k}/\mathfrak{p}$ in $\mathfrak{o}_\mathbf{k}$ subject to $\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv$* $0 \bmod \mathfrak{p}$. *Choose $\omega_* \in \mathfrak{o}_\mathbf{k}$ such that $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}$ has no solution. Then the class $[\eta] \in (1+\mathfrak{p})/(1+\mathfrak{p}^m)$ has the unique representation*

$$[\eta] = \prod_{\nu \in F_e} \prod_{i=1}^{f} [\eta_{i\nu}]^{a_{i\nu}} [\eta_*]^{a_*} \quad \left(\begin{array}{ccccl} 0 & \le & a_{1e_0} & < & p^{\mu_0} \\ 0 & \le & a_{i\nu} & < & \mathrm{ord}([\eta_{i\nu}]) \quad \textit{for } (i,\nu) \neq (1, e_0) \\ 0 & \le & a_* & < & \mathrm{ord}([\eta_*]) \end{array} \right)$$

with $\eta_{i\nu} = 1 + \omega_i\pi^\nu$ and $\eta_* = 1 + \omega_*\pi^{p^{\mu_0}e_nul}$. The corresponding orders are $\mathrm{ord}([\eta_{i\nu}]) = p^{s_\nu}$ *for $(i,\nu) \neq (1, e_0)$ and* $\mathrm{ord}([\eta_*]) = p^{s_*+1}$*, respectively, where $s_* = \lfloor \frac{m-1-p^{\mu_0}e_0}{e} \rfloor$ and s_ν is as defined in theorem* 3.3.

Proof. By the choice of ω_1 and ω_* the representation is unique. The order of $[\eta_*]$ is obtained as follows. e_0 and μ_0 were chosen subject to $\frac{pe}{p-1} = p^{\mu_0}e_0$, therefore $\eta_* = 1 + \omega_0\pi^{p^{\mu_0}e_0}$ is a principal unit of level $p^{\mu_0}e_0$. The p-th powers of $[\eta_*]$ are contained in the systems of generators of the levels $p^{\mu_0}e_0 + se$. The maximal non–negative s satisfying $p^{\mu_0}e_0 + se \le m - 1$ is $s_* = \lfloor \frac{m-1-p^{\mu_0}e_0}{e} \rfloor$. □

We remark that we do not necessarily get a basis representation, since the order of η_{1e_0} is in general not p^{μ_0}. However, in many cases the unique representation is a basis representation.

Corollary 3.7 (Basis Representation, case IIa)**.** *If $(p-1) \mid e$ and the kernel of h_2 is not trivial and*

i.) *$p \le 3$ and $m \le 2e$ or*
ii.) *$p > 3$ and $(p-1)m \le (p+1)e$,*

the unique representation in theorem 3.6 *is a basis representation. In that case we have* $\mathrm{ord}([\eta_{1e_0}]) = p^{\mu_0}$.

Proof. Let $\nu = \frac{e}{p-1} = p^{\mu_0-1}e_0$ and $\eta = \eta_{1e_0}^{p^{\mu_0-1}} = (1+\omega_1\pi^{e_0})^{p^{\mu_0-1}}$, then $\eta \equiv 1 + a\pi^\nu \bmod \mathfrak{p}^{\nu+1}$ holds. We determine the maximal exponent m for which the congruence $\eta^p \equiv 1 \bmod \mathfrak{p}^m$ holds. With the p-th power rule and the choice of ω_1 we get $\eta^p \equiv 1 \bmod \mathfrak{p}^{p\nu+1}$. Comparing the summands with larger powers of p, the proof of the p-th power rule in [Has80, p. 229] shows that

$$m \leq \min(2\nu + e, (p-1)\nu + e) \ .$$

□

In the unique representation of η_{1e_0} the exponent a_{1e_0} was bounded by $a_{1e_0} < p^{\mu_0}$. We can represent $\eta_{1e_0}^{p^{\mu_0}}$ by the other generators and get a relation $[\eta_{1e_0}^{p^{\mu_0}}] = \prod_{i\in F_e}\prod_{j=1}^{f}[\eta_{ij}]^{a_{ij}}[\eta_*]^{a_*}$ with $a_{1e_0} = 0$. From this relation and the (known) orders of the other generators a basis of the group $(1+\mathfrak{p})/(1+\mathfrak{p})^m$ can be derived by computing the Smith Normal Form of the relation matrix.

A unique representation of an element in $(1+\mathfrak{p})/(1+\mathfrak{p})^m$ can be obtained easily with a slightly modified version of algorithm 3.5. If the base level ν' of a level ν is e_0 and $\nu \geq pe/(p-1)$ then ω_1' is set to $h_3^{s_3}(\omega_*)$ and the vector a representing a up to level ν has to be altered accordingly (note that $a \in \mathbb{Z}^{fe+1}$ in this case).

To obtain a set of generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ in case II and case IIa the elements ω_1 and ω_* must be computed. Denote by Q the matrix representing the Frobenius automorphism $x \mapsto x^p$ in the finite field $\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}$. Then ω_0 is the p^{μ_0-1}-th root of a nontrivial element from the kernel of $Q - \varepsilon I$ and ω_* can be chosen from $\mathfrak{o}_{\mathbf{k}}/\mathfrak{p} \setminus \mathrm{range(Q - \varepsilon I)}$.

Proposition 3.8. *In case IIa (see corollary 3.7) a basis of* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *can be computed in* $O\big(ef\log\frac{pe}{p-1}\mathsf{M}_{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{F}_p}(f)\big)$ *bit operations. In case II (see theorem 3.6) a set of generators and a relation matrix can be computed in* $O\big(ef\log p(m + \frac{e}{p-1})\mathsf{M}_{\mathfrak{p}^m} + m(\mathsf{D}_{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{F}_p}(f))\big)$ *bit operations.*

Let $\big((\eta_{11}, \ldots, \eta_{fe}, \eta_*), M\big)$ be a representation of $(1+\mathfrak{p})/(1+p^m)$ as given by theorem 3.6. Let $S = T_L M T_R$ be the Smith normal form of M. Then $\big(T_R(\eta_{11}, \ldots, \eta_{fe}, \eta_*)^T\big)^T$ is a basis of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ which can be computed in $O\big((efm\log p + e^2f^2)\mathsf{M}_{\mathfrak{p}}^m\big)$ bit operations.

Proposition 3.9. *In case II a basis of the group* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *can be obtained in* $O\big(ef(m\log p + \frac{e}{p-1}\log p + ef)\mathsf{M}_{\mathfrak{p}^m} + m(\mathsf{D}_{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{F}_p}(f)) + \mathsf{S}(ef)\big)$ *bit operations. The discrete logarithm of an element can be computed in* $O\big(m(\mathsf{D}_{\mathfrak{o}_{\mathbf{k}}}^{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{F}_p}(f) + f\log p \cdot \mathsf{M}_{\mathfrak{p}^m}) + \mathsf{M}(1, ef, ef)\big)$ *bit operations.*

4. Quadratic Methods

The quadratic method by Cohen, Diaz y Diaz, and Olivier [CDO96, CDO98, Coh00] is based on the following fact.

Lemma 4.1. *Let* $\mathbf{k}$ *be an algebraic number field with maximal order* $\mathfrak{o}_{\mathbf{k}}$ *and let* $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}$ *be a prime ideal. If* $l \leq m \leq 2l$ *then*

$$\Psi : (1+\mathfrak{p}^l)/(1+\mathfrak{p}^m) \to (\mathfrak{p}^l/\mathfrak{p}^m)^+, \ [1+a] \mapsto \overline{a}$$

is an isomorphism.

