On finite arithmetic groups

Dmitry MALININ

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Janvier 2011

IHES/M/11/02

ON FINITE ARITHMETIC GROUPS

Dmitry Malinin

Institut des Hautes Études Scientifiques
Le Bois-Marie 35, route de Chartres
91440 Bures-sur-Yvette, France
E-mail: dmalinin@ihes.fr and dmalinin@gmail.com

Abstract. In this paper we study representations of finite groups stable under Galois operation over arithmetic rings in local and global fields.

We consider a Galois extensions E/F and realization fields of finite subgroups $G \subset GL_n(E)$ stable under the natural operation of the Galois group of E/F; let $E = F(G)$ be a field obtained via adjoining to F all matrix coefficients of all matrices $g \in G$. Though for sufficiently large n and a fixed algebraic number field F every its finite extension E is realizable as $F(G)$ for some group G above, there is only a finite number of possible $F(G)$ if $G \subset GL_n(\mathcal{O}_E)$ for the ring $\mathcal{O}_E$ of integers of E. We study the possible realization fields for finite extensions of $\mathbb{Q}$, $\mathbb{Q}_p$ and global fields of positive characteristic. In particular, for a finite Galois extension $E/\mathbb{Q}$ and any finite subgroup $G \subset GL_n(\mathcal{O}_E)$ which is stable under the natural operation of the Galois group $Gal(E/\mathbb{Q})$ the realization field $\mathbb{Q}(G) = \mathbb{Q}(\zeta_m)$ for an appropriate root ζ_m of 1.

Some related results and conjectures are considered.

1. INTRODUCTION

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 $\mathbb{Q}$ or a field of rational functions $R(x)$ with a finite field R.

Let us denote by $\mathcal{O}_E$ and $\mathcal{O}_F$ 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) $G \subset GL_n(\mathcal{O}_E)$.

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

We intend to discuss the following questions:

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

Key words and phrases. algebraic integers, Galois groups, integral representations, realization fields.

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

Question 3. Is it possible to classify the realization 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. In [M2], [M3], [M4], [M6] it is shown 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 $\mathcal{O}_E$ 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.

In [M4] 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 [BM1], [B], [M6]).

Let K be a totally real algebraic number field with the maximal order $\mathcal{O}_K$, G an algebraic subgroup of the general linear group $GL_n(\mathbb{C})$ defined over the field of rationals $\mathbb{Q}$. Since G can be embedded to $GL_n(\mathbb{C})$, the intersection $G(\mathcal{O}_K)$ of $GL_n(\mathcal{O}_K)$ and $G(K)$, the subgroup of K-rational points of G, can be considered as the group of $\mathcal{O}_K$-points of an affine group scheme over $\mathbb{Z}$, the ring of rational integers. Assume G to be definite in the following sense: the real Lie group $G(\mathbb{R})$ is compact.

The problem which is our starting point is the question:

Does the condition $G(\mathcal{O}_K) = G(\mathbb{Z})$ always hold true for totally real fields K?

This problem is easily reduced to the following conjecture from the representation theory of finite groups:

Let $K/\mathbb{Q}$ be a finite Galois extension of the rationals and $G \subset GL_n(\mathcal{O}_K)$ be a finite subgroup stable under the natural operation of the Galois group $\Gamma = Gal(K/\mathbb{Q})$. Then there is the following

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

There are several reformulations and generalizations of the conjecture.

It is reasonable to consider arithmetic groups defined over algebraic number fields F and to study their subgroups of $\mathcal{O}_F$-points (see [Bo], 7.16); the functor $R_{F/\mathbb{Q}}$ of "restriction of scalars" allows to reduce some problems to considering groups over $\mathbb{Q}$. For a good introduction to the theory of arithmetic groups see [So]. The most interesting questions below are related to groups defined over

$\mathbb{Q}$. We can consider the behavior of automorphism groups of positive definite quadratic $\mathbb{Z}$ - lattices under totally real scalar extensions as a motivation of of our study of finite arithmetic groups, and to ask the following

Question. *If two positive definite quadratic $\mathbb{Z}$-lattices become isomorphic over the ring $\mathcal{O}_K$ of integers of a totally real field extension K of the rationals $\mathbb{Q}$, are they already isomorphic over $\mathbb{Z}$, the ring of rational integers ?*

The following definition (compare also Definition 2 given below in sect. 2 after the formulation of the Main Theorem) can be considered as an another generalization of the "generalized permutation lattice for a group G" in the sense of [We], p. 318.

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

The following conjecture generalizes (and would imply) conjecture 1:

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

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

Both conjectures are true (see [BM1]) and have some extra applications to arithmetic geometry and Galois cohomology [B]. Another application of the conjectures above can be the computation of orders of finite arithmetic groups in $GL_n(K)$. For instance, if K is a totally real algebraic number field and $f(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$ is a positive definite quadratic form, it is possible to estimate the order of the finite orthogonal group $O_f(\mathcal{O}_K) \subset \mathrm{GL}_n(\mathcal{O}_K)$ of this form over $\mathcal{O}_K$ using the formulas for finite integral groups of matrices (see [So], sect. 6.3 and also [Min2]) since $O_f(\mathcal{O}_K) = O_f(\mathbb{Z})$. The order of $O_f(\mathbb{Z})$ is bounded by the number $s(q, n) = \Pi q^{r(q,n)}$, where the product is taken for all primes $q = 2, 3, 5, 7, ...$, and

$$r(q, n) = \Sigma_{i=1}^{\infty} [\frac{n}{q^i(q-1)}].$$

The results below imply the positive solution of the above conjectures (the Main Theorem in sect. 2), the presented proof is shorter than one given in [BM1], and it allows to obtain also a result for Galois stable groups over local fields (theorem 6). The paper is organized as follows. The main results are formulated in sect. 2. In sect. 3 an integrality criterion and the finiteness theorem are proven and some auxiliary results are given for the needs of further sections. Sect. 4 and 5 are devoted to the proofs of theorems describing the structure of Galois stable groups over local and global fields. In sect. 7 a

probabilistic characterization of Galois stable groups over extensions of $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{d})$ is given, and in sect. 6 and 8 we can see, what happens in the case of relative number field extensions and the case of fields of positive characteristic respectively. In the last section some generalizations of Minkowski's result is suggested.

NOTATION

Throughout the paper we will use the following notations.
$\mathbb{Q}, \mathbb{Q}_p, \mathbb{Z}, \mathbb{Z}_p, \mathcal{O}_K$ denote the field of rationals and p-adic rationals, the ring of rational and p-adic rational integers respectively, and the ring of integers of a local field K. $\mathrm{GL}_n(R)$ denotes the general linear group over R. $[E : F]$ denotes the degree of the field extension E/F. For a primitive t-root ζ_t of 1 and a number field E we write $\phi_E(t)d = [E(\zeta_t) : E]$ for the generalized Euler function. I_m denotes 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), rank$M$ and det$M$ are rank and determinant of a matrix M. ${}^tM$ denotes a transposed matrix for M, $diag(d_1, d_2, ..., d_m)$ is a block-diagonal matrix having diagonal components $d_1, d_2, ..., d_n$. We suppose that K is a Galois extension of $\mathbb{Q}_p$. We denote by Γ the Galois group of a normal extension K/F ; if needed we specify K/F as a subscript in $\Gamma_{K/F}$. The symbols $\Gamma_i(\mathfrak{p})$ denote the i-th ramification groups of the prime divisor $\mathfrak{p}$ and $\Gamma_0(\mathfrak{p})$ the inertia group in Γ. In the case of local field extension $K/\mathbb{Q}_p$ we have only one prime ideal over the prime p, hence we will omit the prime divisor $\mathfrak{p}$ in the notation Γ_i,Γ_0. e_i is the order of Γ_i for $i \geq 1$, while e is the order of the inertia group. It is known, that $e = e_0 \cdot e_1$, where e_0 is the index of Γ_1 in Γ_0. 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. If G is a finite linear group, $F(G)$ denotes the field obtained by adjoining the matrix coefficients of all matrices $g \in G$. ζ_m denotes a primitive m-th root of unity. For a local field or an algebraic number field K of finite degree over $\mathbb{Q}_p$ or $\mathbb{Q}$ respectively we use the following notation: K^{ab} is the maximal abelian extension of K (an infinite extension of K) and K_{ab} denotes the maximal abelian subextension of K over $\mathbb{Q}_p$ or $\mathbb{Q}$ respectively. We denote by $\mathbb{Z}_{(p)}$ the localized ring with respect to the multiplicative subset $S := \mathbb{Z} - (p)\mathbb{Z}$, i.e. the rational numbers with denominators coprime to the given prime integer p.

2. FURTHER RESULTS

The following result was obtained in [M4] (see also [M6]).

Theorem 1 (Finiteness Theorem). *1) For a given number field F and integers n and t, there are only a finite number of normal extensions E/F such that $E = F(G)$ and G is a finite abelian Γ-stable subgroup of $GL_n(\mathcal{O}_E)$ 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 $d = [E\colon F]$ and $E = F(G)$ for some finite Γ-stable subgroup G of $GL_n(\mathcal{O}_E)$.

Theorem 2 (see [M4], theorem 1). *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^γ, $\gamma \in \Gamma$ for some $g \in GL_n(E)$.

Remark. *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-stable abelian subgroup $G \subset GL_n(E)$ of exponent t.*

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

Example 1. 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.

Theorem 3 (see [M4], 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^m for some positive integer $m \leq d$.*

In the case of unramified extensions the following theorem for integral representations in a similar situation is proven in [M3]:

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 $G \subset GL_n(\mathcal{O}'_E)$ of exponent t such that $E = F(G)$ where $\mathcal{O}'_E$ is the intersection of valuation rings of all localization rings of $\mathcal{O}_E$ 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 $G \subset GL_n(\mathcal{O}_E)$ 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 $GL_n(\mathcal{O}_E)$.
4) If d is odd, then any G given in 1) is conjugate in $GL_n(F)$ to a subgroup of $GL_n(\mathcal{O}_E)$.

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

Some further results for Galois stable groups G with entries in unramified field extensions of characteristic 0 can be found in [M3] and [M6].

The case $F = \mathbb{Q}$, the field of rationals, is specially interesting since there are no unramified extensions of $\mathbb{Q}$. The following theorem was proven in [BM1] (see also [M2] for the case of totally real extensions) using the classification of finite flat group schemes over $\mathbb{Z}$ annihilated by a prime p obtained by V. A. Abrashkin and J.- M. Fontaine [F]:

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

A similar result can be expected in the case of local field extensions. Consider a finite Galois extension $K/\mathbb{Q}_p$ of the field $\mathbb{Q}_p$ of rational p-adic numbers for $p \neq 2$ and a free $\mathbb{Z}_p$-module M of rank n with basis $m_1, \ldots, m_n$. The group $GL_n(\mathcal{O}_K)$ acts in a natural way on $\mathcal{O}_K \otimes M \cong \bigoplus_{i=1}^n \mathcal{O}_K m_i$. In this case our definition 1 should be modified:

Definition 2. *Consider a finite Galois extension $K/\mathbb{Q}_p$ for $p \neq 2$ and a free $\mathbb{Z}_p$-module M of rank n with basis $m_1, \ldots, m_n$. The group $GL_n(\mathcal{O}_K)$ acts in a natural way on $\mathcal{O}_K \otimes M \cong \bigoplus_{i=1}^n \mathcal{O}_K m_i$. A finite group $G \subset GL_n(\mathcal{O}_K)$ is said to be of A-type, if there exists a decomposition $M = \bigoplus_{i=1}^k M_i$ such that for every $g \in G$ there exists a permutation $\Pi(g)$ of $\{1, 2, \ldots, k\}$ and roots of unity $\epsilon_i(g)$ such that $\epsilon_i(g) g M_i = M_{\Pi(g)i}$ for $1 \leq i \leq k$.*

Example 2. *For a primitive p-root ζ_p of 1 and $\theta = \frac{1}{2}(\zeta_p + \zeta_p^{-1})$ we can consider $K = \mathbb{Q}_p(\theta, \sqrt{1-\theta^2})$ and a Γ-stable subgroup $G \subset GL_n(\mathcal{O}_K)$ generated by matrices $g^c, c \in \mathbb{Z}$, where*

$$g = \begin{vmatrix} \theta & \sqrt{1-\theta^2} \\ -\sqrt{1-\theta^2} & \theta \end{vmatrix}.$$

Note that $K/\mathbb{Q}_p$ is an abelian tamely ramified extension and G is a cyclic subgroup of $GL_2(\mathcal{O}_K)$ of order p. If the odd prime $p \equiv 3(mod 4)$, then $\zeta_p \notin K$ since $\zeta_p = \theta + \sqrt{-1} \cdot \theta^{-1}$ and the congruence $x^2 + 1 \equiv 0(mod p)$ has no solutions iff $p \equiv 3(mod 4)$.

The paper [BM1] gives a more explicit formulation of the Main Theorem above and states the following:

Theorem 5. *Let K be a finite Galois extension of $\mathbb{Q}$ and G be a finite subgroup of $GL_n(\mathcal{O}_K)$ which is stable under the natural operation of the Galois group Γ of the field K. Then G is of A-type and, in particular, $G \subset GL_n(\mathcal{O}_{K_{ab}})$ holds.*

Corollary. *The realization field $\mathbb{Q}(G) = \mathbb{Q}(\zeta_m)$ for any G which satisfies the conditions of the Main Theorem and an appropriate root ζ_m of 1.*

The proof of the corollary follows immediately from the theorem 5 and our definition 1.

Following the result of theorem 5, we can ask 2 questions for the groups G over local fields:

Question 4. *Let K be a finite Galois extension of $\mathbb{Q}_p$ and G be a finite subgroup of $GL_n(\mathcal{O}_K)$ which is stable under the natural operation of the Galois group Γ of the field K. Is it true that $G \subset GL_n(\mathcal{O}_{K_{ab}})$ holds, K_{ab} the maximal abelian subextension of K over $\mathbb{Q}_p$?*

It is known (see [BM1], [M2], [M6]) that for global normal field extensions $K/\mathbb{Q}$ the same question can be reduced to the case of elementary abelian Galois stable p-subgroup $G \subset GL_n(\mathcal{O}_K)$ of exponent p.

Question 5. *Let K be a finite Galois extension of $\mathbb{Q}_p$ with Galois group Γ, and let G be a finite Γ-stable subgroup of $GL_n(\mathcal{O}_K)$. Is it possible to classify all fields $\mathbb{Q}_p(G)$?*

We can give a positive answer to Question 4 for any elementary abelian Γ-stable p-subgroup $G \subset GL_n(\mathcal{O}_K)$. This also shows that for elementary abelian Γ-stable p-groups G above all fields $\mathbb{Q}_p(G)$ are abelian over $\mathbb{Q}_p$.

It follows from example 2 that for abelian extensions $K/\mathbb{Q}_p$ of local fields under the conditions of Question 4 G is not always a group of A-type.

Theorem 6. *Let $K/\mathbb{Q}_p$ ($p \neq 2$) be a normal extension of local fields, let Γ be its Galois group, let $G \subset GL_n(\mathcal{O}_K)$ be an elementary abelian Γ-stable p-subgroup of exponent p, and let $K = \mathbb{Q}_p(G)$. Then $K/\mathbb{Q}_p$ is an abelian field extension.*

The idea of the proof is to show that $K = \mathbb{Q}_p(G)$ has a special ramification structure over $\mathbb{Q}_p$, in particular, the inertia subgroup of Γ is cyclic for the prime divisor of p. For a certain subfield $E \subset K$ let E/F be a Galois extension of fields with the Galois group $\bar{\Gamma} = \{\sigma_1 = 1, \sigma_2, ..., \sigma_t\}$, let $w_1, w_2, \ldots, w_d$ be a basis of $\mathcal{O}_E$ over $\mathcal{O}_F$, and let $\zeta_p \in E$. For the proof of theorem 6 we can use the reduction to the case of group $G \subset GL_n(E)$, which is irreducible under $GL_n(F)$-conjugation and generated by all $g^\gamma, \gamma \in \bar{\Gamma}$ and some $g \in G$. We can use the following criterion of integrality of G:

Theorem 6 allows us to give a new proof of the Main Theorem stated above and proven in [BM1]. In the virtue of theorem 6, the proof of the Main Theorem can be reduced to the situation where K is an unramified extension of the maximal abelian subfield of K over $\mathbb{Q}$.

