Publ. Math. Debrecen
60 / 1-2 (2002), 179–191

On the existence of finite Galois stable groups over integers in unramified extensions of number fields

By D. A. MALININ (Minsk)

Abstract. Let E/F be a normal unramified number field extension with Galois group Γ of degree d, and let $\mathcal{O}_E$ be the ring of integers in E. It is proved that for given integers n, t such that $n \geqslant h\phi_E(t)d$, where h is the exponent of the class group of F and $\phi_E(t)$ is the generalized Euler function, there is a finite abelian Γ-stable subgroup $G \subset GL_n(\mathcal{O}_E)$ of exponent t such that the matrix entries of all $g \in G$ generate E over F. This result has certain arithmetic applications for totally real extensions, and a construction of totally real extensions having a prescribed Galois group is given.

1. Introduction

In this paper we consider some unramified Galois extension E/F of finite degree d with Galois group Γ for number fields E and F, and a finite abelian subgroup $G \subset GL_n(E)$ of given exponent t, where we assume that G is stable under the natural coefficientwise Γ-action.

Throughout this paper $\mathcal{O}_K$ denotes the maximal order of a number field K and $F(G)$ denotes a field that is obtained via adjoining to F all matrix coefficients of all matrices $g \in G$.

The main objective of this paper is to prove the existence of abelian Γ-stable subgroups $G \subset GL_n(R)$ for a given n and a given exponent t of G (R denotes certain Dedekind subrings of E, but the most interesting case is $R = \mathcal{O}_E$) such that $F(G) = E$ provided some reasonable restrictions for the fixed normal extension E/F and integers n, t, d hold true. A

Mathematics Subject Classification: Primary 20C10; Secondary 11R33.
Key words and phrases: integral representations, Galois group, algebraic integers, unramified extensions, Galois algebras.

lower bound for possible degrees n of representations of G is established: $n \geqslant C = C(E, F, d, t, h)$ such that $\phi_E(t)d \leqslant C \leqslant \phi_E(t)dh$, where h is the exponent of the class group of F, $\phi_E(t) = [E(\zeta_t) : E]$ is the generalized Euler function for a field E (ζ_t denotes a primitive t-root of 1). It is also proved that in some cases the upper bound is improvable (Theorem 1, parts 1), 3), 4)) though the lower bound $C = \phi_E(t)d \leqslant n$ can not be improved (Proposition 2).

These results have some applications to finite arithmetic groups, their cohomologies and positive definite quadratic lattices over the rings of integers in totally real number fields (see [B], [M1], [M4]). Some results related to Galois stability for orders in finite dimensional algebras can be found in [RW]. An explicit construction of totally real unramified field extensions is useful in this situation. Some interesting constructions of unramified and totally real (and also imaginary) number fields are obtained in papers [MB], [Ma], [K], [Y], see also [P]; certain computer calculations using KANT and PARI can be helpful for this purpose (see e.g. [Ma], [Y]). Another construction of totally real unramified extensions having a prescribed Galois group is given in Theorem 3.

The paper is organized as follows. The statements of results are given in Section 2; Sections 3, 4, 5 are devoted to their proofs.

Notation

Most of the symbols and notations that we use in this paper are traditional. $\mathbb{Q}$ and $\mathbb{Q}_p$ denote the field of rationals and p-adic rationals. $\mathbb{Z}$ and $\mathbb{N}$ denote the ring of rational integers and natural numbers, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of real and complex numbers. $GL_n(R)$ denotes the general linear group over R. We write $[E : F]$ for the degree of the field extension E/F. The maximal order of a number field K is denoted by $\mathcal{O}_K$. Throughout this paper we write Γ for Galois groups, $\sigma, \gamma \in \Gamma$ for the elements of Γ. We write ζ_t for a primitive t-root of 1; $\phi_K(t) = [K(\zeta_t) : K]$ denotes the generalized Euler function for a field K; I_m stands for a unit $m \times m$-matrix. $\det M$ denotes the determinant of a matrix M, and ${}^tM$ denotes a matrix transposed to M. If G is a finite linear group, $F(G)$ denotes a field obtained by adjoining to F all matrix coefficients of all matrices $g \in G$. For Γ acting on G and any $\sigma \in \Gamma$ and $g \in G$ we write g^σ for the image of g under σ-action. K^Γ denotes a subfield of Γ-stable elements of a field K, $\dim_K A$ denotes the dimension of K-algebra A over a field K. The full matrix algebra over R is denoted by $M_n(R)$.

2. The results

Let E denote a finite extension of an algebraic number field F which is different from F. Let $\mathcal{O}'_E$ denote the intersection of valuation rings of all ramified prime ideals in the ring $\mathcal{O}_E$, and let $\mathcal{O}'_F = F \cap \mathcal{O}'_E$. Since the rings $\mathcal{O}'_E$ and $\mathcal{O}'_F$ are semilocal, it is known that they are principal ideal domains.

