London Mathematical Society ISSN 1461–1570

COMPUTATIONS IN RELATIVE ALGEBRAIC K-GROUPS

WERNER BLEY AND STEPHEN M. J. WILSON

Abstract

Let G be finite group and K a number field or a p-adic field with ring of integers $\mathcal{O}_K$. In the first part of the manuscript we present an algorithm that computes the relative algebraic K-group $K_0(\mathcal{O}_K[G], K)$ as an abstract abelian group. We also give algorithms to solve the discrete logarithm problems in $K_0(\mathcal{O}_K[G], K)$ and in the locally free class group $\mathrm{cl}(\mathcal{O}_K[G])$. All algorithms have been implemented in MAGMA for the case $K = \mathbb{Q}$.

In the second part of the manuscript we prove formulae for the torsion subgroup of $K_0(\mathbb{Z}[G], \mathbb{Q})$ for large classes of dihedral and quaternion groups.

1. *Introduction*

Let G denote a finite group. The study of the locally free class group $\mathrm{cl}(\mathbb{Z}[G])$ has been to a very large extent motivated by questions and conjectures arising in the field of Galois module theory. Among the large amount of existing work we mention Fröhlich's conjecture (proved by Martin Taylor [**19**]) on the Galois module structure of rings of integers in tame Galois extensions of number fields and the Ω-conjectures of Chinburg [**9**], extending and generalizing Fröhlich's conjecture.

The locally free class group $\mathrm{cl}(\mathbb{Z}[G])$ is the subject of the following exact sequence which is a truncation of the K-theory exact sequence of the functor $\otimes_{\mathbb{Z}}\mathbb{R}$ from projective $\mathbb{Z}[G]$-modules to $\mathbb{R}[G]$-modules,

$$K_1(\mathbb{Z}[G]) \longrightarrow K_1(\mathbb{R}[G]) \longrightarrow K_0(\mathbb{Z}[G], \mathbb{R}) \xrightarrow{\partial^0} \mathrm{cl}(\mathbb{Z}[G]) \longrightarrow 0. \tag{1}$$

Here, $K_0(\mathbb{Z}[G], \mathbb{R})$ is the relative K_0 of the functor. (See Section 2.1 for a brief definition of this and similar relative groups or see [**17**, p. 215]. For a more general view see [**1**, VIII §5]). The interest in $K_0(\mathbb{Z}[G], \mathbb{R})$ stems mainly from arithmetic geometry, where in recent years the study of the values of motivic L-functions at the integers has led to some remarkable conjectures formulated in terms of elements in $K_0(\mathbb{Z}[G], \mathbb{R})$. Among this large body of work we mention the Tamagawa Number Conjecture of Bloch and Kato, and in particular its equivariant refinement due to Burns and Flach. In special cases (namely for Tate motives) these conjectures refine and generalize the conjectures of Fröhlich and Chinburg mentioned above, cf. [**7**], [**4**], [**6**]. Stark-type conjectures imply the validity of the Equivariant Tamagawa Number conjectures modulo the rational subgroup $K_0(\mathbb{Z}[G], \mathbb{Q})$ of $K_0(\mathbb{Z}[G], \mathbb{R})$. It is therefore of particular interest to study $K_0(\mathbb{Z}[G], \mathbb{Q})$.

Received 28 February 2008, revised 17 March 2009; *published* 20 November 2009.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

Let K be a number field and write $\mathcal{O}_K$ for its ring of algebraic integers. In [2], Boltje and the first named author described an algorithm for the explicit computation of the locally free class group $\mathrm{cl}(\mathcal{O}_K[G])$. This algorithm was implemented in MAGMA for the case $K = \mathbb{Q}$. Extending the methods of loc.cit., we derive an explicit description of the relative group $K_0(\mathcal{O}_K[G], K)$ which is suitable for numerical computations. Based on this description we develop an algorithm for the computation of $K_0(\mathcal{O}_K[G], K)$ as an abstract abelian group and a further algorithm for the solution of the discrete logarithm problem in this group. (So the latter algorithm takes an element of $K_0(\mathcal{O}_K[G], K)$ and expresses it in terms of the generators given by the former). Using the K-rational analogue (3) of the exact sequence (1) together with an explicit description of ∂^0 this also solves the discrete logarithm problem in $\mathrm{cl}(\mathcal{O}_K[G])$. Finally, we describe how to compute the natural induction, restriction and quotient maps with respect to our explicit description of the relative group.

All algorithms have been implemented in MAGMA for $K = \mathbb{Q}$. We conclude the first part of the manuscript with some remarks on this implementation. The source code and a sample file are available from

http://www.mathematik.uni-kassel.de/~bley/pub.html.

The second part of this manuscript is motivated by the following two observations.

(a) There were few theoretical results for checking the correctness of our implementation.

(b) Our numerical results clearly show that for certain types of groups, namely dihedral and generalized quaternion groups, one could expect nice and systematic results.

We recall that the relative group that we target has a prime-by-prime decomposition

$$K_0(\mathcal{O}_K[G], K) \simeq \coprod_{\mathfrak{p}} K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p}),$$

where the coproduct extends over all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Each of the groups $K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p})$ is finitely generated and modulo torsion is simply described. (It is naturally isomorphic to the character group of G over $K_\mathfrak{p}$.) The more difficult and interesting part is its torsion subgroup,

$$DT(\mathcal{O}_{K_\mathfrak{p}}[G]) := K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p})_{tors}.$$

We point out that if $\mathfrak{p}$ does not divide the order of G, then $DT(\mathcal{O}_{K_\mathfrak{p}}[G])$ is trivial. Indeed, in this case $\mathcal{O}_{K_\mathfrak{p}}[G]$ is a maximal order and we may apply Theorem 2.4, (ii).

By using sequences derived from cartesian squares and the special opportunities afforded by twisted group rings (extending the methods of [21]) we prove the following results.

THEOREM 1.1. *Let G be a quaternion or dihedral group of order $2^n m$ with $(2, m) = 1$.*
(a) Let p be prime such that $p \mid m$ and $p^2 \nmid m$. Then

$$DT(\mathbb{Z}_p[G]) \simeq \mathbb{F}_p^\times \times \prod_{1<d\mid 2^{n-1}m/p} \left(\mathbb{F}_{p^{r_d}}^\times\right)^{s_d/r_d},$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

where s_d is the order of the group $U_d := (\mathbb{Z}/d\mathbb{Z})^\times/\{\pm 1\}$ and r_d is the order of p in U_d.

(b) Suppose that $n = 2$ or 3. Then

$$DT(\mathbb{Z}_2[G]) \simeq C_2 \times C_2^{(n-2)\frac{m+1}{2}} \times \prod_{1<d|m} \left(\mathbb{F}_{2^{r_d}}^\times\right)^{(n-1)s_d/r_d},$$

where s_d is the order of the group $U_d := (\mathbb{Z}/d\mathbb{Z})^\times/\{\pm 1\}$ and r_d is the order of 2 in U_d.

Our methods of proof apply to a much larger class of groups and we refer the reader to Theorem 8.15 for a general result on metacyclic groups. As a further example we state

THEOREM 1.2. *Let A_4 be the alternating group of order 12. Then $DT(\mathbb{Z}_3[A_4])$ and $DT(\mathbb{Z}_2[A_4])$ both have order 2.*

2. *Relative K-groups and their torsion*

Much of this theory goes through very generally (see [**1**, Chapters VII to IX] and e.g. [**22**]) but we restrict ourselves to the cases in point. We suppose that K is a finite extension field of $\mathbb{Q}$ (the *global case*) or of $\mathbb{Q}_p$ (the *local case*). (After Subsection 2.1 we assume that K itself is global.) We put $\mathcal{O}_K$ for the ring of integers of K. Indeed, if L is a sum, $\oplus_i K_i$, of such fields we put $\mathcal{O}_L$ for its maximal order, $\oplus_i \mathcal{O}_{K_i}$, and we denote by $I(L)$ the group of fractional ideals of $\mathcal{O}_L$ (so $I(L) \cong \oplus_i I(K_i)$).

We take $\mathcal{A}$ to be an $\mathcal{O}_K$-order in a semi-simple K-algebra A and we choose a maximal order $\mathcal{M}$ in A containing $\mathcal{A}$. Since the index $|\mathcal{M} : \mathcal{A}|$ is finite, there is a full (two-sided) ideal of $\mathcal{M}$ contained in $\mathcal{A}$ (e.g. $|\mathcal{M} : \mathcal{A}|\,\mathcal{M}$) and we choose such an ideal $\mathfrak{f}$, our *conductor*. We take C to be the centre, $Z(A)$, of A and we put $\mathfrak{g} := \mathcal{O}_C \cap \mathfrak{f}$.

2.1. *Relative K-groups of arithmetic orders*

In this subsection we recall the definition of the relative algebraic K-group of $\mathcal{A}$ with respect to the functor extending its base ring $\mathcal{O}_K$ to a field. We recall also the basic exact sequences in which the relative group lies and relevant facts about reduced norms. We identify a formula for the torsion subgroup of the relative group. For a ring R, we write $\mathcal{P}(R)$ for the category of finitely generated projective R-modules.

Let E/K be a field extension. We consider the category $\Phi(\mathcal{P}(\mathcal{A}), \otimes_{\mathcal{O}_K} E)$ whose objects are triples (P, φ, Q), where $P, Q \in \mathcal{P}(\mathcal{A})$ and $\varphi : P \otimes_{\mathcal{O}_K} E \longrightarrow Q \otimes_{\mathcal{O}_K} E$ is an isomorphism of $A \otimes_K E$-modules. A morphism $(P, \varphi, Q) \longrightarrow (P_1, \varphi_1, Q_1)$ is a pair of morphisms $u : P \longrightarrow P_1$, $v : Q \longrightarrow Q_1$ of $\mathcal{A}$-modules such that $\varphi_1 \circ (u \otimes \mathrm{id}_E) = (v \otimes \mathrm{id}_E) \circ \varphi$. Clearly, this morphism is an isomorphism if and only if u and v are isomorphisms. We denote the isomorphism class of (P, φ, Q) by $((P, \varphi, Q))$. We say that a sequence $0 \longrightarrow (P_1, \varphi_1, Q_1) \longrightarrow (P, \varphi, Q) \longrightarrow (P_2, \varphi_2, Q_2) \longrightarrow 0$ in this category is a short exact sequence if the component sequences $0 \longrightarrow P_1 \longrightarrow P \longrightarrow P_2 \longrightarrow 0$ and $0 \longrightarrow Q_1 \longrightarrow Q \longrightarrow Q_2 \longrightarrow 0$ are short exact sequences.

The group $K_0(\mathcal{A}, \otimes_{\mathcal{O}_K} E)$, the relative K_0 of $\mathcal{A}$ with respect to the functor $\otimes_{\mathcal{O}_K} K$, is the abelian group generated by isomorphism classes of such triples with relations $((P, \varphi, Q)) - ((P_1, \varphi_1, Q_1)) - ((P_2, \varphi_2, Q_2))$ for each short exact sequence

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

as above and $((P,\varphi\psi,R))-((P,\psi,Q))-((Q,\varphi,R))$ for each $P,Q,R\in\mathcal{P}(\mathcal{A})$ and isomorphisms $\varphi: Q\otimes_{\mathcal{O}_K}E\longrightarrow R\otimes_{\mathcal{O}_K}E$ and $\psi: P\otimes_{\mathcal{O}_K}E\longrightarrow Q\otimes_{\mathcal{O}_K}E$. We write $[P,\varphi,Q]$ for the image of $((P,\varphi,Q))$ in $K_0(\mathcal{A},\otimes_{\mathcal{O}_K}E)$. If the ground field K is understood (as in the case where $\mathcal{A}=\mathcal{O}_K[G]$ for some finite group G) one often writes $K_0(\mathcal{A},E)$ for $K_0(\mathcal{A},\otimes_{\mathcal{O}_K}E)$.

In fact, for any such E, $K_0(\mathcal{A},K)$ may be identified with a subgroup of $K_0(\mathcal{A},E)$ and is, indeed, the most interesting part. So we shall restrict our attention to $K_0(\mathcal{A},K)$. It is worth noting that, as can be readily deduced from the work below, if $\mathcal{A}$ is commutative then the group, $I(\mathcal{A})$, of invertible fractional ideals of $\mathcal{A}$ is isomorphic to $K_0(\mathcal{A},K)$ (by $\mathfrak{a}\mapsto[\mathfrak{a},1,\mathcal{A}]$). Thus $K_0(\mathcal{A},K)$ can be viewed as a (commutative) generalization of $I(\mathcal{A})$ for non-commutative $\mathcal{A}$.

We put $DT(\mathcal{A})$ for the torsion subgroup of $K_0(\mathcal{A},K)$. Note that up to a natural isomorphism $K_0(\mathcal{A},K)$ depends only on $\mathcal{A}$, since the functors, $\otimes_{\mathbb{Z}}\mathbb{Q}$, $\otimes_{\mathcal{O}_K}K$ and $A\otimes_{\mathcal{A}}$ from $\mathcal{P}(\mathcal{A})$ to $\mathcal{P}(A)$ are isomorphic. Indeed, $K_0(\mathcal{A},K)$ has an alternative description as $K_0(H^t(\mathcal{A}))$ (also written $K_0T(\mathcal{A})$), the Grothendieck group (with respect to exact sequences) of $H^t(\mathcal{A})$, the category of $\mathbb{Z}$-torsion $\mathcal{A}$-modules of finite projective dimension (see [**1**, p. 432]). It then follows (by using the Chinese Remainder Theorem decomposition of these torsion modules) that, for K global, we have the following decompositions induced by the localisation functors:

$$K_0(\mathcal{A},K)\simeq\coprod_{\mathfrak{p}}K_0(\mathcal{A}_{\mathfrak{p}},K_{\mathfrak{p}}),\quad DT(\mathcal{A})\simeq\coprod_{\mathfrak{p}}DT(\mathcal{A}_{\mathfrak{p}}).\tag{2}$$

The coproducts run over all the non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Here and below we use the following standard notation. If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, then $K_{\mathfrak{p}}$ denotes the completion of K at $\mathfrak{p}$. If M is an $\mathcal{O}_K$-module, we write $M_{\mathfrak{p}}:=M\otimes_{\mathcal{O}_K}\mathcal{O}_{K_{\mathfrak{p}}}$ for the completion of M at $\mathfrak{p}$. Similarly, if V is a K-vector space, we set $V_{\mathfrak{p}}:=V\otimes_K K_{\mathfrak{p}}$.

If $\rho: R\to S$ is a ring homomorphism we write $k_i(\rho): K_i(R)\to K_i(S)$ for the homomorphisms induced by $S\otimes_R$. We recall ([**1**, VII 5.3 or IX 6.3]) that our relative group, as this name suggests, fits into the exact sequence of the functor $A\otimes_{\mathcal{A}}:\mathcal{P}(\mathcal{A})\to\mathcal{P}(A)$:

$$K_1(\mathcal{A})\xrightarrow{k_1(\lambda)}K_1(A)\xrightarrow{\delta_{\mathcal{A}}}K_0(\mathcal{A},K)\xrightarrow{\partial^0}K_0(\mathcal{A})\xrightarrow{k_0(\lambda)}K_0(A)\tag{3}$$

Here $\delta_{\mathcal{A}}([A^n,\varphi])=[\mathcal{A}^n,\varphi,\mathcal{A}^n]$, $\partial^0[P,\varphi,Q]=[P]-[Q]$ and $\lambda:\mathcal{A}\to A$ is the inclusion map.

