NORM RELATIONS AND COMPUTATIONAL PROBLEMS IN NUMBER FIELDS

JEAN-FRANÇOIS BIASSE, CLAUS FIEKER, TOMMY HOFMANN, AND AUREL PAGE

Abstract. For a finite group G, we introduce a generalization of norm relations in the group algebra $\mathbb{Q}[G]$. We give necessary and sufficient criteria for the existence of such relations and apply them to obtain relations between the arithmetic invariants of the subfields of a normal extension of algebraic number fields with Galois group G. On the algorithmic side this leads to subfield based algorithms for computing rings of integers, S-unit groups and class groups. For the S-unit group computation this yields a polynomial time reduction to the corresponding problem in subfields. We compute class groups of large number fields under GRH, and new unconditional values of class numbers of cyclotomic fields.

1. Introduction

Let K/F be a normal extension of number fields with Galois group G. Since the beginning of algebraic number theory, the interaction and relations between the arithmetic invariants of K and its subfields has always been an important topic. For example it was already observed by Dirichlet [20], and later generalized by Walter [52], that for biquadratic fields, that is, $F = \mathbb{Q}$ and $G = C_2 \times C_2$, the class numbers of K and its three nontrivial subfields K_1, K_2, K_3 satisfy the class number formula $h(K) = 2^i \cdot h(K_1)h(K_2)h(K_3)$, where $i \in \mathbb{Z}$ depends on the index of certain unit groups. Thus, once the class numbers of the subfields are known, one can compute the class number of K up to a power of 2.

In the 1950s, Brauer [16] and Kuroda [32] laid the foundation for a systematic study of such class number formulae by connecting them to character theoretic properties of G. More precisely, for a subgroup $H \leq G$ we denote by $\operatorname{Ind}_{G/H}(\mathbf{1}_H)$ the permutation character of G induced by the trivial character of H. For a relation of the form $\sum_{H \leq G} a_H \operatorname{Ind}_{G/H}(\mathbf{1}_H) = 0$ with $a_H \in \mathbb{Z}$, Brauer proved a corresponding relation between zeta functions and arithmetic invariants of the fixed fields K^H (see also [23, Theorem 73]). In connection with class number formulae, the existence of such relations has also been studied from a computational point of view by Bosma and de Smit [15].

A related, more group theoretic notion, is that of a relation of norms of subgroups. For a subgroup $H \leq G$ denote by $N_H = \sum_{h \in H} h \in \mathbb{Q}[G]$ the corresponding norm as an element of the rational group algebra. Then one considers equalities of

Date: April 2, 2025.

2010 *Mathematics Subject Classification.* Primary: 11Y16, 20C05, 11R32; Secondary 11R29, 11R04, 11Y40, 11R18, 11R27.

the form

$$0 = \sum_{H \leq G} a_H N_H \tag{1}$$

in $\mathbb{Q}[G]$ with $a_H \in \mathbb{Z}$. On the number theoretic side this implies, and is equivalent to, $1 = \prod_{H \leq G} \mathrm{N}_{K/K^H}(x)^{a_H}$ for all $x \in K^\times$ (see [3]). The correspondence between relations of characters and norms was already observed by Walter [52], who used them to derive a simple proof of Kuroda's class number formula. A group theoretic study of the lattice of relations between norms was done by Rehm [46]. Under the name idempotent relation, various arithmetic and geometric applications have been given by Kani–Rosen, Park and Yu in [28, 29, 42, 43, 56]. A connection with Arakelov class groups was described by Kontogeorgis in [31].

Although relations between permutation characters and norms have played a significant role in connecting invariants of K and its subfields, both notions have not seen a systematic use in computational algebraic number theory, for example, in the computation of the class group. Until recently, the use of subfields in algorithmic number theory had been restricted to ad-hoc tricks and heuristic observations. Recent work of Bauch, Bernstein, de Valence, Lange and van Vredendaal [10] describes how to reduce the computation of principal ideal generators in multiquadratic fields (that is, $G = C_2^n$) to quadratic subfields, thus for the first time improving (both in theory and practice) upon classical algorithms by exploiting subfields. This was then generalized to the computation of S-units by Biasse and van Vredendaal [13] and to multicubic fields (that is, $G = C_3^n$) by Lesavourey, Plantard and Susilo [35].

The aim of the present paper is to extend these ideas to a larger range of computational problems and to classify those groups G where these improvements apply. To this end, we consider relations of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i \tag{2}$$

in $\mathbb{Q}[G]$ with $d \in \mathbb{Z}_{>0}$, $H_i \leq G$ nontrivial and $a_i, b_i \in \mathbb{Z}[G]$. We refer to those relations as *norm relations*. They generalize the classical relations (1) where the coefficient of the trivial group is nonzero, which are exactly the relations one needs to determine invariants of K from those of its subfields. Although our systematic treatment is new, these norm relations have been used in an ad-hoc way for $G = C_2 \times C_2$ by Wada [50], Bauch, Bernstein, de Valence, Lange and van Vredendaal [10] and Biasse and van Vredendaal [13], and for $G = C_3 \times C_3$ by Parry [44] and Lesavourey, Plantard and Susilo [35]. We give a systematic study of these relations; we link them to fixed point free unitary representations and, from a theorem of Wolf's [55, 51], we obtain the following classification of groups admitting a norm relation (see Theorem 2.11). Interestingly, the relevant condition is exactly the same in the problem coming from geometry and topology (existence of space-forms) as in ours, but the good and bad cases are reversed, as the groups that do not admit a norm relation are exactly the ones that provide an example of a space-form.

Theorem A. The group G admits a norm relation if and only if G contains a non-cyclic subgroup of order pq, where p and q are primes, or a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ where $p = 2^{2^k} + 1$ is a Fermat prime with $k > 1$.

The existence of a norm relation yields the following connection between the class group of K and that of its subfields (see Proposition 3.7). For a subgroup $H \leq G$

and M a $\mathbb{Z}[G]$-module we denote by $M^H = \{m \in M \mid hm = m \text{ for all } h \in H\}$ the fixed points of H in M.

Proposition B. Let G be a finite group that admits a norm relation (2), and let K/F be a Galois extension of number fields with Galois group G. Then the group $\mathrm{Cl}(K) \otimes \mathbb{Z}[1/d]$ is isomorphic to a direct summand of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \otimes \mathbb{Z}[1/d]$, and the group $\mathrm{Cl}(K)/\mathrm{Cl}(K)[d]$ is isomorphic to a subgroup of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i})$.

Compared with Brauer–Kuroda type relations [16, 32, 6, 7] and Mackey functor type relations [14], ours is less precise in that it bounds the class group or the class number without pinning it down exactly, but it is also partly stronger in that norm relations are more frequent than Brauer relations and because it is independent of the coefficients of the relation.

Our algorithmic use of norm relations to leverage information on K from its subfields uses the following simple but crucial statement (see Proposition 3.1).

Proposition C. Let M be a $\mathbb{Z}[G]$-module, and assume we have a norm relation (2). Then the quotient

$$M/(a_1 M^{H_1} + \cdots + a_\ell M^{H_\ell})$$

has exponent dividing d.

In particular, if M is finitely generated, we can use the modules M^{H_i} of fixed points to approximate M by a finite index subgroup, whose index divides a power of d. We show how to leverage this result in the following classical problems from computational algebraic number theory (see Section 4):

(1) computation of the ring of integers $\mathcal{O}_K$,
(2) computation of S-unit groups $\mathcal{O}_{K,S}^\times$,
(3) computation of the class group $\mathrm{Cl}(K)$.

Note that these problems, in particular (2) and (3), are at the core of many algorithmic questions in algebraic number theory and arithmetic geometry, as well as cryptographic applications. We implemented our algorithms for the general case in Hecke [21] and a special algorithm for the abelian case in Pari/GP [49]. Using both implementations, we computed class groups of number fields that are out of reach of other current techniques. For example, consider the normal closure of $x^{10} + x^8 - 4x^2 + 4$, which is a $C_2 \times A_5$ extension of $\mathbb{Q}$ of degree 120 and discriminant $\approx 10^{161}$. Using the first implementation we show that assuming the generalized Riemann hypothesis (GRH) the class number is 1. This computation takes only 6 hours on a single core machine (see Example 5.1). Using the second implementation we determine under GRH the structure of the class group of the cyclotomic field $K = \mathbb{Q}(\zeta_{6552})$ of degree 1728 and discriminant $\approx 10^{5258}$, and in particular we obtain that $h_{6552}^+ = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13$. This computation takes only 4 hours on a single core machine (see Example 5.3).

Our methods are also useful for unconditional determination of class groups. As an example, we certify some new values of class numbers of cyclotomic fields (Theorem 4.29).

Theorem D. The class numbers and class groups in Tables 1 and 2 are correct.

In order to keep the table small, we did not include fields for which the class number was already known unconditionally. We also determined the class group structure of many examples for which the class number was known [37], but it is

Table 1. Class numbers of cyclotomic fields $\mathbb{Q}(\zeta_n)$

n conductor, $\varphi(n)$ degree, h^+ plus part of class number, r_2 2-rank of class group, r_3 3-rank of class group, T_1 time for the conditional computation, T_2 time to unconditionally certify the computation.

n	$\varphi(n)$	h^+	r_2	r_3	T_1	T_2	n	$\varphi(n)$	h^+	r_2	r_3	T_1	T_2
255	128	1	1	1	1 min	3 h	624	192	1	3	4	2.5 min	28 min
272	128	2	4	2	1 min	8 h	720	192	1	3	4	2.5 min	24 min
320	128	1	0	2	25 s	13 h	780	192	1	18	1	6.5 min	6.5 min
340	128	1	3	0	1 min	8 h	840	192	1	6	4	6 min	2 min
408	128	2	5	2	3 min	21 min	455	288	1	14	3	4 min	9 h
480	128	1	3	4	43 s	4 s	585	288	1	7	4	4 min	10.5 h
273	144	1	9	2	34 s	5.5 min	728	288	20	17	14	3 min	2 h
315	144	1	4	2	20 s	4.5 min	936	288	16	11	11	2.5 min	2.5 h
364	144	1	6	5	25 s	11 min	1008	288	16	13	10	2.5 min	5.5 h
456	144	1	1	3	1.5 min	8 h	1092	288	1	24	7	3 min	1 h
468	144	1	3	6	25 s	12 min	1260	288	1	14	7	2.5 min	2 h
504	144	4	9	6	16 s	2 s	1560	384	8	40	5	2 h	3.5 h
520	192	4	18	3	6.5 min	16 min	1680	384	1	12	8	1 h	8 h
560	192	1	3	5	2.5 min	18 min	2520	576	208	38	15	40 min	43 h

likely that the class group structure could be determined by other methods, for instance [2] or by constructing explicit class fields, so we did not include them. According to Miller [37], the largest conductor for which the class number of a cyclotomic field has been computed unconditionally was 420 prior to our work; we raise this record to 2520. Note that our methods are not restricted to cyclotomic fields, but these number fields provide a family of examples to which they often apply and that are of general interest. Our proof of Theorem D does not use special properties of cyclotomic fields other than their Galois group; it would be interesting to combine them with special cyclotomic techniques.

On the theoretical side, assuming GRH we exhibit a polynomial time reduction to proper subfields in the presence of a norm relation (Theorem 4.18).

Theorem E. Assume GRH holds. Let G be a finite group and $\mathcal{H}$ a set of subgroups of G. Assume that there exists a norm relation as in (2) where all H_i belong to $\mathcal{H}$. There exists a deterministic polynomial time algorithm that, on input of

- a number field K,
- an injection $G \to \mathrm{Aut}(K)$,
- a finite G-stable set S of prime ideals of K,
- for each H in $\mathcal{H}$, a basis of the group of S-units of the subfield fixed by H,

returns a $\mathbb{Z}$-basis of the group of S-units of K.

The proof uses an effective version of the Grunwald–Wang theorem under GRH, which is different from other versions found in the literature (for instance [53]) and may be of independent interest (Theorem 4.11), and a bound on the smallest possible value of d in norm relations (Theorem 2.20). We also provide an easily checked criterion for the existence of a norm relation (Proposition 2.10), and a complete classification of optimal norm relations in the abelian case (Theorem 2.28).

In view of the previous theorems, one might ask to which extent norm relations exhaust all possibilities to exploit subfields to compute S-units. We partially answer this by proving the following converse (see Proposition 3.6).

Proposition F. Let K/F be a finite normal extension of number fields with Galois group G, and let $\mathcal{H}$ be a set of nontrivial subgroups of G. Let S be a finite G-stable set of prime ideals of K. Assume that at least one of the following holds:

- F is not totally real,
- there is a real place of F that splits completely in K, or
- there is a prime ideal $\mathfrak{p}$ of F that splits completely in K and such that the primes above $\mathfrak{p}$ are in S.

If the $\mathbb{Z}[G]$-submodule of $\mathcal{O}_{K,S}^{\times}$ generated by the $\mathcal{O}_{K^H,S}^{\times}$ for $H \in \mathcal{H}$ has finite index, then G admits a norm relation with respect to $\mathcal{H}$.

Note that when using a set S that is guaranteed to generate the class group of K by analytic bounds, the third condition of the proposition is usually satisfied.

The paper is structured as follows. In Section 2 we recall the definitions of the classical Brauer relations and relations between norms and introduce our notion of norm relations. We then go on to prove the necessary and sufficient conditions for the existence of these relations. We also investigate arithmetic properties of such relations, which play an important role in the number theoretic applications. We describe these applications in Section 3, where we also explain the consequences of the existence of a norm relation for the invariants of number fields. We then exploit these properties from an algorithmic point of view in Section 4. Finally, in Section 5 we give various examples of computations of class groups of abelian and non-abelian number fields.

Acknowledgment. J.-F. Biasse was supported by National Science Foundation grant 183980, National Science Foundation grant 1846166, National Institute of Standards and Technology grant 60NANB17D184, CyberFlorida Collaborative Seed Grant Program and CyberFlorida Capacity Building Program. C. Fieker was supported by Deutsche Forschungsgemeinschaft — Project-ID 286237555 – TRR 195, Project-ID 460135501 - NFDI 29/1 “MaRDI – Mathematische Forschungsdateninitiative” and the state of Rheinland-Pfalz via the Forschungsinitiative and the “SymbTools” project. T. Hofmann was supported by Deutsche Forschungsgemeinschaft — Project-ID 286237555 – TRR 195; and Project-ID 539387714. A. Page was supported by the ANR grant Ciao ANR-19-CE48-0008. He would like to thank K. Belabas and B. Allombert for improving some Pari/GP functionalities that were useful for this project and for sharing insight on classical computational problems in number fields, A. Bartel for rich discussions about representation theory, and P. Kirchner for a suggestion to improve Theorem 4.18. He also owes some inspiration for this project to a talk given by T. Fukuda about computations of class groups of abelian fields. The authors also wish to thank Gunter Malle for numerous helpful comments, and an anonymous referee for his thorough and thoughtful report that lead to improvements of the paper.

Notations. We will use $x \mapsto \overline{x}$ to denote various canonical projection maps that should be clear from the context.

Let A be a ring, and let $X \subseteq A$ be a subset. We write $\langle X \rangle_A = \sum_{x \in X} AxA$ for the two-sided ideal of A generated by X.

We will denote by 1 the trivial group. Let G be a finite group and R a commutative ring. Let M be an $R[G]$-module. We write $M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}$ for the R-submodule of fixed points under G. In case M is a $\mathbb{Z}$-module whose operation is expressed using multiplicative notation, e.g., the multiplicative group of a field or the multiplicative group of fractional ideals, we write the action of $\mathbb{Z}[G]$ on M as powers, by the formula

$$x^a = \prod_{g \in G} g(x)^{a_g} \text{ for all } x \in M,\ a = \sum_{g \in G} a_g g \in \mathbb{Z}[G].$$

Note that this is a left action, i.e. it satisfies $x^{ab} = (x^b)^a$ for all $a, b \in \mathbb{Z}[G]$.

Let H be a subgroup of G, which we write $H \leq G$. We denote by $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$ the norm element of H. Let M be an $R[H]$-module. We use the notation $\mathrm{Ind}_{G/H}(M)$ for the induction $R[G] \otimes_{R[H]} M$ of M to G. Let χ be the character of a $\mathbb{C}[H]$-module M; we write $\mathrm{Ind}_{G/H}(\chi)$ for the character of $\mathrm{Ind}_{G/H}(M)$, and we write $\mathrm{Res}_{G/H}(\chi)$ for the restriction of χ to H. Let F_1, F_2 be $\mathbb{C}$-valued class functions on G. We write their inner product $\frac{1}{|G|}\sum_{g \in G} F_1(g)\overline{F_2(g)}$ as $\langle F_1, F_2 \rangle_G$. We denote by $\mathbf{1}_G \colon G \to \mathbb{C}^\times$ the trivial character, which satisfies $\mathbf{1}_G(g) = 1$ for all $g \in G$. We denote by φ the Euler totient function.

