www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 2 No. 1 (2013), pp. 199-227.

www.ui.ac.ir

ON FINITE ARITHMETIC GROUPS

DMITRY MALININ

Communicated by Patrizia Longobardi

Abstract. Let F be a finite extension of $\mathbb{Q}$, $\mathbb{Q}_p$ or a global field of positive characteristic, and let E/F be a Galois extension. We study the realization fields of finite subgroups G of $GL_n(E)$ stable under the natural operation of the Galois group of E/F. Though for sufficiently large n and a fixed algebraic number field F every its finite extension E is realizable via adjoining to F the entries of all matrices $g \in G$ for some finite Galois stable subgroup G of $GL_n(\mathbb{C})$, there is only a finite number of possible realization field extensions of F if $G \subset GL_n(O_E)$ over the ring O_E of integers of E. After an exposition of earlier results we give their refinements for the realization fields E/F. We consider some applications to quadratic lattices, arithmetic algebraic geometry and Galois cohomology of related arithmetic groups.

1. Introduction

We consider realization fields for linear representations of certain groups. If for some finite subgroup $f : G \to GL_n(K)$ is a linear representation, we say that $K_1 \subset K$ is a realization field of $f(G)$ if $K_1 = F(f(G))$ for the fixed base field F (e.g., the field $\mathbb{Q}$ of the rational numbers), in other words, K_1 is obtained via adjoining all matrix entries of all $g \in f(G)$ to the field F. We are also interested in the extra condition of stability of $f(G)$ under the natural action of the absolute Galois group $Gal(\bar{F}/F)$ for an algebraic closure $\bar{F}$ of F. This paper contains a survey of related results including our research (jointly with H.-J. Bartels), gives some new results (Theorem 5, Theorem 6, Theorem 10 below) and refinements of known ones as well as a new proof of our result in [4] (the main theorem) based on our expository results, applications of Ihara's theorem and without using the classification of finite group schemes for $p \neq 2$. We give a probabilistic characterization of Galois stable groups (Theorem 9) with new error estimates. We also formulate some new conjectures and open questions.

MSC(2010): Primary: 20C10; Secondary: 20C05, 11R33.

Keywords: algebraic integers, Galois groups, integral representations, realization fields.

Received: 27 December 2012, Accepted: 31 May 2013.

The fundamental theorem of Brauer states that any irreducible representation of a finite group G can be realized in the field $E = \mathbb{Q}(G) = \mathbb{Q}(\zeta_t)$ for some primitive t-root ζ_t of 1, in other words, $C^{-1}GC \subset GL_n(\mathbb{Q}(\zeta_t))$ for some matrix C. Theorem of Brauer implies that an irreducible complex character of G can be realized by a representation defined over the cyclotomic field $\mathbb{Q}(\zeta_t)$. A natural question is: whether or not it is possible to realize G in $GL_n(\mathbb{Z}[\zeta_t])$ over the ring of integers $\mathbb{Z}[\zeta_t]$ of the cyclotomic field $\mathbb{Q}(\zeta_t)$. G. Cliff, J. Ritter and A. Weiss proved [11] that if G is solvable, then one can take the representation to be defined over the ring of integers $\mathbb{Z}[\zeta_t]$. More generally, they asked whether a character that can be realized over a number field can be realized over its ring of integers. This is the case for nilpotent groups of odd order by results of P. Roquette [41]. W. Knapp and P. Schmidt have extended the result of G. Cliff, J. Ritter and A. Weiss. They showed that it is possible to realize G in $GL_n(\mathbb{Z}[\zeta_t])$ over the ring of integers $\mathbb{Z}[\zeta_t]$ if this is true for quasisimple groups. However, this fails for the degree 2 irreducible representation of the quaternion group over the field $\mathbb{Q}(\sqrt{-35})$, and for a certain metacyclic group of order 171.

In this paper we consider a similar question for the realization fields of integral representations stable under the natural Galois action. An extra motivation of this kind of representations is coming from the results of J. Ritter and A. Weiss [39] and [40] where some applications are considered. Another motivation for considering the extra Galois stability condition is coming from classification of automorphism groups of certain curves of genus $g > 1$. G. Cardona [9] studies Galois stability for 2-dimensional representations of quaternion groups and applications to the classification of curves of genus 2 with automorphism group isomorphic to $\widetilde{S}_4$ (and some other automorphism groups).

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

Is it true that there exist a representation $h : G \to GL_n(K)$ over a number field K, normal over F, with Galois group $\Gamma = Gal(K/F)$, such that $h(G)$ is Γ-invariant and the groups $f(G)$ and $h(G)$ are conjugate?

In the case of nilpotent groups of odd order we again refer to the results of P. Roquette [41] to give an affirmative answer.