Remark 2.1. We choose our notation "$DT(\mathcal{A})$" because (see Theorem 2.4(iii)) for a group ring $\mathcal{A}$, at least, $DT(\mathcal{A})$ bears a similar relation to $K_0(\mathcal{A},K)=K_0T(\mathcal{A})$ as the "kernel" subgroup, $D(\mathcal{A})$ does to $K_0(\mathcal{A})$. Indeed, ∂^0 maps $DT(\mathcal{A})$ onto $D(\mathcal{A})$.

We make considerable use of the reduced norm $\mathrm{nr}=\mathrm{nr}_A:A^\times\to C^\times$, of its extension to $K_1(A)$ and of the restriction of this to $K_1(\mathcal{A})$, these last two maps will also be denoted nr. In view of (2) our work on the relative group will be almost exclusively with local orders, even if we keep a global order in mind. We now group together a number of the local results to which we shall need to refer. Recall that $SK_1(\mathcal{A})$ is the kernel of the reduced norm on $K_1(\mathcal{A})$.

A ring R is called (left) hereditary if every left ideal of R is projective as a left R-module. We recall that every maximal order over a Dedekind domain is hereditary.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

THEOREM 2.2. *In the local case:*

(i) $\mathrm{nr} : K_1(A) \longrightarrow C^\times$ *is an isomorphism and* $\mathrm{nr}(A^\times) = C^\times$.

(ii) $\mathrm{nr}_A \circ \delta_{\mathcal{A}}^{-1}$ *induces an isomorphism* $\overline{\mathrm{n}}_{\mathcal{A}} : \delta_{\mathcal{A}}(K_1(A)) \longrightarrow C^\times/\mathrm{nr}(K_1(\mathcal{A}))$. *This is natural with respect to extension of order: if* $\mathcal{B}$ *is an order containing* $\mathcal{A}$ *then we have a commutative square.*

$$\begin{array}{ccc} \delta_{\mathcal{A}}(K_1(A)) & \xrightarrow{\overline{\mathrm{n}}_{\mathcal{A}}} & C^\times/\mathrm{nr}(K_1(\mathcal{A})) \\ \downarrow [\mathcal{B}\otimes_{\mathcal{A}}] & & \downarrow \\ \delta_{\mathcal{B}}(K_1(A)) & \xrightarrow{\overline{\mathrm{n}}_{\mathcal{B}}} & C^\times/\mathrm{nr}(K_1(\mathcal{B})) \end{array}$$

(iii) The map $\mathcal{A}^\times \longrightarrow K_1(\mathcal{A})$ *is surjective and so* $\mathrm{nr}(\mathcal{A}^\times) = \mathrm{nr}(K_1(\mathcal{A}))$.

(iv) If $\mathcal{A}$ *is hereditary then* $\mathrm{nr}(\mathcal{A}^\times) = {\mathcal{O}_C}^\times$.

(v) If A *is commutative then* $SK_1(\mathcal{A}) = \{0\}$ *and* $\mathrm{nr} : K_1(\mathcal{A}) \longrightarrow \mathcal{A}^\times$ *is an isomorphism.*

(vi) $K_0(\mathcal{A})$ *is torsion free.*

Proof. (i) We have $\mathrm{nr}(A^\times) = \mathrm{nr}(K_1(A)) = C^\times$ (see e.g. [**8**, Theorem 7.48] or [**20**, X, Prop. 6]) and, by Wang's theorem [**18**], $SK_1(A) = \{0\}$ (but this case is due to Nakayama and Matsushima [**15**]).
(ii) $\overline{\mathrm{n}}_{\mathcal{A}}$ is the composition of the two isomorphisms

$$\delta_{\mathcal{A}}(K_1(A)) \xrightarrow{(\delta_{\mathcal{A}}^{-1})} K_1(A)/\mathrm{img}(K_1(\mathcal{A})) \xrightarrow{(\mathrm{nr}_A)} C^\times/\mathrm{nr}(K_1(\mathcal{A})).$$

The naturality follows from the fact that $[\mathcal{B}\otimes_{\mathcal{A}}] \circ \delta_{\mathcal{A}} = \delta_{\mathcal{B}}$.
(iii), (v) & (vi) See [**1**, IX 1.4] ($\mathcal{A}$ is semilocal).
(iv) See e.g. [**22**, Theorem 2]. □

Part (ii) is a little unsatisfactory as it involves the rather *ad hoc* $\delta_{\mathcal{A}}(K_1(A))$ (though this may be nicely described as the subgroup of triples involving only free modules). The situation for group rings is neater.

THEOREM 2.3. *In the local case, if* $\mathcal{A}$ *is a group ring or a maximal order then*

(i) In (3), $k_0(\lambda)$ *is an isomorphism and so* $\delta_{\mathcal{A}}(K_1(A)) = K_0(\mathcal{A}, K)$.

(ii) $\overline{\mathrm{n}}_{\mathcal{A}}$ *is an isomorphism* $\overline{\mathrm{n}}_{\mathcal{A}} : K_0(\mathcal{A}, K) \to C^\times/\mathrm{nr}(K_1(\mathcal{A}))$.

(iii) If $\mathcal{A}$ *is a maximal order then* $\overline{\mathrm{n}}_{\mathcal{A}} : K_0(\mathcal{A}, K) \xrightarrow{\sim} C^\times/{\mathcal{O}_C}^\times \cong I(C)$.

Proof. (i) See [**1**, X 1.3 & 1.4] — $\mathcal{A}$ satisfies the Cartan condition [**1**, X 1.7 & 1.8]. For (ii) see Theorem 2.2(ii) and for (iii) see Theorem 2.2(iv). □

It follows from Theorem 2.3(i) (after a certain amount of diagram chasing) that, in the global case, if $\mathcal{A}$ is a group ring or a maximal order then the cokernel of $\delta_{\mathcal{A}}$ consists of the locally trivial elements of $K_0(\mathcal{A})$, that is $\mathrm{cl}(\mathcal{A})$, the locally free class group. So we have an exact sequence

$$K_1(\mathcal{A}) \longrightarrow K_1(A) \longrightarrow K_0(\mathcal{A}, K) \longrightarrow \mathrm{cl}(\mathcal{A}) \longrightarrow 0 \tag{4}$$

(see [**8**, Th. (32.1)] or [**22**, (7)]).

We can now give a formula for $DT(\mathcal{A})$ in terms of reduced norms.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

THEOREM 2.4. *In the local case:*

(i) $\overline{\mathrm{n}}_{\mathcal{A}}$ *gives an isomorphism from* $DT(\mathcal{A})$ *to* ${\mathcal{O}_C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times})$*, and this group is finite.*

(ii) If $\mathcal{A}$ *is hereditary (in particular, if* $\mathcal{A}$ *is a maximal order) then* $DT(\mathcal{A}) = \{0\}$.

(iii) The map on relative groups induced by ring extension $(\mathcal{M}\otimes_{\mathcal{A}})$ *from* $\mathcal{A}$ *to a maximal order gives an exact sequence*

$$0 \longrightarrow DT(\mathcal{A}) \hookrightarrow \delta_{\mathcal{A}}(K_1(A)) \xrightarrow{[\mathcal{M}\otimes]} K_0(\mathcal{M}, K) \longrightarrow 0. \tag{5}$$

(iv) Non-canonically, $\delta_{\mathcal{A}}(K_1(A)) \cong I(C) \times DT(\mathcal{A})$

Proof. Note first that by (3) and Theorem 2.2(vi), $DT(\mathcal{A}) \subseteq \delta_{\mathcal{A}}(K_1(A))$ so that $DT(\mathcal{A}) = \delta_{\mathcal{A}}(K_1(A))_{\mathrm{tors}}$. By Theorem 2.2(ii) and Corollary 2.3, we have a commutative diagram with exact rows and vertical isomorphisms (the one on the left being forced by the other two):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker([\mathcal{M}\otimes]) & \longrightarrow & \delta_{\mathcal{A}}(K_1(A)) & \xrightarrow{[\mathcal{M}\otimes]} & K_0(\mathcal{M}, K) & \longrightarrow & 0 \\ & & \downarrow\wr\,(\overline{\mathrm{n}}_{\mathcal{A}}) & & \downarrow\wr\,\overline{\mathrm{n}}_{\mathcal{A}} & & \downarrow\wr\,\overline{\mathrm{n}}_{\mathcal{M}} & & \\ 0 & \longrightarrow & {\mathcal{O}_C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times}) & \longrightarrow & {C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times}) & \longrightarrow & {C}^{\times}/{\mathcal{O}_C}^{\times} & \longrightarrow & 0 \end{array} \tag{6}$$

We find (recall that the conductor $\mathfrak{f}$ was chosen above) that

$$\begin{aligned} \left|{\mathcal{O}_C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times})\right| = \left|\mathrm{nr}(\mathcal{M}^{\times})/\mathrm{nr}(\mathcal{A}^{\times})\right| &\leqslant \left|\mathcal{M}^{\times}/\mathcal{A}^{\times}\right| \leqslant \left|\mathcal{M}^{\times}/(\mathbb{Z}_p + \mathfrak{f})^{\times}\right| \\ &\leqslant |(\mathcal{M}/\mathfrak{f})^{\times}| < |\mathcal{M}/\mathfrak{f}|. \end{aligned}$$

So $\ker([\mathcal{M}\otimes]) \cong {\mathcal{O}_C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times})$ is finite. Moreover $K_0(\mathcal{M}, K) \cong I(C)$ is torsion free. Thus

$$DT(\mathcal{A}) = \ker([\mathcal{M}\otimes]) \cong {\mathcal{O}_C}^{\times}/\mathrm{nr}(\mathcal{A}^{\times})$$

and we have parts (i) and (iii). Morover, since $I(C)$ is torsion free, (5) splits and part (iv) follows.

Also, part (ii) follows from part (i) and Theorem 2.2(iv). □

In the global case $\mathcal{A}_{\mathfrak{p}}$ is a maximal order for all but finitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$ so we have from (2):

COROLLARY 2.5. *In the global case, also,* $DT(\mathcal{A})$ *is finite.*

We now give a description of $DT(\mathcal{A})$ in terms of calculable finite groups. Recall we have chosen a conductor $\mathfrak{f}$ for $\mathcal{A}$ relative to $\mathcal{M}$ and that $\mathfrak{g} = \mathfrak{f} \cap C$.

THEOREM 2.6. *(i) The reduced norm induces a homomorphism*

$$\mu : K_1(\mathcal{A}/\mathfrak{f}) \longrightarrow (\mathcal{O}_C/\mathfrak{g})^{\times}.$$

(ii) We have a canonical isomorphism $DT(\mathcal{A}) \xrightarrow{\sim} \mathrm{cok}(\mu)$*. In the local case it is induced by* $\overline{\mathrm{n}}_{\mathcal{A}}$*.*

Proof. We consider the local case first.

(i) Put $U_{\mathfrak{f}}(\mathcal{A}) := \{a \in \mathcal{A}^{\times} \mid a \equiv 1 \bmod \mathfrak{f}\}$. Note that $U_{\mathfrak{f}}(\mathcal{A}) = U_{\mathfrak{f}}(\mathcal{M})$. By [2, Cor. 2.4], $\mathrm{nr}(U_{\mathfrak{f}}(\mathcal{A})) = U_{\mathfrak{g}}(\mathcal{O}_C)$. Whence, also, $\mathrm{nr}(U_{\mathfrak{f}M}(M)) = U_{\mathfrak{g}}(\mathcal{O}_C)$, where $M = \mathrm{Mat}_n(\mathcal{A})$. Thus the reduced norm induces a map

$$\tilde{\mu} : \mathrm{GL}(\mathcal{A}/\mathfrak{f}) \longrightarrow (\mathcal{O}_C/\mathfrak{g})^{\times}$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

and hence the map μ of (i).

(ii) We can now construct a diagram with exact rows:

$$\begin{array}{ccccccccc} 0 \to & U_{\mathfrak{f}}(\mathcal{A}) & \longrightarrow & \mathcal{A}^\times & \longrightarrow & (\mathcal{A}/\mathfrak{f})^\times & \to 0 \\ & \downarrow \mathrm{nr} & & \downarrow \mathrm{nr} & & \downarrow \mu' & \\ 0 \to & U_{\mathfrak{g}}(\mathcal{O}_C) & \longrightarrow & \mathcal{O}_C^\times & \longrightarrow & (\mathcal{O}_C/\mathfrak{g})^\times & \to 0 \end{array}$$

where μ' factors via μ and has the same image since the map from $(\mathcal{A}/\mathfrak{f})^\times$ to $K_1(\mathcal{A}/\mathfrak{f})$ is surjective (the ring is semilocal). Now, since the left hand vertical map is surjective, the cokernels of the other two are isomorphic. By Theorem 2.4(i) the cokernel of the central arrow is canonically isomorphic to $DT(\mathcal{A})$.

In the global case, for each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ the work above gives us maps

$$\mu_{\mathfrak{p}} : K_1(\mathcal{A}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}}) \to ((\mathcal{O}_C)_{\mathfrak{p}}/\mathfrak{g}_{\mathfrak{p}})^\times \tag{7}$$

and then isomorphisms induced by the Chinese Remainder Theorem give us our homomorphism μ as the composite

$$\mu : K_1(\mathcal{A}/\mathfrak{f}) \xrightarrow{\sim} \coprod_{\mathfrak{p}} K_1(\mathcal{A}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}}) \xrightarrow{\coprod \mu_{\mathfrak{p}}} \coprod_{\mathfrak{p}} ((\mathcal{O}_C)_{\mathfrak{p}}/\mathfrak{g}_{\mathfrak{p}})^\times \xrightarrow{\sim} (\mathcal{O}_C/\mathfrak{g})^\times .$$

Thus we obtain the composite isomorphism:

$$DT(\mathcal{A}) \xrightarrow{\sim} \coprod_{\mathfrak{p}} DT(\mathcal{A}_{\mathfrak{p}}) \xrightarrow{\sim} \coprod_{\mathfrak{p}} \mathrm{cok}(\mu_{\mathfrak{p}}) \xrightarrow{\sim} \mathrm{cok}(\mu). \tag{8}$$

□

2.2. *Local decomposition and uniformising parameters*

In this section, continuing with the assigments and notation established above, we assume the global case (so K is a finite extension of $\mathbb{Q}$) and set up notation to deal with the decomposition of A and the further decomposition of $A_{\mathfrak{p}}$ for maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$. We finish by describing how, in the case where $\mathcal{A}$ is a group ring, we set up an explicit isomorphism between $K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}})$ and $I(C_{\mathfrak{p}}) \times \mathrm{cok}(\mu_{\mathfrak{p}})$.