A basis of the additive group $\mathfrak{p}^l/\mathfrak{p}^m$ can be computed easily. Let w be an integral basis of $\mathfrak{o}_{\mathbf{k}}$, let $\mathfrak{p}^l$ and $\mathfrak{p}^m$ where $1 \le l \le m$ be given by the matrices A and B, so that $w_l = Aw$ (respectively $w_m = Bw$) is a $\mathbb{Z}$-basis of $\mathfrak{p}^l$ (respectively $\mathfrak{p}^m$). The matrix BA^{-1} represents the elements of $\mathfrak{p}^m$ by the elements of $\mathfrak{p}^l$, as $w_m = BA^{-1}Aw = BAw_l$ Thus BA^{-1} is the matrix of relations of the additive group $\mathfrak{p}^l/\mathfrak{p}^m$ and the components of w_l are its generators. Hence $\mathfrak{p}^l/\mathfrak{p}^m$ is represented by (w_l, BA^{-1}). If $w_l = (w_{l1}, \cdots, w_{ln})^T$ we get the representation

$$(g, M) := \left(\begin{pmatrix} 1 + w_{l1} \\ \vdots \\ 1 + w_{ln} \end{pmatrix}, BA^{-1} \right)$$

for $(1 + \mathfrak{p}^l)/(1 + \mathfrak{p}^m)$ by generators and relations.

In order to obtain a representation of $[b] \in (1 + \mathfrak{p}^l)/(1 + \mathfrak{p}^m)$ by g we need to find $a = (a_1, \cdots, a_n)$ with $[b - 1] = [\sum_{i=1}^n a_i w_{li}]$, then $[b] = [\prod_{i=1}^n (1 + w_l i)^{a_i}]$ holds by lemma 4.1. Let $b \in \mathbb{Z}^n$ with $b - 1 = bw$, then $bw = aAw$. A solution $a \in \mathbb{Z}^n$ of the equation $b = aA$ gives the desired representation.

Let k, l, m with $k \le l \le m$ and $l \le m \le 2l$ be given. Denote the class $1 + a$ modulo $(1 + \mathfrak{p}^j)$ by $[1 + a]_j$.

By the isomorphism theorem the sequence

$$\begin{tikzcd} 1 \arrow[r] & (1+\mathfrak{p}^l)/(1+\mathfrak{p}^m) \arrow[r, "\Psi"] & (1+\mathfrak{p}^k)/(1+\mathfrak{p}^m) \arrow[r, "\Phi"] & (1+\mathfrak{p}^k)/(1+\mathfrak{p}^l) \arrow[r] & 1 \\ & {[1+a]_m} \arrow[r, mapsto] & {[1+a]_m} \arrow[r, mapsto] & {[1+a]_l.} & \end{tikzcd}$$

is exact.

By the definition of the map Φ we have $\Phi([h]_m) = [h]_l$. We are looking for a matrix P with $N[h]_m = P\Psi([g]_m)$. We compute the matrix P by applying the method for computing the representation of elements in $(1+\mathfrak{p}^l)/(1+\mathfrak{p}^m)$ to $N[h]_m$. We obtain the representation

$$\left(\begin{pmatrix} h \\ g \end{pmatrix}, \begin{pmatrix} N & -P \\ 0 & M \end{pmatrix} \right).$$

for $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^m)$. In order to compute $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ one computes iteratively

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

where $s = \lfloor \log_2(m) \rfloor$.

Algorithm 4.2 (Generators and relations, quadratic method).

```
Input:   $\mathfrak{o}_{\mathbf{k}}, \mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}, m \in \mathbb{Z}^{>0}$, integral basis $w$ of $\mathfrak{o}_{\mathbf{k}}$
Output:  Generators and relations of $(g, M)$ of $(1 + \mathfrak{p})/(1 + \mathfrak{p}^m)$
    ∘ Compute generators and relations $(h, N)$ of $(1 + \mathfrak{p})/(1 + \mathfrak{p}^2)$:
        ∘ Compute matrix representations $A, B \in \mathbb{Z}^{n \times n}$ of $\mathfrak{p}, \mathfrak{p}^2$.
        ∘ Set $g \leftarrow (g_1, \ldots, g_n)$ with $g_i = 1 + Aw_i$ for $1 \le i \le n$.
        ∘ Set $M \leftarrow BA^{-1}$.
    ∘ Set $k \leftarrow 2$, $s \leftarrow 2$.
    ∘ While $l \ne m$:
        ∘ Set $l \leftarrow \min(2^s, m)$.
        ∘ Compute generators and relations $(h, N)$ of $(1 + \mathfrak{p}^k)/(1 + \mathfrak{p}^l)$:
            ∘ Compute matrix representations $A, B \in \mathbb{Z}^{n \times n}$ of $\mathfrak{p}^k, \mathfrak{p}^l$.
            ∘ Set $h \leftarrow (h_1, \ldots, h_n)$ with $h_i = 1 + Aw_i$ for $1 \le i \le n$.
            ∘ Set $N \leftarrow BA^{-1}$.
        ∘ Compute $P$, such that $Nh = Pg$ using algorithm 4.3 below.
        ∘ Replace $g \leftarrow \begin{pmatrix} h \\ g \end{pmatrix}$, $M \leftarrow \left(\begin{smallmatrix} N & -P \\ 0 & M \end{smallmatrix}\right)$.
        ∘ Set $k \leftarrow l$, $s \leftarrow s+1$.
    ∘ Return $(g, M)$.
```

A representation of the class of $\eta \in \mathfrak{o}_{\mathbf{k}}$ in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ by generators as computed with algorithm 4.2 can be obtained with the following algorithm.

Algorithm 4.3 (Discrete logarithm in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$, quadratic method)**.**

```
Input:  A maximal order $\mathfrak{o}_{\mathbf{k}}$, a integral basis $w = (w_1, \dots, w_n)$ of $\mathfrak{o}_{\mathbf{k}}$, a
        prime ideal $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}$, $m \in \mathbb{N}$, $\eta \in 1+\mathfrak{p}$
Output: $a$ such that $[ag] = [\eta]$, where $g$ is a set of generators of $(1+\mathfrak{p})/(1+$
        $\mathfrak{p}^m)$ as given by algorithm 4.2
    ∘ Set $k \leftarrow 1$, $a \leftarrow (\,)$.
    ∘ While $k \neq m$:
        ∘ Set $l \leftarrow \min(2k, m)$.
        ∘ Discrete logarithm in in $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$:
            ∘ Find $b \in \mathbb{Z}^n$, such that $\eta - 1 = bw$.
            ∘ Let $A \in \mathbb{Z}^{n \times n}$ be a matrix representation of $\mathfrak{p}^k$. Set $c \leftarrow bA^{-1}$.
            ∘ Set $\eta \leftarrow \eta \cdot (\prod_{i=1}^{n}(1+Aw_i)^{c_i})^{-1}$
        ∘ Replace $a \leftarrow (a\ c)$, $k \leftarrow l$.
    ∘ Return $a$.
```

Matrix representations of $\mathfrak{p}$, $\mathfrak{p}^2$ to $\mathfrak{p}^m$ and the inverses of these matrices can be computed in $O\big(\log m(n\mathsf{M}_{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{Z}}(n))\big)$ bit operations. Algorithm 4.3 computes a representation of an element of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ in $O\big(nm\log p\mathsf{M}_{\mathfrak{p}^m} + \log m\mathsf{D}_{\mathfrak{p}^m}\big)$ bit operations. Algorithm 4.2 returns generators and relations of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ in $O\big(n^2 m\log p\mathsf{M}_{\mathfrak{p}^m} + n\log m\mathsf{D}_{\mathfrak{p}^m} + \log m\mathsf{T}_{\mathbb{Z}}(n)\big)$ bit operations including the computation of the data above.