Let A be a finite abelian group, written additively here. For a prime number p, if A has cardinality mp^k with $k \geq 0$ and m not divisible by p, let $A_p = A/p^k A$ be the p-part of A, and $A_{p'} = A/mA$ be the coprime-to-p part of A. We have $A \cong A_p \times A_{p'}$. For an integer d, denote by $A[d]$ the d-torsion subgroup $\{a \in A \mid da = 0\}$.

2. Brauer and norm relations of finite groups

2.1. Brauer relations and norm relations. Let G be a finite group and let $H \leq G$ be a subgroup. We recall a few basic properties of the norm element $N_H = \sum_{h \in H} h$:

- For all $h \in H$ we have $hN_H = N_H h = N_H$.
- For all $g \in G$ we have $gN_H g^{-1} = N_{gHg^{-1}}$.
- For every $\mathbb{Z}[G]$-module M and $x \in M$, we have $N_H x \in M^H$.
- We have $N_H^2 = |H| \cdot N_H$.
- If R is a commutative ring where $|H|$ is invertible, then $e = \frac{1}{|H|} N_H \in R[G]$ is an idempotent and for every $R[G]$-module M we have $eM = N_H M = M^H$.

Definition 2.1. Let G be a finite group and $\mathcal{H}$ a set of subgroups of G.

(1) A *Brauer relation* $\mathcal{R}$ of G with respect to $\mathcal{H}$ is an equality of the form

$$0 = \sum_{H \in \mathcal{H}} a_H \,\mathrm{Ind}_{G/H}(\mathbf{1}_H)$$

with $a_H \in \mathbb{Q}$, where the equality is as class functions on G. We call $\mathcal{R}$ *useful* if $1 \in \mathcal{H}$ and $a_1 \neq 0$. If $\mathcal{H}$ is the set of all subgroups of G, we simply call $\mathcal{R}$ a Brauer relation.

(2) Let R be a commutative ring. A *norm relation over R with respect to $\mathcal{H}$* (or simply *norm relation* if $R = \mathbb{Q}$) is an equality of the form

$$1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

with $a_i, b_i \in R[G]$ and $H_i \in \mathcal{H}$, $H_i \neq 1$, where the equality holds in $R[G]$.

(3) A *scalar norm relation* $\mathcal{R}$ of G over R with respect to $\mathcal{H}$ is an equality of the form
$$0 = \sum_{H \in \mathcal{H}} a_H N_H$$
with $a_H \in R$ and $a_1 \neq 0$, where the equality holds in the group algebra $R[G]$. If $\mathcal{H}$ is the set of all subgroups of G, we simply call $\mathcal{R}$ a scalar norm relation.

We always omit $\mathcal{H}$ from the terminology when $\mathcal{H}$ is the set of all nontrivial subgroups of G.

Remark 2.2.

(1) In the literature, the term *norm relation* is also used for relations of the form
$$0 = \sum_{H \leq G} a_H N_H$$
with $a_H \in \mathbb{Q}$. In this regard, we consider and generalize classical norm relations with $a_1 \neq 0$. In particular, our norm relations are by definition always nonzero.

(2) Brauer relations of finite groups have been completely classified by Bartel and Dokchitser ([9, 8]).

(3) Let $\tilde{H} \leq H$ be a subgroup. We have $N_H = \sum_{h \in H/\tilde{H}} h N_{\tilde{H}}$, so in a norm relation where H appears we may always replace it by $\tilde{H}$ at the cost of increasing the number of terms.

Example 2.3. Let p be a prime, and let $G = C_p \times C_p$. Then we have the scalar norm relation
$$p = \left(\sum_{C \leq G,\, |C|=p} N_C \right) - N_G.$$
Indeed, every nontrivial element of G has order p, there are $p+1$ subgroups of order p, and every nontrivial element is contained in exactly one of them.

Example 2.4. Let p be a prime, and let q be a prime dividing $p-1$. Let $G = C_p \rtimes C_q$ be a nontrivial semidirect product. Then we have the scalar norm relation
$$p = N_{C_p} + \left(\sum_{C \leq G,\, |C|=q} N_C \right) - N_G.$$
Indeed, every nontrivial element of G has order p or q, there is a unique subgroup of order p, there are p subgroups of order q, and every nontrivial element is contained in exactly one of them.

Example 2.5. Let $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$. Then we have the norm relation
$$2 = N_{\langle \sigma \rangle} + N_{\langle \tau \rangle} - \sigma N_{\langle \sigma\tau \rangle}.$$
This is the relation used by Wada [50], Bauch, Bernstein, de Valence, Lange and van Vredendaal [10] as well as by Biasse and van Vredendaal [13].

Example 2.6. Let $G = C_3 \times C_3 = \langle u, v \rangle$. Then we have the norm relation
$$3 = N_{\langle u \rangle} + N_{\langle v \rangle} + N_{\langle uv \rangle} - (u + uv) N_{\langle u^2 v \rangle}.$$
This is the relation used by Parry [44] and by Lesavourey, Plantard and Susilo [35].

2.2. **Existence of relations.** We now discuss the existence of the various relations. We begin by showing that Brauer and scalar norm relations are in essence the same.

Proposition 2.7. Let G be a finite group and $\mathcal{H}$ a set of subgroups of G.

(1) If
$$0 = \sum_{H \in \mathcal{H}} a_H N_H$$
is a scalar norm relation with respect to $\mathcal{H}$, then
$$0 = \sum_{H \in \mathcal{H}} a_H |H| \operatorname{Ind}_{G/H}(\mathbf{1}_H)$$
is a useful Brauer relation with respect to $\mathcal{H}$.

(2) If
$$0 = \sum_{H \in \mathcal{H}} a_H \operatorname{Ind}_{G/H}(\mathbf{1}_H)$$
is a useful Brauer relation with respect to $\mathcal{H}$ then
$$0 = \sum_{H \in \mathcal{H}} \frac{a_H}{|H|} \sum_{g \in G} N_{gHg^{-1}}$$
is a scalar norm relation; if in addition $\mathcal{H}$ is invariant under conjugation, then
$$0 = \sum_{H \in \mathcal{H}} \left(\frac{1}{|H|} \sum_{g \in G} a_{gHg^{-1}} \right) N_H$$
is a scalar norm relation with respect to $\mathcal{H}$.

Proof. The statements are implicitly contained in [52]. For the sake of completeness we include a proof. We will make use of the fact that
$$\sum_{g \in G} \operatorname{Ind}_{G/H}(\mathbf{1}_H)(g) \cdot g = |H|^{-1} \sum_{g \in G} g N_H g^{-1}$$
for all subgroups $H \leq G$. (1): Assume now that $\sum_{H \in \mathcal{H}} a_H N_H = 0$ is a scalar norm relation. Then also $\sum_{H \in \mathcal{H}} a_H g N_H g^{-1} = 0$ for all $g \in G$ and summing over all $g \in G$ yields
$$0 = \sum_{g \in G} \sum_{H \in \mathcal{H}} a_H g N_H g^{-1} = \sum_{H \in \mathcal{H}} a_H \sum_{g \in G} g N_H g^{-1} = \sum_{H \in \mathcal{H}} a_H |H| |H|^{-1} \sum_{g \in G} g N_H g^{-1}.$$
Hence
$$0 = \sum_{H \in \mathcal{H}} a_H |H| \sum_{g \in G} \operatorname{Ind}_{G/H}(\mathbf{1}_H)(g) \cdot g = \sum_{g \in G} \left(\sum_{H \in \mathcal{H}} a_H |H| \operatorname{Ind}_{G/H}(\mathbf{1}_H)(g) \right) \cdot g$$
in $\mathbb{Q}[G]$. Thus $\sum_{H \in \mathcal{H}} a_H |H| \operatorname{Ind}_{G/H}(\mathbf{1}_H) = 0$ is a Brauer relation, which is useful since $a_1 \neq 0$.

(2): Assume now that $\sum_{H \in \mathcal{H}} a_H \operatorname{Ind}_{G/H}(\mathbf{1}_H) = 0$ is a useful Brauer relation with respect to $\mathcal{H}$. Then from the above computation we conclude that
$$0 = \sum_{g \in G} \sum_{H \in \mathcal{H}} \frac{a_H}{|H|} g N_H g^{-1} = \sum_{H \in \mathcal{H}} \sum_{g \in G} \frac{a_H}{|H|} N_{gHg^{-1}},$$
which is a scalar norm relation since the coefficient of $H = 1$ is $a_1 |G| \neq 0$. If $\mathcal{H}$ is invariant under conjugation, then after reordering this relation becomes the claimed scalar norm relation with respect to $\mathcal{H}$. $\square$

We illustrate the second statement by the following example.

Example 2.8. Consider the symmetric group $G = S_3$ on three letters and the set of subgroups $\mathcal{H} = \{G, C_3, C_2, 1\}$, where C_2 is generated by any of the transpositions. Then G admits the useful Brauer relation

$$0 = \operatorname{Ind}_{G/1}(\mathbf{1}_1) + 2\operatorname{Ind}_{G/G}(\mathbf{1}_G) - \operatorname{Ind}_{G/C_3}(\mathbf{1}_{C_3}) - 2\operatorname{Ind}_{G/C_2}(\mathbf{1}_{C_2}).$$

It is easy to see that G does not admit a scalar norm relation with respect to $\mathcal{H}$. The scalar norm relation given by the proposition is

$$0 = 6N_1 + 2N_G - 2N_{C_3} - 2N_{C_2} - 2N_{C_2'} - 2N_{C_2''},$$

where C_2, C_2', C_2'' are the three subgroups of order 2 of G. Simplified, it becomes

$$3 = N_{C_2} + N_{C_2'} + N_{C_2''} + N_{C_3} - N_G,$$

a special case of Example 2.4.

When $\mathcal{H}$ is the set of all nontrivial subgroups of G, we have the following simple characterization for the existence of Brauer relations.

Theorem 2.9 (Funakura)**.** The group G admits a useful Brauer relation if and only if G contains a non-cyclic subgroup of order pq, where p and q are primes (not necessarily distinct).

Proof. This is [24, Theorem 9]. □

We now turn to the question of existence for norm relations. Together with Theorem 2.9 this will at the same time show that there are in general more norm relations than scalar norm relations. As a first step towards the classification, we formulate a representation theoretic criterion. In the following we denote by $e_1, \dots, e_r$ the central primitive idempotents of the group algebra $\mathbb{Q}[G]$.

Proposition 2.10. Let $\mathcal{H}$ be a set of nontrivial subgroups of a finite group G. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then the following are equivalent:

(1) there exists a norm relation in G with respect to $\mathcal{H}$;
(2) we have $\langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Q}[G]} = \mathbb{Q}[G]$ (as a two sided ideal);
(3) for all $i = 1, \dots, r$, there exists $H \in \mathcal{H}$ such that $e_i N_H \neq 0$;
(4) for every simple $\mathbb{Q}[G]$-module V, there exists $H \in \mathcal{H}$ such that the space of fixed points V^H is nonzero;
(5) for every simple $\overline{\mathbb{Q}}[G]$-module V, there exists $H \in \mathcal{H}$ such that the space of fixed points V^H is nonzero;
(6) for every simple $\mathbb{C}[G]$-module V, there exists $H \in \mathcal{H}$ such that the space of fixed points V^H is nonzero;
(7) for every unitary $\mathbb{C}[G]$-module V, there exists $H \in \mathcal{H}$ such that H has a fixed point on the unit sphere of V with respect to the invariant Hermitian norm.

Proof. The set of elements of the form $\sum_{i=1}^{\ell} a_i N_{H_i} b_i$ with $a_i, b_i \in \mathbb{Q}[G]$ and $H_i \in \mathcal{H}$ is exactly the two-sided ideal $\langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Q}[G]}$. Moreover a two-sided ideal contains 1 if and only if it equals the whole ring. This proves the equivalence between (1) and (2).

For every two-sided ideal J of $\mathbb{Q}[G]$ we have $J = \sum_{i=1}^{r} e_i J$, so $J = \mathbb{Q}[G]$ if and only if $e_i J = e_i \mathbb{Q}[G]$ for every $i \in \{1, \dots, r\}$. In addition, $e_i J$ projects isomorphically to a two-sided ideal in the simple algebra $\mathbb{Q}[G]/(1 - e_i)$, so it is either equal to $e_i\mathbb{Q}[G]$ or zero. Applying this to $J = \langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Q}[G]}$, and noting that $e_iJ = 0$ if and only if $e_iN_H = 0$ for all $H \in \mathcal{H}$, this proves the equivalence between (2) and (3).

For every $\mathbb{Q}[G]$-module V and subgroup $H \le G$, we have $(\frac{1}{|H|}N_H) \cdot V = V^H$. Let $1 \le i \le r$, and let V_i be the (up to isomorphism) unique simple $\mathbb{Q}[G]$-module such that $e_iV_i \neq 0$. Since the simple algebra $\mathbb{Q}[G]/(1-e_i)$ acts faithfully on V_i, we have

$$e_iN_H = 0 \iff N_H \cdot V_i = 0 \iff \left(\frac{1}{|H|}N_H\right) \cdot V_i = 0 \iff V_i^H = 0.$$

This proves the equivalence between (3) and (4).

Let $K \subseteq L$ be subfields of $\mathbb{C}$. For every $K[G]$-module V and every subgroup $H \le G$, we have $\dim_K V^H = \dim_L(V \otimes_K L)^H$; in particular $V^H \neq 0$ if and only if $(V \otimes_K L)^H \neq 0$. In addition, every simple $L[G]$-module is isomorphic to a submodule of $V \otimes_K L$ for some simple $K[G]$-module V. Applying this to $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, we obtain (6) $\Rightarrow$ (5) $\Rightarrow$ (4).

Let W be a simple $\overline{\mathbb{Q}}[G]$-module, and let V be a simple $\mathbb{Q}[G]$-module such that W is isomorphic to a submodule of $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$. Let $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \bigoplus_{j=1}^k W_j$ be a decomposition into simple $\overline{\mathbb{Q}}[G]$-modules, so that W is isomorphic to one of the W_j. Since the W_j are pairwise Galois conjugate, we have $\dim_{\overline{\mathbb{Q}}} W_j^H = \dim_{\overline{\mathbb{Q}}} W_1^H$ for all j, so that $V^H \neq 0$ implies that for all j we have $W_j^H \neq 0$. In particular $W^H \neq 0$ and we get (4) $\Rightarrow$ (5).

The simple $\mathbb{C}[G]$-modules are exactly the $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$ where V ranges over the simple $\overline{\mathbb{Q}}[G]$-modules, so that we have (5) $\Rightarrow$ (6).

Let us prove that (6) implies (7). Let V be a unitary $\mathbb{C}[G]$-module. It contains a simple $\mathbb{C}[G]$-submodule V', and therefore by (6) there exists $H \in \mathcal{H}$ and $v \in (V')^H \setminus \{0\}$, so that $v \in V^H$. Then $v/\|v\|$ is a fixed point of H on the unit sphere of V. Conversely, since every $\mathbb{C}[G]$-module is unitarizable, (7) implies (6). $\square$

This can in turn be used to characterize groups that admit norm relations.

Theorem 2.11. Let G be a finite group. Then the following are equivalent:

(1) the group G admits a norm relation;
(2) the group G admits a norm relation with respect to the set of nontrivial cyclic subgroups of G;
(3) the group G has a non-cyclic subgroup of order pq, where p and q are prime, or a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ where $p > 5$ is prime;
(4) the group G contains a non-cyclic subgroup of order pq, where p and q are prime, or a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ where $p = 2^{2^k} + 1$ is a Fermat prime with $k > 1$.

Proof. Clearly (2) implies (1). The converse follows from Remark 2.2 (3).

Applying criterion (7) of Proposition 2.10, we see that (2) is equivalent to the nonexistence of a unitary $\mathbb{C}[G]$-module V such that for every $g \neq 1$, the element g does not have fixed points on the unit sphere of V, in other words such that G acts freely on the unit sphere of V. The equivalence between this last statement and (3) is Wolf's theorem ([51, Theorem 6.1]).

The equivalence between (3) and (4) follows from observing that when p is not a Fermat prime, we may pick a prime $q \neq 2$ dividing $p - 1$ and an element $a \in \mathbb{F}_p^\times$

of order q, and that the subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ generated by $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is a noncyclic group of order pq. □

Example 2.12. In view of Theorem 2.11 compared with Theorem 2.9, the smallest group that admits a norm relation but no scalar norm relation is the group $\mathrm{SL}_2(\mathbb{F}_{17})$ of cardinality 4896. It admits a norm relation with denominator 17 with respect to the set of subgroups of index at most 1632.

