

FINITE GROUPS OF MATRICES OVER QUADRATIC NUMBER FIELDS.

DANIIL YURSHEVICH

ABSTRACT. In this paper we give an algorithm to determine all finite matrix groups over a number field. Our algorithm is based on the representation theory of finite groups.

INTRODUCTION

The aim of this paper is to give an algorithm to compute finite matrix groups over a number field. Study of finite matrix groups with rational coefficients begun already in XIX century. Minkowski ([16]) proved that the order of a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ is bounded by the constant

$$M(n) := \prod_{p \in \mathbb{P}} p^{\lfloor \frac{n}{p-1} \rfloor + \lfloor \frac{n}{p(p-1)} \rfloor + \lfloor \frac{n}{p^2(p-1)} \rfloor + \dots}.$$

Schur proved that the same bound holds for the order of any finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ under a weaker assumption that only traces of elements are rational.

Finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ are well known, subgroups of $\mathrm{GL}_3(\mathbb{Q})$ where classified in [31] (up to [2]). In higher dimensions primitive irreducible maximal finite subgroups and maximal irreducible finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ were studied in numerous papers (see fi. [6, 7, 8, 12, 15, 17, 24, 23, 22, 21, 20, 19] and the references cited there). Current version of Magma ([3]) contains database Rational Maximal Finite Matrix Groups of dimensions ≤ 31 (it contains in total 354 groups).

Schur ([27]) proved a similar bound $S(n, K)$ of the order of a finite group of matrices with traces in a number field K . If K is a number field with class number equal 1, for instance this holds for $K = \mathbb{Q}$, any finite subgroup of $\mathrm{GL}_n(K)$ is conjugated to a subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$.

Our research was motivated by applications in algebraic geometry, many examples of Calabi-Yau manifolds were constructed as a crepant resolution of singularities of a quotient E^n/G of a Cartesian power E^n of an elliptic curve E by a finite group G acting on E^n and preserving the canonical form ω_{E^n} . Any finite group $G \subset \mathrm{GL}_n(\mathcal{O})$ of matrices with entries in the endomorphism ring $\mathcal{O} = \mathrm{End}(E)$ of E acts in the obvious way on E^n , the action preserve the canonical form when G is contained in the special linear group $\mathrm{SL}_n(\mathcal{O})$. The endomorphism ring of an elliptic curve equals $\mathbb{Z}$ (ordinary) or an order in an imaginary quadratic field (Complex Multiplication).

All examples constructed in that way for finite subgroups $G \subset \mathrm{SL}_n(\mathbb{Z})$ with $n \leq 3$ are well studied [1, 4, 10]. In an arbitrary dimension n we have examples with an action on E^n of $\mathbb{Z}_2^{n-1}$ (for an arbitrary E), $\mathbb{Z}/4^{n-1}$ (for elliptic curves with $j(E) = 1728$), $\mathbb{Z}/3^{n-1}$ and $\mathbb{Z}/6^{n-1}$ (for elliptic curves with $j(E) = 0$) ([5, 11]).

Similar construction exists also for the elliptic curve E_7 with the Weierstrass equation

$$y^2 = 4x^3 + 21x^2 + 28x.$$

The curve E_7 has a complex multiplication by

$$\tau = \zeta_7 + \zeta_7^2 + \zeta_7^4 = \frac{1}{2}(-1 + \sqrt{-7}).$$

The matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & \tau + 1 \\ 0 & 1 & \tau \end{pmatrix}$$

is similar to the diagonal matrix $\text{diag}(\zeta_7, \zeta_7^2, \zeta_7^4)$ and acts on $(E_7)^3$. The quotient of E_7^3 by the cyclic group generated by this matrix has a crepant resolution of singularities which is a Calabi-Yau threefold (for details see [25]). Elliptic curves with complex multiplication corresponds to orders in quadratic field, by the Stark-Heegner theorem there are nine quadratic number fields with class number one and thirteen elliptic curves with CM defined over $\mathbb{Q}$.

The paper is organized as follows, in section 1 we collect information on representations of finite groups that we shall use in this paper. In section 2. we define the Weil restriction of scalars, in section 4. the Schur index of a character and characterize characters afforded by a representation defined over a given number field. In Section 5. we review details of the Schur bound and the reduction method. Finally, section 5. contains description of our algorithm, summary of results for quadratic fields with class number equal one and $n = 3$, details of computations for $\text{GL}_3(\mathbb{Q}[\sqrt{-19}])$ and $\text{SL}_3(\mathbb{Q}[\sqrt{-19}])$.

1. PRELIMINARIES

In this section we will introduce basic notions of representation theory of finite groups. Let G be a finite group.

Definition 1.1. Linear representation of the group G in a vector space V is a homomorphism $\rho : G \rightarrow \text{Aut}(V)$ of the group G into the space of automorphisms of V . Equivalently representation ρ is given by a family $\{\rho_g\}_{g \in G}$ s.t. $\rho_{gh} = \rho_g \rho_h$ for all $g, h \in G$

We call a representation *faithful* if it is injective as homomorphism of groups. Space V is called *representation space*. In this paper we will only be interested in the case where G is finite and vector space is finite dimensional so let's assume further that these conditions hold.

Definition 1.2. Let ρ and ρ' be linear representations of a Group G in vector spaces V and W , respectively. A morphism from ρ to ρ' is a linear map $\tau : V \rightarrow W$ such that for each $g \in G$ we have $\tau \rho_g = \rho'_g \tau$. If additionally τ is an isomorphism then we say that ρ and ρ' are isomorphic.

Here are some examples of representations:

- (1) *Trivial representation.* Take $V = \mathbb{C}$ and $\rho_g = 1$ for all $g \in G$.
- (2) *Regular representation.* Take $V = \mathbb{C}^{|G|}$ and define ρ_g on basis $\{e_h\}_{h \in G}$ of V as $\rho_g(e_h) = e_{gh}$ for all $g, h \in G$.
- (3) *Direct sum of representations.* Having two representations ρ and ρ' in V and W we define the direct sum $\rho \oplus \rho'$ follows: representation space of $\rho \oplus \rho'$ is $V \oplus W$ and $(\rho \oplus \rho')(v, w) = \rho(v) \oplus \rho'(w)$.

Definition 1.3. Let ρ be a linear representation of a group G in a vector space V . The *character* of ρ is the function $\chi : G \rightarrow \mathbb{C}$ defined by $\chi(g) = \text{trace}(\rho_g)$.

Trace of endomorphisms (matrices) is not multiplicative but it satisfies the following property: $\text{trace}(AB) = \text{trace}(BA)$ for any $A, B \in \text{Aut}(V)$. Consequently for any g, h we have $\text{trace}(ghg^{-1}) = \text{trace}((gh)g^{-1}) = \text{trace}(g^{-1}(gh)) = \text{trace}(h) = \text{trace}(h)$ and so $\chi_G(g)$ depends only on conjugacy class of g .

Definition 1.4. Let G be a group and $f : G \rightarrow \mathbb{C}$ some function. We call f class function if $f(g)$ depends only on conjugacy class of g for $g \in G$.

In particular characters of linear representations are class functions and characters are invariants of isomorphism classes of representations. It means that isomorphic representations have the same characters. Another property of characters is that character of direct sum of representations is the sum of characters of summands.

Let's now introduce the scalar product of class functions (in particular of characters): if f and h are class functions then $\langle f, h \rangle = \sum_{g \in G} f(g) \overline{h(g)}$.

Lemma 1.5. *If ρ and ρ' are two representations of G in V and W resp. then $\langle \chi_\rho, \chi_{\rho'} \rangle = \dim(\text{Hom}_G(V, W))$, where $\text{Hom}_G(V, W)$ are G -linear maps between V and W .*

Definition 1.6. A subrepresentation of a given representation ρ in a vector space V is representation ρ' in some subspace W of V such that $\rho'_g = \rho_g|_W$ for all elements of G . We call representation *irreducible* if it has no proper nontrivial subrepresentation.