The primitive idempotents of $C = Z(A)$ will be denoted by $e_1, \ldots, e_r$. For $i = 1, \ldots, r$, we set $A_i := Ae_i$. Then

$$A = A_1 \oplus \cdots \oplus A_r \tag{9}$$

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 $i = 1, \ldots, r$, where D_i is a division ring with $Z(D_i) \cong K_i$. The Wedderburn decomposition (9) induces decompositions

$$C = K_1 \oplus \cdots \oplus K_r \tag{10}$$

and

$$\mathcal{O}_C = \mathcal{O}_{K_1} \oplus \cdots \oplus \mathcal{O}_{K_r} . \tag{11}$$

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

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

$\mathfrak{f}$ 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 $\mathcal{M}_i$ and the ideal $\mathfrak{g} = \mathcal{O}_C \cap \mathfrak{f}$ of $\mathcal{O}_C$ decomposes similarly into ideals $\mathfrak{g}_i = \mathfrak{g}e_i$ of $\mathcal{O}_{K_i}$.

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 ("finite") 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

$$\begin{aligned} A_\mathfrak{p} &\cong K_\mathfrak{p} \otimes_K A \cong \bigoplus_{i=1}^r (K_\mathfrak{p} \otimes_K A_i) \cong \bigoplus_{i=1}^r ((K_\mathfrak{p} \otimes_K K_i) \otimes_{K_i} A_i) \\ &\cong \bigoplus_{i=1}^r \bigoplus_{\mathfrak{P}} (K_i)_\mathfrak{P} \otimes_{K_i} A_i \cong \bigoplus_{i,\mathfrak{P}} A_{i,\mathfrak{P}} \end{aligned} \tag{12}$$

involving various completions, where, for given $i \in \{1, \ldots, r\}$, $\mathfrak{P}$ 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 $\mathcal{L}_i$ of A_i, we denote by $\mathcal{L}_{i,\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of $\mathcal{L}_i$. 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 $\mathfrak{p}$. Similarly we denote by $J(C)$ the group of idèles of C. Again one has a canonical isomorphism

$$C_\mathfrak{p} \cong \bigoplus_{i,\mathfrak{P}} K_{i,\mathfrak{P}} \tag{13}$$

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

Although the torsion subgroup $DT(\mathcal{A})$ of $K_0(\mathcal{A}, K)$ is its most interesting part, we need to be able to deal with the whole of $K_0(\mathcal{A}, K) \cong \coprod_\mathfrak{p} K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p})$ for most applications. In the following proposition we give the way in which we will represent $K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p})$ in the case where $\mathcal{A}$ is a group ring. (This will do in any case where $\delta_{\mathcal{A}_\mathfrak{p}}$ is surjective but, in general, the more varied possibilities for local projectives will need to be taken into account.) We put $\mathfrak{g}_{i,\mathfrak{p}}$ for the $\mathfrak{p}$-part, $(\mathfrak{g}_i)_\mathfrak{p} \cap K_i$, of $\mathfrak{g}_i$ and we will use the decomposition:

$$(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_\mathfrak{p})^\times \simeq \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \tag{14}$$

Proposition 2.7. *Let $\mathcal{A} = \mathcal{O}_K[G]$ for some finite group G. For each pair $(i, \mathfrak{P})$ as in (13) we choose an element $\pi_{i,\mathfrak{P}} \in \mathcal{O}_{K_i}$ which has valuation 1 at $\mathfrak{P}$ and is congruent to 1 modulo $\mathfrak{g}_{\mathfrak{P}'}$ for each other prime $\mathfrak{P}'$ above $\mathfrak{p}$ in K_i/K. Then (with $\mu_\mathfrak{p}$ as in (7)) we have isomorphisms*

$$K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p}) \xrightarrow{\overline{\mathrm{n}}_{\mathcal{A}_\mathfrak{p}}} C_\mathfrak{p}^\times/\mathrm{nr}(\mathcal{A}_\mathfrak{p}^\times) \xrightarrow{\bar{\varphi}} I(C_\mathfrak{p}) \times \mathrm{cok}(\mu_\mathfrak{p}), \tag{15}$$

where $\overline{\mathrm{n}}_{\mathcal{A}_\mathfrak{p}}$ is the natural isomorphism of Theorem 2.2(ii) and $\bar{\varphi}$ is induced by

$$\begin{array}{ccccc} \varphi: & C_\mathfrak{p}^\times & \longrightarrow & I(C_\mathfrak{p}) \times (\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_\mathfrak{p})^\times, \\ \nu = (\nu_1, \ldots, \nu_r) & \mapsto & \left(\left(\prod_\mathfrak{P} \mathfrak{P}^{v_\mathfrak{P}(\nu_i)}\right)_i, (\bar{u}_1, \ldots, \bar{u}_r)\right), \end{array} \tag{16}$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

with $u_i := \nu_i \prod_{\mathfrak{P}} \pi_{i,\mathfrak{P}}^{-v_{\mathfrak{P}}(\nu_i)}$ *(using the localisation of the decomposition (11) on the left and the decomposition (14) on the right).*

Proof. From the diagram (6), by implementing the conclusions of Theorems 2.4(iii), 2.3(i) and 2.6(ii), we have a diagram with exact rows (and canonical maps):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & DT(\mathcal{A}_{\mathfrak{p}}) & \longrightarrow & K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}}) & \xrightarrow{[\mathcal{M}\otimes]} & K_0(\mathcal{M}_{\mathfrak{p}}, K_{\mathfrak{p}}) & \longrightarrow & 0 \\ & & \downarrow\wr\,(\overline{\mathrm{n}}_{\mathcal{A}_{\mathfrak{p}}}) & & \downarrow\wr\,\overline{\mathrm{n}}_{\mathcal{A}_{\mathfrak{p}}} & & \downarrow\wr\,(\overline{\mathrm{n}}_{\mathcal{M}_{\mathfrak{p}}}) & & \\ 0 & \longrightarrow & \mathrm{cok}(\mu_{\mathfrak{p}}) & \longrightarrow & C^{\times}/\mathrm{nr}(\mathcal{A}_{\mathfrak{p}}{}^{\times}) & \xrightarrow{I} & I(C_{\mathfrak{p}}) & \longrightarrow & 0 \end{array} \tag{17}$$

The rows split, since the right hand groups are torsion free, and any splitting of the map I will give an isomorphism between $C_{\mathfrak{p}}^{\times}/\mathrm{nr}(\mathcal{A}_{\mathfrak{p}}^{\times})$ and $I(C_{\mathfrak{p}}) \times \mathrm{cok}(\mu_{\mathfrak{p}})$. Our isomorphism, $\bar{\varphi}$, is given by the splitting which sends the ideal corresponding to the pair $(j, \mathfrak{P})$ to $(a_1, \ldots, a_r) \in \oplus_i K_i$, where $a_i = 1$ except $a_j = \pi_{j,\mathfrak{P}}$. □

Remark 2.8. Since $I(C) \cong \coprod_{\mathfrak{p}} I(C_{\mathfrak{p}})$, isomorphisms from (15), (2) and (8) show that if $\mathcal{A} = \mathcal{O}_K[G]$ then $K_0(\mathcal{A}, K) \cong DT(\mathcal{A}) \oplus I(C) \cong \mathrm{cok}(\mu) \oplus I(C)$.

3. *An algorithm for the computation of* $K_0(\mathcal{A}, K)$

We keep the notation of Section 2 but from here until Section 8, we take K to be an algebraic number field and $\mathcal{A} = \mathcal{O}_K[G]$ for some finite group G. In this section we present an algorithm which computes $K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}})$. By (2) it is straightforward to combine this algorithm for various $\mathfrak{p}$ to obtain $K_0(\mathcal{A}, K)$. The algorithm presented here has been implemented in Magma, cf. [14], however only for $K = \mathbb{Q}$. We expect it to be straightforward to extend it to arbitrary K.

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

3.1. *Computation of* $(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_{\mathfrak{p}})^{\times}$

In [2, Sec. 3.2] it is explained how one can compute the character fields K_i, $i = 1, \ldots, r$, and the two-sided ideal $\mathfrak{f}$. From this the ideals $\mathfrak{g}$ of $\mathcal{O}_C$ and $\mathfrak{g}_i$ of $\mathcal{O}_{K_i}$ are easily deduced.

We note in passing that we can always take take $\mathfrak{f} = |G|\mathcal{M}$ by [8, Th. (27.1)], but algorithmically it is much better to compute the conductor of $\mathcal{A}$ in $\mathcal{M}$ (see also [2, Rem. 3.3]).

We use Algorithm 4.8.17 of [10] to compute the $\mathfrak{p}$-part $\mathfrak{g}_{i,\mathfrak{p}}$ of $\mathfrak{g}_i$ and then we can use the decomposition (14) and Algorithm 4.2.21 of [11] component-wise in order to compute $(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_{\mathfrak{p}})^{\times}$.

3.2. *Computation of* $K_1(\mathcal{A}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})$

The computation of $K_1(\mathcal{A}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})$ is completely analogous to the computation of $K_1(\mathcal{A}/\mathfrak{f})$ which is described in [2, Sec. 3.7]. The only difference is that we have to start with the prime ideal decomposition of $\mathfrak{g}_{\mathfrak{p}}$ in [2, Sec. 3.4], i.e. we only consider prime ideals $\mathfrak{P}$ of $\mathcal{O}_C$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.

3.3. *Computation of reduced norms*

The definition and computation of reduced norms is described in [3, Sec. 3.2], however, we sketch below an alternative algorithm to compute reduced norms based

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

on the computation of reduced traces and Newton's formulae.

We need to calculate the reduced norm $\mathrm{nr}(M)$ of a matrix $M \in \mathrm{Mat}_s(F[G])$, where F is a field of characteristic zero. Let E be an extension of F containing $|G|$th roots of 1 and let X be the set of irreducible characters of G over E. (These can, of course, be calculated from the characters of G over $\mathbb{C}$.) For each $\chi \in X$, let e_χ and $A_\chi = e_\chi E[G]$ be the idempotent and irreducible component of $E[G]$ corresponding to χ. Put $d_\chi = \chi(1_G)$ for the degree of χ. Then

$$\mathrm{nr}(M) = \sum_{\chi \in X} \mathrm{nr}_{A_\chi}(e_\chi M).$$

If we choose an E-isomorphism $\rho_\chi : A_\chi \cong \mathrm{Mat}_{d_\chi}(E)$ then the reduced norm of a matrix $N = (n_{ij}) \in A_\chi$ is given by

$$\mathrm{nr}_{A_\chi}(N) = \det(\rho_\chi(N)),$$

where $\rho_\chi(N) \in \mathrm{Mat}_{sd_\chi}(E)$ is defined by

$$\rho_\chi(N) = (\rho_\chi(n_{ij}))_{1 \leqslant i,j \leqslant s}\,.$$

As in [**3**, Sec. 3.2], we want to calculate this without calculating a matrix representation ρ_χ. We can do this by using the fact that we can easily calculate the trace of $\rho_\chi(b)$ for an element $b \in E[G]$. In fact for $g \in G$, $\chi(g) = \mathrm{Tr}(\rho_\chi(g))$. So, extending χ linearly to $E[G]$ we obtain $\mathrm{Tr}(\rho_\chi(c)) = \chi(c)$ for all $c \in E[G]$ and therefore

$$Tr(\rho_\chi(N)) = \sum_{i=1}^{s} \chi(n_{ii}),$$

or, more generally for a natural number k,

$$Tr(\rho_\chi(N)^k) = \sum_{i=1}^{s} \chi(n_{ii}^{(k)}), \tag{18}$$

where $\left(n_{ij}^{(k)}\right)$ is the matrix N^k. Of course, in (18) we have the sum of the kth powers of the eigenvalues of $\rho_\chi(N)$ and from these sums we can recover the elementary symmetric functions in the eigenvalues, including $\det(\rho_\chi(N))$, by recursively applying Newton's formulae. More explicitly, let $\lambda_1, \ldots, \lambda_{sd_\chi}$ denote the eigenvalues of $\rho_\chi(N)$. We set $s_k := \sum \lambda_i^k$ and write σ_k for the elementary symmetric functions (so $\sigma_{sd_\chi} = \prod \lambda_i$ is the reduced norm which we aim to compute). Then

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \cdots + (-1)^{k-1} s_1 \sigma_{k-1} + (-1)^k k \sigma_k = 0$$

for $k \leqslant sd_\chi$.

3.4. *Computation of* $\mathrm{cok}(\mu_\mathfrak{p})$

Recall the definition of $\mu_\mathfrak{p}$ given in (7). In Subsection 3.2 we computed a set of generators of $K_1(\mathcal{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})$ of the form (u) with $u \in (\mathcal{A}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$. Each such element we lift to an element in $a \in \mathcal{A} \cap A^\times$. By one of the methods of Subsection 3.3 we compute $\mathrm{nr}(a) \in \mathcal{O}_C \simeq \oplus_{i=1}^r \mathcal{O}_{K_i}$ and a representative of $\mathrm{nr}(a)$ by componentwise application of [**11**, Algorithm 4.2.24]. Using the Hermite Normal Form techniques of [**11**, 4.1] we compute $\mathrm{cok}(\mu_\mathfrak{p})$.

This concludes the algorithm for the computation of $DT(\mathcal{A}_\mathfrak{p})$.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

3.5. *Computation of uniformizing elements*

We must choose uniformizing elements as in Proposition 2.7. For each $i \in \{1, \dots, r\}$ and each prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ lying above $\mathfrak{p}$ we compute a uniformizing element $\tilde{\pi}_{i,\mathfrak{P}}$ and solve the system of simultanous congruences

$$\pi_{i,\mathfrak{P}} \equiv \tilde{\pi}_{i,\mathfrak{P}} (\mathrm{mod}\ \mathfrak{P}^2),$$
$$\pi_{i,\mathfrak{P}} \equiv 1 (\mathrm{mod}\ \mathfrak{Q}^{\max(1, v_{\mathfrak{Q}}(\mathfrak{g}))}), \quad \forall \mathfrak{Q} \mid \mathfrak{p}, \quad \mathfrak{Q} \neq \mathfrak{P}.$$

This concludes the algorithm for the computation of $K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p})$.

4. *The logarithm in the relative group*

From the algorithm described in Section 3 we obtain $K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p})$ as the direct product of $\mathrm{cok}(\mu_\mathfrak{p})$, which is presented as an abstract finite abelian group, and the finitely generated free abelian group $I(C_\mathfrak{p})$. Recall that we identified $I(C_\mathfrak{p})$ and $\prod_i \prod_\mathfrak{P} \pi_{i,\mathfrak{P}}^{\mathbb{Z}}$. Hence our representation of $K_0(\mathcal{A}_\mathfrak{p}, K_\mathfrak{p})$ depends on the choice of uniformizing elements $\pi_{i,\mathfrak{P}}$.

Let $[P, \theta, Q] \in K_0(\mathcal{A}, K)$. In this section we develop an algorithm which computes a representative of $[P_\mathfrak{p}, \theta_\mathfrak{p}, Q_\mathfrak{p}]$ in terms of the explicit presentation produced by the algorithm of Section 3.

