Computation of locally free class groups*

Werner Bley†
Fachbereich für Mathematik und Informatik
Universität Kassel
34132 Kassel
Germany
bley@mathematik.uni-kassel.de

Robert Boltje‡
Department of Mathematics
University of California
Santa Cruz, CA 95064
U.S.A.
boltje@ucsc.edu

January 18, 2006

Abstract

We show that the locally free class group of an order in a semisimple algebra over a number field is isomorphic to a certain ray class group. This description is then used to present an algorithm that computes the locally free class group. The algorithm is implemented in MAGMA for the case where the algebra is a group ring over the rational numbers.

Introduction

Throughout this paper we fix a number field K with ring of integers $\mathcal{O}_K$, a finite-dimensional semisimple K-algebra A and an $\mathcal{O}_K$-order $\mathcal{A}$ in A. The purpose of this paper is to give an algorithm that computes the locally free class group $\mathrm{cl}(\mathcal{A})$, cf. [4, (39.12)] for a definition. This was done in [1] in the case that A is commutative, where $\mathrm{cl}(\mathcal{A})$ is isomorphic to the Picard group $\mathrm{Pic}(\mathcal{A})$, cf. [4, (55.26)]. Here we treat the general case. As in [1] we can show that $\mathrm{cl}(\mathcal{A})$ is isomorphic to a quotient of a certain ray class group in the center of A, cf. Corollary 1.9. This is achieved in several steps. We choose a maximal $\mathcal{O}_K$-order $\mathcal{M}$ in A containing $\mathcal{A}$, and a full ideal $\mathfrak{f}$ of $\mathcal{M}$ which is contained in $\mathcal{A}$. A canonical pull-back diagram involving $\mathcal{A}$ and $\mathcal{A}/\mathfrak{f}$ gives rise to a Mayer-Vietoris sequence and the induced exact sequence

$$K_1(\mathcal{A}/\mathfrak{f}) \xrightarrow{\partial} \mathrm{cl}(\mathcal{A},\mathfrak{f}) \longrightarrow \mathrm{cl}(\mathcal{A}) \longrightarrow 0\,,$$

cf. (1.2.b), with a term $\mathrm{cl}(\mathcal{A},\mathfrak{f})$ coming directly from the Mayer-Vietoris sequence. In Theorem 1.5 we use Wilson's idèle theoretic description of locally

*MR Subject Classification 19A31, 16G30
†Research supported by the DFG
‡Research supported by the NSF, DMS-0200592 and 0128969

free class groups, cf. [13], in order to show that the term $\mathrm{cl}(\mathcal{A}, \mathfrak{f})$ is isomorphic to a ray class group.

In the proof of this theorem we make repeatedly use of Theorem 2.2 which is of independent interest. It determines the image under the reduced norm map of higher principal unit groups in the maximal order of a division algebra over a p-adic field.

In the last section we present an algorithm that computes $\mathrm{cl}(\mathcal{A})$ using the ray class group description of $\mathrm{cl}(\mathcal{A}, \mathfrak{f})$ in the case of group algebras $A = KG$, where G denotes a finite group. A maximal order $\mathcal{M}$ containing $\mathcal{A}$ can be computed using an algorithm of Friedrichs, cf. [7]. We then describe how one can compute an ideal $\mathfrak{f}$, the relevant ray class group, generators of $K_1(\mathcal{A}/\mathfrak{f})$, and the map ∂ which turns out to be a reduced norm map. We also show how our approach can be used to compute the kernel group $D(\mathcal{A}) := \ker(\mathrm{cl}(\mathcal{A}) \to \mathrm{cl}(\mathcal{M}))$. It is well known that $D(\mathcal{A})$ does not depend on the choice of the maximal order $\mathcal{M}$.

This algorithm is implemented in MAGMA for group algebras $A = \mathbb{Q}G$ over the rational numbers. The program and tables of locally free class groups of integral grouprings $\mathbb{Z}$[G] for many small groups G are available at `http://www.mathematik.uni-kassel.de/~bley/pub.html`.

1 Locally free class groups in terms of ray class groups

Throughout this paper we fix the following notation:

1.1 Notation Let $\mathcal{O}_K \subset K$ and $\mathfrak{f} \subseteq \mathcal{A} \subseteq \mathcal{M} \subset A$ be as in the introduction. We set $\overline{\mathcal{M}} := \mathcal{M}/\mathfrak{f}$ and $\overline{\mathcal{A}} := \mathcal{A}/\mathfrak{f}$ so that $\overline{\mathcal{A}} \subseteq \overline{\mathcal{M}}$ are finite rings. The canonical map $\mathcal{M} \to \overline{\mathcal{M}}$ will be denoted by $m \mapsto \overline{m}$. We will denote the center of a ring R by $Z(R)$. We set $C := Z(A)$ and denote by $\mathcal{O}_C$ the integral closure of $\mathcal{O}_K$ in C. The primitive idempotents of C will be denoted by $e_1, \dots, e_r$. For $i = 1, \dots, r$, we set $A_i := Ae_i$. Then

$$A = A_1 \oplus \cdots \oplus A_r \tag{1.1.a}$$

is a decomposition into the indecomposable ideals A_i of A. Each A_i is a K-algebra with identity element e_i. By Wedderburn's Theorem, the centers $K_i := Z(A_i)$ are finite field extensions of K via $K \to K_i$, $\alpha \mapsto \alpha e_i$, and we have K-algebra isomorphisms $A_i \cong \mathrm{Mat}_{n_i}(D_i)$ for each $i = 1, \dots, r$, where D_i is a division ring with $Z(D_i) \cong K_i$. The Wedderburn decomposition (1.1.a) induces decompositions

$$C = K_1 \oplus \cdots \oplus K_r \tag{1.1.b}$$

and

$$\mathcal{O}_C = \mathcal{O}_{K_1} \oplus \cdots \oplus \mathcal{O}_{K_r}\,, \tag{1.1.c}$$

where $\mathcal{O}_{K_i}$ denotes the ring of algebraic integers of K_i for $i = 1, \dots, r$. Since $\mathcal{M}$ is a maximal $\mathcal{O}_K$-order of A, it contains the central idempotents e_i and decomposes into $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$ with $\mathcal{M}_i := \mathcal{M}e_i$. As a consequence, the ideal $\mathfrak{f}$ of $\mathcal{M}$ also decomposes into $\mathfrak{f} = \mathfrak{f}_1 \oplus \cdots \oplus \mathfrak{f}_r$ with ideals $\mathfrak{f}_i = \mathfrak{f}e_i$ of $\mathcal{M}_i$.

1.2 We consider the $\mathcal{O}_K$-order

$$\mathcal{D} := \mathcal{D}(\mathcal{A}, \mathfrak{f}) := \{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \mid a_1 \equiv a_2 \mod \mathfrak{f}\}$$

in $A \times A$ which fits into the pull-back diagram

$$\begin{array}{ccc} \mathcal{D} & \xrightarrow{q_1} & \mathcal{A} \\ {\scriptstyle q_2}\downarrow & & \downarrow{\scriptstyle p_1} \\ \mathcal{A} & \xrightarrow{p_2} & \overline{\mathcal{A}} \end{array}$$

of rings. By [4, Theorem 49.27], this leads to an exact sequence

$$K_1(\mathcal{A}) \times K_1(\mathcal{A}) \xrightarrow{p_1/p_2} K_1(\overline{\mathcal{A}}) \xrightarrow{\partial} \mathrm{cl}(\mathcal{D}) \xrightarrow{(q_1, q_2)} \mathrm{cl}(\mathcal{A}) \times \mathrm{cl}(\mathcal{A}) \longrightarrow 0\,.$$

Here, the first map is given by $(x, y) \mapsto (K_1(p_1))(x) \cdot (K_1(p_2))(y)^{-1}$ and the second map is defined as follows. Every element of $K_1(\overline{\mathcal{A}})$ is represented by an element $u \in \overline{\mathcal{A}}^\times$ and such an element is mapped to the class of the locally free $\mathcal{D}$-module

$$M(u) := \{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \mid \overline{a}_1 \cdot u = \overline{a}_2\}\,, \tag{1.2.a}$$

cf. the proof of [4, Theorem 49.27]. We set

$$\mathrm{cl}(\mathcal{A}, \mathfrak{f}) := \ker\bigl(q_2 \colon \mathrm{cl}(\mathcal{D}) \to \mathrm{cl}(\mathcal{A})\bigr)$$

and obtain a short exact sequence

$$K_1(\mathcal{A}) \xrightarrow{p_1} K_1(\overline{\mathcal{A}}) \xrightarrow{\partial} \mathrm{cl}(\mathcal{A}, \mathfrak{f}) \xrightarrow{q_1} \mathrm{cl}(\mathcal{A}) \longrightarrow 0\,, \tag{1.2.b}$$

as can be easily verified.