For the proof of the Main Theorem we can first reduce it to the case of elementary abelian group G (see [BM1], [M2]), next to apply theorem 6 to prove that the field extension $\mathbb{Q}_p(G)/\mathbb{Q}_p$ is abelian and to use the following theorem proven by Y. Ihara:

Let k be a fixed algebraic number field of finite degree over $\mathbb{Q}$, k^{ab} be the maximal abelian extension of k.

Theorem 7 (Y. Ihara, see [A]). *Let L be a finite Galois extension of k. Then, Lk^{ab} is unramified over k^{ab} if and only if, for any prime divisor of L its decomposition group in L/k is commutative.*

We can use Theorem 7 for the case $k = \mathbb{Q}$. The proof of theorem 7 is given in [A], proposition 1.

Finally we use the special ramification properties of the field $K = \mathbb{Q}_p(G)$ in theorem 6 to prove the Main Theorem above using theorem 6 and theorem 7.

3. INTEGRALITY OF GALOIS STABLE REPRESENTATIONS

This section contains some auxiliary results, some of them are contained in slightly different formulations in [M6]. For the convenience of the reader and for the needs of our further proofs these results and proofs are given below.

3.1. Proposition 1. *Let E/F be a normal extension of local fields with Galois group $\Gamma_{E/F} = \mathrm{Gal}(E/F)$ and let E_1, F_1 be rings with quotient fields E and F respectively. If $G \subset GL_n(E_1)$ is a finite $\Gamma_{E/F}$-stable subgroup which has $GL_n(F_1)$-irreducible components $G_1, G_2, \ldots, G_r$, then $F(G)$ is the composite of the fields $F(G_1)$, $F(G_2)$, ... , $F(G_r)$.*

Proof of proposition 1. Let

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

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 $F(G_1)F(G_2)\ldots F(G_r)$, then $g' = g^\gamma g^{-1} \neq I_n$. The blocks G_i in $h^{-1}Gh$ are stable under the action of γ, since $h \in GL_n(F_1)$ and the elements of $F(G_i)$ are fixed by γ. Because

$$h^{-1}gh = \begin{vmatrix} g_1 & & * \\ & \ddots & \\ 0 & & g_r \end{vmatrix}$$

and

$$(h^{-1}gh)^\gamma = h^{-1}g^\gamma h = \begin{vmatrix} g_1 & & *' \\ & \ddots & \\ 0 & & g_r \end{vmatrix}$$

are matrices having the same diagonal components, all eigenvalues of the matrix $g' = g^\gamma g^{-1}$ of finite order are 1 and hence $g' = I_n$. This contradiction completes the proof of proposition 1. □

3.2. In this section we formulate the mentioned criterion for the existence of an integral realization of an elementary abelian p-group G.

Let F be a finite field extension of $\mathbb{Q}_p$ and E, L be finite Galois extensions of F, different from F with Galois groups $\Gamma_{E/F}$ and $\Gamma_{L/F}$ respectively. As above let $\mathcal{O}_E$, $\mathcal{O}_L$ be the corresponding local rings of integers. Let $w_1, w_2, \ldots, w_t$ be a basis of $\mathcal{O}_E$ over $\mathcal{O}_F$, and let D be the discriminant of this basis. Suppose that some matrix g of prime order p has coefficients in E and all $\Gamma_{E/F}$-conjugates g^γ, $\gamma \in \Gamma_{E/F}$ generate a finite abelian group G of exponent p. Let $\sigma_1 = 1$, $\sigma_2, \ldots, \sigma_t$ denote all automorphisms of the Galois group $\Gamma_{E/F}$ of the field E over F.

Assume that $L = E(\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(n)})$ where $\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(n)}$ are the eigenvalues of the matrix g, therefore $L = E(\zeta_p)$, ζ_p is a primitive p-th root of unity. We will reserve the same notations for some extensions of σ_i to L, and the automorphisms of L/F will be denoted $\sigma_1, \sigma_2, \ldots, \sigma_r$ for some $r \geqslant t$. Let E be the field containing $F(G)$ (the field obtained by adjoining to F all coefficients of all $g \in G$). For a suitable choice of t elements of $\{\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(n)}\}$ say $\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(t)}$ we have the following

Proposition 2. *Let G be generated by all $g^\gamma, \gamma \in \Gamma_{E/F}$ and irreducible under $\mathrm{GL}_n(F)$-conjugation. Then G is conjugate in $\mathrm{GL}_n(F)$ to a subgroup of $\mathrm{GL}_n(\mathcal{O}_E)$ if and only if all determinants*

$$d_k = \det \begin{vmatrix} w_1 & \ldots & w_{k-1} & \zeta_{(1)} & w_{k+1} & \ldots & w_t \\ w_1^{\sigma_2} & \ldots & w_{k-1}^{\sigma_2} & \zeta_{(2)}^{\sigma_2} & w_{k+1}^{\sigma_2} & \ldots & w_t^{\sigma_2} \\ \vdots & & & & & & \\ w_1^{\sigma_t} & \ldots & w_{k-1}^{\sigma_t} & \zeta_{(t)}^{\sigma_t} & w_{k+1}^{\sigma_t} & \ldots & w_t^{\sigma_t} \end{vmatrix}$$

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

Note that the conditions of proposition 2 are always true if E is unramified over F since $D\mathcal{O}_E = \mathcal{O}_E$ in this case.

Corollary 1. *If there is an abelian $\Gamma_{E/F}$-stable subgroup $G \subset GL_n(O_E)$ of exponent p generated by g^γ, $\gamma \in \Gamma_{E/F}$ such that $E = F(G) \neq F$, then the $GL_n(F)$-irreducible components $G_i \subset GL_{n_i}(E)$, $i = 1, ..., k$ of G are conjugate in $GL_{n_i}(F)$ to subgroups $G_i' \subset GL_{n_i}(O_E)$ such that $E = F(G_1)F(G_2)...F(G_k)$. In particular, $F(G_i) \neq F$ for some indices i.*

The following corollary shows that the conditions of proposition 2 hold true even if G is not irreducible (for the definition of the semisimple matrices B_i compare the proof of proposition 2).

Corollary 2. *Let E/F be a normal extension of number fields with Galois group $\Gamma_{E/F}$. Let $G \subset GL_n(E)$ be an abelian $\Gamma_{E/F}$-stable subgroup of exponent p generated by g and all matrices $g^\gamma, \gamma \in \Gamma_{E/F}$, and let $E = F(G)$. Then G is conjugate in $GL_n(F)$ to $G' \subset GL_n(\mathcal{O}_E)$ if and only if all eigenvalues of matrices $B_i, i = 1, ..., t$ are contained in $\mathcal{O}_L$, where $L = E(\zeta_p)$. The latter happens if and only if the criterion of proposition 2, 1) holds true, i.e. all determinants*

$$d_k = \det \begin{vmatrix} w_1 & \ldots & w_{k-1} & \zeta_{(1)} & w_{k+1} & \ldots & w_t \\ w_1^{\sigma_2} & \ldots & w_{k-1}^{\sigma_2} & \zeta_{(2)}^{\sigma_2} & w_{k+1}^{\sigma_2} & \ldots & w_t^{\sigma_2} \\ \vdots & & & & & & \\ w_1^{\sigma_t} & \ldots & w_{k-1}^{\sigma_t} & \zeta_{(t)}^{\sigma_t} & w_{k+1}^{\sigma_t} & \ldots & w_t^{\sigma_t} \end{vmatrix}$$

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

Proof of proposition 2.

Using the basis $w_1, ..., w_t$ of $\mathcal{O}_E$ over $\mathcal{O}_F$ we can write

$$g^{\sigma_j} = \sum_{i=1}^{t} {w_i}^{\sigma_j} B_i \quad \text{for} \quad j = 1, ..., t$$

with semisimple matrices $B_i \in M_n(F)$. Since the matrix $W = [w_i^{\sigma_j}]_{j,i}$ is nondegenerate, the matrices B_i can be expressed as a linear combination of g^{σ_j}, $i, j = 1, 2, \ldots, t$:

$$B_i = \sum_{j=1}^{t} m_{ij} g^{\sigma_j},$$

where $[m_{ij}] = W^{-1}$. Since by assumption the matrices g^{σ_j} commute pairwise, all matrices B_i also commute with each other. The irreducibility of G implies that the minimal polynomial of B_i is irreducible over F for each i such that B_i is not zero (see [ST], p. 8, corollary 3 for example). So if one of the eigenvalues of B_i is in $\mathcal{O}_L$ then all of them are since they are Galois conjugate. Using the dual basis $w_1^*, ..., w_t^*$ to $w_1, ..., w_t$ with respect to the trace form one can see that the inverse matrix W^{-1} to $W = [w_i^{\sigma_j}]_{j,i}$ is of the form $W^{-1} = [w_j^{*\sigma_i}]_{j,i}$. In order to prove the claim of the proposition, we need to determine whether or not matrices $B_i, i = 1, ..., t$ are conjugate in $GL_n(F)$ to matrices $B_i' \in M_n(\mathcal{O}_F)$, since for the generator g of G the equation

$$g = B_1 w_1 + B_2 w_2 + \cdots + B_t w_t,$$

holds with $B_i \in M_n(F)$ and $w_1, ..., w_t$ a basis of $\mathcal{O}_E$ over $\mathcal{O}_F$. In fact each semisimple matrix $B_i \in M_n(F)$ is conjugate in $\mathrm{GL}_n(F)$ to a matrix from $M_n(\mathcal{O}_F)$ if and only if all its eigenvalues are contained in $\mathcal{O}_L$ (see lemma 2 below).

Cramer's rule now implies that $w_i^{*\sigma_j} = (-1)^{i+j} W_{i,j} det(W)^{-1}$, where $W_{i,j}$ is the (i, j)-minor of W. Over the splitting field L there is a basis which consists of eigenvectors for G. Let u be one such common eigenvector with

$$g^{\sigma_i} u = t_i u.$$

Then $\zeta_{(i)} := {t_i^{\sigma_i}}^{-1}$ is an eigenvalue of g. It also follows, that u is an eigenvector for B_k with eigenvalue

$$\lambda_k = \sum_{j=1}^{t} m_{kj} t_j = \sum_{j=1}^{t} (-1)^{j+k} W_{j,k} \zeta_{(j)}^{\sigma_j} det(W)^{-1}.$$

The cofactor expansion for determinants implies $\lambda_k = d_k / detW$ and therefore the eigenvalues of B_k are in $\mathcal{O}_L$ iff $detW$ divides d_k, which proves the criterion of proposition 2 and – by the definition of the eigenvalues t_i – also the second statement modulo the proof of the following

Auxiliary lemma. *i) Let all eigenvalues λ_j, $j = 1, 2, \ldots, k$ of the semisimple matrices $B_i \in M_n(F), i = 1 \ldots, t$ be contained in the ring $\mathcal{O}_L$ for some field $L \supset F$. Then B_i are conjugate in $GL_n(F)$ simultaneously to matrices that are contained in $M_n(\mathcal{O}_F)$.*

ii) Conversely, if the semisimple matrices B_i are contained in $M_n(\mathcal{O}_F)$ and B_i are diagonalizable over a field $L \supset F$, then their eigenvalues are contained in $\mathcal{O}_L$.

Proof of the lemma. i) Consider the F-algebra $A = F[B_1, \ldots, B_t]$ generated by the matrices $B_1, \ldots, B_t$. By [ST], ch. 1, sect. 1, corollary 2 we can consider A to be a field extending F. Let $a_1, a_2, \ldots, a_n$ be a basis of $\mathcal{O}_A$ over $\mathcal{O}_F$. Then for any $B \in A$ we have $B = b_1a_1 + \cdots + b_na_n$, and the elements $b_i \in F$ are contained in $\mathcal{O}_F$ iff $B \in \mathcal{O}_A$. But all coefficients k_{ij} of the characteristic polynomials $f_i(x) = k_{i0} + k_{i1}x + ... + k_{in}x^n$ of the matrices B_i are contained in $\mathcal{O}_L$, and $k_{in} = 1$, so $B_i \in A$ are integral over F. It follows that $B_i = b_{i1}a_1 + \cdots + b_{in}a_n$, and $b_{ij} \in \mathcal{O}_F$. If $v \in F^n$ is a non-zero vector in F^n, then $a_1v, a_2v, \ldots, a_nv$ is a basis of F^n, and $B_ia_jv = \sum_k c_{ijk}a_kv$, where $c_{ijk} \in \mathcal{O}_F$. It follows that for any i the matrix $C_i = [c_{ijk}]_{k,j}$ belongs to $GL_n(\mathcal{O}_F)$, and C_i is the matrix of the operator B_i in the basis $a_1v, a_2v, \ldots, a_nv$ of F^n. Therefore, B_i is conjugate in $GL_n(F)$ to C_i for any $i = 1, \ldots, t$.

ii) Consider the characteristic polynomials $f_i(x) = k_{i0} + k_{i1}x + ... + k_{in}x^n$ of the matrices B_i. Since $k_{in} = 1$ and all k_{ij} are in $\mathcal{O}_F$ all roots of $f(x)$ are in $\mathcal{O}_L$. This completes the proof of the Auxiliary lemma.

□

Remark. *In the situation of the Auxiliary lemma, i) the F-algebra $A = F[B_1, \ldots, B_t]$ is isomorphic to the field $L = F[\lambda_1, \ldots, \lambda_k]$ where λ_j, $j = 1, 2, \ldots, k$ are all eigenvalues of the matrices $B_i, i = 1 \ldots, t$.*

Proof of corollary 1. If $G \subset GL_n(O_E)$ is a group of exponent p and $g = B_1w_1 + B_2w_2 + \cdots + B_tw_t$ for a basis $w_1, ..., w_t$ of $\mathcal{O}_E$ over $\mathcal{O}_F$, then $B_i \in M_n(\mathcal{O}_F)$, and it follows from the Auxiliary lemma to proposition 2 that the eigenvalues of B_j are contained in $\mathcal{O}_L$. Notice, that for the second part of the Auxiliary lemma to proposition 2 the irreducibility is not needed. But eigenvalues are preserved under conjugation, so the latter claim is also true for all components G_i. We can apply proposition 2 to $G_i, i = 1, ..., k$. It follows that G_i are conjugate to subgroups $G_i' \subset GL_{n_i}(O_E)$. Now, proposition 1 implies $E = F(G_1)F(G_2)...F(G_k)$. This completes the proof of corollary 1.

□

Proof of corollary 2. Let

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

for $C \in GL_n(F)$ and irreducible components $G_i \subset GL_{n_i}(E), i = 1, ..., k$. Then for $g = B_1w_1 + B_2w_2 + \cdots + B_tw_t$

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

holds with $B'_i = C^{-1}B_iC$. Let us consider the F-algebra A generated by all $B'_i, i = 1, ..., t$ 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. Since $E \supset F(G_i)$ for all i, and $\mathcal{O}_E$ contains all rings $\mathcal{O}_{F(G_i)}$, we can apply proposition 2 to each of them. Notice that in proposition 2 we need not to assume, that $F(G) = E$. proposition 2 implies that each G_i is conjugate in $GL_{n_i}(F)$ to $G'_i \subset GL_{n_i}(\mathcal{O}_E)$ if and only if all eigenvalues of matrices $B'_i, i = 1, ..., t$ are contained in $\mathcal{O}_{L_i}$, where $L_i = F(G_i)(\zeta_p)$ and this happens iff

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

are divisible by $\sqrt{D}$ in the ring $\mathcal{O}_L$. But $F(G) = F(G_1)F(G_2)...F(G_k)$ by proposition 1, and so $L = L_1L_2...L_k$. This completes the proof of corollary 2. □

Proposition 3. *Let a Γ-stable abelian subgroup $G \subset GL_n(E)$ of exponent t be irreducible under $GL_n(F)$-conjugation, and let $E = F(G)$. Then d_t divides n.*

Proof of proposition 3. 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 orders, each of them being $GL_n\big(F(\zeta_t)\big)$-irreducible. This can be seen in the following way. By Wedderburn's theorem the $F(\zeta_t)$-span $F(\zeta_t)G$ of G is a direct sum of fields. So $A = F(\zeta_t)G = \oplus_{i=1}^k e_i(F(\zeta_t)G)$ for some primitive idempotents $e_i, i = 1, ..., k$, and $A_i = e_iF(\zeta_t)G$ are $F(\zeta_t)$-irreducible components of A. But $I_n = e_1 + e_2 + ... + e_n$, and all e_i are conjugate under the action of automorphisms of $F(\zeta_t)/F$. Indeed, if there are at least 2 orbits of elements from the set $\{e_1, ..., e_n\}$ under the action of the Galois group of $F(\zeta_t)/F$ then $I_n = \varepsilon_1 + \varepsilon_2$ for some idempotents $\varepsilon_1, \varepsilon_2 \in M_n(F)$ contrary to the irreducibility of G. Therefore, we can restrict ourselves to considering a $GL_n\big(F(\zeta_t)\big)$-irreducible component of G and use the same notation G for it.