Theorem 1. *Let $d > 1$, $t > 1$ be given rational integers, and let E/F be a normal unramified extension of algebraic number fields of degree d with Galois group Γ.*

1) *If $n \geqslant \phi_E(t)d$, there is a finite abelian Γ-stable subgroup $G \subset GL_n(\mathcal{O}'_E)$ of exponent t such that $E = F(G)$.*
2) *If $n \geqslant \phi_E(t)dh$, and h is the exponent of the class group of F, there is a finite abelian Γ-stable subgroup $G \subset GL_n(\mathcal{O}_E)$ of exponent t such that $E = F(G)$.*
3) *If $n \geqslant \phi_E(t)d$ and h is relatively prime to n, then G given in 1) is conjugate in $GL_n(F)$ to a subgroup of $GL_n(\mathcal{O}_E)$.*
4) *If d is odd, then G given in 1) is conjugate in $GL_n(F)$ to a subgroup of $GL_n(\mathcal{O}_E)$.*

In all cases above G can be constructed as a group generated by matrices $g^\gamma, \gamma \in \Gamma$ for some $g \in GL_n(E)$.

The results related to Galois stability of finite groups in situations similar to ours arise in the theory of definite quadratic lattices, arithmetic groups and Galois cohomologies. More precisely, let E be a totally real number field, H an algebraic subgroup of $GL_n(\mathbb{C})$ defined over a subfield F of E. If H is definite in the following sense: the real Lie group $H(\mathbb{R})$, the subgroup of $\mathbb{R}$-points, is compact, then the subgroup $H(\mathcal{O}_E)$ of $\mathcal{O}_E$-points of H is a finite Γ-stable subgroup, and the latter condition has some interesting consequences ([B], [BK], [M1], see also [Ro]). These results are also closely connected with some aspects of integral representations of finite groups, see [M1], [M2], [M3]. In our context we study whether a given field E normal over F can be realized as a field $E = F(G)$ in both cases $G \subset GL_n(\mathcal{O}'_E)$ and $G \subset GL_n(\mathcal{O}_E)$, and if this is so what are the possible orders n of matrix realizations and the structure of G.

Theorem 1 gives a positive answer to the question: whether it is possible to realize any normal unramified number field extension E/F as

$E = F(G)$ for some $G \subset GL_n(\mathcal{O}_E)$ provided $n \geqslant \phi_E(t)dh$. We prove that any finite normal field extension E/F can be obtained as $F(G)/F$ if $n \geqslant \phi_E(t)d$ for some $G \subset GL_n(E)$. In fact, we construct some Galois algebras in the sense of [ILF], and we establish the lower bounds for their possible dimensions n. In Proposition 2 it is proved that the restrictions for the given integers n, t, and d in Theorem 1 can not be improved.

Proposition 2. *Let E/F be a given normal extension of algebraic number fields with Galois group Γ, $[E : F] = d$, and let $G \subset GL_n(E)$ be a finite abelian Γ-stable subgroup of exponent t such that $E = F(G)$ and n is the minimum possible. Then $n = d\phi_E(t)$ and G is irreducible under conjugation in $GL_n(F)$. Moreover, if G has the minimal possible order, then G is a group of type $(t, t, \ldots, t)$ and order t^m for some positive integer $m \leqslant d$.*

The conditions of the following theorem were considered by L. Moret-Bailly [MB] in more general situation. In general, the existence of global fields with a given Galois group and prescribed local properties for ramification is a rather subtle question. L. Moret-Bailly proved the existence of relative extensions of number fields that have prescribed local structure of ramification over a given set of prime divisors and unramified elsewhere. However, our construction in Theorem 3 gives totally real unramified extensions in a more explicit and simple way.

Theorem 3. *For a given finite group Γ there are infinitely many normal unramified extensions of totally real fields E/F having the Galois group Γ.*

Theorem 3 combined with Theorem 1 can be used for constructioning finite arithmetic subgroups of algebraic groups of definite type that have been mentioned above. For example, let $G(\mathcal{O}_E)$ be a subgroup of $\mathcal{O}_E$-points of the orthogonal group $O_n(f)$ of a totally positive definite quadratic form f (i.e. all conjugates f^σ are positive definite) over a totally real number field $F \subset E$. Then $G(\mathcal{O}_E)$ is finite (see e.g. [R], Theorem A) and stable under the action of Γ, the Galois group of E/F. Theorem 1 gives a construction of a finite Γ-stable $G \subset GL_n(\mathcal{O}_E)$ such that $G \not\subset GL_n(\mathcal{O}_F)$. By Theorem 3 there are infinitely many unramified extensions E/F such that for a totally positive definite quadratic form f determined by a symmetric matrix $\sum_{g\in G} {}^t gg$ we have $G \subset G(\mathcal{O}_E) \not\subset GL_n(F)$, which would be impossible for a wide class of ramified extensions E/F, mainly for $F = \mathbb{Q}$ (see [B], [BK], [M1] and [M4]). Moreover, the condition of Theorem 1 for

G to be abelian is convenient to represent G as a finite commutative etale group scheme using the equivalence between finite etale group schemes and finite Galois modules (see e.g. [W], Sections 6.3 and 6.4).