Even if a group admits both a scalar norm relation and a norm relation, there might still be a difference when it comes to the subgroups that are involved in the relations. The following example illustrates this phenomenon.

Example 2.13. Consider the direct product $G = C_2 \times \mathrm{SU}_3(\mathbb{F}_2)$ of order 432. Then the smallest $n \geq 1$ such that G admits a scalar norm relation with respect to the set of subgroups of index at most n is 72, but the smallest n such that G admits a norm relation with respect to the set of subgroups of index at most n is 54.

Remark 2.14. In addition to an existence criterion like Theorem 2.11 or Proposition 2.10, it would be interesting to establish a complete classification of norm relations similar to the existing one for Brauer relations [9, 8].

2.3. **Arithmetic properties of relations.**

Definition 2.15. Let $\mathcal{H}$ be a set of nontrivial subgroups of G. We define the *optimal denominator* $d(\mathcal{H})$ *relative to* $\mathcal{H}$, to be the unique nonnegative integer such that

$$d(\mathcal{H})\mathbb{Z} = \mathbb{Z} \cap \langle N_H \mid H \in \mathcal{H} \rangle_{\mathbb{Z}[G]}.$$

Let

$$1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

be a norm relation with $H_i \in \mathcal{H}$ and $a_i, b_i \in \mathbb{Q}[G]$. The least common denominator of the coefficients of the a_i and b_i is called the *denominator* of the relation.

Remark 2.16. We have $d(\mathcal{H}) > 0$ if and only if there exists a norm relation over $\mathbb{Q}$. In that case, the optimal denominator divides the denominator of every relation, and there exists a relation with optimal denominator.

For arithmetic applications, it is desirable to have a relation with denominator as small as possible, and more precisely with denominator divisible by as few primes as possible (see Corollary 3.3, Corollary 3.4 and Proposition 3.7). The following proposition characterizes the existence of relations with denominator coprime to a given p. In addition, Theorem 2.20 says that the primes that do not divide $|G|$ can always be removed from the denominator of norm relations.

Remark 2.17. Consider a scalar norm relation $\mathcal{R}$ of the form $0 = \sum_{H \in \mathcal{H}} a_H N_H$ with $a_H \in \mathbb{Z}$. Since $1 = \sum_{H \in \mathcal{H}} -\frac{a_H}{a_1} N_H$, we will view $\mathcal{R}$ as a norm relation and define its denominator to be the denominator of the corresponding norm relation. Thus any scalar norm relation with denominator d is of the form

$$d = \sum_{H \in \mathcal{H}} b_H N_H$$

with $d, b_H \in \mathbb{Z}$ coprime.

Proposition 2.18. Let $\mathcal{H}$ be a set of nontrivial subgroups of G, and let p be a prime number. Let J be the Jacobson radical of $\mathbb{F}_p[G]$. Then the following are equivalent:

(1) $p \nmid d(\mathcal{H})$;
(2) there exists a norm relation over $\mathbb{F}_p$ with respect to $\mathcal{H}$;
(3) there exists an identity of the form
$$1 = \sum_i a_i N_{H_i} b_i$$
where $a_i, b_i \in \mathbb{F}_p[G]/J$ and the identity holds in $\mathbb{F}_p[G]/J$;
(4) for every simple $\mathbb{F}_p[G]$-module V, there exists $H \in \mathcal{H}$ such that $N_H \cdot V \neq 0$;
(5) for every simple $\overline{\mathbb{F}}_p[G]$-module V, there exists $H \in \mathcal{H}$ such that $N_H \cdot V \neq 0$.

Proof. It is clear that (1) implies (2). Conversely, assume that
$$1 = \sum_i \bar{a}_i N_{H_i} \bar{b}_i$$
is a relation over $\mathbb{F}_p$. Pick arbitrary lifts $a_i, b_i \in \mathbb{Z}[G]$ of $\bar{a}_i, \bar{b}_i$, and let
$$\delta = \sum_i a_i N_{H_i} b_i.$$
We have $N_{\mathbb{Z}[G]/\mathbb{Z}}(\delta) \equiv N_{\mathbb{F}_p[G]/\mathbb{F}_p}(1) \equiv 1 \bmod p$, which is nonzero. Therefore the norm is nonzero, the element δ is invertible in $\mathbb{Q}[G]$ and the denominator d of δ^{-1} is coprime to p. We therefore obtain the relation
$$d = \sum_i (d\delta^{-1}) a_i N_{H_i} b_i$$
with $d \in \mathbb{Z}$ coprime to p and $(d\delta^{-1})a_i \in \mathbb{Z}[G]$, and therefore $p \nmid d(\mathcal{H})$. This proves that (2) implies (1).

It is clear that (2) implies (3). Conversely, assume that
$$1 = \sum_i \bar{a}_i N_{H_i} \bar{b}_i$$
holds in $\mathbb{F}_p[G]/J$. Pick arbitrary lifts $a_i, b_i \in \mathbb{F}_p[G]$ of $\bar{a}_i, \bar{b}_i$, and let
$$\delta = \sum_i a_i N_{H_i} b_i.$$
We have $\delta \equiv 1 \bmod J$; since 1 is invertible and J is a nilpotent two-sided ideal, this implies that δ is invertible. We therefore have the relation
$$1 = \sum_i \delta^{-1} a_i N_{H_i} b_i$$
in $\mathbb{F}_p[G]$. This proves that (3) implies (2).

The proof of the equivalence between (3) and (4) is identical to that of Proposition 2.10 by considering the central primitive idempotents of the semisimple algebra $\mathbb{F}_p[G]/J$.

The proof of the equivalence between (4) and (5) is identical to that of Proposition 2.10. □

Remark 2.19. It would be interesting to find a general existence criterion similar to Theorem 2.11 for norm relations over $\mathbb{F}_p$.

Theorem 2.20. Let $\mathcal{H}$ be a set of nontrivial subgroups of G. If $d(\mathcal{H}) > 0$ then $d(\mathcal{H})$ divides $|G|^3$.

Proof. The following proof we will use properties of maximal orders in semisimple algebras, which can be found in [47]. Assume that $d(\mathcal{H}) > 0$, and let p be a prime number. In the following we will denote by $\mathbb{Z}_p$ and $\mathbb{Q}_p$ the ring of p-adic integers and the field of p-adic numbers respectively. Let $\mathcal{O}$ be a maximal order of $\mathbb{Q}_p[G]$ containing $\mathbb{Z}_p[G]$, and let $e_1, \ldots, e_r$ be central primitive idempotents of $\mathbb{Q}_p[G]$ contained in $\mathcal{O}$, which exist since $\mathcal{O}$ is a maximal order [47, Theorem (10.5) (i)].

Let $1 \le i \le r$. By Proposition 2.10, there exists $H = H_i \in \mathcal{H}$ such that $e_i N_H \ne 0$. Let $N_i = e_i N_H$, which satisfies $N_i^2 = |H| \cdot N_i$. By [47, Theorem (17.3) (ii)] there is an isomorphism $\psi\colon \mathcal{O}/(1-e_i) \to \mathrm{M}_n(\Lambda)$ where $\Lambda = \Lambda_i$ is the maximal order of a division algebra over $\mathbb{Q}_p$ and $n = n_i \ge 1$; let v be the normalized valuation of Λ. We extend ψ to $\mathcal{O}$ via $\mathcal{O} \to \mathcal{O}/(1-e_i)$. Write the Smith normal form (see [47, Theorem (17.7)]) of $\psi(N_i)$ as follows: let $U, V \in \mathrm{M}_n(\Lambda)^\times$ and $\lambda_1, \ldots, \lambda_n \in \Lambda$ be such that $U\psi(N_i)V$ is the diagonal matrix $(\lambda_1, \ldots, \lambda_n)$ and $v(\lambda_j) \le v(\lambda_{j+1})$ for all $1 \le j < n$. Since $\lambda_1 \ne 0$, the relation $N_i^2 = |H| \cdot N_i$ implies that $v(\lambda_1) \le v(|H|)$. Let $u_i, v_i \in \mathcal{O}$ be such that $\psi(u_i) = U$ and $\psi(v_i) = V$. For each $1 \le j \le n$, let $a_{i,j}, b_{i,j} \in \mathcal{O}$ be such that $\psi(a_{i,j}) \in \mathrm{M}_n(\Lambda)$ is the matrix with all coefficients 0 except the $(j,1)$-th coefficient equal to 1 and $\psi(b_{i,j}) \in \mathrm{M}_n(\Lambda)$ is the matrix with all coefficients 0 except the $(1,j)$-th coefficient equal to $|H|\lambda_1^{-1} \in \Lambda$. We obtain that $\sum_{j=1}^n \psi(a_{i,j} u_i N_i v_i b_{i,j})$ is $|H|$ times the $n \times n$ identity matrix, and therefore

$$\frac{1}{|H_i|} \sum_{j=1}^{n} e_i a_{i,j} u_i N_i v_i b_{i,j} = e_i.$$

Summing over i, we obtain the norm relation

$$\sum_{i=1}^{r} \sum_{j=1}^{n_i} e_i a_{i,j} u_i \frac{1}{|H_i|} N_{H_i} v_i b_{i,j} = 1.$$

Since $e_i a_{i,j} u_i \in \mathcal{O}$, $v_i b_{i,j} \in \mathcal{O}$, and $\mathcal{O} \subseteq \frac{1}{|G|}\mathbb{Z}_p[G]$ ([19, (27.1) Proposition]), the denominator of this relation divides $|G|^3$ in $\mathbb{Z}_p$, so that $|G|^3 \in d(\mathcal{H})\mathbb{Z}_p$.

Putting all p together, we obtain that $d(\mathcal{H})$ divides $|G|^3$ as claimed. $\square$

Remark 2.21. It is clear from the proof that $|G|^3$ can be replaced with hg^2, where h is the least common multiple of the $|H|$ for $H \in \mathcal{H}$ and $g > 0$ is the smallest integer such that there is a maximal order $\mathcal{O}$ satisfying $\mathbb{Z}[G] \subset \mathcal{O} \subset \frac{1}{g}\mathbb{Z}[G]$.

The following example shows that in general the minimal denominators of scalar and arbitrary norm relations are not equal.

Example 2.22. Let $G = A_5$ be the alternating group on 5 letters, and let $\mathcal{H}$ be the set of subgroups of G of index at most 12 (up to conjugacy, these subgroups are C_5, S_3, D_5, A_4, A_5). Then G admits a scalar norm relation with respect to $\mathcal{H}$. However, all scalar norm relations with respect to $\mathcal{H}$ have denominator supported at $2, 3$ and 5, but G admits a norm relation with respect to $\mathcal{H}$ with denominator supported only at 2 and 5.

2.4. **Norm relations in finite abelian groups.** In the case of abelian groups, there is a second way to turn Brauer relations into norm relations and conversely based on duality.

Definition 2.23. Let G be a finite abelian group. Let $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ be the dual of G. We have a canonical isomorphism $G \to \widehat{\widehat{G}}$ given by $g \mapsto (\chi \mapsto \chi(g))$, and a noncanonical isomorphism $G \cong \widehat{G}$. Let $X \subseteq G$ be a subset; we write $X^\perp = \{\chi \in \widehat{G} \mid \chi(x) = 1 \text{ for all } x \in X\} \subseteq \widehat{G}$.

In the following, whenever we are dealing with an abelian group G, we will use the canonical isomorphism with its bidual and its inverse implicitly to identify subgroups of the dual of $\widehat{G}$ with subgroups of G. Since the 1-dimensional characters of G form a $\mathbb{C}$-basis of the space of class functions of G, this space is canonically isomorphic to $\mathbb{C}[\widehat{G}]$; we will also use this identification implicitly.

Proposition 2.24. Let G be a finite abelian group.

(1) Let $H \leq G$ be a subgroup. We have $\mathrm{Ind}_{G/H}(\mathbf{1}_H) = N_{H^\perp}$.

(2) We have

$$\sum_{H \leq G} a_H \cdot \mathrm{Ind}_{G/H}(\mathbf{1}_H) = 0 \quad \text{(Brauer relation of } G\text{)}$$

if and only if we have

$$\sum_{H \leq \widehat{G}} a_{H^\perp} \cdot N_H = 0 \quad \text{(norm relation of } \widehat{G}\text{)}.$$

The second equality is a norm relation if and only if $a_G \neq 0$.

(3) Let $\mathcal{H}$ be a set of subgroups of G, and let $\mathcal{H}^\perp = \{H^\perp : H \in \mathcal{H}\}$. Then the group G admits a Brauer relation with respect to $\mathcal{H}$ if and only if $\widehat{G}$ admits a norm relation with respect to $\mathcal{H}^\perp$.

Proof. Let $\chi \in \widehat{G}$. By Frobenius reciprocity we have

$$\langle \mathrm{Ind}_{G/H}(\mathbf{1}_H), \chi \rangle_G = \langle \mathbf{1}_H, \mathrm{Res}_{G/H}(\chi) \rangle_H.$$

This inner product equals 1 if $\mathrm{Res}_{G/H}(\chi) = \mathbf{1}_H$, i.e. if $\chi \in H^\perp$, and 0 otherwise, proving the first assertion. The next two follow trivially. $\square$

Remark 2.25. Obviously, we have the corresponding dual statements as follows.

(1) Let $H \leq G$ be a subgroup. We have $N_H = \mathrm{Ind}_{\widehat{G}/H^\perp}(\mathbf{1}_{H^\perp})$.

(2) We have

$$\sum_{H \leq G} a_H \cdot N_H = 0 \quad \text{(norm relation of } G\text{)}$$

if and only if we have

$$\sum_{H \leq \widehat{G}} a_{H^\perp} \cdot \mathrm{Ind}_{\widehat{G}/H}(\mathbf{1}_H) = 0 \quad \text{(Brauer relation of } \widehat{G}\text{)}.$$

The Brauer relation is useful if and only if $a_G \neq 0$.

(3) The group G admits a norm relation with respect to $\mathcal{H}$ if and only if $\widehat{G}$ admits a Brauer relation with respect to $\mathcal{H}^\perp$.

Proposition 2.26. Let μ denote the Möbius function. For $n > 1$ an integer, let $\mathrm{rad}(n) = \prod_{p \mid n} p$, where the product ranges over prime divisors p of n.

Let G be a non-cyclic abelian group.

(1) We have the norm relation $\mathcal{R}_G$:

$$1 = \sum_{C=\langle\chi\rangle\le\widehat{G}\text{ cyclic}} a_{\ker\chi} N_{\ker\chi},$$

where

$$a_{\ker\chi} = \frac{1}{|\ker\chi|} \sum_{C\le C'\le\widehat{G}\text{ cyclic}} \mu([C':C]).$$

(2) We have

$$a_{\ker\chi} = \frac{c}{|G|} \prod_{p|c} \left(1 - p^{r_p-1}\delta_{\chi,p}\right) \prod_{p||G|,\, p\nmid c} \left(-p - p^2 - \cdots - p^{r_p-1}\right)$$

where c denotes the order of χ and in each product p ranges over prime divisors, where $\delta_{\chi,p} = 1$ or 0 according as whether there exists $\chi' \in \widehat{G}$ such that $(\chi')^p = \chi$, and where $r_p = \dim_{\mathbb{F}_p}(G/G^p)$ denotes the p-rank of G.

(3) The denominator of $\mathcal{R}_G$ divides $\frac{|G|}{\mathrm{rad}(|G|)}$, with equality if G is a p-group.

Proof. The first assertion is [24, Corollary 6], applied to the group $\widehat{G}$ and dualized using Proposition 2.24.