Theorem 1.7 (Schur's lemma, [28, Prop. 2.4]). *Let V and W be vector spaces; and let ρ_V and ρ_W be irreducible representations of G in V and W .*

- (1) *If V and W are not isomorphic, then there are no nontrivial G -linear maps between them.*
- (2) *If $V = W$ and $\rho_V = \rho_W$, then the only G -linear maps are the scalar multiples of the identity.*

Theorem 1.8 (Maschke Theorem, [9, Thm. 10.8]). *If ρ is representation of G and ρ' is subrepresentation of ρ , then there is ρ'' such that $\rho \cong \rho' \oplus \rho''$.*

Corollary 1.9. *If ρ is representation of G then there exist $\rho_1, \rho_2, \dots, \rho_n$ irreducible representations of G such that $\rho \cong \rho_1 \oplus \dots \oplus \rho_n$*

Corollary 1.10. *If ρ is irreducible representation and ρ' is some representation of G then number of ρ_i isomorphic to ρ in decomposition if ρ' is equal to $\langle \chi_\rho, \chi_{\rho'} \rangle$.*

This decomposition is unique up to permutation of ρ_i and isomorphism of the summands. More precisely if $\oplus_{i=1}^n \rho_i \cong \oplus_{i=1}^m \rho'_i$ for irreducible representations ρ_i , $i \in \{1, \dots, n\}$ and ρ'_i , $i \in \{1, \dots, m\}$ then $n = m$ and there exist permutation σ of $\{1, \dots, n\}$ such that $\rho_i = \rho_{\sigma(i)}$.

Now, by property of character of direct sum and Corollary 1.9 character of every representation is equal to the sum of characters of irreducible representations with non-negative integer coefficients. Moreover coefficients can be calculated using scalar product of characters. So it is enough to study characters of irreducible representation's.

Corollary 1.11. *The number of irreducible representations of G is finite for every finite group G .*

Theorem 1.12. *Let $\chi_1, \dots, \chi_n$ be characters of all irreducible representations of G (by Corollary 1.11 the number of irreducible representations is finite). Then $\langle \chi_i, \chi_j \rangle = 0$ if $i \neq j$ and $\langle \chi_i, \chi_i \rangle = 1$ otherwise, i.e. characters of irreducible representations form orthonormal system in the space of class functions on G . Moreover, they form orthonormal basis of class functions on G , i.e. every class function can be written as linear combination of characters of irreducible representations with complex coefficients.*

Corollary 1.13. *The number of irreducible representations of every finite group G is equal to class number of G .*

From corollary 1.13 it follows that we can form a $c \times c$ matrix, where c is class number of G , whose rows represent characters of irreducible representations. This matrix is called *character table*.

Decomposition of a representation of a finite group into a direct sum of irreducible representations is not unique, however unique is the "canonical decomposition" obtained by collecting together isomorphic irreducible representations.

Let ρ be a representation of a finite group G . Let $\chi_1, \dots, \chi_c$ be distinct characters of irreducible representations $\rho_1, \dots, \rho_c$ of G . Consider any decomposition $\rho = \tau_1 \oplus \dots \oplus \tau_m$ of ρ into a direct sum of irreducible subrepresentations. Denoting by $\rho_i = \bigoplus_{\chi_{\tau_i} = \chi_i} \tau_i$ the direct sum of representations τ_j 's with the character equal χ_i we get decomposition

$$(1) \quad \rho = \rho_1 \oplus \dots \oplus \rho_s.$$

Definition 1.14. We shall call the decomposition (1) the *canonical decomposition* of the representation ρ .

Theorem 1.15 ([28, Thm. 8]). *Let*

$$\rho = \rho_1 \oplus \dots \oplus \rho_s$$

be a canonical decomposition of a representation ρ of a finite group G . For $i = 1, \dots, s$ the representation ρ_i is uniquely determined, in particular it doesn't depend on the choice of the initially chosen decomposition of ρ into irreducible subrepresentations.

More precisely the projection of ρ onto ρ_i is given by:

$$\frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \rho(g).$$

where n_i is the degree of representation ρ_i .

In particular if representation ρ is defined over K then V_ρ will be defined over K as well.

Definition 1.16. A representation $\rho : G \rightarrow \text{GL}(V)$ of a finite group G is *realizable over a field* $K \subset \mathbb{C}$ iff there exists a basis of V such that matrices of images of all elements of G have coefficients in K .

Equivalently, a representation $\rho : G \rightarrow \text{GL}(V)$ is realizable over field $K \subset \mathbb{C}$ iff there exists a homomorphism $\tau : G \rightarrow \text{GL}(W)$, where W is a vector space over K with an isomorphism $\psi : W \otimes_K \mathbb{C} \rightarrow V$ such that

$$\rho_g = \psi \circ \tau_g \otimes_K \mathbb{C} \circ \psi^{-1}.$$

Corollary 1.17. *If a representation ρ of a finite group is realizable over a field $K \subset \mathbb{C}$ then all components of the canonical decomposition of ρ are also defined over K .*

The above corollary doesn't hold for irreducible components of a representation, in fact every irreducible representation of a finite group is a component of its regular representation which is defined over $\mathbb{Q}$.

Example 1.18. The matrix $M := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ generates a subgroup of $\text{GL}_3(\mathbb{C})$ of order 3, so it defines a degree 2 representation of the group $G := C_3$ which is realizable over $\mathbb{Q}$. This representation is a direct sum of two degree one representations determined by the degree 3 primitive roots of unity ζ_3 and ζ_3^2 , which are clearly not realizable over $\mathbb{Q}$.

Example 1.19. The group generated by matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ is the quaternion Q_8 hence it defines a faithful representation ρ of Q_8 of degree 2 which is not realizable over $\mathbb{Q}$, in fact this representation is realizable over a field $K \subset \mathbb{C}$ iff -1 is a sum of two squares in K (see [28, exerc. 12.3]). On the other hand the representation $\rho^{\oplus 2}$ is realizable over $\mathbb{Q}$, more precisely the

matrices $\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$ generate group isomorphic to Q_8 and it determines

a representation of Q_8 isomorphic to $\rho^{\oplus 2}$ which is defined over $\mathbb{Q}$.

2. WEIL RESTRICTION OF SCALARS

Definition 2.1. A splitting field of a finite group G is a field $K \subset \mathbb{C}$ such that every representation of G over $\mathbb{C}$ can be realized over K , equivalently every irreducible representation can be realized over K .

Clearly, a splitting field of a group G contains the field generated by character value. A splitting field of a finite group is not unique, in fact there can be several distinct minimal splitting fields (cf. Ex. 18). The Brauer Theorem ([28, Thm. 24]) gives a sufficient condition for a splitting field

Theorem 2.2 (Brauer Theorem, [28, Thm. 24]). *Let m be the exponent of a finite group G . If a field $K \subset \mathbb{C}$ contains a primitive root of unity of degree m then K is a splitting field of G .*

Let $K \subset L$ be a field extension of degree $m := [L : K]$. Any representation $\rho : G \rightarrow \text{GL}(V)$ of a finite group G realizable over field L is determined by a homomorphism $\tau : G \rightarrow \text{GL}(W)$ for a vector space W over L with an isomorphism $\psi : W \otimes_L \mathbb{C} \rightarrow V$. The vector space W has a natural structure of a vector space over K , which we shall denote by W_K . Then the group of automorphisms of W_K , which is equal to the group of K -linear automorphisms of W , contains the group of automorphisms of W

$$\text{GL}(W) \subset \text{GL}_K(W) = \text{GL}(W_K).$$

Consequently, the homomorphism τ induces a homomorphism $\tau : G \rightarrow \text{GL}(W)$ and hence a representation

$$\text{Res}_{L/K} \rho : G \rightarrow V_K, \quad \text{where } V_K = W \otimes_K \mathbb{C}.$$

Definition 2.3. The representation $\text{Res}_{L/K} \rho$ is called *the Weil restriction of scalars* of the representation ρ from L to K .