3. Proof of Theorem 1

PROOF of Theorem 1. For any number field extension L/L_1 both of the rings $\mathcal{O}'_L$ and $\mathcal{O}'_{L_1}$ are semilocal, so they are principal ideal rings, and $\mathcal{O}'_L$ has a basis over $\mathcal{O}'_{L_1}$. We start with the proof of 1). For a given basis $w_1, w_2, \ldots, w_n$ of $\mathcal{O}'_E$ over $\mathcal{O}'_F$ we intend to construct a matrix $g = [g_{ij}]_{i,j} = \sum_{i=1}^{d} B_i w_i$ and pairwise commuting matrices B_i in such a way that the normal closure of the field $F(g_{11}, g_{12}, \ldots, g_{nn})$ over F coincides with E, and so the group G generated by $g^\sigma, \sigma \in \Gamma$ is an abelian Γ-stable group of exponent t. Firstly, we determine the eigenvalues that matrices B_i should have if g has the prescribed set of eigenvalues. Collecting the given eigenvalues of pairwise commuting semisimple matrices and using the regular representation, we construct a Γ-stable abelian group G for integral parameters given in proposition.

The proof of 1) is used in the proof of the rest of the theorem. In fact, certain results from the theory of representations of orders in semisimple algebras (see [CR], Section 75) are applied to the order $D = \mathcal{O}_F[B_1, B_2, \ldots, B_d] \subset A$ inside the F-algebra $A = F[B_1, B_2, \ldots, B_d]$. The claim of 2), 3) and 4) is that the construction of the representation of G given in 1) can be realalized over $\mathcal{O}_E$ without using an integral basis of $\mathcal{O}'_E$ over $\mathcal{O}'_F$ (in general, the ring $\mathcal{O}_E$ need not have a basis over $\mathcal{O}_F$.) This can be reached by using the Steinitz–Chevalley theorem for modules over Dedekind rings which is applied to the order D or a direct sum of its copies, and also one Schur's result for 3) and a result proved by FRÖHLICH [F] for 4).

PROOF of 1). We consider two different cases in our proof.

Case 1. We suppose that $F(\zeta_t)$ and E are linearly disjoint over F and $[E : F] = d$. In this case $\phi_E(t) = \phi_F(t)$. Let $w_1 = 1, w_2, \ldots, w_d$ be a basis of $\mathcal{O}'_E$ over $\mathcal{O}'_F$, and let Γ be the Galois group of $E(\zeta_t)$ over $F(\zeta_t)$. Let g be a semisimple $d \times d$-matrix having eigenvalues $\zeta_t, 1, \ldots, 1$. Using the expansion $g = B_1 + w_2 B_2 + \cdots + w_d B_d$ we can construct the matrices B_i, $i = 1, 2, \ldots, d$, and we can prove that the group G generated by $g^\gamma, \gamma \in \Gamma$

is an abelian Γ-stable group of exponent t. Let us consider a matrix $W = [w_i^{\sigma_j}]_{i,j}$ for $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_d\} = \Gamma$. Since E/F is unramified, $\det W$ is a unit of $\mathcal{O}'_E$. Denote by W_i the matrix W whose i-th column is replaced by d chosen eigenvalues $\zeta_t, 1, \ldots, 1$ of g. We can calculate

$$\lambda_i = \frac{\det W_i}{\det W}$$

and construct matrices B_i as the regular representation $B_i = R(\lambda_i)$ of $\lambda_i \in \mathcal{O}'_E[\zeta_t]$ in the basis $w_1, w_2, \ldots, w_d$ of the ring extension $\mathcal{O}'_E[\zeta_t] \supset \mathcal{O}'_F[\zeta_t]$ which is obtained via adjoining ζ_t to the ground ring. Let α_{ij} be the coefficients of the inverse matrix $W^{-1} = [\alpha_{ij}]_{i,j}$. Then $\alpha_{i1}^{\sigma_j} = \alpha_{ij}$ and $\lambda_i = (\zeta_t - 1)\alpha_{i1}$ for $i \neq 1$, and $\lambda_1 = 1 + (\zeta_t - 1)\alpha_{11}$. So $\lambda_i^{\sigma_j} = (\zeta_t - 1)\alpha_{i1}^{\sigma_j} = (\zeta_t - 1)\alpha_{ij}$ for $i \neq 1$, and $\lambda_1^{\sigma_j} = (\zeta_t - 1)\alpha_{11}^{\sigma_j} + 1 = (\zeta_t - 1)\alpha_{1j} + 1$. Since any linear relation