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 O_E and O_F the maximal orders of E and F, and let Γ be the Galois group of E/F. Let $E = F(G)$ be a field obtained via adjoining to F all matrix coefficients of all matrices $g \in G$ for some finite subgroup $G \subset GL_n(E)$. In some previous papers we considered the conditions of existence and non-triviality of Galois action on finite subgroups $G \subset GL_n(R)$, and the cases where R is a Dedekind domain or a field. The condition of integrality of G together with non-triviality of Galois action appears to be quite restrictive. In [27] it was proven that the existence of $G \subset GL_n(R)$ with nontrivial Galois action implies the existence of an abelian subgroup $G \subset GL_n(R)$ with nontrivial Galois action, so in a sense the existence problem can be reduced to the case of abelian Galois stable subgroups $G \subset GL_n(R)$.

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

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

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

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

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 $E/\mathbb{Q}$?*

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 [27], [28], [29], [31] 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 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 [29] 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 [4], [3], [31]).

Let K be a totally real algebraic number field with the maximal order O_K, G an algebraic subgroup of the general linear group $GL_n(\mathbb{C})$ defined over the field of rationals $\mathbb{Q}$. Since $G \subset GL_n(\mathbb{C})$, the intersection $G(O_K)$ of $GL_n(O_K)$ and $G(K)$, the subgroup of K-rational points of G, can be considered as the group of O_K-points of an affine group scheme over $\mathbb{Z}$, 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:

Let K be a totally real number field. Does the condition $G(O_K) = G(\mathbb{Z})$ always hold true?

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

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

There are several reformulations and generalizations of this theorem (earlier just a conjecture).

It is reasonable to consider arithmetic groups defined over algebraic number fields F and to study their subgroups of 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 [44]. 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 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 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 Section 3 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 [48], 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 $GL_n(O_K)$ acts in a natural way on $O_K \otimes M \cong \bigoplus_{i=1}^n O_K m_i$. The finite group $G \subset GL_n(O_K)$ is said to be of A-type, if there exists a decomposition $M = \bigoplus_{i=1}^k M_i$ such that for every $g \in G$ there exists a permutation $\Pi(g)$ of $\{1, 2, \ldots, k\}$ and roots of unity $\epsilon_i(g)$ such that $\epsilon_i(g) g M_i = M_{\Pi(g)i}$ for $1 \leq i \leq k$.*

The following theorem (conjectured earlier) generalizes (and would imply) Theorem A:

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

For totally real fields K Theorem B reduces to Theorem A.

Both Theorems A and B are true (see [4]) and have some extra applications to arithmetic geometry and Galois cohomology [3].

Theorem C (Generalized "Hasse principle").

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

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

is trivial.

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 $f(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$ is a positive definite quadratic form, it is possible to estimate the order of the finite orthogonal group $O_f(O_K) \subset GL_n(O_K)$ of this form over O_K using the formulas for finite integral

groups of matrices (see [44], sect. 6.3 and also [36]) since $O_f(O_K) = O_f(\mathbb{Z})$. 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 $q = 2, 3, 5, 7, \ldots$, and

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

The results of this paper can be reformulated in the terms of finite group schemes and can be applied to abelian varieties over number fields. It will be also reasonable to consider also the case of positive characteristic p (see also Section 9 below).

The results below imply the positive solution of the above conjectures (the Main Theorem in Section 3), the presented proof is shorter than one given in [4], and it allows to obtain also a result for Galois stable groups over local fields. The paper is organized as follows. The main results are formulated in Section 3. In Section 4 an integrality criterion and the finiteness theorem are proven and some auxiliary results are given for the needs of further sections. Section 5 is devoted to the proofs of a theorem describing the structure of Galois stable groups over local and global fields. In Section 7 a probabilistic characterization of Galois stable groups over extensions of $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{d})$ is given, and in Sections 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 are suggested.

2. **Notation**

Throughout the paper we will use the following notations.
$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}$, $\mathbb{Z}_p$, O_K denote the fields of complex and real numbers, 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. $GL_n(R)$ and $M_n(R)$ denote the general linear group and the full matrix group over R respectively. $[E : F]$ 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, $\mathrm{diag}(d_1, d_2, \ldots, d_m)$ is a block-diagonal matrix having diagonal components $d_1, d_2, \ldots, d_n$. 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. For a group G we denote by $|G|$ the order of G.

3. **Some Results on Galois Stability**

The following result was obtained in [29] (see also [31]).

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 $GL_n(O_E)$ 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 $GL_n(O_E)$.