Since $V_K = W \otimes_K \mathbb{C} \cong W \otimes_K (L \otimes_L \mathbb{C}) \cong (W \otimes_K L) \otimes_L \mathbb{C} \cong (L \otimes_K W) \otimes_L \mathbb{C} \cong L \otimes_K (W \otimes_L \mathbb{C}) \cong L \otimes_K V$ we get

$$\dim_{\mathbb{C}} V_K = [L : K] \dim_{\mathbb{C}} V,$$

which means that the degree of the Weil restriction of a representation ρ equals the degree of the original representation ρ multiplied by the degree of the fields extension.

Weil restriction can be also described more explicitly at the level of matrix representation. Let $M \in \text{GL}_n(L)$ be an $n \times n$ invertible matrix with entries in L , it defines an automorphism $\phi_M : L^n \rightarrow L^n$. The field L is a K -vector space of dimension m , choice of a basis of L over K yields an isomorphism between L and K^m . Since ϕ_M is also an automorphism of vector spaces over K it determines an automorphism $\phi_M^K : K^{mn} \rightarrow K^{mn}$ and hence also an invertible $mn \times mn$ matrix $\text{Res}_{L/K} M \in \text{GL}_{mn}(K)$. Definition of $\text{Res}_{L/K}$ depends on a choice of a basis of L^n as a vector space over K - which is equivalent to a choice of an isomorphism of L^n and K^{mn} .

Definition 2.4. The matrix $\text{Res}_{L/K}(M)$ is called the Weil restriction of scalars of M from L to K .

Assume then $\{b_1, \dots, b_m\}$ is an ordered base of L/K and $v_1, \dots, v_n$ is the natural basis of V over L . Then the set of products $(b_i v_j)_{i=1, \dots, m, j=1, \dots, n}$ is a basis of V/K . Assume that the matrix of an endomorphism $F \in \text{End}(V)$ in the chosen base equals $A = (a_{ij})_{i,j=1, \dots, n}$. Now, $F(b_i v_j) = b_i F(v_j) = \sum_{p=1}^n a_{jp} b_i v_p$.

For each element $a \in L$, multiplication by a

$$L \ni x \mapsto ax \in L$$

is a K -endomorphism of L , denote by $\text{Res}_{L/K}(a)$ the matrix of this endomorphism in the base b_i . Then

$$a_{p,j}b_i = \sum_{q=1}^m \text{Res}_{L/K}(a_{p,j})_{q,i} b_q$$

and finally

$$F(b_i v_j) = \sum_{p=1}^n \sum_{q=1}^m \text{Res}_{L/K}(a_{p,j})_{q,i} b_q v_p$$

The explicit matrix of F depends on the order of the base of V over K , for the ordering $\{b_1 v_1, \dots, b_m v_1, \dots, b_1 v_n, b_m v_n\}$, we get the block matrix

$$\begin{pmatrix} \text{Res}_{L/K}(a_{1,1}) & \text{Res}_{L/K}(a_{1,2}) & \cdots & \text{Res}_{L/K}(a_{1,n}) \\ \text{Res}_{L/K}(a_{2,1}) & \text{Res}_{L/K}(a_{2,2}) & \cdots & \text{Res}_{L/K}(a_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Res}_{L/K}(a_{n,1}) & \text{Res}_{L/K}(a_{n,2}) & \cdots & \text{Res}_{L/K}(a_{n,n}) \end{pmatrix}$$

Proposition 2.5. *For a matrix $A(a_{ij})_{i,j=1,\dots,n} \in \text{GL}_n(L)$ we have (in a appropriately ordered base)*

$$\text{Res}_{L/K}(A) = (\text{Res}_{L/K}(a_{i,j}))_{i,j=1,\dots,n}.$$

Let $d = [K[a] : K] = \deg_K a$ be the degree of a over K , denote $r := \frac{m}{d} = [L : K[a]]$ and choose an ordered base $\{f_1, \dots, f_r\}$ of L over $K[a]$. Then

$$a(a^k f_l) = a^{k+1} f_l, \text{ for } k = 0, \dots, d-2,$$

and

$$a(a^{d-1} f_l) = -(c_{d-1} a^{d-1} f_l + \cdots + c_0 f_l),$$

where $P(X) = X^d + c_{d-1} X^{d-1} + \cdots + c_0$ is the minimal polynomial of a over K . Denoting by A_P the companion matrix of P we get that in the base $\{f_1, a f_1, \dots, a^{d-1} f_1, \dots, f_r, \dots, a^{d-1} f_r\}$

$$\text{Res}_{L/K}(a) = \text{diag}(A_P, \dots, A_P)$$

If the extension L/K is Galois with the Galois group $\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_m\}$ the last matrix is similar to

$$\text{diag}(\sigma_1(a), \dots, \sigma_m(a)).$$

For a matrix A with entries in the field L and any automorphism $\sigma \in \text{Aul}(L)$ we denote by A^σ the matrix obtained from A by application of σ to each entry.

Proposition 2.6. *Let $A \in \text{GL}_n(L)$ be an invertible matrix over a field L , assume that L is a finite Galois extension of K with the Galois group $\{\sigma_1, \dots, \sigma_m\}$. Then the matrices*

$$\text{Res}_{L/K}(A) \quad \text{and} \quad \text{diag}(A^{\sigma_1}, \dots, A^{\sigma_m})$$

are similar.

Corollary 2.7.

$$\text{trace}(\text{Res}_{L/K}(A)) = \text{trace}_{L/K}(\text{trace}(A))$$

Clearly, for any automorphism $\sigma \in \text{Gal}_K(L)$ the map $A \mapsto A^\sigma$ defines an automorphism of $\text{GL}_n(L)$, hence for any representation ρ realizable over L we can define a representation ρ^σ .

Corollary 2.8. *For any representation ρ realizable over a field L which is a finite Galois extension of a field K we have*

$$\chi_{\text{Res}_{L/K} \rho} = \text{trace}_{L/K}(\chi_\rho)$$

Theorem 2.9. *Every representation μ realizable over K containing irreducible representation ρ has to contain representation isomorphic to $\text{Res}_{L/K}(\rho)$ as well, where L is some, minimal in sense of inclusion, field over which representation ρ is realizable.*

3. SCHUR INDEX

In the previous section we described two necessary conditions which a representation ρ must satisfy to be defined over a number field K

- values of the character of ρ must belong to K ,
- conjugated by an automorphism of K irreducible representations must belong to ρ with the same multiplicity.

As we noticed in Ex. 1.19 these conditions are not sufficient, there is a degree 2 representation of quaternion group Q_8 which is defined over $\mathbb{Q}[i]$ but is not realizable over $\mathbb{Q}$. As this is the only representation of Q_8 of degree 2, it is isomorphic to its complex conjugate. Consequently a direct sum of two copies of ρ is a representation of degree 4 realizable over $\mathbb{Q}$.

Let $K \subset \mathbb{C}$ be a subfield of the field of complex numbers, χ a character of a finite group G . Denote by $K(\chi)$ extension of the field K by values of the character χ .

Definition 3.1. [9, Def. 41.4] The *Schur index* $m_K(\chi)$ of the character χ is the minimum of extensions degrees $[L : K(\chi)]$ taken over all field L such that $K \subset L \subset \mathbb{C}$ and χ is a character of a representation of G realizable over L .

Remark 3.2. We have $m_K(\chi) = 1$ iff the character χ affords a representation realizable over $K(\chi)$.

Schur index has alternative description based on the Wedderburn Theorem ([9, Thm. 26.4], [28, sect. 12.2]).

Let L be a field extension such that $[L : K(\chi)] = m_K(\chi)$ and let ρ be a representation of G realizable over the field L . Then the Weil restriction $\text{Res}_{L/K(\chi)}(\rho)$ is a representation of G realizable over $K(\chi)$.