Before we sketch the individual steps of the algorithm, we briefly digress to describe the presentation of our data. We always assume that torsion free $\mathcal{O}_K[G]$-modules X are given by a $\mathcal{O}_K$-pseudo-basis as described, for example, in [**11**, Definition 1.4.1]. To be more precise, we assume that $V := K \otimes_{\mathcal{O}_K} X$ is given by an K-basis $v_1, \dots, v_d$ together with matrices $A(\sigma) \in \mathrm{GL}_d(K)$ for each $\sigma \in G$ describing the action of G,

$$(\sigma(v_1), \dots, \sigma(v_d)) = (v_1, \dots, v_d)\, A(\sigma).$$

Then $X = \mathfrak{a}_1 x_1 \oplus \dots \oplus \mathfrak{a}_d x_d$, where each $\mathfrak{a}_i$ is a fractional ideal of $\mathcal{O}_K$ and each $x_i \in V$.

If $[P, \theta, Q] \in K_0(\mathcal{A}, K)$, then we assume that $V := K \otimes_{\mathcal{O}_K} P$, resp. $W := K \otimes_{\mathcal{O}_K} Q$ is given by a K-basis $v_1, \dots, v_d$, resp. $w_1, \dots, w_d$, and with respect to these bases θ is represented by a matrix $A(\theta) \in \mathrm{GL}_d(K)$,

$$(\theta(v_1), \dots, \theta(v_d)) = (v_1, \dots, v_d)\, A(\theta).$$

4.1. *Outline of the algorithm*

We first note that by a fundamental result of Swan (see [**8**, Th. (32.11)]) every finitely generated projective $\mathcal{A}$-module P is locally free. The algorithm in Section 4.2 produces such a local basis which is contained in P.

The algorithm for the logarithm problem essentially consists of the following four steps.

Step 1 Compute $\mathcal{A}_\mathfrak{p}$-bases $\nu_1, \dots, \nu_m \in P$ and $\omega_1, \dots, \omega_m \in Q$ of $P_\mathfrak{p}$ and $Q_\mathfrak{p}$.

Step 2 Compute the matrix $S \in \mathrm{Gl}_m(A) \subseteq \mathrm{Gl}_m(A_\mathfrak{p})$ such that

$$(\theta(\nu_1), \dots, \theta(\nu_m)) = (\omega_1, \dots, \omega_m) S.$$

Step 3 Compute the reduced norm $\mathrm{nr}(S) = (\lambda_1, \dots, \lambda_r) \in Z(A) \subseteq Z(A_\mathfrak{p})$.

Step 4 Calculate $\bar{\varphi}(\mathrm{nr}(S) \bmod \mathrm{nr}(\mathcal{A}_\mathfrak{p}^\times)) \in I(C_\mathfrak{p}) \times \mathrm{cok}(\mu_\mathfrak{p})$, with $\bar{\varphi}$ as in Proposition 2.7.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

We briefly explain Steps 2 to 4. Step 2 is basically linear algebra and needs no further explanations. For Step 3 we can apply one of the two algorithms of Subsection 3.3 and Step 4 is completely explained by Proposition 2.7.

In the next subsection we focus on Step 1, the computation of the local bases.

4.2. *Computation of a local basis*

Let P be a locally free $\mathcal{A}$-module and $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_K$. Let $F = \mathcal{O}_K/\mathfrak{p}$ denote the residue class field. Then $B := \mathcal{A}/\mathfrak{p}\mathcal{A}$ is a finitely generated F-algebra and $P/\mathfrak{p}P$ is a free B-module. Let $J = J(B)$ denote the Jacobson radical of B. We set $\bar{B} := B/J$ and $\bar{P} := (P/\mathfrak{p}P)/J(P/\mathfrak{p}P)$. If $\bar{\omega}_1, \ldots, \bar{\omega}_m \in \bar{P}$ is a $\bar{B}$-basis of $\bar{P}$, then Nakajama's lemma (applied twice) implies that any lift $\omega_1, \ldots, \omega_m \in P$ of $\bar{\omega}_1, \ldots, \bar{\omega}_m$ is an $\mathcal{A}_\mathfrak{p}$-basis of $P_\mathfrak{p}$.

Algorithms for the computation of Jacobson radicals of associative algebras over finite fields are, for example, discussed in [**12**, Sec. 2.3] or [**13**].

The algebra $\bar{B}$ is semisimple and thus isomorphic to a direct product of matrix rings $M_s(E)$, where E is a finite field extension of F. The field E and the matrix rings $M_s(E)$ can be computed by combining the algorithms in [**12**, Sec. 2.4 and 2.5]. The $\bar{B}$-module $\bar{P}$ decomposes according to the decomposition of $\bar{B}$. We are therefore left with the following problem: Given a matrix algebra $M = \mathrm{Mat}_s(E)$ over a (finite) field E and a free M-module X, compute an M-basis of X.

We let e_{kl} denote the matrix $(\alpha_{ij}) \in M$ with $\alpha_{ij} = 0$ for $(i,j) \neq (k,l)$ and $\alpha_{kl} = 1$. Using basic linear algebra we compute an E-basis $\nu_1, \ldots, \nu_{ms}$ of $e_{11}X$, where here m is the M-rank of X. We set

$$w_k = e_{11}\nu_{(k-1)s+1} + \ldots + e_{s1}\nu_{ks}, \quad k = 1, \ldots, m.$$

LEMMA 4.1. *The elements $w_1, \ldots, w_m$ form an M-basis of X.*

Proof. Clearly $Mw_1 + \ldots + Mw_m \subseteq X$. For the inverse inclusion we note that $X = e_{11}X \oplus \ldots \oplus e_{ss}X$. Since $e_{ii}X = e_{i1}e_{11}e_{1i}X \subseteq e_{i1}e_{11}X$ it suffices to prove $e_{11}X \subseteq Mw_1 + \ldots + Mw_m$. This is immediate from $e_{1j}w_k = e_{11}\nu_{(k-1)s+j} = \nu_{(k-1)s+j}$. □

5. *The logarithm in the class group*

We first briefly recall the main results of [**2**]. The sequence [**2**, 1.7a] gives an explicit description of $\mathrm{cl}(\mathcal{A})$ as a quotient of a certain ray class group and in [**2**, Section 3] this is used to construct an algorithm to compute $\mathrm{cl}(\mathcal{A})$ as an abstract abelian group. In this section we describe an approach how to solve the logarithm problem in $\mathrm{cl}(\mathcal{A})$ algorithmically. For a locally free $\mathcal{A}$-module P we develop an algorithm which computes a representative of $[P] - \mathrm{rk}(P)[\mathcal{A}] \in \mathrm{cl}(\mathcal{A})$ in terms of the explicit presentation produced by the algorithm of [**2**].

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 $i \in \{1, \ldots, r\}$ 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

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

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

Note that $P_{\mathfrak{g}}^+$ is a subgroup of $I_{\mathfrak{g}}$. The main result of [**2**] shows that

$$\mathrm{cl}(\mathcal{A}) \simeq \mathrm{cok}\left(K_1(\mathcal{A}/\mathfrak{f}) \xrightarrow{\nu} I_{\mathfrak{g}}/P_{\mathfrak{g}}^+\right), \tag{19}$$

where ν is induced by the reduced norm.

Let P be a finitely generated locally free $\mathcal{A}$-module of rank d. We want to compute $(P) = [P] - d[\mathcal{A}] \in \mathrm{cl}(\mathcal{A})$ as an element of the right hand side in (19). We assume that we can compute an A-basis of $P \otimes_R K$, which in many applications is easy (compared to the problem of computing integral basis). Equivalently, we may assume that $P \subseteq A^d$.

Since we already know how to solve the discrete logarithm problem in the relative groups $K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}})$, the strategy is clear: we consider the element $\omega = [P, \mathrm{id}, \mathcal{A}^d] \in K_0(\mathcal{A}, K)$. Then $\partial^0(\omega) = (P)$ and it suffices for us to solve the discrete logarithm problems for $\omega_{\mathfrak{p}} = [P_{\mathfrak{p}}, \mathrm{id}, \mathcal{A}_{\mathfrak{p}}^d]$ in $K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}})$ for each $\mathfrak{p}$. In fact, we only need to consider the finite set of prime ideals $\mathfrak{p}$ such that $v_{\mathfrak{p}}([\mathcal{A}^d : P]_{\mathcal{O}_K}) \neq 0$, since $\omega_{\mathfrak{p}} = 0$ for any other prime ideal. It remains to provide, for a prime ideal $\mathfrak{p}$, an explicit description of the map

$$\partial_{\mathfrak{p}}^0 : I(C_{\mathfrak{p}}) \times \mathrm{cok}(\mu_{\mathfrak{p}}) \longrightarrow \mathrm{cok}\left(K_1(\mathcal{A}/\mathfrak{f}) \xrightarrow{\nu} I_{\mathfrak{g}}(C)/P_{\mathfrak{g}}^+\right),$$

which is induced by the composite map $K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}}) \subseteq K_0(\mathcal{A}, K) \xrightarrow{\partial^0} \mathrm{cl}(\mathcal{A})$. The map ∂^0 is just the (finite) sum over the $\partial_{\mathfrak{p}}^0$.

Let $\omega_{\mathfrak{p}} \in K_0(\mathcal{A}_{\mathfrak{p}}, K_{\mathfrak{p}})$ be represented by $(\mathfrak{a}, \bar{\xi}) \in I(C_{\mathfrak{p}}) \times \mathrm{cok}(\mu_{\mathfrak{p}})$. Recall that this representation depends on the choice of uniformizing elements $\pi_{i,\mathfrak{P}}$ for the primes $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ lying above $\mathfrak{p}$. The conventions fixed in Proposition 2.7 are crucial for the validity of the following algorithm.

Let

$$\mathfrak{a} = \prod_{i,\mathfrak{P}} \mathfrak{P}^{e_{i,\mathfrak{P}}}, \quad \xi = (\xi_1, \ldots, \xi_r),$$

with elements $\xi_i \in \left(\mathcal{O}_{K_{i,\mathfrak{p}}}/\mathfrak{g}_{i,\mathfrak{p}}\right)^\times$, $i = 1, \ldots, r$. We choose lifts $\eta_i \in \mathcal{O}_{K_i}$ of the elements ξ_i and consider

$$\gamma_i := \eta_i \prod_{\mathfrak{P}} \pi_{i,\mathfrak{P}}^{e_{i,\mathfrak{P}}},$$

where the product extends over all primes $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ above $\mathfrak{p}$. Let now $\alpha_i = (\alpha_{i,\mathfrak{q}})_{\mathfrak{q}} \in J(K_i)$ denote the idèle with $\alpha_{i,\mathfrak{q}} = \gamma_i$ if $\mathfrak{q} = \mathfrak{p}$, and $\alpha_{i,\mathfrak{q}} = 1$ if $\mathfrak{q} \neq \mathfrak{p}$. It follows from the proof of [**2**, Th. 1.5] that the image of α_i in $I_{\mathfrak{g}_i}(K_i)/P_{\mathfrak{g}_i}^+$ can be computed by the following recipe:

Step 1 Compute $\beta \in K_i^{\times +}$ such that

$$v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}\beta - 1) \geqslant v_{\mathfrak{P}}(\mathfrak{g}_i) \text{ for all } \mathfrak{P} \text{ with } \mathfrak{P} \mid \mathfrak{g}_i.$$

Step 1 Compute the ideal $\mathfrak{b}_i = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}\beta_i)}$.

Then $\partial_{\mathfrak{p}}^0(\omega_{\mathfrak{p}}) = \left(\mathfrak{b}_i P_{\mathfrak{g}_i}^+\right)_i \in \oplus_i I_{\mathfrak{g}_i}(K_i)/P_{\mathfrak{g}_i}^+(K_i) \simeq I_{\mathfrak{g}}(C)/P_{\mathfrak{g}}^+(C)$, which can be computed by applying [**11**, Alg. 4.3.2] componentwise. Step 1 can be performed by combining the Chinese Remainder Theorem with [**11**, Alg. 4.2.20].

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

6. *Induction, restriction and quotient map*

For the moment we let R be an integral domain with quotient field K. Let E/K be a field extension and S a subgroup of the finite group G.

We recall that we have canonical homomorphisms

$$\begin{aligned}\mathrm{res}^G_S &: K_0(R[G], E) \longrightarrow K_0(R[S], E),\\ \mathrm{ind}^G_S &: K_0(R[S], E) \longrightarrow K_0(R[G], E).\end{aligned}$$

If S is a normal subgroup we put $\Sigma := G/S$. In this case we also have

$$\mathrm{quot}^G_\Sigma : K_0(R[G], E) \longrightarrow K_0(R[\Sigma], E).$$

We resume the notation of the previous sections, so K denotes a number field as before. The aim of this section is to compute res, ind and quot in terms of given explicit descriptions of the relative groups as products as in Proposition 2.7. For a fixed subgroup S we let $C', \mathfrak{f}', \mathfrak{g}'$ etc. denote the data with respect to the order $\mathcal{O}_K[S]$. We write $\mathrm{Irr}(S)$ for the set of absolutely irreducible characters of S. We fix a Galois extension E of K which is a splitting field for both S and G. Then $\mathrm{Gal}(E/K)$ acts on $\mathrm{Irr}(S)$ and we write $\mathrm{Irr}_K(S)$ for a fixed set of orbit representatives. For $\chi \in \mathrm{Irr}(S)$ we let K_χ denote the field generated over K by the values of χ. With these notations one has

$$\begin{array}{ccc} K_1(K[S]) & \xrightarrow{\subseteq} & K_1(E[S]) \\ \Big\downarrow{\scriptstyle \mathrm{nr}} & & \Big\downarrow{\scriptstyle \mathrm{nr}} \\ \displaystyle\prod_{\chi\in\mathrm{Irr}_K(S)} K_\chi & \longrightarrow & \displaystyle\prod_{\chi\in\mathrm{Irr}_K(S)} \prod_{\tau} E = \prod_{\chi\in\mathrm{Irr}(S)} E, \end{array}$$

where the product over τ extends over all embedings $\tau : K_\chi \hookrightarrow E$, respectively, and the bottom map is given by

$$(\alpha_\chi)_{\chi\in\mathrm{Irr}_K(S)} \mapsto (\tau(\alpha_\chi))_{\chi,\tau}\,. \tag{20}$$

If G denotes a finite group and ψ and χ are two (virtual) characters of G, then $\langle\psi,\chi\rangle_G$ denotes the standard scalar product. For a subgroup S of G and a character ψ of S we write $\mathrm{ind}^G_S(\psi)$ for the induced character. If χ is a character of G, then $\mathrm{res}^G_S(\chi)$ denotes the restriction of χ. Finally, if S is normal and $\Sigma := G/S$, then inf^G_Σ is the inflated character.