Theorem 2 (see [29], 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 [29], 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 $(t, t, \ldots, t)$ 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 [28]:

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

1) If $n \geq \phi_E(t)d$, there is a finite abelian Γ-stable subgroup $G \subset GL_n(O'_E)$ of exponent t such that $E = F(G)$ where O'_E is the intersection of valuation rings of all localization rings of O_E with respect to primes ramified in E/F.
2) If $n \geq \phi_E(t)dh$ and h is the exponent of the class group of F, there is a finite abelian Γ-stable subgroup $G \subset GL_n(O_E)$ of exponent t such that $E = F(G)$.
3) If $n \geq \phi_E(t)d$ and h is relatively prime to n, then any G given in 1) is conjugate in $GL_n(F)$ to a subgroup of $GL_n(O_E)$.
4) If d is odd, then any G given in 1) is conjugate in $GL_n(F)$ to a subgroup of $GL_n(O_E)$.

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

Some further results for Galois stable groups G with entries in unramified field extensions of characteristic 0 can be found in [28] and [31].

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 [4] (see also [27] 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 [17]:

Main Theorem. *Let $K/\mathbb{Q}$ be a normal extension with Galois group Γ, and let $G \subset GL_n(O_K)$ be a finite Γ-stable subgroup. Then $G \subset GL_n(O_{K_{ab}})$ where K_{ab} is the maximal abelian over $\mathbb{Q}$ 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 $GL_n(O_K)$ acts in a natural way on $O_K \otimes M \cong \bigoplus_{i=1}^n O_K m_i$. 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 $GL_n(O_K)$ acts in a natural way on $O_K \otimes M \cong \bigoplus_{i=1}^n O_K m_i$. A finite group $G \subset GL_n(O_K)$ is said to be of A-type, if there exists a decomposition $M = \bigoplus_{i=1}^k M_i$ such that for every $g \in G$ there exists a permutation $\Pi(g)$ of $\{1, 2, \ldots, k\}$ and roots of unity $\epsilon_i(g)$ such that $\epsilon_i(g) g M_i = M_{\Pi(g)i}$ for $1 \leq i \leq k$.*

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 $G \subset GL_n(O_K)$ 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 $GL_2(O_K)$ 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 if and only if $p \equiv 3(mod 4)$.

The paper [4] 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 $GL_n(O_K)$ 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, $G \subset GL_n(O_{K_{ab}})$ 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 a question for the groups G over local fields: *Let K be a finite Galois extension of $\mathbb{Q}_p$ and G be a finite subgroup of $GL_n(O_K)$ which is stable under the natural operation of the Galois group Γ of the field K. Is it true that $G \subset GL_n(O_{K_{ab}})$ holds, K_{ab} the maximal abelian subextension of K over $\mathbb{Q}_p$?*

However, the answer is negative as we can see from the following example:

Example 2A. Let $K = \mathbb{Q}_p(\zeta_p, \sqrt[p]{p+1})$, the extension $K/\mathbb{Q}_p$ is normal and not abelian. We can put

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

Then $g^\gamma, \gamma \in \Gamma = Gal(K/\mathbb{Q}_p)$ and $\zeta_p I_p$ generate a finite Γ-stable subgroup of $GL_p(O_K)$ and $K = \mathbb{Q}_p(G)$.

But an extra condition that $G = G(\mathfrak{p}) = \{g \in G | g \equiv I_n (mod \mathfrak{p})\}$ (for the prime divisor $\mathfrak{p}$ of p in O_K) allows to get a positive answer to the following question for any elementary abelian Γ-stable p-subgroup $G \subset GL_n(O_K)$:

Question 4. *Let K be a finite Galois extension of $\mathbb{Q}_p$ and G be a finite subgroup of $GL_n(O_K)$ which is stable under the natural operation of the Galois group Γ of the field K and $G = G(\mathfrak{p})$ for the prime divisor $\mathfrak{p}$ of p in O_K. Is it true that $G \subset GL_n(O_{K_{ab}})$ holds, K_{ab} the maximal abelian subextension of K over $\mathbb{Q}_p$?*

Example 2 above shows that for abelian extensions $K/\mathbb{Q}_p$ this is still not true without the extra assumption $G = G(\mathfrak{p})$. But Theorem 6 below gives a positive answer to the Question 4 for an elementary abelian Γ-stable p-subgroup $G \subset GL_n(O_K)$ provided $G = G(\mathfrak{p})$.

It is known (see [4], [27], [31]) 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 $G \subset GL_n(O_K)$ of exponent p, moreover, G is generated by its congruence subgroups $G(\mathfrak{p})$ for all prime divisors $\mathfrak{p}$ of p in O_K.