1.3 In the following $\mathfrak{p}$ will usually stand for a maximal ideal of $\mathcal{O}_K$. For an $\mathcal{O}_K$-module M we write $M_\mathfrak{p}$ for the completion at $\mathfrak{p}$. We let

$$J(A) := \{(a_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} A_\mathfrak{p}^\times \mid a_\mathfrak{p} \in \mathcal{A}_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p}\}$$

denote the idèles of A and write $U(\mathcal{A}) = \prod_\mathfrak{p} \mathcal{A}_\mathfrak{p}^\times$ for the subgroup of unit idèles. Here $\mathfrak{p}$ runs through all maximal ideals of $\mathcal{O}_K$. One has canonical isomorphisms

$$\begin{aligned} A_\mathfrak{p} &\cong K_\mathfrak{p} \otimes_K A \cong \bigoplus_{i=1}^r K_\mathfrak{p} \otimes_K A_i \cong \bigoplus_{i=1}^r K_\mathfrak{p} \otimes_K K_i \otimes_{K_i} A_i \\ &\cong \bigoplus_{i=1}^r \bigoplus_\mathfrak{P} (K_i)_\mathfrak{P} \otimes_{K_i} A_i \cong \bigoplus_{i,\mathfrak{P}} A_{i,\mathfrak{P}} \end{aligned} \tag{1.3.a}$$

involving various completions, where, for given $i \in \{1, \dots, r\}$, $\mathfrak{P}$ runs through all maximal ideals of $\mathcal{O}_{K_i}$ dividing $\mathfrak{p}$ and $A_{i,\mathfrak{P}}$ is defined as $(A_i)_{\mathfrak{P}}$. More generally, for any $\mathcal{O}_{K_i}$-submodule $\mathfrak{L}_i$ of A_i, we denote by $\mathfrak{L}_{i,\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of $\mathfrak{L}_i$. Using the above isomorphism, we will often write elements of $J(A)$, resp. $A_{\mathfrak{p}}$, as tuples $(a_{i,\mathfrak{P}})_{i,\mathfrak{P}}$, where $\mathfrak{P}$ ranges over all maximal ideals of $\mathcal{O}_{K_i}$, resp. over those that contain $\mathfrak{p}$. Note that $J(A)$ does not depend on the order $\mathcal{A}$. Similarly we denote by $J(C)$ the group of idèles of C. Again one has a canonical isomorphism

$$C_{\mathfrak{p}} \cong \bigoplus_{i,\mathfrak{P}} K_{i,\mathfrak{P}}$$

and we will write elements in $J(C)$, resp. $C_{\mathfrak{p}}$, often in the form $(\alpha_{i,\mathfrak{P}})_{i,\mathfrak{P}}$.

By $\mathrm{nr}\colon J(A) \to J(C)$ we denote the reduced norm map (which translates into the component-wise reduced norm maps $\mathrm{nr}\colon A_{i,\mathfrak{P}}^{\times} \to K_{i,\mathfrak{P}}^{\times}$ after the above identifications). We recall from [4, Proposition 45.8 and Theorem 7.48] that

$$\mathrm{nr}(J(A)) = J(C) \quad \text{and} \quad \mathrm{nr}(A^{\times}) = C^{\times +}\,,$$

where

$$C^{\times +} := \{c \in C^{\times} \mid c \text{ is positive at quaternionic components}\}\,.$$

The last condition means that if $c = (c_i)$ with $c_i \in K_i^{\times}$ then $\tau(c_i) > 0$ whenever $i \in \{1, \dots, r\}$ and $\tau\colon K_i \to \mathbb{R}$ is a real embedding such that the corresponding scalar extension $A_i \otimes_{K_i,\tau} \mathbb{R}$ is a full matrix ring over the quaternions. Furthermore, we define the subgroup

$$U_{\mathfrak{f}}(\mathcal{A}) := \{(a_{\mathfrak{p}})_{\mathfrak{p}} \in U(\mathcal{A}) \mid a_{\mathfrak{p}} \equiv 1 \mod \mathfrak{f}_{\mathfrak{p}}\}$$

of $U(\mathcal{A})$.

1.4 Next we define commutative invariants in C of the non-commutative data $A, \mathcal{A}$ and $\mathfrak{f}$. With $\mathfrak{f}$ also the ideal $\mathfrak{g} := \mathfrak{f} \cap C$ of $\mathcal{O}_C$ decomposes into $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r$ with ideals $\mathfrak{g}_i = \mathfrak{g} e_i$ of $\mathcal{O}_{K_i}$. We denote by $I_{\mathfrak{g}} = I_{\mathfrak{g}}(C)$ the group of fractional $\mathcal{O}_C$-ideals of C that are coprime to $\mathfrak{g}$ and have

$$I_{\mathfrak{g}}(C) = I_{\mathfrak{g}_1}(K_1) \times \cdots \times I_{\mathfrak{g}_r}(K_r)\,.$$

For each $i \in \{1, \dots, r\}$ we write ∞_i for the formal product over real archimedian places $\tau\colon K_i \to \mathbb{R}$ such that $A \otimes_{K_i,\tau} \mathbb{R}$ is a full matrix ring over the quaternions, and we define the 'ray modulo $\mathfrak{g}\infty$' by

$$P_{\mathfrak{g}}^{+} := \{(\alpha_i \mathcal{O}_{K_i})_i \in I_{\mathfrak{g}} \mid \alpha_i \equiv 1 \mod^{\times} g_i \infty_i, \text{ for all } i = 1, \dots, r\}\,.$$

Note that $P_{\mathfrak{g}}^{+}$ is a subgroup of $I_{\mathfrak{g}}$.

The next theorem gives both an idèle and ideal theoretic description of $\mathrm{cl}(A, \mathfrak{f})$. Note that the ideal theoretic part only involves 'commutative data' located in the center C of A.

1.5 Theorem *There are canonical isomorphisms*

$$\mathrm{cl}(\mathcal{A},\mathfrak{f}) \cong J(C)\big/(C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{A}))) \cong I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+}\,.$$

1.6 Remark It is immediate from the above theorem that $\mathrm{cl}(\mathcal{B},\mathfrak{f}) \cong \mathrm{cl}(\mathcal{M},\mathfrak{f})$ for any $\mathcal{O}_K$-order $\mathcal{B}$ such that $\mathfrak{f} \subseteq \mathcal{B} \subseteq \mathcal{M}$. We also note that $U_{\mathfrak{f}}(\mathcal{B}) = U_{\mathfrak{f}}(\mathcal{M})$. In fact, if $b_{\mathfrak{p}} \in \mathcal{M}_{\mathfrak{p}}^{\times}$ and $b_{\mathfrak{p}} \equiv 1 \mod \mathfrak{f}_{\mathfrak{p}}$, then $b_{\mathfrak{p}}^{-1} \equiv 1 \mod \mathfrak{f}_{\mathfrak{p}}$, and since $\mathfrak{f}_{\mathfrak{p}} \subseteq \mathcal{B}_{\mathfrak{p}}$, both $b_{\mathfrak{p}}$ and $b_{\mathfrak{p}}^{-1}$ are elements of $\mathcal{B}_{\mathfrak{p}}$.

