GALOIS STABILITY FOR INTEGRAL REPRESENTATIONS OF FINITE ABELIAN GROUPS

D.A.Malinin

ABSTRACT

For a given field F of characteristic 0 we consider a normal extension E/F of finite degree d and finite abelian subgroups $G \subset GL_n(E)$ of a given exponent t. We assume that G is stable under the natural action of the Galois group of E/F and consider fields $E=F(G)$ that are obtained via adjoining all matrix coefficients of all matrices $g \in G$ to F. It is proved that under some reasonable restrictions for n any E can be realized as $F(G)$, while if all coefficients of matrices in G are algebraic integers there are only finitely many fields $E=F(G)$ for prescribed integers n and t or prescribed n and d.

1. Introduction

In this paper 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 coefficientwise Γ-action.

Throughout this paper $\mathcal{O}_E$ 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.

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 ([B], see also [Ro]). 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 $G \subset GL_n(\mathcal{O}_E)$, and if this is so what are the possible dimensions n of matrix realizations and the structure of G. Some similar questions for Γ-stable orders in simple algebras are considered in [RW], see also [RW1] 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 Theorem 1 in section 2. In fact, we construct some Galois algebras in the sense of [ILF], and we establish the lower bounds for their possible dimensions n. We show (see

The author had a nice opportunity to work on this subject during his stay at the MPI and would like to express his gratitude for hospitality. The author is grateful to DAAD for support.

Proposition 1 in section 2) that the restrictions for the given integers n, t, and d in Theorem 1 can not be improved. We also study the problem of uniqueness of possible realizations for cyclic, abelian and solvable extensions E/F provided the ground field F contains roots of 1 of an appropriate degree (Theorems 2 and 3 in section 2).

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 $G \subset GL_n(\mathcal{O}_E)$ such that $F(G) \neq F$ is a rather subtle question. In particular, for $F = \mathbb{Q}$ all fields $F(G)$ whose discriminant is divisible by an odd prime must contain non-trivial roots of 1 [BM], [M1].

We determine certain properties of inegral realizations for the groups stable under the Galois action in section 3, and we consider the question, whether the given field E is realizable as $E = F(G)$ for a Γ-stable $G \subset GL_n(\mathcal{O}_E)$. In this situation the typical answer is negative (we discuss it in section 3.1, in particular, see Theorem 4), but some exeptions are possible, specially if some nontrivial roots of 1 are contained in the field E.

The paper continues the research of [M5] and uses the approach from [M1] and [M3] based on the integral representation theory of finite groups. It is organized in the following way. We describe certain Γ-stable groups G over fields and give the statement of the results in section 2 and their proofs in section 4. Section 3 is completely devoted to integral (in $\mathcal{O}_E$ and some other subrings of E) representations of finite groups that are stable under Γ-action. Some of results in this section are valid without restriction for G to be abelian (Theorem 4, Theorem 6, 2), Lemma 1). Section 3 is subdivided in three parts. Some preliminaries are given in 3.0. In 3.1 we prove that "almost all" fields in certain probabilistic sense are not realizable as $F(G)$ (Theorem 4). We also show that there is only a finite number of possible fields $F(G)$ if F, $[F(G) : F]$ and n are fixed, or F, n and t are fixed provided G is abelian of exponent t (Theorem 6) and discuss some related questions. In 3.2 we show the way to apply Theorem 1 to the problem of existence of integral Γ-stable representations. In the end of 3.2 we give an example of a non-maximal order R, $\mathcal{O}_F \subset R \subset \mathcal{O}_E$, where F contains a primitive t-root of 1, such that any Γ-stable subgroup $G \subset GL_n(R)$ of the exponent prime to t is already contained in $GL_n(\mathcal{O}_F)$ where $\mathcal{O}_F$ is the maximal order of F.

Notation

Most of symbols and notations that we use in this paper are traditional. $\mathbb{Q}$ is the field of rationals. $GL_n(R)$ denotes the general linear group over R. $[E : F]$ denotes the degree of the field extension E/F. 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 the unit $m \times m$-matrix, $0_{n,m}$ and 0_m are zero $n \times m$ and $m \times m$-matrices, $e_{i,j}$ are square matrices having the only nonzero element 1 in the position (i, j), $\det M$ is the determinant of a matrix M, $diag(d_1, d_2, ..., d_m)$

is a diagonal matrix having diagonal components $d_1, d_2, ..., d_n$. If G is a finite linear group, $F(G)$ stands for a field obtained by adjoining to F all matrix coefficients of all matrices $g \in G$. The symbol Γ is used to denote Galois groups. 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. $dim_K A$ denotes the dimension of K-algebra A over the field K.

2. Galois stability for representations over fields

Firstly we are interested in the following existence theorem:

Theorem 1. *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 $E = F(G)$.*

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

As a corollary of Theorem 1 we have

Proposition 1. *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 $(t, t, ..., t)$ and order t^d.*

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

Example. Let $d = 2$, $t = 2$. Pick $E = \mathbb{Q}(\sqrt{a})$ 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.

If the ground field F contains roots of 1 of sufficiently large degrees then the construction and the description of finite abelian Γ-stable groups with coefficients in extended fields can be simplified. We shall give an example of such description in the case of a cyclic Kummer extension of fields E/F of degree q which has Galois group Γ generated by a single element σ. We also assume that F contains primitive roots $\zeta = \zeta_t$ and ζ_q of degrees t and q respectively. We assume that some element $\pi \in E$ generates a Kummer basis $1, \pi, \pi^2, ..., \pi^{q-1}$ so that $\pi^q \in F$.

Let q_i be some divisor of q, and let $r_i = \frac{q}{q_i}$. Set

$$B = \begin{vmatrix} 0 & 1 & 0\dots & 0 \\ 0 & 0 & 1\dots & 0 \\ & & \ddots & \\ & & & 1 \\ \pi^{-q} & 0 & 0\dots & 0 \end{vmatrix},$$

the matrix of regular representation of E_1, the subfield of σ^{q_i}-fixed elements of E, over F in the basis $1, \pi^{r_i}, \pi^{2r_i}, ..., \pi^{(q-1)r_i}$ of E/F.

Let us consider the following matrices:

$$g = I_{q_i} + \frac{1}{q_i} \sum_{j=0}^{q_i-1} \pi^{jr_i} (\zeta - 1) B^j; \quad g_1 = I_m \otimes g.$$

Then the group G_{m,q_i} of matrices which is generated by all elements $g_1^{\sigma^i}$, $i = 1, 2, \ldots, q-1$, is a finite abelian Γ-stable subgroup of $GL_{mq_i}(E)$ of exponent t. We intend to describe all Γ-stable subgroups H of exponent t in $GL_n(E)$ for some positive integer n.