In order to prove (2), we rewrite the expression for $a_{\ker\chi}$ as follows.

$$\frac{1}{|\ker\chi|} \sum_{C\le C'\le\widehat{G}\text{ cyclic}} \mu([C':C]) = \frac{c}{|G|} \sum_{d\ge1} \mu(d) |\{C \le C' \le \widehat{G} \mid [C':C] = d\}|.$$

Every C' that appears in this sum is generated by an element χ' of order cd such that $(\chi')^d = \chi$. Moreover, the set of $\chi'' \in \widehat{G}$ that generate the same cyclic group as χ' and satisfy $(\chi'')^d = \chi$ is exactly the set of $\chi'' = (\chi')^k$ where $k \in (\mathbb{Z}/cd\mathbb{Z})^\times$ is such that $k \equiv 1 \bmod c$: there are exactly $\varphi(cd)/\varphi(c)$ such elements. We therefore obtain

$$a_{\ker\chi} = \frac{c}{|G|} \sum_{d||G|} \mu(d) \frac{\varphi(c)}{\varphi(cd)} |\{\chi' \in \widehat{G} \mid (\chi')^d = \chi \text{ and } \chi' \text{ has order } cd\}|.$$

This expression is multiplicative with respect to the decomposition of G into a product of p-Sylow subgroups, so we may assume that G is a nontrivial p-group, in which case $p \mid c$ if and only if $\chi \ne 1$. Each sum then has exactly two nonzero summands corresponding to $d = 1$ and $d = p$, and the $d = 1$ term in the sum is 1, so it suffices to evaluate the summand $d = p$. If $\chi \ne 1$, then every χ' such that $(\chi')^p = \chi$ has order pc, and the number of such elements is $|\widehat{G}[p]|\delta_{\chi,p} = p^{r_p}\delta_{\chi,p}$; moreover $\varphi(c)/\varphi(pc) = 1/p$. If $\chi = 1$, then $c = 1$ and every χ' that has order p satisfies $(\chi')^p = \chi$, and the number of such elements is $|\widehat{G}[p]| - 1 = p^{r_p} - 1$; moreover $\varphi(c)/\varphi(pc) = 1/(p-1)$; finally we have

$$1 - \frac{p^{r_p}-1}{p-1} = -p - p^2 - \cdots - p^{r_p-1},$$

completing the proof of (2).

Let p be a prime divisor of $|G|$ and $\chi \in \widehat{G}$. By inspection, we see that the valuation of $a_{\ker\chi}$ satisfies $v_p(a_{\ker\chi}) \ge 1 - v_p(|G|)$ if $p \nmid c$, and $v_p(a_{\ker\chi}) \ge v_p(c) - v_p(|G|) \ge 1 - v_p(|G|)$ if $p \mid c$. In particular, we always have $v_p(a_{\ker\chi}) \ge 1 - v_p(|G|)$, and if G is a p-group then there is equality for $\chi = 1$; this proves the claim about the denominator of $\mathcal{R}_G$. ∎

Example 2.27. Let $G = C_{18} \times C_2$. Then the denominator of $\mathcal{R}_G$ is 2, but we have $\frac{|G|}{\mathrm{rad}(|G|)} = 6$. This shows that equality in (3) does not always hold.

We can leverage the previous proposition to obtain optimal relations with respect to the denominator and the index of the subgroups involved in the case of abelian groups.

Theorem 2.28. Let G be a finite abelian group, and write $G \cong C \times Q$ where C is the largest cyclic factor of G.

(1) Denominator 1 case.
  (a) The group G admits a denominator 1 norm relation if and only if $|Q|$ is divisible by at least two distinct primes.
  (b) Assume that G admits a denominator 1 norm relation. The smallest $n \geq 1$ such that G admits a denominator 1 norm relation with respect to the set of subgroups of index at most n is
$$n_0 = |C| \cdot \max_p |Q_p|,$$
where p ranges over all prime numbers.
  (c) Assume that G admits a denominator 1 norm relation. Let $\mathcal{H}$ be the union over the prime divisors p of $|G|$ of the set of subgroups H of $G_{p'}$ such that $G_{p'}/H$ is cyclic. Every subgroup in $\mathcal{H}$ has index at most n_0. For each prime number p dividing $|G|$, let d_p be the denominator of $\mathcal{R}_{G_{p'}}$, and let $1 = \sum_p u_p d_p$ be a Bézout identity for the d_p. Then
$$\sum_p u_p d_p \mathcal{R}_{G_{p'}}$$
is a denominator 1 scalar norm relation with respect to $\mathcal{H}$.

(2) Prime power denominator case. Assume that Q is a p-group.
  (a) The group G admits a norm relation if and only if $Q \neq 1$.
  (b) Assume that G admits a norm relation. The smallest $n \geq 1$ such that G admits a norm relation with respect to the set of subgroups of index at most n is $n_0 = |C|$.
  (c) Assume that G admits a norm relation. Let $\mathcal{H}$ be the set of subgroups H of G such that G/H is cyclic. Every subgroup in $\mathcal{H}$ has index at most n_0. Then $\mathcal{R}_{G_p}$ is a scalar norm relation with respect to $\mathcal{H}$ and with denominator $|G_p|/p$.

Proof. Let $\mathcal{H}$ be a set of subgroups of G. Let q be a prime, and assume that G admits a norm relation with respect to $\mathcal{H}$ and with denominator not divisible by q. We claim that $\mathcal{H}$ contains a subgroup of G of index at least $|C| \cdot |Q_q|$. To prove the claim, choose an isomorphism $G \cong G_q \times G_{q'}$, let $\chi \colon G \to \overline{\mathbb{F}}_q^\times$ be a one-dimensional character of maximal order, and let V be the corresponding $\overline{\mathbb{F}}_q[G]$-module. Clearly $G_q \subseteq \ker \chi$ and χ has order $|C_{q'}|$. By Proposition 2.18 (5), there exists $H \in \mathcal{H}$ such that $N_H \cdot V \neq 0$. Since $H_q = H \cap G_q$ acts trivially on V and $q \cdot V = 0$, by Remark 2.2 (3) we have $H_q = 1$, and in particular the index of H in G is divisible by $|G_q|$. Since $|H|$ is not divisible by q, we have
$$N_H \cdot V \neq 0 \iff \frac{1}{|H|} N_H \cdot V \neq 0 \iff V^H \neq 0 \iff H \subseteq \ker \chi.$$

In particular, the index of H in G is divisible by the order $|C_{q'}|$ of χ. Since $|G_q|$ and $|C_{q'}|$ are coprime, the index of H is therefore divisible by $|C_{q'}| \cdot |G_q| = |C| \cdot |Q_q|$ as claimed.

Applying the claim to $q = p$ for each prime divisor p of $|G|$ proves that in (1b) the integer n_0 is indeed a lower bound, and that in (1a) the "only if" direction holds.

Let p be a prime number dividing $|G|$ and let $H \leq G_{p'}$ be a subgroup such that $G_{p'}/H$ is cyclic. Then $|G_{p'}/H|$ divides $|C_{p'}|$, so the index of H in G divides $|C_{p'}| \cdot |G_p| = |C| \cdot |Q_p| \leq n_0$ as claimed in (1c). The existence of the Bézout identity follows from the fact that by Proposition 2.26 (3), for each prime number p dividing $|G|$ the denominator d_p is not divisible by p, and all d_p are divisors of $|G|$. This proves (1c), and therefore completes (1a) and (1b).

Now assume that Q is a p-group. If G admits a norm relation, then applying the above claim to a prime q that does not divide the denominator of the norm relation or $|G|$ proves that in (2b) the integer n_0 is indeed a lower bound, and that in (2a) the "only if" direction holds.

Let $H \leq G$ be a subgroup such that G/H is cyclic. Then $|G/H|$ divides $|C| = n_0$ as claimed in (2c). The rest of (2c) is contained in Proposition 2.26, and therefore completes (2a) and (2b). □

3. Arithmetic applications

Let K/F be a normal extension of algebraic number fields with Galois group G. In this section we will discuss the consequences of the existence of norm relations of G, scalar or not, for the structure and arithmetic properties of K.

In this section, we will consider either a scalar norm relation of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} \tag{$\star$}$$

with $H_i \leq G$, $d \in \mathbb{Z}_{>0}$ and $a_i \in \mathbb{Z}$, or a norm relation

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i \tag{$\star\star$}$$

with $H_i \leq G$, $d \in \mathbb{Z}_{>0}$, $a_i, b_i \in \mathbb{Z}[G]$.

We begin by describing a general statement that holds for arbitrary $\mathbb{Z}[G]$-modules. Let M be a $\mathbb{Z}[G]$-module and $H \leq G$ a subgroup; the action of the norm N_H induces a map $M \to M^H$, which we also denote by N_H.

Proposition 3.1. Let M be a $\mathbb{Z}[G]$-module.

(1) If G admits a scalar norm relation of the form ($\star$), then the exponent of the quotient $M/\sum_{i=1}^{\ell} M^{H_i}$ is finite and divides d.
(2) If G admits a norm relation of the form ($\star\star$), then the exponent of the quotient $M/\sum_{i=1}^{\ell} a_i M^{H_i}$ is finite and divides d.

Proof. Let $m \in M$. In the first case we have

$$d \cdot m = \left(\sum_{i=1}^{\ell} a_i N_{H_i}\right) \cdot m = \sum_{i=1}^{\ell} (a_i N_{H_i} \cdot m) \in \sum_{i=1}^{\ell} M^{H_i},$$

whereas in the second case we have (using the G-invariance of M)

$$d \cdot m = \left(\sum_{i=1}^{\ell} a_i N_{H_i} b_i \right) \cdot m = \sum_{i=1}^{\ell} \bigl(a_i N_{H_i} b_i \cdot m\bigr) \in \sum_{i=1}^{\ell} a_i M^{H_i}. \qquad \square$$

The following proposition shows that the exponent bound is optimal, therefore justifying Definition 2.15.

Proposition 3.2. Let $M = \mathbb{Z}[G]$ be the left regular $\mathbb{Z}[G]$-module, and let $\mathcal{H}$ be a set of nontrivial subgroups of G such that $d(\mathcal{H}) > 0$. Let N be the $\mathbb{Z}[G]$-submodule generated by $\sum_{H \in \mathcal{H}} M^H$. Then the exponent of M/N equals $d(\mathcal{H})$.

Proof. By Proposition 3.1, the exponent divides $d(\mathcal{H})$.

Let $H \in \mathcal{H}$. Then the set of elements of M of the form $N_H g$, where g ranges over a set of representatives of G/H, forms a $\mathbb{Z}$-basis of M^H. The $\mathbb{Z}[G]$-module generated by M^H is therefore the two-sided ideal generated by N_H. Putting all H together, we see that the $\mathbb{Z}[G]$-submodule N equals the two-sided ideal generated by the N_H for $H \in \mathcal{H}$. In particular, the order of the image of 1 in the quotient M/N equals $d(\mathcal{H})$, proving the proposition. $\square$

We will now apply Proposition 3.1 to both the additive and the multiplicative $\mathbb{Z}[G]$-modules attached to K.

3.1. **Additive structure.** Consider $M = \mathcal{O}_K$, the ring of integers of the number field K. For every $H \leq G$ we have $M^H = \mathcal{O}_{K^H}$, where K^H is the fixed field of H. Thus from Proposition 3.1 we obtain the following statement. Recall that an order $\mathcal{O}$ of K is defined to be *p-maximal* if $[\mathcal{O}_K : \mathcal{O}]$ is not divisible by p.

Corollary 3.3.

(1) If G admits a scalar norm relation of the form ($\star$), then the exponent of the quotient
$$\mathcal{O}_K/(\mathcal{O}_{K^{H_1}} + \cdots + \mathcal{O}_{K^{H_\ell}})$$
is finite and divides d. In particular, the ring of integers $\mathcal{O}_K$ is generated, as an abelian group, by the $\mathcal{O}_{K^{H_i}}$ together with any order that is p-maximal at all primes $p \mid d$.

(2) If G admits a norm relation of the form ($\star\star$), then the exponent of the quotient
$$\mathcal{O}_K/(a_1\mathcal{O}_{K^{H_1}} + \cdots + a_\ell\mathcal{O}_{K^{H_\ell}})$$
is finite and divides d. In particular, the ring of integers $\mathcal{O}_K$ is generated, as a $\mathbb{Z}[G]$-module, by the $\mathcal{O}_{K^{H_i}}$ together with any order that is p-maximal at all primes $p \mid d$.

3.2. **Multiplicative structure.** The group $K^\times$ is naturally a $\mathbb{Z}[G]$-module, of which we will consider various submodules as follows. Let S be a G-stable set of non-zero prime ideals of $\mathcal{O}_K$. Recall that

$$\mathcal{O}_{K,S}^\times = \{x \in K^\times \mid v_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}$$

is the group of S-units of K. Let L be a subfield of K; we define the S-units of L as $\mathcal{O}_{L,S'}^\times$ where $S' = \{L \cap \mathfrak{p} \mid \mathfrak{p} \in S\}$. The multiplicative group $M = \mathcal{O}_{K,S}^\times$ is a $\mathbb{Z}[G]$-submodule of $K^\times$ and for $H \leq G$ we have $M^H = \mathcal{O}_{K^H,S}^\times$.

Recall that for a finitely generated subgroup $V \subseteq K^\times$ and $d \in \mathbb{Z}_{>0}$, the *d-saturation of* V is the smallest group $W \subseteq K^\times$ such that $V \subseteq W$ and $K^\times/W$ is

d-torsion-free. Similarly, the *saturation of* V is the smallest group $W \subseteq K^\times$ such that $V \subseteq W$ and $K^\times/W$ is torsion-free. The group V is called *d-saturated* (resp. *saturated*) if V is equal to its d-saturation (resp. saturation).

Note that the S-unit group of K is saturated in $K^\times$, i.e. every element having a nonzero power that is an S-unit of K is itself an S-unit of K. Applying Proposition 3.1 to this situation yields the following.

Corollary 3.4.

(1) If G admits a scalar norm relation of the form ($\star$), then the exponent of the quotient
$$\mathcal{O}_{K,S}^\times/\mathcal{O}_{K^{H_1},S}^\times \cdots \mathcal{O}_{K^{H_\ell},S}^\times$$
is finite and divides d. In particular, the group $\mathcal{O}_{K,S}^\times$ of S-units of K equals the d-saturation of $\mathcal{O}_{K^{H_1},S} \cdots \mathcal{O}_{K^{H_\ell},S}^\times$.

(2) If G admits a norm relation of the form ($\star\star$), then the exponent of the quotient
$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K^{H_1},S}^\times)^{a_1} \cdots (\mathcal{O}_{K^{H_\ell},S}^\times)^{a_\ell}$$
is finite and divides d. In particular, the group $\mathcal{O}_{K,S}^\times$ of S-units of K equals the d-saturation of the $\mathbb{Z}[G]$-module generated by $(\mathcal{O}_{K^{H_1},S}^\times) \cdots (\mathcal{O}_{K^{H_\ell},S}^\times)$.

In view of the previous result, one might ask to what extent the relations between the invariants of K and of its subfields force a norm relation. A positive result in this direction was obtained by Artin in [3] for scalar norm relations, which easily extends to norm relations as follows.

Proposition 3.5. The group G admits a norm relation $d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$ if and only if for all $x \in K^\times$ we have $x^d = \prod_{1 \le i \le \ell} \mathrm{N}_{K/K_i}(x^{b_i})^{a_i}$.

Proof. Consider the element $\sigma = \sum_{i=1}^{\ell} a_i N_{H_i} b_i - d \in \mathbb{Z}[G]$ and assume that the equality in $K^\times$ holds. Thus $x^\sigma = 1$ for all $x \in K^\times$, that is, $\sigma \in \mathrm{Ann}_{\mathbb{Z}[G]}(K^\times)$. Since $\mathrm{Ann}_{\mathbb{Z}[G]}(K^\times) = 0$ by [3, Theorem 5], the result follows. □

Concerning the structure of the S-units, we have the following partial converse to Corollary 3.4. We will not use it in this work, but it answers a natural question: in a normal extension, is the existence of a norm relation necessary to be able to use subfields to recover the group of S-units?

Proposition 3.6. Let K/F be a finite normal extension of number fields with Galois group G, and let $\mathcal{H}$ be a set of nontrivial subgroups of G. Let S be a finite G-stable set of prime ideals of K. Assume that at least one of the following holds:

- F is not totally real,
- there is a real place of F that splits completely in K, or
- there is a prime ideal $\mathfrak{p}$ of F that splits completely in K and such that the primes above $\mathfrak{p}$ are in S.

If the $\mathbb{Z}[G]$-submodule of $\mathcal{O}_{K,S}^\times$ generated by the $\mathcal{O}_{K^H,S}^\times$ for $H \in \mathcal{H}$ has finite index, then G admits a norm relation with respect to $\mathcal{H}$.

Proof. Under the hypotheses of the proposition, the $\mathbb{Q}[G]$-module $\mathcal{O}_{K,S}^\times \otimes \mathbb{Q}$ contains a copy of the regular module modulo the trivial module, and is generated as a $\mathbb{Q}[G]$-module by the union of its fixed points under the subgroups $H \in \mathcal{H}$. Now apply Proposition 2.10 (4) and the fact that for every $H \in \mathcal{H}$ and every simple $\mathbb{Q}[G]$-module V, the module V is generated by V^H if and only if $V^H \neq 0$. □

3.3. **Class group structure.** Let $\mathrm{Cl}(K)$ be the class group of K, which is the quotient of the fractional ideals modulo the principal fractional ideals of K. While $\mathrm{Cl}(K)$ is again a $\mathbb{Z}[G]$-module it is not true that $\mathrm{Cl}(K^H) = \mathrm{Cl}(K)^H$ (in general the natural map $\mathrm{Cl}(K^H) \to \mathrm{Cl}(K)$ is not even injective).