Corollary 3.3 (Schur, [9, p. 479]). *Let L be a finite Galois extension of $\mathbb{Q}$, which is a splitting field of a finite group G and let $\chi_1, \dots, \chi_c$ be all irreducible characters of G . Then a character $\chi = n_1\chi_1 + \dots + n_c\chi_c$ affords a representation of G realizable over a subfield $K \subset L$ iff the following two conditions hold*

- (1) $m_K(\chi_i) \mid n_i$,
- (2) if $\chi_i = \chi_j^\sigma$ is a conjugate of χ_j , $\sigma \in \text{Gal}_K(L)$, then $n_i = n_j$.

4. SCHUR BOUND

In this section we shall recall the Schur bound of the order of a finite group of matrices over a given number field, we shall follow [14, 29].

For an integer $m > 1$ denote by $\zeta_m = e^{\frac{2\pi i}{m}}$ a (fixed) degree m primitive root of unity.

Definition 4.1. For a prime number l define

$$m(K, l) = \min\{m \geq 1 \mid K \cap \mathbb{Q}(\zeta_{l^m}) = K \cap \mathbb{Q}(\zeta_{l^{m+1}}) = \dots\}$$

The chain of inclusions

$$\mathbb{K} \cap \mathbb{Q}(\zeta_l) \subset \mathbb{K} \cap \mathbb{Q}(\zeta_{l^2}) \subset \mathbb{K} \cap \mathbb{Q}(\zeta_{l^3}) \subset \dots$$

stabilizes since $[K : \mathbb{Q}]$ is finite, so $m(K, l)$ is well-defined.

Since

$$[K \cdot \mathbb{Q}(\zeta_{l^m}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}][\mathbb{Q}(\zeta_{l^m}) : \mathbb{Q}]}{[K \cap \mathbb{Q}(\zeta_{l^m}) : \mathbb{Q}]}$$

and

$$[K \cdot \mathbb{Q}(\zeta_{l^{m+1}}) : \mathbb{Q}] = \frac{[K : \mathbb{Q}][\mathbb{Q}(\zeta_{l^{m+1}}) : \mathbb{Q}]}{[K \cap \mathbb{Q}(\zeta_{l^{m+1}}) : \mathbb{Q}]}$$

using the tower law we get for $m \geq 1$

$$[K \cap \mathbb{Q}(\zeta_{l^{m+1}}) : K \cap \mathbb{Q}(\zeta_{l^m})][K \cdot \mathbb{Q}(\zeta_{l^{m+1}}) : K \cdot \mathbb{Q}(\zeta_{l^m})] = l.$$

Lemma 4.2. *If l is an odd prime then the sequence $K \cap \mathbb{Q}(\zeta_{l^m})$ stabilizes at the first equality.*

Proof. Assume to the contrary that

$$K \cap \mathbb{Q}(\zeta_{l^m}) = K \cap \mathbb{Q}(\zeta_{l^{m+1}}) \subsetneq K \cap \mathbb{Q}(\zeta_{l^{m+2}}).$$

Then $K \cap \mathbb{Q}(\zeta_{l^{m+2}})$ is a subfield in $\mathbb{Q}(\zeta_{l^{m+2}})$ which is not contained in $\mathbb{Q}(\zeta_{l^{m+1}})$, hence the degree of the extension $[K \cap \mathbb{Q}(\zeta_{l^{m+2}}) : \mathbb{Q}]$ is divisible by l^{m+1} . Now the degree of $[K \cap \mathbb{Q}(\zeta_{l^{m+2}}) \cap \mathbb{Q}(\zeta_{l^{m+1}}) : \mathbb{Q}] = [K \cap \mathbb{Q}(\zeta_{l^{m+1}}) : \mathbb{Q}]$ is divisible by l^m , consequently $K \cap \mathbb{Q}(\zeta_{l^{m+1}})$ is not a subfield of $\mathbb{Q}(\zeta_{l^m})$ - contrary to $K \cap \mathbb{Q}(\zeta_{l^m}) = K \cap \mathbb{Q}(\zeta_{l^{m+1}})$. $\square$

Consequently, if $K \cap \mathbb{Q}(\zeta_{l^{m+1}}) \supsetneq K \cap \mathbb{Q}(\zeta_{l^m})$ we have $K \cdot \mathbb{Q}(\zeta_{l^{m+1}}) = K \cdot \mathbb{Q}(\zeta_{l^m}) = \dots = K \cdot \mathbb{Q}(\zeta_l)$ and $\zeta_{l^{m+1}} \in K(\zeta_l)$. So, we get another description of the number $m(K, l)$ for an odd prime l

Corollary 4.3.

$$m(K, l) = \max\{d \geq 1 : \zeta_{l^d} \in K(\zeta_l)\}.$$

The last formula gives an easy a priori bound $m \leq v_l(\deg(K))$ of m by the l -adic valuation of the degree of the field K .

The situation is different in the case of $l = 2$, the reason is that for $m \geq 3$ the cyclotomic field $\mathbb{Q}(\zeta_{2^m})$ of degree $\phi(2^m) = 2^{m-1}$ contains three subfields of degree 2^{m-2} corresponding to the three elements of order 2 in the Galois group $\text{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}) \cong (\mathbb{Z}/2^m\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{m-2}\mathbb{Z}$, explicitly they are

$$\mathbb{Q}(\zeta_{2^{m-1}}), \mathbb{Q}(\zeta_{2^m} + \bar{\zeta}_{2^m}), \mathbb{Q}(\zeta_{2^m} - \bar{\zeta}_{2^m}).$$

If $m(K, 2) = 1$ then for any $m \geq 1$ we have $K \cap \mathbb{Q}(\zeta_{2^m}) = \mathbb{Q}$. Similarly, if $m(K, 2) = 2$ then $i \in K$ and for any $m \geq 2$ we have $K \cap \mathbb{Q}(\zeta_{2^m}) = K[\zeta_4] = K[i]$.

On the other hand if $m(K, 2) \geq 3$ then $K \cap \mathbb{Q}(\zeta_{2^{m(K,2)}}) \not\subset \mathbb{Q}(\zeta_{2^{m(K,2)-1}})$, hence $K \cap \mathbb{Q}(\zeta_{2^{m(K,2)}}) = \mathbb{Q}(\zeta_{2^{m(K,2)}})$ or $K \cap \mathbb{Q}(\zeta_{2^{m(K,2)}}) = \mathbb{Q}(\zeta_{2^{m(K,2)}} + \bar{\zeta}_{2^{m(K,2)}})$ or $K \cap \mathbb{Q}(\zeta_{2^{m(K,2)}}) = \mathbb{Q}(\zeta_{2^{m(K,2)}} - \bar{\zeta}_{2^{m(K,2)}})$. In the first case we get $K \cap \mathbb{Q}(\zeta_{2^m}) = \mathbb{Q}(\zeta_{2^m})$ for $1 \leq m \leq m(K, 2)$. In the second case we get $K \cap \mathbb{Q}(\zeta_{2^m}) = \mathbb{Q}(\zeta_{2^m} + \bar{\zeta}_{2^m})$ for $1 \leq m \leq m(K, 2)$. Finally in the third case we get $K \cap \mathbb{Q}(\zeta_{2^m}) = \mathbb{Q}(\zeta_{2^m} - \bar{\zeta}_{2^m})$ for $m = m(K, 2)$ and $K \cap \mathbb{Q}(\zeta_{2^m}) = \mathbb{Q}(\zeta_{2^m} + \bar{\zeta}_{2^m})$ for $1 \leq m < m(K, 2)$.

We have an alternative description of $m(K, 2)$

Proposition 4.4. *Let*

$$m_0 = \max\{d \geq 1 : \zeta_{2^d} \in K(\zeta_4) = K(i)\}.$$

Then

$$m(K, 2) = \begin{cases} m_0, & \text{when } m_0 \geq 3 \\ 2, & \text{when } m_0 = 2 \text{ and } i \in K \\ 1, & \text{when } m_0 = 2 \text{ and } i \notin K \end{cases}$$

Example 4.5. Let $K := \mathbb{Q}(\sqrt{2})$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ and so

$$K \cap \mathbb{Q}(\zeta_2) = \mathbb{Q} = K \cap \mathbb{Q}(\zeta_4) \subsetneq K = K \cap \mathbb{Q}(\zeta_8) = \dots$$

We conclude that $m(K, 2) = 3$ but $\zeta_8 \notin K(\zeta_2)$.

