

Representations of Some Groups and Galois Stability

Dmitry Malinin,

Department of Mathematics, UWI, Mona Campus, Kingston,

dmalinin@gmail.com

¹Nor Haniza Sarmin, ²Nor Muhainiah Mohd Ali

³Noor Asma' Adny Binti Mohd Adnan, ³Zainab Binti Yahya,

^{1,2,3,4}Department of Mathematical Sciences, Faculty of Science,

Universiti Teknologi Malaysia, Skudai, Johor, Malaysia

¹nhs@utm.my, ²normuhainiah@utm.my, ³adny_sabry@yahoo.com, ⁴zainabyahya90@gmail.com

Abstract

We study arithmetic problems for representations of finite groups over algebraic number fields and their orders under the ground field extensions. Let E/F be a Galois extension, and let $G \subset GL_n(E)$ be a subgroup stable under the natural operation of the Galois group of E/F . A concept generalizing permutation modules is used to determine the structure of groups G and their realization fields. We also compare the possible realization fields of G in the cases if $G \subset GL_n(E)$ and if all coefficients of matrices in G are algebraic integers. Some related results and conjectures are considered.

2000 Mathematics Subject Classification: 20C10, 20C05, 11R33

Key words and phrases: algebraic integers, Galois groups, integral representations, realization fields, permutation modules and lattices.

1. Introduction

It is interesting to study the relationship between the classical representations $h : H \rightarrow GL_n(K)$ over fields K and some related representations $f : H \rightarrow GL_n(S)$ over Dedekind rings S in K as well as establishing extra properties of these representations; here we are interested in the property of stability of $h(H)$ under the natural action of

Galois group. This condition was considered earlier for Galois stability of groups and orders in [16] and some other papers. In some mysterious way the representations involved appear to be of special interest for nilpotent groups, many results are just related to representations abelian groups. However, it is also interesting to establish the conditions for existence of faithful representations of groups of the given nilpotency class (see [7], [8], [13] for group representations of nilpotency class 2 and also [13], [14]) having this extra property. It would be interesting to extend our considerations to some other classes of groups [4], [6].

In this paper we study some arithmetic problems for representations of finite groups over algebraic number fields and arithmetic rings under the ground field extensions. We study finite subgroups $G \subset GL_n(S)$ for certain Dedekind rings S in algebraic number fields K with the focus on $S = O_K$, the ring of integers of K .

The following definition and result generalize [20] and [17]:

Definition 1.1. Consider a finite Galois extension K of the rationals \mathbf{Q} and a free \mathbf{Z} -module M of rank n with basis m_1, \dots, 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 $\{1, 2, \dots, k\}$ and roots of unity $\epsilon_i(g)$ such that $\epsilon_i(g)gM_i = M_{\Pi(g)i}$ for $1 \leq i \leq k$.

Fix a prime number p , a primitive p -th root of unity ζ_p , and for the ring of p -adic integers \mathbf{Z}_p set $\pi = 1 - \zeta_p$, $R = \mathbf{Z}_p(\zeta_p)$ and $F_p = R/\pi R$.

We say R -representation M of G for an RG module M which is free of finite rank as an R -module. A permutation lattice (respectively module) for G is a direct sum of $\mathbf{Z}_p G$ (resp. $F_p G$ for a finite field F_p containing p elements) modules of the form $ind_H^G(1)$. A generalized permutation lattice for G is a direct sum of RG -modules of the form $ind_H^G \phi$ for some homomorphism $\phi : H \rightarrow \langle \zeta_p \rangle$ of a subgroup H of G .

Theorem 1.1. ([20], Theorem 3). Let M be an R -representation of the finite p -group G so that $M = M/\pi M$ is a permutation F_p -module of G . Then M is a generalized permutation lattice for G .

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 -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.

We use the following result describing groups of A -type (see Definition 1.1) proven in [2], see Section 3:

Theorem 1.2. *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 is a group of A -type.*

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 were studied by Ritter and Weiss. 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 [18]). We can specify one application of the above result:

Corollary of Theorem 3.1. (Generalized "Hasse principle").

