

ON INTEGRAL REPRESENTATIONS OF FINITE GROUPS

Dmitry Malinin

dmalinin@gmail.com

Let E/F be a Galois extension of finite degree of global fields, i.e. E, F are finite extensions of the field of rationals \mathbf{Q} or a field of rational functions $R(x)$ with a finite field R .

Let us denote by O_E and O_F the maximal orders of E and F , and let Γ be the Galois group of E/F . Let $E = F(G)$ be a field obtained via adjoining to F all matrix coefficients of all matrices $g \in G$ for some finite subgroup $G \subset GL_n(E)$.

We are interested in 3 basic conditions for the Γ -operation on G and the integrality of G .

A. G is Γ -stable under the natural Galois operation.

B. $G \subset GL_n(O_E)$.

C. A primitive t -root of 1 $\zeta_t \notin E$.

We intend to discuss the following questions:

Question 1. Do the conditions A., B. imply $G \subset GL_n(FE_{ab})$, where E_{ab} is the maximal abelian subextension of E/\mathbf{Q} ?

Question 2. Do the conditions A., B., C. imply $G \subset GL_n(F)$?

Question 3. Classify the possible fields $E = F(G)$.

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

Below O_E is the maximal order of E and $F(G)$ is an extension of F generated via adjoining to F all matrix coefficients of all matrices $g \in G$, Γ is the Galois group of E over F .

We prove the existence of abelian Γ -stable subgroups G such that $F(G) = E$ provided some reasonable restrictions on the fixed normal extension E/F and integers n, t, d hold and study the interplay between the existence of Γ -stable groups G over algebraic number fields and over their rings of integers.

The problems below originate from classification problems of positive definite quadratic lattices and their isometries. There is a number of applications to Finite Group Schemes, Arithmetic Algebraic Geometry and Galois cohomology (see [6], [7]).

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} . Since G can be embedding to $GL_n(\mathbf{C})$ the intersection $G(O_K)$ of $GL_n(O_K)$ and $G(K)$, the subgroup of K -rational points of G , can be considered as the group of O_K -points of an affine group scheme over \mathbf{Z} , the ring of rational integers. Assume G to be definite in the

following sense: the real Lie group $G(\mathbf{R})$ is compact. The problem which is our starting point is the question: Does the condition $G(O_K) = G(\mathbf{Z})$ always hold true?

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

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

There are several reformulations and generalizations of the conjecture. Consider an arbitrary not necessarily totally real finite Galois extension K of the rationals \mathbf{Q} and a free \mathbf{Z} -module M of rank n with basis m_1, \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 $1 \leq i \leq k$. The following conjecture generalizes (and would imply) conjecture 1:

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

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

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

The following result was obtained in [1] (see also [2], [4] 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 [1] using the classification of finite flat group schemes over \mathbf{Z} annihilated by a prime p obtained by V. A. Abrashkin and J.- M. Fontaine:

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

Finiteness Theorem (see [8] and [9]). 1) *For a given number field F and integers n and t , there are only a finite number of normal extensions E/F such that $E = F(G)$ and G is a finite abelian Γ -stable subgroup of $GL_n(O_E)$ of exponent t .*

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

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

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

Theorem 3. Let E/F be a given normal extension of algebraic number fields with the Galois group Γ , $[E : F] = d$, and let $G \subset GL_n(E)$ be a finite abelian Γ -stable subgroup of exponent t such that $E = F(G)$ and n is the minimum possible. Then $n = d\phi_E(t)$ and G is irreducible under conjugation in $GL_n(F)$. Moreover, if G has the minimum possible order, then G is a group of type (t, t, \dots, t) and order t^m for some positive integer $m \leq d$.

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

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

In the case of unramified extensions the following theorem for integral representations in a similar situation is proven in [3]:

Theorem 4. Let $d > 1, t > 1$ be given rational integers, and let E/F be an unramified extension of degree d .

1) If $n \geq \phi_E(t)d$, there is a finite abelian Γ -stable subgroup $G \subset GL_n(O'_E)$ of exponent t such that $E = F(G)$ where O'_E is the intersection of valuation rings of all localization rings of O_E with respect to primes ramified in E/F .

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

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

4) If d is odd, then any 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 $g \in GL_n(E)$.

Some further results for Galois stable groups G in relative field extensions of characteristic 0 can be found in [5] and [9].

In the case of fields of positive characteristic we have

Theorem 5. Let F be a global field of a positive characteristic p , and let E be a splitting field of some irreducible polynomial $f(y) \in F[y]$ whose roots are the conjugates of some element $t \in E$. Then $E = F(G)$ for any positive integer n and an appropriate group $G \subset GL_n(E)$. Moreover, if $t \in E$ is an element of O_E , then $G \subset GL_n(O_E)$.

References

- [1] H.-J. Bartels, Dmitry 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.
- [2] Dmitry Malinin, "Galois stability for integral representations of finite groups". Algebra i analiz, vol 12 (2000), p.106–145.
- [3] Dmitry 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.
- [4] Dmitry Malinin, "Integral representations of finite groups with Galois action ", Dokl. Russ. Akad. Nauk, v.349 (1996), p.303–305.
- [5] H.-J. Bartels, Dmitry Malinin, Finite Galois stable subgroups of GL_n in some relative extensions of number fields, Journal of Algebra and Its Applications, vol. 8, Nr. 4 (2009), p. 493–503.
- [6] H.-J. Bartels, Zur Galois Kohomologie definiter arithmetischer Gruppen, J. reine angew. Math., vol. 298 (1978), p. 89–97.
- [7] H.-J. Bartels, Y. Kitaoka, Endliche arithmetische Untergruppen der GL_n , J. reine angew. Math., vol. 313 (1980), p. 151–156.
- [8] Dmitry Malinin. Galois stability, integrality and realization fields for representations of finite Abelian groups, Algebras and representation theory, vol. 6 (2003), nr. 2, p. 215–237.
- [9] Dmitry Malinin, Finite arithmetic groups, a monograph, Minsk, 2009.