Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
25 (2009), 17–27
`www.emis.de/journals`
`ISSN 1786-0091`

ON FINITE LINEAR GROUPS STABLE UNDER GALOIS OPERATION

EKATERINA KHREBTOVA AND DMITRY MALININ

Abstract. We consider a Galois extension E/F of characteristic 0 and realization fields of finite abelian subgroups $G \subset GL_n(E)$ of a given exponent t. We assume that G is stable under the natural operation of the Galois group of E/F. It is proven that under some reasonable restrictions for n any E can be a realization field of G, while if all coefficients of matrices in G are algebraic integers there are only finitely many fields E of realization having a given degree d for prescribed integers n and t or prescribed n and d. Some related results and conjectures are considered.

1. Introduction

In this paper we continue studying some arithmetic problems [4] for representations of finite groups over algebraic number fields and arithmetic rings under the ground field extensions.

We consider some Galois extension E/F of finite degree d with the Galois group Γ for a field F of characteristic 0 and a finite abelian subgroup $G \subset GL_n(E)$ of the given exponent t, where we assume that G is stable under the natural coefficient-wise Γ-operation.

Throughout the paper O_E is the maximal order of E 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 such that $F(G) = E$ provided some reasonable restrictions for the fixed normal extension E/F and integers n, t, d hold and to study the interplay between the existence of Γ-stable groups G over algebraic number fields and over their rings of integers.

2000 *Mathematics Subject Classification.* 20C10, 11R33.

Key words and phrases. integral representations, Galois group, algebraic integers, Galois algebras.

The results related to the Galois stability of finite groups in the situation similar to ours arise in the theory of definite quadratic forms and Galois cohomologies of certain arithmetic groups if F is an algebraic number field and G is realized over its maximal order ([1], see also [12]). 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 $G \subset GL_n(E)$ and $G \subset GL_n(O_E)$, and if this is so what are the possible orders n of matrix realizations and the structure of G. Some similar questions for Γ-stable orders in simple algebras are considered in [10], see also [11] for some applications.

We give a positive answer to the first question: we prove that any finite normal field extension E/F can be obtained as $F(G)/F$ if $n \geq \phi_E(t)d$ where $\phi_E(t) = [E(\zeta_t) : E]$ is the generalized Euler function and ζ_t is a primitive t-root of 1. An explicit construction of these fields is given in Theorems 2 and in section 3. In fact, we construct some Galois algebras in the sense of [3], and we establish the lower bounds for their possible orders n. We show (see Proposition 1 in section 2) that the restrictions for the given integers n, t, and d in Theorem 2 can not be improved.

The situation becomes different if E is an algebraic number field and all matrix coefficients of $g \in G$ are algebraic integers.

The existence of any Galois stable subgroups $G \subset GL_n(O_E)$ such that $F(G) \neq F$ is a rather subtle question. In particular, for $F = \mathbf{Q}$ all fields $F(G)$ whose discriminant is divisible by an odd prime must contain non-trivial roots of 1 [2, 8, 6].

Our results have some applications to positive definite quadratic lattices, see section 2. Note that some interesting results on orthogonal decompositions of integral lattices can be found in [5].

NOTATIONS

We denote $\mathbf{C}$, $\mathbf{R}$ and $\mathbf{Q}$ the fields of complex, real and rational numbers. $\mathbf{Z}$ is the ring of rational integers. $GL_n(R)$ denotes the general linear group over a ring R. $[E : F]$ denotes the degree of the field extension E/F. Throughout this paper we write Γ for Galois groups, $\sigma, \gamma \in \Gamma$ for the elements of Γ. $\Gamma(\mathbf{p}) \subset \Gamma$ denotes the inertia subgroup of a prime ideal $\mathbf{p}$. Finite groups are usually denoted by capital letters G, H, and their elements by small letters, e.g. $g \in G$, $h \in H$. We write ζ_t for a primitive t-root of 1. We denote by $\phi_K(t) = [K(\zeta_t) : K]$ the generalized Euler function for a field K. I_m stands for a unit $m \times m$-matrix. $\det M$ is the determinant of a matrix M. If G is a finite linear group, $F(G)$ stands for 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-operation. $\dim_K A$ denotes the dimension of K-algebra A over the field K. $M_n(R)$ is the full matrix algebra over a ring R. O_K denotes the maximal order of a number field K.