Proposition 3.7. Assume that the group G admits a norm relation ($\star\star$). Define the maps

$$\Phi\colon\ \mathrm{Cl}(K) \to \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}),\ [\mathfrak{a}] \mapsto \left(\mathrm{N}_{K/K^{H_i}}(\mathfrak{a}^{b_i})\right)_i$$

and

$$\Psi\colon \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \longrightarrow \mathrm{Cl}(K),\ ([\mathfrak{a}_i])_i \longmapsto \prod_i [\mathfrak{a}_i \mathcal{O}_K]^{a_i}.$$

Let $R = \mathbb{Z}[\frac{1}{d}]$. Then the map

$$\Phi \otimes R\colon\ \mathrm{Cl}(K) \otimes R \to \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \otimes R$$

is injective, i.e. an isomorphism onto its image, and the map

$$\Psi \otimes R\colon \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \otimes R \longrightarrow \mathrm{Cl}(K) \otimes R$$

is surjective. The image $(\Phi \otimes R)(\mathrm{Cl}(K) \otimes R)$ is a direct summand of the group $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \otimes R$, and the group $\mathrm{Cl}(K)/\mathrm{Cl}(K)[d]$ is isomorphic to a subgroup of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i})$.

Proof. The relation ($\star\star$) shows that $\Psi \circ \Phi\colon\ \mathrm{Cl}(K) \to \mathrm{Cl}(K)$ is the map

$$\Psi \circ \Phi\colon [\mathfrak{a}] \to \prod_i [\mathfrak{a}]^{a_i N_{H_i} b_i} = [\mathfrak{a}]^d,$$

i.e. $\Psi \circ \Phi = d\,\mathrm{Id}$. Since d is invertible in R, this implies that $(\Psi \circ \Phi) \otimes R$ is invertible, and therefore that $\Phi \otimes R$ is injective and $\Psi \otimes R$ is surjective as claimed. Let $A = \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i}) \otimes R$ and $e = d^{-1}(\Phi \circ \Psi) \otimes R\colon A \to A$; then e is an idempotent, so that $A = eA \oplus (1-e)A$, and we have $eA = \Phi(\mathrm{Cl}(K) \otimes R)$ by surjectivity of $\Psi \otimes R$. Finally, we have a surjection $\mathrm{Cl}(K)/\ker\Phi \to \mathrm{Cl}(K)/\mathrm{Cl}(K)[d]$, and Φ induces an injection $\mathrm{Cl}(K)/\ker\Phi \to \bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i})$, proving that $\mathrm{Cl}(K)/\mathrm{Cl}(K)[d]$ is a subquotient of $\bigoplus_{i=1}^{\ell} \mathrm{Cl}(K^{H_i})$. Since every quotient of a finite abelian group B is also isomorphic to a subgroup of B, this proves the proposition. □

3.4. **Analytic structure.** For the sake of completeness, we also mention the following classical consequence for the analytic structure of K. For Brauer relations (and therefore also for scalar norm relations), we have the following well known implications for equalities of zeta functions.

Proposition 3.8. Suppose G admits a useful Brauer relation, written in the form

$$a_1 \operatorname{Ind}_{G/1}(\mathbf{1}_1) = \sum_{1 \neq H \leq G} a_H \operatorname{Ind}_{G/H}(\mathbf{1}_H)$$

with $a_H \in \mathbb{Z}$ and $a_1 > 0$. Then the following equality of zeta functions holds:

$$\zeta_K(s)^{a_1} = \prod_{1 \neq H \leq G} \zeta_{K^H}(s)^{a_H}.$$

Proof. See [22, Theorem 73]. □

4. Computational problems in number fields

We now describe algorithms for solving various computational problems in number fields that exploit the subfield structure as described in Section 3. Let K/F be a normal extension of algebraic number fields with Galois group G.

4.1. **Construction of relations.** We begin by explaining how to find norm relations. First note that if G is abelian, then one can use Theorem 2.28 to write down scalar norm relations directly. In the general case, let us assume that $\mathcal{H}$ is a set of subgroups. Considering the $\mathbb{Q}$-subspace $W = \langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Q}} \subseteq \mathbb{Q}[G]$, there exists a scalar norm relation if and only if $1 \in W$. Thus we can find scalar norm relations by using linear algebra over $\mathbb{Q}$. Similarly, when looking for a scalar norm relation with a specific denominator d, we can check whether $d \in \langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Z}}$ using linear algebra over $\mathbb{Z}$. A similar approach works for norm relations. In this case one has to consider the $\mathbb{Q}$-subspace $W = \langle N_H \mid H \in \mathcal{H}\rangle_{\mathbb{Q}[G]} = \langle gN_H h \mid H \in \mathcal{H}, g, h \in G\rangle_{\mathbb{Q}} \subseteq \mathbb{Q}[G]$. From the basic properties of norm elements, we can obtain a smaller generating set for W by considering only the elements $gN_H h$ with $H \in \mathcal{H}$, $g \in G/H$ and $h \in \mathcal{N}(H)\backslash G$ where $\mathcal{N}(H)$ denotes the normalizer of H in G.

Note that for Brauer relations, a simple linear algebra based method was described by Bosma and de Smit in [15, Section 3].

4.2. **Computing rings of integers.** Let K/F be a normal extension of algebraic number fields with Galois group G. We assume that G admits a norm relation of denominator d of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

with $H_i \leq G$, $d \in \mathbb{Z}$, $a_i, b_i \in \mathbb{Z}[G]$. The classical algorithm for computing the ring of integers $\mathcal{O}_K$ of K, that is, finding a $\mathbb{Z}$-basis of $\mathcal{O}_K$, proceeds by enlarging a starting order $\mathcal{O}$ successively until $\mathcal{O} = \mathcal{O}_K$ holds (see [34, Section 4]); it requires factoring, at least partially, the discriminant of $\mathcal{O}$, which can be hard. Using Corollary 3.3, we may alternatively compute the ring of integers of $\mathcal{O}_K$ using the rings of integers $\mathcal{O}_{K^{H_i}}$ as follows.

(1) For each $1 \leq i \leq \ell$ compute $\mathcal{O}_{K^{H_i}}$ classically (or recursively).
(2) Determine a $\mathbb{Z}$-basis of the order $\mathcal{O}$ generated by $a_1\mathcal{O}_{K^{H_1}} + \cdots + a_\ell\mathcal{O}_{K^{H_\ell}}$.
(3) Return $\mathcal{O} + \mathcal{O}_{p_1} + \cdots + \mathcal{O}_{p_r}$, where $p_1, \ldots, p_r$ denote the prime divisors of d and $\mathcal{O}_{p_i}$ denotes the p_i-maximal overorder of $\mathcal{O}$ (which can be computed efficiently, see [34, Theorem 4.5]).

Remark 4.1.

(1) In case one has a scalar norm relation, that is, $a_i \in \mathbb{Z}$ and $b_i = 1$ for all $1 \leq i \leq \ell$, according to Corollary 3.3 one can replace $\mathcal{O}$ by the order generated by $\mathcal{O}_{K^{H_1}} + \cdots + \mathcal{O}_{K^{H_\ell}}$. In the general case, one can also replace $\mathcal{O}$ by the order generated by the $\mathbb{Z}[G]$-module generated by $\mathcal{O}_{K^{H_1}} + \cdots + \mathcal{O}_{K^{H_\ell}}$.
(2) By Theorem 2.20, we may always choose the relation so that the p_i are among the prime divisors of $|G|$, and are therefore small. In particular, no hard factorization is needed in Step (3).

4.3. **Computing S-unit groups.** Let K/F be a normal extension of algebraic number fields with Galois group G. We assume that G admits a norm relation of denominator d of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

with $H_i \leq G$, $d \in \mathbb{Z}$, $a_i, b_i \in \mathbb{Z}[G]$. Let S be a finite G-stable set of non-zero prime ideals of $\mathcal{O}_K$. Our aim is to describe an algorithm for computing a $\mathbb{Z}$-basis of the S-unit group $\mathcal{O}_{K,S}^\times = \{x \in K \mid v_\mathfrak{p}(x) = 0 \text{ for } \mathfrak{p} \notin S\}$. Based on Corollary 3.4, this can be accomplished by the following steps.

(1) For each subfield $K_i = K^{H_i}$ determine a basis of the S-unit group $\mathcal{O}_{K_i,S}^\times$.
(2) Determine the group $V = (\mathcal{O}_{K_i,S}^\times)^{a_1} \cdots (\mathcal{O}_{K_\ell,S}^\times)^{a_\ell} \subseteq \mathcal{O}_{K,S}^\times$.
(3) Compute and return the d-saturation of V.

Remark 4.2. In case one has a scalar norm relation, that is, $a_i \in \mathbb{Z}$ and $b_i = 1$ according to Corollary 3.4 one can replace V by $\mathcal{O}_{K_i,S}^\times \cdots \mathcal{O}_{K_\ell,S}^\times$.

The computations in Step (1) can be done either using the algorithm of Simon [48, §I.1.2] (see also [18, 7.4.2]) or recursively. As Step (2) needs no further explanation, we will now describe the saturation in Step (3).

Saturation of finitely generated multiplicative groups. Saturation is a well known technique in computational algebraic number theory, used for example in the class and unit group computation of number fields ([45, Section 5.7]) or the number field sieve ([1]).

We will discuss this problem in the following generality. We let $V \subseteq K^\times$ be a finitely generated subgroup. For a fixed integer $d \in \mathbb{Z}_{>0}$, we wish to determine the d-saturation W of V. Recall that this is by definition the smallest group $W \subseteq K^\times$ with $V \subseteq W$ and $K^\times/W$ d-torsion-free. To determine whether a multiplicative group is d-saturated, the following simple result is crucial.

Lemma 4.3. Let $V \subseteq K^\times$ be finitely generated. Then the following hold.

(1) The d-saturation of V contains the d-torsion of $K^\times$.
(2) The group V is d-saturated if and only if V is p-saturated for all primes p dividing d.
(3) For a prime p the group V is not p-saturated if and only if there exists $\alpha \in K^\times \setminus V$ with $\alpha^p \in V$. In this case p divides the index $[\langle V, \alpha\rangle : V]$.
(4) Let p be a prime and assume that V contains the p-torsion of $K^\times$. Then V is p-saturated if and only if $V \cap (K^\times)^p = V^p$.

Proof. (1): Let W be the d-saturation of V and let $\alpha \in K^\times$ with $\alpha^d = 1$. As $K^\times/W$ is d-torsion-free, this implies $\alpha \in W$. Statements (2) and (3) are trivial.

For (4), let us assume that $V \cap (K^\times)^p = V^p$. Now let $\alpha \in K$ with $\alpha^p \in V$. Thus we have $\alpha^p \in V \cap (K^\times)^p = V^p$ and there exists $\beta \in V$ with $\alpha^p = \beta^p$. Since V contains the p-torsion elements of $K^\times$ this implies $\alpha \in V$. Now assume that V is p-saturated and $\alpha \in V \cap (K^\times)^p$. Thus there exists $\beta \in K^\times$ with $\beta^p = \alpha$. As V is p-saturated this implies $\beta \in V$ and $\alpha = \beta^p \in V^p$. $\square$

Thus, from now on we will assume that $d = p$ is a prime. As there exists a polynomial time algorithm to determine the irreducible factors and hence the roots of polynomials over K (see [33]), we may also assume that V contains the p-torsion of $K^\times$.

The previous lemma makes it clear that the key to saturation is the computation of $V \cap (K^\times)^p$. To this end, we want to detect global p-th powers by using local information. This is used for example in the class and unit group computation of number fields ([45, Section 5.7]) or the number field sieve ([1]). The building block is the following special case of the Grunwald–Wang theorem, see [4, Chapter X] or [40, Chapter IX, §1]. Note that since the exponent is prime, there is no obstruction to the Hasse principle for p-th powers. In the following, for a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we will denote by $K_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of K, by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation and by $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ the residue field at $\mathfrak{p}$.

Theorem 4.4 (Grunwald–Wang)**.** For every finite set S of primes of K, the canonical map

$$K^\times/(K^\times)^p \longrightarrow \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p$$

is injective.

To detect local powers, we make use of the following well-known statement.

Proposition 4.5. Let $d \in \mathbb{Z}_{>0}$. Assume that $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$ with $d \notin \mathfrak{p}$ and let $\varpi \in K$ be a local uniformizer at $\mathfrak{p}$. Then the map

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d \longrightarrow \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d, \quad \bar{x} \longmapsto (\overline{v}, \overline{x\varpi^{-v}}) \text{ where } v = v_\mathfrak{p}(x),$$

is an isomorphism. In particular if $V \subseteq K^\times$ is a subgroup with $v_\mathfrak{p}(\alpha)$ divisible by d for all $\alpha \in V$, then

$$\ker(V/V^d \to K_\mathfrak{p}/(K_\mathfrak{p}^\times)^d) = \ker(V/V^d \longrightarrow k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

Proof. This follows from the properties of unit groups in local fields (see [39, Chapter II, §5]) as follows: The map $K_\mathfrak{p}^\times \cong \mathbb{Z} \times \mathcal{O}_{K_\mathfrak{p}}^\times$, $x \mapsto (v_\mathfrak{p}(x), x\varpi^{-v_\mathfrak{p}(x)})$ is an isomorphism and the group $\mathcal{O}_{K_\mathfrak{p}}^\times$ decomposes as $k_\mathfrak{p}^\times \times (1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$. Denote by $q \in \mathbb{Z}$ the prime lying below $\mathfrak{p}$. As $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}} \cong \mathbb{Z}/q^a\mathbb{Z} \times \mathbb{Z}_q^b$ for integers $a, b \in \mathbb{Z}_{\geq 0}$ and $\gcd(d, q) = 1$, the group $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ is d-divisible and therefore $(1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})/(1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})^d = 1$. □

For a prime ideal $\mathfrak{p}$, we now fix a local uniformizer $\varpi \in K$ at $\mathfrak{p}$ and set

$$\chi_\mathfrak{p} \colon K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d \longrightarrow \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d, \quad \bar{x} \longmapsto (\overline{v}, \overline{x\varpi^{-v}}) \text{ where } v = v_\mathfrak{p}(x).$$

Note that for every subgroup $V \subseteq K^\times$, the map $\chi_\mathfrak{p}$ induces a map $V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d$, which by abuse of notation we will also denote by $\chi_\mathfrak{p}$.

Proposition 4.6. Assume that S is a set of prime ideals of $\mathcal{O}_K$ and for $d \in \mathbb{Z}_{>0}$ the canonical map

$$K^\times/(K^\times)^d \longrightarrow \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d$$

is injective. Then for every subgroup group $V \subseteq K^\times$ we have

$$V \cap (K^\times)^d = \bigcap_{\mathfrak{p}\notin S} \ker(V \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d),$$

and if S contains the primes dividing d then

$$(V \cap (K^\times)^d)/V^d = \bigcap_{\mathfrak{p}\notin S} \ker(\chi_\mathfrak{p} \colon V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).$$

In particular these equalities hold for $S = \{\mathfrak{p} \mid d \in \mathfrak{p}\}$ and $d = p$ a prime.

Proof. For the first equality note that the assumption implies

$$V \cap (K^\times)^d = V \cap \bigcap_{\mathfrak{p} \notin S} \ker(K^\times \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d) = \bigcap_{\mathfrak{p} \notin S} \ker(V \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d).$$

Thus, using Proposition 4.5, we obtain

$$\begin{aligned}(V \cap (K^\times)^d)/V^d &= (V \cap \bigcap_{\mathfrak{p} \notin S} \ker(K^\times \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d))/V^d \\ &= \bigcap_{\mathfrak{p} \notin S} \ker(V \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d)/V^d \\ &= \bigcap_{\mathfrak{p} \notin S} \ker(V/V^d \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d) \\ &= \bigcap_{\mathfrak{p} \notin S} \ker(\chi_\mathfrak{p} \colon V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d).\end{aligned}$$

The final statement follows from Theorem 4.4. □

Corollary 4.7. Assume that $V \subseteq K^\times$ is finitely generated, and let p be a prime number. Then there exists a constant $c_0 \in \mathbb{R}_{>0}$ such that

$$(V \cap (K^\times)^p)/V^p = \bigcap_{p \notin \mathfrak{p},\, \mathrm{N}(\mathfrak{p}) \le c_0} \ker(\chi_\mathfrak{p} \colon V/V^p \to \mathbb{Z}/p\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^p).$$

Proof. As V is finitely generated, V/V^p is a finite dimensional $\mathbb{F}_p$-vector space. Thus V/V^p is Artinian and the claim follows from Proposition 4.6. □

Proposition 4.8. Let $c \in \mathbb{R}_{>0}$, $V \subseteq K^\times$ finitely generated, let p be a prime number and let m be the $\mathbb{F}_p$-dimension of the intersection

$$\bigcap_{p \notin \mathfrak{p},\, \mathrm{N}(\mathfrak{p}) \le c} \ker(\chi_\mathfrak{p} \colon V/V^p \to \mathbb{Z}/p\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^p) \subseteq V/V^p,$$

and let $\alpha_1, \dots, \alpha_m \in V$ be such that $\overline{\alpha_1}, \dots, \overline{\alpha_m}$ is an $\mathbb{F}_p$-basis of the intersection.