Proposition 4.4. *A basis of the group $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ can be obtained with the number of bit operations being $O\big(nm\log p(n+\log m)\mathsf{M}_{\mathfrak{p}^m} + n\log m\mathsf{D}_{\mathfrak{p}^m} + \log m\mathsf{T}_{\mathbb{Z}}(n)) + \mathsf{S}(n\log m, n\log m)\big)$ and the discrete logarithm can be computed in $O\big(nm\log p\mathsf{M}_{\mathfrak{p}^m} + \log m\mathsf{D}_{\mathfrak{p}^m} + \mathsf{M}(1, n\log m, n\log m)\big)$*

5. $\mathfrak{p}$-adic Logarithms

In this section we present a third approach to the computation of the discrete logarithm in $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$. These methods can also be used for the computation of generators and relations of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ [Coh00, chapter 4].

For levels greater than $e/(p-1)$ the $\mathfrak{p}$-adic logarithm can be used for the computation of the discrete logarithm. Define

$$\log_{\mathfrak{p}}(1+x) := \sum_{i=1}^{\infty}(-1)^{i-1}\frac{x^i}{i} \quad \text{and} \quad \exp_{\mathfrak{p}}(x) := \sum_{i=0}^{\infty}\frac{x^i}{i!}.$$

Proposition 5.1. *Let $\mathfrak{p}$ be a prime ideal over the prime number p with ramification index $e = v_{\mathfrak{p}}(p)$.*

i.) *The expansion for $\log_{\mathfrak{p}}(1+x)$ converges $\mathfrak{p}$-adically if and only if $v_{\mathfrak{p}}(x) \geq 1$.*

ii.) *Let $x, y \in \mathbf{k}$ with $v_{\mathfrak{p}}(x) \geq 1$ and $v_{\mathfrak{p}}(y) \geq 1$ then $\log_{\mathfrak{p}}\big((1+x)(1+y)\big) = \log_{\mathfrak{p}}(1+x)\log_{\mathfrak{p}}(1+y)$.*

iii.) *Let $x \in \mathbf{k}$ with $v_\mathfrak{p}(x) > e/(p-1)$ then $\log_\mathfrak{p}\big(\exp_\mathfrak{p}(x)\big) = x$ and $\exp_\mathfrak{p}\big(\log_\mathfrak{p}(1+x)\big) = 1+x$.*

iv.) *For any integers l and m with $m > l \geq 1 + \lfloor e/(p-1) \rfloor$ the functions $\log_\mathfrak{p}$ and $\exp_\mathfrak{p}$ are inverse isomorphisms between the multiplicative group $(1+\mathfrak{p}^l)/(1+\mathfrak{p}^m)$ and the additive group $\mathfrak{p}^l/\mathfrak{p}^m$.*

Remark 5.2. Assume $v_\mathfrak{p}(x) > e/(p-1)$ and $i = p^s$. Then

$$v_\mathfrak{p}(x^i/i) = v_\mathfrak{p}(x^{p^s}/p^s) = p^s v_\mathfrak{p}(x) - es > p^s e/(p-1) - es > e(p^{s-1} - s).$$

The inequality $e(p^{s-1} - s) > m$ holds if $i = p^s > pm \geq pm/e$. Thus $\log_\mathfrak{p}$ can be approximated by computing the first m summands of the series for $p \nmid i$ and the summands up to $i = pm$ for $p \mid i$.

The $\mathfrak{p}$-adic logarithm modulo $\mathfrak{p}^m$ can be computed in $O(m\mathsf{M}_{\mathfrak{p}^m})$ bit operations.

Artin-Hasse logarithms yield an inductive method for the computation of the group $(1+p)/(1+p^m)$ of the discrete logarithm similar to the quadratic methods in the previous section. The quadratic methods exploited the isomorphisms $(1 + p^k)/(1+p^{2k}) \cong \mathfrak{p}^k/\mathfrak{p}^{2k}$; the Artin-Hasse logarithm gives the isomorphisms $(1 + p^k)/(1+p^{pk}) \cong \mathfrak{p}^k/\mathfrak{p}^{pk}$. Hence less iterations are necessary using the Artin-Hasse logarithm. Define

$$\mathrm{L}(1+x) := \sum_{i=1}^{p-1} (-1)^{i-1}\frac{x^i}{i} \quad \text{and} \quad \mathrm{E}(x) := \sum_{i=0}^{p-1} \frac{x^i}{i!}.$$

Proposition 5.3. *Let $\mathfrak{p}$ be a prime ideal over the prime number p.*

i.) *The nonzero monomials of the polynomial*

$$\mathrm{L}\big((1+x)(1+y)\big) - \mathrm{L}(1+x) - \mathrm{L}(1+y)$$

are of the form $x^k y^l$ with $k + l \geq p$.

ii.) *If $v_\mathfrak{p}(x) = k$ then $\mathrm{E}(\mathrm{L}(1+x)) \equiv 1 + x \bmod \mathfrak{p}^{pk}$.*

iii.) *If $k < l \leq pk$ then the map*

$$(1+\mathfrak{p}^k)/(1+p^l) \to \mathfrak{p}^k/\mathfrak{p}^l,\ (1+x) \mapsto \mathrm{L}(1+x)$$

is a group isomorphism.

6. Computing the Group of Principal Units and the Discrete Logarithm

A major advantage of the basis (respectively unique) representation of the principal units as given in section 3 is that the structure of the group is given directly. In section 8 we will see how the fact that we know which basis elements are generators for which level can be exploited in the computation of conductors of ray class groups and more general ideal class groups. Very few computations are needed for the computation of a basis of the multiplicative group of the residue class ring.

We combine the methods from sections 3, 4, and 5 to a more efficient algorithm. We use the generators given by theorems 3.3 and 3.6, the quadratic methods for the discrete logarithm for levels up to $\frac{pe}{p-1}$; for levels greater than $\frac{pe}{p-1}$ we use the p-adic logarithm for the computation of the discrete logarithm.

The following algorithm is formulated for case I only. A version for case II requires only minor changes.

Algorithm 6.1 (Discrete Logarithm, combined)**.**

```
Input:  $\eta \in 1+\mathfrak{p}$, $\mathfrak{o}_{\mathbf{k}}$, $\mathfrak{p} \subset \mathfrak{o}_{\mathbf{k}}$, $e$, $f$, $p$, $m \in \mathbb{Z}^{>0}$, a basis $(\eta_{11}, \dots, \eta_{fe})$ of
        $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ as in theorem 3.3.
Output: $a \in \mathbb{Z}^{ef}$ such that $[a^T(\eta_{11}, \dots, \eta_{fe})] = [\eta]$.
  ○ Set $k \leftarrow 1$, $a = (a_{11}, \dots, a_{fe}) \leftarrow 0$.
  ○ While $k < \min\{m, \lceil \frac{pe}{p-1} \rceil\}$:
      ○ Set $l \leftarrow \min\{2k, m, \lceil \frac{pe}{p-1} \rceil\}$.
      ○ Compute a basis $\rho_{11} = \eta_{1t_1}^{p^{s_1}}, \dots, \rho_{f1} = \eta_{ft_1}^{p^{s_1}}, \dots, \rho_{fr} = \eta_{ft_r}^{p^{s_t}}$ of
        $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$.
      ○ Find $(c_{11}, \dots, c_{fr}) \in \mathbb{N}$ with $c_{11}(\rho_{11} - 1) + \cdots + c_{fr}(\rho_{fr} - 1) = \eta - 1$.
      ○ Replace $\eta \leftarrow \eta / \prod_{\nu=1}^{r} \prod_{i=1}^{f} \rho_{i\nu}^{c_{i\nu}}$.
      ○ Replace $a_{1t_1} \leftarrow a_{1t_1} + p^{s_1} c_{11}, \dots, a_{ft_r} \leftarrow a_{ft_r} + p^{s_r} c_{rf}$.
      ○ Replace $k \leftarrow l$.
  ○ If $k < m$ then:
      ○ Compute a basis $\rho_{11} = \log_{\mathfrak{p}} \eta_{11}^{p^{s_1}}, \dots, \rho_{f1} = \log_{\mathfrak{p}} \eta_{f1}^{p^{s_1}}, \dots, \rho_{fe} =$
        $\log_{\mathfrak{p}} \eta_{fe}^{p^{s_e}}$ of $\mathfrak{p}^k/\mathfrak{p}^m$.
      ○ Set $\gamma \leftarrow \log_{\mathfrak{p}} \eta$. Find $(c_{11}, \dots, c_{fe}) \in \mathbb{N}$. with $c_{11}\rho_{11} + \cdots + c_{fe}\rho_{fe} = \gamma$.
      ○ Replace $a \leftarrow \big(a_{11} + p^{s_1} c_{11}, \dots, a_{ef} + p^{s_e} c_{fe}\big)$
  ○ Return $a$.
```