Theorem 2. *Every finite abelian Γ-stable subgroup $H \subset GL_t(E)$ of exponent t is conjugate in $GL_n(E)$ to a subgroup $H_1 \subset \oplus_k G^k$, where $G^i \subset G_{m,q_i}$, or G^k consists of diagonal matrices.*

One application of Theorem 2 is given as an example in the end of section 3.1.

A similar description of finite Γ-stable abelian subgroups of exponent t can be given in the case of finite abelian and solvable extensions. For simplicity we consider the abelian case.

Now, we can extend the result of Theorem 2 to the case of abelian extension E/F provided F contains a primitive roots $\zeta = \zeta_t$ and ζ_l of 1, where l is the exponent of the Galois group Γ of E/F.

Let Γ be a direct sum of cyclic groups whose orders are $q_1, q_2, ..., q_v$. Since E is a composite of cyclic Kummer extensions E_i/F having degree n_i, we can fix a Kummer basis $1, \pi_i, \pi_i^2, ..., \pi_i^{q_i-1}$ for each of them.

The dimension of our matrix realization is $n = mq'_1...q'_k$ for some divisors q'_i of q_i, $k \leq v$. We write $q = q_1q_2...q_k$, $r_i = \frac{q_i}{q'_i}$ and r for the set $(r_1, r_2, ..., r_k)$.

Set $B_0 = I_{mq_i}$,

$$B_i = I_m \otimes \begin{vmatrix} 0 & 1 & 0\ldots & 0 \\ 0 & 0 & 1\ldots & 0 \\ & & \ddots & \\ & & & 1 \\ \pi_i^{-q_i} & 0 & 0\ldots & 0 \end{vmatrix}$$

(all nonzero elements of B_i are: 1 in positions $(12), (23), ...(q'_i - 1, q'_i)$ and $\pi_i^{-q_i}$ in the position $(q'_i 1)$).

Let us construct matrices B_I inductively for indices $I = (i_1, i_2, ..., i_k), k \leq v, 0 \leq i_j < n_j$. Let

$$B_I = \begin{vmatrix} 0_p & I_p & 0_p\ldots & 0_p \\ 0_p & 0_p & I_p\ldots & 0_p \\ & & \ddots & \\ & & & I_p \\ \pi_i^{-q_i} B_{I'} & 0_p & 0_p\ldots & 0_p \end{vmatrix}$$

for $p = q'_1 q'_2 ... q'_{k-1}$, $I' = (i_1, i_2, ..., i_{k-1})$ and $pq_i \times pq_i$-matrices $B(i_1, i_2, ..., i_{k-1}, 0) = diag(B_{I'}, ..., B_{I'})$, where $B_{I'}$ is a $p \times p$-matrix, $i_j = 0, 1, ..., n_j - 1$

Define a matrix as follows:

$$g = \frac{1}{q} \sum_{(i_1 \dots i_k)} ((\zeta_t - 1)\pi_1^{i_1 r_1} \pi_2^{i_2 r_2} ... \pi_k^{i_k r_k} B_{(i_1, i_2, \dots, i_k)} + I_n).$$

Let $G_{m,k,r}$ be the group generated by all matrices $g^\sigma, \sigma \in \Gamma$.

Theorem 3. *Any finite Γ-stable subgroup $G \subset GL_n(E)$ of exponent t is conjugate in $GL_n(F)$ to a subgroup H of the direct sum $\oplus_i G^{(i)}$, where $G^{(i)}$ is contained in either $G_{m,k,r}$ for some integers $m, k (k \leq v)$ and some r, or a group of diagonal matrices.*

The matrices B_I can be transformed to a different simplified form, see Note in the end of the proof of Theorem 3.

The proof of the results of this section will be given in section 4.

3. Galois stability for integral representations

3.0. *Preliminaries.*

In this section we introduce representations over the maximal order $\mathcal{O}_E$ of an algebraic number field E. Therefore, we should distinguish some special properties of the realization fields for Galois stable groups over algebraic number fields and their maximal orders. Integral representations in question are very sensitive to the changing of the ground ring, the ramification index, and the group of units of $\mathcal{O}_E$, specially its torsion subgroup, play an important role ([M1], [M2], [M3]). As it was mentioned in the introduction, the existence of Galois stable subgroups $G \subset GL_n(\mathcal{O}_E)$ such that $F(G) \neq F$ is a rather subtle problem since the Galois stability of G imposes strong restrictions for $F(G)$ such that in the case $F = \mathbb{Q}$ all fields $F(G)$ whose discriminant is divisible by an odd prime must contain some cyclotomic subfield $K \neq \mathbb{Q}$ [BM], [M1]. The question, whether the given field E is realizable as $E = F(G)$ for a Γ-stable G, can be formulated for subgroups $G \subset GL_n(R)$ for certain ring extensions $R \supset R_0$ with quotient fields E and F respectively. In section 3.2 we give an example for the property of non-realizability of the Galois stable matrix groups over certain non-maximal orders in Kummer extensions which can be also compared to the existence of appropriate realizations for abelian groups over fields given in Theorems 2 and 3.

There are numerous classical results related to the description of integral representations of finite abelian groups over Dedekind rings R, specially for the rings of integers $\mathbb{Z}$ or p-adic integers $\mathbb{Z}_p$ and maximal orders of the local fields and the fields of algebraic numbers. Many of them go back to the classification of indecomposable representations that can give an explicit description only for narrow classes of groups rings R (see [R] for a survey and [D] for the classification of finite, wild and tame representation types). The class of matrix groups that are studied in this paper is much more narrow and special since we assume their stability under the natural Galois group action. It is also possible to reduce some general problems concerning these groups to the case of indecomposable or irreducible Galois stable representations. In [M1], [M4] the author has introduced the class $C(F)$ of fields normal over F which are obtained by adjoining to F all coefficients of matrices contained in some finite Γ-stable group $G \subset GL_n(\mathcal{O}_E)$ and implemented the theory of integral representations of finite groups to study $C(F)$ first of all in the case $F = \mathbb{Q}$. The results of this section emanate from the approach of [M1, M4] in the spirit of [M5] and give an extension of results that have been obtained in these papers.

Besides a score of generalizations, finite groups that are stable under Galois action have some interaction with seemingly unrelated results 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 [B], [BK].

Since in our context we are interested in the existence and integral realizability of finite Γ-stable groups, it is convenient to study elementary abelian subgroups of the type $(t, t, ..., t)$ (comp. Proposition 1 in section 2). If F is an algebraic number field, it is proved in [M], [M1] that the general case can be reduced to our situation, more precisely, the existence of Γ-stable groups $G \subset GL_n(F)$ such that $F(G) \neq F$ (for some F, in particular $F = \mathbb{Q}$) implies the existence of abelian Γ-stable groups of exponent p having the same property for some ramified prime p.

These realizations appear to be integral in some special cases (we discuss the case of some cyclic extensions E/F in the end of 3.1) or can be realized integrally (see section 3.2).