6.1. *Restriction*

We recall that $\mathrm{res}^G_S : K_1(E[G]) \longrightarrow K_1(E[S])$ induces the map

$$\begin{aligned}\mathrm{res}^G_S : \prod_{\chi\in\mathrm{Irr}(G)} E &\longrightarrow \prod_{\psi\in\mathrm{Irr}(S)} E,\\ (\alpha_\chi)_{\chi\in\mathrm{Irr}(G)} &\mapsto \left(\prod_{\chi\in\mathrm{Irr}(G)} \alpha_\chi^{\langle\chi,\mathrm{ind}^G_S(\psi)\rangle_G}\right)_{\psi\in\mathrm{Irr}(S)}.\end{aligned} \tag{21}$$

Let now $\omega \in K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p})$ be an element which is represented by $(\mathfrak{a}, \bar{\xi}) \in I(C_\mathfrak{p}) \times \mathrm{cok}(\mu_\mathfrak{p})$, as in Proposition 2.7. Recall that this representation depends on

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

the choice of uniformizing elements $\pi_{i,\mathfrak{P}}$ for the primes $\mathfrak{P}$ of $\mathcal{O}_{K_i}$ lying above $\mathfrak{p}$. We want to construct $\mathrm{res}_S^G(\omega)$ as an element of

$$I(C'_{\mathfrak{p}}) \times \mathrm{cok}\left(\mu'_{\mathfrak{p}} : K_1(\mathcal{O}_{K_{\mathfrak{p}}}[S]/\mathfrak{f}'_{\mathfrak{p}}) \longrightarrow \left(\mathcal{O}_{C',\mathfrak{p}}/\mathfrak{g}'_{\mathfrak{p}}\right)^{\times}\right),$$

where C', $\mu'_{\mathfrak{p}}$, $\mathfrak{f}'$ and $\mathfrak{g}'$ are chosen or defined with respect to $\mathcal{O}_K[S]$ as C, $\mu_{\mathfrak{p}}$, $\mathfrak{f}$ and $\mathfrak{g}$ have been for $\mathcal{A} = \mathcal{O}_K[G]$. Let

$$\mathfrak{a} = \prod_{i,\mathfrak{P}} \mathfrak{P}^{e_{i,\mathfrak{P}}}, \quad \xi = (\xi_1, \ldots, \xi_r),$$

with elements $\xi_i \in \left(\mathcal{O}_{K_i,\mathfrak{p}}/\mathfrak{g}_{i,\mathfrak{p}}\right)^{\times}$, $i = 1, \ldots, r$. From the explicit description of the map φ in Proposition 2.7 we derive the following recipe. We choose lifts $\eta_i \in \mathcal{O}_{K_i}$ which are coprime to $\mathfrak{P}$ for all $\mathfrak{P} \mid \mathfrak{p}$ and consider the elements

$$\beta_i := \eta_i \alpha_i, \text{ where } \alpha_i = \prod_{\mathfrak{P}\mid\mathfrak{p} \text{ in } K_i/K} \pi_{i,\mathfrak{P}}^{e_{i,\mathfrak{P}}}.$$

We now map $(\beta_1, \ldots, \beta_r)$ to $\prod_{\chi\in\mathrm{Irr}(G)} E$ using (20) and call the image $(\alpha_\chi)_{\chi\in\mathrm{Irr}(G)}$. Applying the map res_S^G as in (21) we obtain an element $(\gamma_\psi)_{\psi\in\mathrm{Irr}(S)}$. By general theory $(\gamma_\psi)_{\psi\in\mathrm{Irr}(S)}$ is an element $(\gamma_1, \ldots, \gamma_{r'})$ of the subgroup $\prod_{\psi\in\mathrm{Irr}_K(S)} K_\psi$.

Again by the recipe of Proposition 2.7 we now interpret $(\gamma_1, \ldots, \gamma_{r'})$ as an element of $I_{\mathfrak{p}}(C') \times \mathrm{cok}(\mu'_{\mathfrak{p}})$.

6.2. *Induction*

We recall that $\mathrm{ind}_S^G : K_1(E[S]) \longrightarrow K_1(E[G])$ induces the map

$$\mathrm{ind}_S^G : \prod_{\psi\in\mathrm{Irr}(S)} E \longrightarrow \prod_{\chi\in\mathrm{Irr}(G)} E, \tag{22}$$

$$(\alpha_\psi)_{\psi\in\mathrm{Irr}(S)} \mapsto \left(\prod_{\psi\in\mathrm{Irr}(S)} \alpha_\psi^{\langle \mathrm{res}_S^G \chi, \psi\rangle_S}\right)_{\chi\in\mathrm{Irr}(G)}. \tag{23}$$

The computation of the induction map is now completely analogous to the computation of the restriction map.

6.3. *Quotient*

In this subsection the subgroup S is assumed to be normal and we let $C', \mathfrak{f}', \mathfrak{g}'$, etc., denote the data with respect to the order $\mathcal{O}_K[\Sigma]$.

The map $\mathrm{quot}_\Sigma^G : K_1(E[G]) \longrightarrow K_1(E[\Sigma])$ induces the map

$$\mathrm{quot}_S^G : \prod_{\chi\in\mathrm{Irr}(G)} E \longrightarrow \prod_{\psi\in\mathrm{Irr}(\Sigma)} E, \tag{24}$$

$$(\alpha_\chi)_{\chi\in\mathrm{Irr}(G)} \mapsto \left(\alpha_{\mathrm{inf}_\Sigma^G \psi}\right)_{\psi\in\mathrm{Irr}(\Sigma)}. \tag{25}$$

Again, given this explicit description, the computation of the quotient map is completely analogous to the computation of the restriction map.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

7. *Computational results*

In this section we briefly recount some of the machine computations which we performed in order to check the correctness of our implementation. The interested reader is referred to

http://www.mathematik.uni-kassel.de/~bley/pub.html,

where he can find a batch file which shows how to reproduce these computations.

Our implementation performs well as long as the the groups are of moderate size, say $|G| < 200$. For example, the computation of $K_0(\mathbb{Z}_2[S_5], \mathbb{Q}_2)$ takes about 5 minutes on a 2.2 GHz Dual Core AMD Opteron Processor 275, the computation of $K_0(\mathbb{Z}_3[A_6], \mathbb{Q}_3)$ took about 1 hour. In addition, for computations in the locally free class group one also has to make sure that the character fields $K_i, i = 1, \ldots, r$, are small, say $[K_i : \mathbb{Q}] < 20$. This is explained by the fact, that the algorithm for computing the locally free class group requires the computation of certain ray class groups which is computationally a very hard problem.

For cyclic groups $G = C_p$ of prime order p, one has that $DT(\mathbb{Z}_p[G])$ (i.e. $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{\mathrm{tors}}$) is cyclic of order $p - 1$. We checked this for $p < 100$.

Let D_n denote the dihedral group of order $2n$. For odd n it is known that $DT(\mathbb{Z}_2[D_n])$ is trivial. This was confirmed by our implementation for $n < 100$. For primes p one has $DT(\mathbb{Z}_p[D_p]) \simeq C_{p-1}$, which we also checked for $p < 100$.

We computed $DT(\mathbb{Z}_p[Q_{4n}])$ for $n \leqslant 25$ and p dividing $4n$, where Q_{4n} denotes the generalized quaternion group of order $4n$. In all cases where we have theoretical results by Theorem 1.1 our machine computations gave the correct result.

For $G = A_4$, the alternating group, we computed

$$DT(\mathbb{Z}_2[A_4]) \simeq C_2, \quad DT(\mathbb{Z}_3[A_4]) \simeq C_2,$$

obtaining the correct results (see Theorem 1.2).

We used the results of Breuning [**5**, Lemma 6.7 and Theorem 6.8] to test our implementations of induction and restriction.

In order to verify the correctness of the implementation of the discrete logarithm algorithm in both the relative group and the locally free class group we computed the discrete logarithm of certain Swan modules. Concretely, we computed the Swan subgroup of the locally free classgroup in the situations of [**8**, Theorems (53.13), (53.14), (53.16), (53.19)] for a list of small groups, each time obtaining the correct result.

8. *Some theoretical computations*

In this section, to keep the number of brackets to a minimum we write RG, rather than $R[G]$ for a group ring.

If $\mathcal{A}$ is an order in a semi-simple p-adic algebra A, we will take the isomorphism $\overline{\mathrm{n}}_{\mathcal{A}}$ of Theorem 2.4(i) as an identification so that

$$DT(\mathcal{A}) := \mathcal{O}_C^{\times}/\mathrm{nr}_A(\mathcal{A}^{\times}).$$

We denote by $\pi_{\mathcal{A}}$ the canonical epimorphism from $\mathcal{O}_C^{\times}$ to $DT(\mathcal{A})$. As usual we write $SK_1(\mathcal{A})$ for the kernel of the reduced norm $\mathrm{nr}_A : K_1(\mathcal{A}) \longrightarrow C^{\times}$.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

THEOREM 8.1. *Let p be a prime and let*

$$\begin{array}{ccc} \mathcal{B} & \xrightarrow{\pi_1} & \mathcal{A}_1 \\ \downarrow \pi_2 & & \downarrow \rho_1 \\ \mathcal{A}_2 & \xrightarrow{\rho_2} & T \end{array} \tag{26}$$

be a cartesian square of rings (with at least one of ρ_1 and ρ_2 surjective) where $\mathcal{B}$, $\mathcal{A}_1$ and $\mathcal{A}_2$ are $\mathbb{Z}_p$-orders in semisimple $\mathbb{Q}_p$-algebras B, A_1 and A_2, respectively, and T is finite.

(i) Then we have an exact sequence

$$SK_1(\mathcal{B}) \xrightarrow{\pi_*} SK_1(\mathcal{A}_1) \oplus SK_1(\mathcal{A}_2) \xrightarrow{\rho_*} K_1(T) \xrightarrow{\partial} DT(\mathcal{B}) \to DT(\mathcal{A}_1) \oplus DT(\mathcal{A}_2) \to 0,$$

where $\pi_*(x) = (k_1(\pi_1)(x), k_1(\pi_2)(x))$ and $\rho_*(x,y) = (k_1(\rho_1)(x)/k_1(\rho_2)(y))$.

Assume that $B = A_1 \oplus A_2$ (with π_1 and π_2 the projections so that $\mathcal{B} \subseteq \mathcal{A}_1 \oplus \mathcal{A}_2$) and, for $i = 1, 2$, let $\sigma_i : (\mathcal{O}_{Z(A_i)})^\times \to (\mathcal{O}_{Z(B)})^\times$ be given by $\sigma_1(x) = (x, 1)$, $\sigma_2(x) = (1, 1/x)$. Then

(ii) $\partial \circ k_1(\rho_i) = \pi_{\mathcal{B}} \circ \sigma_i \circ \mathrm{nr}_{A_i} : K_1(\mathcal{A}_i) \to DT(\mathcal{B})$.

Proof. (i) We have a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & SK_1(\mathcal{B}) & \to & SK_1(\mathcal{A}_1) \oplus SK_1(\mathcal{A}_2) & \to & K_1(T) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & K_1(\mathcal{B}) & \xrightarrow{\pi_*} & K_1(\mathcal{A}_1) \oplus K_1(\mathcal{A}_2) & \xrightarrow{\rho_*} & K_1(T) & \to & 0 \\ & & \downarrow \mathrm{nr}_B & & \mathrm{nr}_{A_1} \downarrow \mathrm{nr}_{A_2} & & \downarrow & & \\ 0 \to & \mathcal{O}^\times_{Z(B)} & = & \mathcal{O}^\times_{Z(A_1)} \times \mathcal{O}^\times_{Z(A_2)} & \to & 0 & & & \\ & & \downarrow \pi_{\mathcal{B}} & & \pi_{\mathcal{A}_1} \downarrow \pi_{\mathcal{A}_2} & & & & \\ & & DT(\mathcal{B}) & \to & DT(\mathcal{A}_1) \oplus DT(\mathcal{A}_2) & \to & 0 & & \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

where the second row is the Mayer–Vietoris sequence for the square, c.f. [**1**, VII 4.3]. It is truncated at $K_1(T)$ since the succeeding groups are torsion free by [**1**, IX 1.4]. This gives us our result since (by, for instance, the snake lemma) the cokernel at the top right is isomorphic to the kernel at the bottom left.

(ii) This is clear from the above diagram and follows from the explicit construction of the connecting homomorphism ∂. □

We note the immediate corollary:

COROLLARY 8.2. *Let p be a prime and Δ be a finite abelian group of order prime to p. Then $DT(\mathbb{Z}_p\Delta C_p) \cong (\mathbb{F}_p\Delta)^\times$.*

Proof. Consider the cartesian square:

$$\begin{array}{ccc} \mathbb{Z}_p\Delta C_p & \xrightarrow{\pi_1} & \mathbb{Z}_p[\zeta]\Delta \\ \downarrow \pi_2 & & \downarrow \rho_1 \\ \mathbb{Z}_p\Delta & \xrightarrow{\rho_2} & \mathbb{F}_p\Delta \end{array} \tag{27}$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

where ζ is a pth root of 1, π_1 is induced by an isomorphism $C_p \cong \langle\zeta\rangle$ and π_2 by the trivial character on C_p.

Since $\mathbb{Z}_p[\zeta]\Delta$ and $\mathbb{Z}_p\Delta$ are commutative and semilocal, their SK_1's vanish by [**1**, IX 1.4]. Their DT's vanish (Theorem 2.4 (ii)) because these orders are maximal. Finally $K_1(\mathbb{F}_p\Delta) = \mathbb{F}_p\Delta^\times$ again by [**1**, IX 1.4], so that the result follows by Theorem 8.1. □

It can be quite difficult to determine the structure of $DT(\mathcal{B})$ from the sequence of Theorem 8.1(i) when both the image and the cokernel of ∂ are non-trivial. An easy case is the following.

LEMMA 8.3. *With the data and notation of Theorem 8.1, suppose that $DT(\mathcal{A}_1) = \{1\}$ and that the canonical epimorphism $\pi_{\mathcal{A}_2} : \mathcal{O}^\times_{Z(A_2)} \twoheadrightarrow DT(\mathcal{A}_2)$ is split. Then the ring extension map $\eta : DT(\mathcal{B}) \twoheadrightarrow DT(\mathcal{A}_2)$ is split and therefore $DT(\mathcal{B}) \cong \partial(K_1(T)) \times DT(\mathcal{A}_2)$.*

Proof. We have a commutative diagram with exact second row

$$\begin{array}{ccccc} & & \mathcal{O}^\times_{Z(A_1)} \times \mathcal{O}^\times_{Z(A_2)} & \overset{\tau}{\twoheadrightarrow} & \mathcal{O}^\times_{Z(A_2)} \\ & & \downarrow \pi_{\mathcal{B}} & & \downarrow \pi_{\mathcal{A}_2} \\ \partial(K_1(T)) & \to & DT(\mathcal{B}) & \overset{\eta}{\twoheadrightarrow} & DT(\mathcal{A}_2) \end{array}$$

where τ is the natural projection. Since τ and $\pi_{\mathcal{A}_2}$ are split $\pi_{\mathcal{A}_2}\tau$ is split and hence so is η. □

We continue our analysis of Theorem 8.1 a little further to expose an easy case where the canonical epimorphism $\pi_{\mathcal{B}} : (\mathcal{O}_{Z(B)})^\times \twoheadrightarrow DT(\mathcal{B})$ splits. Consider the map $\partial \circ k_1(\rho_i) : K_1(\mathcal{A}_i) \to DT(\mathcal{B})$, for $i = 1$ or 2. Since its kernel contains $SK_1(\mathcal{A}_i)$, it factors through $K_1(\mathcal{A}_i) \overset{\mathrm{nr}}{\to} \mathrm{nr}(\mathcal{A}_1^\times)$,

$$\begin{array}{ccc} K_1(\mathcal{A}_i) & \xrightarrow{\partial \circ k_1(\rho_i)} & DT(\mathcal{B}) \\ {\scriptstyle \mathrm{nr}}\downarrow & \nearrow_{\hat{\rho}_i} & \\ \mathrm{nr}(\mathcal{A}_i^\times) & & \end{array}$$

where we have put $\hat{\rho}_i$ for the induced map.