For arithmetic groups G defined over \mathbf{Q} such that the group of \mathbf{R} -points $G_{\mathbf{R}}$ is compact, totally real K/\mathbf{Q} and $Gal(K/\mathbf{Q})$ -stable subgroup G_{O_K} of $GL_n(O_K)$ the kernel of the natural cohomology map

$$H^1(Gal(K/\mathbf{Q}), G_{O_K}) \rightarrow \prod_v H^1(Gal(K_v/\mathbf{Q}_v), G_v)$$

is trivial.

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 unity. An explicit construction of these fields is given in Theorems 2.1 and Theorems 2.2 in Section 2. In fact, we construct some Galois algebras in the sense of [5], and we establish the lower bounds for their possible orders n . We show (see Theorem 2.2 in Section 2) that the restrictions for the given integers n , t , and d in Theorem 2.1 cannot 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], [10], [11].

Our results have some applications to positive definite quadratic lattices, see Section 3. Note that some interesting results on orthogonal decompositions of integral lattices can be found in [9], see also [19] for related finite linear groups.

We are also interested in applying our results to other problems using permutation modules and the methods and techniques of [12], [17] where they were applied to the Zassenhaus conjecture for the normalized unit group of the integral group ring of a p -group.

It would be interesting to use the explicit construction of the subgroups $G \subset GL_n(O_{K_{ab}})$ together with Theorem 1.2

Notation

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. $GL_n(S)$ denotes the general linear group over a ring S . $[E : F]$ 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 . $M_n(S)$ is the full matrix algebra over a ring S . Finite groups are usually denoted by capital letters G, H , and their elements by small letters, e.g. $g \in G, h \in H$, $\langle a, b, \dots \rangle$ denotes a group generated by a, b, \dots . 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 the K -algebra A over the field K . O_K denotes the maximal order of a number field K .

2. Galois stable integral 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 2.1. *Let F be an algebraic number field, let d, t be some prescribed positive integers and either $t > 1$ such that $n \geq \phi_E(t)d$, or $t = d = 1$, 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 exponent t such that $E = F(G)$.*

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

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

Proof of Theorem 2.1

If or $t = d = 1$, we have or $E = F$ and $G = \{I_n\}$, in this case the theorem is trivial. If or $t > 1, d = 1$, then $E = F$, $[E(\zeta_t) : E] = \phi_E(t)$, and we can consider an irreducible polynomial $f(x) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0 \in E[x]$ for $k = \phi_E(t)$ such that $f(\zeta_t) = 0$. Since $E = F$, all $a_i \in F$, and we can consider the following matrix corresponding to a regular representation of ζ_t :

$$M = \begin{vmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & \ddots & & & \\ 0 & 0 & \dots & 1 & a_{k-1} \end{vmatrix}$$

We have $M^t = I_k$, and $\langle M \rangle$ is a cyclic group of order t . Next take $g = M \oplus I_{n-k} \in GL_n(E)$, the direct sum of I_{n-k} and M . Then the group $G = \langle g \rangle$, generated by g , satisfies the requirements of the theorem.

Therefore, we can assume that $t > 1$ and $d > 1$.

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 $F(g_{11}, g_{12}, \dots, g_{nm})$ 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 . First 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 2.1

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

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

implies the linear relation

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

for all $\sigma_j \in \Gamma$, this would also imply $\det W^{-1} = 0$, which is impossible. Therefore, $\lambda_1 - 1, \lambda_2, \dots, \lambda_d$ generate the field $E(\zeta_t)$ over $F(\zeta_t)$, and so $B_1 - I_d, B_2, \dots, B_d$ generate $F(\zeta_t)$ -span $F(\zeta_t)[B_1, \dots, B_d]$ over $F(\zeta_t)$. Note that B_i can be expressed as a linear combination

of $g^{\sigma_i}, i = 1, 2, \dots, d$ 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