Our approach to solve the problem of description of all Γ-stable matrix groups up to $GL_n(R)$-conjugation for certain Dedekind rings $R \subset E$ is based on the criterion in 3.2 (Theorem 7) 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 $GL_n(F)$?

3.1. *Quantative results and finiteness theorems.*

Let $\mathcal{O}_K$ and $\mathcal{O}_E$ denote the maximal orders of number fields K and E respectively. The following result establishes "rarity" of possible realizations in the sense of probability to find the given field as a splitting field of a certain polynomial.

Let us suppose that $K = \mathbb{Q}$, the field of rationals, or $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $d \in \mathbb{Z}$. We consider the set $\mathcal{O}(N) = \{\alpha \in \mathcal{O}_K \,\big|\, |N_{K/\mathbb{Q}}(\alpha)| \leq N\}$ where $N_{K/\mathbb{Q}}$ is the norm map. The proof of the following Theorem is based on the result by S. D. Cohen (Theorem 1 in [C]) combined with some asymptotic estimates for the number of integral polynomials having bounded coefficients with respect to the norm and reducible over $K(\sqrt{b})$ (b is contained in a finite set of elements from $\mathcal{O}_K$):

Theorem 4. *Let $v(N)$ denote the total number of polynomials of degree m with coefficients in $\mathcal{O}(N)$, and let $\psi(N)$ denote the number of those polynomials whose splitting fields do not contain any fields $K(G) \neq K$ for $G \subset GL_n(\mathcal{O}_E), E \supset K$ and fixed n. Then*

$$\lim_{N\to\infty} \frac{\psi(N)}{v(N)} = 1.$$

Theorem 4 shows that "almost all" fields are not realizable via adjoining matrix coefficients of Γ-stable groups to the field of rational numbers or its imaginary quadratic extensions if this coefficients are contained in the rings of integers of algebraic number fields.

On the contrary, according to Theorem 1, all algebraic number fields are realizable in our situation if the matrix coefficients are admitted to be contained in the field, not its maximal order.

Proof of Theorem 4. We use properties of distribution of Galois groups of polynomials that were considered by S. D. Cohen [C]. In accordance with [C] the number of polynomials in question having the symmetric Galois group S_m, divided by the total number of polynomials in question, tends to 1 when $N \to \infty$. Therefore, we can consider only the number of these K-irreducible polynomials which are reducible over $K(\sqrt{\alpha})$ for a finite number of α. The elements $\sqrt{\alpha}$ can be contained only in a finite number of extensions $K(G)$ which have no ramified primes $p \geqslant m!+1$ and have degree $m!$ over K. Let us estimate the number of these polynomials. Let$f \in \mathcal{O}(N)[x]$ and $f = g \cdot g'$, $g, g' \in K(\sqrt{\alpha})[x]$. Let $\mathcal{E} \in \mathcal{O}_{K(\sqrt{\alpha})}$ be a unit of infinite order. We can suppose that after some adjustment both height $|g| = \max |a_i|$ of $g = \sum a_i x^i$ and height $|g'|$ of $g' = \sum a'_i x^i$ are equal up to a constant $c = c(K,m)$. Indeed, let $|g| = A$, $|g'| = B$, $|f| = c_0 N$, $c_0 = c_0(K,m)$. Let $t = \log_{\mathcal{E}} \left(\frac{A}{\sqrt{N}}\right)$, then changing g and g' to $p = \mathcal{E}^{-[t]} g$ and $p' = \mathcal{E}^{[t]} g$ respectively we obtain $|p| \sim \sqrt{N}$, $|p'| \sim \sqrt{N}$, that is $|p| \leqslant c_1(K,m)\sqrt{N}$ and $|p'| \leqslant c_2(K,m)\sqrt{N}$. As $p = p_1 + \sqrt{\alpha} p_2$ and $p' = p'_1 + \sqrt{\alpha} p_2$ for $p_i, p'_i \in K[x]$ and $p' = p^{\sigma}$ for nonidentical automorphism σ of $K(\sqrt{\alpha})$ over K, we can see that $|p_i| \leqslant c_3\sqrt{N}$ and $|p'_i| \leqslant c_3\sqrt{N}$ for $i = 1, 2$ and $c_3 = c_3(K,m)$. Therefore, there are only $(c_2\sqrt{N})^{2\cdot(m/2+1)} = c_4 N^{m+2}$, $c_4 = c_4(K,m)$, polynomials that are reducible over $K(\sqrt{\alpha})$. Likewise, there are $c_5 N^{2(m+1)}$, $c_5 = c_5(K,m)$, polynomials f in $\mathcal{O}(N)[x]$ and it is obvious that

$$\lim_{N\to\infty} \frac{c_4 N^{m+2}}{c_5 N^{2m+2}} = 0.$$

So, we showed that the number of polynomials whose splitting fields can contain any $K(G) \neq K$ is small asymptotically, and our estimate completes the proof of Theorem 4.

Let E/F be a given normal extension of algebraic number fields. Then we write Γ_E for the Galois group of E over F. Let $t > 0$ be a given integer. Let ζ_t be a primitive root of 1 of degree t. We use notation $\gamma_t = [E(\zeta_t)\colon F(\zeta_t)]$.

Theorem 5. *Let a Γ_E-stable abelian subgroup $G \subset GL_n(E)$ of exponent t be irreducible under $GL_n(F)$-conjugation, and let $E = F(G)$. Then γ_t divides n.*

Proof of Theorem 5. Let $w_1, w_2, \dots, w_r$ be some basis of $E(\zeta_t)$ over $F(\zeta_t)$. Let G be reducible under conjugation in $GL_n\big(F(\zeta_t)\big)$. Then G splits into components of equal dimensions, each of them being $GL_n\big(F(\zeta_t)\big)$-irreducible. Therefore, we can restrict ourselves to considering a $GL_n\big(F(\zeta_t)\big)$-irreducible component and use the same notation G for it. Let $\varepsilon_i = \sum_j A_{ij} w_j$ be a primitive idempotent of $E(\zeta_t)$-algebra $E(\zeta_t)G$. We can prove that $E(\zeta_t)$ is obtained by adjoining to $F(\zeta_t)$ all eigenvalues of matrices A_{ij}. Indeed, this eigenvalues are equal to $\lambda_{ij} = \frac{\det W_{ij}}{\det W}$ for $W = [w_i^{\sigma_j}]$, where $\Gamma = \{\sigma_1, \sigma_2, \dots, \sigma_r\}$ is the Galois group of $E(\zeta_t)/F(\zeta_t)$, and W_{ij} is obtained from W by replacing its j-th column with ${}^t(0\dots1\dots0)$ (i-th element is 1, all other elements are 0), and λ_{ij} are precisely elements of the matrix W^{-1}. Furthermore, if $\sum \alpha_{ij}\lambda_{ij} = \theta$ is a primitive element of $E(\zeta_t)$ over $F(\zeta_t)$ for some $\alpha_{ij} \in F$, then the matrix $M = \sum \alpha_{ij} A_{ij} \in FG$ and its spectrum consists of all conjugate elements θ^σ, $\sigma \in \Gamma$, in virtue of irreducibility of G. It follows that the number of eigenvalues of M is divisible by γ_t, and γ_t divides n. This completes the proof of our claim.