LEMMA 8.4. *If $\hat{\rho}_i$ is split surjective then $\pi_{\mathcal{B}} : \mathcal{O}^\times_{Z(B)} \to DT(\mathcal{B})$ splits.*

Proof. (We may assume $i = 1$.) Suppose that $\gamma : DT(\mathcal{B}) \to \mathrm{nr}(\mathcal{A}_1^\times)$ splits $\hat{\rho}_1$. Choose $x \in DT(\mathcal{B})$ and $y \in K_1(\mathcal{A}_1)$ such that $\mathrm{nr}_{A_1}(y) = \gamma(x)$. Then

$$\pi_{\mathcal{B}}(\sigma_1(\gamma(x))) = \pi_{\mathcal{B}}(\sigma_1(\mathrm{nr}_{A_1}(y))) = \partial(k_1(\rho_1)(y)) = \hat{\rho}_1(\mathrm{nr}(y)) = \hat{\rho}_1(\gamma(x)) = x.$$

So $\sigma_1 \circ \gamma$ splits $\pi_{\mathcal{B}}$. □

Of course, if $\hat{\rho}_i$ is surjective then $DT(\mathcal{A}_1) = \{1\} = DT(\mathcal{A}_2)$.

The following lemma is useful in applying Theorem 8.1 when the SK_1's do not vanish. What we would like is some easy-to-handle homomorphism $\nu : K_1(T) \to U$ whose kernel is the image of the SK_1's...

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

LEMMA 8.5. *Let $\mathcal{A}$ be an order in a semisimple $\mathbb{Q}_p$-algebra A and let $\rho : \mathcal{A} \to T$ be a ring epimorphism where T is finite. Suppose that we have a group U and homomorphisms ν and ρ' making a commutative square:*

$$\begin{array}{ccc} K_1(\mathcal{A}) & \xrightarrow{\mathrm{nr}_A} & \mathrm{nr}_A(\mathcal{A}^\times) \\ \downarrow k_1(\rho) & & \downarrow \rho' \\ K_1(T) & \xrightarrow{\nu} & U \end{array}$$

(i) We have an exact sequence

$$0 \to \frac{\ker(\rho')}{\mathrm{nr}(\ker(k_1(\rho)))} \longrightarrow \frac{K_1(T)}{k_1(\rho)(SK_1(\mathcal{A}))} \xrightarrow{(\nu)} \rho'(\mathrm{nr}_A(\mathcal{A}^\times)) \to 0$$

where the first map is induced by $k_1(\rho) \circ \mathrm{nr}_A^{-1}$ and the second by ν.

(ii) So if $\ker(\rho') = \mathrm{nr}(\ker(k_1(\rho)))$ we have an exact sequence

$$SK_1(\mathcal{A}) \xrightarrow{k_1(\rho)} K_1(T) \xrightarrow{\nu} \rho'(\mathrm{nr}_A(\mathcal{A}^\times)) \to 0. \tag{28}$$

(iii) In particular, this will hold if T is semisimple and the kernel of ρ' is a pro-p-group.

Proof. (i) and (ii). We may complete the square to a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 \to & SK_1(\mathcal{A}) & \hookrightarrow & K_1(\mathcal{A}) & \xrightarrow{\mathrm{nr}_A} & \mathrm{nr}_A(\mathcal{A}^\times) & \to 0 \\ & \downarrow \rho'' & & \downarrow k_1(\rho) & & \downarrow \rho' & \\ 0 \to & \ker(\nu) & \hookrightarrow & K_1(T) & \xrightarrow{\nu} & U & \end{array}$$

$k_1(\rho)$ is surjective since ρ is surjective and $\mathcal{A}$ is semilocal ([1, IX 1.4(1)]). So $\mathrm{img}(\nu) = \rho'(\mathrm{nr}_A(\mathcal{A}^\times))$ and, by the snake lemma, $\mathrm{coker}(\rho'') \cong \ker(\rho')/\mathrm{nr}(\ker(k_1(\rho)))$.

(iii) If T is semisimple, then $Z(T)$ will be a sum of finite fields of characteristic p. Thus $K_1(T) \cong Z(T)^\times$, and hence the middle group in the sequence of (i) will be of order prime to p. So the first group in the sequence, which is a p-group by assumption, must be trivial. □

To help construct and use a suitable homomorphism ν, as above, we develop further machinery based on the relationship between certain determinant maps and the corresponding reduced norms.

DEFINITION 8.6. Let $\mathcal{A}$ be a ring which is finitely generated and projective as a module over a commutative (but not necessarily central) subring R. We denote by $\det_R$ $(= \det_{\mathcal{A},R})$ the composite

$$\det_R : K_1(\mathcal{A}) \longrightarrow K_1(R) \longrightarrow R^\times$$

of restriction and determinant homomorphisms.

LEMMA 8.7. *Suppose that R and $\mathcal{A}$, as in the above definition, are $\mathbb{Z}_p$-orders in semisimple algebras E and A, respectively (with $E \subset A$). Let $x \in K_1(\mathcal{A})$ with image $\bar{x}$ in $K_1(A)$. Then one has*

$$(i)\ \det_R(x) = \det_E(\bar{x}).$$
$$(ii)\ \det_R(x) = 1 \text{ for } x \in SK_1(\mathcal{A}).$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

Proof. (i) is clear since the ring extensions $\otimes_R E$ and $\otimes_{\mathcal{A}} A$ are both given by extension of scalars functor $\otimes_{\mathbb{Z}}\mathbb{Q}$.

(ii) If $x \in SK_1(\mathcal{A})$, then $\mathrm{nr}_A(\bar{x}) = 1$. Since nr_A is injective this implies $\bar{x} = 1$. So $\det_R(x) = \det_E(\bar{x}) = 1$. □

Let Γ be a finite group. We recall that a Γ-*Galois algebra*, L, is a direct sum of fields on which Γ acts by ring automorphisms, so that Γ permutes the field summands of L transitively and the stabilizer of each summand acts faithfully on that summand. The fixed ring L^Γ is then a field (essentially a "diagonal" embedding of the fixed field of a summand) and $\dim_{L^\Gamma}(L) = |\Gamma|$. It is convenient to note that if K is one of the field summands and Δ is its stabilizer then L is isomorphic, as a Γ-ring, to the co-induced ring $\mathrm{Map}_\Delta(\Gamma, K)$ of Δ-equivariant maps (Δ acting on the left) from Γ to K with Γ action defined by $\gamma(f) : \gamma' \mapsto f(\gamma'\gamma)$.

If the group Γ acts on the ring S by ring automorphisms and ψ is a 2-cocycle in $Z^2(\Gamma, S^\times)$ then the *twisted group ring* (also known as a *crossed product algebra*) $S \rtimes_\psi \Gamma$ is the free S-module

$$S \rtimes_\psi \Gamma := \left\{ \sum_{\gamma\in\Gamma} r_\gamma \hat{\gamma} \;\middle|\; r_\gamma \in S \right\},$$

on the symbols $\{\hat{\gamma} : \gamma \in G\}$ with multiplication defined by the rules

$$\hat{\gamma}\hat{\delta} = \psi(\gamma, \delta)\widehat{\gamma\delta}, \quad \hat{\gamma}r = \gamma(r)\hat{\gamma}$$

for $\gamma, \delta \in \Gamma$ and $r \in S$. If the cocycle is trivial then we may omit it from the notation.

If S is co-induced from a subgroup of Γ, as with a Galois algebra, then this construction produces a ring isomorphic to a matrix ring over a twisted group ring formed with the subgroup:

LEMMA 8.8. *Let Γ be a finite group with subgroup Δ, of index n. Suppose that Δ acts on a commutative ring R by ring automorphisms and put S for the co-induced ring* $\mathrm{Map}_\Delta(\Gamma, R)$. *Choose $\psi \in Z^2(\Gamma, S^\times)$. Then*

$$S \rtimes_\psi \Gamma \cong \mathrm{Mat}_n(R \rtimes_{\psi^!} \Delta),$$

where $\psi^! \in Z^2(\Delta, R^\times)$ is defined by $\psi^!(\delta, \delta') = \psi(\delta, \delta')(1_R)$.

Proof. Take a left transversal $T = \{\tau_1, \ldots, \tau_n\}$ of Δ in Γ. Let $e \in S$ be the characteristic function of Δ (so $e(\gamma)$ is 1 if $\gamma \in \Delta$ and is 0 otherwise). Then $e_i := \tau_i(e)$ is the characteristic function of $\Delta\tau_i^{-1}$. Moreover, the e_i are mutually orthogonal idempotents and add up to 1. Thus, putting $\Phi = S \rtimes_\psi \Gamma$, for brevity, we have

$$\Phi = \bigoplus_{i,j} e_i\Phi e_j = \bigoplus_{i,j} \hat{\tau}_i e \hat{\tau}_i^{-1} \Phi \hat{\tau}_j e \hat{\tau}_j^{-1} = \bigoplus_{i,j} \hat{\tau}_i e \Phi e \hat{\tau}_j^{-1} = \bigoplus_{i,j} \hat{\tau}_i \Lambda \hat{\tau}_j^{-1},$$

where $\Lambda = e\Phi e$. Now $\mathrm{Mat}_n(\Lambda) = \oplus_{i,j}\Lambda E_{i\,j}$, where the $E_{i\,j}$ are the (additive) elementary matrices. So we have a group isomorphism $\rho : \mathrm{Mat}_n(\Lambda) \longrightarrow \Phi$ given by $\rho(\lambda E_{i,j}) = \hat{\tau}_i \lambda \hat{\tau}_j^{-1}$. Moreover, for $\lambda, \lambda' \in \Lambda = e\Phi e$,

$$(\hat{\tau}_i \lambda \hat{\tau}_j^{-1})(\hat{\tau}_k \lambda' \hat{\tau}_l^{-1}) = \begin{cases} \hat{\tau}_i \lambda \lambda' \hat{\tau}_l^{-1} & \text{if } j = k \\ \hat{\tau}_i \lambda \hat{\tau}_j^{-1} e_j e_k \hat{\tau}_k \lambda' \hat{\tau}_l^{-1} = 0 & \text{otherwise,} \end{cases}$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

replicating the behaviour of the λE_{ij}. So ρ is a ring isomorphism, also.

Now

$$\Lambda = \bigoplus_i \bigoplus_{\delta\in\Delta} eS\hat{\delta}\hat{\tau}_i^{-1}e = \bigoplus_i \bigoplus_{\delta\in\Delta} S\hat{\delta}ee_i\hat{\tau}_i^{-1} = \bigoplus_{\delta\in\Delta} (Se)\hat{\delta} = (Se) \rtimes_{e\psi} \Delta,$$

since, for $\gamma, \delta \in \Delta$, we have $e\hat{\gamma}\hat{\delta} = e\psi(\gamma,\delta)\widehat{\gamma\delta}$. Moreover, evaluation at 1_Γ gives a Δ-isomorphism from Se to R. So $\Lambda \cong R \rtimes_{\psi^!} \Delta$. □

(Of course, in the situation of the lemma, the map from $H^2(\Gamma, S^\times)$ to $H^2(\Delta, R^\times)$ induced by "!" is an isomorphism, since $S^\times$ is induced from $R^\times$.)

COROLLARY 8.9. *Assume the situation and notation of Lemma 8.8.*

a) $S \rtimes_\psi \Gamma$ is simple, a maximal order or hereditary if and only if $R \rtimes_{\psi^!} \Delta$ is.

b) Suppose that R is a field and that Δ acts faithfully on R. Then $S \rtimes_\psi \Gamma$ is simple.

c) Suppose that R is a Dedekind domain and that Δ acts faithfully on R. Put $R' = R^\Delta$ and suppose that R is an R'-order. Then $S \rtimes_\psi \Gamma$ is a hereditary or a maximal R'-order according as R is tamely ramified or unramified over R'.

Proof. Assertion a) is immediate from Lemma 8.8 because the properties of being simple, maximal or hereditary hold for a ring Λ if and only if they hold for $\mathrm{Mat}_n(\Lambda)$.

b) That $R \rtimes_{\psi^!} \Delta$ is a simple algebra is a standard result (see e.g. [**16**, 29.6] where $R \rtimes_{\psi^!} \Delta$ would be denoted $(R/R^\Delta, \psi^!)$). The simplicity of $S \rtimes_\psi \Gamma$ follows from part a).

In the same way we candeduce part c) from [**8**, (28.5) and (28.7)]. □

LEMMA 8.10. *Suppose that $A = L \rtimes_\psi \Gamma$ is a twisted group ring where L is a finite direct sum of Γ-Galois algebras and ψ is a 2-cocycle of Γ with coefficients in $L^\times$.*

(i) For $x \in K_1(A)$,

$$\mathrm{nr}_A(x) = \det_L(x)$$

(ii) Suppose $\mathcal{A}$ is a subring of A which is projective over $R = \mathcal{A} \cap L$ and such that the product map $L \otimes_R \mathcal{A} \to A$ is bijective. Then, for $x \in K_1(\mathcal{A})$,

$$\mathrm{nr}_A(x) = \det_R(x).$$

(iii) If $\mathfrak{a}$ is an ideal of R such that $\mathfrak{a}\mathcal{A} = \mathcal{A}\mathfrak{a}$ then we have a commutative square

$$\begin{array}{ccc} K_1(\mathcal{A}) & \xrightarrow{\mathrm{nr}_A} & R^\times \\ \downarrow k_1(\rho) & & \downarrow \sigma \\ K_1(\mathcal{A}') & \xrightarrow{\det_{R'}} & (R')^\times \end{array}$$

where $R' = R/\mathfrak{a}$, $\mathcal{A}' = \mathcal{A}/\mathfrak{a}\mathcal{A}$, $\rho : \mathcal{A} \to \mathcal{A}'$ is the reduction map and σ is its restriction.

(iv) If R is a Γ-invariant subring of L such that ψ has coefficients in $R^\times$, $\mathcal{A} = R \rtimes_\psi \Gamma$ and $\mathfrak{a}$ is a Γ-invariant ideal of R, then the conditions of (ii) and (iii) hold.

Proof. (i) We may assume that L is a single Galois algebra, since the general case follows easily. So L is isomorphic as a ring to K^n for some field K and we may assume that $L = \mathrm{Map}_\Delta(\Gamma, K)$ where $\Delta \subseteq \Gamma$ acts on K as a Galois group.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

Suppose first that $\Delta = \{1\}$. With $R = K$ and $S = L$, we adopt the notation of the proof of Lemma 8.8. Then we may identify Λ with K and $A = \Phi \simeq \mathrm{Mat}_n(K)$. Put $e_{ij} = \hat{\tau}_i e \hat{\tau}_j^{-1}$ (so $e_i = e_{ii}$). Then, with $f_j = \sum_i e_{ij}$, we find that A is free on $\mathbf{f} = \{f_1, \ldots, f_n\}$ over $L = \oplus_i K e_i$.