(1) If $m = 0$, then V is p-saturated.
(2) Assume that V is not p-saturated. Then if c is sufficiently large, there exists $1 \le i \le m$ such that α_i is a p-th power.
(3) Assume that V is p-saturated. Then for c sufficiently large we have $m = 0$.

Proof. First note that by Lemma 4.3 (3) the group V is p-saturated if and only if $V \cap (K^\times)^p = V^p$. Denote the intersection of the kernels by W/V^p. (1): Follows since $(V \cap (K^\times)^p)/V^p \subseteq W/V^p$. (2) and (3): For $c = c_0$ as in Corollary 4.7 we have $W/V^p = (V \cap (K^\times)^p)/V^p$. Now apply Lemma 4.3. □

Algorithm 4.9.

- Input: $V \subset K^\times$ finitely generated.
- Output: statement that V is p-saturated or an element α with $[\langle V, \alpha\rangle : V]$ divisible by p.

(1) Let $c \in \mathbb{R}_{>0}$ be any constant.
(2) Determine an $\mathbb{F}_p$-basis $\overline{\alpha_1}, \dots, \overline{\alpha_m}$ of

$$\bigcap_{p \notin \mathfrak{p},\, \mathrm{N}(\mathfrak{p}) \le c} \ker(V/V^p \to \mathbb{Z}/p\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^p).$$

(3) If $m = 0$, return that V is p-saturated.

(4) If $m > 0$, test whether one of the elements α_i is a p-th power. If there exists α with $\alpha^p = \alpha_i$, return α.
(5) Replace c by $2c$ and go to step (2).

Theorem 4.10. Algorithm 4.9 is correct.

Proof. Follows immediately from Proposition 4.8. □

By iterating Algorithm 4.9 one can compute the p-saturation of V and by repeating this for every prime p dividing d, we obtain the d-saturation of V.

Complexity. In this section we prove polynomial time complexity bounds for the S-units and saturation algorithms. We first need an effective version of the Grunwald–Wang theorem. Related work is presented in [53], but the statement we need is different.

Theorem 4.11 (Effective Grunwald–Wang)**.** Assume GRH. Let $d = p^r$ with p prime and $r \geq 1$. Let K be a number field of degree n, and $L = K(\zeta_d)$. Let S be a finite set of primes of K, let $M_S = \prod_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})$, and let $S_p = S \cup \{\mathfrak{p} \mid p\}$. Let

$$c_0 = 18d^2 \left(2\log|\Delta_K| + 6n\log d + \log M_S\right)^2.$$

Let T be the set of prime ideals $\mathfrak{p}$ of K such that

- $\mathfrak{p} \notin S_p$,
- $\mathfrak{p}$ has residue degree 1,
- $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod p$, and
- $\mathrm{N}(\mathfrak{p}) \leq c_0$.

Let $\alpha \in K^\times$ be such that all valuations of α at primes $\mathfrak{p} \notin S_p$ are divisible by d and such that for every $\mathfrak{p} \in T$, the image of α in $K_\mathfrak{p}^\times$ is a d-th power. Then $\alpha \in (L^\times)^d$. If in addition L/K is cyclic, then $\alpha \in (K^\times)^d$.

Proof. Note that the degree of L/K is at most $\varphi(d)$ and the discriminant Δ_L of L satisfies

$$\Delta_L \mid \Delta_K^{\varphi(d)} \Delta_{\mathbb{Q}(\zeta_d)}^n.$$

We first prove that α is a d-th power in L. By contradiction, assume otherwise and let β be a d-th root of α in some extension of L, so that $L(\beta)/L$ is a cyclic extension of degree $d' \neq 1$ dividing d. Let χ be a faithful 1-dimensional character of $\mathrm{Gal}(L(\beta)/L)$, which we see as a ray class group character of L of some conductor $\mathfrak{f}$ by class field theory. Write $\mathfrak{f} = \mathfrak{f}_{\mathrm{tame}}\mathfrak{f}_{\mathrm{wild}}$ where $\mathfrak{f}_{\mathrm{tame}}$ and $\mathfrak{f}_{\mathrm{wild}}$ are coprime and $\mathfrak{f}_{\mathrm{wild}}$ is supported at primes above p. By the assumption on the valuations of α, the extension $L(\beta)/L$ is unramified outside the prime ideals that do not lie above a prime in S_p; indeed, locally at every such prime $\mathfrak{P}$, the extension is generated by a p^i-th root of a unit of $L_\mathfrak{P}$ for some $i \leq r$. Therefore, by [38, Proposition 2.5] applied to $L(\beta)/L$ and χ, we have

$$\log \mathrm{N}(\mathfrak{f}_{\mathrm{wild}}) \leq 2n\varphi(d)(\log p + \log\varphi(d)) \leq 4nd\log d.$$

In addition, ramification is tame at all primes in S not above p, so we have

$$\mathrm{N}(\mathfrak{f}_{\mathrm{tame}}) \leq M_S^d.$$

By [5, Theorem 4], there exists a prime ideal $\mathfrak{P}$ of L that has residue degree 1 (so that $N(\mathfrak{P}) = 1 \bmod d$), does not lie over primes of S_p, such that $\chi(\mathfrak{P}) \neq 1$ and such that

$$\mathrm{N}(\mathfrak{P}) \leq 18\log^2(\Delta_L^2 \mathrm{N}\mathfrak{f}) \leq 18\left(2d\log|\Delta_K| + 6nd\log d + d\log M_S\right)^2 = c_0.$$

In particular, the prime ideal $\mathfrak{p} = \mathfrak{P} \cap K$ lies in T, so α is a d-th power in $K_{\mathfrak{p}}^{\times}$, and *a fortiori* in $L_{\mathfrak{P}}^{\times}$. This implies that $L(\beta)/L$ is completely split at $\mathfrak{P}$, contradicting the fact that $\chi(\mathfrak{P}) \neq 1$. This proves that $\alpha \in (L^{\times})^d$.

Now assume that L/K is cyclic, and let $L' = K(\zeta_p)$. Let $\beta_1, \ldots, \beta_d \in L$ be the d-th roots of α, so that we have $L' \subseteq L'(\beta_i) \subseteq L$ for all i. Since L/L' is a cyclic extension of degree a power of p, its intermediate extensions are linearly ordered, so that we may choose our numbering so that $L'(\beta_1) \subseteq L'(\beta_i)$ for all i.

Assume for contradiction that the cyclic extension $L'(\beta_1)/L'$ is nontrivial. Then as above there exists a nontrivial character χ of $\mathrm{Gal}(L'(\beta_1)/L')$ and a prime ideal $\mathfrak{P}$ of L' of degree 1 (so that $N(\mathfrak{P}) = 1 \bmod p$) such that $\chi(\mathfrak{P}) \neq 1$ and $\mathfrak{p} = \mathfrak{P} \cap K$ lies in T. By hypothesis, α is a d-th power in $K_{\mathfrak{p}}^{\times}$, so that there exists i such that $\beta_i \in K_{\mathfrak{p}}$; since $L'(\beta_1) \subseteq L'(\beta_i)$, this implies $\beta_1 \in L'_{\mathfrak{P}}$, i.e. $L'(\beta_1)/L'$ is completely split at $\mathfrak{P}$, contradicting $\chi(\mathfrak{P}) \neq 1$. This proves that the extension $L'(\beta_1)/L'$ is trivial, i.e. $\beta_1 \in L'$.

We have $\beta_1^d = \alpha$, so that $\alpha^{[L':K]} = \mathrm{N}_{L'/K}(\alpha) = \mathrm{N}_{L'/K}(\beta_1)^d$, and therefore $\alpha^{[L':K]}$ is a d-th power in K. Since $[L' : K]$ is coprime to d, this implies that α is a d-th power in K, as claimed. $\square$

Remark 4.12.

(1) We did not try to optimize the value c_0, only to obtain an explicit value from readily available results in the literature.
(2) For $\mathfrak{p} \notin S_p$, since the valuations of α at $\mathfrak{p}$ is divisible by d and $p \notin \mathfrak{p}$, the assumption that α is a d-th power in $K_{\mathfrak{p}}^{\times}$ is equivalent to the reduction modulo $\mathfrak{p}$ of $\alpha\varpi^{-v}$ being a d-th power, where $v = v_{\mathfrak{p}}(\alpha)$ and $\varpi \in K$ is such that $v_{\mathfrak{p}}(\varpi) = 1$.

Corollary 4.13. Assume GRH. There exists a deterministic polynomial time algorithm, that given m generators of a subgroup V of $K^{\times}$ and an integer d that is either 2 or a power of an odd prime, determines $\alpha_1, \ldots, \alpha_m \in K^{\times}$ such that $\overline{\alpha_1}, \ldots, \overline{\alpha_m}$ generate $(V \cap (K^{\times})^d)/V^d$.

Proof. Let S be the smallest set of primes of K such that $V \subseteq \mathcal{O}_{K,S}^{\times}$, and $M_S = \prod_{\mathfrak{p} \in S} N(\mathfrak{p})$. Then $\log M_S$ is polynomial in the size of the input, and can be bounded in polynomial time without factoring the given generators of V. From Proposition 4.6 and Theorem 4.11 it follows that

$$(V \cap (K^{\times})^d)/V^d = \bigcap_{d \notin \mathfrak{p}, \mathrm{N}(\mathfrak{p}) \leq c_0} \ker(\chi_{\mathfrak{p}} \colon V/V^d \to \mathbb{Z}/d\mathbb{Z} \times k_{\mathfrak{p}}^{\times}/(k_{\mathfrak{p}}^{\times})^d),$$

where $c_0 = 18d^2 \left(2 \log |\Delta_K| + 6n \log d + \log M_S\right)^2$. Since the number and size of the primes $\mathfrak{p}$ are polynomial in the input, this proves the claim. $\square$

We need an extra technical ingredient: a suitably normalized logarithmic embedding to control the height of S-units that appear.

Definition 4.14. Let K be a number field with r_1 real embeddings and r_2 pairs of conjugate complex embeddings. For $x \in K$, the (logarithmic) *height* of x is

$$\mathrm{h}(x) = \sum_{\sigma} \max\Big(0, n_{\sigma} \log |\sigma(x)|\Big) + \sum_{\mathfrak{p}} \max\Big(0, (\log N\mathfrak{p}) v_{\mathfrak{p}}(x)\Big),$$

where σ ranges over the $r_1 + r_2$ conjugacy classes of complex embeddings of K, and $n_\sigma = 1$ or 2 according to whether σ is real or complex, and $\mathfrak{p}$ ranges over nonzero prime ideals of K.

Let S be a finite set of nonzero prime ideals of K. The *logarithmic embedding* attached to S is the map $\mathcal{L}\colon \mathcal{O}_{K,S}^\times \to \mathbb{R}^{r_1+r_2+|S|}$ defined by

$$\mathcal{L}(x) = \Big(n_\sigma \log|\sigma(x)|\Big)_\sigma \times \Big((\log N\mathfrak{p})v_\mathfrak{p}(x)\Big)_\mathfrak{p}.$$

Lemma 4.15. Use the notations of Definition 4.14. For all $x \in \mathcal{O}_{K,S}^\times$, we have

$$\mathrm{h}(x) \le \sqrt{r_1 + r_2 + |S|} \cdot \|\mathcal{L}(x)\|_2 .$$

Proof. This follows immediately from the inequality between the L^1 and L^2 norms. □

As a conclusion to this section, we prove a polynomial time reduction for the computation of S-units from K to its subfields in the presence of a norm relation.

Algorithm 4.16. Assume that the finite group G admits a norm relation with respect to a set $\mathcal{H}$ of subgroups of G.

- Input: a number field K, an injection $G \to \mathrm{Aut}(K)$, a finite G-stable set S of prime ideals of K, and for each $H \in \mathcal{H}$, a $\mathbb{Z}$-basis B_H of $\mathcal{O}_{K^H,S}^\times$.
- Output: a $\mathbb{Z}$-basis of $\mathcal{O}_{K,S}^\times$.

(1) Let $p_1 = 2 < p_2 < \cdots < p_k$ be the prime divisors of $2|G|$.
(2) Let $B = \bigcup_{H\in\mathcal{H}} \bigcup_{g\in G} g(B_H)$.
(3) Let $V \subseteq \mathcal{O}_{K,S}^\times$ be the subgroup generated by B.
(4) $v \leftarrow$ the 2-adic valuation of $|G|^3$.
(5) $V_1 \leftarrow V$.
(6) Repeat v times
  (a) $V_1 \leftarrow \langle V_1, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m}\rangle$ where $\overline{\alpha_1}, \dots, \overline{\alpha_m}$ is a basis of $(V_1 \cap (K^\times)^2)/V_1^2$.
  (b) reduce the basis of V_1 with respect to B in the sense of [36, Lemma 7.1] in the logarithmic embedding $\mathcal{L}$.
(7) For $i = 2$ to k
  (a) $v \leftarrow$ the p_i-adic valuation of $|G|^3$.
  (b) $V_i \leftarrow$ the p_i-saturation of V by taking d-th roots once, where $d = p_i^v$.
(8) $V \leftarrow V_1 \cdots V_l$.
(9) Return a basis of V.

Remark 4.17. Algorithm 4.16 never writes down an explicit norm relation; it only uses the fact that there exists one. Note that for given $\mathcal{H}$, this can be checked in polynomial time, see Section 4.1.

We now prove the bit complexity of Algorithm 4.16. In order to do so, we use the model of Lenstra [34] to encode the input of the algorithm.

Theorem 4.18. Assume GRH. Let G be a finite group and $\mathcal{H}$ a set of subgroups of G. Assume that there exists a norm relation with respect to $\mathcal{H}$. Then Algorithm 4.16 is a deterministic polynomial time algorithm that, on input of

- a number field K,
- an injection $G \to \mathrm{Aut}(K)$,
- a finite G-stable set S of prime ideals of K,

- for each H in $\mathcal{H}$, a basis of the group of S-units of the subfield fixed by H,

returns a $\mathbb{Z}$-basis of the group of S-units of K.

Proof. Denote by n the degree of the number field K over $\mathbb{Q}$. Note that the height and bitsize of elements are bounded relatively to each other by a polynomial in the size of the input. We will therefore measure the size of various quantities in terms of height, without affecting the polynomial time claim of the algorithm.

Let Σ denote the total size of the input. By hypothesis there exists a norm relation in G. Moreover, by Theorem 2.20, we may assume that the denominator of the relation divides $|G|^3$.

Step (1) only requires factoring $|G| = O(n) = O(\Sigma)$ and therefore takes polynomial time.

After Step (2), since the action of automorphisms does not change the height of elements, the total size of B is $O(n\Sigma)$.

Note that in Steps (3)–(9), one can deduce a basis from a generating set of the groups involved in polynomial time: the algorithms of [25] provide a basis of the relations between the generators, and the Hermite normal form [27] allows us to obtain a basis of the group in polynomial time.

Consider a saturation step (6a) or (7b) corresponding to taking d-th roots. By Corollary 4.13 we can determine generators $\overline{\alpha_1}, \ldots, \overline{\alpha_m}$ of $(V \cap (K^\times)^d)/V^d$ in polynomial time. Computing the roots themselves also takes polynomial time. Moreover, in the loop (6), Step (6b) together with Lemma 4.15 make sure that the size of V_1 stays bounded by a polynomial in Σ independent of the number of steps. Therefore the loops (6) and (7) take polynomial time.

The steps (8) and (9) take polynomial time in the data computed at this point.

The correctness of the algorithm follows from Corollary 3.4 (2). $\square$

Remark 4.19. In Theorem 4.18, the S-units of K and its subfields are represented with respect to an integral basis. It is well known that using this, the representation can require exponentially large coefficients with respect to the discriminant of the field. An alternative approach is to represent the S-units of the input as well as the output, that is, of the subfields as well as of $\mathcal{O}_{K,S}^\times$, using compact representations. That the statement remains true using compact representations follows from [12], where it is shown that compact representations can be computed in polynomial time.

