COEFFICIENT REDUCTION FOR UNITS OF INTEGRAL GROUP RINGS

Abstract. For every finite group G and prime p, we give an arithmetic description of the image of $U(\mathbb{Z}G) \to U(\mathbb{F}_pG)$, a terminating construction of integral representatives for its kernel cosets, and a finite generating algorithm for the kernel. The principal kernel is described up to computable finite index by central units and norm-one congruence groups. This is an internally verified algorithmic candidate for Kourovka 13.1, awaiting human review; adequacy to any stronger intended structural classification and historical priority remain for human assessment.

Problem and claimed scope

Kourovka Problem 13.1, proposed by R. Zh. Aleev, reads as follows in the *Kourovka Notebook*, arXiv:1401.0300v45.

> Let $U(K)$ denote the group of units of a ring K. Let G be a finite group, $\mathbb{Z}G$ the integral group ring of G, and $\mathbb{Z}_pG$ the group ring of G over the residues modulo a prime number p. Describe the homomorphism from $U(\mathbb{Z}G)$ into $U(\mathbb{Z}_pG)$ induced by reducing the coefficients modulo p. More precisely, find the kernel and the image of this homomorphism and an explicit transversal over the kernel.

We write $\mathbb{F}_p$ for the residues modulo p, $R^\times$ for the unit group of a ring R, and $\rho : U(\mathbb{Z}G) \to U(\mathbb{F}_pG)$ for coefficient reduction.

Main result. *The constructions below give, for every finite G and prime p, a terminating algorithm returning a finite generating list for* $\ker\rho$*, the complete finite image, and actual integral coefficient vectors for a transversal. There is no restriction to normalized units, abelian groups, or primes coprime to $|G|$. Part I supplies the arithmetic image criterion, transversal and kernel extensions; Part II supplies finite kernel generators and the central-factor refinement.*

The classical inputs are local maximal-order structure, local norm lifting, the Hasse–Schilling–Maass theorem, strong approximation for norm-one groups, Dirichlet's unit theorem, the character description of real components, and the integral-normalizer algorithm. Sources are cited at their uses. The argument combines explicit residue norm tests, finite positive norm fibers, conductor gluing, prescribed-norm lifts, finite Schreier constructions and central-power corrections. No priority or practical complexity claim is made.

I. Arithmetic image criterion and transversal

I.1. The complete nondefinite-factor criterion

Let F be a number field with integers O, $\mathcal{A}$ a central simple F-algebra, and M a maximal O-order. Let Σ be the real places at which $\mathcal{A}$ is a matrix algebra over $\mathbb{H}$. Put

$$E_\Sigma = \{\epsilon \in O^\times : \sigma(\epsilon) > 0 \text{ for } \sigma \in \Sigma\}.$$

Assume either $\mathcal{A} = F$, or $\mathcal{A}$ has an archimedean completion which is not a division algebra. For a positive integer N let $\mathcal{R}_N = M/NM$ and let

$$V_\Sigma(N) = \text{image}(E_\Sigma \to (O/NO)^\times).$$

Date: Draft: 18 September 2026.

Theorem I.1. *The reduced norm induces a map* $\overline{n} : \mathcal{R}_N^\times \to (O/NO)^\times$, *and*

$$\operatorname{image}(M^\times \to \mathcal{R}_N^\times) = \overline{n}^{-1}(V_\Sigma(N)). \tag{I.1}$$

For $\mathcal{A} = F$ this is the definition of $V_\Sigma(N)$. In other cases it is the explicit arithmetic form of the stable-image obstruction on this maximal order. In particular no generators of $U(\mathbb{Z}G)$, nor their reductions, enter (I.1).

Local lemma. *For a finite completion* F_v *and* $M_v = M \otimes O_v$,

$$\operatorname{nrd}(M_v^\times) = O_v^\times, \qquad \operatorname{nrd}(1 + \pi_v^k M_v) = 1 + \pi_v^k O_v \quad (k \geq 1). \tag{I.2}$$

Indeed M_v is conjugate to $M_r(O_{D_v})$. One may see this without assuming a global matrix-order normal form: M_v stabilizes the right O_{D_v}-lattice obtained by applying an O_v-generating list of M_v to $O_{D_v}^r$. Row reduction over the division valuation ring gives a basis for this full lattice. Its endomorphism order contains M_v, so maximality makes them equal. A maximal unramified subfield L of the local division algebra D_v has degree $\deg(D_v)$; its integers lie in O_{D_v} [7, pp. 27–28, Definition 2.3.0.27]. The diagonal embedding $z \mapsto \operatorname{diag}(z, 1, \ldots, 1)$ has reduced norm $\mathrm{N}_{L/F_v}(z)$. The norm from an unramified extension maps units onto units and $1 + \pi_v^k O_L$ onto $1 + \pi_v^k O_v$ [4, III.2.2 and its proof]. For the latter assertion, the leading term at each successive precision is the surjective residue-field trace; successively correct the error and take the convergent product. This works also at residue characteristic dividing $\deg(D_v)$. The reverse inclusion in (I.2) follows from integrality of reduced characteristic coefficients.