Proof (of Theorem 1.5.) From [13, Theorem 1] we obtain natural isomorphisms

$$\omega\colon \mathrm{cl}(\mathcal{D}) \cong \frac{J(C)\times J(C)}{(C^{\times +}\times C^{\times +})\mathrm{nr}(U(\mathcal{D}))} \tag{1.6.a}$$

and

$$\mathrm{cl}(\mathcal{A}) \cong \frac{J(C)}{(C^{\times +})\mathrm{nr}(U(\mathcal{A}))}\,.$$

Inspecting the definition of these isomorphisms one verifies easily that the map induced by q_2 is translated into a map between the right hand sides of the above equations that is induced by the projection map $J(C)\times J(C) \to J(C)$ onto the second component. Therefore, we obtain an isomorphism

$$\mathrm{cl}(\mathcal{A},\mathfrak{f}) \cong \frac{J(C)\times C^{\times +}\mathrm{nr}(U(\mathcal{A}))}{(C^{\times +}\times C^{\times +})\mathrm{nr}(U(\mathcal{D}))}\,.$$

We will show that the map

$$\frac{J(C)\times C^{\times +}\mathrm{nr}(U(\mathcal{A}))}{(C^{\times +}\times C^{\times +})\mathrm{nr}(U(\mathcal{D}))} \xrightarrow{\ \sigma\ } \frac{J(C)}{C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{A}))} \tag{1.6.b}$$

induced by

$$\big((a_{\mathfrak{p}})_{\mathfrak{p}},(b_{\mathfrak{p}})_{\mathfrak{p}}\big) \mapsto (a_{\mathfrak{p}}/b_{\mathfrak{p}})_{\mathfrak{p}} \in J(C)$$

for $((a_{\mathfrak{p}})_{\mathfrak{p}},(b_{\mathfrak{p}})_{\mathfrak{p}}) \in J(C)\times C^{\times +}\mathrm{nr}(U(\mathcal{A}))$ is an isomorphism. The map is obviously well-defined. Let τ denote the map in the inverse direction induced by

$$J(C) \ni (x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \big((x_{\mathfrak{p}})_{\mathfrak{p}},(1)_{\mathfrak{p}}\big) \in J(C)\times C^{\times +}\mathrm{nr}(U(\mathcal{A}))\,.$$

Again it is straightforward to verify that τ is well-defined. Obviously $\sigma\circ\tau = \mathrm{id}$. In order to show that $\tau\circ\sigma = id$ we have to prove that

$$\big((a_{\mathfrak{p}})_{\mathfrak{p}},(b_{\mathfrak{p}})_{\mathfrak{p}}\big) \equiv \big((a_{\mathfrak{p}}/b_{\mathfrak{p}})_{\mathfrak{p}},(1)_{\mathfrak{p}}\big) \mod (C^{\times +}\times C^{\times +})\mathrm{nr}(U(\mathcal{D}))\,.$$

But this is equivalent to the statement

$$\big((b_{\mathfrak{p}})_{\mathfrak{p}},(b_{\mathfrak{p}})_{\mathfrak{p}}\big) \in (C^{\times +}\times C^{\times +})\mathrm{nr}(U(\mathcal{D})),$$

which is immediate from $(b_{\mathfrak{p}})_{\mathfrak{p}} \in C^{\times +}\mathrm{nr}(U(\mathcal{A}))$. This concludes the proof of $\mathrm{cl}(\mathcal{A},\mathfrak{f}) \cong J(C)\big/(C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{A})))$.

We will now define a map

$$\varphi\colon I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+} \to J(C)/C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) \tag{1.6.c}$$

and show that it is an isomorphism. This will complete the proof of the theorem because of the equation $U_{\mathfrak{f}}(\mathcal{A}) = U_{\mathfrak{f}}(\mathcal{M})$ from Remark 1.6.

For each $i \in \{1, \dots, r\}$ and each maximal ideal $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ we choose a uniformizing element $\pi_{i,\mathfrak{P}}$ and define, for $(\mathfrak{a}_i)_i \in I_{\mathfrak{g}}$,

$$\varphi_0\left((\mathfrak{a}_i)_i\right) := \left(\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\mathfrak{a}_i)}\right)_{i,\mathfrak{P}} \cdot \left(C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M}))\right) .$$

Here $v_{\mathfrak{P}}$ denotes the $\mathfrak{P}$-adic valuation. In order to prove that φ_0 does not depend on the choice of the elements $\pi_{i,\mathfrak{P}}$, it suffices to show that

$$\left(u_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\mathfrak{a}_i)}\right)_{i,\mathfrak{P}} \in \mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) \tag{1.6.d}$$

for units $u_{i,\mathfrak{P}}$ of $\mathcal{O}_{K_{i,\mathfrak{P}}}$. Note that under the identification in (1.3.a), the elements of $U_{\mathfrak{f}}(\mathcal{M})$ consist of tuples $(\lambda_{i,\mathfrak{P}})_{i,\mathfrak{P}}$ satisfying $\lambda_{i,\mathfrak{P}} \in \mathcal{M}_{i,\mathfrak{P}}^{\times}$ and $\lambda_{i,\mathfrak{P}} \equiv 1 \mod \mathfrak{f}_{i,\mathfrak{P}}$ for all i and $\mathfrak{P}$. So we can show (1.6.d) componentwise. For maximal ideals $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ such that $\mathfrak{P} \nmid \mathfrak{g}_i$ we have $\mathfrak{f}_{i,\mathfrak{P}} = \mathcal{M}_{i,\mathfrak{P}}$, so that (1.6.d) holds in the $(i,\mathfrak{P})$-component because $\mathrm{nr}(\mathcal{M}_{i,\mathfrak{P}}^{\times}) = \mathcal{O}_{K_{i,\mathfrak{P}}}^{\times}$ by [4, Proposition 45.8]. For $\mathfrak{P}$ such that $\mathfrak{P} \mid \mathfrak{g}_i$ we have $v_{\mathfrak{P}}(\mathfrak{a}_i) = 0$, so that (1.6.d) is obviously satisfied in the $(i,\mathfrak{P})$-component.

Next we show that $P_{\mathfrak{g}}^{+}$ is contained in $\ker(\varphi_0)$ so that φ_0 induces a well-defined map φ as in (1.6.c). Let $(\alpha_i \mathcal{O}_{K_i})_i \in P_{\mathfrak{g}}^{+}$ and note that

$$\varphi_0\left((\alpha_i\mathcal{O}_{K_i})_i\right) = \left(\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\alpha_i)}\right)_{i,\mathfrak{P}} \equiv \left(\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\alpha_i)}\alpha_i^{-1}\right)_{i,\mathfrak{P}} \mod C^{\times +} .$$

So it suffices to show that

$$\left(\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\alpha_i)}\alpha_i^{-1}\right)_{i,\mathfrak{P}} \in \mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) . \tag{1.6.e}$$

We argue component-wise. For the $(i,\mathfrak{P})$-components with $\mathfrak{P} \nmid \mathfrak{g}_i$ this is again a consequence of the surjectivity of the reduced norm map, cf. [4, Proposition 45.8]. And for $(i,\mathfrak{P})$-components with $\mathfrak{P} \mid \mathfrak{g}_i$ one has

$$\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\alpha_i)}\alpha_i^{-1} = \alpha_i^{-1} \equiv 1 \mod \mathfrak{g}_{i,\mathfrak{P}} .$$

Therefore, (1.6.e) also holds in these $(i,\mathfrak{P})$-component by Corollary 2.3, which is proved in the next section.