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 $GL_n(O_K)$. 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 $G \subset GL_n(O_K)$. 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 Examples 2 and 2A 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 $G \subset GL_n(O_K)$ be an elementary abelian Γ-stable p-subgroup of exponent p, let $G = G(\mathfrak{p})$ for the prime divisor $\mathfrak{p}$ of p, and let $K = \mathbb{Q}_p(G)$. Then $K/\mathbb{Q}_p$ is an abelian field extension.*

Theorem 6 is proven in [6], Theorem 1 using some methods from [4], [1], [10], [42]. The idea of the proof is to show that $K = \mathbb{Q}_p(G)$ has a special ramification structure over $\mathbb{Q}_p$ and to use the congruence properties of $G = G(\mathfrak{p})$, 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 $\bar{\Gamma} = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_t\}$, let $w_1, w_2, \ldots, w_d$ be a basis of O_E over 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 also use a criterion of integrality of G stated in proposition 2 below, find some restrictions for ramification in the realization fields K of G and reduce the problem to a special case of Kummer extensions K of their unramified subfields.

Theorem 6 allows us to give a new proof of the Main Theorem stated above and proven in [4]. 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 [4], [27]), next to apply Theorem 6 to show 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 [2]). *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 [2], Proposition 1.

Finally we apply 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.

4. **Integrality of Galois Stable Representations**

This section contains some auxiliary results, some of them are contained in slightly different formulations in [29], see also [31]. Here we need these results in a more general context, in particular, we use the proofs for local rings. We also give a new proof of Proposition 2 below which is shorter than one in [4]. For the convenience of the reader and for the needs of our further proofs these results and proofs are given in part below. We also explain the finiteness theorem given in Section 3 since we are especially interested in results concerning Galois stability over rings which is essentially different from the corresponding results over fields (Theorems 2 and 3 above).

Proposition 1. *Let E/F be a normal extension of local fields with Galois group $\Gamma_{E/F} = Gal(E/F)$ 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 $G_1, G_2, \dots, G_r$, then $F(G)$ is the composite of the fields $F(G_1)$, $F(G_2)$, ..., $F(G_r)$.*

The proof of Proposition 1 is given in [4], Lemma 1.2.1, and it gives much freedom for the option of E/F and the subrings E_1, F_1 (which may also be fields).

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 O_E, O_L be the corresponding local rings of integers. Let $w_1, w_2, \dots, w_t$ be a basis of O_E over 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 $\sigma_1 = 1$, $\sigma_2, \dots, \sigma_t$ denote all automorphisms of the Galois group $\Gamma_{E/F}$ of the field E over F.

Assume that $L = E(\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(n)})$ where $\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(n)}$ 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 $\sigma_1, \sigma_2, \dots, \sigma_r$ 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 $\{\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(n)}\}$ say $\zeta_{(1)}, \zeta_{(2)}, \dots, \zeta_{(t)}$ we have the following

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

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

are divisible by $\sqrt{D}$ in the ring O_L.

Note that the conditions of Proposition 2 are always true if E is unramified over F since $DO_E = O_E$ in this case. A similar result is proven in [4], but the proof of Proposition 2 below is shorter.

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 $G_i \subset GL_{n_i}(E)$, $i = 1, \dots, k$ of G are conjugate in $GL_{n_i}(F)$ to subgroups $G_i' \subset GL_{n_i}(O_E)$ such that $E = F(G_1)F(G_2)\dots F(G_k)$. 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.

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 $g = B_1w_1 + B_2w_2 + \cdots + B_tw_t$, $(B_i \in M_n(F))$, and all matrices $g^\gamma, \gamma \in \Gamma_{E/F}$, and let $E = F(G)$. Then G is conjugate in $GL_n(F)$ to $G' \subset GL_n(O_E)$ if and only if all eigenvalues of matrices $B_i, i = 1, \ldots, t$ are contained in O_L, where $L = E(\zeta_p)$. The latter happens if and only if the criterion of Proposition 2, 1)* holds true.

Proof of Proposition 2.

Using the basis $w_1, \ldots, w_t$ of O_E over O_F we can write

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

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 [45], p. 8, corollary 3 for example). So if one of the eigenvalues of B_i is in O_L then all of them are since they are Galois conjugate. Using the dual basis $w_1^*, \ldots, w_t^*$ to $w_1, \ldots, w_t$ 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 $B_i, i = 1, \ldots, t$ are conjugate in $GL_n(F)$ to matrices $B_i' \in M_n(O_F)$, since for the generator g of G the equation

$$g = B_1w_1 + B_2w_2 + \cdots + B_tw_t,$$

holds with $B_i \in M_n(F)$ and $w_1, \ldots, w_t$ a basis of O_E over O_F. In fact each semisimple matrix $B_i \in M_n(F)$ is conjugate in $GL_n(F)$ to a matrix from $M_n(O_F)$ if and only if all its eigenvalues are contained in 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 $\lambda_k = d_k / \det(W)$ and therefore the eigenvalues of B_k are in O_L if and only if $\det(W)$ 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, $j = 1, 2, \dots, k$ of the semisimple matrices $B_i \in M_n(F)$, $i = 1, \dots, t$ be contained in the ring O_L for some field $L \supset F$. Then B_i are conjugate in $GL_n(F)$ simultaneously to matrices that are contained in $M_n(O_F)$. ii) Conversely, if the semisimple matrices B_i are contained in $M_n(O_F)$ and B_i are diagonalizable over a field $L \supset F$, then their eigenvalues are contained in O_L.*