Furthermore we define another invariant $t(K, l)$

$$t(K, l) = [\mathbb{Q}(\zeta_{l^{m(K, l)}}) : K \cap \mathbb{Q}(\zeta_{l^{m(K, l)}})] = [K(\zeta_{l^{m(K, l)}}) : K]$$

For an odd prime l we can repeat the above arguments to get

$$t(K, l) = [K(\zeta_l) : K].$$

Again, for $l = 2$ the formula is slightly more complicated, if $m(K, 2) \geq 3$ we get a sequence of strict inclusions

$$K \cap \mathbb{Q}(\zeta_4) \subsetneq K \cap \mathbb{Q}(\zeta_8) \subsetneq \cdots \subsetneq K \cap \mathbb{Q}(\zeta_{2^{m(K,2)}})$$

and hence a sequence of equalities

$$K(\zeta_4) = K(\zeta_8) = \cdots = K(\zeta_{2^{m(K,2)}})$$

Finally we get in the case of $l = 2$, $m(K, 2) \geq 3$

$$t(K, 2) = [K(\zeta_4) : K] = [K(i) : K].$$

If $m(K, 2) = 1$ then $K \cap \mathbb{Q}(\zeta_2) = \mathbb{Q} = \mathbb{Q}(\zeta_2)$ and if $m(K, 2) = 2$ then $K \cap \mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$, in both cases we get $t(K, 2) = 1$.

Definition 4.6. The *Schur number* of a number field K is

$$S(n, K) = 2^{n - \lfloor \frac{n}{t(K,2)} \rfloor} \prod_l l^{\left(m(K,l) \lfloor \frac{n}{t(K,l)} \rfloor + \sum_{i=1}^{\infty} \lfloor \frac{n}{l^i t(K,l)} \rfloor \right)}$$

Denote by $S(n, K, l) = S(n, K)_l$ the l -part of $S(n, K)$, for l an odd prime

$$S(n, K, l) = l^{\left(m(K,l) \lfloor \frac{n}{t(K,l)} \rfloor + \sum_{i=1}^{\infty} \lfloor \frac{n}{l^i t(K,l)} \rfloor \right)},$$

while for $l = 2$ we have

$$S(n, K, 2) = 2^{\left(n - \lfloor \frac{n}{t(K,2)} \rfloor + m(K,2) \lfloor \frac{n}{t(K,2)} \rfloor + \sum_{i=1}^{\infty} \lfloor \frac{n}{2^i t(K,2)} \rfloor \right)}.$$

Schur ([27]) proved the following bound of the order of a finite matrix group over a number field.

Theorem 4.7 (Schur's bound, [14]). *Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ such that traces of all elements of G belongs to a fixed number field K . Then the order of G divides $S(n, K)$.*

The corresponding bound of the order of a matrix l -group is sharp and an analogon of the Sylow theorem holds

Proposition 4.8. *Let l be a prime and let G be a finite l -subgroup of $\mathrm{GL}_n(K)$. Then $|G| \leq S(n, K, l)$.*

Moreover this bound is sharp and if H is an l -subgroup of maximal order then there exist $M \in \mathrm{GL}_n(K)$ such that G is a subgroup of mHm^{-1} .

Lemma 4.9. *Assume that K is the field of fraction of a Principal Ideal Domain $\mathcal{O} \subset K$ and let $G \subset \mathrm{GL}_n(K)$ be a finite matrix group. Then G is conjugate in $\mathrm{GL}_n(K)$ to a subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$.*

Proof. Consider the finitely generated $\mathcal{O}$ -module of rank n

$$M := \sum_{g \in G} g\mathcal{O}^n.$$

Since $\mathcal{O}$ is Principal Ideal Domain the $\mathcal{O}$ -module M is isomorphic to $\mathcal{O}^n$. It means that there exists $A \in \mathrm{GL}_n(K)$ such that $M = A\mathcal{O}^n$. The module M is stable under the action of G , i.e. for any $g \in G$ we have $gM = M$ and consequently $A^{-1}gA \in \mathrm{GL}_n(\mathcal{O})$. The group $A^{-1}GA$ is a subgroup of $\mathrm{GL}_n(\mathcal{O})$ conjugate to G . $\square$

For a number field K we shall denote by $\mathcal{O}_K \subset K$ the ring of integers in K i.e, the integral closure of $\mathbb{Z}$ in K .

Proposition 4.10. *If G is finite subgroup of $\mathrm{GL}_n(K)$ and $\mathcal{O}_K$ is Principal Ideal Domain then G is conjugate in $\mathrm{GL}_n(K)$ to a subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$.*

If K is an arbitrary number field then $\mathcal{O}_K$ may not be a Principal Ideal Domain, it is however always a Dedekind domain. Consequently, for any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ the localization $\mathcal{O}_{K,\mathfrak{p}}$ is a Principal Ideal Domain and any finite subgroup of $\mathrm{GL}_n(K)$ is conjugate to a subgroup in $\mathrm{GL}_n(\mathcal{O}_{K,\mathfrak{p}})$.

The ideal $\mathfrak{p}$ has norm $\mathcal{N}(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$. Reduction modulo the maximal ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ of $\mathcal{O}_{K,\mathfrak{p}}$ yields a homomorphism:

$$\mathrm{GL}_n(\mathcal{O}_{K,\mathfrak{p}}) \rightarrow \mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})}).$$

If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where p is a rational prime. In this situation $p\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^e$, where e is a positive integer called ramification index of $\mathfrak{p}$.

Lemma 4.11 ([Lemma 9 from [14]]). *The kernel of the reduction homomorphism above has at most p -torsion. Any torsion element g in the kernel has order p^i for some $p^i \leq \frac{ep}{p-1}$.*

Corollary 4.12. *Let K be a number field, $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal with ramification index $e < p-1$. Then the kernel*

$$\ker\left(\mathrm{GL}_n(\mathcal{O}_{K,\mathfrak{p}}) \longrightarrow \mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})})\right)$$

is torsion free. In particular every finite subgroup of $\mathrm{GL}_n(K)$ is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{F}_{\mathcal{N}(\mathfrak{p})})$.

Proposition 4.13. *Let ρ_1 and ρ_2 be two faithful representations of a finite group G in the same vector space V with conjugate images in $\mathrm{GL}(V)$. Then there is an automorphism $\phi \in \mathrm{Aut}(G)$ such that representations ρ_1 and $\rho_2 \circ \phi$ have equal character.*

Proof. Replacing ρ_2 with an isomorphic (conjugate) representation, we may assume that images of ρ_1 and ρ_2 are equal. Now, ρ_1 and ρ_2 are isomorphisms of G onto the same subgroup of $\mathrm{GL}(V)$, and we can define an automorphism $\phi \in \mathrm{Aut}(G)$ by $\phi := \rho_2^{-1} \circ \rho_1$. $\square$

5. ALGORITHM

In this section we shall describe main steps of the algorithm. Given a number field K and a positive integers compute all finite subgroups in $\mathrm{GL}_n(K)$. In each step of the algorithm we refer to an appropriate function in Magma code (sec. 6)

1. **schurBound:**

Compute the Schur bound $S(n, K)$: corollary 4.3 gives an easy explicit bound l_0 much that for any prime $l \geq l_0$ we have $S(n, k, l) = 1$, for a finite set of primes we compute $M(n, K, l)$ using the alternative descriptions of $m(K, l)$ and $t(K, l)$.