4.4. **Computing class groups.** Assume that K/F is a normal extension of number fields with Galois group G that admits a norm relation

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

with $H_i \leq G$, $d \in \mathbb{Z}$, $a_i, b_i \in \mathbb{Z}[G]$. We now describe how to use this to determine the class group of K from the class groups of the subfields K^{H_i}. Let S be a finite set of prime ideals that generates the class group $\mathrm{Cl}(K)$ of K. Assuming the generalized Riemann hypothesis (GRH) we can use for example Bach's bound on the maximal norm of the prime ideals required to generate $\mathrm{Cl}(K)$ and the set $S = \{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq 12 \cdot \log(|\Delta_K|)^2\}$ (see [5]) or one can compute an ad-hoc set S using the methods of [11] or [26].

Using S-units. Using the algorithm of Section 4.3 we can determine a $\mathbb{Z}$-basis of the S-unit group $\mathcal{O}_{K,S}^\times$. Now as in Buchmanns's algorithm [17], consider the map

$$\varphi\colon \mathcal{O}_{K,S}^\times \longrightarrow \mathbb{Z}^{|S|},\ \alpha \longmapsto (v_\mathfrak{p}(\alpha))_{\mathfrak{p}\in S}.$$

Then $\mathrm{Cl}(K) \cong \mathrm{coker}(\varphi)$, since the sequence $\mathcal{O}_{K,S}^\times \xrightarrow{\varphi} \mathbb{Z}^{|S|} \xrightarrow{\psi} \mathrm{Cl}(K) \to 0$ is exact, where $\psi((v_\mathfrak{p})_{\mathfrak{p}\in S}) = [\prod_{\mathfrak{p}\in S}\mathfrak{p}^{v_\mathfrak{p}}]$.

Direct computation. We now consider the map $\mathrm{Cl}(K)\otimes\mathbb{Z}[\frac{1}{d}] \to \bigoplus_{i=1}^{\ell}\mathrm{Cl}(K^{H_i})\otimes\mathbb{Z}[\frac{1}{d}]$, $[\mathfrak{a}] \mapsto ([\mathrm{N}_{K/K^{H_i}}(\mathfrak{a}^{b_i})])$, which by Proposition 3.7 is an isomorphism. Hence $\mathrm{Cl}(K)\otimes\mathbb{Z}[\frac{1}{d}] \cong \langle\Phi(\mathfrak{p}) \mid \mathfrak{p}\in S\rangle\otimes\mathbb{Z}[\frac{1}{d}]$. In particular, if one is interested only in the p-part of the class group for some prime p not dividing d or if the denominator d of the norm relation is equal to 1, this provides a second way to determine the structure of the class group.

4.5. **Class groups of abelian extensions.** In this section we describe a Las Vegas algorithm based on the ideas above to compute the class group of an abelian field. Contrary to Algorithm 4.16 and its variants, the algorithm we present here never computes an explicit d-th root, and therefore completely avoids using LLL, and does not need a Bach-type bound to certify its correctness, making it very fast in practice. This is possible because we are only asking for the structure of the class group and not for explicit units, S-units or generators of ideals, which would be computationally harder.

Let K/F be a normal extension of number fields with abelian Galois group G.

Write $G \cong C \times Q$ where C is the largest cyclic factor of G. According to Theorem 2.28, we will have the following three cases.

(1) The order $|Q|$ has at least two distinct prime divisors. Write $Q \cong P_1 \times \cdots \times P_k$ with P_i abelian p_i-groups with p_i distinct primes. This case does not require any saturation, and reduces to computations of class groups in various subfields K_j/F with Galois groups that are isomorphic to subgroups of $C \times P_i$.
(2) The group Q is a nontrivial p-group for some prime p. Then we apply the methods from Section 4.3 , using a relation with denominator a power of p. This case requires p-saturation, and reduces to computations of class groups and units in various subfields K_i/F with Galois groups that are isomorphic to subgroups of C.
(3) We have $Q = 1$: then the norm relation method does not apply, so we simply use Buchmann's algorithm [17] (or any other algorithm that can compute the class group and units).

The algorithms corresponding to cases (1) and (2) are the following.

Algorithm 4.20. Assume $|Q|$ has at least two distinct prime divisors. Write $Q \cong P_1 \times P_2 \times \cdots \times P_k$ with P_i abelian p_i-groups (case 1 above).

- Input: K/F with Galois group G.
- Output: the class group $\mathrm{Cl}(K)$.

(1) Use Theorem 2.28 to write a norm relation with denominator 1, involving a collection (H_j) of subgroups of G such that each G/H_j is isomorphic to a subgroup of some $C \times P_i$.
(2) Compute the subfields $K_j = K^{H_j}$.

(3) Compute the class groups of the subfields K_j, and for each subfield, a set S_j of prime ideals that generates the class group.
(4) Let $S = \bigcup_j \{\mathfrak{p}\mathcal{O}_K \mid \mathfrak{p} \in S_j\}$.
(5) Compute the image $\mathcal{C}$ of S in $\bigoplus_j \mathrm{Cl}(K_j)$ under the map Φ of Proposition 3.7.
(6) Return $\mathcal{C}$.

Remark 4.21. The ideals in S are not necessarily prime, but we only use the property that their images generate the class group $\mathrm{Cl}(K)$.

Proposition 4.22. Algorithm 4.20 correctly computes the class group of K.

Proof. By the surjectivity part of Proposition 3.7, S generates the class group of K. By the injectivity part of Proposition 3.7, $\mathcal{C}$ is isomorphic to the class group of K. This prove the correctness of the algorithm. □

Algorithm 4.23. Assume Q is a nontrivial p-group (case 2 above).

- Input: K/F with Galois group G.
- Output: the class group $\mathrm{Cl}(K)$.

(1) Use Theorem 2.28 to write a norm relation with denominator d a power of p, involving a collection (H_i) of subgroups of G such that each G/H_i is isomorphic to a subgroup of C.
(2) Compute the subfields $K_i = K^{H_i}$, and their class groups and units.
(3) Compute the coprime-to-p part of $\mathrm{Cl}(K)$ as follows.
 (a) For each K_i, compute a set S_i of prime ideals that generates the coprime-to-p part of the class group.
 (b) Let $S' = \bigcup_i \{\mathfrak{p}\mathcal{O}_K \mid \mathfrak{p} \in S_i\}$.
 (c) Compute the image $\mathcal{C}_{p'}$ of S' in $\bigoplus_i \mathrm{Cl}(K_i)_{p'}$ under the map Φ of Proposition 3.7.
(4) Let $h_{p'} = |\mathcal{C}_{p'}|$.
(5) Compute the roots of unity W in K.
(6) By seeing the relation as a Brauer relation using Proposition 2.7, compute $\mathrm{HR}_K = h_K \mathrm{Reg}_K$ from the same quantity in the subfields using Proposition 3.8 and the analytic class number formula.
(7) Compute the subgroup U_0 of $\mathcal{O}_K^\times$ generated by $\bigcup_i \mathcal{O}_{K_i}^\times$, and the regulator R_0 of U_0; let r_0 be the number of generators of U_0.
(8) Initialize a set T of prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) \equiv 1 \bmod d$.
 The primes in T will be used to detect d-th powers.
(9) Initialize a set $S_\mathbb{Q}$ of prime numbers, and compute the set S of all prime ideals of K above the primes in $S_\mathbb{Q}$.
 We hope that S will generate the p-part of the class group.
(10) Compute the p-part of $\mathrm{Cl}(K)$ as follows.
 (a) Compute the subgroup U_S of $\mathcal{O}_{K,S}^\times$ generated by $\bigcup_i \mathcal{O}_{K_i,S}^\times$; let r be the number of generators of U_S.
 (b) Compute the map

$$f\colon \mathbb{Z}^r \longrightarrow U_S \longrightarrow \mathbb{Z}^S \oplus \bigoplus_{\mathfrak{p}\in T} \mathbb{F}_\mathfrak{p}^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^{|S|+|T|}$$

 given by the valuations at prime ideals in S and discrete logarithms in $\mathbb{F}_\mathfrak{p}^\times$ for $\mathfrak{p} \in T$.

(c) Compute $V_S = \ker f$ and $V_0 = \ker\big(f\colon \mathbb{Z}^{r_0} \to U_0 \to (\mathbb{Z}/d\mathbb{Z})^T\big)$.
(d) Compute $u = \big|V_0/\big(V_0^d \cdot (W \cap V_0)\big)\big|$.
(e) Compute the subgroup V generated by the image of $U_S \to \mathbb{Z}^S$ and $\frac{1}{d}$ times the image of $V_S \to U_S \to \mathbb{Z}^S$.
(f) Compute the p-part $\mathcal{C}_p$ of $\mathbb{Z}^S/V$.
(g) Let $h_p = |\mathcal{C}_p|$.
(h) If $h_{p'}R_0h_p/u > \mathrm{HR}_K/2$, then return $\mathcal{C}_{p'} \times \mathcal{C}_p$; otherwise increase T and $S_{\mathbb{Q}}$ and go back to (10a).

Remark 4.24. As before, the ideals in S' are not necessarily prime. In our implementation, which is restricted to $F = \mathbb{Q}$, we initialize T with $|T| = 10 +$ unit rank of K, and we increase it by adding random prime ideals of norm $\approx (d\log|\Delta_K|)^2$; we initialize $S_{\mathbb{Q}}$ with $S_{\mathbb{Q}} = \emptyset$, and we increase it by adding random primes of norm $\approx (\log|\Delta_K|)^2$ that split completely in K.

Proposition 4.25. If Algorithm 4.23 terminates, then its output is correct.

Proof. By the surjectivity part of Proposition 3.7, S' generates the coprime-to-p part of the class group of K. By the injectivity part of Proposition 3.7, $\mathcal{C}_{p'}$ is isomorphic to the coprime-to-p part of the class group of K; in particular $h_{p'} = |\mathrm{Cl}_{p'}|$. At Step 10a, U_S satisfies $\mathcal{O}_{K,S}^\times/U_S$ has exponent dividing d by Corollary 3.4. Therefore, the subgroup V of $\mathbb{Z}^S$ computed at Step 10e contains the image of $\mathcal{O}_{K,S}^\times$; in particular h_p is a divisor of the p-part of the subgroup of the class group generated by S, and equals the p-class number if and only if S generates the p-part of $\mathrm{Cl}(K)_p$ and V equals the image of $\mathcal{O}_{K,S}^\times$. In addition Reg_K is a p-power multiple of R_0/u by Corollary 3.4. Therefore, if the algorithm terminates, then $h_{p'}R_0h_p/u = h_K\mathrm{Reg}_K = \mathrm{HR}_K$, the group $\mathcal{C}_p$ is isomorphic to $\mathrm{Cl}(K)_p$, and the output is correct. □

Remark 4.26. It may happen that Algorithm 4.23 does not terminate if K has an obstruction to the Hasse principle for d-th powers. These obstructions are characterized by the Grunwald–Wang theorem, and can only happen if $d \geq 8$ is a power of 2. We currently do not know how to avoid this without computing an actual d-th root in K.

Remark 4.27. If one only needs the structure of the class group of K as an abstract abelian group, as opposed to having explicit ideal classes as generators, one may replace the use of Proposition 3.7 in Algorithms 4.20 and 4.23 by [14, Proposition 2.2 and Corollary 1.4].

4.6. **Unconditional computations.** Computations of class groups are typically done under GRH and later certified by a different algorithm. The algorithms of Section 4.5 are oblivious to the method used to compute the information in the subfields: if the class group, regulator, unit and S-unit groups of the subfields are correct, then so is the output of Algorithms 4.20 and 4.23. However, it can take a very long time to fully certify the information from the subfields. In this section, we describe a method to certify the class group structure assuming only partial information on the subfields. This is easy in Algorithm 4.20: since the class group is computed via Proposition 3.7 or Remark 4.27, it is correct as soon as the class groups of the subfields are correct. Throughout this section, we will refer to the notations in Algorithm 4.23, such as U_0, V_S, etc. It will be convenient to have, for various objects, a separate notation for the correct one and the one that was computed; we will denote the latter with a tilde: for instance $\mathcal{O}_K^\times$ is the unit group of $\mathcal{O}_K$ and $\widetilde{\mathcal{O}_K^\times}$ is the subgroup that was computed.

Proposition 4.28. Let K/F be a normal extension of number fields with Galois group G as in Algorithm 4.23. Let

$$c_0 \operatorname{Ind}_{G/1} \mathbf{1}_1 = \sum_i c_i \operatorname{Ind}_{G/H_i}(\mathbf{1}_{H_i})$$

be the Brauer relation used in Step 6 with $c_i \in \mathbb{Z}$ and $c_0 > 0$. Assume the following:

(1) for all i, the computed class group $\widetilde{\mathrm{Cl}(K_i)}$ is correct;
(2) for all i, the computed group of roots of unity in K_i is correct, and the computed group of roots of unity in K is correct;
(3) for all i, the computed unit group $\widetilde{\mathcal{O}_{K_i}^\times}$ is a subgroup of $\mathcal{O}_{K_i}^\times$ of finite index at most $B_i \geq 1$ and of index coprime to p;
(4) for all i, the computed S-unit group $\widetilde{\mathcal{O}_{K_i,S}^\times}$ is a subgroup of $\mathcal{O}_{K_i,S}^\times$ of finite index coprime to p;
(5) at the end of the algorithm, we have

$$\left|\left(\frac{\widetilde{h_{p'}}\widetilde{R_0}\widetilde{h_p}/\tilde{u}}{\widetilde{\mathrm{HR}_K}}\right)^{c_0} - 1\right| < d^{-(|S|+r_0)c_0} \prod_i B_i^{-|c_i|}.$$

Then the class group output by Algorithm 4.23 is correct.

Proof. Since the coprime-to-p-part of the class group is computed via Proposition 3.7 or Remark 4.27, it is correct by Assumption (1). We now focus on the p-part. Let U_0 be the subgroup of $\mathcal{O}_K^\times$ generated by the $\mathcal{O}_{K_i}^\times$, and define U_S similarly for S-units. Let R_0 be the regulator of U_0. Let h_p and $h_{p'}$ be the p-part and coprime-to-p-part of the class number of K. Let $u = [\mathcal{O}_K^\times/W : U_0/W]$ where W is the group of roots of unity in K. Let $\mathrm{HR}_K = h_K \mathrm{Reg}_K$. We have

$$h_{p'} R_0 h_p / u = \mathrm{HR}_K. \tag{3}$$

Let

$$\rho_1 = \frac{\widetilde{h_{p'}}\widetilde{R_0}\widetilde{h_p}/\tilde{u}}{\widetilde{\mathrm{HR}_K}}$$

be the quantity appearing in Assumption (5), which we expect to be 1. Since the coprime-to-p-part of the class group is correct, we have $\widetilde{h_{p'}} = h_{p'}$. Let w_i be the number of roots of unity in K_i and w_0 the number of roots of unity in K. By the analytic class number formula and Proposition 3.8, we have

$$\left(\frac{\mathrm{HR}_K}{w_0}\right)^{c_0} = \prod_i \left(\frac{h_{K_i}\mathrm{Reg}_{K_i}}{w_i}\right)^{c_i}.$$

By Assumptions (1) and (2) and Step 6 we have

$$\left(\frac{\widetilde{\mathrm{HR}_K}}{w_0}\right)^{c_0} = \prod_i \left(\frac{h_{K_i}\widetilde{\mathrm{Reg}_{K_i}}}{w_i}\right)^{c_i}.$$

The quotient of these two equations gives two expressions for a quantity that we denote by ρ_2:

$$\rho_2 = \left(\frac{\widetilde{\mathrm{HR}_K}}{\mathrm{HR}_K}\right)^{c_0} = \prod_i \left(\frac{\widetilde{\mathrm{Reg}_{K_i}}}{\mathrm{Reg}_{K_i}}\right)^{c_i}.$$

Then by Assumption (3), ρ_2 is a positive rational number whose numerator and denominator are bounded by $\prod_i B_i^{|c_i|}$ and such that $v_p(\rho_2) = 0$. Let

$$\rho_3 = \frac{\widetilde{R_0}\widetilde{h_p}/\tilde{u}}{R_0 h_p/u},$$

which is a positive rational number since $\widetilde{U_0}$ is a finite index subgroup of U_0. By Assumption (3), the ratio $\frac{\widetilde{R_0}}{R_0}$ is an integer coprime to p. Both $h_p/\widetilde{h_p}$ and $u/\tilde{u}$ are rational numbers that are powers of p. Moreover, by Assumption (4), they are integers (see also proof of Proposition 4.25): $\widetilde{h_p}$ can be strictly smaller than h_p only if S does not generate the p-part of the class group or if T is insufficient to correctly detect the d-th powers in $\mathcal{O}_{K,S}^\times$, yielding extra elements in the computed group of principal ideals; similarly $\tilde{u}$ can be strictly smaller than u only if T is insufficient to correctly detect the d-th powers in $\mathcal{O}_K^\times$. In particular, if $h_p = \widetilde{h_p}$ and $u = \tilde{u}$ then the computed p-part of the class group is correct. The ratio $\rho_4 = \dfrac{h_p/u}{\widetilde{h_p}/\tilde{u}}$ is therefore also an integer and a power of p; moreover, we have $\rho_4 \le d^{|S|+r_0}$ by construction. By equation (3) we have

$$\rho_1^{c_0} = \rho_2^{-1}\rho_3^{c_0}.$$

Putting together the previous observations, we obtain that $\rho_1^{c_0}$ is a rational number with denominator at most

$$B = d^{(|S|+r_0)c_0}\prod_i B_i^{|c_i|}$$

and we have $v_p(\rho_1) = v_p(\rho_3) = -v_p(\rho_4)$. Finally, by Assumption (5), we have $|\rho_1^{c_0} - 1| < B^{-1}$, so that $\rho_1^{c_0} = 1$. This proves that $v_p(\rho_4) = -v_p(\rho_1) = 0$ and therefore $\rho_4 = 1$, proving that the computed p-part of the class group of K is correct. □

Theorem 4.29. The class numbers and class groups in Tables 1 and 2 are correct.