Let $\varepsilon_i = \sum_j a_{ij}w_j$, $a_{ij} \in M_n(F(\zeta_t))$ 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, we can consider just one eigenvalue λ_{ij} of

each matrix a_{ij}. Simultaneous diagonalization of matrices ε_i and a_{ij} gives a system of linear equations in x_{ij} that can be determined using the Cramer's rule. The eigenvalues of a_{ij} are equal to its solutions $x'_{ij} = \lambda_{ij} = \frac{\det W_{ij}}{\det W}$ and their conjugates, where $W = [w_i^{\sigma_j}]$, $\Gamma = \{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ 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 ${}^t(0 \ldots 1 \ldots 0)$ (i-th element is 1, all other elements are 0). This can be done in the same way as in proposition 2 in sect. 3.1. It is obvious that λ_{ij} are precisely the elements of the matrix W^{-1}. But the coefficients of W generate $E(\zeta_t)$ over $F(\zeta_t)$, and so the coefficients of W^{-1} generate $E(\zeta_t)$ over $F(\zeta_t)$ as well. This proves our claim.

Furthermore, if $\sum k_{ij}\lambda_{ij} = \theta$ is a primitive element of $E(\zeta_t)$ over $F(\zeta_t)$ for some $k_{ij} \in F(\zeta_t)$, then the matrix $m = \sum k_{ij}a_{ij} \in M_n(F(\zeta_t))$ and its spectrum consists of all conjugate elements θ^σ, $\sigma \in \Gamma$, in virtue of irreducibility of G. Indeed, $m \in M_n(F(\zeta_t))$, so its characteristic polynomial $f(x) \in F(\zeta_t)[x]$, and all its roots are the eigenvalues of m together with their conjugates, and they have equal multiplicities. But m commutes elementwise with all $g \in G$ since all $a_{ij} \in E(\zeta_t)G$. If $f(x)$ had other roots, the matrix m would be reducible under $GL_n(F(\zeta_t))-$conjugation together with all elements of FG (see e.g. [G], ch. VIII). It follows that the number of eigenvalues of m is divisible by d_t, and d_t divides n. This completes the proof of proposition 3.

Here we can prove the Finiteness Theorem formulated in sect. 2:

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

Proof of Theorem 1. 1) In the virtue of proposition 1 from sect. 3.1 we can restrict ourselves to considering only irreducible G. It follows from integrality in $\mathcal{O}_E$ of all coefficients of G and Γ-stability of G that only divisors of t can ramify in E. Indeed, let $\mathfrak{p}$ be a ramified divisor of a prime p in $F(G)/F$. Then the inertia subgroup $\Gamma(\mathfrak{p}) \subset \Gamma$ of $\mathfrak{p}$ is not trivial, and there is $\gamma \in \Gamma(\mathfrak{p})$ and $g \in G$ such that $g^\gamma \neq g$, and $h = g^\gamma g^{-1} \equiv I_n (mod \mathfrak{p})$. But it is well known ([Min], [Min2], [Min3]) that if $h \equiv I_n (mod \mathfrak{p})$ then $h^{p^k} = I_n$ for some integer k. Therefore, p divides the order of G. According to proposition 3, the degree $[E\colon F]$ is restricted by a constant that depends only on t and n. Furthermore, it follows from the formula (see [N], proposition 4.9, p.159)

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

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 prescribed 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) Let us denote $d_1 = [E : \mathbb{Q}] = [F : \mathbb{Q}] \cdot d$. We claim that if prime p is ramified in E, then $\frac{d_1}{p-1} \geqslant 1$, that is $p \leqslant d_1 + 1$. Bartels proved in [B] that the absolute ramification index $e = e(E/\mathbb{Q})$ of p in this situation satisfies inequality $e \geqslant p-1$, and it is clear that $d_1 = [E : \mathbb{Q}]$ is always not less than e. Indeed, let $e < p-1$. Take any $g \in G, \gamma \in \Gamma(\mathfrak{p})$, the inertia group of $\mathfrak{p}$, for some prime divisor $\mathfrak{p}$ of p such that $h = g^\gamma g^{-1} \neq I_n$. Then $h \equiv I_n (mod \mathfrak{p})$ and for some positive integer t $h_1 = h^{p^t}$ is a matrix of order p, $h_1 \neq I_n, h_1^p = I_n$. Since $h_1 \equiv I_n (mod \mathfrak{p})$ we have $h_1 = I_n + \pi^m A$ for some prime element π of the localization $\mathcal{O}$ of $\mathcal{O}_E$ with respect to $\mathfrak{p}$, $A \in M_n(\mathcal{O})$ and the maximal possible m. Then

$$I_n = (I_n + \pi^m A)^p = I_n + p\pi^m(A + \pi^m B) + \pi^{mp} A^p.$$

This implies $pA + \pi^{m(p-1)} A^p \equiv 0_n (mod p\pi)$, and so $\pi^{m(p-1)}$ divides p. But this is impossible if $e < p-1$. We proved the claim $e \geqslant p-1$, and the number of ramified primes is restricted. Now we can use the proof given in 1). This completes the proof of Theorem 1.

3.3. Lemma 1. *Let $K/\mathbb{Q}_p$ be a finite extension, and let $\zeta_p \in \mathcal{O}_K$. Let $p = \mathfrak{p}^e$, $e = p-1$. Let G be a finite subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$ and $g \equiv I_n (\mathrm{mod}\, \mathfrak{p})$ for all $g \in G$. Then G is conjugate in $\mathrm{GL}_n(\mathcal{O}_K)$ to an abelian group of diagonal matrices of exponent p.*

Proof of Lemma 1. It is a generalization of the well known argument proposed by Minkowski [Min]. It is easy to prove that G is abelian of exponent p. Let π be the prime element of $\mathcal{O}_K$. Let $g_1 = I_n + \pi B_1, g_2 = I_n + \pi B_2$ for some $g_1, g_2 \in G$. Then $g_i^{-1} \equiv I_n - \pi B_i (\mathrm{mod}\, \pi^2)$, $i = 1, 2$ and $h = g_1 g_2 g_1^{-1} g_2^{-1} \equiv I_n (\mathrm{mod}\, \pi^2)$. It follows from lemma 1.5.1, (ii) in [BM1] that $h = I_n$, and the same lemma 1.5.1, (ii) in [BM1] shows that $g^p = I_n$ for any $g \in G$. First of all, G is conjugate over $\mathcal{O}_K$ to a group of triangular matrices, since G is abelian and $\mathcal{O}_K$ is a local ring, see [CR] theorem (73.9) and the remarks in [CR] on p. 493. On the other hand, we can describe explicitely the matrix M such that

$$M^{-1} g M = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$$

is a diagonal matrix for a triangular matrix g of order p which is congruent to $I_n (\mathrm{mod}\, \mathfrak{p})$. Indeed, let $g \in G$ and

$$g = \begin{vmatrix} \zeta_{(1)} I_{t_1} & P_2^1 \ldots & P_k^1 \\ 0 & \zeta_{(2)} I_{t_2} \ldots & P_k^2 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \zeta_{(k)} I_{t_k} \end{vmatrix},$$

and let

$$S = \begin{vmatrix} I_{t_1} & 0 \dots & A_1 \\ 0 & I_{t_2} \dots & A_2 \\ \vdots & \ddots & \vdots \\ 0 & \dots & I_{t_k} \end{vmatrix}$$

for $t_1 + t_2 + ... + t_k = n$ and $t_1 \leq t_2 \leq ... \leq t_k$, $\zeta_{(i)}, i = 1, 2, ..., k$ are appropriate p-roots of 1. We consider

$$S^{-1}gS = \begin{vmatrix} \zeta_{(1)}I_{t_1} & * \dots & M_k^1 \\ 0 & \zeta_{(2)}I_{t_2} \dots & M_k^2 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \zeta_{(k)}I_{t_k} \end{vmatrix},$$

and we find the system of conditions for providing $M_k^i = 0_{t_i,t_k}$, the zero $t_i \times t_k$-matrix. We have the following system of conditions:

$$\begin{cases} \zeta_{(1)}(1 - \zeta_{(k)}\zeta_{(1)}^{-1})A_1 + P_2^1 A_2 + ... + P_{k-1}^1 A_{k-1} + P_k^1 = 0_{t_1,t_k} \\ \dots \\ \zeta_{(k-2)}A_{k-2}(1 - \zeta_{(k)}\zeta_{(k-2)}^{-1}) + P_{k-1}^{k-2}A_{k-1} + P_k^{k-2} = 0_{t_{k-2},t_k} \\ \zeta_{(k-1)}A_{k-1}(1 - \zeta_{(k)}\zeta_{(k-1)}^{-1}) + P_k^{k-1} = 0_{t_{k-1},t_k}. \end{cases}$$

The condition $g \equiv I_n (\mathrm{mod}\, \mathfrak{p})$ implies $P_i^j \equiv 0_{t_j t_i} (\mathrm{mod}\, \mathfrak{p})$, and we can find $A_i, 1 \leq i \leq k-1$ sequentially using the results of previous steps:

$$A_{k-1} = -\frac{P_k^{k-1}}{\zeta_{(k-1)}(1 - \zeta_{(k)}\zeta_{(k-1)}^{-1})},$$

$$A_{k-2} = -\frac{(P_k^{k-2} + P_{k-1}^{k-2}A_{k-1})}{\zeta_{(k-2)}(1 - \zeta_{(k)}\zeta_{(k-2)}^{-1})},$$

$$A_{k-3} = -\frac{(P_k^{k-3} + P_{k-1}^{k-3}A_{k-1} + P_{k-2}^{k-3}A_{k-2})}{\zeta_{(k-3)}(1 - \zeta_{(k)}\zeta_{(k-3)}^{-1})},$$

and so on. Now, using induction on the degree n we can find a matrix M that transforms g to a diagonal form as required.

Since G is an abelian group of exponent p this allows to prove our claim locally over the ring $\mathcal{O}_K$. □

Using the same argument for global fields in [BM1] we proved

Lemma 1A. *Let $\mathcal{O}$ be a Dedekind ring in an algebraic number field, and let $\zeta_p \in \mathcal{O}$. Let $p = \mathfrak{p}^e$, $e = p - 1$. Let G be a finite subgroup of $\mathrm{GL}_n(\mathcal{O})$ and $g \equiv I_n (\mathrm{mod}\, \mathfrak{p})$ for all $g \in G$. Then G is conjugate in $\mathrm{GL}_n(\mathcal{O})$ to an abelian group of diagonal matrices of exponent p.*

Remark that for global fields in [BM1] we use statement (81.20) in [CR] for proving our result globally for the given Dedekind ring (compare for this also the proof of (81.20) and (75.27) in [CR]).

3.4. Lemma 2. *Let L be an extension of $\mathbb{Q}_p$ and $\mathfrak{p}$ a prime ideal in the field $L(\zeta_p)$. Suppose that L is unramified at $\mathfrak{p}$. Let Γ denote the Galois group of $L(\zeta_p)$ over L. If G is a finite Γ-stable subgroup of $\mathrm{GL}_n(\mathcal{O}_{L(\zeta_p)})$ consisting of matrices g, $g \equiv I_n (\mathrm{mod}\,\mathfrak{p})$, then G is conjugate in $\mathrm{GL}_n(\mathcal{O}_L)$ to an abelian group of diagonal matrices of exponent p.*

Proof of Lemma 2. We can assume that for some matrix $g \in G$ and a generator σ of Γ the condition $g^\sigma = g^\alpha$, $1 < \alpha < p$, is fulfilled. Indeed, by lemma 1 G is an abelian group of exponent p, so it can be considered as an $F_p\Gamma$ - module over the field F_p of p elements. Since Γ is a cyclic group of order $p-1$ generated by an element σ this element determines an automorphism of G and all its eigenvalues are contained in F_p. In fact, its matrix is diagonalizable over F_p because the order of σ is prime to p. Hence we can take $g \in G$ to be an eigenvector of this automorphism and so $g^\sigma = g^\alpha$, $1 < \alpha < p$ since not all eigenvalues are 1. Now lemma 1 provides the existence of a matrix $M \in \mathrm{GL}_n(\mathcal{O}_{L(\zeta_p)})$ such that $M^{-1}GM$ is a group of diagonal matrices. We shall show that α coincides with the integer β, $\zeta_p^\sigma = \zeta_p^\beta$, $1 < \beta < p$. Let us suppose that $M^{-1}gM = h = \mathrm{diag}(\lambda_1 I_{n_1}, \lambda_2 I_{n_2}, \ldots, \lambda_m I_{n_m})$, $\lambda_j \in L(\zeta_p)$, then $h^\sigma = h^\beta$ and $(M^\sigma)^{-1} g^\sigma M^\sigma = h^\beta$. Since $M^{-1}g^\alpha M = h^\alpha$ and $g^\sigma = g^\alpha$, it is obvious that

$$(M^\sigma)^{-1} M h^\alpha M^{-1} M^\sigma = h^\beta.$$

As Γ coincides with the inertia group of the ideal $\mathfrak{p}$ and $M \in \mathrm{GL}_n(\mathcal{O}_{L(\zeta_p)})$, it follows that $M^\sigma \equiv M (\mathrm{mod}\,\mathfrak{p})$. Therefore, the congruence $M^{-1}M^\sigma \equiv I_n (\mathrm{mod}\,\mathfrak{p})$ is valid and conjugation by matrix $M^{-1}M^\sigma$ maps diagonal elements of h^α to diagonal elements of h^β. But if $\alpha \neq \beta$, then the matrix $M^{-1}M^\sigma$ must have at least one diagonal element $d_{ii} = 0$, which is impossible. We proved our claim, and $\alpha = \beta$. We obtained also that $M^{-1}M^\sigma = \lambda = \mathrm{diag}(d_1, d_2, \ldots, d_m)$ for some $n_j \times n_j$-matrices d_j. Let us introduce the following matrix:

$$M_1 = \frac{1}{p-1}(M^{\sigma_1} + M^{\sigma_2} + \cdots + M^{\sigma_{p-1}}), \quad M_1 = [m_{ij}], \quad m_{ij} \in \mathcal{O}_{L(\zeta_p)},$$

$\sigma_1, \sigma_2, \ldots, \sigma_{p-1}$ are all elements of Γ. It is clear, that $M_1 \equiv M (\mathrm{mod}\,\mathfrak{p})$ and $\det M_1 \equiv \det M (\mathrm{mod}\,\mathfrak{p})$. It follows that $M_1 \in \mathrm{GL}_n(\mathcal{O}_{L(\zeta_p)})$. Furthermore, M_1 is stable under elementwise Γ-action, so all m_{ij} are Γ-stable and $m_{ij} \in L$. Hence $M_1 \in \mathrm{GL}_n(L)$. Since $M^\sigma = M\lambda$, it follows that $M_1^{-1}GM_1$ is contained in the group of diagonal matrices, as it was claimed.