Choose $\mu \in A^\times$ and let $\hat{\mu} \in \mathrm{Aut}_A(A)$ be right multiplication by μ. With ρ as in Lemma 8.8, let $\rho^{-1}(\mu) = M = (m_{ij}) \in \mathrm{Mat}_n(K)$, so that $\mu = \sum_{ij} m_{ij} E_{ij}$. Then $f_k \mu = \sum_j m_{kj} f_j$. Thus the matrix (with respect to $\mathbf{f}$) of $\hat{\mu} \in \mathrm{Aut}_L(A)$ is M and $\det_L(\mu) = \det(M) = \mathrm{nr}(\mu)$.

In the general case put $F = L^\Gamma$, identified naturally with K^Δ. Let N be a field extension of F containing a copy of K. Then $L \otimes_F N \cong (K \otimes_F N)^{|\Gamma/\Delta|} \cong N^{|\Gamma|}$ and $(L \otimes_F N)^\Gamma \cong N$. So $L \otimes_F N$ is a Γ-Galois algebra which is "completely split" as above and we can apply the above work to $A \otimes_F N = (L \otimes_F N) \rtimes_\psi \Gamma$. Thus, with $\hat{\mu} \in \mathrm{Aut}_A(A)$, as above,

$$\det_L(\hat{\mu}) \otimes 1 = \det_{L \otimes N}(\hat{\mu} \otimes 1) = \mathrm{nr}_{A \otimes N}(\mu \otimes 1) = \mathrm{nr}_A(\mu) \otimes 1$$

Thus $\det_L(\mu) = \mathrm{nr}(\mu)$, as required.

Parts (ii), (iii) and (iv) are immediate. □

COROLLARY 8.11. *Suppose that we have L, A, R, $\mathcal{A}$, $\mathfrak{a}$, R' and $\mathcal{A}'$ as in Lemma 8.10(i)-(iii) and such that L is finite dimensional over $\mathbb{Q}_p$ and $\mathcal{A}'$ is finite.*

(i) Then we have an exact sequence

$$0 \to \frac{\ker(\rho) \cap \mathrm{nr}(\mathcal{A}^\times)}{\mathrm{nr}(\ker(k_1(\rho)))} \longrightarrow \frac{K_1(\mathcal{A}')}{k_1(\rho)(SK_1(\mathcal{A}))} \xrightarrow{(\det_{R'})} \rho(\mathrm{nr}(\mathcal{A}^\times)) \to 0,$$

where $(\det_{R'})$ is induced by $\det_{R'}$

(ii) Suppose, further, that we have a cartesian square as in Theorem 8.1 such that $\rho_1 : \mathcal{A}_1 \to T$ is $\rho : \mathcal{A} \to \mathcal{A}'$ as above and that

(a) $\ker(\rho) \cap \mathrm{nr}(\mathcal{A}^\times) = \mathrm{nr}(\ker(k_1(\rho)))$ and
(b) $\mathcal{A}_2$ is projective over a commutative subring R_2 such that $\rho_2(R_2) \subseteq R'$ and $\mathcal{A}' \cong R' \otimes_{R_2} \mathcal{A}_2$.

Then we have an exact sequence

$$0 \to \rho(\mathrm{nr}(\mathcal{A}^\times)) \xrightarrow{\overline{\partial}_\rho} DT(\mathcal{B}) \to DT(\mathcal{A}) \oplus DT(\mathcal{A}_2) \to 0,$$

where, for $x \in \mathrm{nr}(\mathcal{A}^\times)$, $\overline{\partial}_\rho(\rho(x)) = (x, 1)\mathrm{nr}(\mathcal{B}^\times)$.

Proof. (i) In Lemma 8.5, take $\rho : \mathcal{A} \to T$ to be $\rho : \mathcal{A} \to \mathcal{A}'$, $\nu = \det_{R'}$ and $\rho' : \mathrm{nr}(\mathcal{A}^\times) \to (R')^\times$ to be the restriction of σ (and hence of ρ). Then $\ker(\rho') = \ker(\rho) \cap \mathrm{nr}(\mathcal{A}^\times)$ and the result follows.

(ii) From $\mathcal{A}' \cong R' \otimes_{R_2} \mathcal{A}_2$ we deduce

$$\rho_2(\det_{R_2}(x)) = \det_{R'}(k_1(\rho_2)(x))$$

for all $x \in K_1(\mathcal{A}_2)$. Hence $k_1(\rho_2)(\ker(\det_{R_2})) \subseteq \ker(\det_{R'})$. In addition, by Lemma 8.7 we have

$$k_1(\rho_2)(SK_1(\mathcal{A}_2)) \subseteq k_1(\rho_2)(\ker(\det_{R_2})).$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

We consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & SK_1(\mathcal{A}) & \longrightarrow & K_1(\mathcal{A}) & \xrightarrow{\mathrm{nr}_A} & \mathrm{nr}_A(\mathcal{A}^\times) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle k_1(\rho)} & & \downarrow{\scriptstyle \rho'} & & \\ 0 & \longrightarrow & \ker(\det_{R'}) & \longrightarrow & K_1(\mathcal{A}') & \xrightarrow{\det_{R'}} & (R')^\times & & \end{array} \tag{29}$$

By (a) we have $\mathrm{nr}_A(\ker(k_1(\rho))) = \ker(\rho')$, so that

$$\ker(\det_{R'}) = k_1(\rho)(SK_1(\mathcal{A})) = k_1(\rho)(SK_1(\mathcal{A})) + k_1(\rho_2)(SK_1(\mathcal{A}_2)).$$

By Theorem 8.1(i) we have

$$0 \longrightarrow \frac{K_1(\mathcal{A}')}{\ker(\det_{R'})} \xrightarrow{\partial} DT(\mathcal{B}) \longrightarrow DT(\mathcal{A}) \oplus DT(\mathcal{A}_2) \longrightarrow 0.$$

The exact sequence follows now since $\frac{K_1(\mathcal{A}')}{\ker(\det_{R'})} \simeq \rho(\mathrm{nr}_A(\mathcal{A}^\times))$, as is implied by the snake lemma applied to diagram (29).

Moreover if $x \in \mathrm{nr}(\mathcal{A}^\times)$ and $y \in K_1(\mathcal{A})$ such that $\mathrm{nr}(y) = x$ then

$$\overline{\partial}_\rho(\rho(x)) = \partial(k_1(\rho)(y)) \overset{8.1(\mathrm{ii})}{=} (\mathrm{nr}(y), 1)\mathrm{nr}(\mathcal{B}^\times) = (x, 1)\mathrm{nr}(\mathcal{B}^\times),$$

as required. □

Remark 8.12. By Lemma 8.5(iii), if $\ker(\rho') = \ker(\rho) \cap \mathrm{nr}(\mathcal{A}^\times)$ is a pro-p-group and $\mathcal{A}'$ is semisimple then (a) of Corollary 8.11(ii) holds. Moreover, the semisimplicity of $\mathcal{A}'$ implies that $\rho(\mathrm{nr}(\mathcal{A}^\times))$ is a finite group of order prime to p. Therefore the restriction $\rho' : \mathrm{nr}(\mathcal{A}^\times) \to \rho(\mathrm{nr}(\mathcal{A}^\times))$ splits. By Theorem 8.1(ii) we have the following diagram

$$\begin{array}{ccc} K_1(\mathcal{A}) & \xrightarrow{\partial \circ k_1(\rho)} & DT(\mathcal{B}) \\ \downarrow{\scriptstyle \mathrm{nr}} & \overset{\hat{\rho}}{\nearrow} & \uparrow{\scriptstyle \bar{\partial}_\rho} \\ \mathrm{nr}(\mathcal{A}^\times) & \xrightarrow{\rho} & \rho(\mathrm{nr}(\mathcal{A}^\times)) \end{array}$$

Hence if the rest of the conditions in Corollary 8.11(ii) hold and $\overline{\partial}_\rho$ is an isomorphism then, by Lemma 8.4, $\pi_{\mathcal{B}}$ splits. □

We are now in position to prove Theorem 1.2.

Proof of Theorem 1.2. The alternating group A_4 is the semidirect product $V \rtimes C_3$ of the Klein group by a group of order 3 acting faithfully.

Correspondingly, C_3 acts on $\mathbb{Q}V \cong \mathbb{Q} \oplus \mathbb{Q}V/(s) \cong \mathbb{Q} \oplus \mathbb{Q}^{(3)}$, where s is the sum of the elements of V and C_3 permutes the factors of $\mathbb{Q}V/(s)$ which is, therefore, a C_3-Galois algebra.

So $\mathbb{Q}A_4 \cong (\mathbb{Q}V) \rtimes C_3 \cong \mathbb{Q}C_3 \oplus \big((\mathbb{Q}^{(3)}) \rtimes C_3\big) \cong \mathbb{Q}C_3 \oplus \mathrm{Mat}_3(\mathbb{Q})$, by Lemma 8.8.

(i) Also $\mathbb{Z}_3V/(S) \cong \mathbb{Z}_3^3$. So, similarly, $\mathbb{Z}_3A_4 \cong \mathbb{Z}_3C_3 \oplus \mathrm{Mat}_3(\mathbb{Z}_3)$.

Hence $DT(\mathbb{Z}_3A_4) \cong DT(\mathbb{Z}_3C_3) \cong \mathbb{F}_3^\times$ by Corollary 8.2.

(ii) Pushing out the projections of $\mathbb{Z}_2A_4$ onto its images in the factors of the decompostion $\mathbb{Q}_2A_4 \cong \mathbb{Q}_2C_3 \oplus (\mathbb{Q}_2V/(s)) \rtimes C_3$, we obtain the following cartesian square:

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

$$\begin{array}{ccc} \mathbb{Z}_2A_4 & \longrightarrow & (\mathbb{Z}_2V/(s)) \rtimes C_3 \\ \downarrow & & \downarrow \rho_1 \\ \mathbb{Z}_2C_3 & \xrightarrow{\rho_2} & (\mathbb{Z}/4)C_3. \end{array} \tag{30}$$

Put, now, $\mathcal{A}_1 = (\mathbb{Z}_2V/(s)) \rtimes C_3$ to save space. Now both $DT(\mathbb{Z}_2C_3)$ and $SK_1(\mathbb{Z}_2C_3)$ are trivial, by Theorem 2.2(iv) and (v). Therefore Theorem 8.1 gives us the exact sequence:

$$SK_1(\mathcal{A}_1) \to K_1((\mathbb{Z}/4)C_3) \to DT(\mathbb{Z}_2A_4) \to DT(\mathcal{A}_1) \to 0. \tag{31}$$

Now $Z(\mathcal{A}_1) = \mathbb{Z}_2$ and the reduced norm (of $\mathbb{Q}\mathcal{A}_1$) restricted to the centre is just cubing. But $\mathbb{Z}_2^\times$ is a pro-2-group and so the cubing map $\mathbb{Z}_2^\times \to \mathbb{Z}_2^\times$ is an isomorphism. Thus, simply by considering elements in the centre, we can conclude that

$$\mathrm{nr}(K_1(\mathcal{A}_1)) = \mathbb{Z}_2^\times = \mathcal{O}^\times_{Z(\mathbb{Q}\mathcal{A}_1)}. \tag{32}$$

So $DT(\mathcal{A}_1)$ is trivial.

Again, virtually the same argument shows that

$$\mathrm{nr}(\ker(k_1(\rho_1))) = \ker(\rho_1) \cap \mathbb{Z}_2^\times. \tag{33}$$

Thus, by Corollary 8.11(i) and (31), $DT(\mathbb{Z}_2A_4) \cong \rho_1(\mathbb{Z}_2^\times) = (\mathbb{Z}/4)^\times$. □

Lemma 8.13. *Let R be a semisimple ring, Γ a finite group which acts on R by ring automorphisms and $\psi \in Z^2(G, R^\times)$. Suppose that there exists an element $u \in R$ such that $\mathrm{Tr}_\Gamma(u) := \sum_{\gamma\in\Gamma} \gamma(u) = 1$. Then $R \rtimes_\psi \Gamma$ is semisimple.*

Proof. Let $f : V \longrightarrow W$ an epimorphism of $R \rtimes_\psi \Gamma$-modules. We choose a R-splitting $s' : W \longrightarrow V$ of f. Then $s := \sum_{\gamma\in\Gamma} \gamma u s \gamma^{-1}$ is the desired $R \rtimes_\psi \Gamma$-splitting of f. □

Theorem 8.14. *Suppose that p is a prime, $C_p = \langle\sigma\rangle$ is a cyclic group of order p, Γ is a finite group, $\overline{\Gamma}$ is a quotient of Γ and L is a p-adic $\overline{\Gamma}$-Galois algebra which is unramified over $\mathbb{Q}_p$. Let Γ act on C_p so that the total action of Γ on LC_p is faithful. Put S for the maximal order of L and $\mathcal{B} = (SC_p) \rtimes_\epsilon \Gamma$, where ϵ is a 2-cycle in $Z^2(\Gamma, S^\times)$. Then $DT(\mathcal{B}) \cong (S^\Gamma/(p))^\times$ and $\pi_\mathcal{B}$ splits.*

Proof. Consider the Cartesian square of ring epimorphisms:

$$\begin{array}{ccc} SC_p \rtimes_\epsilon \Gamma & \xrightarrow{\pi_1} & S[\zeta] \rtimes_\epsilon \Gamma \\ \downarrow & & \downarrow \rho_1 \\ S \rtimes_\epsilon \Gamma & \xrightarrow{\rho_2} & (S/p) \rtimes_\epsilon \Gamma \end{array} \tag{34}$$

where $S[\zeta] = S \otimes \mathbb{Z}[\zeta]$ with ζ a pth root of 1 and π_1 is induced by an isomorphism $C_p \cong \langle\zeta\rangle$. Name the rings in the square $\mathcal{B}$, $\mathcal{A}_1$, $\mathcal{A}_2$ and T as in the square (26).

The summands of $L[\zeta]$ are tame extensions of those of L and thus the orders $\mathcal{A}_1$ and $\mathcal{A}_2$ are hereditary by Corollary 8.9. Therefore $DT(\mathcal{A}_1)$ and $DT(\mathcal{A}_2)$ are trivial by Theorem 2.2(iv). In particular, $\mathrm{nr}(\mathcal{A}_1^\times) = Z(\mathcal{A}_1)^\times = (S[\zeta]^\Gamma)^\times$, so that $\rho_1(\mathrm{nr}(\mathcal{A}_1^\times)) = (S^\Gamma/(p))^\times$.

Take the square (34) to be that of Corollary 8.11(ii), with $R = S[\zeta]$, $\mathfrak{a} = (1-\zeta)$ and, up to an obvious isomorphism, $R' = S/(p)$. Then condition (b) is satisfied by taking $R_2 = S$. Since p is unramified in S, the ring R' is a finite sum of fields and is

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

therefore semisimple. Moreover there exists $u \in R'$ such that $\mathrm{Tr}_\Gamma(u) = 1$, so that by Lemma 8.13 we conclude that T is semisimple. In addition, $\ker(\rho) \cap R^\times = 1-(1-\zeta)R$ is a pro-p-group so, by Remark 8.12, condition (a) of Corollary 8.11 is satisfied and the result follows by Corollary 8.11. □

THEOREM 8.15. *Let G be the group extension $(\Delta C_p) \rtimes_\psi \Gamma$, where p is a prime number and*

(i) *Γ and Δ are finite abelian groups of order prime to p,*

(ii) *Γ acts by group automorphisms on Δ and C_p with the action on C_p being faithful and*

(iii) *ψ is a 2-cocycle in $Z^2(\Gamma, \Delta)$.*

Then

$$DT(\mathbb{Z}_p G) \cong ((\mathbb{Z}_p\Delta)^\Gamma/(p))^\times$$

(Note that alternative descriptions are $((\mathbb{F}_p\Delta)^\Gamma)^\times$ and $(\mathcal{M}/(p))^\times$, where $\mathcal{M}$ is the maximal order in $(\mathbb{Q}\Delta)^\Gamma$.)

