Journal of Algebra 657 (2024) 81–108

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Research Paper

On the existence of free sublattices of bounded index and arithmetic applications

Henri Johnston [a,*], Alex Torzewski [b,c]

[a] *Department of Mathematics and Statistics, University of Exeter, Exeter, EX4 4QF, United Kingdom*
[b] *Department of Mathematics, King's College London, Strand, London, WC2R 2LS, United Kingdom*
[c] *Heilbronn Institute for Mathematical Research, Bristol, BS8 1UG, United Kingdom*

ARTICLE INFO

Article history:
Received 1 September 2023
Available online 24 May 2024
Communicated by Gunter Malle

MSC:
16H20
11R33
11R27
11G05
11G10

Keywords:
Lattices
Orders
Normal integral bases
Minkowski units
Abelian varieties

ABSTRACT

Let $\mathcal{O}$ be a Dedekind domain whose field of fractions K is a global field. Let A be a finite-dimensional separable K-algebra and let Λ be an $\mathcal{O}$-order in A. Suppose that X is a Λ-lattice such that $K \otimes_{\mathcal{O}} X$ is free of some finite rank n over A. Then X contains a (non-unique) free Λ-sublattice of rank n. The main result of the present article is to show there exists such a sublattice Y such that the generalised module index $[X : Y]_{\mathcal{O}}$ has explicit upper bounds with respect to division that are independent of X and can be chosen to satisfy certain conditions. We give examples of applications to the approximation of normal integral bases and strong Minkowski units, and to the Galois module structure of rational points over abelian varieties.

* Corresponding author.
E-mail addresses: H.Johnston@exeter.ac.uk (H. Johnston), alex.torzewski@gmail.com (A. Torzewski).
URLs: https://mathematics.exeter.ac.uk/staff/hj241 (H. Johnston), https://nms.kcl.ac.uk/alex.torzewski/ (A. Torzewski).

https://doi.org/10.1016/j.jalgebra.2024.05.016

1. Introduction

Let A be a finite-dimensional semisimple $\mathbb{Q}$-algebra and let Λ be an order in A. For example, if G is a finite group, then the group ring $\mathbb{Z}[G]$ is an order in the group algebra $\mathbb{Q}[G]$. A Λ-lattice is a (left) Λ-module that is finitely generated and torsion-free over $\mathbb{Z}$. A special case of the Jordan–Zassenhaus theorem says that for each positive integer t, there are only finitely many isomorphism classes of Λ-lattices of $\mathbb{Z}$-rank at most t.

Now fix a positive integer n. Then there exists a positive integer m with the following property: given any Λ-lattice X such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free of rank n as an A-module, there exists a free Λ-sublattice Y of X such that the index $[X : Y]$ is at most m. To see this, first note that by clearing denominators of a free basis of $\mathbb{Q} \otimes_{\mathbb{Z}} X$ over A, any such X must contain a (non-unique) free Λ-sublattice of rank n, necessarily of finite index m_X in X. Since the Jordan–Zassenhaus theorem implies that there are only finitely many choices for X up to isomorphism, we may take m to be the maximal m_X as X ranges over all such choices. Masser–Wüstholz [41,42] defined the *class index* $i_n(\Lambda)$ to be the smallest possible value of m. Using methods from the geometry of numbers, they were able to provide upper bounds for $i_n(\Lambda)$ in special cases that led to results on the existence of isogenies between abelian varieties of small degrees (see also [34]).

We can in fact consider bounds that are also upper bounds with respect to division. In the above argument, we can instead take m to be any common multiple of the m_X. Then m has the following property: given any Λ-lattice X such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free of rank n as an A-module, there exists a free Λ-sublattice Y of X such that $[X : Y]$ divides m. The main goals of the present article are to give explicit choices of m with this property and to give examples of arithmetic applications. In fact, the setting generalises to the case in which Λ is an $\mathcal{O}$-order where $\mathcal{O}$ is a Dedekind domain whose field of fractions K is a global field assumed not to be equal to $\mathcal{O}$, and A is a finite-dimensional semisimple K-algebra. In this situation, the group index $[X : Y]$ is replaced by the generalised module index $[X : Y]_{\mathcal{O}}$. The main result, Theorem 4.5, gives upper bounds for this index with respect to division that are independent of X and can be chosen to satisfy certain conditions. The proof of this result requires the hypothesis that A is a separable K-algebra; if K is of characteristic zero, then this follows automatically from the assumption that A is semisimple.

We now give examples of the algebraic results and arithmetic applications. The following result is a weaker version of Theorem 5.3 obtained via specialisation and Remark 7.2.

Theorem 1.1. *Let G be a finite group and let k be a positive integer. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any $\mathbb{Z}[G]$-lattice X such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free of rank n over $\mathbb{Q}[G]$, there exists a free $\mathbb{Z}[G]$-sublattice Z of X such that the index $[X : Z]$ divides $i \cdot |G|^{\lceil 3|G|/2 \rceil n}$.*

In Theorem 5.3, we also give conditions on G under which we can take $i = 1$ (see also §5.4). The term $|G|^{\lceil 3|G|/2 \rceil n}$ is a crude but neat upper bound for a more precise

expression that will be made explicit. The following result is Theorem 5.15, which is just one example of the stronger results that can be obtained in special cases.

Theorem 1.2. *Let G be a finite group and suppose that there exist positive integers $t, n_1, \dots, n_t$ such that $\mathbb{Q}[G] \cong \prod_{i=1}^{t} \mathrm{Mat}_{n_i}(\mathbb{Q})$. If X is an $\mathbb{Z}[G]$-lattice such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free of rank n over $\mathbb{Q}[G]$, then there exists a free $\mathbb{Z}[G]$-sublattice Z of X such that $[X : Z]$ divides*

$$\left(|G|^{|G|} \prod_{i=1}^{t} n_i^{-n_i^2} \right)^{\frac{3n}{2}}.$$

Before sketching the ideas used in the proof of the main result, we discuss how a variant of Theorem 1.1 can be applied in the following arithmetic situation. Let L/K be a finite Galois extension such that K is equal to either $\mathbb{Q}$ or an imaginary quadratic field. Let $G = \mathrm{Gal}(L/K)$ and let μ_L denote the roots of unity of L. In this setting, $\mathcal{O}_L^{\times}/\mu_L$ is a $\mathbb{Z}[G]$-lattice and one can show that L/K has a so-called *Minkowski unit*, that is, an element $\varepsilon \in \mathcal{O}_L^{\times}/\mu_L$ such that $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathcal{O}_L^{\times}/\mu_L) = \mathbb{Q}[G] \cdot \varepsilon$. Such an ε is said to be a *strong Minkowski unit* if $\mathcal{O}_L^{\times}/\mu_L = \mathbb{Z}[G] \cdot \varepsilon$. The existence of strong Minkowski units (which some authors refer to as Minkowski units) has been studied in numerous articles; see Remark 8.3. In §8, we give several results on the approximation of strong Minkowski units. The following result is a weakening of Theorem 8.5 obtained via Remark 8.6.

Theorem 1.3. *Let G be a finite group and let k be a positive integer. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any finite Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$ and K equal to either $\mathbb{Q}$ or an imaginary quadratic field, there exists a Minkowski unit $\varepsilon \in \mathcal{O}_L^{\times}/\mu_L$ such that the index $[\mathcal{O}_L^{\times}/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/K)] \cdot \varepsilon]$ divides $i \cdot |G|^{\lceil 3|G|/2 \rceil - 2}$.*

Again, stronger results can be obtained in special cases. Analogous applications to the approximation of normal integral bases are given in §7 and to the Galois module structure of rational points on abelian varieties are given in §9.

We now outline the ideas used in the proof of the main result Theorem 4.5. Let $\mathcal{O}$ be a Dedekind domain whose field of fractions K is a global field and assume that $\mathcal{O} \neq K$. Let A be a finite-dimensional separable K-algebra and let Λ be an $\mathcal{O}$-order in A. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A containing Λ. Note that the existence of $\mathcal{M}$ is ensured by the separability hypothesis on A and that the choice of $\mathcal{M}$ need not be unique. Let X be a Λ-lattice such that $K \otimes_{\mathcal{O}} X$ is free of rank 1 over A (the higher rank case is similar). We consider the unique $\mathcal{M}$-lattice ${}^{\mathcal{M}}X$ contained in X that is maximal with respect to inclusion. Then ${}^{\mathcal{M}}X$ is locally free over $\mathcal{M}$, and as explained in Corollary 4.2, ${}^{\mathcal{M}}X$ contains a free $\mathcal{M}$-sublattice $\mathcal{M} \cdot \varepsilon$ with an index that can be controlled (the key ingredients here are the Jordan–Zassenhaus theorem and Roiter's lemma). Hypotheses on $\mathcal{M}$ can also be given to ensure that this index is trivial (see Lemma 2.2). We then

obtain a bound on the index $[X : \Lambda \cdot \varepsilon]_{\mathcal{O}}$ by taking the product of bounds on the indices corresponding to each of the three inclusions

$$\Lambda \cdot \varepsilon \subseteq \mathcal{M} \cdot \varepsilon \subseteq {}^{\mathcal{M}}X \subseteq X.$$

Note that $[\mathcal{M} \cdot \varepsilon : \Lambda \cdot \varepsilon]_{\mathcal{O}} = [\mathcal{M} : \Lambda]_{\mathcal{O}}$, which is equal to the product of the indices of the localisations of $\mathcal{M}$ and Λ. Moreover, $[X : {}^{\mathcal{M}}X]_{\mathcal{O}}$ divides $[\mathcal{M}X : {}^{\mathcal{M}}X]_{\mathcal{O}}$, where $\mathcal{M}X$ is the unique $\mathcal{M}$-lattice containing X that is minimal with respect to inclusion. In Corollary 3.3, we show that $[\mathcal{M}X : {}^{\mathcal{M}}X]_{\mathcal{O}}$ divides $[\mathcal{M} : J]_{\mathcal{O}}$ where J is any full two-sided ideal of $\mathcal{M}$ contained in Λ. Again, $[\mathcal{M} : J]_{\mathcal{O}}$ can be computed by localisation. Crucially, the product of bounds of indices obtained is independent of the choice of Λ-lattice X.

If G is a finite group such that $|G|$ is invertible in K and $\Lambda = \mathcal{O}[G]$, then J can be taken to be the (left) conductor of $\mathcal{M}$ into Λ (the left and right conductors are equal in this case) and $[\mathcal{M} : J]_{\mathcal{O}}$ can be computed explicitly using Jacobinski's conductor formula [23]. We also obtain an explicit formula for $[\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}}$, which may be of independent interest. Note that in the setting of Theorem 1.1 with $n = 1$, the term $|G|^{\lceil 3|G|/2 \rceil}$ is a crude but neat upper bound for $[\mathcal{M} : \mathbb{Z}[G]] \cdot [\mathcal{M} : J] = [\mathcal{M} : \mathbb{Z}[G]]^3$ and the term i is the upper bound for $[{}^{\mathcal{M}}X : \mathcal{M} \cdot \varepsilon]$ given by Corollary 4.2. Moreover, we can take $i = 1$ when $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2 (see §5.4 for conditions on G under which this holds).

Acknowledgements

The authors are grateful to Werner Bley, Nigel Byott, Frank Calegari, Hebert Gangl, Tommy Hofmann, Donghyeok Lim, Daniel Macias Castillo, Alexandre Maksoud and John Nicholson for helpful comments and discussions. The authors are indebted to the anonymous referee for carefully reading the manuscript, for corrections to the statements of Proposition 5.11 and Lemma 8.2, and for drawing their attention to the work of Masser–Wüstholz.

2. Preliminaries on lattices and orders

For further background, we refer the reader to [11,46,21]. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. To avoid trivialities, we assume that $\mathcal{O} \neq K$.

2.1. Lattices over Dedekind domains

An *$\mathcal{O}$-lattice M* is a finitely generated torsion-free $\mathcal{O}$-module, or equivalently, a finitely generated projective $\mathcal{O}$-module. Using the former definition and the fact that $\mathcal{O}$ is noetherian, we see that any $\mathcal{O}$-submodule of an $\mathcal{O}$-lattice is again an $\mathcal{O}$-lattice.

For any finite-dimensional K-vector space V, an $\mathcal{O}$-lattice in V is a finitely generated $\mathcal{O}$-submodule M of V. Given such an M, we define a K-vector subspace of V by

$$KM := \{\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in K, m_i \in M\}$$

and say that M is a *full* $\mathcal{O}$-lattice in V if $KM = V$. Each $\mathcal{O}$-lattice M may be viewed as a full $\mathcal{O}$-lattice in the finite-dimensional K-vector space $K \otimes_{\mathcal{O}} M$ by identifying M with its image $1 \otimes M$. We may identify $K \otimes_{\mathcal{O}} M$ with KM.

Let M and N be a pair of full $\mathcal{O}$-lattices in a finite-dimensional K-vector space V. Since N contains a K-basis for V, for each $m \in M$ there is a nonzero $r \in \mathcal{O}$ such that $rm \in N$. Therefore there exists a nonzero $r \in \mathcal{O}$ such that $rM \subseteq N$ since M is finitely generated over $\mathcal{O}$.