□

The same argument for global fields proves

Lemma 2A. *Let L be an extension of $\mathbb{Q}$ and $\mathfrak{p}$ a prime ideal in the field $L(\zeta_p)$. Suppose that L is unramified at $\mathfrak{p}$ and let $\mathcal{O}_\mathfrak{p}$ denote the valuation ring of the ramified prime ideal $\mathfrak{p}$ in $L(\zeta_p)$. Let Γ denote the Galois group of $L(\zeta_p)$ over L. If G is a finite Γ-stable subgroup of $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$ consisting of matrices*

g, $g \equiv I_n(\mathrm{mod}\,\mathfrak{p})$, then G is conjugate in $\mathrm{GL}_n(L \cap \mathcal{O}_\mathfrak{p})$ to an abelian group of diagonal matrices of exponent p.

The detailed proofs of lemmata 1A and 2A (using the arguments above) are given in [BM1] (see lemma 1.5.2 and corollary 1.5.3 in [BM1]).

4. PROOF OF THEOREM 6

First of all we do not change the claim of theorem 6 when we adjoin ζ_p to K and simultaneously enlarge the elementary abelian p-group G by the scalar diagonal matrices $diag({\zeta_p}^m, {\zeta_p}^m, ..., {\zeta_p}^m)$, $0 \leq m \leq p-1$ if necessary. So let us assume $\zeta_p \in K$ and $diag(\zeta_p, \zeta_p, ..., \zeta_p) \in G$.

Similar to the case of rings in global fields (compare the corresponding results in [BM1] and [M2]) we need for the proof of theorem 6 in a first step the reduction to the case of an irreducible group G and later a criterion for the existence of integral realizations of an abelian matrix group.

Reduction to the case of an irreducible group G.

Here a matrix group $G \subset GL_n(R)$ is called reducible in $GL_n(R)$ or simply R-reducible (R a ring or a field) if there exist $h \in GL_n(R)$ such that

$$h^{-1}Gh \subset \left| \begin{matrix} G_1 & * \\ 0 & G_2 \end{matrix} \right|,$$

and G is irreducible otherwise.

The reduction to the case of an irreducible group G can be done using proposition 1 (see 3.1). Note, that under the assumption $diag(\zeta_p, \zeta_p, ..., \zeta_p) \in G$ also the irreducible components G_i contain scalar matrices $diag(\zeta_p, \zeta_p, ..., \zeta_p)$ of the appropriate size.

Since the composition of abelian field extensions of $\mathbb{Q}_p$ is again abelian, we can for the proof of theorem 6 restrict ourself to the case of an $\mathbb{Q}_p$-irreducible elementary abelian p-group $G \subset GL_n(\mathcal{O}_K)$.

Assume that theorem 6 is not true in general. Then there would exist a local field K normal over $\mathbb{Q}_p$ and an irreducible elementary abelian p-group $G \subset GL_n(\mathcal{O}_K)$ with a suitable number n such that K is generated over $\mathbb{Q}_p$ by the coefficients of the matrices $g \in G$ and this extension is not abelian. Let us assume that G is a minimal counterexample to the claim of theorem 6, minimal in the following sense: the degree $[K{\mathbb{Q}_p}^{ab} : {\mathbb{Q}_p}^{ab}]$ is minimal. Notice that this degree is greater than 1, since G is a counterexample to the claim of theorem 6 by assumption. Here ${\mathbb{Q}_p}^{ab}$ denotes the maximal abelian extension of $\mathbb{Q}_p$.

For the proof we distinguish essentially two cases depending on the ramification index e of $\mathbb{Q}_p(G)$ over $\mathbb{Q}_p$. In both cases we need a criterion for the existence of integral realizations of an abelian matrix group. It shows that the existence of G in question is possible only if certain determinants d_k are divisible by the root of the discriminant D of a certain field extension (for the details

see below and proposition 2). We will show, that for a minimal counterexample this condition is violated which gives the desired contradiction.

Recall, that e denotes the order of the inertia group, e_1 the order of the first ramification group and e_0 index of Γ_1 in Γ_0. It is known, that e_0 divides $p^f - 1$, where f is the degree of the unique prime in K over the prime p, in particular, e_0 is prime to p and the equation $e \cdot f = [K : \mathbb{Q}_p]$ holds.

If we adjoin roots of unity to K the degree $[K{\mathbb{Q}_p}^{ab} : {\mathbb{Q}_p}^{ab}]$ remains unchanged, furthermore if we adjoin ζ_t, for t prime to p – for instance $t = e_0$ or a divisor of e_0 – we do not change the ramification index e of K over $\mathbb{Q}_p$ (see for instance [8], ch. IV §4). Now let K_1 and K_0 denote the subfields of Γ_1- and Γ_0-fixed elements of K respectively, i.e. the first ramification field and the inertia subfield of K. Γ_1 and Γ_0 are normal subgroups of the Galois group of $K/\mathbb{Q}_p$, therefore K_1 and K_0 are Galois extensions of $\mathbb{Q}_p$, K_1 is tamely ramified and K_0 is unramified over $\mathbb{Q}_p$. In particular K_0 is a cyclic extension of $\mathbb{Q}_p$, hence $K_0 \subset K_{ab}$ and K_1/K_0 is cyclic. Let $G_0 = G^{\Gamma_1}$ denote the subgroup of elements in G that are fixed by the first ramification group Γ_1. Since G and Γ_1 are p-groups, G_0 is not trivial. Moreover, since Γ_1 is also normal in Γ_0, G_0 is a $Gal(K_1/K_0)$ stable subgroup of G. Consider the field $\mathbb{Q}_p(G_0)$ obtained by adjoining the matrix coefficients of all $g \in G_0$ to $\mathbb{Q}_p$. As a subfield of K_1 it is a tamely ramified extension of $\mathbb{Q}_p$. We put $e_0' := [K_0(G_0) : K_0]$ the degree of $K_0(G_0)/K_0$ which is also the ramification degree of $K_0(G_0)$ and set $t := e_0'$, which is prime to p, as remarked above. If we set $E = K_0(G_0)(\zeta_t)$ and $F = K_0(\zeta_t)$, we obtain a cyclic extension E/F such that $\zeta_t \in F$ for $t = e_0'$. Then E/F is a Galois extension of degree t, totally ramified and tamely ramified and $G_0 \subset \mathrm{GL}_n(\mathcal{O}_E)$ and G_0 is a $Gal(E/F)$- stable subgroup of $GL_n(\mathcal{O}_E)$. We distinguish two cases:
Case I: e_0' does not divide $p-1$ and case II: e_0' is a divisor of $p-1$.

We start with

Case I. e_0' does not divide $p-1$.

For later use in the proof, we notice: Since $(p) = (\zeta_p - 1)^{p-1}$ as principal ideals in $\mathbb{Q}_p(\zeta_p)$ holds we have for the corresponding ideals in $\mathcal{O}_{E\cdot\mathbb{Q}_p(\zeta_p)}$ the equation $(\mathfrak{p})^{e_0'} = (p) = (\zeta_p - 1)^{p-1}$, here denotes $\mathfrak{p}$ the prime divisor of p in $\mathcal{O}_E$. Since $p \geq 3$, $\left(\left[\frac{e_0'}{2}\right] + 1\right)(p-1) > e_0'$ holds, hence $\mathfrak{p}^{[t/2]+1}$ does not divide $(\zeta_p - 1)$ in $\mathcal{O}_{E(\zeta_p)}$.

Recall, that G is supposed to be a minimal counterexample to theorem 6 and $\mathbb{Q}_p$-irreducible. There is a matrix $g \in G_0$ such that matrices $g^\gamma, \gamma \in \Gamma$ generate G. Indeed, if matrices $g^\gamma, \gamma \in \Gamma$ generate a proper subgroup G_1 of G for any $g \in G_0$, then G_1 would be a group with coefficients contained in K_{ab}, since G is a minimal counterexample. But then the order e_0' would divide $p-1$, because $\mathbb{Q}_p(G_0)/\mathbb{Q}_p$ is tamely ramified at p, and as an abelian subextension of $\mathbb{Q}_p(G_1)$ contained in $\mathbb{Q}_p(\zeta_m)$ for a suitable integer m with p divides m, but $p^2 \nmid m$. But this contradicts the assumption that e_0' does not divide $p-1$. Therefore, there is a matrix $g \in G_0$ such that matrices $g^\gamma, \gamma \in \Gamma$ generate G. Choose a

generator σ of the Galois group of the cyclic extension E/F. The order of σ is $t = e_0'$, which by assumption does not divide $p-1$.

For a subgroup $\overline{G}_0$ of G_0 generated by a single element of G_0 which also satisfies the conditions of the case I we will later apply a criterion for the existence of integral realizations in the general linear group. It shows that the existence of the counterexample G in question is possible only if certain determinants d_k are divisible by the root of the discriminant D of the corresponding extension of number fields (see below and proposition 2 in sect. 3). Here in case I we use this for a certain subextension of the cyclic extension E/F which is also totally and tamely ramified with respect to the prime ideal over the fixed prime p.

So, in a first step we replace G_0 by a smaller subgroup $\overline{G}_0$ generated by a single element of G_0 which also satisfies the conditions of the case I. For this purpose take an arbitrary $g \in G_0$ such that $g^\gamma, \gamma \in \Gamma$ generate G and consider the subgroups $\overline{G}_0$ of G_0 generated by the elements $g^{\sigma^i}, i = 1, 2, ..., t$, that means by the orbit of g under the action of $\Gamma_{E/F}$, the Galois group of E/F. G_0 is covered by all these $\Gamma_{E/F}$-stable subgroups $\overline{G}_0$ for different g, and $F(G_0)$ is hence the composit of all the corresponding field extensions over F generated by the coefficients of these matrix subgroups $\overline{G}_0$ of G_0 for the different g. Since $F(G_0)/F$ is a cyclic totally ramified extension whose Galois group is generated by an element σ of order t equal to the ramification index of $F(G_0)/F$ and since the field $F(G_0)/F$ is a composite of the above mentioned subfields, say E_i, these extensions E_i/F are also cyclic and totally tamely ramified. We can conclude, that the ramification index of $F(G_0)/F$ is the least common multiple of the ramification indices of the different E_i/F. Since the order $t = e_0'$ of σ does not divide $p-1$, at least one of these fields E_i must have a ramification index say $\bar{t}$ which does not divide $p-1$.

Let us now fix such a subgroup $\overline{G}_0$ of G_0, with corresponding field extension $F(\overline{G_0})/F$ and ramification index $\bar{t}$ dividing t but not dividing $p-1$. $\overline{G_0}$ is not cyclic, since the group of Galois automorphisms $\Gamma_{F(\overline{G_0})/F}$, which induce automorphisms of $\overline{G_0}$, is of order not dividing $p-1$.

Since E/F is a cyclic Kummer extension, for $E' = F(\overline{G_0}) \subset E$ the extension E'/F is also a cyclic Kummer extension, and there are an integer $\bar{t}$ dividing t, $\overline{\sigma} \in \Gamma_{E/F}$ and a basis $1, \overline{\pi}, \overline{\pi}^2, \ldots, \overline{\pi}^{\bar{t}-1}$ such that $\overline{\pi}^{\bar{t}} \in F, \overline{\pi}^{\overline{\sigma}} = \overline{\pi}\zeta_{\bar{t}}$ and the Galois group $\Gamma_{E'/F}$ of E'/F is generated by $\overline{\sigma}$. Moreover, both extensions E/F and E'/F are totally ramified, and $\bar{t}$ is the ramification index of E'/F, so we have as earlier the following inequality: $\left(\left[\frac{\bar{t}}{2}\right]+1\right)(p-1) > \bar{t}$, and for the prime ideal $\mathfrak{p}'$ in E' $\mathfrak{p}'^{[\bar{t}/2]+1}$ does not divide $(\zeta_p - 1)$ in $E'(\zeta_p)$.

We use the statement of proposition 2 and its corollary 2 for the rings $\mathcal{O}_{E'}$ and $\mathcal{O}_F$ and a basis $1, \overline{\pi}, \overline{\pi}^2, \ldots, \overline{\pi}^{\bar{t}-1}$ such that $\overline{\pi}^{\bar{t}} \in F$. The Galois group $\Gamma_{E'/F}$ of E'/F, is generated by $\overline{\sigma}$, $\overline{\sigma}$ is of order $\bar{t}$ and we can consider the action of $\Gamma_{E'/F}$ on the basis $1, \overline{\pi}, \ldots, \overline{\pi}^{\bar{t}-1}$ in the following way: $(\overline{\pi}^i)^{\overline{\sigma}} = \overline{\pi}^i \zeta_{\bar{t}}^i$. For the matrix $W = [(\overline{\pi}^i)^{\overline{\sigma}^j}]_{i,j=0}^{\bar{t}-1}$ we have then

$$\det W = \overline{\pi}^{\bar{t}(\bar{t}-1)/2} \prod_{0\leqslant i<j\leqslant \bar{t}-1} (\zeta_{\bar{t}}^{j} - \zeta_{\bar{t}}^{i}).$$

Using proposition 2 or, alternatively, corollary 1 or corollary 2 of proposition 2, we will prove that $\overline{G_0} \subset GL_n(\mathcal{O}_F)$. For this purpose let us consider the determinants of the matrices W_j that are obtained from W by changing elements of j-th column of W to appropriate p-roots $\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(\bar{t})}$ of 1 that are the eigenvalues of the matrices $g^{\overline{\sigma}^i}, i = 1, 2, ..., \bar{t}$ for some $g \in \overline{G_0}$, according to proposition 2 (see sect. 3.1). Notice, that we can assume that $\bar{t} > 2$, since p is odd and $\bar{t}$ does not divide $p-1$. We will show that a generating matrix $g_0 \in \overline{G_0}$ is not contained in $GL_n(\mathcal{O}_{E'(\zeta_p)})$, then $g_0 \notin GL_n(\mathcal{O}'_E)$, and this contradiction is exactly the aim of our proof of the case 1). For simplicity let $\zeta = \zeta_{\bar{t}}$, but reserve previous notation for ζ_p for the rest of this proof. Consider the matrices

$$M_j = \begin{vmatrix} 1 & \overline{\pi} & \ldots & \overline{\pi}^{j-2} & \zeta_{(1)} - 1 & \overline{\pi}^{j} & \ldots & \overline{\pi}^{\bar{t}-1} \\ 1 & \overline{\pi}\zeta & \ldots & \overline{\pi}^{j-2}\zeta^{j-2} & \zeta_{(2)} - 1 & \overline{\pi}^{j}\zeta^{j} & \ldots & \overline{\pi}^{\bar{t}-1}\zeta^{\bar{t}-1} \\ \vdots & & & & & & & \\ 1 & \overline{\pi}\zeta^{\bar{t}-1} & \ldots & (\overline{\pi}^{j-2})^{\overline{\sigma}^{\bar{t}-1}} & \zeta_{(\bar{t})} - 1 & (\overline{\pi}^{j})^{\overline{\sigma}^{\bar{t}-1}} & \ldots & (\overline{\pi}^{\bar{t}-1})^{\overline{\sigma}^{\bar{t}-1}} \end{vmatrix},$$

$j = 2, \ldots, \bar{t}$ that are obtained from W_j by subtracting the first column of W_j from the j-th column of W_j.