Proof of Auxiliary Lemma. i) Consider the F-algebra $A = F[B_1, \dots, B_t]$ generated by the matrices $B_1, \dots, B_t$. By [45], ch. 1, Section 1, Corollary 2 we can consider A to be a field extending F. Let $a_1, a_2, \dots, a_n$ be a basis of O_A over O_F. Then for any $B \in A$ we have $B = b_1a_1 + \dots + b_na_n$, and the elements $b_i \in F$ are contained in O_F if and only if $B \in O_A$. But all coefficients k_{ij} of the characteristic polynomials $f_i(x) = k_{i0} + k_{i1}x + \dots + k_{in}x^n$ of the matrices B_i are contained in O_L, and $k_{in} = 1$, so $B_i \in A$ are integral over F. It follows that $B_i = b_{i1}a_1 + \dots + b_{in}a_n$, and $b_{ij} \in O_F$. If $v \in F^n$ is a non-zero vector in F^n, then $a_1v, a_2v, \dots, a_nv$ is a basis of F^n, and $B_ia_jv = \sum_k c_{ijk}a_kv$, where $c_{ijk} \in O_F$. It follows that for any i the matrix $C_i = [c_{ijk}]_{k,j}$ belongs to $GL_n(O_F)$, and C_i is the matrix of the operator B_i in the basis $a_1v, a_2v, \dots, a_nv$ of F^n. Therefore, B_i is conjugate in $GL_n(F)$ to C_i for any $i = 1, \dots, t$.

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

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

Proof of Corollary 1. If $G \subset GL_n(O_E)$ is a group of exponent p and $g = B_1w_1 + B_2w_2 + \dots + B_tw_t$ for a basis $w_1, \dots, w_t$ of O_E over O_F, then $B_i \in M_n(O_F)$, and it follows from Auxiliary Lemma to Proposition 2 that the eigenvalues of B_j are contained in O_L. Notice, that for the second part of 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, $i = 1, \dots, k$. It follows that G_i are conjugate to subgroups $G_i' \subset GL_{n_i}(O_E)$. Now, Proposition 1 implies $E = F(G_1)F(G_2) \dots F(G_k)$. 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 $G_i \subset GL_{n_i}(E)$, $i = 1, \dots, k$. Then for $g = B_1w_1 + B_2w_2 + \dots + B_tw_t$

$$C^{-1}gC = \begin{vmatrix} g_1 & & * \\ & \ddots & \\ 0 & & g_k \end{vmatrix} = B_1'w_1 + B_2'w_2 + \dots + B_t'w_t$$

holds with $B_i' = C^{-1}B_iC$. Let us consider the F-algebra A generated by all $B_i', i = 1, \dots, t$ 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 O_E contains all rings $O_{F(G_i)}$, 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 $G_i' \subset GL_{n_i}(O_E)$ if and only if all eigenvalues of matrices B_i', $i = 1, \dots, t$ are contained in O_{L_i}, where $L_i = F(G_i)(\zeta_p)$ and this happens if and only if

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

are divisible by $\sqrt{D}$ in the ring O_L. But $F(G) = F(G_1)F(G_2)\dots F(G_k)$ by Proposition 1, and so $L = L_1L_2\dots L_k$. This completes the proof of Corollary 2.

The following proposition is proven in [29] (Proposition 2, p. 229).

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.*

Here we can prove the Finiteness Theorem formulated in Section 3.

Proof of Theorem 1. 1) In the virtue of Proposition 1 from Section 4 we can restrict ourselves to considering only irreducible G. It follows from integrality in 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 ([35], [36], [37]) 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 [38], 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 [3] 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 O of O_E with respect to $\mathfrak{p}$, $A \in M_n(O)$ 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 $pA+\pi^{m(p-1)}A^p \equiv 0_n(modp\pi)$, 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.

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

Proof of Lemma 1. It is a generalization of the argument of Minkowski [35]. Prove that G is abelian of exponent p. Let π be the prime element of 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 $g_i^{-1} \equiv I_n - \pi B_i(mod\pi^2)$, $i = 1, 2$ and $h = g_1g_2g_1^{-1}g_2^{-1} \equiv I_n(mod\pi^2)$. It follows from Lemma 1.5.1, (ii) in [4] that $h = I_n$, and the same Lemma 1.5.1, (ii) in [4] shows that $g^p = I_n$ for any $g \in G$. First of all, G is conjugate over O_K to a group of triangular matrices, since G is abelian and O_K is a local ring, see [14] Theorem (73.9) and the remarks in [14] on p. 493. On the other hand, we can describe explicitly the matrix M such that

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

is a diagonal matrix for a triangular matrix g of order p which is congruent to $I_n(mod\mathfrak{p})$. 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

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

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

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

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:

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

The condition $g \equiv I_n(mod\mathfrak{p})$ implies $P_i^j \equiv 0_{t_j t_i}(mod\mathfrak{p})$, 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 O_K.