For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, let $\mathcal{O}_{\mathfrak{p}}$ denote the localisation of $\mathcal{O}$ at $\mathfrak{p}$. Let $\widehat{\mathcal{O}}_{\mathfrak{p}}$ denote the completion of $\mathcal{O}$ at $\mathfrak{p}$ and let $\widehat{K}_{\mathfrak{p}}$ denote its field of fractions. For an $\mathcal{O}$-lattice M, we define the localisation M at $\mathfrak{p}$ to be the $\mathcal{O}_{\mathfrak{p}}$-lattice $M_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} M$ and the completion of M at $\mathfrak{p}$ to be the $\widehat{\mathcal{O}}_{\mathfrak{p}}$-lattice $\widehat{M_{\mathfrak{p}}} := \widehat{\mathcal{O}}_{\mathfrak{p}} \otimes_{\mathcal{O}} M$. By identifying M with its image $1 \otimes M$, we may view M as embedded in $M_{\mathfrak{p}}$. Viewing M and each $M_{\mathfrak{p}}$ as embedded in KM, we have $M = \bigcap_{\mathfrak{p}} M_{\mathfrak{p}}$, where $\mathfrak{p}$ ranges over all maximal ideals of $\mathcal{O}$ (see [46, (4.21)]).

2.2. Generalised module indices

Much of the material in the following paragraph is explained in more detail in [18, §3]. Let M, N be full $\mathcal{O}$-lattices in a finite-dimensional K-vector space V. First consider the case in which $\mathcal{O}$ is a discrete valuation ring. Then M and N are both free and of equal rank over $\mathcal{O}$, and so there exists an $\alpha \in \mathrm{Aut}_K(V)$ with $\alpha(M) = N$. Moreover, α is unique modulo $\mathrm{Aut}_{\mathcal{O}}(N)$; hence its determinant is unique modulo $\mathcal{O}^\times$, and so the ideal $[M : N]_{\mathcal{O}} := \mathcal{O}\det(\alpha)$ is a uniquely defined fractional ideal of $\mathcal{O}$. Now consider the case in which $\mathcal{O}$ is an arbitrary Dedekind domain. For almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ we have $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ and hence $[M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{\mathcal{O}_{\mathfrak{p}}} = \mathcal{O}_{\mathfrak{p}}$ (see [11, Exercise 4.7]). Therefore there is a unique fractional ideal $[M : N]_{\mathcal{O}}$ of $\mathcal{O}$ such that $([M : N]_{\mathcal{O}})_{\mathfrak{p}} = [M_{\mathfrak{p}} : N_{\mathfrak{p}}]_{\mathcal{O}_{\mathfrak{p}}}$ for all $\mathfrak{p}$. Note that if M_1, M_2, M_3 are full $\mathcal{O}$-lattices in V, then $[M_1 : M_3]_{\mathcal{O}} = [M_1 : M_2]_{\mathcal{O}} \cdot [M_2 : M_3]_{\mathcal{O}}$. Moreover, if $\mathcal{O}'$ is a Dedekind domain containing $\mathcal{O}$, then $\mathcal{O}' \otimes_{\mathcal{O}} [M : N]_{\mathcal{O}} = [\mathcal{O}' \otimes_{\mathcal{O}} M : \mathcal{O}' \otimes_{\mathcal{O}} N]_{\mathcal{O}'}$. If $N \subseteq M$ are $\mathbb{Z}$-lattices of equal rank, then we abbreviate $[M : N]_{\mathbb{Z}}$ to $[M : N]$, which is consistent with the fact that $[M : N]_{\mathbb{Z}}$ is the $\mathbb{Z}$-ideal generated by the usual group index of N in M.

Lemma 2.1. *Suppose we have a diagram of $\mathcal{O}$-lattices with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0, \end{array}$$

such that $KN_i = KM_i$ *for* $i = 1, 2, 3$. *Then* $[M_2 : N_2]_{\mathcal{O}} = [M_1 : N_1]_{\mathcal{O}} \cdot [M_3 : N_3]_{\mathcal{O}}$.

Proof. For $i = 1, 3$, fix K-linear maps $\alpha_i \colon KM_i \to KM_i$ such that $\alpha_i(M_i) = N_i$. Let $\pi \colon N_2 \to N_3$ denote the map in the above diagram. Since N_3 is $\mathcal{O}$-projective, there exists an $\mathcal{O}$-section $s \colon N_3 \to N_2$ of π. Then define $\tilde{\alpha}_3 \colon KM_3 \to KM_2$ by $\tilde{\alpha}_3 = (K \otimes_{\mathcal{O}} s) \circ \alpha_3$. Fixing an $\mathcal{O}$-linear splitting $M_2 \cong M_1 \oplus M_3$ (which exists since M_3 is $\mathcal{O}$-projective) and thus a K-linear splitting $KM_2 \cong KM_1 \oplus KM_3$, we then obtain a K-linear map $\alpha_2 := (\alpha_1 + \tilde{\alpha}_3) \colon KM_2 \to KM_2$ such that $\alpha_2(M_2) = N_2$ and $\alpha_1(M_1) = N_1$. Hence, with respect to a K-basis of KM_2 extending a K-basis of KM_1, the matrix representing α_2 is block upper triangular. Consequently, $\det(\alpha_2) = \det(\alpha_1)\det(\alpha_3)$, and thus we obtain the desired result. □

2.3. Duals of lattices

Let M be an $\mathcal{O}$-lattice. The linear dual $M^\vee := \mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O})$ is also an $\mathcal{O}$-lattice and there is a canonical identification $(M^\vee)^\vee = M$. Moreover, $(-)^\vee$ is inclusion-reversing. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, we have $(M_{\mathfrak{p}})^\vee = (M^\vee)_{\mathfrak{p}}$. Together with the fact that determinants are invariant under transposition, this implies that if M and N are full $\mathcal{O}$-lattices in a finite-dimensional K-vector space V, then $[M : N]_{\mathcal{O}} = [N^\vee : M^\vee]_{\mathcal{O}}$.

2.4. Lattices over orders

Let A be a finite-dimensional K-algebra and let Λ be an $\mathcal{O}$-*order* in A, that is, a subring of A that is also a full $\mathcal{O}$-lattice in A. Note that Λ is both left and right noetherian since Λ is finitely generated over $\mathcal{O}$. A left Λ-*lattice* X is a left Λ-module that when considered as an $\mathcal{O}$-module is also an $\mathcal{O}$-lattice; in this case, KX may be viewed as a left A-module.

Henceforth all modules (resp. lattices) shall be assumed to be left modules (resp. lattices) unless otherwise stated. Two Λ-lattices are said to be isomorphic if they are isomorphic as Λ-modules.

For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, the localisation $\Lambda_{\mathfrak{p}}$ is an $\mathcal{O}_{\mathfrak{p}}$-order in A, and the completion $\widehat{\Lambda}_{\mathfrak{p}}$ is a $\widehat{\mathcal{O}}_{\mathfrak{p}}$-order in $\widehat{K}_{\mathfrak{p}} \otimes_K A$. Localising a Λ-lattice X at $\mathfrak{p}$ yields a $\Lambda_{\mathfrak{p}}$-lattice $X_{\mathfrak{p}}$, and completing X at $\mathfrak{p}$ yields a $\widehat{\Lambda}_{\mathfrak{p}}$-lattice $\widehat{X}_{\mathfrak{p}}$. Given Λ-lattices X and Y, we have that $X_{\mathfrak{p}} \cong Y_{\mathfrak{p}}$ as $\Lambda_{\mathfrak{p}}$-lattices if and only if $\widehat{X}_{\mathfrak{p}} \cong \widehat{Y}_{\mathfrak{p}}$ as $\widehat{\Lambda}_{\mathfrak{p}}$-lattices (see [46, (18.2)]). For a positive integer n, a Λ-lattice X is said to be *locally free of rank* n, if for each maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, the $\Lambda_{\mathfrak{p}}$-lattice $X_{\mathfrak{p}}$ is free of rank n, or equivalently, the $\widehat{\Lambda}_{\mathfrak{p}}$-lattice $\widehat{X}_{\mathfrak{p}}$ is free of rank n. Note that every locally free Λ-lattice is projective by [11, (8.19)].

2.5. Maximal orders

Suppose that A is a separable finite-dimensional K-algebra (see [46, §7c]). A *maximal* $\mathcal{O}$-order in A is an $\mathcal{O}$-order that is not properly contained in any other $\mathcal{O}$-order in A.

For any $\mathcal{O}$-order Λ in A, there exists a (not necessarily unique) maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ by [46, (10.4)]. If $\mathcal{M}$ is a maximal $\mathcal{O}$-order, X is an $\mathcal{M}$-lattice, and n is a positive integer, then by [11, (31.2)(iii)] we have that KX is free of rank n over A if and only if X is locally free of rank n.

2.6. Locally free class groups and cancellation properties

Suppose that K is a global field and that A is separable finite-dimensional K-algebra. Let Λ be an $\mathcal{O}$-order A. Let $P(\Lambda)$ be the free abelian group generated by symbols $[X]$, one for each isomorphism class of locally free Λ-lattices X, modulo relations $[X] = [X_1]+[X_2]$ whenever $X \cong X_1 \oplus X_2$. We define the *locally free class group* $\mathrm{Cl}(\Lambda)$ of Λ to be the subgroup of $P(\Lambda)$ consisting of all elements that can be written in the form $[X] - [Y]$, with X, Y locally free and $KX \cong KY$.

We remark that $[X] - [Y] = 0$ in $\mathrm{Cl}(\Lambda)$ if and only if X is *stably isomorphic to* Y, that is, $X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)}$ for some positive integer k (here $\Lambda^{(k)}$ denotes the direct sum of k copies of Λ). The order Λ is said to have the *locally free cancellation property* if given any pair of locally free Λ-lattices X and Y,

$$X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \text{ for some } k \in \mathbb{Z}_{\geq 0} \implies X \cong Y.$$

Moreover, Λ is said to have the *stably free cancellation property* if this holds in the special case that Y is free. If A satisfies the so-called *Eichler condition* relative to $\mathcal{O}$, then Λ has the locally free cancellation property; this condition is satisfied if A is commutative (see [12, §51] for further details).

If n is a positive integer and Y is any locally free Λ-lattice of rank n, then by [11, (31.14)] there exists a locally free Λ-lattice X in A such that $Y \cong \Lambda^{(n-1)} \oplus X$. Hence every element of $\mathrm{Cl}(\Lambda)$ is expressible in the form $[X_1]-[X_2]$, where X_1 and X_2 are locally free Λ-lattices in A. In particular, the Jordan–Zassenhaus theorem [46, (26.4)] implies that $\mathrm{Cl}(\Lambda)$ is finite. Moreover, for each such pair X_1, X_2, there exists another such lattice X_3 such that $X_2 \oplus X_3 \cong \Lambda \oplus X_1$ by [11, (31.7)]. Therefore every element of $\mathrm{Cl}(\Lambda)$ is in fact expressible in the form $[X] - [\Lambda]$ for some locally free Λ-lattice X in A.

The following result is easily deduced from the above discussion.

Lemma 2.2. *The following statements are equivalent:*

(i) *every locally free Λ-lattice is in fact free;*
(ii) *every locally free Λ-lattice of rank 1 is in fact free;*
(iii) $\mathrm{Cl}(\Lambda)$ *is trivial and Λ has the stably free cancellation property;*
(iv) $\mathrm{Cl}(\Lambda)$ *is trivial and Λ has the locally free cancellation property.*

Remark 2.3. Lemma 2.2 will often be applied in the case that Λ is a maximal $\mathbb{Z}$-order. Smertnig and Voight [50, Theorem 1.3] have classified all maximal $\mathbb{Z}$-orders in totally

definite quaternion algebras with the locally free cancellation property, and from this it is straightforward to determine whether any given maximal $\mathbb{Z}$-order in a finite-dimensional semisimple $\mathbb{Q}$-algebra has the locally free cancellation property. See also Remark 5.12.

3. Overlattices and sublattices for overorders

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and assume that $\mathcal{O} \neq K$.

3.1. Setup and definitions

Let A be a finite-dimensional K-algebra. Let $\Lambda \subseteq \Gamma$ be $\mathcal{O}$-orders in A and let X be a Λ-lattice. Define

$$\Gamma X := \{\gamma_1 m_1 + \gamma_2 m_2 + \cdots + \gamma_r m_r \mid r \in \mathbb{Z}_{\geq 0}, m_i \in X, \gamma_i \in \Gamma\} \subseteq KX.$$

This is the unique Γ-lattice in KX containing X that is minimal with respect to inclusion.

There exists a nonzero $r \in \mathcal{O}$ such that $r\Gamma \subseteq \Lambda$ (see §2.1) and so $r\Gamma X$ is a Γ-lattice contained in X of finite index. Since the sum of any two Γ-lattices contained in X is also a Γ-lattice contained in X, we see that there exists a unique Γ-lattice contained in X that is maximal with respect to inclusion, which we shall denote by ${}^{\Gamma}X$.