2. **finiteFieldOrder:**

Find an ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ with the ramification index $e(\mathfrak{p}) < p - q$ and determine the prime power $q = \mathcal{N}(\mathfrak{p})$

3. **subgroupsNonchecked:**

Find all subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$, up to isomorphism, with order dividing Schur's bound, where q is the prime power from the previous step.

Now, we have a list of finite groups that may be isomorphic to a subgroup of $\mathrm{GL}_3 K$. Then for each subgroup G in the list we perform the following:

4. **characterSumsOfFaithfulRepresentations:**

Compute all irreducible characters of G of degree not exceeding n and add characters from an orbit of the Galois group of the field K over $\mathbb{Q}$ multiplied by the Schur index (of any character from the orbit). Compute sums of obtained characters which are faithful and have degree equal n .

5. **autGroups:**

Compute automorphisms of the group G , for each automorphism determine the induced permutation on the set of conjugacy classes of G , remove from the list characters that differ by an action of a permutation induced by an automorphism.

Images of representations afforded by characters from the constructed list **resCT** are all finite subgroups of $\mathrm{GL}(n, K())$.

6. Decompose the characters from the list **irrResCT**. For every irreducible summand construct an irreducible G -modules over K afforded by it. This yields a list **irrGModules** of irreducible G -modules over K . Decompose every character in the list **resCT** as sums of characters of G -modules from **irrGModules**. Using this decomposition compute representations affording all characters in **resCT**.

It might happen that the character of constructed representation differs from a given character in **resCT**, the reason is that the computation of irreducible G -modules can produce G -modules over a field different from K . In this situation we use a slower method where we compute Absolutely Irreducible Modules, and then apply Wei restriction.

By the Stark–Heegner theorem [30] there are nine imaginary quadratic fields K whose ring of integers $\mathcal{O}_K$ is a Principal Ideals Domain in the table we list some results of computations:

n	K	$S(n, K)$	# finite subgroups of $\mathrm{GL}(n, K)$	# finite subgroups of $\mathrm{SL}(n, K)$
2	$\mathbb{Q}$	24	10	5
3	$\mathbb{Q}$	48	32	11
4	$\mathbb{Q}$	5760	227	106
5	$\mathbb{Q}$	11520	955	226
3	$\mathbb{Q}[\sqrt{-1}]$	384	178	28
3	$\mathbb{Q}[\sqrt{-2}]$	96	48	16
3	$\mathbb{Q}[\sqrt{-3}]$	1286	352	40
3	$\mathbb{Q}[\sqrt{-7}]$	336	41	15
3	$\mathbb{Q}[\sqrt{-11}]$	48	37	13
3	$\mathbb{Q}[\sqrt{-19}]$	48	40	14
3	$\mathbb{Q}[\sqrt{-43}]$	48	40	14
3	$\mathbb{Q}[\sqrt{-67}]$	48	40	14
3	$\mathbb{Q}[\sqrt{-163}]$	48	40	14

5.1. **Finite subgroups of $\mathrm{GL}(3, \mathbb{Q}\sqrt{-19})$ and $\mathrm{SL}(3, \mathbb{Q}\sqrt{-19})$.**

Although the Schur bound for $S(3, \mathbb{Q}\sqrt{-19}) = S(3, \mathbb{Q}) = 48$, numbers of finite subgroups of $\mathrm{GL}(3, \mathbb{Q}\sqrt{-19})$ and $\mathrm{SL}(3, \mathbb{Q}\sqrt{-19})$ are strictly larger than the numbers of finite subgroups of $\mathrm{GL}(3, \mathbb{Q})$ and $\mathrm{SL}(3, \mathbb{Q})$, respectively. Finite subgroups of $\mathrm{GL}(3, \mathbb{Q}\sqrt{-19})$ are isomorphic to the

following

$$C_1, C_2, C_2, C_2, C_3, C_4, C_4, C_2^2, C_2^2, C_2^2, S_3, S_3, C_6, C_6, C_6, C_2 \times C_4, Q_8, Q_8, C_2^3, \\ D_4, D_4, D_4, D_6, D_6, D_6, D_6, C_3 \rtimes C_4, C_3 \rtimes C_4, A_4, C_2 \times C_6, C_2 \times Q_8, C_2 \times D_4, C_2 \times C_3 : C_4, \\ \text{SL}(2, 3), C_2^2 \times S_3, S_4, S_4, C_2 \times A_4, C_2 \times \text{SL}(2, 3), C_2 \times S_4$$

Two (non-isomorphic) groups in that list realize the Schur bound $S(3, \mathbb{Q}\sqrt{-19}) = 48$

$$C_2 \times \text{SL}(2, 3) \cong \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & \frac{1}{2}(\sqrt{-19}-3) \\ 0 & \frac{1}{2}(\sqrt{-19}+3) & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2}(\sqrt{-19}+3) & 3 \\ 0 & \frac{1}{2}(\sqrt{-19}-3) & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} -1 & 0 & 0 \\ 0 & \frac{1}{2}(-\sqrt{-19}+3) & \frac{1}{2}(-\sqrt{-19}-1) \\ 0 & -3 & \frac{1}{2}(\sqrt{-19}-3) \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle$$

and

$$C_2 \times S_4 \cong \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ -1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle$$

The character of the group $C_2 \times S_4$ equals

χ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_2	1	-1	-1	1	1	1	1	-1	1	-1	-1	-1	-1	1
χ_3	1	1	1	1	$-\zeta_3 - 1$	ζ_3	1	1	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$	ζ_3
χ_4	1	1	1	1	ζ_3	$-\zeta_3 - 1$	1	1	ζ_3	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$
χ_5	1	-1	-1	1	ζ_3	$-\zeta_3 - 1$	1	-1	ζ_3	$\zeta_3 + 1$	$-\zeta_3$	$\zeta_3 + 1$	$-\zeta_3$	$-\zeta_3 - 1$
χ_6	1	-1	-1	1	$-\zeta_3 - 1$	ζ_3	1	-1	$-\zeta_3 - 1$	$-\zeta_3$	$\zeta_3 + 1$	$-\zeta_3$	$\zeta_3 + 1$	ζ_3
χ_7	2	2	-2	-2	-1	-1	0	0	1	1	1	-1	-1	1
χ_8	2	-2	2	-2	-1	-1	0	0	1	-1	-1	1	1	1
χ_9	2	-2	2	-2	$\zeta_3 + 1$	$-\zeta_3$	0	0	$-\zeta_3 - 1$	$-\zeta_3$	$\zeta_3 + 1$	ζ_3	$-\zeta_3 - 1$	ζ_3
χ_{10}	2	2	-2	-2	$-\zeta_3$	$\zeta_3 + 1$	0	0	ζ_3	$-\zeta_3 - 1$	ζ_3	$\zeta_3 + 1$	$-\zeta_3$	$-\zeta_3 - 1$
χ_{11}	2	2	-2	-2	$\zeta_3 + 1$	$-\zeta_3$	0	0	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$	$-\zeta_3$	$\zeta_3 + 1$	ζ_3
χ_{12}	2	-2	2	-2	$-\zeta_3$	$\zeta_3 + 1$	0	0	ζ_3	$\zeta_3 + 1$	$-\zeta_3$	$-\zeta_3 - 1$	ζ_3	$-\zeta_3 - 1$
χ_{13}	3	-3	-3	3	0	0	-1	1	0	0	0	0	0	0
χ_{14}	3	3	3	3	0	0	-1	-1	0	0	0	0	0	0

where $\zeta_3 = \exp(\frac{2\pi i}{3})$ is a third root of unity.