Next we define a map

$$\psi_0\colon J(C) \to I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+} .$$

Given an idèle $\alpha = (\alpha_{i,\mathfrak{P}})_{i,\mathfrak{P}} \in J(C)$ we apply the Weak Approximation Theorem and choose an element $\beta = (\beta_i)_i \in C^{\times +}$ such that

$$v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}\beta_i - 1) \geqslant v_{\mathfrak{P}}(\mathfrak{g}_i), \quad \text{for all } (i,\mathfrak{P}) \text{ with } \mathfrak{P} \mid \mathfrak{g}_i. \tag{1.6.f}$$

Then we set

$$\psi_0(\alpha) := \left(\prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}\beta_i)} \right)_i \cdot P_{\mathfrak{g}}^+ .$$

We have to show that ψ_0 does not depend on the choice of the element β. Suppose that $\gamma = (\gamma_i)_i \in C^{\times +}$ is another choice such that (1.6.f) is satisfied. Then it suffices to show that

$$\left(\prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}\beta_i) - v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}\gamma_i)} \right)_i = \left(\frac{\beta_i}{\gamma_i} \mathcal{O}_{K_i} \right)_i \in P_{\mathfrak{g}}^+ .$$

But this is an obvious consequence of (1.6.f) and the definition of $P_{\mathfrak{g}}^+$.

If $\alpha = (\alpha_i)_i \in C^{\times +} \subseteq J(C)$, then we may choose $\beta_i = \alpha_i^{-1}$. This shows that $C^{\times +}$ is contained in $\ker(\psi_0)$. If $\alpha = (\alpha_{i,\mathfrak{P}})_{i,\mathfrak{P}} \in \mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M}))$, then Corollary 2.3 (proved in the next section) shows that we may choose $\beta = 1$. This shows that $\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M}))$ is contained in $\ker(\psi_0)$. Therefore, ψ_0 induces a group homomorphism

$$\psi \colon J(C)/C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) \to I_{\mathfrak{g}}/P_{\mathfrak{g}}^+ . \tag{1.6.g}$$

Next we verify that $\psi \circ \varphi = \mathrm{id}$. Let $\mathfrak{a} = (\mathfrak{a}_i)_i \in I_{\mathfrak{g}}$. Then $(\psi \circ \varphi)(\mathfrak{a} \cdot P_{\mathfrak{g}}^+) = \psi\left((\pi_{i,\mathfrak{P}}^{v_{\mathfrak{P}}(\mathfrak{a}_i)})_{i,\mathfrak{P}} \cdot C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) \right)$. Since $v_{\mathfrak{P}}(\mathfrak{a}_i) = 0$ for all $(i, \mathfrak{P})$ such that $\mathfrak{P} \mid \mathfrak{g}_i$ we may choose $\beta = 1$, which immediately implies $\psi \circ \varphi = \mathrm{id}$.

Now let $\alpha = (\alpha_{i,\mathfrak{P}})_{i,\mathfrak{P}} \in J(C)$ and suppose that $\beta \in C^{\times +}$ satisfies (1.6.f). In order to show that $\varphi \circ \psi = \mathrm{id}$ we must show that

$$\left(\alpha_{i,\mathfrak{P}} \pi_{i,\mathfrak{P}}^{-v_{\mathfrak{P}}(\beta_i \alpha_{i,\mathfrak{P}})} \right)_{i,\mathfrak{P}} \in C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) . \tag{1.6.h}$$

Since $\beta \in C^{\times +}$, this is equivalent to

$$\left(\beta_i \alpha_{i,\mathfrak{P}} \pi_{i,\mathfrak{P}}^{-v_{\mathfrak{P}}(\beta_i \alpha_{i,\mathfrak{P}})} \right)_{i,\mathfrak{P}} \in C^{\times +}\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{M})) .$$

However, the last statement is again implied by [4, Proposition 45.8], Corollary 2.3 and (1.6.f). □

1.7 Using the isomorphisms in Theorem 1.5, the short exact sequence (1.2.b) yields a short exact sequence

$$K_1(\overline{\mathcal{A}}) \xrightarrow{\hat{\partial}} I_{\mathfrak{g}}/P_{\mathfrak{g}}^+ \xrightarrow{q_2} \mathrm{cl}(\mathcal{A}) \longrightarrow 0 . \tag{1.7.a}$$

Since $\overline{\mathcal{A}}$ is a semilocal ring, the canonical map $\pi \colon \overline{\mathcal{A}}^{\times} \to K_1(\overline{\mathcal{A}})$ is surjective (cf. [4, Theorem 40.31]) and the image of $\hat{\partial}$ in (1.7.a) is equal to the image of the composition

$$\nu \colon \overline{\mathcal{A}}^{\times} \xrightarrow{\pi} K_1(\overline{\mathcal{A}}) \xrightarrow{\hat{\partial}} I_{\mathfrak{g}}/P_{\mathfrak{g}}^+ . \tag{1.7.b}$$

The map ν is given explicitly by the next proposition.

1.8 Proposition *Let $x \in \overline{\mathcal{A}}^{\times}$ and let $a \in \mathcal{A}$ such that $\overline{a} = x$. Then $\nu(x)$ is equal to the class of the ideal $\mathrm{nr}(a)\mathcal{O}_C \in I_{\mathfrak{g}}$ in $I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+}$.*

Proof The map ν is the composite

$$\overline{\mathcal{A}}^{\times} \xrightarrow{\partial \circ \pi} \mathrm{cl}(\mathcal{D}) \xrightarrow{\omega} \frac{J(C) \times J(C)}{(C^{\times +} \times C^{\times +})\mathrm{nr}(U(\mathcal{D}))} \xrightarrow{\psi \circ \sigma} I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+}\,,$$

where ∂ originates from the Mayer-Vietoris sequence and ω, σ, ψ are defined in (1.6.a), (1.6.b), (1.6.g), respectively.

By the theory of Mayer-Vietories sequences, cf. proof of [4, Theorem (49.27)], we have $(\partial \circ \pi)(\bar{a}) = M(\bar{a})$, cf. (1.2.a). In order to describe the image of the class of $M(\bar{a})$ under ω we have to find a $\mathcal{D}_{\mathfrak{p}}$-basis $\lambda_{\mathfrak{p}}$ of $M(\bar{a})_{\mathfrak{p}}$ for each $\mathfrak{p}$. For each $\mathfrak{p}$, the ring $\mathcal{A}_{\mathfrak{p}}$ is semilocal, so that we may choose $a_{\mathfrak{p}} \in \mathcal{A}_{\mathfrak{p}}^{\times}$ such that $\bar{a}_{\mathfrak{p}} \equiv x \mod \mathfrak{f}_{\mathfrak{p}}$, cf. [4, Lemma 50.7]. One easily shows that one can choose

$$\lambda_{\mathfrak{p}} = \begin{cases} (1,1), & \text{if } \mathfrak{f}_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}, \\ (1, a_{\mathfrak{p}}), & \text{if } \mathfrak{f}_{\mathfrak{p}} \neq \mathcal{M}_{\mathfrak{p}}. \end{cases}$$

By the definition of ω the image of the class of $M(\bar{a})$ is therefore represented by $(y_{\mathfrak{p}}, z_{\mathfrak{p}}) \in J(C) \times J(C)$ with

$$(y_{\mathfrak{p}}, z_{\mathfrak{p}}) = \begin{cases} (1,1), & \text{if } \mathfrak{f}_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}, \\ (1, \mathrm{nr}(a_{\mathfrak{p}})), & \text{if } \mathfrak{f}_{\mathfrak{p}} \neq \mathcal{M}_{\mathfrak{p}}. \end{cases}$$

It follows from the definition of σ together with Corollary 2.3, that we may choose $\beta = \mathrm{nr}(a)$ in the definition of ψ. The result now follows easily. □

The following corollary is now immediate.