2. Integral representations stable under the Galois operation

Let K be a totally real algebraic number field with the maximal order O_K, G an algebraic subgroup of the general linear group $GL_n(\mathbf{C})$ defined over the field of rationals $\mathbf{Q}$. Because of the embedding of G in $GL_n(\mathbf{C})$ the intersection $G(O_K)$ of $GL_n(O_K)$ and $G(K)$, the subgroup of K-rational points of G, can be considered as the group of O_K-points of an affine group scheme over $\mathbf{Z}$, the ring of rational integers. Assume G to be definite in the following sense: the real Lie group $G(\mathbf{R})$ is compact. The problem which is our starting point is the question: Does the condition $G(O_K) = G(\mathbf{Z})$ always hold true?

This problem is easily reduced to the following conjecture from the representation theory: Let $K/\mathbf{Q}$ be a finite Galois extension of the rationals and $G \subset GL_n(O_K)$ be a finite subgroup stable under the natural operation of the Galois group $\Gamma := \mathrm{Gal}(K/\mathbf{Q})$. Then there is the following

Conjecture 1. If K is totally real, then $G \subset GL_n(\mathbf{Z})$.

There are several reformulations and generalizations of the conjecture. Consider an arbitrary not necessarily totally real finite Galois extension K of the rationals $\mathbf{Q}$ and a free $\mathbf{Z}$-module M of rank n with basis $m_1, \ldots, m_n$. The group $GL_n(O_K)$ acts in a natural way on $O_K \otimes M \cong \bigoplus_{i=1}^n O_K m_i$. The finite group $G \subset GL_n(O_K)$ is said to be of A-type, if there exists a decomposition $M = \bigoplus_{i=1}^k M_i$ such that for every $g \in G$ there exists a permutation $\Pi(g)$ of $\{1, 2, \ldots, k\}$ and roots of unity $\epsilon_i(g)$ such that $\epsilon_i(g) g M_i = M_{\Pi(g)i}$ for $1 \leq i \leq k$. The following conjecture generalizes (and would imply) conjecture 1:

Conjecture 2. Any finite subgroup of $GL_n(O_K)$ stable under the Galois group $\Gamma = \mathrm{Gal}(K/\mathbf{Q})$ is of A-type.

For totally real fields K conjecture 2 reduces to conjecture 1.

Both conjectures are true in the case of Galois field extension $K/\mathbf{Q}$ with odd discriminant. Also some partial answers are given in the case of field extensions $K/\mathbf{Q}$ which are unramified outside 2.

Let $F(G)$ denote the field obtained via adjoining to F the matrix coefficients of all matrices $g \in G$. The following result was obtained in [2] (see also [8], [6] for the case of totally real fields).

The case $F = \mathbf{Q}$, the field of rationals, is specially interesting. The following theorem was proven in [2] using the classification of finite flat group schemes over $\mathbf{Z}$ annihilated by a prime p obtained by V. A. Abrashkin and J.-M. Fontaine:

Theorem 1. *Let $K/\mathbf{Q}$ be a normal extension with Galois group Γ, and let $G \subset GL_n(O_K)$ be a finite Γ-stable subgroup. Then $G \subset GL_n(O_{K_{ab}})$ where K_{ab} is the maximal abelian over $\mathbf{Q}$ subfield of K.*

Similar results for totally real extensions $K/\mathbf{Q}$ were considered earlier. In this case there are some interesting arithmetic applications to positive definite quadratic lattices and Galois cohomology.

Let us formulate a criterion for the existence of an integral realization of an abelian group G with properties introduced above. This theorem has interesting applications in [2], and [8].