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

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

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

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

We have $F(\zeta_t)G = F(\zeta_t)[\langle g^{\sigma_1}, \dots, g^{\sigma_d} \rangle] = F(\zeta_t)[(g - I_d)^{\sigma_1}, \dots, (g - I_d)^{\sigma_d}]$, 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 -operation is d , we can use the coefficients of matrices $M^{\sigma_i}, i = 1, 2, \dots, d$ 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 $F(\zeta_t)$ 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 $\dim_F FFG = \dim_E EG, E$ 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 2.1 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 $\Gamma_0 = \{\sigma'_1, \sigma'_2, \dots, \sigma'_d\}$ 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 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

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

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 E over 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 $\dim_F F G' = \dim_F F[B_1 - I_d, B_2, \dots, B_d] = \dim_E E G' = d$ for G' generated by $g^{\sigma_i'}, i = 1, 2, \dots, d$. 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 $g_0^{\sigma_i}, i = 1, 2, \dots, d$. 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 one required in the formulation of Theorem 2.1. In this way we can construct a Γ -stable group G that satisfies the conditions of Theorem 2.1.

This completes the proof of Theorem 2.1.

As a corollary of Theorem 2.1 we have

Theorem 2.2. *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. In particular, it shows that there is an infinite number of realization fields $E = \mathbf{Q}(\mathbf{G})$ for the fixed integers $d = t = 2$ (which is not the case if $G \subset GL_n(O_E)$).

Example 2.1. *Let $d = 2, t = 2$. Pick $E = \mathbf{Q}(\sqrt{a})$ and $g = \begin{pmatrix} 0 & 1 \\ a^{-1} & 0 \end{pmatrix} \sqrt{a}$ 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. Note that $G \not\subset GL_n(O_E)$ in this example.*

Proof of Theorem 2.2.

We can use the proof of Theorem 2.1.

Let $G \subset GL_n(E)$ be a group given in the formulation of Theorem 1.1, and let n be minimal possible. Then we have the following decomposition of E -span $A = EG$:

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

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 $e_1 = \varepsilon_1^{\sigma_1} + \dots + \varepsilon_1^{\sigma_d}$ 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 Theorem 2.1 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 $I_n = \varepsilon_1 + \dots + \varepsilon_k$ 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 $T : C \rightarrow GL_r(E)$ 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 $g^\gamma, \gamma \in \Gamma$ 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 $m \leq d$. This completes the proof of Theorem 2.2.

Let G be a finite group and $f : G \rightarrow GL_n(\mathbf{C})$ a complex representation of G . Let F be the field generated by the traces of $\{f(g) : g \in G\}$. In this context it would be reasonable to ask a question:

Question. Is it true that there exist a representation $h : G \rightarrow GL_m(K)$ over a number field K , normal over F with Galois group $\Gamma = Gal(K/F)$, which is similar to $f(G)$, $h(G) = M^{-1}f(G)M$ for some $M \in GL_m(\mathbf{C})$, such that $h(G)$ is Γ -invariant?

3. Galois stable integral representations

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 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 $\Gamma := Gal(K/\mathbf{Q})$. Then there is the following

Conjecture 3.1. *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} . The following conjecture generalizes (and would imply) conjecture 1:

Conjecture 3.2. *Any finite subgroup of $GL_n(O_K)$ stable under the Galois group $\Gamma = Gal(K/\mathbf{Q})$ is of A -type.*

For totally real fields K , the only roots of unity contained in K are 1 and -1. Hence conjecture 2 reduces to conjecture 1.

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 [10], [11] 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 3.1. *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 is a group of A -type in the sense of our definition given in the introduction.*

Corollary 3.1. *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.

But if an extension E/F of number fields is unramified, the situation is completely different, see proposition below.

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 [10].