For a right Λ-lattice X, we define $X\Gamma$ and X^{Γ} similarly. Note that ${}^{\Gamma}\Lambda$ (resp. Λ^{Γ}) coincides with the right (resp. left) conductor of Γ into Λ (see [11, (27.2)]).

3.2. Bounds on indices

The following result gives a bound on

$$[\Gamma X : {}^{\Gamma}X]_{\mathcal{O}} = [\Gamma X : X]_{\mathcal{O}} \cdot [X : {}^{\Gamma}X]_{\mathcal{O}}$$

that only depends on Γ and Λ, and not on the particular choice of lattice X.

Proposition 3.1. *Let A be a finite-dimensional K-algebra and let $\Lambda \subseteq \Gamma$ be $\mathcal{O}$-orders in A. Let J be any full two-sided ideal of Γ contained in Λ. Let X be a Λ-lattice such that ΓX is locally free of rank n over Γ. Then $[\Gamma X : {}^{\Gamma}X]_{\mathcal{O}}$ divides $[\Gamma : J]_{\mathcal{O}}^{n}$.*

Remark 3.2. There are many possible choices of J, and the best choice will be context specific. For example, a weak but general choice is $J = [\Gamma : \Lambda]_{\mathcal{O}} \cdot \Gamma$. Moreover, J can always be taken to be the two-sided ideal of Γ generated by the central conductor of Γ into Λ, that is, by $\{x \in C \mid x\Gamma \subseteq \Lambda\}$, where C denotes the centre of A.

Proof of Proposition 3.1. Since J is a left Γ-lattice contained in Λ, we have that JX is a left Γ-lattice contained in X. Hence JX is contained in ${}^{\Gamma}X$. The chain of containments

$$JX \subseteq {}^{\Gamma}X \subseteq X \subseteq \Gamma X$$

implies that $[\Gamma X : {}^{\Gamma}X]_{\mathcal{O}}$ divides $[\Gamma X : JX]_{\mathcal{O}}$. Thus it remains to show that

$$[\Gamma X : JX]_{\mathcal{O}} = [\Gamma : J]^n_{\mathcal{O}}.$$

Since indices are defined locally and $([\Gamma X : JX]_{\mathcal{O}})_{\mathfrak{p}} = [\Gamma_{\mathfrak{p}} X_{\mathfrak{p}} : J_{\mathfrak{p}} X_{\mathfrak{p}}]_{\mathcal{O}_{\mathfrak{p}}}$ for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, we can and do assume without loss of generality that $\mathcal{O}$ is a discrete valuation ring. Then by hypothesis there exist $\varepsilon_1, \dots, \varepsilon_n \in \Gamma X$ such that $\Gamma X = \Gamma\varepsilon_1 \oplus \cdots \oplus \Gamma\varepsilon_n$. Since J is a right Γ-module, we have

$$JX = J\Gamma X = J(\Gamma\varepsilon_1 \oplus \cdots \oplus \Gamma\varepsilon_n) = J\varepsilon_1 \oplus \cdots \oplus J\varepsilon_n.$$

Therefore

$$[\Gamma X : JX]_{\mathcal{O}} = [\Gamma\varepsilon_1 \oplus \cdots \oplus \Gamma\varepsilon_n : J\varepsilon_1 \oplus \cdots \oplus J\varepsilon_n]_{\mathcal{O}} = [\Gamma : J]^n_{\mathcal{O}}. \quad \square$$

Corollary 3.3. *Let A be a separable finite-dimensional K-algebra and let Λ be an $\mathcal{O}$-order in A. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A containing Λ and let J be any full two-sided ideal of $\mathcal{M}$ contained in Λ. Let X be a Λ-lattice such that KX is free of rank n over A. Then $[\mathcal{M}X : {}^{\mathcal{M}}X]_{\mathcal{O}}$ divides $[\mathcal{M} : J]^n_{\mathcal{O}}$.*

Proof. Since KX is free of rank n over A, we have that $\mathcal{M}X$ is locally free of rank n over $\mathcal{M}$ (see §2.5), and so the desired result follows directly from Proposition 3.1. $\square$

Remark 3.4. In Proposition 3.1 and Corollary 3.3, the order Λ can be replaced by the so-called *associated order* $\mathcal{A}(X) = \{\alpha \in A \mid \alpha X \subseteq X\}$. Thus if the containment $\Lambda \subseteq \mathcal{A}(X)$ is strict, then working over $\mathcal{A}(X)$ may allow a choice of $J \subseteq \mathcal{A}(X)$ with improved index $[\mathcal{M} : J]_{\mathcal{O}}$. For example, if $\mathcal{M}$ is a maximal order containing Λ and we take $X = \mathcal{M}$, then $\mathcal{A}(X) = \mathcal{M}$ and so we can take $J = \mathcal{M}$, which is consistent with the fact that $\mathcal{M}X = X = {}^{\mathcal{M}}X$ in this situation. Of course, the disadvantage of this approach is that $\mathcal{A}(X)$ depends on X.

3.3. Duals and overorders

For an $\mathcal{O}$-order Λ in a finite-dimensional K-algebra and any left (resp. right) Λ-lattice X, the dual $X^\vee = \mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O})$ has the structure of a right (resp. left) Λ-lattice, and there is a canonical identification $(X^\vee)^\vee = X$.

Lemma 3.5. *Let $\Lambda \subseteq \Gamma$ be $\mathcal{O}$-orders in a finite-dimensional K-algebra.*

(i) *If X is a left Λ-lattice, then we have an equality of right Γ-lattices $(\Gamma X)^\vee = (X^\vee)^\Gamma$ and an equality of indices $[\Gamma X : X]_{\mathcal{O}} = [X^\vee : (X^\vee)^\Gamma]_{\mathcal{O}}$.*

(ii) *If X is a right Λ-lattice, then we have an equality of left Γ-lattices $(X\Gamma)^\vee = {}^\Gamma(X^\vee)$ and an equality of indices $[X\Gamma : X]_\mathcal{O} = [X^\vee : {}^\Gamma(X^\vee)]_\mathcal{O}$.*

Proof. We only prove part (i). Since $(-)^\vee$ reverses inclusions, $(\Gamma X)^\vee$ is a right Γ-lattice contained in $X^\vee$. Hence $(\Gamma X)^\vee$ is contained in $(X^\vee)^\Gamma$ by definition of the latter. Dualising, we also have that

$$\Gamma X = ((\Gamma X)^\vee)^\vee \supseteq ((X^\vee)^\Gamma)^\vee. \tag{3.1}$$

Since $((X^\vee)^\Gamma)^\vee$ is itself a left Γ-lattice containing X, this forces equality in (3.1) and hence $(\Gamma X)^\vee = (X^\vee)^\Gamma$ as desired. Finally, since $(-)^\vee$ preserves indices (see §2.3) we have that $[\Gamma X : X]_\mathcal{O} = [X^\vee : (\Gamma X)^\vee]_\mathcal{O} = [X^\vee : (X^\vee)^\Gamma]_\mathcal{O}$. □

3.4. The commutative separable setting

In the setting of commutative separable algebras, the following result of Fröhlich is a refinement of Corollary 3.3.

Theorem 3.6 *(Fröhlich [17]). Let A be a commutative separable finite-dimensional K-algebra and let Λ be an $\mathcal{O}$-order in A. Let $\mathcal{M}$ be the unique maximal $\mathcal{O}$-order in A. Let X be a Λ-lattice such that KX is free of rank n over A. Then both $[\mathcal{M}X : X]_\mathcal{O}$ and $[X : {}^\mathcal{M}X]_\mathcal{O}$ divide $[\mathcal{M} : \Lambda]^n_\mathcal{O}$.*

Proof. The claim that $[\mathcal{M}X : X]_\mathcal{O}$ divides $[\mathcal{M} : \Lambda]^n_\mathcal{O}$ is contained in [17, Theorem 4].

It remains to show that $[X : {}^\mathcal{M}X]_\mathcal{O}$ divides $[\mathcal{M} : \Lambda]^n_\mathcal{O}$. Since A is separable there is an isomorphism of (right) A-modules $A \cong \mathrm{Hom}_K(A, K)$ induced by the pairing of [11, (7.41)]. Thus there are A-module isomorphisms

$$K(X^\vee) \cong \mathrm{Hom}_K(KX, K) \cong \mathrm{Hom}_K(A^{(n)}, K) \cong \mathrm{Hom}_K(A, K)^{(n)} \cong A^{(n)}.$$

Lemma 3.5(ii) implies that $[X : {}^\mathcal{M}X]_\mathcal{O} = [X^\vee\mathcal{M} : X^\vee]_\mathcal{O} = [\mathcal{M}X^\vee : X^\vee]_\mathcal{O}$, where in the last equality, we consider $X^\vee$ as a left $\mathcal{M}$-lattice, as we may since $\mathcal{M}$ is commutative. Moreover, since $K(X^\vee)$ is free of rank n over A, the first claim and the appropriate substitution imply that $[\mathcal{M}X^\vee : X^\vee]_\mathcal{O}$ divides $[\mathcal{M} : \Lambda]^n_\mathcal{O}$. □

Remark 3.7. [5, §7, Example 1] shows that the result analogous to Theorem 3.6 does not always hold in the noncommutative separable setting.

4. Free sublattices of bounded index

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Assume that K is a global field and that $\mathcal{O} \neq K$. Let A be a separable finite-dimensional K-algebra.

4.1. Free sublattices of locally free lattices

The following result gives a bound on the index of a free sublattice in a locally free lattice.

Proposition 4.1. *Let Γ be an $\mathcal{O}$-order in A and let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}$. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: for every locally free Γ-lattice X, there exists a free Γ-sublattice Y of X such that $[X : Y]_{\mathcal{O}}$ divides $\mathcal{I}$.*

Proof. By [11, (31.14)], for a positive integer n and a locally free Γ-lattice X of rank n, there exists a locally free Γ-lattice W of rank 1 such that $X \cong \Gamma^{(n-1)} \oplus W$. Thus the problem reduces to the case of locally free Λ-lattices W of rank 1. The number of isomorphism classes of such lattices is finite by the Jordan–Zassenhaus theorem [46, (26.4)]. For each such class, choose a representative W and note that by Roiter's lemma [11, (31.6)] there exists an embedding $\iota_W : \Gamma \hookrightarrow W$ such that $[W : \iota_W(\Gamma)]_{\mathcal{O}}$ is coprime to $\mathcal{K}$. Now take $\mathcal{I}$ to be any common multiple of the (finite number of) ideals $[W : \iota_W(\Gamma)]_{\mathcal{O}}$ as W varies. □

Corollary 4.2. *Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A and let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}$. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any $\mathcal{M}$-lattice X such that KX is free as an A-module, there exists a free $\mathcal{M}$-sublattice Y of X such that $[X : Y]_{\mathcal{O}}$ divides $\mathcal{I}$.*

Proof. Let X be an $\mathcal{M}$-lattice. Then KX is free as an A-module if and only if $\mathcal{M}X$ is locally free over $\mathcal{M}$ (see §2.5). Hence the result follows from Proposition 4.1. □

Remark 4.3. If Γ (resp. $\mathcal{M}$) satisfies the equivalent conditions of Lemma 2.2, then it is clear that we can take $\mathcal{I} = \mathcal{O}$ in Proposition 4.1 (resp. Corollary 4.2).

Given a finite set S of maximal ideals of $\mathcal{O}$, let $\mathcal{O}_S = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}$, where $\mathfrak{p}$ ranges over all maximal ideals of $\mathcal{O}$ not in S. We include the following result for general interest.

Corollary 4.4. *Let Γ be an $\mathcal{O}$-order in A and let T be a finite set of maximal ideals of $\mathcal{O}$. Then there exists a finite set S of maximal ideals of $\mathcal{O}$ such that $S \cap T = \emptyset$ and $\mathcal{O}_S \otimes_{\mathcal{O}} \Gamma$ satisfies the equivalent conditions of Lemma 2.2.*

Proof. If $\mathcal{K}$ is the product of the maximal ideals in T and $\mathcal{I}$ is the ideal given by Proposition 4.1, then we can take S to be the set of maximal ideals dividing $\mathcal{I}$. □

4.2. The main theorem

The main theorem of the present article is as follows.