Let E, L be finite extensions of a number field F. Let O'_E, O'_F, O'_L be semilocal rings that are obtained by intersection of valuation rings of all ramified prime ideals in the rings O_E, O_F, O_L. If $F = \mathbf{Q}$ we can define O_F to be the intersection of F and O_E. Let $w_1, w_2, \dots, w_d$ be a basis of O'_E over O'_F, and let D be a square root of the discriminant of this basis. By the definition $D^2 = \det[Tr_{E/F}(w_i w_j)]_{ij}$. It is known that $D = \det[w_m^{\sigma_k}]_{k,m}$. Let us suppose that some matrix $g \in GL_n(E)$ has order t ($g^t = I_n$) and all Γ-conjugates g^γ, $\gamma \in \Gamma$ generate a finite subgroup $G \subset GL_n(E)$ of exponent t. Let $\sigma_1 = 1$, $\sigma_2, \dots, \sigma_d$ denote all automorphisms of the Galois group Γ of E over F. Assume that $L = E(\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(n)})$ where $\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(n)}$ are the eigenvalues of the matrix g. We shall reserve the same notations for certain fixed extensions of σ_i to L. Automorphisms of L over F will be denoted $\sigma_1, \sigma_2, \dots, \sigma_r$, $r > d$. Theorem 2 below implies the existence of the group G provided $n \geq \phi_E(t)[E : F]$. Let $E = F(G)$ be obtained by adjoining to F all coefficients of all $g \in G$. For an appropriate set of d eigenvalues $\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(d)}$ which depends on the primitive idempotents of algebra LG the following Theorem is true (see also [2]):

Theorem A. *Let $G \subset GL_n(E)$ be irreducible under $GL_n(F)$-conjugation. Then G is conjugate in $GL_n(F)$ to a subgroup of $GL_n(O'_E)$ if and only if all determinants*

$$D_k = \det \begin{vmatrix} w_1 & \dots & w_{k-1} & \zeta_{(1)} & w_{k+1} & \dots & w_d \\ w_1^{\sigma_2} & \dots & w_{k-1}^{\sigma_2} & \zeta_{(2)}^{\sigma_2} & w_{k+1}^{\sigma_2} & \dots & w_d^{\sigma_2} \\ \vdots & & & & & & \\ w_1^{\sigma_d} & \dots & w_{k-1}^{\sigma_d} & \zeta_{(t)}^{\sigma_d} & w_{k+1}^{\sigma_d} & \dots & w_d^{\sigma_d} \end{vmatrix}$$

are divisible by D in the ring O'_L.

In this theorem G is Γ-stable and generated by g and all $g^\gamma, \gamma \in \Gamma$ but this condition is not very restrictive for 2 reasons. Firstly, any Γ-stable subgroup $H \in GL_n(E)$ contains subgroups like G. And by Theorem 3 below, if H is a minimal subgroup of exponent t with the property $E = F(H)$, then H is just of the form given in Theorem A.

The proof of Theorem A is constructive. It is based on the commutativity of the L-algebra LG, the L-span of G, and uses a system of linear equations that arises from simultaneous diagonalization of commuting matrices

$$g = \sum_{i=1}^{d} w_i B_i, g^\sigma = \sum_{i=1}^{d} w_i^\sigma B_i, \ \sigma \in \Gamma,$$

whose solutions are the eigenvalues of commuting matrices B_i, $i = 1, 2, \dots, d$.

In fact, we prove that the eigenvalues of $B_1, B_2, \dots, B_d$ are just the elements of the set $\{(D_j D^{-1})^\gamma$, γ are varying in the Galois group of $L/F\}$.

We also use the fact that each semisimple matrix $B \in GL_n(F)$ is conjugate in $GL_n(F)$ to a matrix from $GL_n(O'_F)$ if and only if all its eigenvalues are contained in O'_L (see [2, 8]):

Lemma 1. *1) Let all eigenvalues λ_i, $i = 1, 2, \dots, n$ of a semisimple matrix $B \subset GL_n(F)$ be contained in the ring O'_L for some field $L \supset F$. Then B is conjugate in $GL_n(F)$ to a matrix that is contained in $GL_n(O'_F)$.*

2) Conversely, if a matrix B is contained in $GL_n(O'_F)$, then its eigenvalues are contained in O'_L.