$$k_1(\lambda_1 - 1) + \sum_{i=2}^{d} k_i \lambda_i = 0, \quad k_i \in F(\zeta_t),\ i = 1, 2, \ldots, d$$

implies the linear relation

$$k_1(\lambda_1^{\sigma_j} - 1) + \sum_{i=2}^{d} k_i \lambda_i^{\sigma_j} = 0, \quad k_i \in F(\zeta_t),\ i = 1, 2, \ldots, d$$

for all $\sigma_j \in \Gamma$, this would also imply $\det W^{-1} = 0$, which is impossible. Therefore, $\lambda_1 - 1, \lambda_2, \ldots, \lambda_d$ generate the field $E(\zeta_t)$ over$F(\zeta_t)$, and so $B_1 - I_d, B_2, \ldots, B_d$ generate the $F(\zeta_t)$-span $F(\zeta_t)[B_1, \ldots, B_d]$ over $F(\zeta_t)$. Note that B_i can be expressed as a linear combination of g^{σ_i}, $i = 1, 2, \ldots, d$ with coefficients in E : $B_i = \sum_{j=1}^{d} \alpha_{ij} g^{\sigma_j}$. This can be obtained from the system of matrix equations

$$g^{\sigma_j} = \sum_{i=1}^{d} w_i^{\sigma_j} B_i, \quad j = 1, 2, \ldots, d$$

if we consider B_i as indeterminates. Since G has exponent t, $F(\zeta_t)$ is a splitting field for G, the group generated by all $g^\sigma, \sigma \in \Gamma$. Therefore, the dimension of $E(\zeta_t)$-span $E(\zeta_t)G = E(\zeta_t) \otimes_{F(\zeta_t)} F(\zeta_t)G$ over $E(\zeta_t)$ is d, and so the $F(\zeta_t)$-dimension of the $F(\zeta_t)$-span $F(\zeta_t)G$ is also d.

Let us denote by E' the image of $E(\zeta_t)$ under the regular representation of $E(\zeta_t)$ over $F(\zeta_t)$ in the basis $w_1, \dots, w_d$. Then $A = E(\zeta_t)G = E(\zeta_t) \otimes_{F(\zeta_t)} F(\zeta_t)G$, the $E(\zeta_t)$-span of G, is the Galois E'-algebra in the sense of [ILF], that is, it is an associative and commutative separable E'-algebra having a normal basis. We can choose idempotents

$$\varepsilon_i = \frac{1}{\zeta_t - 1}(g^{\sigma_j} - I_d), \quad j = 1, 2, \dots, d$$

as a normal basis of A over E' so that $\varepsilon_j = \varepsilon_1^{\sigma_j}$.

We have $F(\zeta_t)G = F(\zeta_t)[< g^{\sigma_1}, \dots, g^{\sigma_d} >] = F(\zeta_t)[(g - I_d)^{\sigma_1}, \dots, (g - I_d)^{\sigma_d}]$, and $\dim_{F(\zeta_t)} F(\zeta_t)G = d$. As the length of the orbit of $M = [m_{ij}] = (g - I_d)$ under Γ-action is d, we can use the coefficients of matrices M^{σ_i}, $i = 1, 2, \dots, d$ to construct an element $\theta = \sum_{i,j} k_{ij} m_{ij}$, $k_{ij} \in F(\zeta_t)$, which generates a normal basis of $E(\zeta_t)/F(\zeta_t)$. Therefore, for any given $\alpha \in E(\zeta_t)$ we have $\alpha = \sum_i k_i \theta^{\sigma_i}$ for some $k_i \in F(\zeta_t)$.

Therefore, our choice of eigenvalues implies that $F(\zeta_t)(G) = E(\zeta_t)$.

Now, we can apply the regular representation R_F of $\mathcal{O}'_F[\zeta_t]$ over $\mathcal{O}'_F$ to matrices $M = [m_{ij}]_{i,j}, m_{ij} \in \mathcal{O}'_F[\zeta_t]$ in the following way: $R_F(M) = [R_F(m_{ij})]_{i,j}$. So, using R_F for all components of matrices $B_i \in M_n(F(\zeta_t))$ we can obtain an abelian subgroup $G \subset GL_{n_1}(E), n_1 = [F(\zeta_t) : F]d$ of exponent t which is Γ-stable if we identify the isomorphic Galois groups of the extensions E/F and $E(\zeta_t)/F(\zeta_t)$. We have again $\dim_F FG = \dim_E EG$, E is again a Galois algebra, and $F(G) = E$. Now, using the natural embedding of G to $GL_n(E), n \geqslant n_1$, we complete the proof of Theorem 1 in the Case 1).