Characters χ_7 and χ_8 have the Schur index over $\mathbb{Q}$ equal to 2, while their Schur index over $\mathbb{Q}(\sqrt{-19})$ (also over $\mathbb{Q}(\sqrt{-d})$ for all Heegner numbers except 7) equals 1. Kernels of χ_7 and χ_8 are groups of order 2 generated by matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

respectively. Sums of characters

$$\begin{array}{c|cccccccccccccc} \chi_2 + \chi_7 & 3 & 1 & -3 & -1 & 0 & 0 & 1 & -1 & 2 & 0 & 0 & -2 & -2 & 2 \\ \chi_2 + \chi_8 & 3 & -3 & 1 & -1 & 0 & 0 & 1 & -1 & 2 & -2 & -2 & 0 & 0 & 2 \end{array}$$

are faithful. They differ by an automorphism of the group $C_2 \times \text{SL}(2, 3)$, consequently they define different embedding of that group with equal images. Note, that the kernel of the character χ_2 equals $\text{SL}(2, 3)$.

Finite subgroups of $GL(3, \mathbb{Q}(\sqrt{-19}))$ that are not conjugate to a subgroup of $GL(3, \mathbb{Q})$ are isomorphic to

$$Q_8, Q_8, C_3 \rtimes C_4, C_3 \rtimes C_4, C_2 \times Q_8, C_2 \times C_3 \rtimes C_4, SL(2, 3), C_2 \times SL(2, 3)$$

6. MAGMA

We have implemented the algorithm presented in the previous section in the computer algebra system MAGMA

```

schurBoundForPrime := function(n, l, field)
    local mseq, t, m, schurBoundRes, field1;
    if Degree(field) eq 1
        then m:=1; t:=l-1;
    else
        if l eq 2 then
            field1:=RelativeField(field, CompositeFields(field, CyclotomicField(4))[1]);
            t:=Degree(field1);
            m:=1;
            while IsSubfield(CyclotomicField(2^(m+1)), field1)
                do m:=m+1;
            end while;
            if m eq 2 and not IsSquare(field!-1) then
                m:=1;
                t:=1;
            end if;
        else
            field1:=RelativeField(field, CompositeFields(field, CyclotomicField(1))[1]);
            t:=Degree(field1);
            m:=1;
            while IsSubfield(CyclotomicField(1^(m+1)), field1)
                do m:=m+1;
            end while;
        end if;
    end if;
    if l eq 2 then
        schurBoundRes:=2^(n-Floor(n/t));
    else
        schurBoundRes:=1;
    end if;
    schurBoundRes:=schurBoundRes*l^(m*Floor(n/t)+Valuation(Factorial(Floor(n/t)), l));
    return(schurBoundRes);
end function;

schurBound := function(n, field)
    local l;
    return(&*[schurBoundForPrime(n, l, field): l in PrimesUpTo(n*AbsoluteDegree(field)+2)]);
end function;

orderOfFiniteFieldForPrime := function(l, field)
    local primedIdeal, ramificationIndex;
    primeIdeal, ramificationIndex:=Explode(Factorization(l*Integers(field))[1]);
    if ramificationIndex lt l-1 then
        return (Norm(primeIdeal));
    else
        return -1;
    end if;
end function;

```

```

finiteFieldOrder := function(n, field)
  local L, n0, mB, orders, order;
  n0 := NextPrime(100*n*Degree(field)+5);
  orders := [ orderOfFiniteFieldForPrime(11, field) : 11 in PrimesUpTo(n0) ];
  orders := [ ooo : ooo in orders | ooo ge 5 ];
  order := Min(orders);
  return order;
end function;

subgroupsNonchecked := function(n, field)
  local fford, mbound, subgroups, subgroupsI;
  fford := finiteFieldOrder(n, field);
  mbound := schurBound(n, field);
  subgroups := [(G' subgroup) : G in Subgroups(GL(n, fford) : OrderDividing := mbound)];
  for k := #subgroups to 1 by -1 do
    for m := k-1 to 1 by -1 do
      if IsIsomorphic(subgroups[k], subgroups[m] : SmallOuterAutGroup := 200000000) then
        Remove(~subgroups, k);
        break;
      end if;
    end for;
  end for;
  return subgroups;
end function;

function get_CF_subfield(CF, K) local L, S, t;
  if Degree(CF) eq 1 or Degree(K) eq 1 then
    return Rationals();
  end if;
  L := Factorization(PolynomialRing(CF) ! DefiningPolynomial(K));
  S := OptimizedRepresentation(sub<CF | &cat[Coefficients(t[1]) : t in L]>);
  return S;
end function;

characterSums := function(n, CharacterList)
  local CLSplit, result, fixedClasses, decomp, triples;
  CLSplit := [];
  result := {};
  for k := 1 to n do
    Append(~CLSplit, [cl : cl in CharacterList | cl[1] eq k]);
  end for;
  fixedClasses := [[{i : i in [1..#cl] | cl[i] eq cl[1]} : cl in CLSplit[k] ] : k in [1..n]];
  for part in Partitions(n) do
    ttuples := CartesianProduct([ [1..#fixedClasses[ttt]] : ttt in part ]);
    tuples := [[x : x in ttt] : ttt in ttuples];
    tuples := [x : x in tuples | &meet[fixedClasses[part[i]][x[i]] : i in [1..#part]] eq {1}];
    result join := {&+[CLSplit[part[i]][tt[i]] : i in [1..#part]] : tt in tuples};
  end for;
  return SetToSequence(result);
end function;

charactersOfFaithfulRepresentations := function(n, group, field)
  local CT, schInd, irrCT, EirrCT, character, resCT, EresCT, newChar, conjClasses,
    nClasses, autGroup, classMap, permGroup, charRing, resIrrCT, galOrb, schGalChar,
    characterSum, decCharacterSum, irrResCT;
  conjClasses := ConjugacyClasses(group);
  nClasses := Nclasses(group);

```

```

autGroup:=AutomorphismGroup(group);
classMap:=ClassMap(group);
permGroup:=sub<Sym(nClasses)|[[classMap((autGroup.k)(conjClasses[i][3]))): i in
[1..nClasses]]: k in [1..Ngens(autGroup)]]>;
charRing:=CharacterRing(group);
CT:=CharacterTable(group);
CT:=[ct: ct in CT| ct[1] le n];
resCT:=[];
schResCT:=[];
resIrrCT:=[];
irrCT:=CT;
while #irrCT gt 0 do
  galOrb:=GaloisOrbit(irrCT[1], get_CF_subfield(CharacterField(irrCT[1]), field));
  schInd:=SchurIndex(irrCT[1], field);
  schGalChar:=schInd*(&+galOrb);
  if schGalChar[1] le n then
    Append(~resCT, schGalChar);
  end if;
  irrCT:=RemoveIrreducibles(galOrb, irrCT);
end while;
resCT:=characterSums(n, resCT);
EresCT:=[[ccc[i]: i in [1..#ccc]]: ccc in resCT];
k:=1;
while k lt #EresCT do
  cccc:={{EresCT[k][i^g]: i in [1..#EresCT[k]]}: g in permGroup};
  for j:=#EresCT to k+1 by -1 do
    if EresCT[j] in cccc
      then Remove(~EresCT, j);
    end if;
  end for;
  k:=k+1;
end while;
if #EresCT gt 0 then
  characterSum:=charRing!(&+[EresCT[i][j]: i in [1..#EresCT]]: j in [1..nClasses]);
  decCharacterSum:=Decomposition(CT, characterSum);
  irrResCT:=[CT[ii]: ii in [1..#CT]|decCharacterSum[ii] ne 0];
else
  irrResCT:=CT;
end if;
return EresCT, irrResCT, CT, charRing;
end function;

weilRestriction:=function (algNum, F, L)
  local tt;
  if L eq Rationals() then return Matrix(Rationals(), 1, 1, [algNum]); end if;
  tt:=IsSubfield(F, L);
  tt:=IsSubfield(Parent(algNum), L);
  return RepresentationMatrix(RelativeField(F, L)!algNum);
end function;

weilRestrictionMatrix:=function (alpmat, F, L)
  return BlockMatrix(Nrows(alpmat), Ncols(alpmat), [weilRestriction(alpmat[i][j], F, L): i in
[1..Nrows(alpmat)], j in [1..Ncols(alpmat)]]);
end function;

representationsFromCharacters :=function(n, group, field)