We note that the reduction to the case of an irreducible group G is motivated by the following easy lemma [2, 8]:

Lemma 2. *If $G \subset GL_n(E_1)$ is a finite Γ-stable subgroup which has $GL_n(F_1)$-irreducible components $G_1, G_2, \dots, G_r$, and E_1, F_1 are rings having quotient fields E and F respectively, then $F(G)$ is the composite of fields $F(G_1)$, $F(G_2)$, $\dots$, $F(G_r)$.*

Theorem A can be used in the problem of existence for Γ-stable subgroups $G \subset GL_m(O'_E)$ with the property $F(G) \neq F$ for some integer m. The following Corollary of Theorem A reduces the problem of existence for Γ-stable groups G to the case of $GL_n(F)$-irreducible G.

Theorem A. *If there is an abelian Γ-stable subgroup $G \subset GL_m(O'_E)$ generated by g^γ, $\gamma \in \Gamma$ such that $E = F(G) \neq F$ as above, then $GL_m(F)$-irreducible components $G_i \subset GL_{m_i}(E)$, $i = 1, \dots, k$ of G are conjugate in $GL_{m_i}(F)$ to subgroups $G'_i \subset GL_{m_i}(O'_E)$ such that $E = F(G_1)F(G_2)\dots F(G_k)$. In particular, $F(G_i) \neq F$ for some indices i.*

Proof of Theorem B. If $G \subset GL_m(O'_E)$ is a group of exponent t and

$$g = B_1 w_1 + B_2 w_2 + \dots + B_d w_d$$

for a basis $w_1, \dots, w_d$ of O'_E over O'_F, then $B_i \in M_m(O'_F)$, and it follows from Lemma 1 that the eigenvalues of B_j are contained in O'_L. But eigenvalues are preserved under conjugation, so the latter claim is also true for all components G_i. We can apply Theorem A to $G_i, i = 1, \dots, k$. It follows that G_i are conjugate to subgroups $G'_i \subset GL_{m_i}(O'_E)$. Now, Lemma 2 implies $E = F(G_1)F(G_2)\dots F(G_k)$. This completes the proof of Theorem B. ☐

Theorem A. *Let E/F be a normal extension of number fields with Galois group Γ. Let $G \subset GL_n(E)$ be an abelian Γ-stable subgroup of exponent t generated by $g = B_1 w_1 + B_2 w_2 + \dots + B_d w_d$ and all matrices $g^\gamma, \gamma \in \Gamma$, and let $E = F(G)$. Then G is conjugate in $GL_n(F)$ to $G \subset GL_n(O'_F)$ if and only if all eigenvalues of matrices $B_i, i = 1, \dots, d$ are contained in O'_L, where $L = E(\zeta_t)$.*

Proof of Theorem C. Let

$$C^{-1} G C = \begin{vmatrix} G_1 & & * \\ & \ddots & \\ 0 & & G_k \end{vmatrix}$$

for $C \in GL_n(F)$ and irreducible components $G_i \subset GL_{n_i}(E), i = 1, \ldots, k$. Then

$$C^{-1}gC = \begin{vmatrix} g_1 & & * \\ & \ddots & \\ 0 & & g_k \end{vmatrix} = B'_1 w_1 + B'_2 w_2 + \cdots + B'_d w_d$$

for $B'_i = C^{-1}B_iC$. Let us consider F-algebra A generated by all $B'_i, i = 1, \ldots, d$ over F. Since A is semisimple, it is completely reducible. It follows that matrices B'_i are simultaneously conjugate in $GL_n(F)$ to the block-diagonal form. Therefore, G is conjugate in $GL_n(F)$ to a direct sum of its irreducible components G_i. We can apply Theorem A to each of them. Theorem B implies that each G_i is conjugate in $GL_{n_i}(F)$ to $G'_i \subset GL_{n_i}(O'_F)$ if and only if all eigenvalues of matrices $B'_i, i = 1, \ldots, d$ are contained in O'_{L_i}, where $L_i = F(G_i)(\zeta_t)$. But $F(G) = F(G_1)F(G_2)\ldots F(G_k)$ by Lemma 2, and so $L = L_1L_2\ldots L_k$. This completes the proof of Theorem C. □