Let E, L be finite normal extensions of a number field F . Remark that the theorems below remain true also in the case of local fields L, E, F that are finite extensions of \mathbf{Q}_p ,

the rational p -adic number field. Let S_E, S_F, S_L be Dedekind rings in E, F, L with the fields of fractions E, F, L respectively such that S_E and S_L are free S_F -modules (and have S_F -bases), and both S_E and S_L are invariant under automorphisms of E/F and L/F respectively. If $F = \mathbf{Q}$ we can define S_F to be the intersection of F and S_E . For example, semilocal rings S_E, S_F, S_L that are obtained by intersection of valuation rings of all ramified prime ideals in the rings O_E, O_F, O_L satisfy the above conditions, as well as O_E, O_F and O_L themselves, provided O_E and O_L have O_F -bases (the latter is always true for $F = \mathbf{Q}$). Let w_1, w_2, \dots, w_d be a basis of S_E over S_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 $g^\gamma, \gamma \in \Gamma$ 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 2.1 from Section 2 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 3.2. *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 $GL_n(S_E)$ if and only if all determinants*

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

are divisible by D in the ring S_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. First, any Γ -stable subgroup $H \in GL_n(E)$ contains subgroups like G . And by Theorem 2.2 in Section 2, 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 3.2.

The proof of Theorem 3.2 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 $\{(D_j D^{-1})^\gamma, \gamma \text{ are varying in the Galois group of } L/F\}$.

We also use the fact that each semisimple matrix $B \in GL_n(F)$ is conjugate in $GL_n(F)$ to a matrix from $GL_n(S_F)$ if and only if all its eigenvalues are contained in S_L (see [2], [10]):

Lemma 3.1. 1) Let all eigenvalues $\lambda_i, i = 1, 2, \dots, n$ of a semisimple matrix $B \in GL_n(F)$ be contained in the ring S_L for some field $L \supset F$. Then B is conjugate in $GL_n(F)$ to a matrix that is contained in $GL_n(S_F)$. 2) Conversely, if a matrix B is contained in $GL_n(S_F)$, then its eigenvalues are contained in S_L .

We note that the reduction to the case of an irreducible group G is motivated by the following easy lemma [2], [10]:

Lemma 3.2. 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 3.2 can be used in the problem of existence for Γ -stable subgroups $G \subset GL_m(S_E)$ with the property $F(G) \neq F$ for some integer m . The following Corollary of Theorem 3.2 reduces the problem of existence for Γ -stable groups G to the case of $GL_n(F)$ -irreducible G .

In the case of unramified extensions the following proposition for integral representations in a similar situation is proven in [15] and can be extended to the case of Dedekind rings S_E considered here. However, in the parts 2) and 3) of the following proposition the statement is stronger if G is conjugate in $GL_n(F)$ to a subgroup of $GL_n(O_E)$ since in the most interesting cases $O_E \subset S_E$:

Proposition 3.1. Let $d > 1, t > 1$ be given rational integers, and let E/F be an unramified extension of degree d . Let h be the exponent of the class group of F .

1) If $n \geq \phi_E(t)d$, there is a finite abelian Γ -stable subgroup $G \subset GL_n(S_E)$ of exponent t such that $E = F(G)$.

2) If $n \geq \phi_E(t)dh$, there is a finite abelian Γ -stable subgroup $G \subset GL_n(O_E)$ of exponent t such that $E = F(G)$.

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

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

Theorem 3.3. If there is an abelian Γ -stable subgroup $G \subset GL_m(S_E)$ generated by $g^\gamma, \gamma \in \Gamma$ 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

$G'_i \subset GL_{m_i}(S_E)$ 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 3.3.

If $G \subset GL_m(S_E)$ is a group of exponent t and $g = B_1w_1 + B_2w_2 + \dots + B_dw_d$ for a basis w_1, \dots, w_d of S_E over S_F , then $B_i \in M_m(S_F)$, and it follows from Lemma 3.1 that the eigenvalues of B_j are contained in S_L . But eigenvalues are preserved under conjugation, so the latter claim is also true for all components G_i . We can apply Theorem 3.2 to $G_i, i = 1, \dots, k$. It follows that G_i are conjugate to subgroups $G'_i \subset GL_{m_i}(S_E)$. Now, Lemma 3.2 implies $E = F(G_1)F(G_2)\dots F(G_k)$. This completes the proof of Theorem 3.3.