1.9 Corollary *If $a_1, \ldots, a_s$ are elements in $\mathcal{A}$ such that $\pi(\overline{a}_1), \ldots, \pi(\overline{a}_s)$ are generators of $K_1(\overline{\mathcal{A}})$, and if U is the subgroup of $I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+}$ generated by the classes of the ideals $\mathrm{nr}(a_j)\mathcal{O}_C$, $j = 1, \ldots, s$, then there exists an isomorphism*

$$\mathrm{cl}(\mathcal{A}) \cong \left(I_{\mathfrak{g}}/P_{\mathfrak{g}}^{+}\right)/U\,.$$

2 A local result

The aim of this section is to provide Corollary 2.3 which was needed in the proof of Theorem 1.5.

2.1 Notation Throughout this section we assume the following notation. We deviate from our general assumption in the introduction and assume (for this section only) that K is a finite extension field of the field $\mathbb{Q}_p$ of p-adic numbers. We write $\mathcal{O}$ for its valuation ring, $\mathfrak{p}$ for its maximal ideal, and choose a prime element π (so that $\mathfrak{p} = \pi\mathcal{O}$).

Furthermore, we denote by D a division ring with $Z(D) = K$. We refer the reader to [10, Section 14] for standard results in this situation. One has $[D : K] = n^2$ for some $n \in \mathbb{N}$. We denote by Δ the maximal order of D, and by $\mathfrak{P}$ the unique maximal (two-sided) ideal of Δ. Every non-zero (two-sided) ideal of Δ is of the form $\mathfrak{P}^k$ for some $k \in \mathbb{N}_0$.

If $q := |\mathcal{O}/\mathfrak{p}|$, then we can choose a root of unity ω of order $q^n - 1$ in Δ. For given $\pi \in \mathcal{O}$ and ω there exist an element $\pi_D \in \mathfrak{P}$ and a natural number $r \in \{1, \ldots, n\}$ which is coprime to n such that

$$\mathfrak{P} = \pi_D \Delta = \Delta \pi_D \,, \quad \pi_D^n = \pi \,, \quad \pi_D \omega \pi_D^{-1} = \omega^{q^r} \,. \tag{2.1.a}$$

By $\mathrm{nr} \colon D \to K$ we denote the reduced norm map.

2.2 Theorem *For every $k \in \mathbb{N}_0$ and $t \in \{1, \ldots, n\}$ one has*

$$\mathrm{nr}(1 + \mathfrak{P}^{kn+t}) = 1 + \mathfrak{p}^{k+1} \,.$$

Proof The unramified extension $W := K(\omega)$ of K has degree n and is a splitting field for D. Moreover, by the paragraphs preceding [10, Theorem 14.5], the set $\{1, \pi_D, \ldots, \pi_D^{n-1}\}$ is an $\mathcal{O}_W$-basis of Δ. We denote by θ the Galois automorphism of W over K with $\theta(\omega) = \omega^{q^r}$. Note that θ generates the Galois group $\mathrm{Gal}(W/K)$. As in the proof of [10, Theorem 14.6], we obtain an isomorphism $W \otimes_K D \to \mathrm{Mat}_n(W)$ of W-algebras such that

$$1 \otimes \pi_D \mapsto \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & \cdots & 0 & 1 \\ \pi & 0 & \cdots & 0 & 0 \end{pmatrix}$$

and

$$1 \otimes w \mapsto \begin{pmatrix} w & & & \\ & \theta(w) & & \\ & & \ddots & \\ & & & \theta^{n-1}(w) \end{pmatrix}$$

for $w \in W$. If $\delta = a_0 + a_1 \pi_D + \ldots + a_{n-1} \pi_D^{n-1}, a_i \in \mathcal{O}_W$, is an arbitrary element in Δ, then $1 \otimes \delta \mapsto A(\delta)$ with

$$A(\delta) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & & a_{n-1} \\ \theta(a_{n-1})\pi & \theta(a_0) & \theta(a_1) & \cdots & & \theta(a_{n-2}) \\ \theta^2(a_{n-2})\pi & \theta^2(a_{n-1})\pi & \theta^2(a_0) & \cdots & & \theta^2(a_{n-3}) \\ \vdots & \vdots & \vdots & & & \vdots \\ \theta^{n-1}(a_1)\pi & \theta^{n-1}(a_2)\pi & \theta^{n-1}(a_3)\pi & \cdots & \theta^{n-1}(a_{n-1})\pi & \theta^{n-1}(a_0) \end{pmatrix}$$

An elementary computation using $\pi_D^n = \pi$ shows that

$$A(\delta \pi_D^{kn+t}) = \begin{pmatrix} a_{n-t}\pi^{k+1} & & & * \cdot \pi^k \\ & & \ddots & \\ * \cdot \pi^{k+2} & & & \theta^{n-1}(a_{n-t})\pi^{k+1} \end{pmatrix}$$

for any $k \in \mathbb{N}_0$ and $t \in \{1, \dots, n\}$. There are always n consecutive diagonals involving a factor π^{k+1}, including the main diagonal. For $t = 1$ this block of n diagonals extends from the bottom left corner to the main diagonal. For $t = n$ it extends from the main diagonal to the top right corner. While t moves from 1 to n this block moves diagonally from the lower left to the upper right corner. Every entry to the left and below this block is divisible by π^{k+2} and every entry to the right and above this block is divisible by π^k. Since $\mathrm{nr}(1+\delta) = \det(1 + A(\delta))$, it follows immediately that

$$\mathrm{nr}(1 + \mathfrak{P}^{kn+t}) \subseteq 1 + \mathfrak{p}^{k+1}\,,$$

for $k \in \mathbb{N}_0$ and $t \in \{1, \dots, n\}$.

Next we will show that

$$\frac{1 + \mathfrak{P}^{kn+t}}{1 + \mathfrak{P}^{(k+1)n+t}} \xrightarrow{\mathrm{nr}} \frac{1 + \mathfrak{p}^{k+1}}{1 + \mathfrak{p}^{k+2}} \tag{2.2.a}$$

is surjective for $k \geqslant 0$ and $t \in \{1, \dots, n\}$. Without loss of generality we may assume $t = n$. For $b \in \mathcal{O}$ we have to find $\delta \in \Delta$ such that

$$\mathrm{nr}(1 + \delta\pi_D^{(k+1)n}) \equiv 1 + b\pi^{k+1} \mod 1 + \mathfrak{p}^{k+2}\,.$$

Since W/K is unramified, there exists an element $a \in \mathcal{O}_W$ such that $\mathrm{Tr}_{W/K}(a) = b$. Setting $\delta = a$ we obtain

$$\begin{aligned}\mathrm{nr}(1 + a\pi_D^{(k+1)n}) &\equiv \det \begin{pmatrix} 1 + a\pi^{k+1} & & & * \\ 0 & 1 + \theta(a)\pi^{k+1} & & \\ & & \ddots & \\ 0 & & & 1 + \theta^{n-1}(a)\pi^{k+1} \end{pmatrix} \\ &\equiv 1 + \mathrm{Tr}_{W/K}(a)\pi^{k+1} \equiv 1 + b\pi^{k+1} \mod \mathfrak{p}^{k+2}\,.\end{aligned}$$