Case 2. By virtue of Case 1 we can consider the case when the intersection $F_0 = E \cap F(\zeta_t) \neq F$. We can use the regular representation R of $\mathcal{O}'_E$ over $\mathcal{O}'_F$. Let $\Gamma_0 = \{\sigma'_1, \sigma'_2, \dots, \sigma'_d\}$ be the set of some extensions of elements $\Gamma = \{\sigma_1, \sigma_2, \dots, \sigma_d\}$ to $E(\zeta_t)/F$, and let $w_1 = 1, w_2, \dots w_d$ be a basis of $\mathcal{O}'_E$ over $\mathcal{O}'_F$. So we can use our previous notation and apply a similar argument as in the Case 1 of the proof for the construction of $g = \sum_{i=1}^d B_i w_i$ and matrices B_i as the regular representations R_0 of eigenvalues

$$\lambda_i = \frac{\det W_i}{\det W} = \sum_{j=1}^{\phi_E(t)} \lambda_{ij} \zeta^j, \quad i = 1, 2, \dots, d,$$

in the following way: we consider

$$B_i = R_0(\lambda_i) = \sum_{j=1}^{\phi_E(t)} R(\lambda_{ij})\zeta^j,$$

where R is the regular representation of $\mathcal{O}'_E$ over $\mathcal{O}'_F$. We also have $\lambda_1^{\sigma'_j} = \alpha_{1j} + 1, \lambda_i^{\sigma'_j} = \alpha_{ij}$ for $j = 2, \dots, d$. Now, if we have any linear relation between the rows of the matrix $[\alpha_{ij}(\zeta_t^{\sigma'_j} - 1)]_{i,j}$, this would imply a linear relation between its columns, and so the columns of $W^{-1} = [\alpha_{ij}]$ are linearly dependent, and $\det W^{-1} = 0$ which is a contradiction. So, again we obtain that $\lambda_1 - 1, \lambda_2, \dots, \lambda_d$ are linearly independent over F, so $\dim_F FG' = \dim_F F[B_1 - I_d, B_2, \dots, B_d] = \dim_E EG' = d$ for G' generated by $g^{\sigma'_i}$, $i = 1, 2, \dots, d$. As earlier we can consider the regular representation $R_E(B_i)$ for the coefficients of matrices B_i in the ring extension $\mathcal{O}'_E[\zeta_t] \supset \mathcal{O}'_E$. So we obtain $g_0 = \sum_{i=1}^d R_E(B_i)w_i$, and we can take a group G generated by all $g_0^{\sigma_i}$, $i = 1, 2, \dots, d$. Since $[E(\zeta_t) : F] = [E(\zeta_t) : E][E : F] = \phi_E(t)d$, the order $n = \phi_E(t)d$ coincides with the integer required in the formulation of Theorem 1. In this way we can construct a Γ-stable group G that satisfies the conditions of 1) in Theorem 1.

Proof of 2). Let us consider an $\mathcal{O}_F$-order $D{=}\mathcal{O}_F[B_1, B_2, \dots, B_d]{\subset}A$ in a semisimple F-algebra $A = F[B_1, B_2, \dots, B_d]$ where B_i are $n' \times n'$-matrices taken from 1). Using our construction of B_i we can assume $n' = \phi_E(t)d$. Let M be the corresponding representation module in n'-dimensional F-vector space V. We claim that the matrices B_i from 1) can be realalized over $\mathcal{O}_F$ via taking a direct sum of h copies of $\mathcal{O}_F$-module M. We can use the Steinitz–Chevalley theorem (see e.g. [CR]) for M to obtain a decomposition: $M = v_1\mathcal{O}_F + v_2\mathcal{O}_F + \dots + v_{n'-1}\mathcal{O}_F + v_{n'}\mathfrak{a}\mathcal{O}_F$ for some elements $v_1, v_2, \dots, v_{n'} \in V$ and some fractional ideal $\mathfrak{a}$ of $\mathcal{O}_F$. Taking a direct sum $M_1 = \oplus M$ of h copies of M we conclude that the Steinitz class of M_1 is $\mathfrak{a}^h$, so it is trivial, and M_1 becomes a free $\mathcal{O}_F$-module: $M_1 = c_1\mathcal{O}_F + c_2\mathcal{O}_F + \dots + c_{hn'}\mathcal{O}_F$ for some elements $c_1, c_2, \dots, c_{hn'} \in FM_1$. Therefore, the matrices $B'_1 = \oplus_1^h B_1, B'_2 = \oplus_1^h B_2, \dots, B'_d = \oplus_1^h B_d$ (h copies of B_i) are $GL_n(F)$-conjugate to matrices contained in $GL_{hn'}(\mathcal{O}_F)$ (we can consider $n = hd\phi_E(t)$ for a moment, and later extend the result to any $n \geqslant hd\phi_E(t)$ via taking direct sums). We can conclude that all matrices $g^\sigma, \sigma \in \Gamma$ are also conjugate in $GL_n(F)$ to matrices contained in

$GL_n(O_E)$. Since G is generated by these matrices, we obtain the claim of 3) for matrices of order $hd\phi_E(t)$. For extending this result to arbitrary $n \geqslant hd\phi_E(t)$ we can fix positive integers k and r with $n = khd\phi_E(t)+r, r < hd\phi_E(t)$ and take a direct sum of k copies of the constructed realization G and r copies of unit representations. This completes the proof of 2).