The same local integral-matrix description shows that reduced norm is unchanged modulo NO_v when its argument is unchanged modulo NM_v. More explicitly, O_{D_v} is a free right O_L-lattice of rank $\deg(D_v)$, so left multiplication embeds $M_r(O_{D_v})$ into an integral matrix algebra over O_L; the determinant is its reduced norm. The coefficients descend to O_v, and divisibility by N descends because O_L is unramified over O_v. These local congruences prove that $\overline{n}$ is well-defined globally. Units of $\mathcal{R}_N$ lift locally to units of M_v at every $v \mid N$, since NM_v lies in the Jacobson radical. Their norms are consequently units modulo NO.

Proof of (I.1). Necessity is immediate from reduced norm and its real positivity. For sufficiency choose $c \in \mathcal{R}_N^\times$ and $\epsilon \in E_\Sigma$ with $\overline{n}(c) = \epsilon \bmod NO$. At each $v \mid N$ choose a unit lift a_v of c. By (I.2) there is $t_v \in 1 + NM_v$ with $\operatorname{nrd}(t_v) = \epsilon / \operatorname{nrd}(a_v)$; set $b_v = a_v t_v$. For v not dividing N choose $b_v \in M_v^\times$ with norm ϵ, again by (I.2). Thus $b = (b_v)$ is a finite adele, integral and invertible everywhere, with norm ϵ and prescribed residue c.

The Hasse–Schilling–Maass theorem gives $x \in \mathcal{A}^\times$ with $\operatorname{nrd}(x) = \epsilon$ [2, Theorem 2]. Strong approximation for $\mathcal{A}^1 = \ker(\operatorname{nrd} : \mathcal{A}^\times \to F^\times)$, with all infinite places removed, says that $\mathcal{A}^1$ is dense in the finite norm-one adeles [8, Remark 28.6.11]. Apply it to the nonempty open set of z for which xz belongs to $M_v^\times$ for every finite v and xz is congruent to c modulo NM_v for $v \mid N$. It contains $x^{-1}b$. For a global such z, $u = xz$ belongs to $M^\times$ and reduces to c. This proves (I.1). The hypotheses for this density are precisely those stated before (I.1), apart from the field case, already handled separately. □

Stable formulation. For every maximal order M in a central simple number-field algebra, including a definite quaternion algebra, stabilization gives

$$\operatorname{coker}\bigl(K_1(M) \to K_1(M/NM)\bigr) = (O/NO)^\times / V_\Sigma(N). \tag{I.1s}$$

Indeed apply Theorem I.1 to $M_n(M)$ for $n \geq 2$. Its underlying algebra has a nondivision archimedean completion, its real norm-sign conditions are still Σ, and its integral units are $\mathrm{GL}_n(M)$. The local lemma and CRT show that its residual reduced norm is onto $(O/NO)^\times$. Its unit image is the full inverse image of $V_\Sigma(N)$, hence is normal and contains all commutators. Passing to the stable group and then its abelianization proves (I.1s). Thus (I.1) is precisely the

unstabilized norm criterion on the nondefinite factors, and (I.5) below records the additional unstable information needed on the definite factors. No assertion that stable and unstable images agree on those factors is made.

I.2. Ray-class formulation and effective lifts

The finite group $V_\Sigma(N)$ is computed from ordinary number-field units: take a finite generating list, impose the finitely many sign equations at Σ, then reduce the resulting generators modulo NO. Retain a word in those generators for each element of $V_\Sigma(N)$. Thus each accepted c comes with an actual $\epsilon \in E_\Sigma$.