We note that the reduction to the case of an irreducible group G is motivated by the following lemma:

Lemma 1. *If $G \subset GL_n(E_1)$ is a finite Γ_E-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 $F(G_1)$, $F(G_2)$, ..., $F(G_r)$.*

Proof of Lemma 1. Let

$$G^1 = h^{-1}Gh \subset \begin{vmatrix} G_1 & & * \\ & \ddots & \\ 0 & & G_r \end{vmatrix}$$

for $h \in GL_n(F_1)$. If there exists $g \in G$ such that $g^\gamma \neq g$ for some automorphism γ of $F(G)$ over $F(G_1)F(G_2)\dots F(G_r)$, then $g_1 = g^\gamma g^{-1} \neq I_n$. But all eigenvalues of g_1 are 1. This contradiction completes the proof of Lemma 1.

Clifford's theory of restriction of irreducible representations to the normal subgroups allows us to describe non-abelian subgroups $G \subset GL_n(\mathcal{O}_E)$.

We can give some quantative characterizations of groups G in question.

Theorem 6. *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_E-stable subgroup of $GL_n(\mathcal{O}_E)$ 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_E-stable subgroup G of $GL_n(\mathcal{O}_E)$.

But if we admit the ground ring to be the field E instead of $\mathcal{O}_E$ we can compare Theorem 6 and the following

Proposition 2. *For a given number field F and given integers $d > 1, t > 1$ and $n \geqslant [F(\zeta_t)\colon F] \cdot d$, there are infinitely many normal extensions E/F of degree d such that $E = F(G)$ for some finite Γ_E-stable abelian subgroup $G \subset GL_n(E)$ of exponent t.*

Proposition 2 is an immediate corollary of Theorem 1.

Proof of Theorem 6. 1) In virtue of Lemma 1 we can restrict ourselves to considering only irreducible G. It follows from integrality in $\mathcal{O}_E$ of all coefficients of G that only divisors of t can ramify in E, and in accordance with Theorem 5 the degree $[E\colon F]$ is restricted by a constant that depends only on t and n. Furthermore, it follows from the formula

$$d_{K/\mathbb{Q}} = N_{K_0/\mathbb{Q}}(d_{K/K_0}) d^r_{K_0/\mathbb{Q}}, \quad r = [K\colon K_0]$$

for discriminants of the tower $K \supset K_0 \supset \mathbb{Q}$ of number fields that there is only a finite number of unramified extensions of the given number field of the prescribed degree. Since the number of algebraic number fields having the prescribeded discriminant is finite, and the power of the given ramified prime p that divides the discriminant of number field having the prescribed degree is restricted, we can obtain only a finite number of possibilities for the given n and t. Therefore, we have only a finite number of fields E that satisfy our conditions.

2) We can note that if prime p is ramified in E, then $\frac{d}{p-1} \geqslant 1$, that is $p \leqslant d+1$. Indeed, Bartels proved in [B] that ramification index e of p in this situation satisfies inequality $e \geqslant p-1$, and it is clear that $d = [E : F]$ is always not less than e. Now we can use the proof given in 1).

Example. If the ground field F contains roots of 1 of sufficiently large degrees the description of finite abelian Γ_E-stable groups can be simplified. Here we give an example in the case of a cyclic ramified extension of the number fields E/F of a prime degree q whose Galois group Γ_E is generated by an element σ. Let us suppose that all prime ideals $\mathfrak{q}$ of $\mathcal{O}_E$ that do not divide a prime $p \neq q$ are unramified in E/F and the field F contains some primitive roots of 1 ζ and ζ_q of degrees p and q respectively. Moreover, we assume that there exists an element $\pi \in \mathcal{O}_F$ which is an uniformizing element in all ramified ideals of

E, $\pi^q \in F$ and the norm $N_{E/F}(\pi)$ divides p. Set $b = \frac{1}{q}(1+\pi+\pi^2+\cdots+\pi^{q-1})$. Let $(\zeta-1)B$ be a matrix of the regular representation of an element $(\zeta-1)\pi^{-1}$ in the ring $\mathcal{O}_F[b, b^\sigma, \ldots, b^{\sigma^{q-1}}]$. Let us consider the following matrices:

$$g = I_q + \frac{1}{q}\sum_{i=0}^{q-1} \pi^i(\zeta-1)B^i; \quad g_1 = I_m \otimes g.$$

It is not difficult to prove that the group G_m of matrices which is generated by all elements $g_1^{\sigma^i}$, $i = 1, 2, \ldots, q-1$, is a finite abelian Γ_E-stable subgroup of $GL_{mq}(\mathcal{O}_E)$ of exponent p.

We can use Theorem 2 to state that every finite abelian Γ_E-stable subgroup $H \subset GL_t(E)$ of exponent p is conjugate in $GL_t(E)$ to a subgroup $H_1 \subset \oplus G^i$, where either $G^i \subset G_m$ or G^i consists of diagonal matrices.

3.2. *On the existence of integral representations stable under Galois action.*

Let us formulate a criterion for the existence of an integral realization of an abelian group G with properties introduced above.

Let E, L be finite extensions of a number field F. Let $\mathcal{O}'_E$, $\mathcal{O}'_F$, $\mathcal{O}'_L$ be semilocal rings that are obtained by intersection of valuation rings of all ramified prime ideals in the rings $\mathcal{O}_E$, $\mathcal{O}_F$, $\mathcal{O}_L$. Let $w_1, w_2, \ldots, w_d$ be a basis of $\mathcal{O}'_E$ over $\mathcal{O}'_F$, and let D be the discriminant of this basis. Let us suppose that some matrix g of prime order p has coefficients in E and all Γ-conjugates g^γ, $\gamma \in \Gamma$ generate a finite group G of exponent t. Let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_d$ denote all automorphisms of the Galois group Γ of E over F. Assume that $L = E(\zeta_1, \zeta_2, \ldots, \zeta_d)$ where $\zeta_1, \zeta_2, \ldots, \zeta_d$ are the eigenvalues of the matrix g. We shall reserve the same notations for certain fixed extensions of σ_i to L. Let $E = F(G)$ be obtained by adjoining to F all coefficients of all $g \in G$. For an appropriate set of d eigenvalues $\zeta_1, \zeta_2, \ldots, \zeta_d$ which depends on the primitive idempotents of algebra LG we the following Theorem is true:

Theorem 7. *Let G be irreducible under $GL_n(F)$-conjugation. Then G is conjugate in $GL_n(F)$ to a subgroup of $GL_n(\mathcal{O}'_E)$ if and only if all determinants*

$$d_k = \det \begin{vmatrix} w_1 & \ldots & w_{k-1} & \zeta_1 & w_{k+1} & \ldots & w_d \\ w_1^{\sigma_2} & \ldots & w_{k-1}^{\sigma_2} & \zeta_2^{\sigma_2} & w_{k+1}^{\sigma_2} & \ldots & w_d^{\sigma_2} \\ \vdots & & & & & & \\ w_1^{\sigma_d} & \ldots & w_{k-1}^{\sigma_d} & \zeta_t^{\sigma_d} & w_{k+1}^{\sigma_d} & \ldots & w_d^{\sigma_d} \end{vmatrix}$$

are divisible by $\sqrt{D}$ in the ring $\mathcal{O}'_L$.