The number of basis elements for $(1+\mathfrak{p}^k)/(1+\mathfrak{p}^l)$ which are p-th powers of generators of lower levels is at most $f\frac{pe}{p-1} - ef$. Thus the $\rho_{i\nu}$ for levels less than $\frac{pe}{p-1}$ can be computed in $O\big(\log \frac{pe}{p-1}\big(\frac{pe}{p-1} - e\big)\mathsf{M}_{\mathfrak{p}^m}\big)$ bit operations. The $\rho_{i\nu}$ for levels greater than $\frac{pe}{p-1}$ can be computed in $O\big(ef \log p \mathsf{M}_{\mathfrak{p}^m} + m\mathsf{M}_{\mathfrak{p}^m}\big)$ bit operations. In addition it is convenient to have matrix representations of the ideal $\mathfrak{p}^p, \mathfrak{p}^{p^2}, \dots, \mathfrak{p}^{\frac{pe}{p-1}}, \mathfrak{p}^m$ in order to reduce the representations in $\mathfrak{p}^k/\mathfrak{p}^l$. The matrix representations of these ideals can be computed in $O\big(\log m(n\mathsf{M}_{\mathfrak{p}^m} + \mathsf{T}_{\mathbb{Z}}(n))\big)$ bit operations. Computing the Hermite Normal form of the matrices $(\rho_{11} \ \dots \ \rho fe)$ in advance will speed up the computation of the discrete logarithm, this can be done in $O\big(\log \frac{pe}{p-1} \mathsf{T}_{\mathbb{Z}}(n)\big)$.

Proposition 6.2. *In case I and case IIa (case II) a basis (unique) representation of an element in* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *can be computed in*

$$O\big(\big(m + \log \tfrac{pe}{p-1} ef \log p\big)\mathsf{M}_{\mathfrak{p}^m}\big)$$

bit operations. Assume $m \geq \frac{pe}{p-1}$*. Then in case I and case IIa a basis of* $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *can be computed in*

$$O\big((n \log m + m + ef \log p)\mathsf{M}_{\mathfrak{p}^m} + \log m \mathsf{T}(n)\big)$$

bit operations. In case II a basis of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ *can be computed with the number of bit operations being*

$$O\big((n \log m + m + ef \log p \log \tfrac{pe}{p-1})\mathsf{M}_{\mathfrak{p}^m} + \log m \mathsf{T}(n) + \mathsf{S}(ef)\big).$$

The quadratic method from section 4 is implemented in the computer algebra system PARI/GP [BB$^+$99]. In the computer algebra systems KASH/KANT [Po$^+$00, DF$^+$96] and MAGMA [BC95] a combination of the methods from sections 3 and 4 is used.

7. Computing Ray Class Groups

Let $\mathfrak{m}_0$ be an integral ideal and $\mathfrak{m}_\infty$ a formal product of real infinite places of $\mathbf{k}$. Then $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$ is called a *congruence module.* Let $a^{(i)} \in \mathbb{C}$ be the ith conjugate of $a \in \mathbf{k}$. Multiplicative congruences with respect to a finite place contained in the congruence module are defined by

$$a \equiv 1 \bmod^* \mathfrak{p}^m :\Leftrightarrow v_\mathfrak{p}(a-1) \geq m$$

and for a real infinite place $\mathfrak{p}_\infty^{(i)}$ by

$$a \equiv 1 \bmod^* (\mathfrak{p}_\infty^{(i)})^m :\Leftrightarrow a^{(i)} > 0.$$

Let $\mathbf{I}^\mathfrak{m} := \{\mathfrak{a} \in \mathbf{I_k} \mid \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1\}$ and $\mathbf{H}_\mathfrak{m} := \{(a) \in \mathbf{H_k} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$. Then the ray class group modulo $\mathfrak{m}$ is defined as $\mathbf{Cl}_\mathbf{k}^\mathfrak{m} := \mathbf{I}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}$.

Let $\mathbf{H}^\mathfrak{m} := \{\mathfrak{a} \in \mathbf{H_k} \mid \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1\}\}$, $\mathbf{k}_\mathfrak{m} := \{a \in \mathbf{k} \mid a \equiv 1 \bmod^* \mathfrak{m}\}$, $\mathbf{k}^\mathfrak{m} := \{a \in \mathbf{k} \mid \gcd((a), \mathfrak{m}_0) = 1\}$, $\mathbf{U_k}$ the group of units of $\mathfrak{o}_\mathbf{k}$ and $\mathbf{U}_\mathfrak{m} := \{u \in \mathbf{U_k} \mid u \equiv 1 \bmod^* \mathfrak{m}\}$. We will compute the ray class group $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}$ in the way the following diagram from [Lan94] suggests.

$$\begin{tikzcd}
 & & \mathbf{I}^\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{I_k} \arrow[d, dash] \\
 & \mathbf{k}^\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{H}^\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{H_k} \\
\mathbf{U_k} \arrow[r] \arrow[d, dash] & \mathbf{U_k}\mathbf{k}_\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{H}_\mathfrak{m} & \\
\mathbf{U}_\mathfrak{m} \arrow[r] & \mathbf{k}_\mathfrak{m} & &
\end{tikzcd}$$

We note that corresponding vertical lines represent isomorphisms of factor groups. Horizontal arrows denote natural embeddings.