For completeness such a central-unit generating list does not require an oracle. Enumerate algebraic integers and test $\mathrm{N}_{F/\mathbb{Q}}(u) \in \{1,-1\}$. Let $\varrho = r_1 + r_2 - 1$. Search for ϱ units whose logarithmic embedding vectors are linearly independent in the product-formula hyperplane; dovetail all tuples and increasing interval precision to certify a nonzero minor. Dirichlet guarantees eventual success (and the rank-zero case starts with the empty list) [3, Theorems 5.1, 5.9 and Proposition 5.8]. Their logarithmic parallelepiped gives an explicit upper bound C_{bd} for the absolute values of all conjugates of a unit reduced into it. Enumerate the finitely many algebraic integers whose conjugates have absolute value at most C_{bd}, using a larger rational enclosure if needed, and keep those of absolute norm 1. Together with the initial independent units these generate every unit: multiplying an arbitrary unit by powers of the initial list puts its log vector in that parallelepiped. The finite bounded enumeration includes all torsion. Exact arithmetic and certified embedding bounds give a terminating procedure. Finite sign and residue kernels are then ordinary abelian-group computations. The lattice property invoked here is the usual logarithmic form of Dirichlet's theorem.

There is also the exact sequence

$$E_\Sigma \longrightarrow (O/NO)^\times \longrightarrow \mathrm{Cl}_{(N,\Sigma)}(F) \longrightarrow \mathrm{Cl}_\Sigma(F) \longrightarrow 1. \tag{I.3}$$

Here the first class group has finite modulus NO and sign conditions Σ; the second has only sign conditions. To define the middle map, lift a residue t to an element a of O positive at Σ and send t to $[(a)]$. A positive lift exists by adding a sufficiently large positive integer multiple of N. Two such lifts have positive ratio congruent to 1 at primes over N, so the map is well-defined. Its kernel consists exactly of residues of E_Σ: if $[(a)]$ is trivial, write $(a) = (b)$ with b positive and $b = 1 \bmod NO$ locally at primes over N; then a/b is the required positive unit. The last map and its exactness follow by removing the finite congruences. Therefore (I.1) may equivalently be tested by vanishing of this explicit ray-class element. Formula (I.3) is proved here, not used as an unquoted external input.

Fix an ordered $\mathbb{Z}$-basis of M and order its coefficient vectors first by maximum absolute coefficient, then lexicographically within each finite box shell. Once ϵ has been selected, enumerate vectors u in this order until

$$u = c \bmod NM, \qquad \mathrm{nrd}(u) = \epsilon. \tag{I.4}$$

Theorem I.1 proves termination. Since ϵ is a unit, the reduced characteristic equation gives $u^{-1} \in M$, so (I.4) returns an actual unit. This is a search in a specified norm fiber with guaranteed existence after the finite arithmetic image test; it does not first generate $U(\mathbb{Z}G)$.

I.3. Generality of the norm criterion

The nondefinite hypothesis occurs only in the strong-approximation step. Every matrix algebra of matrix size > 1 qualifies, including matrices over a totally definite quaternion algebra. A division algebra of degree > 2 also qualifies at infinity; the only noncommutative exceptions are

totally definite quaternion division algebras over totally real centres. Quaternion algebras with both ramified and split real places qualify as well.

Nicholson uses the stronger-looking convention that the real semisimple algebra has no simple $\mathbb{H}$ factor [5, p. 3]. For $\mathbb{Q}G$ this agrees with excluding precisely the totally definite quaternion division factors: if an irreducible complex character gives a real $\mathbb{H}$ factor, its degree is 2 and its Frobenius–Schur indicator is -1. The indicator is rational and Galois invariant, since $\nu(\chi) = |G|^{-1}\sum_{g\in G}\chi(g^2)$. Every conjugate is therefore quaternionic, all conjugates of its character field are real, and the rational component is a quaternion division algebra ramified at all real embeddings. Conversely such a rational component gives $\mathbb{H}$ at each real embedding. This argument uses the standard character/real-component correspondence, not a convention change for arbitrary semisimple $\mathbb{Q}$-algebras [1, §4.1, Problem 4.1, Definition 4.3 and Theorem 4.4].

The theorem itself applies more broadly than Nicholson's real convention: it uses the explicit strong-approximation hypothesis stated in Section I.1. No claim of failure is made outside that hypothesis. The remaining compact factors are handled directly in Section I.4, without applying approximation.