Note that the conditions of Theorem 7 are always true if E is unramified over F since $D\mathcal{O}'_E = \mathcal{O}'_E$ in this case.

The proof of Theorem 7 is constructive. It is based on the commutativity of the L-algebra LG and uses a system of linear equations that arises from simultaneous diagonalization of commuting matrices

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

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

Using some F-irreducible component of a semisimple algebra FG and concidering eigenvalues of B_i and g^{σ_j}, we can obtain the following system of linear equations in indeterminates x_i, $i = 1, ..., d$:

$$\begin{cases} x_1 w_1 + x_2 w_2 + \cdots + x_t w_t = \zeta_1, \\ x_1 w_1^{\sigma_2} + x_2 w_2^{\sigma_2} + \cdots + x_d w_t^{\sigma_2} = \zeta_2^{\sigma_2}, \\ \vdots \\ x_1 w_1^{\sigma_d} + x_2 w_2^{\sigma_d} + \cdots + x_t w_t^{\sigma_d} = \zeta_d^{\sigma_d}, \end{cases} \tag{$*$}$$

The discriminant of this system is $\sqrt{D}$, where $D = \det[\mathrm{Tr}_{E/F}(w_i w_j)]_{ij}$ is the discriminant of basis $w_1, w_2, \ldots, w_d$. The solutions of system (*) are $x_i' = d_k(\sqrt{D})^{-1}$. It follows from Γ-stability of the abelian group G that we can also obtain a system $\{\lambda_i = (x_i')^{\sigma_j},\ j = 1, 2, \ldots, t\}$ of all different eigenvalues of the matrix B_i, Conversely, if we pick a system $\{\lambda_i = (x_i')^{\sigma_j},\ j = 1, 2, \ldots, d\}$ of eigenvalues with an appropriate multiplicity and use the regular representation in the basis $w_1, w_2, \ldots, w_d$ of diagonal matrices whose diagonal elements are ordered in accordance with the action of automorphisms of L over F, we can obtain pairwise commuting matrices B_i and write $g = w_1 B_1 + w_2 B_2 + \cdots + w_d B_d$. On the other hand, the values $\lambda_j^{\sigma_j}$ are defined by λ_j and correspond uniquely to the eigenvalues of matrices g^{σ_i}, which are defined in a natural way, and g^{σ_j} commute with each other. Matrices g^{σ_i} generate a finite abelian Γ-stable group of exponent t.

We also use the fact that each semisimple matrix $B \in GL_n(\mathcal{O}_L')$ is conjugate in $GL_n(F)$ to a matrix from $GL_n(\mathcal{O}_F')$ if and only if all its eigenvalues are contained in $\mathcal{O}_L'$:

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

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

Proof of Lemma 2. 1) If we consider the regular representation $R : \lambda_i \to GL_d(F)$ in the integral basis $w_1, w_2, ..., w_d$, then λ_i and all its Γ-conjugates are eigenvalues of $R(\lambda_i)$ and all coefficients of $R(\lambda_i)$ are contained in $\mathcal{O}_F'$. Taking the direct sum of all irreducible components of these regular representations R with respect to all classes of Γ-conjugate eigenvalues and an appropriate multiplicity we obtain the representation $R_1 : B \to GL_n(\mathcal{O}_F')$. The matrix B is conjugate to $R_1(B)$ as we can see via reducing both semisimple matrices B and $R_1(B)$ to the same rational normal form by conjugation in $GL_n(F)$.

2) Consider the characteristic polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ of the matrix B. Since $a_n = 1$ and all a_i are in $\mathcal{O}'_F$ all roots of $f(x)$ are in $\mathcal{O}'_E$. This completes the proof of the Lemma 2.

The structure of semisimple matrices B_i, $i = 1, 2, \dots, d$ and their pairwise commutativity implies that they are conjugate to integral (in $\mathcal{O}'_L$) matrices simultaneously if all eigenvalues are in $\mathcal{O}'_L$.

Applying this to matrices B_i we can obtain the proof of theorem 7.

Remark. *The previous reasons remain true for other Dedekind subrings $R \subset L$. In particular, Theorem 7 can be proved for any semilocal rings R_E, R_F and R_L that are contained in $\mathcal{O}'_E, \mathcal{O}'_F$ and $\mathcal{O}'_L$ respectively and can also be modified for the rings of integers $\mathcal{O}_E, \mathcal{O}_F$ and $\mathcal{O}_L$.*

The question whether Γ-stability of a finite group G of matrices having coefficients in an extended ring $R \supset R_0$ (where $R_0 = R^\Gamma$ is a subring of Γ-fixed elements) implies that $G \subset GL_n(R_0)$ has in general a negative answer. This depends strongly on the structure of the group of units of R. But the answer can be positive even in the case when R_0 contains nontrivial t-roots of 1. Here we give an example for groups G of order prime to the integer t.

Let L/K be a cyclic ramified tame Kummer extension of algebraic number fields of degree t having the Galois group Γ which is generated by an element σ. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the maximal orders of K and L, and let $\mathfrak{p}$ be some prime divisor of $\mathcal{O}_L$ which is ramified in L/K. So the primitive t-root $\zeta = \zeta_t$ of 1 is contained in K, and there is a prime element $\pi \in \mathcal{O}_L$ of $\mathfrak{p}$ such that $\pi^\sigma = \pi\zeta$. Let $R = \mathcal{O}_K[1, \pi, \pi^2, ..., \pi^{t-1}]$, and let $G \subset GL_n(R)$ be a Γ-stable finite subgroup whose order m is prime to t.