Algorithm 7.1 (Ray Class Group)**.**

```
Input:   $\mathfrak{o}_\mathbf{k}, \mathbf{U_k}, \mathbf{Cl_k}, \mathfrak{m} = \mathfrak{m}_0\,\mathfrak{m}_\infty$
Output:  $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}$
    ◦ Compute $\mathbf{k}^\mathfrak{m}/\mathbf{k}_\mathfrak{m} \cong (\mathfrak{o}_\mathbf{k}/\mathfrak{m}_0)^* \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}$.
    ◦ Compute $\mathbf{U_k}/\mathbf{U}_\mathfrak{m}$ via the image of $\mathbf{U_k}$ in $\mathbf{k}^\mathfrak{m}/\mathbf{k}_\mathfrak{m}$.
    ◦ Factor $(\mathbf{k}^\mathfrak{m}/\mathbf{k}_\mathfrak{m})$ by $(\mathbf{U_k}/\mathbf{U}_\mathfrak{m})$.
    ◦ Compute generators of $\mathbf{Cl_k}$ which are prime to $\mathfrak{m}_0$.
    ◦ Compute a basis of $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}$.
```

We already described the computation of $(\mathfrak{o}_\mathbf{k}/\mathfrak{m}_0)^*$. For the computation of $\mathbf{k}^\mathfrak{m}/\mathbf{k}_\mathfrak{m}$ we also need generators of $\mathbf{k}^{\mathfrak{m}_\infty}/\mathbf{k}_{\mathfrak{m}_\infty} \cong \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}^{*>0}$. Assume $\mathfrak{m}_\infty = \mathfrak{p}_\infty^{(\nu_1)} \cdots \mathfrak{p}_\infty^{(\nu_s)}$. We are looking for generators ϑ_i of the group $\mathbf{k}^{\mathfrak{m}_\infty}/\mathbf{k}_{\mathfrak{m}_\infty}$ satisfying $\vartheta_i \equiv 1 \bmod^* \mathfrak{m}_0$. The approximation theorem assures the existence of $\vartheta_1, \ldots, \vartheta_s$ subject to

$$\begin{array}{ccll}
\vartheta_j & \equiv & -1 & \bmod^* \mathfrak{p}_\infty^{(\nu_j)} \ , \\
\vartheta_j & \equiv & 1 & \bmod^* \mathfrak{p}_\infty^{(\nu_i)}, \quad i = 1, \ldots, s, \quad i \neq j \ , \\
\vartheta_j & \equiv & 1 & \bmod^* \mathfrak{m}_0 \ .
\end{array}$$

Let $a_1, \ldots, a_n$ be a basis of $\mathfrak{m}_0$, and let $\mathbf{x} \in \mathbb{Z}^n$ be a solution of the system of inequalities

$$\begin{array}{rcl}
1 + x_1 a_1^{(\nu_j)} + \cdots + x_n a_n^{(\nu_j)} & < & 0 \\
1 + x_1 a_1^{(\nu_i)} + \cdots + x_n a_n^{(\nu_i)} & > & 0, \quad i = 1, \ldots, s, \quad i \neq j \ .
\end{array}$$

Then $\vartheta_j = \mathbf{x}(a_1, \ldots, a_n)^{\mathrm{T}}$ fulfils the congruences listed above. To obtain $\mathbf{x}$ we solve a system of linear equations

$$\begin{array}{rcl} 1 + \bar{x}_1 a_1^{(\nu_j)} + \cdots + \bar{x}_n a_n^{(\nu_j)} & = & -a \\ 1 + \bar{x}_1 a_1^{(\nu_i)} + \cdots + \bar{x}_n a_n^{(\nu_i)} & = & a, \quad i = 1, \ldots, s, \ i \neq j \end{array}$$

for $a := \frac{1}{2}\sum_{i=1}^{n} |a_i|$. From the real solution $\bar{\mathbf{x}}$ of that system we then obtain $\mathbf{x}$ by rounding all coordinates to their closest integer: $x_i = \lfloor \bar{x}_i \rceil \ (1 \leq i \leq s)$.

We compute the group $\mathbf{U}/\mathbf{U}_{\mathfrak{m}}$ via the image of $\mathbf{U}$ in $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. For this we calculate the images of a system of generators of $\mathbf{U}$ in $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. Then the factor group of the finite groups $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$ and $\mathbf{U}/\mathbf{U}_{\mathfrak{m}}$ is calculated by computing a normal form for the matrix of relations for the generators as outlined in [CDO96].

Algorithms for the computation of class groups of algebraic number fields are presented in [Coh93], [Hes96], and [PZ89]. Generators of the class group which are prime to $\mathfrak{m}_0$ are easily calculated by algorithm 7 in [Coh96]. It remains to compute the factor group of $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}}$ and $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ to get $\mathbf{Cl}_{\mathbf{k}}^{\mathfrak{m}} = \mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$.

8. Computing Conductors, Discriminants and Signatures

Let $\mathfrak{m}$ be a congruence module and $\mathbf{Cl}_{\mathbf{k}}^{\mathfrak{m}} = \mathbf{I}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ be the ray class group modulo $\mathfrak{m}$. Let $\mathbf{J}_{\mathfrak{m}}$ be an *ideal group* which can be defined with $\mathfrak{m}$, i.e. which satisfies $\mathbf{I}^{\mathfrak{m}} \supset \mathbf{J}_{\mathfrak{m}} \supset \mathbf{H}_{\mathfrak{m}}$

The conductor $\mathfrak{f}$ of an ideal group is the smallest congruence module $\mathfrak{f}$ with which that ideal group can be defined.

In the sequel we explain how to calculate conductors of ray class groups. It is clear from the diagram of the previous section that we do not need to compute the entire ray class group. It clearly suffices to compute $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}} \cong (\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}})/(\mathbf{U}/\mathbf{U}_{\mathfrak{m}})$. An ideal group, which can be defined with $\mathfrak{m}_1$ and with $\mathfrak{m}_2$, can also be defined with $\gcd(\mathfrak{m}_1, \mathfrak{m}_2)$. Hence, if for each $\mathfrak{p} \mid \mathfrak{m}$ the integer $j_{\mathfrak{p}}$ is the largest exponent such that $\mathfrak{n}_{\mathfrak{p}} = \mathfrak{m}/\mathfrak{p}^{j_{\mathfrak{p}}}$ is integral and that $\mathbf{H}^{\mathfrak{n}_{\mathfrak{p}}}/\mathbf{H}_{\mathfrak{n}_{\mathfrak{p}}} = \mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$, then $\mathfrak{f}$ is is the greatest common divisor of all these $\mathfrak{n}_{\mathfrak{p}}$. We determine $j_{\mathfrak{p}}$ as the largest integer i for which the groups $\mathbf{H}^{\mathfrak{m}}/\mathbf{H}_{\mathfrak{m}}$ and $\mathbf{H}^{\mathfrak{m}/\mathfrak{p}^i}/\mathbf{H}_{\mathfrak{m}/\mathfrak{p}^i}$ still coincide.

It can be easily deduced from theorems 3.3 and 3.6 that for any prime ideal $\mathfrak{p}$ and any $k > 0$ the same representatives for the classes of generators can be used for $\mathbf{k}^{\mathfrak{p}^k}/\mathbf{k}_{\mathfrak{p}^k}$ and $\mathbf{k}^{\mathfrak{p}^{k-1}}/\mathbf{k}_{\mathfrak{p}^{k-1}}$. With respect to basis representations of $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^k)^*$ we only need to change the orders of the generators to get a basis for $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^{k-1})^*$. In the case of a unique representation, also the relation for $\eta_{1e_0}^{p^{\mu_0}}$ must be replaced by the order of η_{1e_0} in the step from level $k = \frac{pe}{p-1}$ to level $k - 1 = \frac{pe}{p-1} - 1$.

Since the same representatives for the classes of generators of $\mathbf{k}^{\mathfrak{p}^k}/\mathbf{k}_{\mathfrak{p}^k}$ and $\mathbf{k}^{\mathfrak{p}^{k-1}}/\mathbf{k}_{\mathfrak{p}^{k-1}}$ can be chosen, the representation of the image of the generators of $\mathbf{U}$ by the generators of $\mathbf{k}^{\mathfrak{p}^k}/\mathbf{k}_{\mathfrak{p}^k}$ is a representation by the generators of $\mathbf{k}^{\mathfrak{p}^{k-1}}/\mathbf{k}_{\mathfrak{p}^{k-1}}$ as well. So the relation matrix of $(\mathbf{k}^{\mathfrak{p}^{k-1}}/\mathbf{k}_{\mathfrak{p}^{k-1}})/(\mathbf{U}/\mathbf{U}_{\mathfrak{p}^{k-1}})$ can be derived from the relation matrix of $(\mathbf{k}^{\mathfrak{p}^k}/\mathbf{k}_{\mathfrak{p}^k})/(\mathbf{U}/\mathbf{U}_{\mathfrak{p}^k})$ by a simple change of the orders of the generators and, in the case of a unique representation, also by replacing the relation for η_{1e_0} as described above.