PROOF of 3). This follows from the assertion (75.5) in [CR] applied to the order $D=\mathcal{O}_F[B_1, B_2, \ldots, B_d] \subset A$ in the F-algebra $A=F[B_1, B_2, \ldots, B_d]$. Since all matrices B_i, $i = 1, 2, \ldots, d$ are conjugate in $GL_n(F)$ to matrices contained in $GL_n(O_F)$ (here we can consider $n = d\phi_E(t)$) we conclude that all matrices $g^\sigma, \sigma \in \Gamma$ are also conjugate in $GL_n(F)$ to matrices from $GL_n(O_E)$. Since G is generated by these matrices, we obtain the claim of 3).

PROOF of 4). By [F], Theorem 4.3, in any normal unramified number fields extension of odd degree the ring of integers has a free basis. In our case $\mathcal{O}_E = w_1\mathcal{O}_F + w_2\mathcal{O}_F + \cdots + w_d\mathcal{O}_F$ for some $w_1, w_2, \ldots, w_d$. Therefore, the matrices B_i, $i = 1, 2, \ldots, d$ are conjugate in $GL_n(F)$ to matrices from $GL_n(\mathcal{O}_F)$ (and our argument of 1) can be directly applied to the rings $\mathcal{O}_E$ and $\mathcal{O}_F$ instead of $\mathcal{O}'_E$ and $\mathcal{O}'_F$). This implies that G is conjugate in $GL_n(F)$ to a subgroup of $GL_n(\mathcal{O}_E)$ as it was claimed.

This completes the proof of Theorem 1. □

4. Proof of Proposition 2

PROOF of Proposition 2. We can use the proof of Theorem 1.

Let $G \subset GL_n(E)$ be a group given in the formulation of Proposition 2, and let n be the minimum possible. Then we have the following decomposition of the E-span $A = EG$:

$$A = \varepsilon_1 A + \varepsilon_2 A + \cdots + \varepsilon_k A$$

for some primitive idempotents $\varepsilon_1, \ldots, \varepsilon_k$ of A.ε_i are conjugate under the action of the Galois group $\Gamma = \{\sigma_1, \ldots, \sigma_d\}$. For if the sum of $\varepsilon_i^{\sigma_j}$, $j = 1, 2, \ldots, d$ is not I_n, then $I_n = e_1 + e_2$ for $e_1 = \varepsilon_1^{\sigma_1} + \cdots + \varepsilon_1^{\sigma_d}$ and $e_2 = I_n - e_1$, and e_1, e_2 are fixed by Γ, so e_1, e_2 are conjugate in $GL_n(F)$ to a diagonal form. Since either of 2 components e_iG has rank smaller than n, there is a matrix group satisfying the conditions of Proposition 2 of smaller than n degree.

Therefore, $\varepsilon_i = \varepsilon_1^{\sigma_i}$, $k = d$ and the idempotents $\varepsilon_1, \ldots, \varepsilon_d$ form a normal basis of A. But the rank of a matrix ε_i is not smaller than $\phi_E(t)$. Indeed, $\varepsilon_i G$ contains an element $\varepsilon_i g$, for some $g \in G$ of order t such that $(\varepsilon_i g)^t = \varepsilon_i$, but $(\varepsilon_i g)^k \neq \varepsilon_i$ for $k < t$. We can find $g \in G$ in the following way. Since $I_n = \varepsilon_1 + \cdots + \varepsilon_k$ for any $h \in G$ of order t there is ε_j such that $(\varepsilon_j h)^t = \varepsilon_j$, but $(\varepsilon_j h)^k \neq \varepsilon_j$ for $k < t$, and the same property holds for $\varepsilon_j h$ with any $\sigma \in \Gamma$. Then using the property of normal basis $\varepsilon_k = \varepsilon_1^{\sigma_k}$ we can take $g = h^{\sigma_j^{-1}\sigma_i}$.

So, the irreducible component $\varepsilon_i G$ determines a faithful irreducible representation of a cyclic group generated by g. But if $T : C \to GL_r(E)$ is a faithful irreducible representation of a cyclic group C generated by an element g of order t, its degree r is equal to $\phi_E(t)$. It follows that the rank of matrices ε_i is $\phi_E(t)$. So the dimension of A over E is $\phi_E(t)d$.