By induction on l it follows easily that

$$\mathrm{nr}_l \colon \frac{1 + \mathfrak{P}^{kn+t}}{1 + \mathfrak{P}^{(k+l)n+t}} \longrightarrow \frac{1 + \mathfrak{p}^{k+1}}{1 + \mathfrak{p}^{k+l+1}}$$

is surjective for all $k \geqslant 0$ and $l \geqslant 1$. Hence we have a short exact sequence of projective systems (indexed by l) of finite abelian groups

$$0 \to (\ker(\mathrm{nr}_l))_l \longrightarrow \left(\frac{1 + \mathfrak{P}^{kn+t}}{1 + \mathfrak{P}^{(k+l)n+t}}\right)_l \xrightarrow{\mathrm{nr}} \left(\frac{1 + \mathfrak{p}^{k+1}}{1 + \mathfrak{p}^{k+l+1}}\right)_l \to 0\,.$$

Since $\ker(\mathrm{nr}_l)$ is a finite abelian group for all l, it satisfies clearly the Mittag-Leffler condition, so that

$$\varprojlim_l \frac{1 + \mathfrak{P}^{kn+t}}{1 + \mathfrak{P}^{(k+l)n+t}} \xrightarrow{nr} \varprojlim_l \frac{1 + \mathfrak{p}^{k+1}}{1 + \mathfrak{p}^{k+l+1}} \tag{2.2.b}$$

is surjective by [8, Proposition 9.1]. Since Δ, resp. $\mathcal{O}$, is complete relative to the $\mathfrak{P}$-adic, resp. $\mathfrak{p}$-adic, valuation, we derive from (2.2.b) immediately the assertion of the theorem. □

2.3 Corollary *Let $K/\mathbb{Q}_p$ be a finite field extension and let $A \cong \mathrm{Mat}_m(D)$ be a finite dimensional central simple K-algebra, where D is a division ring with $Z(D) = K$ and $[D : K] = n^2$. Furthermore, let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A and let $\mathfrak{P}$ be the maximal ideal of $\mathcal{M}$. Then*

$$\mathrm{nr}(1 + \mathfrak{P}^{kn+t}) = 1 + \mathfrak{p}^{k+1}$$

for all $k \in \mathbb{N}_0$ and all $t \in \{1, \ldots, n\}$.

Proof This is an immediate consequence of Theorem 2.2, [10, Theorem 17.3] and the formula

$$\mathrm{nr}_{A/K}(X) = \mathrm{nr}_{D/K}(\mathrm{Ddet}(X))$$

for any $X \in \mathrm{GL}_m(D)$ (see [4, Equation (7.42)]). Here $\mathrm{Ddet}\colon \mathrm{GL}_m(D) \to D^\times_{\mathrm{ab}}$ denotes the Dieudonné determinant. □

3 An algorithm to compute $\mathrm{cl}(\mathcal{A})$ in the group algebra case

In this section we present an algorithm which computes the locally free class group $\mathrm{cl}(\mathcal{A})$ of any $\mathcal{O}_K$-order $\mathcal{A}$ in the group algebra KG of a finite group G. Moreover, the algorithm computes the so-called kernel group $D(\mathcal{A})$, namely the kernel of the canonical map $\mathrm{cl}(\mathcal{A}) \to \mathrm{cl}(\mathcal{M})$, where $\mathcal{M}$ is a maximal $\mathcal{O}_K$-order of KG containing $\mathcal{A}$. It is well-known that $D(\mathcal{A})$ does not depend on the choice of $\mathcal{M}$. The algorithm presented here has been implemented in Magma, cf. [9], however only for $K = \mathbb{Q}$. We expect it to be straightforward to extend it to arbitrary K.

3.1 Input: We assume that we are given a number field K, its ring of integers $R := \mathcal{O}_K$, a finite group G and an R-order $\mathcal{A}$ of KG.

3.2 Computation of $I_{\mathfrak{g}}/P^+_{\mathfrak{g}}$:

(a) Compute the order n of G, the exponent e of G, and the character table of G. The character table comes with a set $\mathcal{C}$ of representatives of conjugacy classes of G.

(b) Define $L := K(\zeta)$, where $\zeta \in \mathbb{C}$ is a root of unity of order e and compute $\Omega := \mathrm{Gal}(L/K)$.

(c) Compute representatives $\chi_1, \ldots, \chi_r$ of the Ω-orbits of the set $\mathrm{Irr}(G)$ of irreducible characters of G. Denote by X_i the Ω-orbit of χ_i. Furthermore, for $i = 1, \ldots, r$, compute the number field $K_i := K(\{\chi_i(g) \mid g \in \mathcal{C}\})$ and its ring of integers $R_i := \mathcal{O}_{K_i}$.

(d) For $\chi \in \mathrm{Irr}(G)$ let $e_\chi := \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$ be the corresponding primitive central idempotent of the group algebra LG. Then, $e_i := \sum_{\chi \in X_i} e_\chi$, $i = 1, \ldots, r$, are the primitive central idempotents of $A := KG$.

(e) Using the Round 2-algorithm described in [7, Kapitel 3 and 4] compute a maximal R-order $\mathcal{M}$ in A that contains $\mathcal{A}$.

(f) Applying [7, Algorithmus (2.16)] compute the left conductor $\mathfrak{c}_l := \{x \in A \mid x\mathcal{M} \subset \mathcal{A}\}$, the right conductor $\mathfrak{c}_r := \{x \in A \mid \mathcal{M}x \subset \mathcal{A}\}$ and $\mathfrak{f} := \mathfrak{c}_r \cdot \mathfrak{c}_l$. Then $\mathfrak{f}$ is an ideal of $\mathcal{M}$ that is contained in $\mathcal{A}$. Compute $\mathfrak{f}_i := \mathfrak{f} \cdot e_i$ for $i = 1, \ldots, r$.

(g) Compute the unique K-algebra map $K_i \to A_i$ with the property that $\chi_i(g) \mapsto \sum_{\chi \in X_i} \chi(g) e_\chi$. This map identifies K_i with $Z(A_i)$. Using this identification, compute the ideal $\mathfrak{g}_i := R_i \cap \mathfrak{f}_i$ of R_i for $i = 1, \ldots, r$.

(h) For $i = 1, \ldots, r$ compute the Frobenius-Schur indicator $c(\chi_i) := |G|^{-1} \sum_{g \in G} \chi_i(g^2)$ of χ_i. It is known that $c(\chi_i) \in \{-1, 0, 1\}$, cf. [11, Section 13.2]. Obviously, $c(\chi) = c(\chi_i)$ for every $\chi \in X_i$. A Galois automorphism $\tau \in \Omega$ is a real embedding such that $A_i \otimes_{K_i, \tau} \mathbb{R}$ is a matrix algebra over the quaternions if and only if the Schur-Frobenius indicator equals -1, cf. [11, Section 13.2]. This allows to compute ∞_i for $i = 1, \ldots, r$.

(i) Using Algorithm 4.3.1 of [3] component-wise compute the ray class group $I_\mathfrak{g}/P_\mathfrak{g}^+$.

3.3 Remark For computational reasons we wish to choose $\mathfrak{f}$ as large as possible. For special orders $\mathcal{A}$ there may be better ways to compute an ideal $\mathfrak{f}$ than the one described in (f). For example, if $\mathcal{A} = \mathcal{O}_K G$ is the integral group ring, then $\mathfrak{c}_r = \mathfrak{c}_l$, cf. [4, Theorem (27.8)], so that we can take $\mathfrak{f} = \mathfrak{c}_r = \mathfrak{c}_l$. Then $\mathfrak{f}$ is the largest ideal of $\mathcal{M}$ that is contained in $\mathcal{A}$.