Using the same argument for global fields in [4] we proved

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

Remark that for global fields in [4] 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 [14]).

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 $GL_n(O_{L(\zeta_p)})$ consisting of matrices g, $g \equiv I_n(mod\mathfrak{p})$, then G is conjugate in $GL_n(O_L)$ 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 $M \in GL_n(O_{L(\zeta_p)})$ 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 $M \in GL_n(O_{L(\zeta_p)})$, it follows that $M^\sigma \equiv M(mod\mathfrak{p})$. Therefore, the congruence $M^{-1}M^\sigma \equiv I_n(mod\mathfrak{p})$ 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:

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

$\sigma_1, \sigma_2, \ldots, \sigma_{p-1}$ are all elements of Γ. It is clear, that $M_1 \equiv M(mod\mathfrak{p})$ and $detM_1 \equiv detM(mod\mathfrak{p})$. It follows that $M_1 \in GL_n(O_{L(\zeta_p)})$. Furthermore, M_1 is stable under elementwise Γ-action, so all m_{ij} are Γ-stable and $m_{ij} \in L$. Hence $M_1 \in GL_n(L)$. Since $M^\sigma = M\lambda$, it follows that $M_1^{-1} G M_1$ 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 $O_\mathfrak{p}$ 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 $GL_n(O_\mathfrak{p})$ consisting of matrices g, $g \equiv I_n(mod\mathfrak{p})$, then G is conjugate in $GL_n(L \cap O_\mathfrak{p})$ 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 [4] (see Lemma 1.5.2 and Corollary 1.5.3 in [4]).

5. **Proof of The Main Theorem**

Now we can use Theorem 6 for a proof of the Main Theorem formulated in Section 3, which is simpler than the proof given in [4].

According to [4] and [27], 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, and G is generated by its congruence subgroups $G(\mathfrak{p}) := \{g \in G, g \equiv I_m(mod\mathfrak{p})\}$ for prime divisors $\mathfrak{p}$ of p and G is generated by its congruence subgroups $G(\mathfrak{p})$ for all prime divisors $\mathfrak{p}$ of p in O_K.

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. Let us denote by $Z_\mathfrak{p} \subset \Gamma = Gal(K/\mathbb{Q})$ the decomposition group of a prime divisor $\mathfrak{p}$ of p. $Z_\mathfrak{p}$ can be identified with $Gal(K\mathbb{Q}_p/\mathbb{Q}_p)$. Note that $G(\mathfrak{p})$ is stable under the action of $Z_\mathfrak{p}$. Let θ be an element generating $\mathbb{Q}(G(\mathfrak{p}))$: $\mathbb{Q}(G(\mathfrak{p})) = \mathbb{Q}(\theta)$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal irreducible polynomial of θ with roots $\theta_1 = \theta, \theta_2, \ldots, \theta_k$. Since $G(\mathfrak{p})$ is $Z_\mathfrak{p}$- stable, the

local extension $\mathbb{Q}_p(G(\mathfrak{p}))/\mathbb{Q}_p = \mathbb{Q}_p(\theta)/\mathbb{Q}_p$ is normal, and therefore $f(x)$ splits in $\mathbb{Q}_p(\theta)[x]$:

$$f(x) = (x-\theta_1)(x-\theta_2)\dots(x-\theta_k), \text{ and } \theta_i \in \mathbb{Q}_p.$$

We can assume that G is a minimal counterexample to the Main Theorem, and $K = \mathbb{Q}(G)$. If K is not unramified over K_{ab}, its maximal abelian over $\mathbb{Q}$ subfield, then $Z = Z_{\mathfrak{p}}$ has a nontrivial commutator subgroup $Z' \neq \{1\}$, and the commutator subgroup $\Gamma'_{\mathfrak{p}}$ of the Galois group of $\Gamma_{\mathfrak{p}} = Gal(\mathbb{Q}_p(G(\mathfrak{p}))/\mathbb{Q}_p)$ is also nontrivial, since it can be canonically identified with Z'. Moreover, the action of $\Gamma'_{\mathfrak{p}}$ on $G(\mathfrak{p})$ is not trivial, and $g^{\gamma} \neq g$ for some $g \in G(\mathfrak{p})$ and $\gamma \in Z'$, so the extension $K_{\mathfrak{p}}/\mathbb{Q}_p = K\mathbb{Q}_p/\mathbb{Q}_p = \mathbb{Q}_p(\theta)/\mathbb{Q}_p$ is not abelian. But in the virtue of Theorem 6, this is not possible. Now let the extension $K\mathbb{Q}_p/\mathbb{Q}_p = \mathbb{Q}_p(\theta)/\mathbb{Q}_p$ be abelian.