Let us consider the symmetric matrix $\Lambda = [\zeta^{(i-1)(j-1)}]_{i,j=1}^{\bar{t}}$. The determinant of this matrix Λ is

$$det\Lambda = \prod_{0\leqslant i<j\leqslant \bar{t}-1} (\zeta^j - \zeta^i) = \prod_{1\leqslant j\leqslant \bar{t}-1} (\zeta^j - 1) \cdot \prod_{0<i<j\leqslant \bar{t}-1} (\zeta^j - \zeta^i),$$

and one can easily calculate the inverse: $\Lambda^{-1} = [\frac{\zeta^{-(j-1)(i-1)}}{\bar{t}}]_{i,j=1}^{\bar{t}}$. This gives the easy calculation of the (jk)-th cofactor of W_j in the following expansion:

$$\det W_j = detM_j = \theta_{j1}(\zeta_{(1)} - 1) + \theta_{j2}(\zeta_{(2)} - 1) + \cdots + \theta_{j\bar{t}}(\zeta_{(\bar{t})} - 1),$$

namely

$$\theta_{jk} = \overline{\pi}^{\bar{t}(\bar{t}-1)/2-(j-1)} \cdot (\Lambda^{-1})_{jk} \cdot det\Lambda.$$

Notice, that Λ and Λ^{-1} are integral matrices, since $\bar{t}$ is a p-adic unit. In order to apply the criterion of proposition 2, we consider the quotients

$$\frac{detW_j}{detW}$$

for the different indices j. Since $detW = \overline{\pi}^{\bar{t}(\bar{t}-1)/2} \cdot det\Lambda$, we have:

$$\frac{detW_j}{detW} = \overline{\pi}^{-(j-1)} \cdot ((\zeta_{(1)}-1)(\Lambda^{-1})_{j1} + (\zeta_{(2)}-1)(\Lambda^{-1})_{j2} + \cdots + (\zeta_{(\bar{t})}-1)(\Lambda^{-1})_{j\bar{t}}).$$

If all these elements for $j = 2, \ldots, \bar{t}$ were integral in $E'(\zeta_p)$, then we could conclude, that the vector

$$\overline{\pi}^{-(j-1)} \cdot \Lambda^{-1} \cdot \begin{vmatrix} \zeta_{(1)} - 1 \\ \zeta_{(2)} - 1 \\ \vdots \\ \zeta_{(\bar{t})} - 1 \end{vmatrix}$$

has also integral entries, the same would be true for

$$\overline{\pi}^{-(j-1)} \cdot \Lambda \cdot \Lambda^{-1} \cdot \begin{vmatrix} \zeta_{(1)} - 1 \\ \zeta_{(2)} - 1 \\ \vdots \\ \zeta_{(\bar{t})} - 1 \end{vmatrix},$$

which means, that all elements $\overline{\pi}^{-(j-1)} \cdot (\zeta_{(k)} - 1)$ would be integral, i.e. $\overline{\pi}^{-(j-1)} \cdot (\zeta_p - 1)$ is integral in $E'(\zeta_p)$. Since $\bar{t}$ does not divide $p-1$ and p is an odd prime, we have $\bar{t} \geq 3$. As already stated above for the prime ideal $\mathfrak{p}'$ in E' $\mathfrak{p}'^{[\bar{t}/2]+1}$ does not divide $(\zeta_p - 1)$ in $E'(\zeta_p)$, we therefore obtain the desired contradiction, so in the terms of proposition 2 (see sect. 3.1) $d_j \cdot (\sqrt{D})^{-1}$ can not be contained in $\mathcal{O}_L$, $L = E'(\zeta_p)$. By proposition 2 and its corollary 2 this implies that the above generating matrix $g \notin GL_n(\mathcal{O}_L)$ and so $G_0 \not\subset GL_n(\mathcal{O}_E)$. This is a contradiction.

Case II. e_0 divides $p-1$.

Now we can consider the case II. We recall the notation from the beginning of the proof of theorem 6. Below $K = \mathbb{Q}_p(G)$ is Galois over $\mathbb{Q}_p$, $p > 2$ and $G_0 = G^{\Gamma_1}$ is the subgroup of elements in G that are fixed by the first ramification group Γ_1 for the prime divisor $\mathfrak{p}$ of p, and e_0' denotes the ramification index of $\mathbb{Q}(G_0)$ over $\mathbb{Q}_p$ with respect to $\mathfrak{p}$. For case II we assume that e_0' is a divisor of $p-1$ since e_0 divides $p-1$ and e_0' divides e_0.

Adjoining a p-th root of unity ζ_p to K and extending the Galois operation to this larger field $K(\zeta_p)$ does not influence the validity of condition II, e_0' is still a divisor of $p-1$, moreover, it is equal to $p-1$, in particular, $e_0' > 1$ for $p > 2$. Note that the subgroup $G_0(\mathfrak{p}) = \{g \in G_0, g \equiv I_n (mod \mathfrak{p})\}$ is not trivial as a subgroup of matrices $g^{-1}g \equiv I_n (mod \mathfrak{p}), g \in G$ is not trivial and is a nontrivial p-group and its subgroup of Γ_1-fixed elements is not trivial, and according to lemma 1 in sect. 3 (which is a generalization of Minkowski's lemma) we have that the ramification index of $\mathbb{Q}_p(G_0(\mathfrak{p}))$ over $\mathbb{Q}_p$ is $p-1$. Simultaneously we can adjoin scalar matrices $\zeta_p I_n$ to G, this preserves Γ-stability and (if necessary) $GL_n(\mathbb{Q}_p)$-irreducibility of G, so $K(\zeta_p)$ is precisely the field obtained by adjoining the matrix coefficients of all matrices $g \in G$ to $\mathbb{Q}_p$. So we can and do assume that $\zeta_p \in K$ without loss of generality. As it was already mentioned in the beginning of the proof of theorem 6, we can assume that G is $GL_n(\mathbb{Q}_p)$-irreducible and

that G is a minimal counterexample to theorem 6 such that the degree $[K{\mathbb{Q}_p}^{ab} : {\mathbb{Q}_p}^{ab}]$ is minimal. Therefore, also in case II let $G \subset GL_n(\mathcal{O}_K)$ be a minimal counterexample such that the extension $\mathbb{Q}_p(G)/\mathbb{Q}_p$ is not abelian. For the treatment of case II we distinguish two subcases:

case II a): $\Gamma_1(\mathfrak{p})$ is trivial, i.e. K is tamely ramified over $\mathbb{Q}_p$.

and

case II b): $\Gamma_1(\mathfrak{p})$ is not trivial, i.e. K is wildly ramified over $\mathbb{Q}_p$.

We start with case II a).

Since the extension $K/\mathbb{Q}_p$ is tame and normal, and the ramification index $e = e(K/\mathbb{Q}_p)$ is a divisor of $p-1$, so $K(\zeta_p)/\mathbb{Q})$ is also tame and normal, and the ramification index $e(K(\zeta_p)/\mathbb{Q}_p) = p-1$. Therefore, $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ is unramified, so $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, \zeta_m)$ for some primitive root ζ_m of unity with m not divisible by p (see, for instance, [N], theorem 5.9), and we have:
$K \subset K(\zeta_p) = \mathbb{Q}_p(\zeta_p, \zeta_m)$. This implies that the field K is abelian over $\mathbb{Q}_p$, contrary to our assumption concerning the minimal counterexample G.

Now we consider case II b), where K is wildly ramified.

We assume that $\zeta_p \in K$. Since $\mathbb{Q}_p(\zeta_p)$ is a tame extension of $\mathbb{Q}_p$, Γ_1 operates trivially on the p-th roots of unity ζ_p, hence K^{Γ_1} contains also ζ_p. Take now in lemma 2 (see appendisect. 3) $K_0 = K^{\Gamma_0}$, then this field is unramified over $\mathbb{Q}_p$ for the prime divisor $\mathfrak{p}$ of p. Lemma 2 shows: up to conjugation in $GL_n(\mathbb{Z}_p)$

$$G_0(\mathfrak{p}) = \{g \in G_0, g \equiv I_n (mod \mathfrak{p})\}$$

consists of diagonal matrices. The group $G(\mathfrak{p}) := \{g \in G, g \equiv I_n(mod\mathfrak{p})\}$ is a nontrivial p-group and therefore $G_0(\mathfrak{p}) \neq \{I_n\}$ is not trivial as the subgroup of Γ_1-fixed elements of a nontrivial p-group. G is abelian and therefore in the centralizer of every matrix $h \in G_0(\mathfrak{p})$. If, in particular, $h = diag(l_1 I_{n_1}, \ldots, l_k I_{n_k})$, then $g = diag(g_1, \ldots, g_k), g_i \in GL_{n_i}(\mathcal{O}_K)$ holds for every $g \in G$ and therefore we can split G into $GL_n(\mathcal{O}_{K^{\Gamma_0}})$-irreducible components. In this decomposition we choose an irreducible component $G' \subset GL_m(\mathcal{O}_K)$ of G with a suitable natural number m such that G' has nontrivial Γ_1-action. Moreover, the described decomposition is stable under the operation of Γ_0 (see lemma 2), in particular, Γ_0 operates on the group G'.

If G'_0 denotes the subgroup of Γ_1-fixed elements of G', then the group

$$G'_0(\mathfrak{p}) := \{g \in G'_0, g \equiv I_m (mod \mathfrak{p})\}$$

consists of scalar matrices. The conditions on the ramification of case II are also satisfied for G' and G'_0 instead of G and G_0. But now the group $G'_0(\mathfrak{p})$ is equal to the group

$$\mu := \{\zeta I_m, \zeta^p = 1\}.$$

Let us now consider the Galois equivariant

$$\psi = \psi_m : G' \to GL_{m^p}(K)$$

given by $\psi(g) = g^{\otimes^p}$. The kernel of ψ is the set of all scalar matrices contained in G'. This kernel is not trivial, since $G'_0(\mathfrak{p}) \subset Ker\psi$. Hence we have:

There is an exact sequence

$$1 \longrightarrow \mu \longrightarrow G' \longrightarrow \psi(G') \longrightarrow 1$$

of Γ_0-invariant groups.

The aim of our proof is to use the above homomorphism $\psi = \psi_m$ for the construction of a certain group G'_1 in $G' \subset GL_m(K)$ such that: $K^{\Gamma_1}(G'_1)$ is an extension of K^{Γ_1} with $\zeta_p \in K^{\Gamma_1}(G'_1)$, $e'_0 = p-1$ and $K^{\Gamma_1}(G'_1)/K^{\Gamma_1}$ is an elementary abelian Kummer extension. In a second step a careful study of the Galois action of Γ_0 on G'_1 will then show that the constructed group G'_1 can not exist. This will give the desired contradiction.

We will use the following lemma for our proofs of theorems 6 and the Main Theorem, so we use it for the local and the global case. Since in the global situation the ramification and the inertia groups depend on the choice of the prime $\mathfrak{p}$ over p we use the notation $\Gamma_0(\mathfrak{p})$, $\Gamma_1(\mathfrak{p})$ respectively.

Lemma 3. *Let K/R be a finite Galois extension of either $R = \mathbb{Q}$ or $R = \mathbb{Q}_p$ with a Galois group Γ, and let $G \subset GL_n(\mathcal{O}_K)$ be a Γ-stable subgroup such that $R(G) \neq R$. Assume that $\zeta_p \in K$, then there is a subgroup $G'_1 \subset G' \subset GL_{m'}(K)$ such that $K^{\Gamma_1(\mathfrak{p})}(G'_1)$ is an extension of $K^{\Gamma_1(\mathfrak{p})}$ with $\zeta_p \in K^{\Gamma_1(\mathfrak{p})}(G'_1,)$ $e_0 = p-1$ and $K^{\Gamma_1(\mathfrak{p})}(G'_1)/K^{\Gamma_1(\mathfrak{p})}$ is an elementary abelian Kummer extension. In our construction G'_1 is generated by elements $g^\delta, \delta \in \Gamma_0(\mathfrak{p})$ for some $g \in GL_{m'}(K)$, and g is not fixed by $\Gamma_1(\mathfrak{p})$.*

Proof of lemma 3.

Construction of G'_1

We have $H := \psi(G')^{\Gamma_1(\mathfrak{p})} \neq \{I_m\}$ since both $\psi(G')$ and $\Gamma_1(\mathfrak{p})$ are p-group. We notice (and use this later), that

(i) H is $\Gamma_0(\mathfrak{p})$- stable, since $\Gamma_1(\mathfrak{p})$ is a normal subgroup of $\Gamma_0(\mathfrak{p})$, and

(ii) the action of $\Gamma_0(\mathfrak{p})$ on H is given by the cyclotomic character.

More precisely, we have for $h \in H$ and $\delta \in \Gamma_0(\mathfrak{p})$ $h^\delta = h^{\chi(\delta)}$. Here $\chi(\delta)$ denotes the unique integer modulo p such that $\zeta^\delta = \zeta^{\chi(\delta)}$ holds for all p-th root of unity ζ and $\delta \in \Gamma_0(\mathfrak{p})$. This is an immediate corollary of lemma 2 and lemma 2A.

Now, if there exist a $g \in \psi^{-1}(H)$ having nontrivial $\Gamma_1(\mathfrak{p})$-action, then define G'_1 as the subgroup of $\psi^{-1}(H)$ generated by all $g^\delta, \delta \in \Gamma_0(\mathfrak{p})$. If such an element g does not exist in $\psi^{-1}(H)$, we can suppose, that $\psi(G')$ has nontrivial $\Gamma_1(\mathfrak{p})$-action (since otherwise g with the needed property would exist). Now consider

a suitable irreducible component G'' of $\psi(G')$ having nontrivial $\Gamma_1(\mathfrak{p})$-action and apply the corresponding map ψ' to G''. For simplicity we call this map ψ' also simply ψ. If $\psi(G'')$ is fixed elementwise by $\Gamma_1(\mathfrak{p})$, again we have the needed element $g \in G''$ with nontrivial $\Gamma_1(\mathfrak{p})$-action, and we can define G_1'' in G'' correspondingly. Otherwise, we take an irreducible component $G''' \subset \psi(G'')$ having nontrivial $\Gamma_1(\mathfrak{p})$-action etc. Since the order of the groups $G', G'', G''', ...$ is becoming smaller and smaller (the kernel of the different maps ψ is not trivial), we will have at last $G^{(i)}$ to be fixed by $\Gamma_1(\mathfrak{p})$ with the least possible i, so we have the needed element $g \in G^{(i-1)}$ with nontrivial $\Gamma_1(\mathfrak{p})$-action. Instead of G_1' we consider then the subgroup of $\psi^{-1}(\psi(G^{(i-1)})^{\Gamma_1(\mathfrak{p})})$ generated by all $g^\delta, \delta \in \Gamma_0(\mathfrak{p})$. For simplicity let us call these groups again G_1', G' and again we denote by m the degree of the corresponding linear group.

□

We continue with the proof of case II b).

2) Study of the Galois action of $\Gamma_0(\mathfrak{p})$ *on* G_1' *and on* $K^{\Gamma_0(\mathfrak{p})}(G_1')$.

For $g \in G_1'$ and for $\gamma \in \Gamma_1(\mathfrak{p})$ we have $\psi(g^\gamma)\psi(g)^{-1} = \psi(g)^\gamma \psi(g^{-1}) = \psi(g)\psi(g)^{-1} = I_m$. This implies $g^\gamma = g\zeta$ for any $\gamma \in \Gamma_1(\mathfrak{p})$ with a suitable p-th root of unity $\zeta = \zeta_\gamma$.

Let σ be an element of $\Gamma_0(\mathfrak{p})$, whose image in $\Gamma_0(\mathfrak{p})/\Gamma_1(\mathfrak{p})$ is a generator of $\Gamma_0(\mathfrak{p})/\Gamma_1(\mathfrak{p})$ and take $g \in G_1'$ such that G_1' (according to our construction in lemma 3) is generated by all elements $g^\delta, \delta \in \Gamma_0(\mathfrak{p})$ and g is not fixed by $\Gamma_1(\mathfrak{p})$.

There are two possibilities: $g^{-1}g^\sigma \in GL_m(K^{\Gamma_1(\mathfrak{p})})$ or $g^{-1}g^\sigma$ is not fixed by the ramification group $\Gamma_1(\mathfrak{p})$.

In the first of these two cases we claim that $g^\sigma = g\zeta_\sigma$ for a suitable p-th root of unity ζ_σ. Let us prove this and show how to get the desired contradiction in that case. For this purpose notice that $d := g^{-1}g^\sigma \equiv I_m (mod \mathfrak{p})$ and therefore using lemma 2 we can diagonalize this matrix d over $GL_m(\mathcal{O}_{K^{\Gamma_0(\mathfrak{p})}})$. But since G' is irreducible over $GL_m(\mathcal{O}_{K^{\Gamma_0(\mathfrak{p})}})$ it follows, that $d = \zeta_\sigma I_m$, for a suitable root of unity ζ_σ.

Now we have $g^\sigma = g\zeta_\sigma$ and at the same time $g^\gamma = g\zeta_\gamma$ for any $\gamma \in \Gamma_1(\mathfrak{p})$. Since $\Gamma_1(\mathfrak{p})$ operates trivially on the p-th roots of unity ζ we obtain: $g^\sigma = g^{\gamma^k}$, for some integer k and therefore the two Galois automorphisms σ and γ^k coincide on $K^{\Gamma_0(\mathfrak{p})}(G_1')$ since g is any generator of G_1'. This gives the contradiction in the case, where $g^{-1}g^\sigma \in GL_m(K^{\Gamma_1(\mathfrak{p})})$.