I.4. All-G conductor formula

Let $\Lambda = \mathbb{Z}G$ and let $\Omega = \prod_j M_j$ be a maximal order in $\mathbb{Q}G$ containing Λ. Choose a positive integer m with $m\Omega \subseteq \Lambda$. Set $N = pm$, $J = N\Omega$, $A_{\mathrm{res}} = \Omega/J$, $B_{\mathrm{res}} = \Lambda/J$ inside A_{res}, and let $\pi : B_{\mathrm{res}} \to \Lambda/p\Lambda$ be the natural map. In particular $J \subseteq p\Lambda$. Split the simple factors into $\mathcal{E}$ (those in Theorem I.1, including fields) and $\mathcal{Q}$ (totally definite quaternion division factors).

For $j \in \mathcal{E}$ set $C_j = \overline{n}_j^{-1}(V_{\Sigma_j}(N))$. For $i \in \mathcal{Q}$ write O_i for the integers of the totally real centre F_i. Choose representatives ϵ_{it} of $O_i^{\times,+}/(O_i^{\times})^2$ and set

$$\begin{aligned} W_i &= \bigcup_t \{w \in M_i : \mathrm{nrd}(w) = \epsilon_{it}\}, \\ C_i &= \mathrm{image}(O_i^{\times})\,\mathrm{image}(W_i) \quad \text{in } (M_i/NM_i)^{\times}. \end{aligned} \tag{I.5}$$

Every W_i is finite and can be explicitly enumerated: the positive definite rational quadratic form $q_i^+(w) = \mathrm{Tr}_{F_i/\mathbb{Q}}(\mathrm{nrd}(w))$ bounds the coefficient vectors of w by $q_i^+(w) = \mathrm{Tr}(\epsilon_{it})$. If Q_{Gram} is its Gram matrix in a $\mathbb{Z}$-basis, then $|x_k|^2 \le \mathrm{Tr}(\epsilon_{it})(Q_{\mathrm{Gram}}^{-1})_{kk}$ supplies finite coordinate bounds. Test the exact norm equation within these bounds. Dirichlet gives a finite list of square classes and computes the central residue subgroup from number-field units. Retain actual central-unit words and actual w for all residues in C_i.

Indeed $M_i^{\times} = O_i^{\times}W_i$: for a unit u, write its positive norm as $\epsilon_{it}a^2$ and take $w = a^{-1}u$. Conversely all aw in this expression have unit norm and inverse in M_i. Thus each C_j, for either kind of factor, is exactly the image of $M_j^{\times}$. Put $C_{\mathrm{res}} = \prod_j C_j$ and $\mathcal{D} = B_{\mathrm{res}}^{\times} \cap C_{\mathrm{res}}$.

Theorem I.2. *For every finite G and every prime p,*

$$\mathrm{image}\big(U(\mathbb{Z}G) \to U(\mathbb{F}_pG)\big) = \pi(\mathcal{D}). \tag{I.6}$$

There is no restriction on p relative to $|G|$, m, or a component discriminant. All objects on the right are finite residue rings, number-field unit residue groups (equivalently the ray-class tests (I.3)), and the finite positive norm sets W_i. In particular (I.6) contains no original $U(\mathbb{Z}G)$ image oracle.

Proof. A unit of Λ reduces to an element of $B_{\mathrm{res}}^{\times}$ and of C_{res}. Conversely if $b \in \mathcal{D}$, choose $u \in \Omega^{\times}$ lifting it componentwise by (I.4) and (I.5). As b is represented by Λ and $J \subseteq \Lambda$, $u \in \Lambda$. Because $b^{-1} \in B_{\mathrm{res}}$, the same reasoning puts $u^{-1} \in \Lambda$. Hence $u \in \Lambda^{\times}$, and reducing further gives $\pi(b)$. This proves (I.6). □

Explicit transversal. Enumerate the finite rings A_{res} and B_{res} from their additive bases and multiplication tables, compute $\mathcal{D}$ by the preceding finite tests, and compute $H_{\mathrm{im}} = \pi(\mathcal{D})$. For every $h \in H_{\mathrm{im}}$ choose the first $b \in \mathcal{D}$ with $\pi(b) = h$ in a fixed ordering. Lift its $\mathcal{E}$-coordinates by (I.4), its $\mathcal{Q}$-coordinates by the stored aw in (I.5), and reassemble the resulting u in Ω. The proof of (I.6) proves $u \in \Lambda^\times$. Output this one u for each h; choose $u = 1$ for $h = 1$. The coefficient vectors in the group basis are integral and form a transversal over the reduction kernel. Every search terminates, and the choice rules make the output unambiguous after fixing the arithmetic input bases and number-field fundamental units.