Proof. We apply our Pari/GP implementation of Algorithms 4.20 and 4.23 with GRH-conditional computations in the subfields. Then we verify the hypotheses of Proposition 4.28: Assumption (2) is automatically guaranteed by the Pari/GP functions (as this can be done in polynomial time); Assumptions (1), (3) and (4) are checked with a modified version of the Pari/GP function `bnfcertify`; Assumption (5) is checked by computing the relevant quantity up to sufficiently high accuracy. This proves that the class group structures are correct. We compute the minus part of the class number by the analytic class number formula [54, Theorem 4.17], and we deduce the plus part of the class number from it. □

5. Numerical examples

We have implemented the algorithms from Section 4 for computing S-unit and class groups in Hecke [21] and Pari/GP [49]. More precisely, we implemented in Pari/GP the algorithms of Section 4.5 (with the variant of Remark 4.27) that are restricted to abelian groups, and in Hecke the algorithms of Sections 4.1, 4.3 and 4.4 that can handle arbitrary groups. The Pari/GP implementation is available at [41]. In this section we report on some numerical examples obtained using these implementations. All the computations performed in this section assume GRH.

We begin with a non-abelian example taken from the database of Klüners and Malle ([30]).

Example 5.1. The splitting field K of the irreducible polynomial $f = x^{10} + x^8 - 4x^2 + 4 \in \mathbb{Q}[x]$ has Galois group $C_2 \times A_5$ and discriminant $2^{210} \cdot 17^{80} \approx 10^{161}$. Our implementation in Hecke shows that the class group of K is trivial. As we use the algorithm using S-units of Section 4.4, we also obtain generators for the unit group and obtain the value

$$5892293459976073400931514779079 58.37876...$$

for the regulator of K. The algorithm uses a relation of $C_2 \times A_5$ with denominator 1 involving subfields of degree at most 60. The computation takes 6 hours on a single core machine.

The remaining examples all concern number fields with abelian Galois group. Here, we use the Algorithms of Section 4.5.

Example 5.2. Let $K = \mathbb{Q}(\zeta_{216})$, which has Galois group over $\mathbb{Q}$ isomorphic to $C_{18} \times C_2 \times C_2$, degree 72 and discriminant $\approx 10^{129}$. Our Pari/GP implementation computes in 6 seconds that the class group of K is isomorphic to $C_{1714617} \cong C_{3^2} \times C_{19} \times C_{37} \times C_{271}$. Pari/GP computes the same result in 15 minutes, and magma in 5 hours. Our algorithm uses a relation with denominator 4, and starts by computing the class group and units of 8 subfields of degree up to 18. It then starts with $S = \emptyset$, which turns out to be a generating set for the 2-class group of K. The algorithm therefore only needs to compute a single kernel modulo 4 to determine the correct class group at 2; the units of the subfields generate a subgroup of index 2^{11} of $\mathcal{O}_K^\times$.

Example 5.3. Let $K = \mathbb{Q}(\zeta_{6552})$ which has Galois group over $\mathbb{Q}$ isomorphic to $C_{12} \times C_6^2 \times C_2^2$, degree 1728 and discriminant $2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$. Our Pari/GP implementation computes in 4.2 hours that the class group of K is isomorphic to

$$\begin{aligned}
&C_e \times C_{123903346647650690244963498417984355147621683400320}\\
&\times C_{582777587574759236929319 2320} \times C_{20985241981415724230 40}\\
&\times C_{33847164486154393920} \times C_{7383876252480} \times C_{101148989760}^2\\
&\times C_{50574494880}^2 \times C_{276363360}^5 \times C_{7469280}^2 \times C_{3734640}^8 \times C_{196560}^2\\
&\times C_{98280} \times C_{32760}^4 \times C_{6552}^{26} \times C_{3276}^2 \times C_{252} \times C_{84}^3 \times C_{12}^{29} \times C_6^8 \times C_2^{11}
\end{aligned}$$

where

$$\begin{aligned}
e \quad = \quad &349380029706737059104248223565319692883897548638392856641627842\\
&662891732318286799812329621077189995594165744361859090214550165\\
&7345555588705897299490131506759682326353657 60,
\end{aligned}$$

and that $h_{6552}^+ = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13$. Our algorithm uses a relation with denominator 1 involving 62 subfields of degree at most 192. The computations in those subfields recursively uses relations with denominators supported at a single primes (2 or 3), involving a total of 672 subfields of degree at most 12.

References

[1] L. M. Adleman. Factoring numbers using singular integers. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, page 64–71, New York, NY, USA, 1991. Association for Computing Machinery. 22, 23

[2] M. Aoki and T. Fukuda. An algorithm for computing p-class groups of abelian number fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 56–71. Springer, Berlin, 2006. 4

[3] E. Artin. Linear mappings and the existence of a normal basis. In *Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948*, pages 1–5. Interscience Publishers, Inc., New York, 1948. 2, 19

[4] E. Artin and J. Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original. 23

[5] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990. 25, 28

[6] A. Bartel. On Brauer-Kuroda type relations of S-class numbers in dihedral extensions. *J. Reine Angew. Math.*, 668:211–244, 2012. 3

[7] A. Bartel and B. de Smit. Index formulae for integral Galois modules. *J. Lond. Math. Soc. (2)*, 88(3):845–859, 2013. 3

[8] A. Bartel and T. Dokchitser. Brauer relations in finite groups II: Quasi-elementary groups of order $p^\alpha q$. *J. Group Theory*, 17(3):381–393, 2014. 7, 11

[9] A. Bartel and T. Dokchitser. Brauer relations in finite groups. *J. Eur. Math. Soc.*, 17(10):2473–2512, 2015. 7, 11

[10] J. Bauch, D. Bernstein, H. de Valence, T. Lange, and C. van Vredendaal. Short generators without quantum computers: the case of multiquadratics. In *Advances in cryptology—EUROCRYPT 2017. Part I*, volume 10210 of *Lecture Notes in Comput. Sci.*, pages 27–59. Springer, Cham, 2017. 2, 7

[11] K. Belabas, F. Diaz y Diaz, and E. Friedman. Small generators of the ideal class group. *Math. Comp.*, 77(262):1185–1197, 2008. 28

[12] J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 893–902. ACM, New York, 2016. 28

[13] J.-F. Biasse and C. van Vredendaal. Fast multiquadratic S-unit computation and application to the calculation of class groups. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 103–118. Math. Sci. Publ., Berkeley, CA, 2019. 2, 7

[14] R. Boltje. Class group relations from Burnside ring idempotents. *J. Number Theory*, 66(2):291–305, 1997. 3, 31

[15] W. Bosma and B. de Smit. Class number relations from a computational point of view. In *Computational algebra and number theory (Milwaukee, WI, 1996)*, volume 31, no. 1-2, pages 97–112. Elsevier, 2001. 1, 21

[16] R. Brauer. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachr.*, 4:158–174, 1951. 1, 3

[17] J. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres*, pages 27–41, Paris, 1988-89. 29

[18] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. 22

[19] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. 13

[20] G. L. Dirichlet. Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes. Première partie. *J. Reine Angew. Math.*, 24:291–371, 1842. 1

[21] C. Fieker, W. Hart, T. Hofmann, and F. Johansson. Nemo/hecke: Computer algebra and number theory packages for the julia programming language. In M. Burr, C. Yap, and M. Safey El Din, editors, *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017*, pages 157–164. ACM, 2017. 3, 33

[22] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993. 21

[23] A. Fröhlich and C. T. C. Wall. Equivariant Brauergroups in algebraic number theory. In *Colloque de Théorie des Nombres (Univ. de Bordeaux, Bordeaux, 1969)*, pages 91–96. Bull. Soc. Math. France, Mém No. 25. Soc. Math. France, 1971. 1

[24] T. Funakura. On Artin theorem of induced characters. *Comment. Math. Univ. St. Paul.*, 27(1):51–58, 1978/79. 9, 15

[25] G. Ge. *Algorithms related to multiplicative representations of algebraic numbers*. PhD thesis, University of California, Berkeley, 1993. 28

[26] L. Grenié and G. Molteni. Explicit bounds for generators of the class group. *Math. Comp.*, 87(313):2483–2511, 2018. 28

[27] J.L. Hafner and K.S. McCurley. Asymptotically fast triangulation of matrices over rings. In *SODA '90: Proceedings of the first annual ACM-SIAM symposium on Discrete algorithms*, pages 194–200, Philadelphia, PA, USA, 1990. Society for Industrial and Applied Mathematics. 28

[28] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989. 2

[29] E. Kani and M. Rosen. Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties. *J. Number Theory*, 46(2):230–254, 1994. 2

[30] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001. 34

[31] A. Kontogeorgis. Actions of Galois groups on invariants of number fields. *J. Number Theory*, 128(6):1587–1601, 2008. 2

[32] S. Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950. 1, 3

[33] A. K. Lenstra. Factoring polynomials over algebraic number fields. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 245–254. Springer, Berlin, 1983. 22

[34] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992. 21, 27

[35] A. Lesavourey, T. Plantard, and W. Susilo. Short Principal Ideal Problem in multicubic fields. *J. Math. Cryptol.*, 14(1):359–392, 2020. 2, 7

[36] D. Micciancio and S. Goldwasser. *Complexity of lattice problems*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 2002. 27

[37] J. C. Miller. Class numbers of real cyclotomic fields of composite conductor. *LMS J. Comput. Math.*, 17(suppl. A):404–417, 2014. 3, 4

[38] M. R. Murty, V. K. Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988. 25

[39] J. Neukirch. *Algebraic number theory*. Comprehensive Studies in Mathematics. Springer-Verlag, 1999. ISBN 3-540-65399-6. 23

[40] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2008. 23

[41] A. Page. abelianbnf, 2020. Available at https://hal.inria.fr/hal-02961482. 33

[42] H. Park. *Idempotent relations and the conjecture of Birch and Swinnerton-Dyer*. PhD thesis, Brown University, 1990. 2

[43] H. Park. Relations among Shafarevich-Tate groups. *Sūrikaisekikenkyūsho Kōkyūroku*, 998:117–125, 1997. 2

[44] C. J. Parry. Class number formulae for bicubic fields. *Illinois J. Math.*, 21(1):148–163, 1977. 2, 7

[45] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1989. 22, 23

[46] H. P. Rehm. Über die gruppentheoretische Struktur der Relationen zwischen Relativnormabbildungen in endlichen Galoisschen Körpererweiterungen. *J. Number Theory*, 7:49–70, 1975. 2

[47] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series.* The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor. 13

[48] D. Simon. *Équations dans les corps de nombres et discriminants minimaux.* PhD thesis, Université Bordeaux I, 1998. 22

[49] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.13.1`, 2021. available from `http://pari.math.u-bordeaux.fr/`. 3, 33

[50] H. Wada. On the class number and the unit group of certain algebraic number fields. *J. Fac. Sci. Univ. Tokyo Sect. I*, 13:201–209 (1966), 1966. 2, 7

[51] C. T. C. Wall. On the structure of finite groups with periodic cohomology. In *Lie groups: structure, actions, and representations*, volume 306 of *Progr. Math.*, pages 381–413. Birkhäuser/Springer, New York, 2013. 2, 10

[52] C. D. Walter. Kuroda's class number relation. *Acta Arith.*, 35(1):41–51, 1979. 1, 2, 8

[53] S. Wang. Grunwald-Wang theorem, an effective version. *Sci. China Math.*, 58(8):1589–1606, 2015. 4, 25

[54] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. 33

[55] J. A. Wolf. *Spaces of constant curvature*. AMS Chelsea Publishing, Providence, RI, sixth edition, 2011. 2

[56] H. Yu. Idempotent relations and the conjecture of Birch and Swinnerton-Dyer. *Math. Ann.*, 327(1):67–78, 2003. 2

Appendix A. Class groups of large cyclotomic fields

Table 2. Class groups of cyclotomic fields $\mathbb{Q}(\zeta_n)$

n conductor, $\varphi(n)$ degree, h^+ plus part of class number, Cl list of cyclic factors of the class group, with multiplicities denoted by exponents.

n	$\varphi(n)$	h^+	Cl
255	128	1	$[198604775280, 85]$
272	128	2	$[38972318856432, 48, 16^2]$
320	128	1	$[2679767564295, 51, 17^2]$
340	128	1	$[189394569680, 80^2]$
408	128	2	$[383350665840, 48, 16^2, 2]$
480	128	1	$[208430880, 1680, 84, 21]$
273	144	1	$[112080696, 11544, 8^2, 4^3, 2^2]$
315	144	1	$[58787820, 606060, 28, 4]$
364	144	1	$[1212120, 4680, 1560^2, 78, 2]$
456	144	1	$[4536718103988, 1197, 171, 19]$
468	144	1	$[130450320, 102960, 468, 117, 3^2]$
504	144	4	$[39312, 13104, 252^3, 126, 2^3]$
520	192	4	$[3008481840, 808080, 21840, 80, 16, 8^3, 4^5, 2^5]$
560	192	1	$[334945469854703482320, 302640, 60, 3^2]$
624	192	1	$[5435580272293080, 79560, 79560, 195, 65, 5]$
720	192	1	$[145097043589680, 261908020920, 390, 15]$
780	192	1	$[3256946160, 208^3, 104, 8^5, 4^4, 2^4]$
840	192	1	$[4316155222640, 404040, 1560, 780, 2^2]$
455	288	1	$[2552186819979516720, 39582182640, 161616, 7696, 3848, 52^4, 4, 2^4]$
585	288	1	$[20973979753397601680869341964560, 7405922160, 10920, 5460, 52, 2^2]$
728	288	20	$[127601328297438646560, 241506720, 622440, 4680^3, 312^2, 24, 12^2, 6^3, 2^3]$
936	288	16	$[380292996258447608175840, 4957112160, 6552^2, 3276^3, 156^2, 12^2]$
1008	288	16	$[13191784813235120785056, 2542176, 6552^2, 3276^4, 156^2, 52, 2^2]$
1092	288	1	$[1873781327428920, 23030280, 10920^2, 2184, 312^2, 104^2, 8^4, 4^5, 2^6]$
1260	288	1	$[302534211670334280, 8464152747960, 32760, 10920, 2184, 168^2, 8, 4^2, 2^4]$
1560	384	8	$[397816187272397451623520, 98585760, 1616160, 43680, 21840, 1040^4, 208, 16^3, 8^7, 4^{10}, 2^{10}]$
1680	384	1	$[20781830230484468879265337592380391572320, 156767520, 22395360, 605280, 3120, 1560^3, 40, 4^2, 2]$
2520	576	208	$[197258297436388965346129923485464425191214071085120, 112607968430745627840, 366503875920, 2424240, 65520, 32760^5, 6552, 2184^3, 312, 8^4, 4^5, 2^{14}]$

Department of Mathematics and Statistics, University of South Florida, 4202 East Fowler Ave, CMC342, Tampa, FL 33620-5700, USA
Email address: biasse@usf.edu

Fachbereich Mathematik, Technische Universitat Kaiserslautern, 67663 Kaiserslautern, Germany
Email address: fieker@mathematik.uni-kl.de

Department Mathematik, Universität Siegen, Postfach, 57068 Siegen, Germany
Email address: tommy.hofmann@uni-siegen.de

INRIA, Univ. Bordeaux, CNRS, IMB, UMR 5251, F-33400 Talence, France
Email address: aurel.page@inria.fr