If G is generated by g^γ, $\gamma \in \Gamma$ and its order is minimal, Γ-stability implies that g has d conjugates under Γ-action, and so G is an abelian group of type $(t, \ldots, t)$ and order t^m for some positive integer $m \leqslant d$. This completes the proof of Proposition 2. □

5. Proof of Theorem 3

Proof of Theorem 3. Firstly, a totally real normal extension $L/\mathbb{Q}$ of degree $n = l!$ will be constructed. For this purpose we can fix primes q_1, q_2, q_3 such that q_1 and a are relatively prime, and choose a polynomial $H(x) = (x - a_1 q_1)(x - a_2 q_2) \ldots (x - a_l q_l) + a q_1$ whose group has a transposition and one or 2 factors of odd degree modulo q_2, a $(l-1)$-cycle modulo q_3 for integers a_i large enough compared to $|q_1 a|$ and small compared to $|a_i - a_j|$, $i \neq j$ such that all roots of $H(x)$ are real. The splitting field L of $H(x)$ is totally real, and its Galois group is the symmetric group S_l.

Fix the set R of all primes ramified in $L/\mathbb{Q}$.

Let us consider the following conditions:

1) $F(x) = (x - b_1 p_1)(x - b_2 p_1) \ldots (x - b_n p_1) + p_1 b$
2) $b_1, b_2, \ldots, b_n \in \mathbb{Z}$ are different, and p_1 does not divide b. $2bn < (\prod_{j=1(j\neq i)}^{n} |b_i - b_j|) p_1^{n-2}$ for $i = 1, \ldots, n$.
3) $F(x)$ has a transposition and 1 or 2 factors of odd degree modulo p_2.
4) $F(x)$ has an $(n-1)$-cycle modulo p_3.

5) p_1, p_2, p_3 are primes not contained in $R \cup q$, and $q \notin R$ is a prime congruent to 1 modulo n.

The conditions 1) and 2) guarantee irreducibility of $F(x)$ since $F(x)$ is an Eisensteinian polynomial, and also all roots of $F(x)$ are real. Indeed, the coefficient of x^{n-1} in $x^n F(1/x + b_i p_1)$ is equal to $\prod_{j=1(j\neq i)}^{n}(b_i p_1 - b_j p_1)$. Hence for the roots $x_1, x_2, \ldots, x_n$ of $F(x)$ the following equality holds:

$$\left|\frac{1}{x_1 - b_i p_1} + \frac{1}{x_2 - b_i p_1} + \ldots \frac{1}{x_n - b_i p_1}\right| = \left|\frac{\prod\limits_{j=1(j\neq i)}^{n} |b_i p_1 - b_j p_1|}{b p_1}\right|,$$

and so

$$|x_{k_i} - b_i p_1| \leqslant \frac{n b p_1}{\prod\limits_{j=1(j\neq i)}^{n} |b_i p_1 - b_j p_1|}$$

provided $|x_{k_i} - b_i p_1| \leqslant |x_j - b_i p_1|$ for all $j \neq k_i$. Now, if $2nbp_1 < \prod_{j=1(j\neq i)}^{n} |b_i p_1 - b_j p_1|$, then $|x_{k_i} - b_j p_1| \leqslant \frac{1}{2}$, and all roots x_{k_i} are contained in the circles of radius $\frac{1}{2}$ with different centres $b_j p_1$, so there are no complex conjugates among x_{k_i}.

The conditions 3) and 4) imply coincidence of the Galois group of $F(x)$ and the symmetric group S_n.

It follows from the Frobenius density theorem ([Fr], see also [Ch], Theorem 42) that a given polynomial has the same factorization corresponding to the permutation of the given cycle type modulo infinitely many primes. Hence there is an integer M not divisible by p_1, p_2, p_3, q and the primes from R such that the congruence

6) $f(x) \equiv F(x) \pmod{M}$
implies that the Galois group of $f(x)$ is S_n.

Let K be the splitting field of $f(x)$. Then the q-cyclotomic field $\mathbb{Q}(\zeta_q)$ has a subfield of degree n over $\mathbb{Q}$ which can be determined as a splitting field of an integral polynomial $k(x)$. Let $h(x)$ be a polynomial of degree n whose splitting field is L. By Krasner's lemma there is $t_1 \in \mathbb{N}$ such that the congruences

7) $f(x) \equiv h(x) \pmod{p^{t_1}}$ for all $p \in R$
imply coincidence of the localizations: $L\mathbb{Q}_p = K\mathbb{Q}_p$ for $p \in R$. If the

maximal abelian subfield K_{ab} of K is not $\mathbb{Q}$ then $K_{ab} = \mathbb{Q}(\sqrt{r})$ for some $r \in \mathbb{Z}$, and for a large enough integer t_2 the congruence

8) $f(x) \equiv k(x) \pmod{q^{t_2}}$
implies $K \cap L = \mathbb{Q}$ by considering the ramification at q. But the composite KL is unramified over K because $L\mathbb{Q}_p = K\mathbb{Q}_p$ for all primes p ramified in L.