We can prove that $G \subset GL_n(R_0)$ for $R_0 = \mathcal{O}_K$. For this purpose let us consider any $g \in G$ and its expansion

$$g = B_0 + \pi B_1 + \pi^2 B_2 + ... + \pi^{t-1} B_{t-1},$$

where all $n \times n$-matrices B_i have coefficients in $\mathcal{O}_K$. If there is an element $\gamma \in \Gamma$ that acts non-identically on g we can suppose that $\gamma = \sigma^r$ and its order is q^i for some prime q (if needed we can replace γ by some its power that does not fix g). Then we have

$$g - g^\gamma = (1 - \zeta^r)\pi B_1 + (1 - \zeta^{2r})\pi^2 B_2 + ... + (1 - \zeta^{(n-1)r})\pi^{t-1} B_{t-1}$$

Note that all elements $1 - \zeta^{rj}, j = 1, ..., n-1$ divide the prime q. We can consider the following congruences

$$g \equiv g^\gamma (mod(1 - \zeta^r)), g^{-1}g^\gamma \equiv I_n(mod(1 - \zeta^r)).$$

Let $h = g^{-1}g^\gamma$. Then $h = I_n + B$ for some $n \times n$-matrix B such that $B \equiv 0_n(mod(1 - \zeta^r))$. In virtue of the well-known properties of matrices congruent to I_n (see [Min1], sect.1, [Min2], sect.1, [Min3], p.186, [B], Hilfssatz 1, [M3], lemma 1 and [M2]) this congruence implies that the order of h is some power of q. But this is impossible since the orders of Γ and G have no common divisors.

Therefore, the natural Γ-action on G is trivial, Γ fixes all $g \in G$, and $G \subset GL_n(O_K)$.

4. Proof of theorems 1, 2, 3 and Proposition 1

Proof of Theorem 1. For a given basis $w_1, w_2, ..., w_n$ 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 $F(g_{11}, g_{12}, ..., g_{nn})$ 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.

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 $w_1 = 1, w_2, ..., w_d$ 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 $\zeta_t, 1, ..., 1$. Using the expansion $g = B_1 + w_2 B_2 + ... + w_d B_d$ we can construct the matrices $B_i, i = 1, 2, ..., d$, 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 $\sigma_1 = 1, \sigma_2, ..., \sigma_d = \Gamma$. Denote by W_i the matrix W whose i-th column is replaced by d chosen eigenvalues $\zeta_t, 1, ..., 1$ of g. We can calculate

$$\lambda_i = \frac{detW_i}{detW}$$

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 $\lambda_j = (\zeta_t - 1)\alpha_{ij}$ 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

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

implies the linear relation

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

for all $\sigma_j \in \Gamma$, this would also imply $detW^{-1} = 0$, which is impossible. Therefore, $\lambda_1 - 1, \lambda_2, ..., \lambda_d$ generate the field $E(\zeta_t)$ over$F(\zeta_t)$, and so $B_i - I_d, B_2, ..., B_d$

generate $F(\zeta_t)$-span $F(\zeta_t)[B_1, ..., B_d]$ over $F(\zeta_t)$. Note that B_i can be expressed as a linear combination of $g^{\sigma_i}, i = 1, 2, ..., d$ 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

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

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 [ILF], that is, it is an associative and commutative separable E'-algebra having a normal basis. We can choose idempotents

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

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

We have $F(\zeta_t)G = F(\zeta_t)[< g^{\sigma_1}, ..., g^{\sigma_d} >] = F(\zeta_t)[(g - I_d)^{\sigma_1}, ..., (g - I_d)^{\sigma_d}]$, 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 $M^{\sigma_i}, i = 1, 2, ..., d$ 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 $G \subset GL_m(E), m = [F(\zeta_t) : F]d$ 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 $GL_n(E), n \geq m$, we complete the proof of Theorem in the case 1).

2) We 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 $\Gamma_0 = \{\sigma'_1, \sigma'_2, ..., \sigma'_d\}$ be the set of some extensions of elements $\Gamma = \{\sigma_1, \sigma_2, ..., \sigma_d\}$ to $E(\zeta_t)/F$, and let $w_1 = 1, w_2, ...w_d$ be a basis of E over F. So we can use our previous notation and go through a similar argument as in 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

$$\lambda_i = \frac{detW_i}{detW} = \sum_{j=1}^{\phi_E(t)} \lambda_{ij} \zeta^j, i = 1, 2, ..., d,$$

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 $j = 2, ..., d$. 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 $detW^{-1} = 0$ which is a contradiction. So, again we obtain that $\lambda_1 - 1, \lambda_2, ..., \lambda_d$ are linearly independent over F, so $dim_F FG' = dim_F F[B_1 - I_d, B_2, ..., B_d] = dim_E EG' = d$ for G' generated by $g^{\sigma'_i}, i = 1, 2, ..., d$. As earlier we can consider the elementwise 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 $g_0^{\sigma_i}, i = 1, 2, ..., d$. Since $[E(\zeta_t) : F] = [E(\zeta_t) : E][E : F] = \phi_E(t)d$, the dimension $n = \phi_E(t)d$ 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 1.

This completes the proof of Theorem 1.

Proof of Proposition 1. It follows from the proof of Theorem 1.

If $T : C \to GL_k(E)$ is an irreducible representation of a cyclic group C generated by an element g of order t, its degree is equal to $\phi_E(t)$ if $T(g) \neq I$. We have the following decomposition of E-span $A = EG$:

$$A = \varepsilon_1 A_1 + \varepsilon_2 A_2 + ... + \varepsilon_d A_d$$

for the primitive idempotents $\varepsilon_1, ..., \varepsilon_d$ forming a normal basis of A, and 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 $g_\gamma.\gamma \in \Gamma$ and its order is minimal, Γ-stability implies that g has d orbits under Γ-action, and so G an abelian group of type $(t, ..., t)$ and order t^d.

Proof of Theorem 2. Let H be an abelian Γ-stable subgroup of $GL_t(E)$ of exponent t. Let us consider F-span FH and the system of primitive orthogonal idempotents $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ of F-algebra FH. We can separate the orbits of this idempotents under Γ-action. We obtain a system $\{\varepsilon_\lambda\}_{\lambda \in I}$ of one-element orbits and a system of orbits having q_i elements $\{\varepsilon_j, \varepsilon_j^\sigma, \ldots, \varepsilon_j^{\sigma^{q_i-1}}\}_{j \in J}$. We also consider idempotents e_l that are sums of all idempotents contained in the l-th orbit and the associated decomposition of

$$A = FH = e_1 A_1 + e_2 A_2 + ... + e_k A_k,$$

so that e_l are Γ-stable and correspond to some Γ-stable component of H.