Theorem 3.4. *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 $g = B_1w_1 + B_2w_2 + \dots + B_dw_d$ and all matrices $g^\gamma, \gamma \in \Gamma$, and let $E = F(G)$. Then G is conjugate in $GL_n(F)$ to $G \subset GL_n(S_F)$ if and only if all eigenvalues of matrices $B_i, i = 1, \dots, d$ are contained in S_L , where $L = E(\zeta_t)$.*

Proof of Theorem 3.4.

Let

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

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

$$C^{-1}gC = \begin{vmatrix} g_1 & & * \\ & \ddots & \\ 0 & & g_k \end{vmatrix} = B'_1w_1 + B'_2w_2 + \dots + B'_dw_d$$

for $B'_i = C^{-1}B_iC$. Let us consider F -algebra A generated by all $B'_i, i = 1, \dots, d$ 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 3.2 to each of them. Theorem 3.3 implies that each G_i is conjugate in $GL_{n_i}(F)$ to $G'_i \subset GL_{n_i}(S_F)$ if and only if all eigenvalues of matrices $B'_i, i = 1, \dots, d$ are contained in S_{L_i} , where $L_i = F(G_i)(\zeta_t)$. But $F(G) = F(G_1)F(G_2)\dots F(G_k)$ by Lemma 3.2, and so $L = L_1L_2\dots L_k$. This completes the proof of Theorem 3.4.

The approach to describe all Γ -stable matrix groups up to $GL_n(S)$ -conjugation for certain Dedekind rings $S \subset E$ can be based on either of Theorems 3.2, Theorems 3.3 or Theorems 3.4 for the existence of integral realizations of the given Γ -stable subgroup $G \subset GL_n(E)$. Therefore, 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 $GL_n(S)$ 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 $G \subset GL_n(S)$ which is not contained in $GL_n(F)$? Theorem 3.2 and Theorem 3.3 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 2.1 (see Section 2) provides a construction of a Γ -stable subgroup $G \subset GL_n(E)$ such that $E = F(G)$. Our argument in proof of Theorems 2.1 and Theorems 2.2 in Section 2 specify that G can be chosen as a group generated by g^γ , $\gamma \in \Gamma$. Theorem 3.2 allows us to check efficiently, whether it is possible to realize G over the ring S_E , in the terms of the basis of S_E over S_F and t . In the case if $S_E = O_E$ a free O_F -module (and O_E has an O_F -basis) the argument in Theorem 3.2 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 S . If a list of Γ -stable finite subgroups $G \subset GL_n(E)$ is given, we can apply Theorem 3.2 to their generating elements.

Note that in the case of relative extensions E/F of algebraic number fields ($F \neq \mathbf{Q}$), which was considered in [3], the situation is more complicated, and there are series of examples of nontrivial subgroups $G \subset GL_n(O_E)$ due to the existence of unramified extensions of the ground field F and the structure of the groups of units in O_E . The following example is given in the case of a ramified totally real extension E/F and a Galois stable $G \subset GL_2(E)$ of order 4 such that $F(G) \neq F$.

Example 3.1. Let

$$g := \begin{vmatrix} \sqrt{3 + \sqrt{2}} & -\sqrt{2 + \sqrt{2}} \\ \sqrt{2 + \sqrt{2}} & -\sqrt{3 + \sqrt{2}} \end{vmatrix},$$

let $E = F(\sqrt{3 + \sqrt{2}})$, $F = \mathbf{Q}(\sqrt{3 + \sqrt{2}} \cdot \sqrt{2 + \sqrt{2}})$. Then E/F is ramified at 2, the ramification is wild, and $G = \{g, -g, I_2, -I_2\} \subset GL_2(O_E)$ is a Γ -stable subgroup of order 4 and exponent 2.

Acknowledgement. The authors are grateful to the referees for useful suggestions.