We can find a polynomial $f(x)$ satisfying the conditions 1)–8) so that its roots are real, according to 2). Indeed, using the weak approximation theorem (or the Chinese reminder theorem), we can satisfy 1) and 3)–8), and in the factorization $f(x) = (x - c_1)(x - c_2)\dots(x - c_n) + c_0$ the numbers c_i can be increased via adding some multiples of the moduli of congruences 3)–8) in order to make c_i, $i = 1, \dots, n$ big enough compared to c_0 and small compared to $|c_i - c_j|$, $i \neq j$ $(i, j \neq 0)$. Therefore, the fields $E = LK$ and K are totally real and the extension E/K is unramified, normal, and its Galois group is S_l. By Galois theory, for a prescribed finite group $\Gamma \subset S_l$ (we can take $l = |\Gamma|$) there is a normal subextension E/F, where $F = E^{\Gamma}$ is a subfield of Γ-fixed elements of E, which is also unramified and has Γ as the Galois group. This remark completes the proof of Theorem 3. □

References

[B] H.-J. Bartels, Zur Galoiskohomologie definiter arithmetischer Gruppen, *J. reine angew. Math.* **298** (1978), 89–97.

[BK] H.-J. Bartels and Y. Kitaoka, Endliche arithmetische Untergruppen der GL_n, *J. reine angew. Math.* **313** (1980), 151–156.

[Ch] N. G. Chebotarev, Foundations of Galois theory, vol. II, *OGIZ*, *Leningrad–Moscow*, 1937; German transl.: *Noordhoff,* 1950.

[CR] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, *Interscience*, *New York*, 1962.

[Fr] G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe, *Sitzber. Preussen Akad. Wiss.* (1896), 689–705.

[F] A. Fröhlich, Discriminants of algebraic number fields, *Math Zeitschr.* **74** (1960), 18–28.

[ILF] V. V. Ishkhanov, B. B. Lur'e and D. K. Faddeev, The embedding problem in Galois theory, *"Nauka"*, *Moscow*, 1988.

[K] T. Kondo, Algebraic number fields with the discriminant equal to that of quadratic number field, *J. Math. Soc. Japan* **47**, Nr. 1 (1995), 31–36.

[Ma] Christian Maire, On infinite unramified extensions, *Pacific J. Math.* **192**, Nr. 1 (2000), 135–142.

[M1] D. A. Malinin, Galois stability for integral representations of finite groups, *Algebra i analiz* **12**, Nr. 3 (2000), 106–145; English translation in *St. Petersburg Math. J.* **12**, Nr. 3.

[M2] D. A. Malinin, Integral representations of p-groups over local fields, *Dokl. Akad. Nauk SSSR* **309**, Nr. 5 (1989), 1060–1063; English translation in *Sov. Math. Dokl.* **40** (1990), Nr. 3.

[M3] D. A. Malinin, Integral representations over local fields for p-groups of a given class of nilpotency, *Algebra i analiz* **10**, Nr. 1 (1998), 58–67; English translation in *St. Petersburg Math. J.* **10**, Nr. 1.

[M4] D. A. Malinin, Integral representations of finite groups with Galois action, *Dokl. Russ. Akad. Nauk* **349**, Nr. 3 (1996), 303–305.

[MB] L. Moret-Bailly, Extensions de corps globaux a ramification et groupe de Galois donnes, *C.R. Acad. Sci. Paris* **311** (1990), 273–276.

[P] M. Pohst, Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper, *J. Reine angew. Math.* **278/279** (1975), 278–300.

[R] K. G. Ramanathan, The theory of units of quadratic and Hermitian forms, *Amer. J. of Math.* **73** (1951), 233–255.

[RW] J. Ritter and A. Weiss, Galois action on integral representations, *J. London Math. Soc. (2)* **46** (1992), 411–431.

[Ro] J. Rohlfs, Arithmetische definierte Gruppen mit Galois-operation, *Invent. Math.* **48** (1978), 185–205.

[W] W. C. Waterhouse, Introduction to affine group schemes, *Springer–Verlag, New York, Berlin, Heidelberg*, 1979.

[Y] K. Yamamura, Maximal unramified extensions of imaginary quadratic fields of small conductors, *Journal de Theorie des Nombres de Bordeaux* **9** (1997), 405–448.

D. A. MALININ
BELARUSIAN STATE PEDAGOGICAL UNIVERSITY MINSK, BELARUS
SOVETSKAYA STR. 18
220050 MINSK
BELARUS

E-mail: malinin@bspu.unibel.by

(Received April 23, 2001; revised September 6, 2001)