In the alternative case $g_0 := g^{-1}g^\sigma$ is not fixed by the ramification group $\Gamma_1(\mathfrak{p})$. Now consider the group $\widetilde{G} \subset G_1'$ generated by all elements ${g_0}^\delta, \delta \in \Gamma_0(\mathfrak{p})$. Since for any $\delta \in \Gamma_0(\mathfrak{p})$ we have

$$\psi({g_0}^\delta) = \psi(g_0)^\delta = \psi(g_0)^{\chi(\delta)} = \psi({g_0}^{\chi(\delta)}),$$

it follows that ${g_0}^\delta = {g_0}^{\chi(\delta)}\zeta_\delta$ with suitable p-th roots of unity ζ_δ depending on the Galois automorphism δ. Therefore the group $\widetilde{G}$ is generated by g_0 and $\zeta_p I_m$ and the order of $\widetilde{G}$ is p^2.

Define $\widetilde{K} := K^{\Gamma_0(\mathfrak{p})}(\widetilde{G})$, which is Galois over $K^{\Gamma_0(\mathfrak{p})}$ by definition of $\widetilde{G}$. We study the Galois action on $\widetilde{K}$ (like on $K^{\Gamma_0(\mathfrak{p})}(G_1')$ in the first case). For this purpose we denote by $\widetilde{\Gamma_0(\mathfrak{p})}$ and $\widetilde{\Gamma_1(\mathfrak{p})}$ the corresponding inertia respectively ramification groups of the extension $\widetilde{K}/K^{\Gamma_0(\mathfrak{p})}$. We have $\widetilde{\Gamma_1(\mathfrak{p})} \neq \{1\}$ since the $\Gamma_1(\mathfrak{p})$-action on $\widetilde{G}$ is not trivial. We then claim first, that p is the highest p-power dividing the order of $\widetilde{\Gamma_0(\mathfrak{p})}$. The Galois group $\widetilde{\Gamma_0(\mathfrak{p})}$ of $\widetilde{K}/K^{\Gamma_0(\mathfrak{p})}$ is contained in the group of linear automorphism of $\widetilde{G}$ (considered as a 2-dimensional vector space over the field F_p of p elements), so its order divides the order of $GL_2(F_p)$, which equals to $(p^2-1)(p^2-p)$. This implies that p^2 does not divide the order of $\widetilde{\Gamma_0(\mathfrak{p})}$, so the Galois group of $\widetilde{K}/\widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}$ is cyclic of order p, as claimed above.

Note that the inertia subgroup of $\widetilde{\Gamma_0(\mathfrak{p})}$, so the Galois group of $\widetilde{K}/\widetilde{K}^{\widetilde{\Gamma_0(\mathfrak{p})}}$ has the order $p(p-1)$.

Hence $\widetilde{K} = \widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}(\sqrt[p]{u})$ with $u \in \widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}$. Now $\sigma(\widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}) = \widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}$ since $\widetilde{\Gamma_1(\mathfrak{p})}$ is a normal subgroup of $\widetilde{\Gamma_0(\mathfrak{p})}$. Therefore, $\widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}(\sqrt[p]{u}) = \widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}}(\sqrt[p]{u^\sigma})$, and one concludes:

$$\sqrt[p]{u^\sigma}(\sqrt[p]{u})^{-1} \in \widetilde{K}^{\widetilde{\Gamma_1(\mathfrak{p})}} \subset K^{\Gamma_1(\mathfrak{p})}.$$

Since ${g_0}^{-1}{g_0}^{\gamma} = \zeta_\gamma I_m$ for all $\gamma \in \Gamma_1(\mathfrak{p})$ we have $g_0 = \sqrt[p]{u}g_1$ with $g_1 \in GL_m(K^{\Gamma_1(\mathfrak{p})})$. It follows that

$$g_0^{-1}g_0^{\sigma} \in GL_m(K^{\Gamma_1(\mathfrak{p})})$$

and we can apply lemma 2 to this element. Like in the first of the considered two cases with g_0 instead of g we can conclude that ${g_0}^{\sigma} = g_0\zeta_\sigma$ for a suitable p-th root of unity ζ_σ. The contradiction follows then analogously to the first case for $g^{-1}g^{\sigma} \in GL_m(K^{\Gamma_1(\mathfrak{p})})$, but here we can replace g by g_0.

□

Note that under the conditions of lemma 3 in the case of a global field extension $K/\mathbb{Q}$ for $R = \mathbb{Q}$ we can use lemmata 1A and 2A instead of lemma 1 and lemma 2 in the argument 2) above. So we can summarize the argument given in 2) as

Résumé. *Under the conditions of lemma 3 let σ be an element of $\Gamma_0(\mathfrak{p})$, whose image in $\Gamma_0(\mathfrak{p})/\Gamma_1(\mathfrak{p})$ is a generator of $\Gamma_0(\mathfrak{p})/\Gamma_1(\mathfrak{p})$ and take $g \in G_1'$ such that G_1' (according to the construction in lemma 3) is generated by all elements $g^\delta, \delta \in \Gamma_0(\mathfrak{p})$ and g is not fixed by $\Gamma_1(\mathfrak{p})$.*

There are two possibilities:

1. $g^{-1}g^{\sigma} \in GL_m(K^{\Gamma_1(\mathfrak{p})})$. Then for any $\gamma \in \Gamma_1(\mathfrak{p})$ we have $g^{\sigma} = g^{\gamma^k}$, for some integer k.

2. $g^{-1}g^{\sigma}$ is not fixed by the ramification group $\Gamma_1(\mathfrak{p})$. In this case there exist an element $g_0 \in G_1'$ and a subgroup $\widetilde{G} \subset G_1'$ generated by all elements ${g_0}^\delta$, $\delta \in \Gamma_0(\mathfrak{p})$ the condition ${g_0}^{\sigma} = g_0\zeta_\sigma$ for a suitable p-th root of unity ζ_σ holds true. Then for any $\gamma \in \Gamma_1(\mathfrak{p})$ we have $g_0^{\sigma} = g_0^{\gamma^k}$, for some integer k.

Both conditions lead to a contradiction for a minimal counterexample G such that $R(G) \neq R$ and the extension $R(G)/R$ is not abelian.

5. PROOF OF THE MAIN THEOREM

Now we can use theorem 6 for a proof of the Main Theorem formulated in sect. 2, which is shorter than the proof given in [BM1].

According to [BM1], we can reduce the general situation to the case, when $K/\mathbb{Q}$ is unramified outside a fixed prime $p \neq 2$, and G is an elementary abelian p-group.

Let $K = \mathbb{Q}(G)$ for a Γ-stable elementary abelian p-group G satisfying the conditions of the Main Theorem formulated in the introduction. In the virtue of theorem 6 we can assume that for the completion $K_{\mathfrak{p}}$ of K with respect to any prime divisor $\mathfrak{p}$ of p the extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ is abelian. Furthermore since we can assume that K is unramified outside p, we have cyclic in particular abelian decomposition groups of the finite primes not dividing p. But then according to theorem 7 for this extension $K/\mathbb{Q}$ we have: K/K_{ab} is unramified (here K_{ab} denotes the maximal abelian over $\mathbb{Q}$ subfield of K).

As mentioned above we have a Galois extension $K = \mathbb{Q}(G)$ unramified outside a fixed prime p, $p > 2$. Consider $G_0 = G^{\Gamma_1(\mathfrak{p})}$ the subgroup of elements in G that are fixed by the first ramification group $\Gamma_1(\mathfrak{p})$ for some prime divisor $\mathfrak{p}$ of p, and e_0' denotes the ramification index of $\mathbb{Q}(G_0)$ over $\mathbb{Q}$ with respect to $\mathfrak{p}$. Since the ramification structure of $K\mathbb{Q}_p/\mathbb{Q}_p$ is the same as in $K/\mathbb{Q}$, the value of e_0' is a divisor of $p-1$, and $e_0' = p-1$ since for any ramified prime divisor $\mathfrak{p}$ of a ramified prime p the principal congruence subgroup $G(\mathfrak{p}) = \{g \in G, g \equiv I_n (mod \mathfrak{p})\}$ is not trivial provided the operation of Γ on G is not trivial.

As earlier in the proof of theorem 6, we see that adjoining a p-th root of unity ζ_p to K and extending the Galois operation to this larger field does not influence the validity of condition that e_0' is equal to $p-1$. So we can and do assume $\zeta_p \in K$ without loss of generality. After adjoining ζ_p to K we can suppose, that $e_0' = p-1$. As it follows from proposition 1 and its corollaries in 3.2, we can assume that G is $GL_n(\mathbb{Q})$-irreducible and that G is a counterexample to the Main Theorem with minimal order. Therefore, let $G \subset GL_n(\mathcal{O}_K)$ be a minimal counterexample such that the degree $[\mathbb{Q}(G)\mathbb{Q}^{ab} : \mathbb{Q}^{ab}]$ is minimal and, in particular, the extension $\mathbb{Q}(G)/\mathbb{Q}$ is not abelian.

Like in the proof of theorem 6, we have to distinguish two cases:

case a): $\Gamma_1(\mathfrak{p})$ is trivial, i.e. K is tamely ramified over $\mathbb{Q}$.

and

case b): $\Gamma_1(\mathfrak{p})$ is not trivial, i.e. K is wildly ramified over $\mathbb{Q}$.

We start with case a), since we can use an argument of the proof of case I of theorem 6.

First, let us assume that $p \neq 3$. We will consider the case $p = 3$ separately below. We have the following conditions:

$$\left(\left[\frac{e_0'}{2}\right] + 1\right)(p-1) > e_0',$$

and: $\mathfrak{p}^{[t/2]+1}$ does not divide $(\zeta_p - 1)$ for $t = e_0' = p - 1$.

In the case if the group generated by all $g^\gamma, \gamma \in \Gamma$ for a $g \in G$ is not cyclic, we can apply the argument of the proof of case I of theorem 6, which implies that the conditions of proposition 1 are not satisfied for the group generated by all $g^\gamma, \gamma \in \Gamma$, and so $G \not\subset \mathrm{GL}_n(\mathcal{O}_K)$.

Therefore, G should be cyclic, and $g^\gamma = g^a$ for all $g \in G$ and any $\gamma \in \Gamma_0(\mathfrak{p})$. Moreover, a is the same for all g. Indeed, if $g^\gamma = g^a$ and ${g_1}^\gamma = {g_1}^b$, with $a \neq b$, then the elements $(gg_1)^\gamma$, $\gamma \in \Gamma$ would generate a noncyclic group. So we have $g^{\gamma\sigma} = g^{\sigma\gamma}$ for any $\gamma \in \Gamma_0, \sigma \in \Gamma$. This implies $g^\gamma = g^{\sigma\gamma\sigma^{-1}}$. If G is generated by all $g^\gamma, \gamma \in \Gamma$, this implies the coincidence of all inertia groups Γ_0. Since $\Gamma_0 = \Gamma$ is cyclic, it follows that $\mathbb{Q}(G)$ must coincide with $\mathbb{Q}(\zeta_p)$. Indeed, for any $g \in G$ the matrix $h = g^{-1}g^\gamma \equiv I_n (mod \mathfrak{p})$ (here γ is a generator of Γ_0), so by lemma 2A (see sect. 3, 3.4) is conjugate over $\mathbb{Z}_{(p)}$, the valuation ring of p, to a diagonal matrix d with p-roots of unity as diagonal elements. Therefore, $C^{-1}hC = d$ for an invertible matrix C with entries in $\mathbb{Z}_{(p)}$, and $\mathbb{Q}(G) = \mathbb{Q}(C^{-1}GC)$. If $C^{-1}hC = g' = [g_{ij}] \in C^{-1}GC$, then $g_{ij}^\gamma = g_{ij}\zeta_{(ij)}$ for some p-roots of unity $\zeta_{(ij)}$. Since $\mathbb{Q}(g_{11}, g_{12}, \ldots, g_{nn})$ adjoined by all entries of g' is a Kummer cyclic extension of $\mathbb{Q}$ containing ζ_p, this field should coincide with $\mathbb{Q}(\zeta_p)$, and this is true for any $g' \in C^{-1}GC$. This argument implies that $\mathbb{Q}(G) = \mathbb{Q}(C^{-1}GC) = \mathbb{Q}(\zeta_p)$.

The case $p = 3$ should be considered separately. We can use discriminant estimates for the field $K = \mathbb{Q}(G)$. It follows from corollary 1 of theorem 2.11 in [N], p. 69, and proposition 4.9 in [N], p. 159, that there are no finite unramified extensions of the field $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ having degree $d > 1$ over $\mathbb{Q}(\sqrt{-3})$. This implies that $K = \mathbb{Q}(\sqrt{-3})$, and this field is abelian. This contradicts our assumption concerning the minimal counterexample G.

Now we consider case b) and assume that K is wildly ramified. We assumed $\zeta_p \in K$. Since $\mathbb{Q}(\zeta_p)$ is a tame extension of $\mathbb{Q}$, Γ_1 operates trivially on the p-th roots of unity ζ_p, hence K^{Γ_1} contains also ζ_p. Take now in lemma 2A $L = K^{\Gamma_0}$, then this field is unramified over $\mathbb{Q}$ for the prime divisor $\mathfrak{p}$ of p. Lemma 2A shows: up to conjugation in $GL_n(\mathcal{O}_\mathfrak{p} \cap K^{\Gamma_0})$, where $\mathcal{O}_\mathfrak{p}$ is the valuation ring of of $K^{\Gamma_0}(\zeta_p)$ at $\mathfrak{p}$, the group $G_0(\mathfrak{p}) = \{g \in G_0, g \equiv I_n (mod \mathfrak{p})\}$ consists of diagonal matrices. The group $G(\mathfrak{p}) := \{g \in G, g \equiv I_n (mod \mathfrak{p})\}$ is a nontrivial p-group and therefore $G_0(\mathfrak{p}) \neq \{I_n\}$ is not trivial as the subgroup of Γ_1-fixed elements of a nontrivial p-group. G is abelian and therefore in the centralizer of every matrix $h \in G_0(\mathfrak{p})$. If, in particular, $h = diag(l_1 I_{n_1}, \ldots, l_k I_{n_k})$, then $g = diag(g_1, \ldots, g_k), g_i \in GL_{n_i}(K)$ holds for every $g \in G$, and therefore we can split G into $GL_n(\mathcal{O}_\mathfrak{p} \cap K^{\Gamma_0})$-irreducible components. In this decomposition we

choose an irreducible component $G' \subset GL_m(K)$ of G with a suitable natural number m such that G' has nontrivial Γ_1-action. Moreover, the described decomposition is stable under the operation of Γ_0 (see lemma 2A in sect. 3, 3.4), in particular Γ_0 operates on the group G'.

If G'_0 denotes the subgroup of Γ_1-fixed elements of G', then the group

$$G'_0(\mathfrak{p}) := \{g \in G'_0, g \equiv I_m(mod\mathfrak{p})\}$$

consists of scalar matrices. The conditions on the ramification $e'_0 = p-1$ are also satisfied for G' and G'_0 instead of G and G_0. But now the group $G'_0(\mathfrak{p})$ is equal to the group $\mu := \{\zeta I_m, \zeta^p = 1\}$ containing only scalar matrices.

Note that in the case of global field $K/\mathbb{Q}$ and a Galois stable subgroup $G \subset GL_n(\mathcal{O}_K)$ the same groups $G_0(\mathfrak{p})$ and $G'_0(\mathfrak{p})$ are conjugate to groups of scalar matrices, but according to lemma 2A, the conjugation is performed in $GL_n(\mathcal{O}_\mathfrak{p} \cap K^{\Gamma_0})$, where $\mathcal{O}_\mathfrak{p}$ is the valuation ring of of $K^{\Gamma_0}(\zeta_p)$ at $\mathfrak{p}$.

Now we need to use the Galois equivariant homomorphism

$\psi = \psi_m : G' \to GL_{m^p}(K)$ given by $\psi(g) = g^{\otimes^p}$, which was defined earlier. The kernel of ψ is the set of all scalar matrices contained in G'. This kernel is not trivial, since $G'_0(\mathfrak{p}) \subset Ker\psi$, and there is an exact sequence
$1 \longrightarrow \mu \longrightarrow G' \longrightarrow \psi(G') \longrightarrow 1$ of Γ_0-invariant groups.