I.5. Structural kernel

Let $D_0 = \{b \in \mathcal{D} : \pi(b) = 1\}$; choose a lift $s_b \in \Lambda^\times$ as above for every $b \in D_0$. Put $\Gamma_j(N) = \ker(M_j^\times \to (M_j/NM_j)^\times)$ and $\Gamma = \prod_j \Gamma_j(N)$. Since $J \subseteq p\Lambda$, $\Gamma \subseteq \Lambda^\times$ and reduces to 1 modulo $p\Lambda$. The reduction map gives

$$1 \longrightarrow \Gamma \longrightarrow \ker\rho \longrightarrow D_0 \longrightarrow 1, \qquad \ker\rho = \coprod_{b\in D_0} s_b\Gamma. \tag{I.7}$$

The groups Γ_j have explicit arithmetic descriptions. For $j \in \mathcal{E}$ set

$$H_j(N) = \{x \in M_j : \mathrm{nrd}(x) = 1,\ x = 1 \bmod NM_j\},$$
$$E_{\Sigma_j}(N) = \{\epsilon \in E_{\Sigma_j} : \epsilon = 1 \bmod NO_j\}.$$

Then the norm map yields an exact sequence

$$1 \longrightarrow H_j(N) \longrightarrow \Gamma_j(N) \longrightarrow E_{\Sigma_j}(N) \longrightarrow 1. \tag{I.8}$$

Surjectivity follows from the proof of Theorem I.1 with prescribed ϵ and $c = 1$. Thus generators for the finitely generated abelian group $E_{\Sigma_j}(N)$ have explicit lifts by (I.4). The group $H_j(N)$ is the integral-point group of an explicitly given norm-one equation with linear congruences in the maximal-order lattice. For field factors $H_j(N) = 1$. For $i \in \mathcal{Q}$ the direct description is

$$\Gamma_i(N) = \{aw : w \in W_i,\ a \in O_i^\times,\ aw = 1 \bmod NM_i\}. \tag{I.9}$$

For a fixed w, the permissible a are either empty or a coset of the central unit subgroup congruent to 1 modulo NO_i, determined in a finite residue group. Hence (I.9) is a finite union of computable abelian-unit cosets.

Equations (I.7)–(I.9) are a kernel description in independent arithmetic terms; they do not present $H_j(N)$ by finitely many generators. In the algorithmic interpretation of the problem, a full output package requires such generating lists (or a separately verified algorithm for them). Part I supplies a complete image criterion and actual transversal, and an exact structural kernel reduction. Part II supplies the finite generating lists.

II. Arithmetic kernel generators and central factors

We complete the arithmetic description by computing finite generating lists for every group

$$H_j(N) = \{u \in M_j : \mathrm{nrd}(u) = 1,\ u = 1 \bmod NM_j\},$$

and hence for the original reduction kernel. The algorithm takes the maximal-order data from Part I, not generators of $U(\mathbb{Z}G)$. For $N \geq 3$ the principal kernel is also an explicit finite extension of a direct product of central units and norm-one groups; totally definite quaternion factors contribute only central units.

Let $\Lambda = \mathbb{Z}G$, let $\Omega = \prod_j M_j$ be a maximal order in $\mathbb{Q}G$ containing Λ, and write $\mathcal{A}_j = \mathbb{Q}Ge_j$ for its rational simple factors. Let F_j be the centre, O_j its ring of integers, and d_j the degree of

$\mathcal{A}_j$ over F_j. Fix bases and a positive integer m with $m\Omega \subseteq \Lambda$. Put $N = pm$ and $J = N\Omega$, so $J \subseteq p\Lambda$.

II.1. Finite generators for each maximal-order unit group

For one factor $\mathcal{A} = \mathbb{Q}Ge$, $M = M_j$, right multiplication by $g^{-1}e$ defines an integral unimodular matrix R_g on the lattice M. Indeed ge and $g^{-1}e$ belong to M. The set $F_{\mathrm{mat}} = \{R_g : g \in G\}$ is an explicit finite matrix group; repeated matrices are discarded. With this convention $R_gR_h = R_{gh}$.

Use Opgenorth's algorithm to compute a finite symmetric generating list S_W for $W = N_{\mathrm{GL}(M)}(F_{\mathrm{mat}})$ [6, §§1–3, Theorems 2.2 and 3.6(i)]. The exact known input used is: the full integral normalizer of an explicitly given finite unimodular group has a terminating generator algorithm, returning actual integral matrices. Conjugation maps W to the finite permutation group of F_{mat}. Compute its image by breadth-first multiplication and retain a lift of every image element. Finite Schreier yields generators of $C_{\mathrm{cent}} = C_{\mathrm{GL}(M)}(F_{\mathrm{mat}})$. It is not necessary that W induce every automorphism of F_{mat}.