Remark. Theorems A, B, C remain true for some other Dedekind subrings $R \subset L$. They can also be modified for the rings of integers O_E, O_F and O_L provided O_E and O_L have O_F-basises (the latter is always true for $F = \mathbf{Q}$).

The approach to describe all Γ-stable matrix groups up to $GL_n(R)$-conjugation for certain Dedekind rings $R \subset E$ can be based on either of Theorems A, B, C for the existence of integral realization of the given Γ-stable subgroup $G \subset GL_n(E)$. So, if we have a description of G up to $GL_n(F)$-conjugation, we can also determine whether G is $GL_n(F)$-conjugate to a subgroup of $GL_n(R)$ for any fixed n, E and F. In fact, we have an algorithm to answer the question: for a given field extension E/F is it possible to find a Γ-stable subgroup $G \subset GL_n(R)$ which is not contained in $GL_n(F)$? Theorem A and Theorem B reduce this question to the case of $GL_n(F)-$irreducible G.

Actually, for a given Galois extension E/F having Galois group Γ and given t and n with $\phi_E(t)[E : F] \leq n$ Theorem 2 (see section 4) provides a construction of a Γ-stable subgroup $G \subset GL_n(E)$ such that $E = F(G)$. Our argument in proof of Theorems 2 and 3 below specify that G can be chosen as a group generated by g^γ, $\gamma \in \Gamma$. Theorem A allows us to check efficiently, whether it is possible to realize G over the ring O'_E, in the terms of the basis of O'_E over O'_F and t. Certain refinement of our argument in Theorem A for O_E instead of O'_E provided O_E is a free O_F-module (and O_E has an O_F-basis) makes possible to apply this approach to subgroups $G \subset GL_n(O_E)$, in particular for $F = \mathbf{Q}$, as well as for other arithmetic rings R. If a list of Γ-stable finite subgroups $G \subset GL_n(E)$ is given, we can apply Theorem A to their generating elements.

Now we can formulate the following finiteness theorem for groups G in question (see [4], Theorem 3 and also [8]).

Theorem (Finiteness Theorem). *1) For a given number field F and integers n and t, there are only a finite number of normal extensions E/F such that $E = F(G)$ and G is a finite abelian Γ-stable subgroup of $GL_n(O_E)$ of exponent t.*

2) For a given number field F and integers n and $d = [E\colon F]$, there is only a finite number of fields $E = F(G)$ for some finite Γ-stable subgroup G of $GL_n(O_E)$.

3. Galois stability for representations over fields

We are interested in the following existence theorem. Note that the proof is constructive, so we can give explicitly the structure and the construction of the abelian Γ- stable subgroup $G \subset GL_n(E)$ in the theorem below.

Theorem 2. *Let F be a field of characteristic 0, let $d > 1, t > 1$ and $n \geq \phi_E(t)d$ be given integers, and let E be a given normal extension of F having the Galois group Γ and degree d. Then there is an abelian Γ- stable subgroup $G \subset GL_n(E)$ of the exponent t such that $E = F(G)$.*

In fact, G can be generated by matrices g^γ, $\gamma \in \Gamma$ for some $g \in GL_n(E)$.

Note that the order $n = d\phi_E(t)$ in our construction is the minimum possible.

Proof of Theorem 2. For a given basis $w_1, w_2, \dots, w_n$ of E/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 $F(g_{11}, g_{12}, \dots, g_{nn})$ 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 Theorem 2.

We consider two different cases in our proof.