Now we can use lemma 3 proven in sect. 3 above for the construction of a subgroup $G'_1 \subset G' \subset GL_m(K)$ such that: $K^{\Gamma_1}(G'_1)$ is an extension of K^{Γ_1} with $\zeta_p \in K^{\Gamma_1}(G'_1)$, tame ramification index $e'_0 = p-1$ and $K^{\Gamma_1}(G'_1)/K^{\Gamma_1}$ is an elementary abelian Kummer extension.

Finally, a careful study of the Galois action of Γ_0 on G'_1 shows that the constructed group G'_1 can not exist if $\mathbb{Q}(G'_1) \neq \mathbb{Q}$ and $\mathbb{Q}(G'_1)/\mathbb{Q}$ is not abelian. For proving this we can apply R*ésumé* formulated in the end of sect. 3.

□

6. THE CASE OF RELATIVE EXTENSIONS OF NUMBER FIELDS

It is known that if E/F has unramified subextensions E_1/F, $E_1 \subset E$, then there exist examples of Galois stable finite groups $G \subset GL_n(\mathcal{O}_E)$ (see [M3] for an explicit construction). This is completely different from the situation where $F = \mathbb{Q}$ and there are no unramified extensions of the ground field $\mathbb{Q}$. We can consider the role of the group of units of the ring of integers $\mathcal{O}_E$ for the existence of finite $Gal(E/F)$-stable subgroups $G \subset GL_n(\mathcal{O}_E)$.

It is also difficult to transfer the idea of reduction to the case of abelian Galois stable groups G of composite order.

Example 3. It is difficult to transfer the idea of reduction to abelian Galois stable groups G of composite order. For $p \neq 2$ the simplest example can be

constructed as follows: Let

$$g_2 := \begin{vmatrix} 0 & \sqrt[p]{u} \\ (\sqrt[p]{u})^{-1} & 0 \end{vmatrix}$$

and $g := diag(g_2, I_{p-2}) \in GL_p(\mathcal{O}_K)$. Then $g^\gamma, \gamma \in \Gamma$ and $\zeta_p I_p$ generate a finite Γ-stable nonabelian subgroup of $GL_p(\mathcal{O}_K)$ of order divisible by 2 and p.

Example 4. Let

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

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

Example 5. The difficulties to extend the result of the Main Theorem to the case of relative extensions over a ground field F ramified over $\mathbb{Q}$ can be illustrated using the following construction:

If there exist an intermediate extension $L = F(\sqrt[p]{u}) \subset E$ for some unit $u \in \mathcal{O}_E$, we can put

$$g = \begin{vmatrix} 0 & \sqrt[p]{u} & 0 \dots & 0 \\ 0 & 0 & \sqrt[p]{u} \dots & 0 \\ \vdots & \ddots & \ddots & \\ 0 & \dots & 0 & \sqrt[p]{u} \\ \sqrt[p]{u}^{1-p} & \dots & 0 & 0 \end{vmatrix}$$

Then $g^\gamma, \gamma \in \Gamma$ and $\zeta_p I_p$ generate a finite Γ-stable subgroup of $GL_p(\mathcal{O}_E)$.

Hence for relative extensions $E/F, L \neq F$ and some units u it may happen that neither $F(\zeta_p, \sqrt[p]{u}) \subset FE_{ab}$ nor $F(\sqrt[p]{u})/F$ is unramified, when $L = F(\zeta_p)$.

However, some progress is still possible to give a positive answer for relative extensions of number fields that satisfy the following

Assumption. *Consider relative extensions K/F which are of the form $K = TF$. Here we assume: T is a finite Galois over $\mathbb{Q}$ and unramified outside the rational primes $p_1, p_2, ...p_k$, and $F/\mathbb{Q}$ is a number field unramified in $p_1, p_2, ..., p_k$. So we suppose that $(d(F/\mathbb{Q}), p_i) = 1$ for all indices i and the discriminant $d(F/\mathbb{Q})$ of $F/\mathbb{Q}$. We consider finite subgroups G of $GL_n(\mathcal{O}_K)$ that are stable under the natural operation of the Galois group $Gal(K/F)$.*

It is possible to reduce our considerations to the case of the only one prime $p_1 = p$.

Theorem 8. *Let F be a number field of discriminant $d(F)$ not divisible by an odd prime p and let T be a finite Galois extension of $\mathbb{Q}$ of discriminant coprime to $d(F)$. Set $K = TF$. If G is a finite $Gal(K/F)$-stable p-subgroup of $GL_n(\mathcal{O}_K)$ then $G \subset GL_n(FT_{ab})$ where T_{ab} is the maximal abelian subextension*

of $T/\mathbb{Q}$ (or equivalently, the commutator subgroup of $Gal(K/F)$ acts trivially on G).

The proof of theorem 8 is given in [BM2].

Remark. *Under the assumptions of theorem 8 for K and F there do not exist unramified intermediate extensions between K and F .*

7. RARITY OF Γ-STABLE REPRESENTATIONS

Let $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{d})$ and d is a negative rational integer. We consider the set $O(N) = \{\alpha \in \mathcal{O}_K \big| \, |N_{K/\mathbb{Q}}(\alpha)| \leqslant N\}$ where $N_{K/\mathbb{Q}}$ is the norm map. The proof of the following theorem (see [M4], theorem 4) is based on the result by S. D. Cohen (see 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 $\mathcal{O}_K$). Here estimates of the error term are added.

Theorem 9. *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*

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

The error term can be estimated in the case $K = \mathbb{Q}$ as $v(N) - \psi(N) = o(N^{m+0.5}(lnN)^2)$.

Theorem 3 shows that "almost all" fields are not realizable via adjoining matrix coefficients of of all matrices $g \in G$ for Γ-stable groups G to K, the field of rational numbers or its imaginary quadratic extensions, if these coefficients are contained in the rings of integers of algebraic number fields.

Remark that we can also consider other number fields, but it will be necessary to rearrange the definition of $\mathcal{O}(N)$, compare [C]. Note that proof below, specially in the case 1), can produce explicit estimates, and we can also use the estimates in [K1], [K2], [Gal].

Proof of theorem 9. We use properties of distribution of Galois groups of polynomials that were considered by S. D. Cohen [C], for the case $K = \mathbb{Q}$ see also [VW]. According to [C] the number of polynomials in question having the symmetric Galois group S_m, divided by the total number of polynomials in question, approaches 1 when $N \to \infty$. Therefore, we can consider only the number of these K-irreducible polynomials that 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 $K(G)$ that have no ramified primes $p \geqslant m! + 1$ (since p must divide the order of $\Gamma = S_n$) and have degree $m!$ over K. Let us estimate the

number of these polynomials. However, if $K = \mathbb{Q}$, the situation is simplier, and we have to check only 2 possible extensions of $\mathbb{Q}$: the fields $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{-3}]$.

1) Let us consider the case $K = \mathbb{Q}$.

Note that in the virtue of the above result on the symmetric Galois group S_m our Main Theorem (see also theorem 2 in [M2]) which implies that only for fields $\mathbb{Q}(G)$ containing nontrivial roots of 1 it may happen that $\mathbb{Q}(G) \neq \mathbb{Q}$, we have to eliminate a possibility that $\mathbb{Q}(G)$ has nontrivial roots of 1 and simultaneously the Galois group of $Gal(\mathbb{Q}(G)/\mathbb{Q})$ is S_m. The latter is possible only if one of the primitive roots $\zeta_4 = i$ or $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ is in $K\mathbb{Q}(G)$.

Let us start from the case $i \in \mathbb{Q}(G)$. Let $k, l, k + l = m$ be positive integers such that an integral polynomial $A(x)$ satisfies the conditions of theorem 9, $A(x) = a(x)b(x)$ with $a(x) = \sum_{i=0}^{k} a_i x^i, a_i \in \mathbb{Z}[i]$, and $b(x) = \sum_{j=0}^{l} b_j x^j, b_j \in \mathbb{Z}[i]$, and $a_0 \neq 0, a_k \neq 0, b_0 \neq 0, b_l \neq 0$. Since the number of possible polynomials $A(x)$ with either the first or the last coefficient equal 0 is $\sim N^m$ while the total number of polynomials in $\mathcal{O}(N)[x]$ is $\sim N^{m+1}$, so the polynomials $A(x)$ with either the first or the last coefficient equal 0 do not give any contribution asymptotically. Let us show that the number of the sets of coefficients $(a_0, a_1, \dots, a_k, b_0, b_1, \dots, b_l)$ admissible for polynomials $a(x), b(x)$ also do not contribute anything asymptotically. The ring $\mathbb{Z}[i]$ is euclidean, and $\pm 1, \pm i$ are the only invertible elements in $\mathbb{Z}[i]$, also for any integer D $|ab| \leqslant |D|$ imply $|b| \leqslant |D|$ or $|a| \leqslant |D|$. This implies $|a_i| \leqslant C(m)N$ and $|b_j| \leqslant C(m)N$ where $C = C(m)$ depends only on m. Also we have $1 \leqslant |a_0 b_0| \leqslant N$ and $1 \leqslant |a_k b_l| \leqslant N$. Let us estimate the number $L(N)$ of pairs of Gaussian integers $a, b \in \mathbb{Z}[i]$ such that $1 \leqslant |ab| \leqslant N$. We can write $a = a_1' + a_2' i = c_1(\alpha_1 + \alpha_2 i)$ where c_1, α_1, α_2 are rational integers, α_1, α_2 are coprime, so c_1 is the greatest common divisor $c_1 = (\alpha_1, \alpha_2)$of α_1, α_2. Also, let $b = b_1' + b_2' i = c_2(\beta_1 + \beta_2 i)$ where c_2, β_1, β_2 are rational integers, and $c_2 = (\beta_1, \beta_2)$. It is known (see [D], ch. 4, sect. 68 or [Cas], ch. 9, sect. 6 and appendix B) that the number $F(t)$ of primitive representations of a positive integer t as a sum of 2 squares does not exceed $c_f 2^s$ where c_f is a constant depending only on the form $f(x_1, x_2) = x_1^2 + x_2^2$, the sum of 2 squares, $c_f = 4$ in our case, and s is the number of distinct prime divisors of t. Denote by $M(j)$ the number of all pairs of integers c_1, c_2 such that $|c_1 c_2| \leqslant j$ (note that both c_1 and c_2 can be positive or negative). Then (see e.g. [HW], p.264) $M(j) \sim 4([j/1]+[j/2]+\dots+[j/k]+\dots) = 4(j \cdot lnj + O(j))$, where $[x]$ denotes the greatest integer $\leqslant x$. Note that we can always write $F(t) \leqslant c_f t$. Let us estimate the number $L(N)$ of integers a, b introduced above. We can use that also $F(t) = c_f 2^s = o(t)$, and also $F(t) = c_f 2^s = o(t^{1/4})$ for $t \geqslant N^{1/4}$ (see e.g. [HW], 18.7, p.270).

$$L(N) = \sum_{t=1}^{N} M(N/t)F(t) = o(\sum_{t=1}^{N^{\frac{1}{4}}} (N/t \cdot ln(N/t))t) + o(\sum_{t=N^{\frac{1}{4}}}^{N} (N/t \cdot ln(N/t))t^{\frac{1}{4}}) =$$

$$o(\int_1^{N^{\frac{1}{4}}} N \cdot ln(N/x)dx) + o(\int_{N^{\frac{1}{4}}}^{N} N \cdot ln(N/x)dx^{\frac{1}{4}}) = o(N^{\frac{5}{4}} lnN)$$

So the number of possible systems of (a_0, a_k, b_0, b_l) involving 2 couples (a_0, b_0) and (a_k, b_l) of coefficients is $o(N^{2.5}(lnN)^2)$. This estimate may be improved but this is not essential for our theorem. Finally, the number of polynomials $A(x)$ that are reducible in $\mathbb{Z}[i][x]$ is $o(N^{k-1}N^{l-1}N^{2.5}(lnN)^2) = o(N^{m+0.5}(lnN)^2) = o(N^{m+1})$, and we can combine this estimate with the estimate in [C] (see also [Gal]), which implies that the number of polynomials $A(x) = \sum_{i=0}^{m} p_i x^i \in \mathcal{O}(N)[x]$ whose Galois group is not symmetric is $O(N^{m+0.5}lnN)$. So our claim is true for polynomials in $\mathbb{Z}[i][x]$.

In a similar way we can consider the polynomials $A(x) \in \mathbb{Z}[\zeta_3][x]$. The number of these polynomials can be estimated using the quadratic form $f(x_1, x_2) = x_1^2 - x_1x_2 + x_2^2$ corresponding to multiplication in the ring $\mathbb{Z}[\zeta_3]$, which is equivalent to the form $f(y_1, y_2) = y_1^2 + y_1y_2 + y_2^2$, where $x_1 = y_1 + y_2, x_2 = y_2$. The constant c_f for this form is $c_f = 6$ (see [D], ch. 4, sect. 70 or [Cas], ch. 9, sect. 6 and appendix B), and our argument can be used without changes in the case of the ring $\mathbb{Z}[\zeta_3]$ instead of $\mathbb{Z}[i]$.

2)Let us consider the case $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $d \in \mathbb{Z}$.

Let$f \in \mathcal{O}(N)[x]$ and $f = g \cdot g'$, $g, g' \in K(\sqrt{\alpha})[x]$, $\sqrt{\alpha} \notin K$. Let $\mathcal{E} \in \mathcal{O}_{K(\sqrt{\alpha})}$ be a unit of infinite order. We can suppose that after some adjustment both the height $|g| = \max|a_i|$ of $g = \sum a_i x^i$ and the 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

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

Note that the number of polynomials $f \in \mathcal{O}(N)[x]$ that are reducible already in $\mathcal{O}(N)[x]$ do not give any contribution asymptotically. Moreover, according to the result in [C], the number of polynomials in $O(N)[x]$ whose Galois group is not symmetric do not contribute asymptotically as well. So, we have shown that the number of polynomials whose splitting fields can contain any $K(G) \neq K$ is small asymptotically, and this completes the proof of theorem 9.

□

8. GALOIS STABLE GROUPS OVER FIELDS OF CHARACTERISTIC $p > 0$

In the case of fields of positive characteristic we have

Theorem 10. *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 $\mathcal{O}_E$ then $G \in GL_n(\mathcal{O}_E)$.*

Proof of theorem 10.

Let

$$g_t := \begin{vmatrix} 1 & t & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ \dots & \dots & \dots & \ddots & \\ 0 & 0 & \dots & \dots & 1 \end{vmatrix}.$$

Then $g_t^p = I_n$, the identity $n \times n$-matrix, and for any automorphism σ of E

$$g_t^\sigma = \begin{vmatrix} 1 & t^\sigma & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ \dots & \dots & \dots & \ddots & \\ 0 & 0 & \dots & \dots & 1 \end{vmatrix}.$$

We have $(g_t^\sigma)^p = I_n$, and the product of any 2 matrices g_t^σ for any automorphisms σ of E is still a $n \times n$ unitriangular matrix of order p. Therefore, a group G generated by all matrices g_t^σ is a finite abelian group of exponent p with nontrivial Galois operation of Γ such that $E = F(G) \neq F$ provided $t \notin F$. □

The reason for this constructive realizability of the above field E of characteristic p is that elements in G are not semisimple, the situation is completely different for fields E, F of characteristic 0, and even for extensions E/F of fields of characteristic $p > 0$, provided the order of G is not divisible by p.