For completeness, C_{cent} is the left regular image of $M^\times$. A $\mathbb{Q}$-linear map X_{lin} commuting with F_{mat} commutes with right multiplication by all of $\mathcal{A}$, since $\{ge : g \in G\}$ spans $\mathcal{A}$. Hence $X_{\mathrm{lin}}(a) = X_{\mathrm{lin}}(e)a$ for every $a \in \mathcal{A}$. If X_{lin} is an integral lattice automorphism, $u = X_{\mathrm{lin}}(e)$ belongs to M and its inverse map similarly equals left multiplication by an element of M. Thus $u \in M^\times$. Conversely every left multiplication by a unit of M belongs to C_{cent}. Reading $X_{\mathrm{lin}}(e)$ from each computed generator of C_{cent} therefore gives a finite symmetric list S generating *all* of $M^\times$.

The normalizer input is independent of the original group-ring unit group. It uses only the projected finite group acting on M and the Opgenorth theorem; no generic real-arithmetic or simple-module oracle is needed.

II.2. Removing the infinite norm image by central powers

Write $E = O_F^\times$, $d = \deg_F(\mathcal{A})$, and $U = M^\times$. Obtain a finite central-unit list by the Dirichlet lattice algorithm already described in Section I.2. Define $q : U \to E/E^d$ by $q(u) = \mathrm{nrd}(u)E^d$. This is well-defined because reduced norms of units of M are central units. Its target is finite. Compute $Q_{\mathrm{nrd}} = q(U)$ from $q(S)$, with lifts $t_\xi \in U$ and $t_1 = 1$, and set

$$B_S = \{t_\xi s t_{\xi q(s)}^{-1} : \xi \in Q_{\mathrm{nrd}},\ s \in S\}.$$

The list B_S generates $U_0 = \ker q$. Choose $a_b \in E$ with $a_b^d = \mathrm{nrd}(b)$ for every $b \in B_S$. Then

$$S_1 = \{a_b^{-1}b : b \in B_S\} \ \cup\ \{\zeta 1_{\mathcal{A}} : \zeta \in F,\ \zeta^d = 1\} \tag{II.1}$$

generates $U^1 = \{u \in M : \mathrm{nrd}(u) = 1\}$.

Proof. Scalar units are central and $\mathrm{nrd}(a1_{\mathcal{A}}) = a^d$, so every displayed generator has norm 1. Write $h \in U^1$ as a word in B_S and their inverses. Substituting $b = a_b(a_b^{-1}b)$ and moving all scalar factors to the front gives $h = ah_0$, where h_0 is generated by the first part of (II.1), and $a \in E$. Taking norms gives $a^d = 1$, so the second part of (II.1) accounts for a. No multiplicative root selection or splitting assumption is made. □

All central computations terminate without a presentation of E. From a generating list $e_1, \dots, e_k$, list the d^k products with exponents $0, \dots, d-1$. Two products have the same class in E/E^d precisely when $T^d -$ their ratio has a root in F. Exact number-field polynomial factorization decides this and finds a root. Such a root and its inverse are integral over O_F, so it belongs to E. The same operation finds each a_b and all roots of $T^d - 1$ in F. Redundant unit generators are therefore harmless. For $d = 1$ the output group is trivial.

II.3. Congruence generators

Make S_1 symmetric. Enumerate its image Q_N in $(M/NM)^\times$ and retain word lifts $v_y \in U^1$, with $v_1 = 1$. Then

$$S_N = \{v_y s v_{y\,\mathrm{red}_N(s)}^{-1} : y \in Q_N,\ s \in S_1\} \tag{II.2}$$

generates $H_M(N)$. Here red_N denotes reduction modulo NM. There are at most $N^{\mathrm{rank}_{\mathbb{Z}} M}$ residue vectors, so breadth-first enumeration terminates when the queue becomes empty.

Both Schreier assertions used here follow from the same identity. For a word $s_1 \cdots s_\ell$ in a kernel, insert a chosen lift of the image of each prefix between successive letters. The resulting factors $t_{\text{image(prefix)}}\, s_i\, t^{-1}_{\text{image(next prefix)}}$ telescope to the word. Each factor is in the kernel, proving both inclusions.