Theorem 4.5. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Assume that K is a global field and that $\mathcal{O} \neq K$. Let A be a separable finite-dimensional K-algebra and let Λ be an $\mathcal{O}$-order in A. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A containing Λ and let J be any full two-sided ideal of $\mathcal{M}$ contained in Λ. Let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}$. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any Λ-lattice X such that KX is free of rank n over A, there exists a free Λ-sublattice Z of X such that $[X : Z]_{\mathcal{O}}$ divides $\mathcal{I} \cdot [\mathcal{M} : \Lambda]_{\mathcal{O}}^{2n}$ if A is commutative or $\mathcal{I} \cdot [\mathcal{M} : J]_{\mathcal{O}}^{n} \cdot [\mathcal{M} : \Lambda]_{\mathcal{O}}^{n}$ otherwise. Moreover, if $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}$.*

Proof. Let $\mathcal{I}$ be the ideal of $\mathcal{O}$ given by Corollary 4.2. If $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}$ by Remark 4.3. Then there exists a free $\mathcal{M}$-sublattice Y of ${}^{\mathcal{M}}X$ such that $[{}^{\mathcal{M}}X : Y]_{\mathcal{O}}$ divides $\mathcal{I}$. Let $\varepsilon_1, \dots, \varepsilon_n$ be a free $\mathcal{M}$-basis of Y, so that $Y = \mathcal{M}\varepsilon_1 \oplus \cdots \oplus \mathcal{M}\varepsilon_n$, and let $Z = \Lambda\varepsilon_1 \oplus \cdots \oplus \Lambda\varepsilon_n$. Then $Z \subseteq Y \subseteq {}^{\mathcal{M}}X \subseteq X$ and $[X : Z]_{\mathcal{O}} = [X : {}^{\mathcal{M}}X]_{\mathcal{O}} \cdot [{}^{\mathcal{M}}X : Y]_{\mathcal{O}} \cdot [Y : Z]_{\mathcal{O}}$. Note that $[Y : Z]_{\mathcal{O}} = [\mathcal{M} : \Lambda]_{\mathcal{O}}^{n}$. Moreover, Corollary 3.3 implies that $[X : {}^{\mathcal{M}}X]_{\mathcal{O}}$ divides $[\mathcal{M} : J]_{\mathcal{O}}^{n}$, and under the assumption that A is commutative, Theorem 3.6 implies that in fact $[X : {}^{\mathcal{M}}X]_{\mathcal{O}}$ divides $[\mathcal{M} : \Lambda]_{\mathcal{O}}^{n}$. Therefore we obtain the desired result. □

Remark 4.6. The statement of Theorem 4.5 extends to Λ-lattices X admitting a surjection $A^{(n)} \twoheadrightarrow KX$ of A-modules. More specifically, the ideal $\mathcal{I}$ has the following property: given any Λ-lattice X admitting a surjection $A^{(n)} \twoheadrightarrow KX$ of A-modules, there exists a Λ-sublattice Z of X generated by at most n elements such that $[X : Z]_{\mathcal{O}}$ divides $\mathcal{I} \cdot [\mathcal{M} : J]_{\mathcal{O}}^{n} \cdot [\mathcal{M} : \Lambda]_{\mathcal{O}}^{n}$. This can be seen as follows. There exists an A-module B such that $KX \oplus B \cong A^{(n)}$. Thus given any full Λ-lattice W in B, the Λ-lattice $X \oplus W$ satisfies the conditions of Theorem 4.5 and so admits a free Λ-sublattice Z' of index dividing $\mathcal{I} \cdot [\mathcal{M} : J]_{\mathcal{O}}^{n} \cdot [\mathcal{M} : \Lambda]_{\mathcal{O}}^{n}$, and the image of Z' under the projection $X \oplus W \twoheadrightarrow X$ is the desired sublattice Z. Of course, one should expect stronger bounds if one specifies the isomorphism class of KX; one such situation is considered in §6.

5. Group rings

5.1. Conductors of group rings

The extra structure of group rings is exploited in the following result, which will allow us to make an optimal choice of the two-sided ideal J that appears in the statement of Theorem 4.5.

Proposition 5.1. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K \neq \mathcal{O}$. Let G be a finite group and let Γ be an $\mathcal{O}$-order in $K[G]$ containing $\mathcal{O}[G]$. Then $\mathcal{O}[G]^{\Gamma} = {}^{\Gamma}\mathcal{O}[G]$ and we have*

$$[\Gamma : \mathcal{O}[G]]_{\mathcal{O}} = [\mathcal{O}[G] : {}^{\Gamma}\mathcal{O}[G]]_{\mathcal{O}} = [\Gamma : {}^{\Gamma}\mathcal{O}[G]]_{\mathcal{O}}^{\frac{1}{2}}. \tag{5.1}$$

Moreover, if $|G|$ is invertible in K and $\Gamma = \mathcal{M}$ is a maximal $\mathcal{O}$-order, then this index is independent of the choice of $\mathcal{M}$.

Remark 5.2. In the case that $|G|$ is invertible in K and $\Gamma = \mathcal{M}$ is a maximal $\mathcal{O}$-order, Jacobinski has given an explicit description of $\mathcal{O}[G]^\Gamma = {}^\Gamma\mathcal{O}[G]$ (see Theorem 5.5) and this leads to an explicit formula for the index of (5.1) (see Corollary 5.6).

Proof of Proposition 5.1. Given an $\mathcal{O}$-order Λ in $K[G]$, let Λ^{op} denote the $\mathcal{O}$-order defined by the image of Λ under the involution on $K[G]$ induced by $g \mapsto g^{-1}$. Any left (resp. right) Λ-lattice carries a canonical structure of a right (resp. left) Λ^{op}-lattice with g^{-1} acting as g did previously. Given a left (resp. right) Λ-lattice X, we denote by X^* the dual lattice $X^\vee = \mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O})$ considered as a left (resp. right) Λ^{op}-lattice. Note that for a left Λ-lattice X, we have $[(X^\vee)\Lambda : X^\vee]_{\mathcal{O}} = [\Lambda X^* : X^*]_{\mathcal{O}}$, etc.

Now observe that Γ^{op} is an $\mathcal{O}$-order containing $\mathcal{O}[G] = \mathcal{O}[G]^{\mathrm{op}}$. Hence $\Gamma^{\mathrm{op}}\mathcal{O}[G] = \Gamma^{\mathrm{op}} = \mathcal{O}[G]\Gamma^{\mathrm{op}}$. We also have that

$$(\Gamma^{\mathrm{op}}\mathcal{O}[G])^\vee = (\mathcal{O}[G]^\vee)^{\Gamma^{\mathrm{op}}} = {}^\Gamma(\mathcal{O}[G]^*),$$
$$(\mathcal{O}[G]\Gamma^{\mathrm{op}})^\vee = {}^{\Gamma^{\mathrm{op}}}(\mathcal{O}[G]^\vee) = (\mathcal{O}[G]^*)^\Gamma,$$

where in each case the first equality follows from Lemma 3.5 and the second equality follows from the definition of $(-)^*$. Therefore ${}^\Gamma(\mathcal{O}[G]^*) = (\mathcal{O}[G]^*)^\Gamma$. Furthermore, there is an $\mathcal{O}[G] = \mathcal{O}[G]^{\mathrm{op}}$-isomorphism $\mathcal{O}[G]^* \xrightarrow{\sim} \mathcal{O}[G]$ given by $\mathbb{1}_g \mapsto g$, where $\mathbb{1}_g$ denotes the element of $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[G], \mathcal{O})$ defined by $h \mapsto 0$ for $h \neq g$ and $g \mapsto 1$. Hence we conclude that ${}^\Gamma\mathcal{O}[G] = \mathcal{O}[G]^\Gamma$.

We have that $[\Gamma : \mathcal{O}[G]]_{\mathcal{O}} = [\Gamma^{\mathrm{op}} : \mathcal{O}[G]^{\mathrm{op}}]_{\mathcal{O}}$ since $(-)^{\mathrm{op}}$ is an $\mathcal{O}$-linear isomorphism. As $\mathcal{O}[G] = \mathcal{O}[G]^{\mathrm{op}}$, we then have

$$\begin{aligned}
[\Gamma : \mathcal{O}[G]]_{\mathcal{O}} &= [\Gamma^{\mathrm{op}} : \mathcal{O}[G]]_{\mathcal{O}} \\
&= [(\mathcal{O}[G])^\vee : ((\mathcal{O}[G])^\vee)^{\Gamma^{\mathrm{op}}}]_{\mathcal{O}} \\
&= [\mathcal{O}[G]^* : {}^\Gamma((\mathcal{O}[G])^*)]_{\mathcal{O}} \\
&= [\mathcal{O}[G] : {}^\Gamma\mathcal{O}[G]]_{\mathcal{O}},
\end{aligned}$$

where the second equality follows from Lemma 3.5(i). Since

$$[\Gamma : {}^\Gamma\mathcal{O}[G]]_{\mathcal{O}} = [\Gamma : \mathcal{O}[G]]_{\mathcal{O}} \cdot [\mathcal{O}[G] : {}^\Gamma\mathcal{O}[G]]_{\mathcal{O}},$$

the second equality of (5.1) follows.

For the last statement, note that the hypotheses ensure that $K[G]$ is separable and hence maximal orders exist (see §2.5). For any $\mathcal{O}$-order Λ in $K[G]$, let $\mathrm{Disc}(\Lambda)$ denote the discriminant of Λ with respect to the reduced trace map $\mathrm{tr} : K[G] \to K$. Then $\mathrm{Disc}(\mathcal{M})$ is independent of the choice of maximal $\mathcal{O}$-order $\mathcal{M}$ of $K[G]$ by [46, (25.3)]. Moreover,

by [11, (26.3)(iii)] we have $\mathrm{Disc}(\mathcal{O}[G]) = [\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}}^2 \cdot \mathrm{Disc}(\mathcal{M})$, and so $[\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}}$ is independent of the choice of $\mathcal{M}$. □

5.2. The main theorem for group rings

We now obtain a more precise version of Theorem 4.5 for lattices over group rings.

Theorem 5.3. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Assume that K is a global field and that $\mathcal{O} \neq K$. Let G be a finite group such that $|G|$ is invertible in K. Set $s = 2$ if G is abelian and $s = 3$ otherwise. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in $K[G]$ containing $\mathcal{O}[G]$. Let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}$. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any $\mathcal{O}[G]$-lattice X such that KX is free of rank n over $K[G]$, there exists a free $\mathcal{O}[G]$-sublattice Z of X such that $[X : Z]_{\mathcal{O}}$ divides $\mathcal{I} \cdot [\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}}^{sn}$. Moreover, if $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}$.*

Remark 5.4. In the case $\mathcal{O} = \mathbb{Z}$, explicit conditions on G under which $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2 are given in Proposition 5.11 and Corollary 5.13.

Proof of Theorem 5.3. We apply Theorem 4.5 with $\Lambda = \mathcal{O}[G]$. If G is abelian, then the desired result follows directly. Otherwise, by Proposition 5.1 we can and do take $J = \mathcal{O}[G]^{\mathcal{M}} = {}^{\mathcal{M}}\mathcal{O}[G]$, and we have $[\mathcal{M} : J]_{\mathcal{O}}^n \cdot [\mathcal{M} : \Lambda]_{\mathcal{O}}^n = [\mathcal{M} : \Lambda]_{\mathcal{O}}^{3n}$. □

5.3. Jacobinski's formula and the index of a group ring in a maximal order

For further details on the following setup and notation, we refer the reader to [11, §27] and the references therein.

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K \neq \mathcal{O}$. Let G be a finite group such that $|G|$ is invertible in K. Then $K[G]$ is a separable finite-dimensional K-algebra. We may write $K[G] = A_1 \times \cdots \times A_t$, where each A_i is a simple K-algebra. For each i, let K_i denote the centre of A_i. Then each K_i is a finite separable field extension of K, and there exist integers $n_1, \ldots, n_t$ such that $\dim_{K_i} A_i = n_i^2$ for each i. Let tr_i denote the reduced trace from A_i to K (see [11, §7D]). Then $\mathrm{tr}_i = T_{K_i/K} \circ \mathrm{tr}_{A_i/K_i}$, where $T_{K_i/K}$ is the ordinary trace from K_i to K, and tr_{A_i/K_i} is the reduced trace from A_i to K_i.

Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order such that $\mathcal{O}[G] \subseteq \mathcal{M} \subseteq K[G]$. For each i, let $\mathcal{M}_i = \mathcal{M} \cap A_i$, let $\mathcal{O}_i$ denote the integral closure of $\mathcal{O}$ in K_i, and define the *inverse different* of $\mathcal{M}_i$ with respect to tr_i to be $\mathcal{D}_i^{-1} = \{x \in A_i : \mathrm{tr}_i(x\mathcal{M}_i) \subseteq \mathcal{O}\}$. Then $\mathcal{M} = \mathcal{M}_1 \times \cdots \times \mathcal{M}_t$ and each $\mathcal{D}_i^{-1}$ is a two-sided $\mathcal{M}_i$-lattice containing $\mathcal{M}_i$.

Theorem 5.5 *(Jacobinski [23]). In the notation above, we have*

$$ {}^{\mathcal{M}}\mathcal{O}[G] = \mathcal{O}[G]^{\mathcal{M}} = \bigoplus_{i=1}^{t} |G| n_i^{-1} \mathcal{D}_i^{-1}. $$

A less explicit version of the following result is given in [13, Proposition 3.6].

Corollary 5.6. *In the notation above, we have*

$$[\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}} = [\mathcal{O}[G] : {}^{\mathcal{M}}\mathcal{O}[G]]_{\mathcal{O}} = \left(|G|^{|G|} \prod_{i=1}^{t} \left(n_i^{[K_i:K]n_i^2} [\mathcal{D}_i^{-1} : \mathcal{M}_i]_{\mathcal{O}} \right)^{-1} \right)^{\frac{1}{2}},$$

and this index is independent of the choice of $\mathcal{M}$.