9. SOME REMARKS ON THE ORDERS OF FINITE ARITHMETIC GROUPS

As it has been already mentioned in the introduction, one of the applications of the Main Theorem of this paper is the computation of orders of finite arithmetic groups in $GL_n(K)$. If K is a totally real algebraic number field and $f(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$ is a positive definite quadratic form, the order of the finite orthogonal group $O_f(\mathcal{O}_K) \subset \mathrm{GL}_n(\mathcal{O}_K)$ of this form over $\mathcal{O}_K$ does not depend on the field K and can be estimated using the Minkowski

formulas for finite integral groups of matrices obtained using reduction modulo primes p and the fact that there is no torsion in the kernel of this reduction for odd p ([So], sect. 6.3 and [Min2]) since $O_f(\mathcal{O}_K) = O_f(\mathbb{Z})$. The order of $O_f(\mathbb{Z})$ is bounded by the number $s(q,n) = \Pi q^{r(q,n)}$, where the product is taken for all primes $q = 2, 3, 5, 7, ...$, and

$$r(q,n) = \Sigma_{i=1}^{\infty}[\frac{n}{q^i(q-1)}].$$

Remark that any finite subgroup $G \subset GL_n(\mathcal{O}_K)$ is a subgroup of $O_q(\mathcal{O}_K)$ for some quadratic form $q(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$.

There are some generalizations of this result of Minkowski using both algebraic (see e. g. [Fe]) and analytic (see e. g. [LN]) methods.

It is possible to generalize the above formula for finite subgroups of $\mathrm{GL}_n(\mathcal{O}_K)$ for some cyclotomic fields K using lemmas 2 and 2A (p.16, 17, see also 3.3, p.14) for $K = \mathbb{Q}(\zeta_p)$ and $K = \mathbb{Q}_p(\zeta_p)$ since the ramification indices of these fields are $p-1$. However, the kernel of reduction of $\mathrm{GL}_n(O_K)$ modulo prime divisor of p may contain a p-group of any prescribed nilpotency class for extensions $K/\mathbb{Q}$ with large ramification.

Indeed, let us consider the following p-group of nilpotency class l, determined by generators $a, b_1, ..., b_l$ and relations $b_i^p = 1, b_ib_j = b_jb_i, i = 1, 2, ..., l; ab_1 = b_1a, b_{i-1} = b_iab_i^{-1}a^{-1}, i = 1, 2, ..., l; a^n = 1$, where $n = p^t \geq l > p^{t-1}$ and t is a suitable integer. Let H be the abelian subgroup of G generated by $b_1, ..., b_l$, and let χ denote the character of H given on the generators as follows: $\chi(b_1) = \zeta_p$–a primitive p-root of 1, $\chi(b_i) = 1, i = 2, ..., l$. The character χ together with the decomposition of G into cosets with respect to H: $G = 1.H + a.H + ... + a^{n-1}.H$ gives rise to an induced representation $R = Ind\chi_H^G$ of G. For the $n \times n$-matrices e_{ij} having precisely one nonzero entry in the position (i,j) equal to 1 we can define a $n \times n$-matrix using the binomial coefficients $\begin{pmatrix} n-j \\ i-j \end{pmatrix}$:

$$C = \Sigma_{n \geq i \geq j \geq 1}(-1)^{i-j} \begin{pmatrix} n-j \\ i-j \end{pmatrix} e_{ij}.$$

Theorem 11. *Let $\mathbb{Q}_p(\zeta_{p^\infty})$ denotes the extension of $\mathbb{Q}_p$ obtained by adjoining all roots $\zeta_{p^i}, i = 1, 2, 3, ...$ of p-primary orders of 1, let π be the uniformizing element of a finite extension $K/\mathbb{Q}_p$ such that $K \subset \mathbb{Q}_p(\zeta_{p^\infty})$, and let $D = diag(1, \pi, \pi^2, ..., \pi^{n-1})$. Then the representation $R_\pi = D^{-1}C^{-1}RCD$ of G is a faithful, absolute irreducible representation in $\mathrm{GL}_n(\mathcal{O}_K)$ by matrices congruent to $I_n(mod\pi)$. Moreover, such representations are pairwise nonequivalent over $\mathcal{O}_{\mathbb{Q}_p(\zeta_{p^\infty})}$, and for the lower central series $G = G_l \supset G_{l-1} \supset ... \supset G_0 = \{I_n\}$ of G all elements of $R_\pi(G_{l-i+1})$ are congruent to $I_n(mod\pi^{iw})$ if the elements of $R_\pi(G)$ are congruent to $I_n(mod\pi^w)$.*

For the proof of theorem 11 (which is constructive) see [M7], see also [M8]. Remark that the construction of theorem 11 can be realized also over the integers of cyclotomic subextensions $K \subset \mathbb{Q}(\zeta_{p^\infty})$ of $\mathbb{Q}$ and other global fields.

The following proposition is used in the proof of the following propositions (see [M8], lemma 1):

Proposition 4. *Let L be an ideal in a Dedekind ring S of characteristic 0, let $\{0\} \neq L \neq S$, and let g be some $n \times n$-matrix of finite order congruent to $I_n(modL)$. Then L contains a prime p and $g^{p^j} = I_n$ for some integer $j \geqslant 0$. In particular, a finite group of matrices congruent to $I_n(modL)$ is a p-group. Let $L = \mathfrak{p}$ be a prime ideal containing p having the ramification index e with respect to p, let $g \equiv I_n(mod\mathfrak{p}^r)$, and let*

$$\lambda p^{i-1}(p-1) \leqslant \frac{e}{r} < p^i(p-1), i \geqslant 0, \lambda = min\{1, i\}.$$

Then $g^{p^i} = I_n$, in particular, any finite group of matrices congruent to $I_n(mod\mathfrak{p}^t)$ is trivial if $e < t(p-1)$.

Remind that for a primitive t-root ζ_t of 1 $\phi_K(t)d = [K(\zeta_t) : K]$ denotes the generalized Euler function. The following propositions allow to estimate the order of Sylow q-subgroups of $GL_n(\mathcal{O}_K/\mathfrak{p})$, the reduction is considered modulo some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.

The proof of the following propositions is technical; it is based on the reduction modulo some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that its norm C is a prime integer and the kernel of the reduction of $\mathrm{GL}_n(\mathcal{O}_K)$ $(mod\mathfrak{p})$ has no q-torsion for a given prime $q \neq 2$ and the multiplicative order of $N_{K/\mathbb{Q}}(\mathfrak{p})(modq^t)$ is $\phi_K(q^t)$, there is an infinite number of ideals like this (which can be shown using the Chebotarev's density theorem). Note that, according to proposition 4, for any $g \equiv I_n(mod\mathfrak{J}), g \in GL_n(O_K)$ the ideal $\mathfrak{J}$ of O_K should divide some prime p. It is easy to show (see [M9], remark 2), that $N_{K/\mathbb{Q}}(\mathfrak{J}) \leqslant p^{\frac{d}{p-1}}$ for $d = [K : \mathbb{Q}]$. This implies that the reduction $(mod\mathfrak{J})$ is trivial if $N_{K/\mathbb{Q}}(\mathfrak{J}) > p^{\frac{d}{p-1}}$, moreover, if $N_{K/\mathbb{Q}}(\mathfrak{J}) > 2^d$. For $q = 2$ the same result is true if $\sqrt{-1} \in K$ since $2^d \geqslant p^{\frac{d}{p-1}}$. It is possible to determine the structure of a p-subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$ having the maximal possible order with some modifications in the case $p = 2$. The theorems describing the maximal p-subgroups of $\mathrm{GL}_n(K)$ over fields can be found in [LP], in particular, it is proven that there is only one conjugacy class of maximal p-subgroups of $\mathrm{GL}_n(K)$ for $p > 2$. Howewer, equivalence of subgroups in $\mathrm{GL}_n(\mathcal{O}_K)$ over $\mathcal{O}_K$ is a more subtle question.

Proposition 5. *Let q be an odd prime. There is a prime ideal $\mathfrak{p} \in \mathcal{O}_K$ with the norm $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ – a prime integer – such that the order of a Sylow q-subgroup of $GL_n(\mathcal{O}_K/\mathfrak{p})$ is bounded by the number $S_K(q, n) = q^{R_K(q,n)}$, for any matrix $g \in \mathrm{GL}_n(\mathcal{O}_K)$ of order q the condition $g \equiv I_n(mod\mathfrak{p})$ implies $g = I_n$ and*

$$R_K(q, n) = \Sigma_{i=1}^{\infty}[\frac{n}{\phi_K(q^i)}].$$

Let us consider an integer $h = [\frac{n}{\phi_K(q)}]$ and a wreath product $H = M\ wr\ S_n$ of the symmetric group S_h and the matrix group $M = diag(g_1, g_2, ..., g_h, I_k)$ for $k = n - h\phi_K(q)$ and $g_i \in C_{q^j}$ for a cyclic group $C_{q^j} \subset \mathrm{GL}_{\phi_K(q)}(\mathcal{O}_K)$ with the operation of S_n (which can be identified to a subgroup P_h of block-permutation matrices $P \in \mathrm{GL}_n(\mathcal{O}_K)$) on M determined by permutations of diagonal blocks

g_1: $P \cdot diag(g_1, g_2, ..., g_h, I_k) = diag(g_{P(1)}, g_{P(2)}, ..., g_{P(h)}, I_k), P \in P_h$. H is naturally isomorphic to the group consisting of matrices $mp \in \mathrm{GL}_n(\mathcal{O}_K)$ for $m \in M$ and $p \in P_h$. Set $H = I_n$ in the case $n < \phi_K(q)$.

Proposition 6. *For a prime q let m be the maximal integer with the property $\phi_K(q^m) = \phi_K(q)$.*

1)For an odd prime q there is a q-subgroup of $H = M$ wr S'_h, where $M = diag(g_1, g_2, ..., g_h, I_k), g_i \in C_{q^m}$, C_{q^m} is a cyclic subgroup of order q^m in $\mathrm{GL}_{\phi_K(q^m)}(\mathcal{O}_K)$ and S'_h is a Sylow q-subgroup of S'_h, and the order $|H|$ of the q-subgroup H is equal to

$$S_K(q, n) = q^{\Sigma_{i=1}^{\infty}[\frac{n}{\phi_K(q^i)}]}.$$

There are no q-subgroups in $\mathrm{GL}_n(\mathcal{O}_K)$ of order greater than $|H|$.

2) For $q = 2$ let $L = K(\sqrt{-1})$. There is a 2-subgroup of $H = M$ wr S'_h, where $M = diag(g_1, g_2, ..., g_h, I_k), g_i \in C_{2^m}$, C_{q^m} is a cyclic subgroup of order q^m in $\mathrm{GL}_{\phi_L(q^m)}(\mathcal{O}_L)$ and S'_h is a Sylow q-subgroup of S'_h, and the order $|H|$ of the group H is equal to

$$S_L(2, n) = 2^{\Sigma_{i=1}^{\infty}[\frac{n}{\phi_L(q^i)}]}.$$

There are no 2-subgroups in $\mathrm{GL}_n(\mathcal{O}_L)$ (and therefore in $\mathrm{GL}_n(\mathcal{O}_K)$) of order greater than $|H|$.

Note that $|H| = 1$ if $n < \phi_K(q)$.

The order of any finite subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$ can be bounded by the constant

$$T_K(q, n) = \Pi q^{\Sigma_{i=1}^{\infty}[\frac{n}{\phi_K(q^i)}]},$$

where the product is taken for all primes $q = 2, 3, 5, 7, ...$ This is a generalization of the above result by H. Minkowski [Min2].

References

[A] M. Asada, *On unramified Galois extensions over maximum abelian extensions of algebraic number fields*, Mathematische Annalen **270, 4** (1985), 477-487.

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

[BM1] H.-J. Bartels, D. A. Malinin, *Finite Galois stable subgroups of GL_n*, Lecture Notes In Pure And Applied Mathematics **243** (2006), In: Noncommutative Algebra and Geometry, Edited by C. de Concini, F. van Oystaeyen, N. Vavilov and A. Yakovlev, 1–22.

[BM2] H.-J. Bartels, D. A. Malinin, *Finite Galois stable subgroups of GL_n in some relative extensions of number fields*, Journal of Algebra and Its Applications **8** (2009), 493–503.

[BM3] H.-J. Bartels, D. A. Malinin, *Finite Galois stable subgroups of GL_n over local fields*, in preparation.

[Bo] A. Borel, *Introduction aux groupes arithmtiques*, Hermann, 1969.

[Cas] Cassels J. W. S., *Rational quadratic forms. London Mathematical Society Monographs, 13.*, Academic Press, London–New York, 1978..

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

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

[D] P. G. Lejeune Dirichlet, *Vorlesungen ueber Zahlentheorie. (German) Herausgegeben und mit Zusaetzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage*, Chelsea Publishing Co., New York, 1968.

[Fe] W. Feit, *Finite linear groups and theorems of Minkowski and Schur*, Proc. Amer. Math. Soc. **125** (1997), 1259-1262.

[F] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur $\mathbb{Z}$*, Invent. math. **81** (1985), 515–538.

[Gal] P. X. Gallagher, *The large sieve and probabilistic Galois theory. In: Proc. Symp. pure Math.* **XXIV** (1973), 91–101.

[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.

[HW] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers. The fourth edition.*, Oxford University Press, Oxford, 1975.

[K1] H. W. Knohloch, *Zum Hilbertschen Irreduzibilität*, Abh. Math. Sem. Hamburg **19** (1955), 176–190.

[K2] H. W. Knobloch, *Die Seltenheit der reduzibien Polynome*, Jber. Deutch. Math. Verein. **1** (1956), 12–19.

[LP] C. R. Leedham-Green, W. Plesken, *Some remarks on Sylow subgroups of general linear groups*, Math. Z. **191** (1986), 529-535.

[LN] G. Levitt, J.-L. Nicolas, *On the maximum order of torsion elements in $GL(n, Z)$ and $Aut(F_n)$*, J. Algebra **208** (1998), 630–642.

[M1] D. A. Malinin, *Integral representations of finite groups with Galois operation*, Dokl. Russ. Akad. Nauk **349** (1996), 303–305.

[M2] D. A. Malinin, *Galois stability for integral representations of finite groups*, Algebra i Analiz **12** (2000), 106–145 (Russian); English transl. in St.-Petersburg Math. J. **12**, N 3.

[M3] D. A. Malinin, *On the existence of finite Galois stable groups over integers in unramified extensions of number fields*, Publ. Mathem. Debrecen **60** (2002), N 1-2, 179–191.

[M4] D. A. Malinin, *Galois stability, integrality and realization fields for representations of finite Abelian groups*, Algebras and representation theory **6** (2003), N 2, 215–237.

[M5] D. A. Malinin, *Some integral representations of finite groups and their arithmetic applications, In: Algebraic Geometry and Its Applications* (2008), World Scientific, 467–480.

[M6] D. A. Malinin, *Finite arithmetic groups: a monograph*, Minsk, 2009.

[M7] D. A. Malinin, *Integral representations of p-groups of given nilpotency class over local fields*, Algebra i analiz **10** (1998), N 1, 58–67 (Russian); English transl. in St.-Petersburg Math. J. **10**, N 1, 45–52.

[M8] D. A. Malinin, *On integral representations of finite p-groups over local fields*, Dokl. Akad. Nauk USSR **309** (1989), 1060–1063 (Russian); English transl. in Sov. Math. Dokl. **40** (1990), N 3, 619–622.

[M9] D. A. Malinin, *On integral representations of finite nilpotent groups*, Vestnik Beloruss. State Univ. Ser. 1 (1993), N 1, 27–29.

[Min] H. Minkowski, *Über den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen*, J. reine angew. Math. **100** (1887), 449–458.

[Min2] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. Reine Angew. Math. **101,** (1887), N 3, 196–202.

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

[N] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers. Second edition*, Springer-Verlag, Berlin; PWN – Polish Scientific Publishers, Warsaw, 1990.

[S] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

[So] Christophe Soulé, *An introduction to arithmetic groups, in "Number theory, Physics and Geometry II", Eds.: P.Cartier, B.Julia, P. Moussa, P. Vanhove*, Springer, 2006, pp. 247-276.

[ST] D. A. Suprunenko, R. I. Tyshkevich, *Commutative Matrices*, Academic Press, New York and London, 1968.

[VW] B. L. Van der Waerden, *Die Seltenheit der reguziblen Gleichungen mit Affekt*, Math. Ann. (1934. B. 109, S. 13–16.).

[W] L. C. Washington, *Introduction to Cyclotomic Fields, second edition*, Springer, New York Berlin Heidelberg, 1997.

[We] A. Weiss, *Rigidity of p-adic p-torsion*, Annals of Math. **127** (1988), 317–322.