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 in [4] and [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 Section 4, 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 $G \subset GL_n(O_K)$ 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.

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).

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 $g^\gamma, \gamma \in \Gamma_0(\mathfrak{p})$ for a $g \in G$ is not cyclic, we can apply the argument of the proof of case I of the main theorem in [4], which implies that the conditions of Proposition 2 concerning the determinants d_k are not satisfied for the group generated by all $g^\gamma, \gamma \in \Gamma_0(\mathfrak{p})$, and so $G \not\subset GL_n(O_K)$.

Therefore, G should be cyclic, and $g^\gamma = g^a$ for all $g \in G$ and any $\gamma \in \Gamma_0 = \Gamma_0(\mathfrak{p})$. Moreover, a is the same for all g. Indeed, if $g^\gamma = g^a$ and ${g_1}^\gamma = {g_1}^b$, with $a \neq b$, $g \neq I_n$, $g_1 \neq I_n$, then the elements $(gg_1)^\gamma$, $\gamma \in \Gamma_0(\mathfrak{p})$ 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 $\Gamma_0(\mathfrak{p})$ for all prime divisors $\mathfrak{p}$ of p. 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 Section 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 [38], p. 69, and Proposition 4.9 in [38], 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 that $\zeta_p \in K$. 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 $GL_n(O_\mathfrak{p} \cap K^{\Gamma_0})$, where $O_\mathfrak{p}$ is the valuation ring of $K^{\Gamma_0}(\zeta_p)$ at $\mathfrak{p}$, the group $G_0 = G_0(\mathfrak{p}) = \{g \in G_0, g \equiv I_n(mod\mathfrak{p})\}$ consists of diagonal matrices. The group $G = G(\mathfrak{p}) := \{g \in G, g \equiv I_n(mod\mathfrak{p})\}$ 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, $h = \mathrm{diag}(l_1 I_{n_1}, \ldots, l_k I_{n_k})$, then $g = \mathrm{diag}(g_1, \ldots, g_k), g_i \in GL_{n_i}(K)$ holds for every $g \in G$, and therefore we can split G into $GL_n(O_\mathfrak{p} \cap K^{\Gamma_0})$-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 Section 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

$$G_0' = G_0'(\mathfrak{p}) := \{g \in G_0', g \equiv I_m(mod\mathfrak{p})\}$$

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 $G \subset GL_n(O_K)$ 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 $GL_n(O_\mathfrak{p} \cap K^{\Gamma_0})$, where $O_\mathfrak{p}$ is the valuation ring 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.

The following lemma is proven in [6] and follows easily from the argument above. It can be used both 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 $G \subset GL_n(O_K)$ 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 $\Gamma_1(\mathfrak{p})$.*

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 the extension $R(g, \zeta_p)/R(\zeta_p)$ is unramified.
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 the extension $R(g_0, \zeta_p)/R(\zeta_p)$ is unramified.

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.

Now we can use Lemma 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. We can use the argument from the proof of the case II, b) of the main theorem in [4] (or alternatively Theorem 1 in [6]) which gives a group $G'_1 \subset GL_m(O_{K_\mathfrak{p}})$ generated by matrices g_1 and $\zeta_p I_m$ with a realization field $E = L(G'_1)$, L is unramified over $\mathbb{Q}_p$, and E/L a normal non-abelian field extension, $E = L(\zeta_p, \sqrt[p]{u})$ for some $u \in L$. But the Galois group of E/L having these properties is not abelian. This gives a contradiction with Theorem 6.

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 $G \subset GL_n(O_E)$ (see [28] 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 O_E for the existence of finite $Gal(E/F)$-stable subgroups $G \subset GL_n(O_E)$.

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

Example 3. It is difficult to transfer the idea of reduction to abelian Galois stable groups G of a 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 $g := \mathrm{diag}(g_2, I_{p-2}) \in GL_p(O_K)$. Then $g^\gamma, \gamma \in \Gamma$ and $\zeta_p I_p$ generate a finite Γ-stable nonabelian subgroup of $GL_p(O_K)$ 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 $G = \{g, -g, I_2, -I_2\} \subset GL_2(O_E)$ 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 exists an intermediate extension $L = F(\sqrt[p]{u}) \subset E$ for some unit $u \in O_E$, 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 $GL_p(O_E)$.

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 $p_1, p_2, \dots, p_k$, and $F/\mathbb{Q}$ is a number field unramified in $p_1, p_2, \dots, p_k$. 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 $GL_n(O_K)$ 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 $GL_n(O_K)$ 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 [5].