```

```

local EresCT, irrResCT, CT, charRing, representations, resCT, irrGModules,
charIrrGModules, decomp, rest, newModule, absIrrModules, absCT, absDecomp, absRest,
newAbsIrrMod, reprField, weilResModule, irrModules;
EresCT, irrResCT, CT, charRing := charactersOfFaithfulRepresentations(n, group, field);
if #EresCT eq 0 then
    return [];
end if;
representations := [];
resCT := [charRing!chr: chr in EresCT];
irrGModules := [(irrMod): irrMod in IrreducibleModules(group, field: Characters:=irrResCT)|
    Dimension(irrMod) le n];
charIrrGModules := [Character(irrMod): irrMod in irrGModules];
for character in resCT do
    decomp, rest := Decomposition(charIrrGModules, character);
    if rest eq Zero(charRing) then
        newModule := DirectSum(MultisetToSequence({*irrGModules[i]^Integers()!decomp[i]: i in
[1..#decomp]*})));
        Include(~representations, sub<GL(n, field)| ActionGenerators(newModule)>);
    else
        printf "Warning: Using slow method\n";
        absIrrModules := AbsolutelyIrreducibleModules(group);
        absCT := [Character(module): module in absIrrModules];
        absDecomp, absRest := Decomposition(absCT, character);
        newAbsIrrMod := [];
        for i:=1 to #absIrrModules do
            reprField := BaseRing(absIrrModules[i]);
            weilResModule := GModule(group, [weilRestrictionMatrix(mat, Rationals(), reprField):
mat in ActionGenerators(absIrrModules[i])]);
            weilResModule := ChangeRing(weilResModule, field);
            irrModules := Decomposition(weilResModule);
            Include(~newAbsIrrMod, irrModules[1]);
        end for;

        newModule := DirectSum(MultisetToSequence({*newAbsIrrMod[i]^Integers()!absDecomp[i]: i in
[1..#absDecomp]*})));
        if Character(newModule) eq character then
            Include(~representations, MatrixGroup(newModule));
        else
            return "Reconstruction of representation from character failed,
representation afforded by character %o is missing\n", character;
        end if;
    end if;
end for;
return representations;
end function;

gln:=function(n, field: progress:=false)
local resSubgroups, subGroups;
if Degree(field) eq 1 then
   ffield:=QNF();
else
   ffield:=field;
end if;
subGroups:=subgroupsNonchecked(n, field);
nn:=1;
resSubgroups:=[];
for subgroupsNC in subGroups do
    if progress then

```

```

    printf "\b"^(Ceiling(Log(10,#subGroups))+31) cat "Checking subgroup No. %*o of %o
",Ceiling(Log(10,#subGroups)),nn,#subGroups;
end if;
    nn:=nn+1;
    resSubgroups cat:=representationsFromCharacters(n,subgroupsNC,field);
end for;
printf "\n\n";
return (resSubgroups);
end function;

sln:=function(n,field: progress:=false)
    local glnList,slnList;
    glnList:=gln(n,field: progress);
    slnList:=[g: g in glnList|forall{gg: gg in GeneratorsSequence(g)|Determinant(gg) eq 1}];
    return slnList,glnList;
end function;

```

REFERENCES

- [1] M. Andreatta, J. Wiśniewski, *On the Kummer construction*. Rev. Mat. Complut. 23 (2010), no. 1, 191–215.
- [2] E. Ascher, H. Grimmer, *Comment on a paper by Tahara on the finite subgroups of $GL(3, \mathbb{Z})$* . Nagoya Math. J. 48 (1972), 203.
- [3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.
- [4] D. Burek, *Zeta function of some Kummer Calabi-Yau 3-folds*. Manuscripta Math. 174 (2024), no. 3-4, 703–730.
- [5] D. Burek, *Higher dimensional Calabi-Yau manifolds of Kummer type*. Math. Nachr. 293 (2020), no. 4, 638–650.
- [6] R. Bülow, J. Neubüser, H. Wondratschek, *On crystallography in higher dimensions. I. General definitions*, Acta Cryst. (1971). A27, 517–520.
- [7] R. Bülow, J. Neubüser and H. Wondratschek, *On crystallography in higher dimensions. II. Procedure of computation in $\mathbf{R}_4$* Acta Cryst. (1971). A27, 520–523.
- [8] R. Bülow, J. Neubüser and H. Wondratschek, *On crystallography in higher dimensions. III. Results in $\mathbf{R}_4$* Acta Cryst. (1971). A27, 523–535.
- [9] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006.
- [10] S. Cynk, M. Schütt, *Generalised Kummer constructions and Weil restrictions*. J. Number Theory 129 (2009), no. 8, 1965–1975.
- [11] S. Cynk and K. Hulek, *Higher-dimensional modular Calabi-Yau manifolds*, Canad. Math. Bull. 50 (2007), 486–503.
- [12] E. C. Dade, *The maximal finite groups of 4×4 integral matrices*. Illinois J. Math. 9 (1965), 99–122.
- [13] S. A. Filippini, A. Garbagnati, *A rigid Calabi-Yau three-fold*. Adv. Theor. Math. Phys. 15 (2011), no. 6, 1745–1787.
- [14] R. M. Guralnick, M. Lorenz, *Orders of finite groups of matrices*. Groups, rings and algebras, 141–161, Contemp. Math., 420, Amer. Math. Soc., Providence, RI, 2006.
- [15] J. Kuzmanovich, A. Pavlichenkov, *Finite groups of matrices whose entries are integers*. Amer. Math. Monthly 109 (2002), no. 2, 173–186.
- [16] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*. J. Reine Angew. Math. 101 (1887), 196–202.
- [17] G. Nebe. *Finite subgroups of $GL_n(\mathbb{Q})$ for $25 \leq n \leq 31$* . Comm. Algebra, 24(7), 2341–2397, 1996.
- [18] G. Nebe and W. Plesken. *Finite rational matrix groups*. Mem. Amer. Math. Soc., 116(556), 1995.

- [19] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. V. The eight-dimensional case and a complete description of dimensions less than ten*, Math. Comp. **34** (1980), no. 149, 277–301.
- [20] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. IV. Remarks on even dimensions with applications to $n = 8$* , Math. Comp. **34** (1980), no. 149, 259–275.
- [21] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. III. The nine-dimensional case*, Math. Comp. **34** (1980), no. 149, 245–258.
- [22] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. II. The six dimensional case*, Math. Comp. **31** (1977), no. 138, 552–573.
- [23] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. I. The five and seven dimensional cases*, Math. Comp. **31** (1977), no. 138, 536–551.
- [24] W. Plesken and M. E. Pohst, *On maximal finite irreducible subgroups of $\mathrm{GL}(n, \mathbf{Z})$. I. The five and seven dimensional case. II. The six dimensional case*, Bull. Amer. Math. Soc. **82** (1976), no. 5, 757–758.
- [25] S.-S. Roan, *Intermediate Jacobian and Some Arithmetic Properties of Kummer-surface-type CY 3-folds*, arXiv:math/0407193 [math.AG].
- [26] P. Samuel, Algebraic theory of numbers. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, MA, 1970.
- [27] I. Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen*. Berl. Ber. 1905, 77-91 (1905).
- [28] J.-P. Serre. *Linear Representations of Finite Groups. Graduate Texts in Mathematics*, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977.
- [29] J.-P. Serre, *Bounds for the orders of the finite subgroups of $G(k)$* . Group representation theory, 405–450, EPFL Press, Lausanne, 2007.
- [30] H. M. Stark, *On the "gap" in a theorem of Heegner*. J. Number Theory 1 (1969), 16–27.
- [31] K. I. Tahara, *On the finite subgroups of $\mathrm{GL}(3, \mathbf{Z})$* . Nagoya Math. J. 41 (1971), 169–209.

FACULTY OF MATHEMATICS AND INFORMATICS, JAGIELLONIAN UNIVERSITY, KRAKÓW, POLAND
 Email address: daniil.yurshevich@student.uj.edu.pl