The same can be done for $(\mathbf{k}^{\mathfrak{n}}/\mathbf{k}_{\mathfrak{n}})/(\mathbf{U}/\mathbf{U}_{\mathfrak{n}})$ and $(\mathbf{k}^{\mathfrak{n}/\mathfrak{p}}/\mathbf{k}_{\mathfrak{n}/\mathfrak{p}})/(\mathbf{U}/\mathbf{U}_{\mathfrak{n}/\mathfrak{p}})$ since they are direct products of groups $(\mathfrak{o}_{\mathbf{k}}/\mathfrak{p}^k)^*$ and the corresponding groups for the infinite places. A comparison can easily be carried out via the Hermite normal forms of the corresponding relation matrices. It is even faster to consider the diagonal elements of the Hermite normal form of the first relation matrix and to determine whether the changed orders for the second matrix change the Hermite normal form. The infinite places are treated similarly.

Let $\mathbf{J}_\mathfrak{m}$ be an ideal group defined with $\mathfrak{m}$. For $\mathfrak{n} \mid \mathfrak{m}$ let Φ denote the surjection from $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}$ to $\mathbf{Cl}_\mathbf{k}^\mathfrak{n}$. For the computation of the conductor of $\mathbf{I}^\mathfrak{m}/\mathbf{J}_\mathfrak{m}$ we use that $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}/(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m}) \cong \mathbf{I}^\mathfrak{m}/\mathbf{J}_\mathfrak{m}$. For $\mathbf{Cl}_\mathbf{k}^\mathfrak{n}/\Phi(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m}) = \mathbf{Cl}_\mathbf{k}^\mathfrak{m}/(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m})$ the ideal class group $\mathbf{I}^\mathfrak{m}/\mathbf{J}_\mathfrak{m}$ can also be defined with $\mathfrak{n}$. We proceed as in the case of ray class groups; we compare the groups $\mathbf{Cl}_\mathbf{k}^\mathfrak{n}/\Phi(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m})$ and $\mathbf{Cl}_\mathbf{k}^\mathfrak{m}/(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m})$ via their relation matrices, which in addition to the relations for $\mathbf{H}^\mathfrak{m}/\mathbf{H}_\mathfrak{m}$ contain the relations for the generators of $\mathbf{Cl}_\mathbf{k}$ and the relation for the factorisation by $\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m}$.

Let $\mathbf{K}/\mathbf{k}$ be the ray class field corresponding to the module $\mathfrak{m}$. In [CDO98, Theorem 3.3] Cohen, Oliver and Diaz y Diaz develop a formula for the relative discriminant $\mathfrak{d}_{\mathbf{K}/\mathbf{k}}$. For $\mathfrak{n} \mid \mathfrak{m}$ set $h_{\mathfrak{n},\mathbf{J}_\mathfrak{m}} := \#(\mathbf{Cl}_\mathbf{k}^\mathfrak{n}/\Phi(\mathbf{J}_\mathfrak{m}/\mathbf{H}_\mathfrak{m}))$. Then the relative discriminant is

$$\mathfrak{d}_{\mathbf{K}/\mathbf{k}} = \prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{m_\mathfrak{p} h_{\mathfrak{m},\mathbf{J}_\mathfrak{m}} - \sum_{1 \le k \le m_\mathfrak{p}} h_{\mathfrak{m}/\mathfrak{p}^k,\mathbf{J}_\mathfrak{m}}} \quad .$$

The ray class numbers $h_{\mathfrak{m}/\mathfrak{p}^k,\mathbf{J}_\mathfrak{m}}$ can be easily computed with the same methods which we used for the conductor. Finally, let (r_1, r_2) be the signature of $\mathbf{k}$ and (R_1, R_2) the signature of $\mathbf{K}$. Specialising the formula for signatures of ray class fields from [CDO98, Theorem 3.3] we get $R_1 = r_1 h_{\mathfrak{f},\mathbf{J}_\mathfrak{m}}$.

9. The global function field case

In this section we discuss the respective theory and algorithms in the global function field case.

9.1. Ray divisor class groups.

Let $\mathbf{k}/\mathbb{F}_q$ denote a global function field over the finite field of q elements and characteristic p. Unlike the number field case, for global function fields there is no canonical maximal order. It is hence more natural to work with divisors instead of ideals. Let $\mathbf{D}$ denote the group of divisors and $\mathbf{P}$ the subgroup of principal divisors (a), $a \in \mathbf{k}^*$. The divisor class group $\mathbf{Cl}$ is defined as $\mathbf{D}/\mathbf{P}$.

Let $\mathfrak{m} \in \mathbf{D}$ be an effective divisor, which we again call congruence module. For $a \in \mathbf{k}$ we say that $a \equiv 1 \bmod^* \mathfrak{m}$, if $v_\mathfrak{p}(a-1) \ge v_\mathfrak{p}(\mathfrak{m})$ for all places $\mathfrak{p}|\mathfrak{m}$. We further define the subgroups $\mathbf{D}^\mathfrak{m} := \{\, \mathfrak{a} \in \mathbf{D} \mid \gcd(\mathfrak{a}, \mathfrak{m}) = 0 \,\}$, $\mathbf{P}^\mathfrak{m} := \mathbf{P} \cap \mathbf{D}^\mathfrak{m}$, $\mathbf{k}^\mathfrak{m} := \{\, a \in \mathbf{k}^* \mid (a) \in \mathbf{P}^\mathfrak{m} \,\}$, $\mathbf{k}_\mathfrak{m} := \{\, a \in \mathbf{k}^\mathfrak{m} \mid a \equiv 1 \bmod^* \mathfrak{m} \,\}$ and $\mathbf{P}_\mathfrak{m} := \{\, (a) \in \mathbf{P}^\mathfrak{m} \mid a \in \mathbf{k}_\mathfrak{m} \,\}$. The ray divisor class group $\mathbf{Cl}_\mathfrak{m}$ for the congruence module $\mathfrak{m}$ is defined as $\mathbf{D}^\mathfrak{m}/\mathbf{P}_\mathfrak{m}$.

Let H be a subgroup of $\mathbf{D}^\mathfrak{m}$ and $U_H := \{\, a \in \mathbf{k}^\mathfrak{m} \mid (a) \in H \,\}$. We then obtain the following diagram, similar to the number field case:

$$\begin{tikzcd}
 & & & \mathbf{D}^\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{D} \arrow[d, dash] \\
 & \mathbf{k}^\mathfrak{m} \arrow[r] \arrow[d, dash] & \mathbf{P}^\mathfrak{m} \arrow[r] \arrow[d, dash] & H + \mathbf{P}^\mathfrak{m} \arrow[r] \arrow[d, dash] & H + \mathbf{P} \\
U_H \arrow[r] \arrow[d, dash] & U_H \mathbf{k}_\mathfrak{m} \arrow[r] \arrow[d, dash] & H \cap \mathbf{P}^\mathfrak{m} + \mathbf{P}_\mathfrak{m} \arrow[r] & H + \mathbf{P}_\mathfrak{m} & \\
U_H \cap \mathbf{k}_\mathfrak{m} \arrow[r] & \mathbf{k}_\mathfrak{m}. & & &
\end{tikzcd} \tag{1}$$

Again corresponding vertical lines represent isomorphisms of factor groups and horizontal arrows denote natural embeddings. For $H = \{0\}$ we have $U_H = \mathbb{F}_q^*$.