REFERENCES

- [1] H.-J. Bartels, "Zur Galoiskohomologie definiter arithmetischer Gruppen" *J. reine angew. Math.* (1978), vol 298, p. 89–97
- [2] H.-J. Bartels, D. Malinin, "Finite Galois stable subgroups of GL_n ." In: *Noncommutative Algebra and Geometry*, Edited by C. de Concini, F. van Oystaeyen, N. Vavilov and A. Yakovlev, *Lecture Notes In Pure And Applied Mathematics*, vol. 243 (2006), p. 1–22.
- [3] H.-J. Bartels, D. Malinin, "Finite Galois stable subgroups of GL_n in some relative extensions of number fields", *Journal of Algebra and its Applications*, vol. 8, No. 4 (2009) 493-503.
- [4] A. Erfanian, F.N. Abd Manaf, F.G. Russo, N.H. Sarmin, "On The Exterior Degree of The Wreath Product of Finite Abelian Groups", accepted to *Bulletin of the Malaysian Mathematical Sciences Society*
- [5] V.V. Ishkhanov, B.B. Lurje, D.K. Faddeev "The embedding problem in Galois theory", "Nauka", Moscow, 1988
- [6] H.M Jafarabadi, N.H. Sarmin, M.R. Molaei, "Completely Simple and Regular Semi Hypergroups", *Bulletin of the Malaysian Mathematical Sciences Society*, Vol 35, nr 1, 335-343
- [7] L.C. Kappe, Nor Muhainiah Mohd Ali, N.H. Sarmin, "On the capability of finitely generated non-torsion groups of nilpotency class 2. *Glasgow Math. J.* 53 (2011), no. 2, 411-417.
- [8] L.C. Kappe, M.P. Visscher, N.H. Sarmin, "Two-generator two-groups of class two and their nonabelian tensor squares. *Glasgow Math. J.* 41 (1999), no. 3, 417-430.
- [9] A.I. Kostrikin, Pham Huu Tiep, "Orthogonal Decompositions and Integral Lattices". Walter de Gruyter, Berlin, New York. 1994.
- [10] D. Malinin, "Galois stability for integral representations of finite groups". *Algebra i analiz*, vol 12 (2000), p. 106–145.
- [11] D. Malinin, "Integral representations of finite groups with Galois action", *Dokl. Russ. Akad. Nauk*, v.349 (1996), p.303–305.

- [12] D. Malinin, "Integral representations of p -groups of the given nilpotency class over local fields", "Algebra and analiz" v.10 (1998), p.58–67.
- [13] D. Malinin, Integral representations of p -groups of given nilpotency class over local fields. Algebra i analiz (1998), vol. 10, 58–67 (Russian), English transl. in St.-Petersburg Math. J., vol 10, 45–52
- [14] D. Malinin, On integral representations of finite p -groups over local fields. Dokl. Akad. Nauk USSR (1989), vol. 309, 1060–1063 (Russian), English transl. in Sov. Math. Dokl. (1990). vol. 40, 619–622
- [15] D. Malinin, " On the existence of finite Galois stable groups over integers in unramified extensions of number fields ". Publ. Mathem. Debrecen, v.60/1-2 (2002), p. 179–191.
- [16] J. Ritter, A. Weiss, Galois action on integral representations. J. London Math. Soc. (2) (1992), vol. 46, 411–431
- [17] K. W. Roggenkamp, "Subgroup rigidity of p -adic group rings (Weiss arguments revisited)", J. London Math. Soc. (2), vol 46 (1992), p. 432-448
- [18] J. Rohlfs, " Arithmetische definierte Gruppen mit Galois-operation ", Invent. Math. (1978),vol. 48, p. 185–205
- [19] Pham Huu Tiep, A. E. Zalesski, "Some aspects of finite linear groups: A survey". J. Math. Sciences, vol. 100 (2000), p. 1893-1914
- [20] A. Weiss, "Rigidity of p -adic p -torsion", Annals of Math. (1988), vol 127, p. 317–322