Proof. By Theorem 5.5 we have

$$\begin{aligned}
[\mathcal{M} : {}^{\mathcal{M}}\mathcal{O}[G]]_{\mathcal{O}} &= \prod_{i=1}^{t} [\mathcal{M}_i : (|G| n_i^{-1} \mathcal{D}_i^{-1})]_{\mathcal{O}} \\
&= \prod_{i=1}^{t} (|G| n_i^{-1})^{\dim_K A_i} [\mathcal{M}_i : \mathcal{D}_i^{-1}]_{\mathcal{O}} \\
&= |G|^{|G|} \prod_{i=1}^{t} (n_i^{[K_i:K]n_i^2} [\mathcal{D}_i^{-1} : \mathcal{M}_i]_{\mathcal{O}})^{-1},
\end{aligned}$$

where in the last equality we have used that $\dim_K A_i = [K_i : K] n_i^2$ for each i and that $\prod_{i=1}^{t} \dim_K A_i = |G|$. The desired result now follows from Proposition 5.1. □

Corollary 5.7. *In the notation above, if $A_i \cong \mathrm{Mat}_{n_i}(K)$ for $i = 1, \ldots, t$, then*

$$[\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}} = [\mathcal{O}[G] : {}^{\mathcal{M}}\mathcal{O}[G]]_{\mathcal{O}} = \left(|G|^{|G|} \prod_{i=1}^{t} n_i^{-n_i^2} \right)^{\frac{1}{2}}.$$

Proof. The hypotheses imply that $K_i = K$ and $\mathcal{D}_i^{-1} = \mathcal{M}_i$ for $i = 1, \ldots, t$. Thus the desired result follows from Corollary 5.6. □

A result similar to the following is given in [13, p. 173, (11)].

Corollary 5.8. *In the notation above, if G is abelian, then*

$$[\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}} = [\mathcal{O}[G] : {}^{\mathcal{M}}\mathcal{O}[G]]_{\mathcal{O}} = \left(|G|^{|G|} \prod_{i=1}^{t} (\Delta_{K_i/K})^{-1} \right)^{\frac{1}{2}},$$

where $\Delta_{K_i/K}$ denotes the discriminant of $\mathcal{O}_i$ with respect to $\mathcal{O}$.

Proof. Since A is commutative, for every i we have $n_i = 1$, $A_i = K_i$, and $\mathcal{M}_i = \mathcal{O}_i$. Thus the reduced trace tr_i coincides with the ordinary trace $T_{K_i/K}$ and so

$$\mathcal{D}_i^{-1} = \{x \in K_i : T_{K_i/K}(x\mathcal{O}_i) \subseteq \mathcal{O}\}$$

is the usual inverse different of $\mathcal{O}_i$ with respect to $\mathcal{O}$. Moreover,

$$[\mathcal{D}_i^{-1} : \mathcal{M}_i]_{\mathcal{O}} = [\mathcal{D}_i^{-1} : \mathcal{O}_i]_{\mathcal{O}} = [\mathcal{O}_i : \mathcal{D}_i]_{\mathcal{O}} = \mathrm{Norm}_{K_i/K}(\mathcal{D}_i) = \Delta_{K_i/K},$$

where for the third equality, it suffices to first localise and then consider the determinant of the K-linear endomorphism of K_i given by multiplication by a generator of $\mathcal{D}_i$. Therefore the desired result now follows from Corollary 5.6. □

We now make the last result completely explicit in the case $K = \mathbb{Q}$.

Proposition 5.9. *Let G be a finite abelian group and let e denote its exponent. Let $\mathcal{M}$ be the unique maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. Then*

$$[\mathcal{M} : \mathbb{Z}[G]] = \left(|G|^{|G|} \prod_{d|e} \left(d^{-\phi(d)} \prod_{p|d} p^{\frac{\phi(d)}{p-1}} \right)^{t_d} \right)^{\frac{1}{2}},$$

where t_d denotes the number of cyclic subgroups of G of order d and $\phi(-)$ denotes the Euler totient function.

Proof. By [1, Theorem 2], we have $\mathbb{Q}[G] \cong \prod_{d|e} \mathbb{Q}(\zeta_d)^{(t_d)}$, where $\mathbb{Q}(\zeta_d)^{(t_d)}$ denotes the direct product of t_d copies of $\mathbb{Q}(\zeta_d)$ (see also [45]). Moreover,

$$\Delta^{-1}_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} = \left(d^{-\phi(d)} \prod_{p|d} p^{\frac{\phi(d)}{p-1}} \right) \mathbb{Z}$$

by [54, Proposition 2.7]. Therefore the desired result now follows from a straightforward calculation and Corollary 5.8 in the case $K = \mathbb{Q}$. □

The following special case is equivalent to [55, Lemma 5.2], which was proven using different methods.

Corollary 5.10. *Let p be a prime, let k be a positive integer, and let G be the cyclic group of order p^k. Let $\mathcal{M}$ be the unique maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. Then*

$$[\mathcal{M} : \mathbb{Z}[G]] = p^{1+p+\cdots+p^{k-1}}.$$

5.4. The case of group rings over the integers

Let $\mathbb{H}$ denote the quaternion division algebra over $\mathbb{R}$. For a finite group G, let $\mathrm{Irr}_{\mathbb{C}}(G)$ denote the set of complex irreducible characters of G. Recall that $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ is said to

be an *irreducible symplectic character* if it is real-valued and the corresponding factor of $\mathbb{R}[G]$ is isomorphic to the ring of $k \times k$ matrices over $\mathbb{H}$, for some positive integer k. For each $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$, let $\mathbb{Q}(\chi)$ denote the field generated by the values of χ, and let $C(\chi)$ be the narrow class group of $\mathbb{Q}(\chi)$ if χ is symplectic, and the usual ideal class group of $\mathbb{Q}(\chi)$ otherwise.

The following result is well-known to experts, but the authors were unable to locate it in this precise form in the literature.

Proposition 5.11. *Let G be a finite group and let $\mathcal{M}$ be a maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. Suppose that no factor of $\mathbb{R}[G]$ is isomorphic to the quaternions $\mathbb{H}$. Then $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2 if and only if $C(\chi)$ is trivial for each $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$.*

Proof. The hypothesis on $\mathbb{R}[G]$ ensures that $\mathbb{Q}[G]$ satisfies the Eichler condition relative to $\mathbb{Z}$ (see [12, §51A]). Hence Jacobinski's cancellation theorem [12, (51.24)] implies that every $\mathbb{Z}$-order in $\mathbb{Q}[G]$, in particular $\mathcal{M}$, has the locally free cancellation property. Now write $\mathbb{Q}[G] = A_1 \times \cdots \times A_t$, where each A_i is a simple $\mathbb{Q}$-algebra. For each i, let K_i denote the centre of A_i and let $\mathcal{M}_i = A_i \cap \mathcal{M}$. Then $\mathcal{M} = \mathcal{M}_1 \times \cdots \times \mathcal{M}_t$ and $\mathrm{Cl}(\mathcal{M}) \cong \mathrm{Cl}(\mathcal{M}_1) \oplus \cdots \oplus \mathrm{Cl}(\mathcal{M}_t)$. Each K_i is isomorphic to $\mathbb{Q}(\chi)$ for some $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ and by [12, (49.32)] $\mathrm{Cl}(\mathcal{M}_i)$ is isomorphic to $C(\chi)$. Therefore we obtain the 'if' direction of the desired equivalence. The 'only if' direction now follows from the fact that $\{K_i : 1 \leq i \leq t\} = \{\mathbb{Q}(\chi) : \chi \in \mathrm{Irr}_{\mathbb{C}}(G)\}$. □

Remark 5.12. The hypothesis in Proposition 5.11 that no factor of $\mathbb{R}[G]$ is isomorphic to the quaternions $\mathbb{H}$ can be weakened to the requirement that $\mathcal{M}$ has the locally free cancellation property (or the stably free cancellation property). Maximal $\mathbb{Z}$-orders with the locally free cancellation property in $\mathbb{Q}[G]$ for G a binary polyhedral group have been classified in [51, Theorem II]. For example, for $2 \leq n \leq 5$ every maximal $\mathbb{Z}$-order in $\mathbb{Q}[Q_{4n}]$ satisfies the equivalent conditions of Lemma 2.2, where Q_{4n} denotes the generalised quaternion group of order $4n$. See also Remark 2.3.

Corollary 5.13. *Let G be a finite abelian group and let e denote its exponent. Define*

$$\Sigma = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25,$$
$$26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 40, 42, 44, 45, 48, 50, 54, 60, 66, 70, 84, 90\}$$

and let $\mathcal{M}$ be the unique maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. Then $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2 if and only if $e \in \Sigma$.

Proof. First write $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ for positive integers $k, n_1, \ldots, n_k$ such that $n_i \mid n_{i+1}$ for $1 \leq i \leq k-1$. Then $e = n_k$ and $\{\mathbb{Q}(\chi) : \chi \in \mathrm{Irr}_{\mathbb{C}}(G)\} = \{\mathbb{Q}(\zeta_d) : d \mid e\}$. Since $\mathbb{Z}[\zeta_d]$ is the ring of integers of $\mathbb{Q}(\zeta_d)$, this implies that

$$\{C(\chi) : \chi \in \mathrm{Irr}_{\mathbb{C}}(G)\} = \{\mathrm{Cl}(\mathbb{Z}[\zeta_d]) : d \mid e\}.$$

The set Σ is precisely the set positive integers n for which $\mathrm{Cl}(\mathbb{Z}[\zeta_n]) = 0$ by [35]; see also [54, Theorem 11.1] (note that we include choices of n such that $n \equiv 2 \bmod 4$). It can easily be checked that Σ is also precisely the set of choices of e for which $\mathrm{Cl}(\mathbb{Z}[\zeta_d]) = 0$ for all $d \mid e$. Since no factor of $\mathbb{Q}[G]$ is isomorphic to the quaternions $\mathbb{H}$, the desired result now follows from Proposition 5.11. □

Remark 5.14. The hypotheses of Proposition 5.11 and Corollary 5.13 are much weaker than $\mathrm{Cl}(\mathbb{Z}[G])$ itself being trivial. If G is a finite abelian group, then a result of Ph. Cassou-Noguès [10] shows that $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial if and only if either $G \cong C_2 \times C_2$ or $G \cong C_n$ where $1 \leq n \leq 11$ or $n \in \{13, 14, 17, 19\}$. If G is a finite non-abelian non-dihedral group, then a result of Endô and Hironaka [15] shows that $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial if and only if $G \cong A_4$, S_4 or A_5 (the if direction was already shown by Reiner and Ullom [47]). For partial results in the dihedral case, see [16].

Many specialisations of Theorem 5.3 can now be obtained by applying the results of §5.3, Proposition 5.11 and/or Corollary 5.13; the following is just one such example.

Theorem 5.15. *Let G be a finite group and suppose that there exist positive integers $t, n_1, \ldots, n_t$ such that $\mathbb{Q}[G] \cong \prod_{i=1}^{t} \mathrm{Mat}_{n_i}(\mathbb{Q})$. If X is an $\mathbb{Z}[G]$-lattice such that $\mathbb{Q}X$ is free of rank n over $\mathbb{Q}[G]$, then there exists a free $\mathbb{Z}[G]$-sublattice Z of X such that $[X : Z]$ divides*

$$\left(|G|^{|G|}\prod_{i=1}^{t} n_i^{-n_i^2}\right)^{\frac{3n}{2}}.$$

Proof. Proposition 5.11 implies that any maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$ satisfies the equivalent conditions of Lemma 2.2. Thus the result follows from Theorem 5.3 and Corollary 5.7. □

Remark 5.16. The collection of finite groups G satisfying the hypothesis of Theorem 5.15 is closed under direct products and includes symmetric groups and hyperoctahedral groups (e.g. the dihedral group of order 8). See [49] and [24] for more on this topic.

6. Group rings modulo trace

Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K \neq \mathcal{O}$. Let G be a finite group such that $|G|$ is invertible in K and let $\mathrm{Tr}_G = \sum_{g \in G} g$. Then both $K[G]$ and its quotient $K[G]/(\mathrm{Tr}_G)$ are separable finite-dimensional K-algebras. The purpose of this section is to consider lattices over the $\mathcal{O}$-order $\mathcal{O}[G]/(\mathrm{Tr}_G)$.

Let $e = 1 - |G|^{-1}\mathrm{Tr}_G$, which is a central idempotent of $K[G]$. Let $\pi_e : K[G] \to eK[G]$ be the projection map associated to e. Given a subset $X \subseteq K[G]$, let $X_e = \pi_e(X)$ and let $X^{1-e} = X \cap \ker(\pi_e)$. In particular, $K[G]_e = eK[G] \cong K[G]/(\mathrm{Tr}_G)$ and $K[G]^{1-e} = \mathrm{Tr}_G K$.

Let $\Lambda = \mathcal{O}[G]$ and let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in $K[G]$ containing Λ. Then $\mathcal{M}_e = e\mathcal{M}$ is a maximal $\mathcal{O}$-order of $K[G]_e$ containing Λ_e. By Proposition 5.1, ${}^{\mathcal{M}}\Lambda$ is a two-sided ideal of $\mathcal{M}$ contained in Λ. Hence $({}^{\mathcal{M}}\Lambda)_e$ is a choice of two-sided ideal of $\mathcal{M}_e$ contained in Λ_e. This is not necessarily the largest such choice, but its form allows us to make use of our previous computations.