Using this in the diagram (1) we get the canonical exact sequence of abelian groups

$$0 \longrightarrow \mathbb{F}_q^* \longrightarrow \mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}} \longrightarrow \mathbf{Cl}_{\mathfrak{m}} \longrightarrow \mathbf{D}^{\mathfrak{m}}/\mathbf{P}^{\mathfrak{m}} \longrightarrow 0. \tag{2}$$

In view of [CDO98, Proposition 1.2] this means that in order to compute $\mathbf{Cl}_{\mathfrak{m}}$ we need to compute generators and relations for $\mathbf{D}^{\mathfrak{m}}/\mathbf{P}^{\mathfrak{m}}$ and $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$. To link these we also need to compute the actual elements of $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$ corresponding to relations of $\mathbf{D}^{\mathfrak{m}}/\mathbf{P}_{\mathfrak{m}}$ and to express these in the generators of $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$.

The computation of generators and relations for $\mathbf{Cl} = \mathbf{D}/\mathbf{P}$ is described in [Hes99]. From these generators and relations corresponding to divisors and principal divisors in $\mathbf{D}^{\mathfrak{m}}$ and $\mathbf{P}^{\mathfrak{m}}$ respectively can for example be obtained by applying the approximation theorem analogously to the number field case. The actual element in $\mathbf{k}^{\mathfrak{m}}$ (mod $\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$) corresponding to a relation, i.e. the generator of a principal divisor in $\mathbf{P}^{\mathfrak{m}}$, can efficiently be computed. Furthermore, it is also possible to find the expression of a divisor class (given by a divisor) in the generators of $\mathbf{Cl}$. For details we refer to [Hes99].

Once generators and relations for $\mathbf{Cl}_{\mathfrak{m}}$ are computed as above the task of expressing a given element of $\mathbf{Cl}_{\mathfrak{m}}$ represented by a divisor $\mathfrak{a} \in \mathbf{D}^{\mathfrak{m}}$ can be solved as follows: We first express $\mathfrak{a}$ in the representatives of the generators of $\mathbf{D}^{\mathfrak{m}}/\mathbf{P}^{\mathfrak{m}}$, up to a principal divisor (b) in $\mathbf{P}^{\mathfrak{m}}$ for $b \in \mathbf{k}^{\mathfrak{m}}$. Then b is expressed in the representatives of the generators of $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$, up to an element of $\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$.

9.2. Multiplicative groups of residue class rings.

We are left to describe how generators and relations for $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$ are computed and how an element of $\mathbf{k}^{\mathfrak{m}}$ (mod $\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$) can be expressed in these generators.

We first consider $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. Let $\mathfrak{o}_{\mathfrak{p}}$ denote the valuation ring of $\mathfrak{p}$ such that $\mathfrak{p}$ is the maximal ideal of $\mathfrak{o}_{\mathfrak{p}}$. It is straightforward to see that the canonical map of multiplicative groups $\mathbf{k}^{\mathfrak{m}} \longrightarrow \prod_{\mathfrak{p}|\mathfrak{m}}\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}\bigr)^*$ has kernel $\mathbf{k}_{\mathfrak{m}}$. Using the weak approximation theorem we also see that it is surjective so that we obtain $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}} \cong \prod_{\mathfrak{p}|\mathfrak{m}}\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}\bigr)^*$, in analogy to the number field case. Once we have generators and relations for each of the $\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}\bigr)^*$ their disjoint union will give generators and relations for $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. We remark that we do not have to compute actual elements of $\mathbf{k}^{\mathfrak{m}}$. We obtain generators and relations for $\mathbf{k}^{\mathfrak{m}}/\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$ by expressing a generator of $\mathbb{F}_q^*$ in the generators of $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$ and by adding the obtained expression to the relations of $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. Finally, to find the expression of an element of $\mathbf{k}^{\mathfrak{m}}$ (mod $\mathbb{F}_q^*\,\mathbf{k}_{\mathfrak{m}}$) in the generators we do so for every local factor $\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}\bigr)^*$.

We next need to explain how generators and relations for $\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{m}\bigr)^*$ for $m \in \mathbb{Z}^{\geq 1}$ can be determined and how an element in $\mathfrak{o}_{\mathfrak{p}}^*$ (mod $\mathfrak{p}^m$) can be expressed in these generators. In analogy to the number field case we have $\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{m}\bigr)^* \cong (\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^m)$ where $(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p})^*$ is mapped to the group of $(q^{\deg(\mathfrak{p})}-1)$th roots of unity in $\bigl(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^{m}\bigr)^*$.

It is well known that the order of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ is $(q^{\deg(\mathfrak{p})})^{m-1}$. For $a \in \mathbb{R}^{\geq 0}$ and setting $\min\{\,\} := 0$ define $\lceil a \rceil_p := \min\{\, p^l \mid a \leq p^l,\ l \in \mathbb{Z}^{\geq 0}\,\}$. The following lemma immediately gives us generators and relations for $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$.

Lemma 9.1. *Let $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$ and B be a system of representatives in $\mathfrak{o}_{\mathfrak{p}}$ of the $\mathbb{F}_p$-vector space $\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}$. Let $U_{\beta,j}$ denote the subgroup of $(1+\mathfrak{p})/(1+\mathfrak{p}^m)$ generated by $(1+\beta\pi^j)\,U_{\mathfrak{p}}^{(m)}$ for $\beta \in B$ and $j \geq 1$, j coprime to p. The groups $U_{\beta,j}$ have pairwise* *trivial intersection and are of order* $|U_{\beta,j}| = \lceil m/j \rceil_p$. *Moreover,*

$$(1+\mathfrak{p})/(1+\mathfrak{p}^m) = \prod \{\, U_{\beta,j} \,|\, \beta \in B,\ 1 \leq j \leq m-1,\ \gcd(j,p) = 1 \,\}.$$

Proof. Follows from [Aue99, p. 39]. □

Assume for given $a \in (1+\mathfrak{p})/(1+\mathfrak{p}^m)$ we want to find the expression of a as a power product of the generators of the Lemma. The most elementary way of achieving this is by a Gaussian elimination procedure as done in Algorithm 3.5. The methods of section 4 can also be used. The $\mathfrak{p}$-adic logarithm in section 5 does not carry over, because we work in characteristic p and would have to divide by p in the series expansion of $\log_{\mathfrak{p}}$ and $\exp_{\mathfrak{p}}$. However, the Artin-Hasse logarithm can be applied, Proposition 5.3 remains true in characteristic p. This appears to be a very efficient way for computing the expression of a in the generators.

9.3. **Conductors.** Let H be a subgroup of $\mathbf{Cl}_{\mathfrak{m}}$. If $\mathfrak{m}' \leq \mathfrak{m}$ is another congruence module we have a natural epimorphism $\Phi_{\mathfrak{m}'} : \mathbf{Cl}_{\mathfrak{m}} \longrightarrow \mathbf{Cl}_{\mathfrak{m}'}$. There is a unique smallest congruence module $\mathfrak{f} \leq \mathfrak{m}$ such that $\mathbf{Cl}_{\mathfrak{f}}/\Phi_{\mathfrak{f}}(H) \cong \mathbf{Cl}_{\mathfrak{m}}/H$. This congruence module is called the conductor of H. The conductor of $\mathbf{Cl}_{\mathfrak{m}}$ is defined to be the conductor of its zero subgroup $H = \{0\}$.