Let G_0 be the group containing H which is generated by matrices $h\varepsilon_i + (I_t - \varepsilon_i)$, $h \in H$, $i = 1, 2, \ldots, r$. G_0 is a finite Γ-stable abelian group of exponent dividing t, the set of eigenvalues for generators of G_0 is $\{1, \zeta^{\alpha_i}\}$ for an appropriate $\alpha_i \in \{1, 2, \ldots, t\}$. The group G_0 is conjugate in $GL_t(F)$ to the direct sum of matrix groups G_{0i}, $i \in I$ and G_{0j}, $j \in J$ that correspond to the orbits of minimal idempotents e_l, as can be seen by decomposing the algebra $A = FG_0$ into the sum $\oplus_{i=1}^r \varepsilon_i(FG_0)$ of primitive components. Here the components that correspond to the indices $i \in I$ are t-roots of 1, and taken together they compose a subgroup of the group of diagonal matrices of an appropriate dimension. The components corresponding to the indices $j \in J$ are matrix groups that are irreducible with respect to $GL_{q_i v}(F)$-conjugation, where v denotes the rank of the idempotent of the corresponding component. Let $C = e_l = (\varepsilon + \varepsilon^\sigma + \cdots + \varepsilon^{\sigma^{q_i-1}})G_0$ be one of these components. The matrix group C_1 that corresponds to this component is contained in $GL_{q_i v}(F)$ and is generated by its cyclic subgroups corresponding to matrices $\varepsilon^{\sigma^i} g + (I - \varepsilon^{\sigma^i})$, $g \in G_0$. (Indeed, the component $\varepsilon^{\sigma^i} G_0$ is generated by the only matrix $\varepsilon^{\sigma^i} g$ for some $g \in G_0$, otherwise there would exist $h_1, h_2 \in \varepsilon^{\sigma^i} G_0$ which are not powers of each other, and so some matrix $h = h_1^\alpha h_2^\beta \neq \varepsilon^{\sigma^i}$ and one of its eigenvalues is 1; therefore, we could obtain an idempotent $\varepsilon_1 = \frac{1}{p}\sum_{i=0}^{p-1} h^i$, and $\varepsilon^{\sigma^i} = \varepsilon_1 + (\varepsilon^{\sigma^i} - \varepsilon_1)$, and this contradicts the primitivity of idempotent ε^{σ^i}). Therefore, G_0 is generated by the matrices $h = \varepsilon g + (I_{q_i v} - \varepsilon)$ and all h^{σ^j}, $j = 1, 2, \ldots, q_i - 1$ for some matrix g from the chosen component C. Let us consider the following expansion of the matrix h in the basis $1, \pi^{r_i}, \pi^{2r_i}, \ldots, \pi^{(q_i-1)r_i}$ of extension E/F:

$$h = B_q + \pi^{r_i} B_1 + \pi^{2r_i} B_2 + \cdots + \pi^{(q_i-1)r_i} B_{q_i-1}.$$

We obtain

$$B_j = \frac{1}{q}\big((\pi^{-jr_i} h) + (\pi^{-jr_i} h)^\sigma + \cdots + (\pi^{-jr_i} h)^{\sigma^{q_i-1}}\big), \quad j = 1, 2, \ldots, q_i - 1.$$

Considering eigenvalues of matrices h and B_j we obtain: $B_{q_i} = I_{q_i v} + \frac{1}{q}(\zeta - 1)I_{q_i v}$, $B_j = B_1^j$, and the matrix B_1 is conjugate in $GL_n(F)$ to the matrix

$$\pi^{-q_i} I_v \otimes e_{q_i 1} + I_v \otimes e_{12} + I_v \otimes e_{23} + \cdots + I_v \otimes e_{q_i-1, q_i},$$

and it coincides with $I_v \otimes B$.

So, components $e_i A$ determine either a component $C_1 \in GL_{vq_i}(E)$ of G_0 which is just the group G_{v,q_i} specified in Theorem 2, or a subgroup of diagonal matrices. This completes the proof of Theorem 2.

Proof of Theorem 3. We can consider the following sums:

$$S_{(i_1 \ldots i_k)} = \frac{1}{q_1 \ldots q_k} \sum_{\gamma \in \Gamma} (\pi_1^{-i_1} \ldots \pi_k^{-i_k} g)^\gamma$$

and also expansion of g via the basis $\pi_1^{i_1}\pi_2^{i_2}...\pi_k^{i_k}, 0 \le i_j < q_j, j = 1, 2, ..., k$ as

$$g = \sum_{(i_1...i_k)} Q_{(i_1...i_k)}\pi_1^{i_1}...\pi_k^{i_k}.$$

Since $\pi_i^{q_i} \in F$ and $B_{(i_1...i_k)} \subset GL_n(F)$ we obtain $S_{(i_i,...,i_k)} = Q_{(i_1,...,i_k)} = \frac{1}{q}B_{(i_1,...,i_k)}(\zeta - 1) + \delta I_n$ for $\delta = 0$ if $(i_1, ..., i_k) \neq 0$ and $\delta = 0$ if $(i_1, ..., i_k) = 0$.

Let G be an arbitrary subgroup $G \subset GL_n(F)$ given in Theorem 2. We denote by $E_0 = F(G)$ the field obtained by adjoining to F all matrix coefficients of all elements $g \in G$. Let the Galois group Γ of E_0/F be the direct sum of cyclic subgroups of orders $q_1, ..., q_k$ and let Γ_1, ...,Γ_q be generated by automorphisms $\sigma_1, ..., \sigma_q$ respectively. We consider the system of primitive orthogonal idempotents $\varepsilon_1, ..., \varepsilon_r$ of the F-algebra FG and the Γ-orbits of each ε_i. So FG splits into a direct sum of irreducible components, and G is conjugate in $GL_n(F)$ to a direct sum of $GL_n(F)$-irreducible components. So we can restrict ourselves by considering the particular case of $GL_n(F)$- irreducible group G. Let us represent g as

$$g = \frac{1}{q}\sum_{(i_1...i_k)} ((\zeta - 1)B_{(i_1...i_k)}\pi_1^{i_1}...\pi_k^{i_k} + I_n),$$

and let us introduce the matrices C_i given as coefficients in the expansion $g = \sum_{j=0}^{q-1} C_j\pi_k^j$. On the other part, matrices C_i can be again expanded as $C_i = \sum_{j=0}^{q_{k-1}-1} C_{ij}\pi_{k-1}^j$ and so on. Finally, we can obtain the coefficients $C_{(j_1,...,j_k)} = Q_{(j_1,...,j_k)}$. Let us denote by I, J the indices $(i_1, ..., i_l), (j_1, ..., j_l)$. Let F_l be the subfield of elements in E_0 fixed by $\sigma_l, ..., \sigma_k$. Then C_i can be given by the formula $C_I = \sum_{i_l=0}^{q_l-1}(\pi^{-i_l}C_J)^{\sigma_l^{i_l}}$. Using conjugation by matrices from $GL_n(F_i)$ we can transform C_I to the direct sum of matrices $C'_I = \sum_{j_l=0}^{q_l-1} \pi_l^{j_i} M_I$ for

$$M_I = \begin{vmatrix} 0_p & I_p & 0_p \dots & 0_p \\ 0_p & 0_p & I_p \dots & 0_p \\ & & \ddots & \\ & & & I_p \\ \pi_l^{-q_l}C_J^{q_l} & 0_p & 0_p \dots & 0_p \end{vmatrix}$$

$I = (i_1, ..., i_l)$ for $i_l \neq 0$ or to $M_l = diag(C_J, ..., C_J)$ if $i_l = 0$.