Lemma 6.1. *We have* $[\mathcal{M}_e : \Lambda_e]_{\mathcal{O}} = |G|^{-1}[\mathcal{M} : \Lambda]_{\mathcal{O}}$ *and* $[\Lambda_e : ({}^{\mathcal{M}}\Lambda)_e]_{\mathcal{O}} = [\mathcal{M} : \Lambda]_{\mathcal{O}}$.

Proof. Consider the following diagram of $\mathcal{O}$-lattices with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda^{1-e} & \longrightarrow & \Lambda & \longrightarrow & \Lambda_e & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{M}^{1-e} & \longrightarrow & \mathcal{M} & \longrightarrow & \mathcal{M}_e & \longrightarrow & 0. \end{array}$$

Then by Lemma 2.1 we have $[\mathcal{M} : \Lambda]_{\mathcal{O}} = [\mathcal{M}^{1-e} : \Lambda^{1-e}]_{\mathcal{O}} \cdot [\mathcal{M}_e : \Lambda_e]_{\mathcal{O}}$. Note that $\mathcal{M}^{1-e} = \left(|G|^{-1}\mathrm{Tr}_G\right) \cdot \mathcal{O}$ and $\Lambda^{1-e} = \mathcal{M}^{1-e} \cap \Lambda = \mathrm{Tr}_G \cdot \mathcal{O}$. Hence $[\mathcal{M}^{1-e} : \Lambda^{1-e}]_{\mathcal{O}} = |G|$, and so we obtain the first equality.

Similarly, we also have the following diagram of $\mathcal{O}$-lattices with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & ({}^{\mathcal{M}}\Lambda)^{1-e} & \longrightarrow & {}^{\mathcal{M}}\Lambda & \longrightarrow & ({}^{\mathcal{M}}\Lambda)_e & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Lambda^{1-e} & \longrightarrow & \Lambda & \longrightarrow & \Lambda_e & \longrightarrow & 0. \end{array} \tag{6.1}$$

Then by Lemma 2.1 we have $[\Lambda : {}^{\mathcal{M}}\Lambda]_{\mathcal{O}} = [\Lambda^{1-e} : ({}^{\mathcal{M}}\Lambda)^{1-e}]_{\mathcal{O}} \cdot [\Lambda_e : ({}^{\mathcal{M}}\Lambda)_e]_{\mathcal{O}}$. By maximality of ${}^{\mathcal{M}}\Lambda$, the subset $({}^{\mathcal{M}}\Lambda)^{1-e}$ is the largest $\mathcal{M}^{1-e}$-sublattice contained in Λ^{1-e}. Since $\mathcal{M}^{1-e} \cong \mathcal{O}$, we find that Λ^{1-e}, an $\mathcal{O}$-lattice, is already a $\mathcal{M}^{1-e}$-sublattice so that the left vertical map of (6.1) is an equality. Hence we have $[\Lambda_e : ({}^{\mathcal{M}}\Lambda)_e]_{\mathcal{O}} = [\Lambda : {}^{\mathcal{M}}\Lambda]_{\mathcal{O}}$. But $[\Lambda : {}^{\mathcal{M}}\Lambda]_{\mathcal{O}} = [\mathcal{M} : \Lambda]_{\mathcal{O}}$ by Proposition 5.1, and thus we obtain the desired result. □

Theorem 6.2. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Assume that K is a global field and that $\mathcal{O} \neq K$. Let G be a finite group such that $|G|$ is invertible in K. Set $s = 2$ if G is abelian and $s = 3$ otherwise. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in $K[G]$ containing $\mathcal{O}[G]$. Let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}$. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any $\mathcal{O}[G]/(\mathrm{Tr}_G)$-lattice X such that KX is free of rank n over $K[G]/(\mathrm{Tr}_G)$, there exists a free $\mathcal{O}[G]/(\mathrm{Tr}_G)$-sublattice Z of X such that $[X : Z]_{\mathcal{O}}$ divides $\mathcal{I} \cdot |G|^{-2n} \cdot [\mathcal{M} : \mathcal{O}[G]]_{\mathcal{O}}^{sn}$. Moreover, if $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}$.*

Proof. Let $\Lambda = \mathcal{O}[G]$. Then $\mathcal{M}_e$ is a maximal $\mathcal{O}$-order of $K[G]_e$ containing $\Lambda_e = \mathcal{O}[G]/(\mathrm{Tr}_G)$. Note that if $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then so

does $\mathcal{M}_e$. By Lemma 6.1 we have $[\mathcal{M}_e : \Lambda_e]_{\mathcal{O}} = |G|^{-1}[\mathcal{M} : \Lambda]_{\mathcal{O}}$. By Proposition 5.1, $J := ({}^{\mathcal{M}}\Lambda)_e$ is a two-sided ideal of $\mathcal{M}_e$ contained in Λ_e. Then we have

$$[\mathcal{M}_e : \Lambda_e]_{\mathcal{O}} \cdot [\mathcal{M}_e : J]_{\mathcal{O}} = [\mathcal{M}_e : \Lambda_e]^2_{\mathcal{O}} \cdot [\Lambda_e : J]_{\mathcal{O}} = |G|^{-2} \cdot [\mathcal{M} : \Lambda]^3_{\mathcal{O}}.$$

Therefore we obtain the desired result by applying Theorem 4.5 for the $\mathcal{O}$-order Λ_e, the maximal $\mathcal{O}$-order $\mathcal{M}_e$ and the ideal J. □

7. Application: approximation of normal integral bases

We refer the reader to [19] for an overview of normal integral bases, on which there is a vast literature. In this section, we consider examples of applications of the algebraic machinery of previous sections to the approximation of normal integral bases.

Beyond the base field and the isomorphism type of the Galois group, the following result does not use any arithmetic information about the Galois extensions concerned.

Theorem 7.1. *Let K be a number field and let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}_K$. Let G be a finite group and let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in $K[G]$ containing $\mathcal{O}_K[G]$. Set $s = 2$ if G is abelian and $s = 3$ otherwise. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}_K$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$, there exists $\alpha \in \mathcal{O}_L$ such that $[\mathcal{O}_L : \mathcal{O}_K[\mathrm{Gal}(L/K)] \cdot \alpha]_{\mathcal{O}}$ divides $\mathcal{I} \cdot [\mathcal{M} : \mathcal{O}_K[G]]^s_{\mathcal{O}_K}$. Moreover, if $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}_K$.*

Proof. The normal basis theorem says that for a finite Galois extension of fields L/K we have $L \cong K[\mathrm{Gal}(L/K)]$ as $K[\mathrm{Gal}(L/K)]$-modules. Therefore the desired result now follows easily from Theorem 5.3 with $n = 1$ and $\mathcal{O} = \mathcal{O}_K$. □

Remark 7.2. An explicit formula for $[\mathcal{M} : \mathcal{O}_K[G]]_{\mathcal{O}_K}$ is given in Corollary 5.6. In particular, a weak but general bound is that $[\mathcal{M} : \mathcal{O}_K[G]]^s_{\mathcal{O}_K}$ divides $|G|^{\lceil s|G|/2 \rceil}$.

By making the further assumption that the extensions concerned are at most tamely ramified, we obtain the following result with a stronger conclusion.

Theorem 7.3. *Let K be a number field, let $\mathcal{K}$ be any nonzero ideal of $\mathcal{O}_K$, and G be a finite group. Then there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}_K$, that can be chosen to be coprime to $\mathcal{K}$, with the following property: given any at most tamely ramified Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$, there exists $\alpha \in \mathcal{O}_L$ such that $[\mathcal{O}_L : \mathcal{O}_K[\mathrm{Gal}(L/K)] \cdot \alpha]_{\mathcal{O}_K}$ divides $\mathcal{I}$. Moreover, if $\mathcal{O}_K[G]$ satisfies the equivalent conditions of Lemma 2.2, then we can take $\mathcal{I} = \mathcal{O}_K$.*

Proof. For an at most tamely ramified Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$, we have that $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-lattice of rank 1 by [19, Chapter I, §3, Corollary 2],

for example. Therefore the desired result now follows easily from Proposition 4.1 with $\mathcal{O} = \mathcal{O}_K$ and $\Gamma = \mathcal{O}_K[G]$. □

Remark 7.4. Improved bounds can be obtained in special cases. For example, if G is a finite group with no irreducible symplectic characters (e.g. G is abelian or of odd order), then every (at most) tamely ramified Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ has a normal integral basis by a special case of Taylor's proof [53] of a conjecture of Fröhlich (see [19, §I] for an overview). Moreover, if G is a finite abelian group, then Leopoldt's theorem [26] (see also [27]) implies that for every Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$, there exists $\alpha \in \mathcal{O}_L$ such that $[\mathcal{O}_L : \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})] \cdot \alpha]$ divides $[\mathcal{M} : \mathbb{Z}[G]]$, where $\mathcal{M}$ is the unique maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. By contrast, Theorems 7.1 and 7.3 are very general and their short proofs use little or no arithmetic information about the particular field extensions concerned.

8. Application: approximation of strong Minkowski units

In this section, we consider examples of applications of the algebraic machinery of previous sections to the approximation of strong Minkowski units.

Definition 8.1. Let L/K be a Galois extension of number fields and let $G = \mathrm{Gal}(L/K)$. Let μ_L denote the roots of unity of L. An element $\varepsilon \in \mathcal{O}_L^\times/\mu_L$ is said to be

(i) a *Minkowski unit* of L/K if $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathcal{O}_L^\times/\mu_L) = \mathbb{Q}[G] \cdot \varepsilon$,
(ii) a *strong Minkowski unit* of L/K if $\mathcal{O}_L^\times/\mu_L = \mathbb{Z}[G] \cdot \varepsilon$.

The following result is well known.

Lemma 8.2. *Let L/K be a Galois extension of number fields and let $G = \mathrm{Gal}(L/K)$. If K is equal to either $\mathbb{Q}$ or an imaginary quadratic field then L/K has a Minkowski unit. Moreover, if either L is totally real or K is imaginary quadratic, then $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathcal{O}_L^\times/\mu_L) \cong \mathbb{Q}[G]/(\mathrm{Tr}_G)$ as $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-modules (and as $\mathbb{Q}[G]$-modules).*

Proof. By definition, L/K has a Minkowski unit if and only if $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times$ is cyclic as a $\mathbb{Q}[G]$-module. By a theorem of Herbrand (see [52, Chapter I, §4.3], for example) there is an isomorphism $(\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_L^\times) \oplus \mathbb{Q} \cong \mathbb{Q}[S_\infty]$ of $\mathbb{Q}[G]$-modules, where S_∞ denotes the set of infinite places of L. So the existence of a Minkowski unit is implied by $\mathbb{Q}[S_\infty]$ being cyclic as a $\mathbb{Q}[G]$-module, which is equivalent to S_∞ being transitive as a G-set. This occurs precisely when K has a unique infinite place. If either L is totally real or K is imaginary quadratic, then the unique infinite place of K splits completely in L/K and thus $\mathbb{Q}[S_\infty] \cong \mathbb{Q}[G]$ as $\mathbb{Q}[G]$-modules. □

Remark 8.3. The existence of strong Minkowski units (which some authors refer to as Minkowski units) in special cases has been studied in numerous articles, including [44,36,

7,14,37–39,6,28,29,20,9,40,31–33], as well as [43, §3.3 & §3.5.1] and the references therein. Also see the articles cited below.

Remark 8.4. If $L/\mathbb{Q}$ is a Galois extension with $[L:\mathbb{Q}]$ odd, then L is totally real and $\mathcal{O}_L^\times/\mu_L \cong \{u \in \mathcal{O}_L^\times : \mathrm{Norm}_{L/\mathbb{Q}}(u) = 1\}$ as $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$-lattices.

The following result is a strong refinement and generalisation of [30, Theorem 1], [2, Proposition 5.2] and [3, Theorem 3.3], which only consider finite cyclic or abelian totally real extensions of $\mathbb{Q}$ and do not actually bound the index in question.

Theorem 8.5. *Let G be a finite group and let k be a positive integer. Set $s = 2$ if G is abelian and $s = 3$ otherwise. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any finite Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$ and K equal to either $\mathbb{Q}$ or an imaginary quadratic field, there exists a Minkowski unit $\varepsilon \in \mathcal{O}_L^\times/\mu_L$ such that $[\mathcal{O}_L^\times/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/K)] \cdot \varepsilon]$ divides $i \cdot |G|^{-2}[\mathcal{M} : \mathbb{Z}[G]]^s$, where $\mathcal{M}$ is a maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$.*

Remark 8.6. An explicit formula for $[\mathcal{M} : \mathbb{Z}[G]]$ is given in Corollary 5.6. In particular, a weak but general bound is that $|G|^{-2}[\mathcal{M} : \mathbb{Z}[G]]^s$ divides $|G|^{\lceil s|G|/2\rceil - 2}$.