3.4 Before we turn to the algorithm for the computation of generators of $K_1(\overline{\mathcal{A}})$ we state two preparatory lemmas.

Let $\mathfrak{g} = \prod_{\mathfrak{P} \in \mathcal{P}} \mathfrak{P}^{e_\mathfrak{P}}$ be the prime ideal decomposition of $\mathfrak{g}$ in $\mathcal{O}_C$, and set $\mathcal{P}' := \{\mathfrak{P} \cap \mathcal{A} \mid \mathfrak{P} \in \mathcal{P}\}$, a set of prime ideals of $\mathcal{A} \cap \mathcal{O}_C$. For every $\mathfrak{p} \in \mathcal{P}'$ consider the ideal

$$\mathfrak{q} := \bigcap_{\substack{\mathfrak{P} \in \mathcal{P} \\ \mathfrak{P} \cap \mathcal{A} = \mathfrak{p}}} (\mathfrak{P}^{e_\mathfrak{P}} \cap \mathcal{A}) \,.$$

These are precisely the factors in the primary decomposition of $\mathfrak{g}$, cf. [1, Prop. 3.2]. We write $\mathcal{Q}$ for the set of ideals $\mathfrak{q}$.

3.5 Lemma *Assume the above notations. Then one has*

$$\mathfrak{f} = \bigcap_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f}) = \prod_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f}) \,.$$

Proof For $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathcal{Q}$, $\mathfrak{q}_1 \neq \mathfrak{q}_2$, one has

$$(\mathfrak{q}_1\mathcal{A} + \mathfrak{f}) + (\mathfrak{q}_2\mathcal{A} + \mathfrak{f}) = \mathcal{A}, \quad (\mathfrak{q}_1\mathcal{A} + \mathfrak{f})(\mathfrak{q}_2\mathcal{A} + \mathfrak{f}) = (\mathfrak{q}_2\mathcal{A} + \mathfrak{f})(\mathfrak{q}_1\mathcal{A} + \mathfrak{f}).$$

It follows easily that $\bigcap_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f}) = \prod_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f})$. Since $\mathfrak{g} = \prod_{\mathfrak{q} \in \mathcal{Q}} \mathfrak{q}$ we conclude $\mathfrak{f} \subseteq \bigcap_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f}) = \prod_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\mathcal{A} + \mathfrak{f}) \subseteq \mathfrak{f}$. □

3.6 Lemma *Let $\pi\colon T \to S$ be an epimorphism of rings. Suppose that* $\ker(\pi)$ *is contained in the Jacobson radical $J(T)$ of T. If $s \in S^\times$, then every preimage t of s is a unit in T.*

Proof This follows immediately from $tT + \ker(\pi) = T = Tt + \ker(\pi)$ and Nakayama's lemma. □

3.7 Computation of generators of $K_1(\overline{\mathcal{A}})$:

(a) Applying the Chinese remainder theorem, cf. [12, Theorem A10], to the decomposition of Lemma 3.5, we obtain

$$\mathcal{A}/\mathfrak{f} \cong \prod_{\mathfrak{q}\in\mathfrak{Q}} \mathcal{A}/(\mathfrak{q}\mathcal{A}+\mathfrak{f})\,, \tag{3.7.a}$$

This induces a decomposition $K_1(\overline{\mathcal{A}}) \cong \prod_{\mathfrak{q}\in\mathfrak{Q}} K_1(\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f})$ and our task is reduced to finding generators of the group $K_1(\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f})$ for every $\mathfrak{q} \in \mathfrak{Q}$.

Let $\mathfrak{q} \in \mathfrak{Q}$ and let $\mathfrak{p} \in \mathcal{P}'$ be the associated prime ideal of $\mathcal{A} \cap \mathcal{O}_C$. Then we have a natural surjective ring homomorphism $\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f} \to \mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$ and there exists a unique prime number p such that $p \in \mathfrak{p}$. Thus, the latter ring is an algebra over the field $\mathbb{F}_p$ with p elements. We have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \dfrac{1+\mathfrak{p}\mathcal{A}+\mathfrak{f}}{1+\mathfrak{q}\mathcal{A}+\mathfrak{f}} & \longrightarrow & (\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f})^\times & \longrightarrow & (\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f})^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U & \longrightarrow & K_1(\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f}) & \longrightarrow & K_1(\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}) & \longrightarrow & 1
\end{array}$$

with natural maps, where U is defined as the kernel of the bottom right horizontal map. Since $\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f}$ and $\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$ are semilocal rings, the middle and right vertical maps are surjective, cf. [4, Theorem 40.31]. By a result of Vaserstein, cf. [4, Remark 40.32(ii)], the kernel of the right vertical map is generated by all elements of the form $(1+xy)(1+yx)^{-1}$ with $x, y \in \mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$ such that $(1+xy)$ and $(1+yx)$ are units in $\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$. The same statement holds for $\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f}$. Since $\mathfrak{p}^l \subseteq \mathfrak{q}$ for some $l \in \mathbb{N}$, the ideal $\mathfrak{p}\mathcal{A}+\mathfrak{f}/\mathfrak{q}\mathcal{A}+\mathfrak{f}$ is contained in the Jacobson radical $J(\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f})$. Thus, every lift of a unit of $\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$ to $\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f}$ is a unit, cf. Lemma 3.6. This implies that the top right horizontal map is surjective, as well as the induced map between the kernels of the middle and right vertical maps. The snake lemma now implies that the left vertical map is surjective. Thus, we obtain an exact sequence

$$\frac{1+\mathfrak{p}\mathcal{A}+\mathfrak{f}}{1+\mathfrak{q}\mathcal{A}+\mathfrak{f}} \to K_1(\mathcal{A}/\mathfrak{q}\mathcal{A}+\mathfrak{f}) \to K_1(\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}) \to 1\,.$$

So our task is reduced to finding generators of $\frac{1+\mathfrak{p}\mathcal{A}+\mathfrak{f}}{1+\mathfrak{q}\mathcal{A}+\mathfrak{f}}$ and $K_1(\mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f})$.

(b) In order to compute generators of the multiplicative group $\frac{1+\mathfrak{p}\mathcal{A}+\mathfrak{f}}{1+\mathfrak{q}\mathcal{A}+\mathfrak{f}}$ we use the filtration

$$\mathfrak{p}\mathcal{A}+\mathfrak{f} \supseteq (\mathfrak{q}+\mathfrak{p}^2)\mathcal{A}+\mathfrak{f} \supseteq (\mathfrak{q}+\mathfrak{p}^4)\mathcal{A}+\mathfrak{f} \supseteq \cdots \supseteq (\mathfrak{q}+\mathfrak{p}^{2^{l-1}})\mathcal{A}+\mathfrak{f} \supseteq \mathfrak{q}\mathcal{A}+\mathfrak{f}$$

with l minimal such that $\mathfrak{p}^{2^l} \subseteq \mathfrak{q}$. For each integer $m \geqslant 0$, the map $x \mapsto x-1$ induces an isomorphism

$$\frac{1+(\mathfrak{q}+\mathfrak{p}^{2^m})\mathcal{A}+\mathfrak{f}}{1+(\mathfrak{q}+\mathfrak{p}^{2^{m+1}})\mathcal{A}+\mathfrak{f}} \to \frac{(\mathfrak{q}+\mathfrak{p}^{2^m})\mathcal{A}+\mathfrak{f}}{(\mathfrak{q}+\mathfrak{p}^{2^{m+1}})\mathcal{A}+\mathfrak{f}}$$

of abelian groups. Assuming that each of the modules can be represented by a $\mathbb{Z}$-basis, we apply Hermite normal form techniques to compute a $\mathbb{Z}$-basis for the right hand side. Lifting generators of $\frac{1+(\mathfrak{q}+\mathfrak{p}^{2^m})\mathcal{A}+\mathfrak{f}}{1+(\mathfrak{q}+\mathfrak{p}^{2^{m+1}})\mathcal{A}+\mathfrak{f}}$ to $1+(\mathfrak{q}+\mathfrak{p}^{2^m})\mathcal{A}+\mathfrak{f}$ and collecting these elements for $m=0,\ldots,l-1$ yields a set of elements of $\mathcal{A}$, whose classes modulo $1+\mathfrak{q}\mathcal{A}+\mathfrak{f}$ generate $\frac{1+\mathfrak{p}\mathcal{A}+\mathfrak{f}}{1+\mathfrak{q}\mathcal{A}+\mathfrak{f}}$.