We can repeat this construction for all indices J and I and $l \le k$, $(l \ge 1)$ and descend the chain of fields $F_l \supset F_{l-1} \supset ... \supset F_1$ for the coefficients $C_{(i_1,...,i_k)}$ in the expansion of g in the basis of E/F. This allows us to complete the proof if we can transform all other matrices $h \in G$ to the same form simultaneously. We can do it using the following lemma (for the general theory of commuting matrices (see [G], chapter 8 or [ST]).

Lemma. *Let the set of matrices M be some block-diagonal matrices $diag(M_1, ..., M_k)$ which are contained in $GL_s(K)$ for a field K, and let the matrices $M_i \in GL_{s_i}(K)$ form a $GL_s(K)$-irreducible component of degree s_i. Then all matrices $h \in GL_s(K)$ that commute elementwise with matrices in M, can be written as $[g_{ij}]$ for $s_i \times s_i$-matrices g_{ij} that are nondegenerate if components M_i and M_j are equivalent and a zero matrix otherwise.*

The proof of this lemma follows immediately from the Schur lemma. According to the Schur lemma, any linear operator $\rho : K^n \to K^m$ that satisfies the condition $\rho\delta_1(g) = \delta_2(g)\rho$ for two irreducible representations $g \to \delta_1(g) \in GL_n(K)$ and $g \to \delta_2(g) \in GL_m(K)$ over K and all g, is a zero operator if δ_1 and δ_2 are not equivalent and a nondegenerate operator otherwise.

Note. Matrices $B_{(i_1,...,i_r)}$ in Theorem 3 can be conjugateded to a different form. Let us consider an $l_i \times l_i$-matrix

$$M_i = \sum_{i=1}^{q_i-1} I_m \otimes e_{i,i+1} + I_m \otimes e_{q_i 1}$$

for $l_i = mq_1q_2...q_i$ and a matrix $B'_j = B_j$. Let

$$B'_{(j_i,...,j_i)} = B'_{(j_1,...,j_{i-1})} \otimes (M_i)^{j_i}.$$

It is easy to see that $B'_{(j_1,...,j_i)}$ is conjugate in $GL_{l_i}(F)$ to the matrix $B_{(j_1,...,j_i)}$ which is given in Theorem 3. Indeed, if

$$T = \sum_{i=1}^{q_i-1} (I_m \otimes A) \otimes e_{i,i+1} + (I_m \otimes A) \otimes e_{n1}$$

and $D = diag(I_m, I_m \otimes A, ..., I_m \otimes A^{q_i-1})$ then

$$DTD^{-1} = \sum_{i=1}^{q_i-1} I_m \otimes e_{i,i+1} + (I_m \otimes A^{q_i}) \otimes e_{n1}$$

for a nondegenerate $m \times m$ matrix A. Theorem 3 remains valid if we replace matrices $B_{(j_1,...,j_k)}$ with the matrices $B'_{(j_1,...,j_k)}$ and use a similar argument as in the proof of Theorem 3.

The result obtained in Theorem 3 can be generalized for solvable extensions E/F with Galois groups Γ if we generalize the construction of matrices B_i in Theorem 3. For this we can suppose that F contains primitive roots of 1 of degrees t and $q = [E : F]$. We can take subnormal series $\Gamma = \Gamma_0 \supset \Gamma_1 \supset ... \supset \Gamma_v = 1$ having cyclic factors Γ_i/Γ_{i+1} and the corresponding chain of fields $F = K_0 \subset K_1 \subset ... \subset K_v = E$. We can choose an appropriate basis $\pi_j^k, k = 0, 1, ..., q_j - 1$ for the field extension K_{j+1}/K_j such that $\pi_j^{q_j} \in K_j$ and appropriate generators of Galois groups act on π_j by ζ_j-multiplication. Using the regular representation of E in F-basis $\pi_1^{\alpha_1}\pi_2^{\alpha_2}...\pi_v^{\alpha_v}, 0 \leq \alpha_i < q_i$ of E we can construct the matrices-coefficients $R_{(i_1,...,i_v)}$ in the expansion of g:

$$g = \sum_{(i_1,...,i_v)} R_{(i_1,...,i_v)}\pi_1^{\alpha_1}\pi_2^{\alpha_2}...\pi_v^{\alpha_v}$$

in such a way that $g^t = I$ and $gg^\sigma = g^\sigma g$ for all $\sigma \in \Gamma$. So matrices $I_m \otimes g^\sigma, \sigma \in \Gamma$ generate a finite abelian Γ-stable matrix group of exponent t. The constructions from Theorems 1 and 2 give an explicite form of $R_{(i_1,...,i_v)}$, and the results analogous to the Theorems 2 and 3 can be obtained for arbitrary Γ-stable abelian matrix groups of exponent t.

References

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

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

[BM] H.-J. Bartels, D.A. Malinin, *Finite Galois stable subgroups of GL_n (in preparation).*

[C] S. D. Cohen, *The distribution of the Galois groups of integral polynomials*, Ill. J. Math. **23** (1979), 135–152.

[D] E. Dieterich, *Representation types of group rings over complete discrete valuation rings II In: Orders and their applications. Proceedings, 1984. Lecture Notes in Mathematics 1142. Edited by I.Reiner and K.W. Roggenkamp* (1985), Springer-Verlag, Berlin etc., 112–125.

[G] F.R. Gantmakher, *The theory of matrices*, 4th ed., "Nauka", Moscow, 1988; English transl. of 1st ed., Vols 1, 2, Chelsea, New York, 1959.

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

[M1] D.A.Malinin, *Galois stability for integral representations of finite groups*, (to appear in St. Petersburg Math.J.).

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

[M3] D.A.Malinin, *Integral representations over local fields for p-groups of a given class of nilpotency*, St. Petersburg Math.J. **10, N 1** (1999), 45–52.

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

[M5] D.A. Malinin, *On integral representations of finite abelian groups stable under Galois action*, Preprint MSLU N 42 (1998), 32 p.

[Min1] H.Minkowski, *Über den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen*, J. Reine Angew. Math. **100, no. 4** (1887), 449–458.

[Min2] H.Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. Reine Angew. Math. **101, no. 3** (1887), 196–202.

[Min3] H.Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig–Berlin, 1910.

[R] I.Reiner, *A survey of integral representation theory*, Bull. Amer. Math. Soc. **76** (1970), 159–227.

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

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

[RW1] J.Ritter and A.Weiss, *Regulators and Galois stability*, Math. Nachr. **46** (1992), 27–41.

[ST] D.A. Suprunenko, R.I. Tyshkevich, *Commutative Matrices*, "Nauka i technika", Minsk, 1966; English transl. Academic press, New York, 1968.

Belarusian State Pedagogical University, Minsk, Belarus
Sovetskaya str. 18, 220050 Minsk, Belarus
e-mail: malinin@bspu.unibel.by