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 $w_1 = 1, w_2, \dots, w_d$ be a basis of $E(\zeta_t)$ over $F(\zeta_t)$, 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 $\zeta_t, 1, \dots, 1$. Using the expansion

$$g = B_1 + w_2 B_2 + \cdots + w_d B_d$$

we can construct the matrices $B_i, i = 1, 2, \dots, d$, 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 the matrix $W = [w_i^{\sigma_j}]_{i,j}$ for $\{\sigma_1 = 1, \sigma_2, \dots, \sigma_d\} = \Gamma$. Denote by W_i the matrix W whose i-th column is replaced by d chosen eigenvalues $\zeta_t, 1, \dots, 1$ of g. We can calculate

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

and construct matrices B_i as regular representations $B_i = R(\lambda_i)$ of λ_i in $E(\zeta_t)/F(\zeta_t)$. Let $\alpha_{i,j}$ be the coefficients of the inverse matrix $W^{-1} = [\alpha_{i,j}]_{i,j}$. 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

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

implies the linear relation

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

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 $B_i - I_d, B_2, \ldots, B_d$ generate $F(\zeta_t)$-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 $g^{\sigma_i}, i = 1, 2, \ldots, d$ 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

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

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 $F(\zeta_t)$-dimension of $F(\zeta_t)$-span $F(\zeta_t)G$ is also d.

Let us denote by E' the image of $E(\zeta_t)$ under the regular representation of $E(\zeta_t)/F(\zeta_t)$ over $F(\zeta_t)$. 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 [3], that is, it is an associative and commutative separable E'-algebra having a normal basis. We can choose idempotents

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

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

We have $F(\zeta_t)G = F(\zeta_t)[< g^{\sigma_1}, \ldots, g^{\sigma_d} >] = F(\zeta_t)[(g - I_d)^{\sigma_1}, \ldots, (g - I_d)^{\sigma_d}]$, 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-operation is d, we can use the coefficients of matrices $M^{\sigma_i}, i = 1, 2, \ldots, d$ 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 $F(\zeta_t)$ over F to matrices $M = [m_{ij}]_{i,j}, m_{i,j} \in F(\zeta_t)$ 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 the Galois algebra, and $F(G) = E$. Now, using the natural embedding of G to $GL_n(E), n \geq n_1$, we complete the proof of Theorem 1 in the case 1).

2) In virtue of 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 E over F. Let $\Gamma_0 = \{\sigma'_1, \sigma'_2, \ldots, \sigma'_d\}$ be the set of some extensions of elements $\Gamma = \{\sigma_1, \sigma_2, \ldots, \sigma_d\}$ to $E(\zeta_t)/F$, and let $w_1 = 1, w_2, \ldots w_d$ be a basis of E over F. So we can use our previous notation and go through a similar argument as in the part 1) of the proof for construction of $g = \sum_{i=1}^d B_i w_i$ and matrices B_i as the regular representations R_0 of eigenvalues

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

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 E over F. We also have

$$\lambda_1^{\sigma'_j} = \alpha_{1j} + 1, \lambda_i^{\sigma'_j} = \alpha_{ij}$$

for $j = 2, \ldots, d$. 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 $\lambda_1 - 1, \lambda_2, \ldots, \lambda_d$ are linearly independent over F, so

$$\dim_F FG' = \dim_F F[B_1 - I_d, B_2, \ldots, B_d] = \dim_E EG' = d$$

for G' generated by $g^{\sigma'_i}, i = 1, 2, \ldots, d$. As earlier we can consider the element-wise regular representation $R_E(B_i)$ of matrices B_i in the field extension $E(\zeta_t)/E$. So we obtain $g_0 = \sum_{i=1}^d R_E(B_i) w_i$, and we can take the group G generated by all $g_0^{\sigma_i}, i = 1, 2, \ldots, d$. 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 one required in the formulation of Theorem 1. In this way we can construct a Γ-stable group G that satisfies the conditions of Theorem 2. □

As a corollary of Theorem 2 we have

Theorem 3. *Let E/F be a given normal extension of algebraic number fields with the 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 minimum possible order, then G is a group of type $(t, t, \dots, t)$ and order t^m for some positive integer $m \leq d$.