(c) We put $B := \mathcal{A}/\mathfrak{p}\mathcal{A}+\mathfrak{f}$ and note that B is a finite $\mathbb{F}_p$-algebra. In order to compute generators of $K_1(B)$ we use the same arguments as above to obtain an exact sequence

$$1+J \to K_1(B) \to K_1(B/J) \to 1\,,$$

where J denotes the Jacobson radical of B. Algorithms for the computation of the Jacobson radical of associative algebras over $\mathbb{F}_p$ are, for example, discussed in [5, Sec. 2.3] or [6].

This reduces the problem to the computation of generators of $K_1(B/J(B))$ and of $1+J(B)$. The finite ring B/J is semisimple and thus isomorphic to a direct product of matrix rings $\mathrm{Mat}_s(F)$ over finite fields. In order to compute these simple components one can adapt the algorithms described in [5, Sec. 2.4] (see also [7, Sec. 5.2.1]). This leads to a probabilistic algorithm, which performs very well in practice.

Let now $\mathrm{Mat}_s(F)$ be a simple component of B. Using the fact that the canonical maps $F^\times \to K_1(F) \to K_1(\mathrm{Mat}_s(F))$ are isomorphisms, leaves us with the problem of finding a generator of $F^\times$, which we solve by trial and error.

Finally, we still have to find generators of $1+J$. For that purpose we consider again a filtration, namely

$$1+J \supseteq 1+J^2 \supseteq 1+J^4 \supseteq \cdots \supseteq 1+J^{2^{l-1}} \supseteq 1\,,$$

with l minimal such that $J^{2^l}=0$. Then we use the isomorphisms $1+J^{2^m}/1+J^{2^{m+1}} \to J^{2^m}/J^{2^{m+1}}$ induced by $x \mapsto x-1$, for $m=0,\ldots,l-1$. The latter groups are $\mathbb{F}_p$-vector spaces and we compute a basis and proceed similar as in part (b).

3.8 Computation of the image of $\hat{\partial}\colon K_1(\overline{\mathcal{A}}) \to I_\mathfrak{g}/P_\mathfrak{g}^+$: In the previous subsection, generators of $K_1(\overline{\mathcal{A}})$ of the form (u) with $u \in \overline{\mathcal{A}}^\times$ were computed.

Each such u we lift to an element $a \in \mathcal{A}$. Then, by Proposition 1.8, it suffices to compute the ideal $\mathrm{nr}(a)\mathcal{O}_C$. Instead of computing $\mathrm{nr}(a)\mathcal{O}_C$ we write $a = (a_i)_i$ with $a_i \in A_i$ and compute the norm $\alpha_i := N_{A_i/K_i}(a_i) \in R_i$. If $\dim_{K_i} A_i = n_i$, then one has $N_{A_i/K_i}(a_i) = \mathrm{nr}(a_i)^{n_i}$. But knowing the ideal $N_{A_i/K_i}(a_i)R_i$ allows us to compute the ideal $\mathrm{nr}(a_i)R_i$ in the free abelian group $I(K_i)$ of fractional ideals. Now we only have to compute the representative of $(\mathrm{nr}(a_i)R_i)_i$ in $I_{\mathfrak{g}}/P_{\mathfrak{g}}^+$ by component-wise application of [3, Algorithm 4.3.2].

3.9 Computation of $D(G)$: Consider the commutative diagram

$$\begin{array}{ccccccccc} & & & & K_1(\overline{\mathcal{A}}) & \longrightarrow & I_{\mathfrak{g}}/P_{\mathfrak{g}}^+ & \longrightarrow & \mathrm{cl}(\mathcal{A}) \longrightarrow 0 \\ & & & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & 0 & \longrightarrow & I_1/P_1^+ & \xrightarrow{\sim} & \mathrm{cl}(\mathcal{M}) & \longrightarrow & 0 \end{array}$$

with exact rows as in (1.7.a), where we write I_1 for $I_{\mathcal{O}_C}$ and P_1^+ for $P_{\mathcal{O}_C}^+$. Since the vertical maps are surjective with respective kernels $K_1(\overline{\mathcal{A}})$, $(I_{\mathfrak{g}} \cap P_1^+)/P_{\mathfrak{g}}^+$, and $D(\mathcal{A})$, the snake lemma yields an exact sequence

$$K_1(\overline{\mathcal{A}}) \xrightarrow{\hat{\partial}} (I_{\mathfrak{g}} \cap P_1^+)/P_{\mathfrak{g}}^+ \longrightarrow D(\mathcal{A}) \longrightarrow 0\,.$$

Generators of $K_1(\overline{\mathcal{A}})$ have already been computed in 3.7, and the image of these generators under $\hat{\partial}$ is computed as in 3.8.

3.10 Remark We conclude the paper with a remark on our implentation. We decided to choose the algebra system MAGMA because it includes both algorithms for group and representation theory and number theory. Many of the features that we need are already implemented in MAGMA, most importantly the computation of character tables and the computation of ray class groups in number fields. Moreover, we use many of the MAGMA functions which deal with associative algebras over finite fields. Here we should at least mention the computation of Jacobson radicals.

We computed a large number of locally free class groups for integral group rings $\mathbb{Z}G$. Our implementation performs well as long as the character fields $K_i, i = 1, \ldots, r$, are small, say $[K_i : \mathbb{Q}] < 20$. This is explained by the fact, that from the algorithmic point of view the computation of ray class groups is a very hard problem. It seems to be the most difficult and time-consuming part of the algorithm.

References

[1] W. Bley, M. Endres: Picard groups and refined discrete logarithms. *LMS J. Comput. Math.* **8** (2005), 1–16.

[2] H. Cohen: A course in computational algebraic number theory. Springer GTM **138**, New York - Heidelberg 1995.

[3] H. Cohen: Advanced topics in computational number theory. Springer GTM **193**, New York - Heidelberg, 2000.

[4] C. Curtis, I. Reiner: Methods of representation theory, volume I and II. Wiley, 1981 and 1987.

[5] W. Eberly: Computations for Algebras and Group Representations. Doctoral Thesis, University of Toronto, 1989.

[6] K. Friedl, L. Rónyai: polynomial time solutions for some problems in computational algebra. Proceedings, 17th ACM Symposium on Theory of Computing, Providence, 1985, 153–162.

[7] C. Friedrichs: Berechnung von Maximalordnungen über Dedekindringen. Doctoral Thesis, Technische Universität Berlin, 2000.

[8] R. Hartshorne: Algebraic geometry. Springer, New York - Heidelberg 1977.

[9] MAGMA, Version V2.12, Sydney 2005.

[10] I. Reiner: Maximal orders. Academic Press, London 1975.

[11] J. P. Serre: Représentations linéaires des groupes finis. $3^{\text{ème}}$ éd., Hermann, Paris 1978.

[12] R. G. Swan: K-theory of finite groups and orders. Lecture Notes in Math. 149, Springer Verlag 1970.

[13] S. M. J. Wilson: Reduced norms in the K-theory of orders, *J. Algebra* **46** (1977), 1–11.