Remark 8.7. It is interesting to compare Theorem 8.5 with [4, Theorem 1.1], which in the case that $L/\mathbb{Q}$ is a finite Galois extension asserts the existence of a Minkowski unit ε such that the index $[\mathcal{O}_L^\times/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})] \cdot \varepsilon]$ is bounded by an expression involving the Weil height of ε, the regulator of L, the degree $[L:\mathbb{Q}]$ and $\mathrm{rank}_{\mathbb{Z}}\mathcal{O}_L^\times$.

Proof of Theorem 8.5. Let $\Gamma = \mathbb{Z}[G]/(\mathrm{Tr}_G)$. By Theorem 6.2 there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any Γ-lattice X such that $\mathbb{Q}X \cong \mathbb{Q}[G]/(\mathrm{Tr}_G)$ as $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-modules, there exists a free Γ-sublattice Y of X such that $[X : Y]$ divides $i \cdot |G|^{-2}[\mathcal{M} : \mathbb{Z}[G]]^s$. Note that if $\varepsilon \in X$ is a free Γ-generator of Y, then $Y = \Gamma \cdot \varepsilon = \mathbb{Z}[G] \cdot \varepsilon$. For L/K with either L totally real or K imaginary quadratic, the desired result now follows from Lemma 8.2 after fixing an isomorphism $\mathrm{Gal}(L/K) \cong G$. For L/K with L totally imaginary and $K = \mathbb{Q}$, the result follows from Lemma 8.2 and Remark 4.6. □

Corollary 8.8. *Let G be a finite group and let $\mathcal{M}$ be a maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$. Suppose that $\mathcal{M}$ satisfies the equivalent conditions of Lemma 2.2 (see §5.4 for conditions on G under which this holds). Set $s = 2$ if G is abelian and $s = 3$ otherwise. Then given any finite Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$ and K equal to either $\mathbb{Q}$ or an imaginary quadratic field, there exists a Minkowski unit $\varepsilon \in \mathcal{O}_L^\times/\mu_L$ such that $[\mathcal{O}_L^\times/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/K)] \cdot \varepsilon]$ divides $|G|^{-2}[\mathcal{M} : \mathbb{Z}[G]]^s$.*

Proof. Under the hypotheses on $\mathcal{M}$, the desired result follows as in the proof of Theorem 8.5 after noting that we can take $i = 1$ in the application of Theorem 6.2. □

Remark 8.9. Let $L/\mathbb{Q}$ be a finite Galois extension such that L is CM and let L^+ denote its maximal totally real subfield. Let $\varepsilon \in \mathcal{O}_{L^+}^\times/\{\pm 1\}$ be a Minkowski unit of $L^+/\mathbb{Q}$ and by abuse of notation let this also denote its image in $\mathcal{O}_L^\times/\mu_L$. By [54, Theorem 4.12] we have that $[\mathcal{O}_L^\times : \mu_L\mathcal{O}_{L^+}^\times] = 1$ or 2, and so $[\mathcal{O}_L^\times/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]\cdot\varepsilon]$ divides $2[\mathcal{O}_{L^+}^\times/\{\pm 1\} : \mathbb{Z}[\mathrm{Gal}(L^+/\mathbb{Q})]\cdot\varepsilon]$. Thus ε is also a Minkowski unit of $L/\mathbb{Q}$, and we obtain stronger analogues of Theorem 8.5 and Corollary 8.8 in this situation.

The above results can be strengthened for extensions of prime degree.

Theorem 8.10. *Let p be an odd prime and let k be a positive integer. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any cyclic field extension L/K with $[L : K] = p$ and K equal to either $\mathbb{Q}$ or an imaginary quadratic field, there exists a Minkowski unit $\varepsilon \in \mathcal{O}_L^\times/\mu_L$ such that $[\mathcal{O}_L^\times/\mu_L : \mathbb{Z}[\mathrm{Gal}(L/K)]\cdot\varepsilon]$ divides i.*

Proof. Let G be the cyclic group of order p and let $\mathcal{M} = \mathbb{Z}[G]/(\mathrm{Tr}_G)$. Then $\mathcal{M} \cong \mathbb{Z}[\zeta_p]$, which is a maximal $\mathbb{Z}$-order. By Corollary 4.2 there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any $\mathcal{M}$-lattice X such that $\mathbb{Q}X$ is free of rank 1 as a $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-module, there exists a free $\mathcal{M}$-sublattice Y of X such that $[X : Y]$ divides i. Note that if $\varepsilon \in X$ is a free $\mathcal{M}$-generator of Y, then $Y = \mathcal{M}\cdot\varepsilon = \mathbb{Z}[G]\cdot\varepsilon$. The desired result now follows from Lemma 8.2 since the hypotheses ensure that either L is totally real or K is imaginary quadratic. □

The following result is not new, as it is the combination of [56] (see also [8, Corollary]) and an easy consequence of [22, Théorèm]; we include it for completeness.

Corollary 8.11. *Let p be a prime such that $3 \leq p \leq 19$. Then every cyclic field extension L/K with $[L : K] = p$ and K equal to either $\mathbb{Q}$ or an imaginary quadratic field has a strong Minkowski unit.*

Proof. In the proof of Theorem 8.10, adding the hypothesis that $p \leq 19$ implies that $\mathcal{M} \cong \mathbb{Z}[\zeta_p]$ has trivial class group and so satisfies the equivalent conditions of Lemma 2.2. Hence we can take $i = 1$ by Remark 4.3, and this implies the desired result. □

Remark 8.12. It is interesting to compare Theorem 8.10 to (i) [8, Theorem] when $K = \mathbb{Q}$ and (ii) [22, Théorèm] when K is imaginary quadratic. Result (i) considers cyclic extensions $L/\mathbb{Q}$ of odd prime degree p and gives sufficient conditions on ideals of $\mathbb{Z}[\zeta_p]$ of norm equal to the class number h_L of $\mathcal{O}_L$ for both the existence and non-existence of a strong Minkowski unit of $L/\mathbb{Q}$. The proof uses the fact that $\mathcal{O}_L^\times/\{\pm 1\}$ contains a free $\mathbb{Z}[\zeta_p]$-submodule of index h_L generated by a cyclotomic unit. Result (ii) is analogous and uses elliptic units. By contrast, the proof and statement of Theorem 8.10 do not depend on the particular extension L/K.

9. Application: rational points on abelian varieties

In this section, we consider examples of applications of the algebraic machinery of previous sections to the Galois module structure of rational points of abelian varieties. By the Mordell–Weil theorem, for every abelian variety A over a number field K, the group $A(K)/A(K)_{\mathrm{tors}}$ is a free $\mathbb{Z}$-module of finite rank. If L/K is a Galois extension of number fields, then $A(L)/A(L)_{\mathrm{tors}}$ is a $\mathbb{Z}[\mathrm{Gal}(L/K)]$-lattice, so is amenable to study via our methods.

Theorem 9.1. *Let G be a finite group and let k be a positive integer. Set $s = 2$ if G is abelian and $s = 3$ otherwise. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any Galois extension of number fields L/K with $\mathrm{Gal}(L/K) \cong G$, and any abelian variety A/K such that $\mathbb{Q} \otimes_{\mathbb{Z}} A(L)$ is cyclic as a $\mathbb{Q}[G]$-module, there exists $\varepsilon \in A(L)/A(L)_{\mathrm{tors}}$ such that $[A(L)/A(L)_{\mathrm{tors}} : \mathbb{Z}[G] \cdot \varepsilon]$ is finite and divides $i \cdot [\mathcal{M} : \mathbb{Z}[G]]^s$, where $\mathcal{M}$ is any maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$.*

Remark 9.2. An explicit formula for $[\mathcal{M} : \mathbb{Z}[G]]$ is given in Corollary 5.6. In particular, a weak but general bound is that $[\mathcal{M} : \mathbb{Z}[G]]^s$ divides $|G|^{\lceil s|G|/2 \rceil}$.

Remark 9.3. Let G be a finite group. The isomorphism class of a finite-dimensional $\mathbb{Q}[G]$-module V is entirely determined by the values of $\dim_{\mathbb{Q}} V^H$ as H runs over a set of representatives of the set of cyclic subgroups of G up to conjugacy (see [48, §13.1, Corollary to Theorem 30′]). In particular, V is free of rank 1 if and only if $\dim_{\mathbb{Q}} V^H = [G : H]$ for all cyclic subgroups H of G up to conjugacy.

Proof of Theorem 9.1. By Theorem 5.3, there exists a positive integer i, which can be chosen to be coprime to n, with the following property: given any $\mathbb{Z}[G]$-lattice X such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free of rank 1 as a $\mathbb{Q}[G]$-module, there exists a free $\mathbb{Z}[G]$-sublattice Y of X such that $[X : Y]$ divides $i \cdot [\mathcal{M} : \mathbb{Z}[G]]^s$. By Remark 4.6, i also has the property that given any $\mathbb{Z}[G]$-lattice X such that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is cyclic as a $\mathbb{Q}[G]$-module, there exists a cyclic $\mathbb{Z}[G]$-sublattice Y of X such that $[X : Y]$ divides $i \cdot [\mathcal{M} : \mathbb{Z}[G]]^s$. In particular, this holds for $X = A(L)/A(L)_{\mathrm{tors}}$ after fixing an isomorphism $G \cong \mathrm{Gal}(L/K)$. □

Theorem 9.4. *Let p be an odd prime and let k be a positive integer. Then there exists a positive integer i, which can be chosen to be coprime to k, with the following property: given any cyclic extension L/K of number fields with $[L : K] = p$ and any abelian variety A/K such that $\mathrm{rank}_{\mathbb{Z}} A(K) = 0$ and $\mathrm{rank}_{\mathbb{Z}} A(L) = p - 1$, there exists $\varepsilon \in A(L)/A(L)_{\mathrm{tors}}$ such that $[A(L)/A(L)_{\mathrm{tors}} : \mathbb{Z}[\mathrm{Gal}(L/K)] \cdot \varepsilon]$ is finite and divides i.*

Proof. Let G be the cyclic group of order p and let $\mathcal{M} = \mathbb{Z}[G]/(\mathrm{Tr}_G)$. Then $\mathcal{M} \cong \mathbb{Z}[\zeta_p]$, which is a maximal $\mathbb{Z}$-order. By Corollary 4.2 there exists a positive integer i, which can be chosen to be coprime to n, with the following property: given any $\mathcal{M}$-lattice X such

that $\mathbb{Q}X \cong \mathbb{Q}[G]/(\mathrm{Tr}_G)$ as $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-modules, there exists a free $\mathcal{M}$-sublattice Y of X such that $[X : Y]$ divides i. After fixing an isomorphism $G \cong \mathrm{Gal}(L/K)$, the desired result now follows since the rank hypotheses ensure that $\mathbb{Q} \otimes_{\mathbb{Z}} (A(L)/A(L)_{\mathrm{tors}}) \cong \mathbb{Q}[G]/(\mathrm{Tr}_G)$ as $\mathbb{Q}[G]$-modules (see Remark 9.3) and hence as $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-modules. □

Remark 9.5. Note that for $\mathbb{Q} \otimes_{\mathbb{Z}} (A(L)/A(L)_{\mathrm{tors}})$ to be cyclic as a $\mathbb{Q}[G]/(\mathrm{Tr}_G)$-module, it is necessary that $\mathrm{rank}_{\mathbb{Z}} A(L) = 0$ or $p - 1$.

Corollary 9.6. *Let p be a prime such that $3 \leq p \leq 19$. Then given any cyclic extension of number fields L/K with $[L : K] = p$ and any abelian variety A/K such that $\mathrm{rank}_{\mathbb{Z}} A(K) = 0$ and $\mathrm{rank}_{\mathbb{Z}} A(L) = p - 1$, there exists $\varepsilon \in A(L)/A(L)_{\mathrm{tors}}$ such that $A(L)/A(L)_{\mathrm{tors}} = \mathbb{Z}[\mathrm{Gal}(L/K)] \cdot \varepsilon$.*

Proof. In the proof of Theorem 9.4, the additional hypothesis that $p \leq 19$ implies that $\mathcal{M} \cong \mathbb{Z}[\zeta_p]$ has trivial class group and so satisfies the equivalent conditions of Lemma 2.2. Hence we can take $i = 1$ by Remark 4.3, and this implies the desired result. □

Theorem 9.7. *Let p be a prime, let F be an imaginary quadratic field with discriminant coprime to p, and let $\mathcal{K}$ be a nonzero ideal of $\mathcal{O}_F$. Then there exists an ideal $\mathcal{I}$ of $\mathcal{O}_F$, which can be chosen to be coprime to $\mathcal{K}$, with the following property: given any cyclic extension of number fields L/K with $[L : K] = p$ and such that K contains F, and any elliptic curve E/K with complex multiplication by $\mathcal{O}_F$ and with $\mathrm{rank}_{\mathbb{Z}} E(K) = 0$ and $\mathrm{rank}_{\mathbb{Z}} E(L) = 2(p-1)$, there exists $\varepsilon \in E(L)/E(L)_{\mathrm{tors}}$ such that $[E(L)/E(L)_{\mathrm{tors}} : \mathcal{O}_F[\mathrm{Gal}(L/K)] \cdot \varepsilon]_{\mathcal{O}_F}$ divides $\mathcal{I}$.*

Proof. Let G be the cyclic group of order p. The discriminant of $\mathbb{Z}[\zeta_p]$ is a power of p and in particular is coprime to the discriminant of $\mathcal{O}_F$. Hence $\mathbb{Q}(\zeta_p)$ and F are linearly disjoint over $\mathbb{Q}$. Moreover, by [25, III, §3, Proposition 17] we have $\mathcal{O}_F[\zeta_p] = \mathcal{O}_{F(\zeta_p)}$. Thus $\mathcal{O}_F[G]/(\mathrm{Tr}_G) \cong \mathcal{O}_F[\zeta_p]$ is a maximal $\mathcal{O}_F$-order. By Corollary 4.2 there exists a nonzero ideal $\mathcal{I}$ of $\mathcal{O}_F$, which can be chosen to be coprime to $\mathcal{K}$, with the following property: given any $\mathcal{O}_F[G]/(\mathrm{Tr}_G)$-lattice X such that $F \otimes_{\mathcal{O}_F} X \cong F[G]/(\mathrm{Tr}_G)$ as $F[G]/(\mathrm{Tr}_G)$-modules, there exists a free $\mathcal{O}_F[G]/(\mathrm{Tr}_G)$-sublattice Y of X such that $[X : Y]_{\mathcal{O}_F}$ divides $\mathcal{I}$.