Alternatively, finite Schreier applied directly to S and reduction modulo NM gives a finite list G_M generating

$$\Gamma_M(N) = \ker(M^\times \to (M/NM)^\times). \tag{II.3}$$

Use (II.2) for the required norm-one generators and (II.3) for the shortest assembly of the original kernel. No strong-approximation hypothesis is required for these algorithms, and all d, signatures and N work.

II.4. Reassembling the original reduction kernel

Set $A_{\mathrm{res}} = \Omega/J$, $B_{\mathrm{res}} = \Lambda/J$ inside A_{res}, and let $\pi : B_{\mathrm{res}} \to \Lambda/p\Lambda$ be the natural map. From the factor-unit lists compute the finite image C_{res} of $\Omega^\times$ in $A_{\mathrm{res}}^\times$ and retain unit lifts of every $c \in C_{\mathrm{res}}$. Set

$$D_0 = \{b \in B_{\mathrm{res}}^\times \cap C_{\mathrm{res}} : \pi(b) = 1\}.$$

Every $b \in D_0$ has an explicit lift $s_b \in \Omega^\times$. It belongs to Λ because its residue is in B_{res} and $J \subseteq \Lambda$. Likewise $s_b^{-1} \in \Lambda$ since $b^{-1} \in B_{\mathrm{res}}$. Thus s_b belongs to the original reduction kernel K. Take $s_1 = 1$.

Reduction modulo J gives the exact sequence

$$1 \longrightarrow \prod_j \Gamma_j(N) \longrightarrow K \longrightarrow D_0 \longrightarrow 1. \tag{II.4}$$

In particular K is generated by the lists G_{M_j} from (II.3), embedded one factor at a time, together with $\{s_b : b \in D_0\}$. Indeed multiplying an arbitrary kernel element by the inverse of its selected residue lift puts it in $\prod_j \Gamma_j(N)$. All these units have actual integral coefficient vectors in the original group basis, since $J \subseteq p\Lambda$. The norm criterion of Part I can still compute C_{res} arithmetically and its image/transversal remain unchanged.

Sections II.1–II.4 prove the complete finite-generator addition. Their only non-elementary generator inputs are the normalizer algorithm and the central number-field unit algorithm.

II.5. The central factors of the principal kernel

Torsion lemma. If $\mathcal{R}$ is an order in a finite-dimensional rational algebra and $N \geq 3$, then $\ker(\mathcal{R}^\times \to (\mathcal{R}/N\mathcal{R})^\times)$ is torsion-free. To prove this, represent a finite-order $u = 1 + Nx$ on the integral lattice $\mathcal{R}$ by its left multiplication $U_{\mathrm{mat}} = I + NX_{\mathrm{tor}}$. The matrix U_{mat} is diagonalizable over $\mathbb{C}$ with roots of unity as eigenvalues, so X_{tor} is diagonalizable and its eigenvalues have absolute value at most $2/N < 1$. Every eigenvalue α is an algebraic integer, all of whose conjugates are also eigenvalues of X_{tor}. If α were nonzero, its algebraic norm would be a nonzero integer of absolute value less than 1. Therefore $X_{\mathrm{tor}} = 0$ and $u = 1$.

For a central simple factor write

$$E(N) = \{a \in O_F^\times : a = 1 \bmod NO_F\}, \qquad \Delta_M(N) = E(N)H_M(N).$$

The equality $M \cap F = O_F$ implies that scalar congruence modulo NM is exactly congruence modulo NO_F. Both factors in $\Delta_M(N)$ lie in $\Gamma_M(N)$; they commute, and their intersection is the group of dth roots of unity in $E(N)$. For $N \geq 3$ this is trivial by the torsion lemma. Hence multiplication gives the *internal direct product*

$$\Delta_M(N) = E(N) \times H_M(N). \tag{II.5}$$

Moreover

$$\Gamma_M(N)/\Delta_M(N) \cong \mathrm{nrd}(\Gamma_M(N))/E(N)^d. \tag{II.6}$$

Indeed a unit of $\Gamma_M(N)$ whose norm is a^d for $a \in E(N)$ becomes an element of $H_M(N)$ after division by a. Conversely every element of $\Delta_M(N)$ has norm in $E(N)^d$. The quotient in (II.6) is finite: $E(N)$ has finite index in E, and E is finitely generated. It is computable from the norm images of the generators (II.3) in $E/E(N)^d$. For the nondefinite factors, the norm theorem of Part I identifies the numerator more explicitly as $E_\Sigma(N)$; that identification is not needed for (II.5)–(II.6).