In the case of quadratic extensions we can give an obvious example.

Example. Let $d = 2$, $t = 2$. Pick $E = \mathbf{Q}(\sqrt{a})$ and $g = \begin{vmatrix} 0 & 1 \\ a^{-1} & 0 \end{vmatrix} \sqrt{a}$ for any $a \in F$ which is not a square in F. Then Γ is a group of order 2 and $G = \{I_2, -I_2, g, -g\}$ is a Γ-stable abelian group of exponent 2.

Proof of Theorem 3. We can use the proof of Theorem 2.

Let $G \subset GL_n(E)$ be a group given in the formulation of Proposition 1, and let n be minimal possible. Then we have the following decomposition of E-span $A = EG$:

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

for some primitive idempotents $\varepsilon_1, \dots, \varepsilon_k$ of A. ε_i are conjugate under the operation of the Galois group $\Gamma = \{\sigma_1, \dots, \sigma_d\}$. For if the sum of $\varepsilon_i^{\sigma_j}, j = 1, 2, \dots, d$ 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 and so e_1, e_2 are conjugate in $GL_n(F)$ to a diagonal form. Since either of 2 components $e_i G$ has rank smaller than n, there is a group satisfying the conditions of Proposition 1 of smaller than n degree.

Therefore, $\varepsilon_i = \varepsilon_1^{\sigma_i}$, $k = d$ and the idempotents $\varepsilon_1, \dots, \varepsilon_d$ 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 true 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-operation, and so G an abelian group of type $(t, \dots, t)$ and order t^m for some positive integer $m \leq d$. ☐

In the case of unramified extensions the following theorem for integral representations in a similar situation is proven in [9]:

Theorem. *Let $d > 1, t > 1$ be given rational integers, and let E/F be an unramified extension of degree d.*
1)If $n \geq \phi_E(t)d$, there is a finite abelian Γ- stable subgroup $G \subset GL_n(O'_E)$ of exponent t such that $E = F(G)$.
2)If $n \geq \phi_E(t)dh$ and h is the exponent of the class group of F, there is a finite abelian Γ-stable subgroup $G \subset GL_n(O_E)$ of exponent t such that $E = F(G)$.

3)If $n \geq \phi_E(t)d$ *and* h *is relatively prime to* n*, then* G *given in 1) is conjugate in* $GL_n(F)$ *to a subgroup of* $GL_n(O_E)$*.*
4)If d *is odd, then* G *given in 1) is conjugate in* $GL_n(F)$ *to a subgroup of* $GL_n(O_E)$*.*

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

References

[1] H.-J. Bartels. Zur Galoiskohomologie definiter arithmetischer Gruppen. *J. Reine Angew. Math.*, 298:89–97, 1978.

[2] H.-J. Bartels and D. A. Malinin. Finite Galois stable subgroups of GL_n. In *Noncommutative algebra and geometry*, volume 243 of *Lect. Notes Pure Appl. Math.*, pages 1–22. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] V. V. Ishkhanov, B. B. Lur′e, and D. K. Faddeev. *The embedding problem in Galois theory*, volume 165 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1997. Translated from the 1990 Russian original by N. B. Lebedinskaya.

[4] E. S. Khrebtova and D. Malinin. On finite Galois stable arithmetic groups and their applications. *J. Algebra Appl.*, 7(6):773–783, 2008.

[5] A. I. Kostrikin and P. H. Tiệp. *Orthogonal decompositions and integral lattices*, volume 15 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1994.

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

[7] D. A. Malinin. Integral representations of p-groups of a given class of nilpotency over local fields. *Algebra i Analiz*, 10(1):58–67, 1998.

[8] D. A. Malinin. Galois stability for integral representations of finite groups. *Algebra i Analiz*, 12(3):106–145, 2000.

[9] D. A. Malinin. On the existence of finite Galois stable groups over integers in unramified extensions of number fields. *Publ. Math. Debr*