Let E, L and K be as in the theorem and fix an isomorphism $G \cong \mathrm{Gal}(L/K)$. By assumption, E has CM by $\mathcal{O}_F$ defined over K. The commuting Galois action and action by endomorphisms then give $E(L)/E(L)_{\mathrm{tors}}$ the structure of an $\mathcal{O}_F[G]$-lattice. Moreover, as $\mathrm{rk}_{\mathbb{Z}} E(K) = 0$, it is in fact a $\mathcal{O}_F[G]/(\mathrm{Tr}_G)$-lattice and since $\mathrm{rank}_{\mathbb{Z}} E(L) = 2(p-1)$, we have that $\dim_{\mathbb{Q}} F \otimes_{\mathcal{O}_F} (E(L)/E(L)_{\mathrm{tors}}) = 2(p-1)$. Since F and $\mathbb{Q}(\zeta_p)$ are linearly disjoint, the unique $F[G]/(\mathrm{Tr}_G)$-module with these properties is $F[G]/(\mathrm{Tr}_G)$ itself. Therefore $E(L)/E(L)_{\mathrm{tors}}$ is an example of an $\mathcal{O}_F[G]/(\mathrm{Tr}_G)$-lattice such that $F \otimes_{\mathcal{O}_F} X \cong F[G]/(\mathrm{Tr}_G)$. □

Remark 9.8. Since $\mathbb{Q}(\zeta_p)$ and F are linearly disjoint over $\mathbb{Q}$, the $F[G]/(\mathrm{Tr}_G)$-module $F \otimes_{\mathcal{O}_F} (E(L)/E(L)_{\mathrm{tors}})$ is cyclic if and only if either $\mathrm{rank}_{\mathbb{Z}} E(L) = 0$ or $2(p-1)$.

Corollary 9.9. *Let p be a prime, let F be an imaginary quadratic field with discriminant coprime to p such that $\mathcal{O}_{F(\zeta_p)}$ has trivial class group. Then for every cyclic extension of number fields L/K such that K contains F and $[L:K]=p$, and for every elliptic curve E/K with complex multiplication by $\mathcal{O}$ and with $\operatorname{rank}_{\mathbb{Z}} E(K) = 0$ and $\operatorname{rank}_{\mathbb{Z}} E(L) = 2(p-1)$, we have that $E(L)/E(L)_{\mathrm{tors}}$ is free as an $\mathcal{O}_F[G]/(\mathrm{Tr}_G)$-module.*

Proof. In the proof of Theorem 9.7, the additional hypothesis that $\mathcal{O}_{F(\zeta_p)}$ has trivial class group ensures that $\mathcal{O}_F/(\mathrm{Tr}_G) \cong \mathcal{O}_{F(\zeta_p)}$ satisfies the equivalent conditions of Lemma 2.2. Hence we can take $\mathcal{I} = \mathcal{O}_F$ by Remark 4.3, and this implies the desired result. □

Data availability

No data was used for the research described in the article.

References

[1] R.G. Ayoub, C. Ayoub, On the group ring of a finite abelian group, Bull. Aust. Math. Soc. 1 (1969) 245–261. MR 252526.
[2] T. All, On p-adic annihilators of real ideal classes, J. Number Theory 133 (7) (2013) 2324–2338. MR 3035966.
[3] T. All, On the p-adic completion of the units of a real abelian number field, J. Number Theory 136 (2014) 1–21. MR 3145320.
[4] S. Akhtari, J.D. Vaaler, Minkowski's theorem on independent conjugate units, Eur. J. Math. 3 (1) (2017) 111–149. MR 3610268.
[5] D.W. Ballew, Numerical invariants and projective modules, J. Algebra 17 (1971) 555–574. MR 274497.
[6] L. Bouvier, J.-J. Payan, Modules sur certains anneaux de Dedekind. Application à la structure du groupe des classes et à l'existence d'unités de Minkowski, J. Reine Angew. Math. 274/275 (1975) 278–286, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. MR 0374084.
[7] L. Bouvier, J.-J. Payan, Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p, p), Ann. Inst. Fourier (Grenoble) 29 (1) (1979) 171–187. MR 526783.
[8] A. Brumer, On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Jpn. 21 (1969) 357–358. MR 0244193.
[9] D. Burns, On the Galois structure of units in number fields, Proc. Lond. Math. Soc. (3) 66 (1) (1993) 71–91. MR 1189093.
[10] Ph. Cassou-Noguès, Classes d'idéaux de l'algèbre d'un groupe abélien, Université de Bordeaux, Talence, 1972, Thèse présentée à l'Université de Bordeaux I, Talence, pour l'obtention du titre de Docteur en Mathématiques (mention: Mathématiques Pures). MR 0340393.
[11] C.W. Curtis, I. Reiner, Methods of Representation Theory. Vol. I, Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 632548 (82i:20001).
[12] C.W. Curtis, I. Reiner, Methods of Representation Theory. Vol. II, Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 892316 (88f:20002).
[13] I. Del Corso, F. Ferri, D. Lombardo, How far is an extension of p-adic fields from having a normal integral basis?, J. Number Theory 233 (2022) 158–197. MR 4356849.
[14] D. Duval, Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type (p, p), J. Number Theory 13 (2) (1981) 228–245. MR 612684.
[15] S. Endô, Y. Hironaka, Finite groups with trivial class groups, J. Math. Soc. Jpn. 31 (1) (1979) 161–174. MR 519042.
[16] S. Endô, T. Miyata, On the class groups of dihedral groups, J. Algebra 63 (2) (1980) 548–573. MR 570730.

[17] A. Fröhlich, Invariants for modules over commutative separable orders, Quart. J. Math. Oxford Ser. (2) 16 (1965) 193–232. MR 0210697.
[18] A. Fröhlich, Local fields, in: Algebraic Number Theory, Proc. Instructional Conf., Brighton, 1965, Academic Press, London, 1967, pp. 1–41. MR 236145.
[19] A. Fröhlich, Galois Module Structure of Algebraic Integers, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), vol. 1, Springer-Verlag, Berlin, 1983. MR 717033.
[20] A. Fröhlich, Units in real abelian fields, J. Reine Angew. Math. 429 (1992) 191–217. MR 1173123.
[21] A. Fröhlich, M.J. Taylor, Algebraic Number Theory, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934.
[22] R. Gillard, Unités elliptiques et unités de Minkowski, J. Math. Soc. Jpn. 32 (4) (1980) 697–701. MR 589107.
[23] H. Jacobinski, On extensions of lattices, Mich. Math. J. 13 (1966) 471–475. MR 204538.
[24] D. Kletzing, Structure and Representations of **Q**-Groups, Lecture Notes in Mathematics, vol. 1084, Springer-Verlag, Berlin, 1984. MR 765700.
[25] S. Lang, Algebraic Number Theory, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723.
[26] H.W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math. 201 (1959) 119–149. MR 108479.
[27] G. Lettl, The ring of integers of an abelian number field, J. Reine Angew. Math. 404 (1990) 162–170. MR 1037435.
[28] R. Marszałek, Minkowski units in certain metacyclic fields, Acta Arith. 51 (4) (1988) 381–391. MR 971088.
[29] R. Marszałek, Minkowski units in a class of metabelian fields, J. Number Theory 37 (1) (1991) 67–91. MR 1089790.
[30] F. Marko, On the existence of p-units and Minkowski units in totally real cyclic fields, Abh. Math. Semin. Univ. Hamb. 66 (1996) 89–111. MR 1418221.
[31] F. Marko, On the existence of Minkowski units in totally real cyclic fields, J. Théor. Nr. Bordx. 17 (1) (2005) 195–206. MR 2152220.
[32] R. Marszałek, Units in real abelian fields, Acta Arith. 146 (2) (2011) 115–151. MR 2747023.
[33] R. Marszałek, Units in real cyclic fields, Funct. Approx. Comment. Math. 45 (2011) 139–153. MR 2865419.
[34] D. Masser, Multiplicative isogeny estimates, J. Aust. Math. Soc. Ser. A 64 (2) (1998) 178–194. MR 1619802.
[35] J.M. Masley, H.L. Montgomery, Cyclotomic fields with unique factorization, J. Reine Angew. Math. 286 (287) (1976) 248–256. MR 429824.
[36] N. Moser, Unités et nombre de classes d'une extensions dièdrale de **Q**, Astérisque 24–25 (1975) 29–35. MR 0376610.
[37] N. Moser, Sur les unités d'une extension galoisienne non abélienne de degré pq du corps des rationnels, p et q nombres premiers impairs, Ann. Inst. Fourier (Grenoble) 29 (1) (1979) 137–158. MR 526781.
[38] N. Moser, Unités et nombre de classes d'une extension galoisienne diédrale de **Q**, Abh. Math. Semin. Univ. Hamb. 48 (1979) 54–75. MR 537446.
[39] N. Moser, Théorème de densité de Tchebotareff et monogénéité de modules sur l'algèbre d'un groupe métacyclique, Acta Arith. 42 (3) (1983) 311–323. MR 729740.
[40] M. Mazur, S.V. Ullom, Galois module structure of units in real biquadratic number fields, Acta Arith. 111 (2) (2004) 105–124. MR 2039416.
[41] D.W. Masser, G. Wüstholz, Factorization estimates for abelian varieties, Publ. Math. Inst. Hautes Études Sci. (81) (1995) 5–24. MR 1361754.
[42] D.W. Masser, G. Wüstholz, Refinements of the Tate conjecture for abelian varieties, in: Abelian Varieties, Egloffstein, 1993, de Gruyter, Berlin, 1995, pp. 211–223. MR 1336608.
[43] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004. MR 2078267.
[44] J.-J. Payan, Sur les unités de Minkowski, in: Séminaire Delange-Pisot-Poitou (15e année: 1973/74), Théorie des nombres, Fasc. 1, Exp. No. 19, 1975, p. 6. MR 0404203.
[45] S. Perlis, G.L. Walker, Abelian group algebras of finite order, Trans. Am. Math. Soc. 68 (1950) 420–426. MR 34758.
[46] I. Reiner, Maximal Orders, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, With a foreword by M.J. Taylor. MR 1972204.

[47] I. Reiner, S. Ullom, Remarks on class groups of integral group rings, in: Symposia Mathematica, Vol. XIII, Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972, Academic Press, London, 1974, pp. 501–516. MR 0367043.
[48] J.-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York-Heidelberg, 1977, Translated from the second French edition by Leonard L. Scott. MR 0450380.
[49] L. Solomon, Rational characters and permutation characters, in: Symposia Mathematica, Vol. XIII, Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972, Academic Press, London, 1974, pp. 453–466. MR 0357573.
[50] D. Smertnig, J. Voight, Definite orders with locally free cancellation, Trans. Lond. Math. Soc. 6 (1) (2019) 53–86. MR 4105795.
[51] R.G. Swan, Projective modules over binary polyhedral groups, J. Reine Angew. Math. 342 (1983) 66–172. MR 703486.
[52] J. Tate, Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$, in: Dominique Bernardi, Norbert Schappacher (Eds.), Lecture Notes, in: Progress in Mathematics, vol. 47, Birkhäuser Boston, Inc., Boston, MA, 1984. MR 782485.
[53] M.J. Taylor, On Fröhlich's conjecture for rings of integers of tame extensions, Invent. Math. 63 (1) (1981) 41–79. MR 608528.
[54] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575.
[55] C. Wittmann, Zeta functions of integral representations of cyclic p-groups, J. Algebra 274 (1) (2004) 271–308. MR 2040875.
[56] B.A. Zeĭnalov, The Units of a Cyclic Real Field, Dagestan State Univ. Collection Sci. Papers, Math. Phys., Dagestan. Kniž. Izdat., Makhachkala, 1965, pp. 21–23 (Russian). MR 0217045.