Proof. We can represent $\mathbb{Q}_p\Delta$ as a direct sum $\bigoplus_{ij} F_{ij}$ of p-adic fields where, for each i, $\{F_{ij}\}$ is an orbit under the action of Γ. The sum $L_i = \bigoplus_j F_{ij}$ of an orbit is then a Galois algebra for some quotient $\overline{\Gamma}_i$ of Γ. Since the order of Δ is prime to p the Galois algebras L_i are unramified.

Now $\mathbb{Z}_p\Delta$ is the maximal order in $\mathbb{Q}_p\Delta$ and so is the direct sum of the maximal orders S_i in each L_i. Morover ψ splits up as the sum of 2-cocycles ψ_i in $Z^2(\Gamma, S_i^\times)$. Thus

$$\mathbb{Z}_p G = (\mathbb{Z}_p\Delta C_p) \rtimes_\psi \Gamma = \bigoplus_i (S_i C_p) \rtimes_{\psi_i} \Gamma.$$

Hence, by Theorem 8.14,

$$DT(\mathbb{Z}_p G) = \bigoplus_i DT((S_i C_p) \rtimes_{\psi_i} \Gamma) \cong \bigoplus_i (S_i^\Gamma/(p))^\times = ((\mathbb{Z}_p\Delta)^\Gamma/(p))^\times,$$

as required. □

Taking $\Delta = \{1\}$ we have

COROLLARY 8.16. *Let $G = C_p \rtimes \Gamma$, where p is a prime and Γ is a group of automorphisms of C_p. Then $DT(\mathbb{Z}_p G) \cong \mathbb{F}_p^\times$.* □

REMARK 8.17. Let K be an abelian extension of $\mathbb{Q}$ of degree d and with conductor n (or $n\infty$). Let $H(K)$ be the kernel of the natural (Artin) map $(\mathbb{Z}/n)^\times \to \mathrm{Gal}(K/\mathbb{Q})$. If p is a prime not dividing n then $\mathcal{O}_K/(p) \cong (\mathbb{F}_{p^r})^{d/r}$, where r is the order of the image of p in $(\mathbb{Z}/n)^\times/H(K)$ (and hence the order of the Frobenius at p in $\mathrm{Gal}(K/\mathbb{Q})$).

After these preparations we are finally in position to prove Theorem 1.1.

Proof of Theorem 1.1. Let G be a dihedral or quaternion group of order $2^n m$ with odd m and let p be a prime such that $p \mid m$ and $p^2 \nmid m$. Then

$$G = (\Delta C_p) \rtimes_\psi \Gamma,$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

with $\Delta \simeq C_{2^{n-1}m/p}$, $\Gamma \simeq C_2$ acting by inversion and $\psi \in Z^2(\Gamma, C_{2^{n-1}})$ (for details see, for example, [**8**, Examples (7.39), (7.40)]). So, by Theorem 8.15, we have $DT(\mathbb{Z}_p[G]) \simeq (\mathcal{M}/(p))^\times$, where $\mathcal{M}$ denotes the maximal order in $(\mathbb{Q}\Delta)^\Gamma$. Now

$$(\mathbb{Q}\Delta)^\Gamma \simeq \prod_{d||\Delta|} \mathbb{Q}(\zeta_d)^+,$$

where $\mathbb{Q}(\zeta_d)^+$ denotes the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_d)$. Part (a) follows from Remark 8.17.

We now turn to prove part (b) and first assume that $|G| = 4m$ with odd m. Then $\mathbb{Z}_2C_m$ is the maximal order in $\mathbb{Q}_2C_m$ and is therefore isomorphic to

$$\prod_{1\leqslant d|m} S_d,$$

where $S_d = \mathbb{Z}[\zeta_d] \otimes \mathbb{Z}_2$. Since $G = C_mC_2 \rtimes_\psi \Gamma$ we obtain

$$\mathbb{Z}_2G \cong \prod_{1\leqslant d|m} (S_dC_2) \rtimes_\psi \Gamma.$$

Now

$$S_1C_2 \rtimes_\psi \Gamma \cong \begin{cases} \mathbb{Z}_2V, & \text{if } G \text{ is dihedral,} \\ \mathbb{Z}_2C_4, & \text{if } G \text{ is quaternion,} \end{cases}$$

and, therefore, in either case,

$$DT(S_1C_2 \rtimes_\psi \Gamma) \cong C_2.$$

For $1 < d \mid m$ we set $\mathcal{A}_d := S_dC_2 \rtimes_\psi \Gamma$ and $A_d := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{A}_d$. Then A_d is a sum of Γ-Galois algebras and so, by Theorem 8.14,

$$DT(\mathcal{A}_d) \cong (S_d^\Gamma/(2))^\times \cong (\mathbb{Z}[\zeta_d]^\Gamma/(2))^\times. \tag{35}$$

and

$$\pi_{\mathcal{A}_d} : \mathcal{O}^\times_{Z(A_d)} \longrightarrow DT(\mathcal{A}_d) \text{ splits.} \tag{36}$$

The result for $n = 2$ now follows from (35) combined with Remark 8.17.

Henceforth we assume $n = 3$, so that $|G| = 8m$ with odd m. Then with the same notation as before

$$\mathbb{Z}_2G \cong \bigoplus_{1\leqslant d|m} (S_dC_4) \rtimes_\psi \Gamma.$$

Now

$$S_1C_4 \rtimes_\psi \Gamma \cong \begin{cases} \mathbb{Z}_2Q_8, & \text{if } G \text{ is quaternion,} \\ \mathbb{Z}_2D_8, & \text{if } G \text{ is dihedral,} \end{cases}$$

and therefore, in either case

$$DT(S_1C_4 \rtimes_\psi \Gamma) \cong C_2^2.$$

Suppose that $1 < d \mid m$. We have a cartesian square:

$$\begin{array}{ccc} S_dC_4 \rtimes_\psi \Gamma & \longrightarrow & S_d[i] \rtimes_\psi \Gamma \\ \downarrow & & \downarrow \rho_1 \\ S_dC_2 \rtimes_\psi \Gamma & \xrightarrow{\rho_2} & (S_d/2)C_2 \rtimes_\psi \Gamma \end{array}$$

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

where $S_d[i] = \mathbb{Z}[\zeta_d, i] \otimes \mathbb{Z}_2$.

Since d is odd and greater than 1, $\mathbb{Z}[\zeta_d, i]$ is the ring of integers in $\mathbb{Q}[\zeta_d, i]$ and $\mathbb{Q}[\zeta_d, i]$ is unramified over $\mathbb{Q}[\zeta_d, i]^\Gamma$. Thus $\mathbb{Z}[\zeta_d, i] \rtimes_\psi \Gamma$ is a maximal order in $\mathbb{Q}[\zeta_d, i] \rtimes_\psi \Gamma$. Localizing, therefore, $DT(S_d[i] \rtimes_\psi \Gamma) = \{0\}$, $\mathrm{nr}((S_d[i] \rtimes_\psi \Gamma)^\times) = (S_d[i]^\Gamma)^\times$ and $\mathrm{nr}(1 + 2S_d[i] \rtimes_\psi \Gamma) = 1 + 2\,(S_d[i])^\Gamma$, since even $\mathrm{nr}(1 + 2S_d[i]) = 1 + 2\,(S_d[i])^\Gamma$. (On $\mathbb{Q}S_d[i]$, the reduced norm coincides with the algebra norm (componentwise the field norms) into $(S_d[i])^\Gamma$. Since the extension is unramified, this norm preserves the unit filtration.)

From the last two equations it follows immediately that

$$\ker(\rho_1) \cap \mathrm{nr}((S_d[i] \rtimes \Gamma)^\times) = 1 + 2\,(S_d[i])^\Gamma = \mathrm{nr}(\ker(k_1(\rho_1))).$$

We set $S_d^+ := S_d^\Gamma$ and $S_d^- := \{a \in S_d \mid \gamma(a) = -a\}$, where $\Gamma = \langle\gamma\rangle$. It follows easily that

$$\rho_1(\mathrm{nr}((S_d[i] \rtimes \Gamma)^\times)) = \{\bar{a} + \bar{b} \in \left(\frac{S_d}{(2)}C_2\right)^\Gamma \mid a \in S_d^+, b \in S_d^-, a + bi \in S_d[i]^\times\}.$$

Since S_d is unramified over S_d^Γ, it is Γ-cohomologically trivial. Therefore, there exists for each $b \in S_d^-$ an element $c \in S_d$ such that $\gamma(c) - c = b$. It follows that $b + 2c \in S_d^+$, so that indeed

$$\rho_1(\mathrm{nr}((S_d[i] \rtimes \Gamma)^\times)) = ((S_d)^\Gamma/(2)\,C_2)^\times.$$

Therefore, from Corollary 8.11(ii), we have an exact sequence

$$0 \to ((S_d)^\Gamma/(2)\,C_2)^\times \to DT((S_dC_4) \rtimes_\psi \Gamma) \to DT((S_dC_2) \rtimes_\psi \Gamma) \to 0.$$

By (36) and Lemma 8.3 this sequence is split. Moreover, we have an exact sequence

$$0 \to 1 + (1 - \sigma)(S_d)^\Gamma/(2) \to ((S_d)^\Gamma/(2)\,C_2)^\times \to ((S_d)^\Gamma/(2))^\times \to 0,$$

where σ generates C_2. This sequence also splits since the first group is an elementary abelian 2-group (of rank $\phi(d)/2$) and the third has odd order (since 2 is unramified in S_d). Using the result and work of the case $n = 2$, the present result now follows. □

As special cases we explicitly state

COROLLARY 8.18. *Let p be an odd prime number and let G be a quaternion or dihedral of order $2^n p$. Then $DT(\mathbb{Z}_pG)$ is isomorphic,*

(i) if $n = 1$, to $\mathbb{F}_p^\times$;

(ii) if $n = 2$, to $(\mathbb{F}_p^\times)^{(2)}$;

(iii) if $n = 3$, to $(\mathbb{F}_p^\times)^{(3)}$;

(iv) if $n = 4$, to $(\mathbb{F}_p^\times)^{(5)}$ or $(\mathbb{F}_p^\times)^{(3)} \times \mathbb{F}_{p^2}^\times$ according as $p \equiv \pm 1$ or ± 3 mod 8;

(v) if $n = 5$, to $(\mathbb{F}_p^\times)^{(9)}$, $(\mathbb{F}_p^\times)^{(5)} \times (\mathbb{F}_{p^2}^\times)^{(2)}$ or $(\mathbb{F}_p^\times)^{(3)} \times \mathbb{F}_{p^2}^\times \times \mathbb{F}_{p^4}^\times$, according as, mod 16, $p \in \{\pm 1\}$, $\{\pm 9\}$ or $\{\pm 3, \pm 5\}$.

COROLLARY 8.19. *(i) Let G be quaternion or dihedral of order 60, then*

(a) $DT(\mathbb{Z}_3G) \cong (\mathbb{F}_3^\times)^{(2)} \times (\mathbb{F}_9^\times)^{(2)}$ and (b) $DT(\mathbb{Z}_5G) \cong (\mathbb{F}_5^\times)^{(4)}$.

(ii) Let G be quaternion or dihedral of order 84, then

(a) $DT(\mathbb{Z}_3G) \cong (\mathbb{F}_3^\times)^{(2)} \times (\mathbb{F}_{27}^\times)^{(2)}$ and (b) $DT(\mathbb{Z}_7G) \cong (\mathbb{F}_7^\times)^{(4)}$.

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

References

1. H.Bass, Algebraic K-theory, Benjamin, New York 1968. 166, 168, 169, 170, 182, 183, 184
2. W. Bley, R. Boltje, *Computation of locally free class groups*, in F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory, Lecture Notes in Computer Science **4076**, Springer (2006), 72–86. 167, 171, 174, 177, 178
3. W. Bley, M. Breuning, *Exact algorithms for p-adic fields and epsilon constant conjectures*, preprint 2006, to appear in Illinois Journal of Mathematics. 174, 175
4. W. Bley, D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. **87** (2003), 545–590. 166
5. M. Breuning, Equivariant epsilon constants for Galois extensions of number fields and p-adic fields, Phd thesis, King's College London, 2004. 181
6. M. Breuning, D. Burns, *Leading terms of Artin L-functions at $s = 0$ and $s = 1$*, Compositio Math. **143** (2007), 1427–1464. 166
7. D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math. **129** (2001), 203–237. 166
8. C. Curtis, I. Reiner, Methods of representation theory, volume I and II. Wiley, 1981 and 1987. 170, 174, 176, 181, 186, 191
9. T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. **121** (1985), 351–376. 166
10. H. Cohen, *A course in computational algebraic number theory*, Springer Verlag (1993). 174
11. H. Cohen, *Advanced topics in computational number theory*, Springer Verlag (2000). 174, 175, 176, 178
12. W. Eberly, Computations for Algebras and Group Representations, Phd thesis, University of Toronto, 1989. 177
13. K. Friedl, L. Rónyai, *Polynomial time solutions for some problems in computational algebra*, in Proceedings, 17th ACM Symposium on Theory of Computing, Providence, 1985, 153–162. 177
14. Magma, Version V2.14-9, Sydney. 174
15. T. Nakayama and Y. Matsushima, *Über die multiplikative Gruppe einer p-adischen Divisionsalgebra*, Proc. Imp. Acad. Tokyo **19** (1943) 622–628. 170
16. I. Reiner, Maximal orders, Academic Press, London 1975. 186
17. R. G. Swan, *Algebraic K-theory*, Lecture Notes in Mathematics **76**, Springer Verlag (1968). 166
18. S. Wang, *On the commutator group of a simple algebra*, Amer. J. Math. **72** (1950) 323–334 170
19. M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Inventiones Mathematicae, **63** (1981),41–79. 166
20. André Weil, *Basic Number Theory*, Springer-Verlag (1974). 170
21. S. M. J. Wilson, *Twisted group rings and ramification*, Proc. London Math. Soc. **31** (1975), 311–330. 167

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press

22. S. M. J. Wilson, *Reduced norms in the K-Theory of orders*, Journal of Algebra **46** (1977), 1–11. 168, 170

Werner Bley bley@mathematik.uni-kassel.de

Fachbereich für Mathematik der Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel
Germany

Stephen M. J. Wilson s.m.j.wilson@durham.ac.uk

Heilbronn Institute for Mathematical Research
University Of Bristol
Royal Fort Annexe
Clifton, Bristol BS8 1TW
United Kingdom

https://doi.org/10.1112/S1461157000001480 Published online by Cambridge University Press