Definite quaternion refinement. If $\mathcal{A}$ is a totally definite quaternion division algebra and $N \geq 3$, then

$$H_M(N) = 1, \qquad \Gamma_M(N) = E(N). \tag{II.7}$$

The group M^1 is finite: at every real embedding its elements lie on the compact norm-one sphere, and M is a lattice. Thus $H_M(N) = 1$ by the torsion lemma. The canonical quaternion conjugation preserves M, since $\overline{x} = \mathrm{trd}(x) - x$ and $\mathrm{trd}(x) \in O_F$. If $u \in \Gamma_M(N)$, then $\overline{u}$ also does, and $u\overline{u}^{-1} \in H_M(N)$. It is therefore 1, so $u = \overline{u}$ is central. Conversely $E(N)$ is visibly contained in $\Gamma_M(N)$.

These conclusions apply to the conductor modulus used here whenever G is nontrivial. The trivial central idempotent $e_{\mathrm{triv}} = |G|^{-1}\sum_{g\in G} g$ belongs to every maximal order containing Λ: adjoining this central integral idempotent would otherwise enlarge the order. Since $me_{\mathrm{triv}} \in \Lambda$, $|G|$ divides m. Consequently $N = pm \geq 4$ for nontrivial G. For $G = 1$ the unit group is $\{1, -1\}$, so its reduction kernel is immediate.

Thus (II.4) is a finite extension of the explicit direct product

$$P = \left(\prod_j E_j(N)\right) \times \left(\prod_{j\in\mathcal{E}} H_j(N)\right). \tag{II.8}$$

Here P is normal in K: central units are fixed under conjugation, and each $H_j(N)$ is normal in $M_j^\times$. Its index is

$$[K : P] = |D_0| \prod_{j\in\mathcal{E}} [\mathrm{nrd}(\Gamma_j(N)) : E_j(N)^{d_j}]. \tag{II.9}$$

All finite factors in (II.9) are computable as above. Each $E_j(N)$ is free abelian of the Dirichlet rank of F_j. In particular the compact quaternion factors contribute no nonabelian principal congruence group at the conductor modulus. This refines the finite-union description of those factors in Part I without changing its image criterion.

Scope for human review

Together the two parts supply a terminating finite kernel-generator list, the finite image, and actual integral representatives for every finite group and prime. The result is an algorithmic candidate; adequacy to any stronger intended structural classification and historical priority require human assessment.

References

1. Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina, *Introduction to representation theory*, Author's lecture notes, 2011, 10 January 2011; Section 4.1.
2. Daniel Goldstein and Murray Schacher, *Norms in central simple algebras*, Pacific Journal of Mathematics **292** (2018), no. 2, Article beginning on p. 373; Theorem 2.
3. J. S. Milne, *Algebraic number theory*, Author's course notes, Theorems 5.1 and 5.9; Proposition 5.8.
4. ———, *Class field theory*, Author's course notes, version 3.10, Chapter III, Proposition 2.2 and its proof, pp. 80–81.
5. John Nicholson, *A cancellation theorem for modules over integral group rings*, Accepted manuscript, UCL Discovery, 2020, Online/in-press record; the convention on p. 3 is used.
6. Jürgen Opgenorth, *Dual cones and the Voronoi algorithm*, Experimental Mathematics **10** (2001), no. 4, 599–608.
7. Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, Ph.D. thesis, Université de Bordeaux, 2014, Defended 15 July 2014.
8. John Voight, *Quaternion Algebras, chapter 28*, Graduate Texts in Mathematics 288, Springer, 2021, Remark 28.6.11.

Methods and AI disclosure

This note was produced by an automated research pipeline using `gpt-6-astra` through Codex. Each of the two claim packages passed two independent blind adversarial verification passes and a separate citation audit. The proofs are faithfully converted from the verified source texts, with notation disambiguated. Independent Python and GAP corroboration completed 6/6 cases for Part I and 7/7 finite analogues and 2/2 positive central-unit-rank cases for Part II. No computation is a proof premise or a full implementation of the normalizer algorithm. Scripts, transcripts, source records and reports are preserved under `problems/13.1/` in the accompanying repository; the source texts are `solution/r2-structural.md` and `solution/r3-kernel-generators.md`, with reviews `verification/r2c1b-v1.md`, `r2c1b-v2.md`, `r3c1b-v1.md` and `r3c1b-v2.md`. Bounded novelty searches found no exact prior package and do not certify originality. This is an internally verified candidate awaiting human review, with no claim of Notebook acceptance.