Using the definition there is a straightforward way of computing the conductor of a subgroup H of $\mathbf{Cl}_{\mathfrak{m}}$. Namely, we successively check for all smaller congruence modules $\mathfrak{m}' < \mathfrak{m}$ whether the isomorphy holds. If not, we take the next $\mathfrak{m}'$. If yes, we replace $\mathfrak{m}$ by $\mathfrak{m}'$ and H by $\Phi(H)$ and start from the beginning. At the end, $\mathfrak{m}$ is smallest possible. Because of the uniqueness property $\mathfrak{m}$ must be the conductor of the original H.

A more explicit way is given by the diagram (1) above. Assume the subgroup of $\mathbf{Cl}_{\mathfrak{m}}$ is the image of a divisor group $H \subseteq \mathbf{D}^{\mathfrak{m}}$. The conductor is a smallest congruence module $\mathfrak{m}'$ such that $U_H\,\mathbf{k}_{\mathfrak{m}'}/\mathbf{k}_{\mathfrak{m}'} \cong U_H\,\mathbf{k}_{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. In the case of $H = \{0\}$ we see from the exact sequence (2) above and since the cardinality of $(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^m)^*$ changes if m changes that $\mathfrak{m}$ already is the conductor of $\mathbf{Cl}_{\mathfrak{m}}$. The computation of the conductor for general H using the isomorphy amounts to two major steps:

In the first step we need to determine generators of U_H. If $h_1, \ldots, h_r$ are the divisor classes in $\mathbf{Cl}$ of the generators of H we compute the kernel of $\mathbb{Z}^r \longrightarrow \mathbf{Cl}$, $(\lambda_i)_i \mapsto \sum_i \lambda_i h_i$. To carry out this computation we need to know generators and relations of $\mathbf{Cl}$ and need to express the classes h_i in these generators. From the kernel we obtain a basis of $H \cap \mathbf{P}^{\mathfrak{m}}$ and can reconstruct the corresponding elements in U_H.

In the second step we express the generators of U_H in the generators of $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$. Joining these expressions and the relations of $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$ yields the relations of $\mathbf{k}^{\mathfrak{m}}/U_H\,\mathbf{k}_{\mathfrak{m}}$. Now, analogously to the number field case, for smaller $\mathfrak{m}'$ there is no need to recompute the expressions for the generators of U_H. We only have to adjust the orders of the generators of $\mathbf{k}^{\mathfrak{m}}/\mathbf{k}_{\mathfrak{m}}$ in the relation matrix for $\mathbf{k}^{\mathfrak{m}'}/U_H\,\mathbf{k}_{\mathfrak{m}'}$. Once we obtain a different relation module, $\mathfrak{m}'$ is too small. Successive testing and descending again exhibits the smallest congruence module preserving the isomorphy.

9.4. **Class field discriminants and genera.** Let $\mathfrak{m}$ be a congruence module. From class field theory we know that the abelian extensions $\mathbf{K}/\mathbf{k}$ of conductor less than or equal to $\mathfrak{m}$ correspond inclusion reversing to subgroups H of $\mathbf{Cl}_{\mathfrak{m}}$ of finite index. The conductor of $\mathbf{K}/\mathbf{k}$ is equal to the conductor of H.

Let $h_{\mathfrak{m}',H} := \mathbf{Cl}_{\mathfrak{m}'}/\Phi_{\mathfrak{m}'}(H)$ for the natural epimorphism $\Phi_{\mathfrak{m}'} : \mathbf{Cl}_{\mathfrak{m}} \longrightarrow \mathbf{Cl}_{\mathfrak{m}'}$ and let $\mathfrak{d}_{\mathbf{K}/\mathbf{k}}$ denote the discriminant of $\mathbf{K}/\mathbf{k}$. Using the same proof as in [CDO98] we obtain

$$\mathfrak{d}_{\mathbf{K}/\mathbf{k}} = (h_{\mathfrak{m},H})\,\mathfrak{m} - \sum_{\mathfrak{p}|\mathfrak{m}} \left(\sum_{k=1}^{v_{\mathfrak{p}}(\mathfrak{m})} h_{\mathfrak{m}-k\mathfrak{p},H} \right) \mathfrak{p}.$$

Let $\deg(H) := \min\{\deg(\mathfrak{a}) \mid \mathfrak{a} + \mathbf{P}_{\mathfrak{m}} \in H\}$. Because H is of finite index in $\mathbf{Cl}_{\mathfrak{m}}$, $\deg(H) \geq 1$ holds. Let $\mathbb{F}_{q_1}$ be the full constant field of $\mathbf{K}$. From class field theory we have $[\mathbf{K} : \mathbf{k}] = h_{\mathfrak{m},H}$ and $[\mathbb{F}_{q_1} : \mathbb{F}_q] = \deg(H)$. Furthermore, the norm of the different of $\mathbf{K}/\mathbf{k}$ down to $\mathbf{k}$ equals $\mathfrak{d}_{\mathbf{K}/\mathbf{k}}$, and $[\mathbb{F}_{q_1} : \mathbb{F}_q]$-times the degree of the different equals the degree of the discriminant. If $g_{\mathbf{k}}$ and $g_{\mathbf{K}}$ denote the genus of $\mathbf{k}$ and $\mathbf{K}$ respectively we obtain from the Hurwitz genus formula

$$\deg(H)(g_{\mathbf{K}} - 1) = h_{\mathfrak{m},H}\left(g_{\mathbf{k}} - 1 + \frac{\deg(\mathfrak{m})}{2} \right) - \frac{1}{2} \sum_{\mathfrak{p}|\mathfrak{m}} \left(\sum_{k=1}^{v_{\mathfrak{p}}(\mathfrak{m})} h_{\mathfrak{m}-k\mathfrak{p},H} \right) \deg(\mathfrak{p}).$$

Using the methods from section 9.3 we can compute the numbers $h_{\mathfrak{m}-k\mathfrak{p},H}$ easily. We are thus able to determine the discriminant $\mathfrak{d}_{\mathbf{K}/\mathbf{k}}$ and the genus $g_{\mathbf{K}}$.

References

[Aue99] Roland Auer, *Ray Class Fields of Global Function Fields with Many Rational Places*, Carl-von-Ossietzky-Universität, Oldenburg, 1999.

[BB+99] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *The Computer Algebra System PARI-GP*, Université Bordeaux I, 1999, `ftp://megrez.math.u-bordeaux.fr/pub/pari/`

[BC95] W. Bosma and J.J. Cannon, *Handbook of Magma functions*, School of Mathematics, University of Sydney, Sydney, 1995.

[CDO96] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Computing ray class groups, conductors and discriminants*, ANTS II (Henri Cohen, ed.), LNCS 1122, Springer, 1996, 49–57.

[CDO98] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Computing ray class groups, conductors and discriminants*, Math. Comp. **67** (1998).

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

[Coh96] Henri Cohen, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), 1681–1699.

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

[DF+96] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, KANT V4, J. Symb. Comp. **11** (1996), 267–283.

[Fie00] Claus Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303.

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

[Hes96] Florian Heß, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, TU - Berlin, 1996, `http://www.math.TU-Berlin.DE/~kant/publications/diplom/hess.ps.gz`.

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

[Lan94] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer Verlag, Berlin, 1994.

[Pau96] Sebastian Pauli, *Zur Berechnung von Strahlklassengruppen*, Diplomarbeit, TU - Berlin, 1996, `http://www.math.TU-Berlin.DE/~kant/publications/diplom/pauli.ps.gz`.

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

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

[SWD] Oliver Schirokauer, Damian Weber, and Thomas Denny, *Discrete Logarithms: The Effectiveness of the Index Calculus Method*, ANTS II (Henri Cohen, ed.), LNCS 1122, Springer, 1996, 337–361.

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

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