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 $O'(N) = \{\alpha \in O_K \big| \, |N_{K/\mathbb{Q}}(\alpha)| \leqslant N\}$ where $N_{K/\mathbb{Q}}$ is the norm map. The proof of the following theorem (see [29], Theorem 4) is based on the result by S. D. Cohen (see Theorem 1 in [13]) 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 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 $O'(N)$, and let $\psi(N)$ denote the number of those polynomials whose splitting fields do not contain any fields $K(G) \neq K$ for $G \subset GL_n(O_E), E \supset K$ 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 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 $O'(N)$, compare [13]. Note that proof below, specially in the case 1), can produce explicit estimates, and we can also use the estimates in [22], [23], [18].

Proof of Theorem 9. We use properties of distribution of Galois groups of polynomials that were considered by S. D. Cohen [13], for the case $K = \mathbb{Q}$ see also [46]. According to [13] 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 simpler, 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 [27]) 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 $O'(N)[x]$ 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 $(a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_l)$ 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 [15], ch. 4, Section 68 or [12], ch. 9, Section 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. [20], p.264) $M(j) \sim 4([j/1] + [j/2] + \cdots + [j/k] + \ldots) = 4(j \cdot lnj + O(j))$, 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. [20], 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 $A(x) = \sum_{i=0}^{m} p_i x^i \in O'(N)[x]$ 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 [15], ch. 4, Section 70 or [12], ch. 9, Section 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$f \in O'(N)[x]$ and $f = g \cdot g'$, $g, g' \in K(\sqrt{\alpha})[x]$, $\sqrt{\alpha} \notin K$. Let $\mathcal{E} \in O_{K(\sqrt{\alpha})}$ 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 $(c_2\sqrt{N})^{2\cdot(m/2+1)} = c_4N^{m+2}$, $c_4 = c_4(K, m)$, polynomials that are reducible over $K(\sqrt{\alpha})$. Likewise, there are $c_5N^{2(m+1)}$, $c_5 = c_5(K, m)$, polynomials f in $O'(N)[x]$ and it is obvious that

$$\lim_{N\to\infty} \frac{c_4N^{m+2}}{c_5N^{2m+2}} = 0.$$

Note that the number of polynomials $f \in O'(N)[x]$ that are reducible already in $O'(N)[x]$ do not give any contribution asymptotically. Moreover, according to the result in [13], 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 O_E then $G \subset GL_n(O_E)$.*

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 $f(x_1, x_2, \dots, x_n) \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ is a positive definite quadratic form, the order of the finite orthogonal group $O_f(O_K) \subset GL_n(O_K)$ of this form over 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 ([44], Section 6.3 and [36]) since $O_f(O_K) = O_f(\mathbb{Z})$. 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 $q = 2, 3, 5, 7, \dots$, and

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

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

There are some generalizations of this result of Minkowski using both algebraic (see [43], [16]) and analytic (see e. g. [25]) methods.

It is possible to generalize the above formula for finite subgroups of $GL_n(O_K)$ for some cyclotomic fields K using Lemmas 2 and 2A (Section 4) 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 $GL_n(O_K)$ 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 $a, b_1, \dots, b_l$ and relations $b_i^p = 1, b_i b_j = b_j b_i, i = 1, 2, \dots, l; ab_1 = b_1 a, b_{i-1} = b_i a b_i^{-1} a^{-1}, i = 1, 2, \dots, l; a^n = 1$, 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 $b_1, \dots, b_l$, 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, $\chi(b_i) = 1, i = 2, \dots, l$. The character χ together with the decomposition of G into cosets with respect to H: $G = 1 \centerdot H + a \centerdot H + \dots + a^{n-1} \centerdot H$ 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 $\begin{pmatrix} n-j \\ i-j \end{pmatrix}$:

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

Theorem 11. *Let $\mathbb{Q}_p(\zeta_{p^\infty})$ denotes the extension of $\mathbb{Q}_p$ obtained by adjoining all roots $\zeta_{p^i}, i = 1, 2, 3, \dots$ 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 $D = \mathrm{diag}(1, \pi, \pi^2, \dots, \pi^{n-1})$. Then the representation $R_\pi = D^{-1}C^{-1}RCD$ of G is a faithful, absolute irreducible representation in $GL_n(O_K)$ by matrices congruent to $I_n(mod\pi)$. Moreover, such representations are pairwise nonequivalent over $O_{\mathbb{Q}_p(\zeta_{p^\infty})}$, and for the lower central series $G = G_l \supset G_{l-1} \supset \dots \supset G_0 = \{I_n\}$ 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 [33], see also [34]. 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 [34], 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 $GL_n(O_K/\mathfrak{p})$, the reduction is considered modulo some prime ideal $\mathfrak{p} \subset O_K$.

The proof of the following propositions is technical; it is based on the reduction modulo some prime ideal $\mathfrak{p} \subset O_K$ such that its norm C is a prime integer and the kernel of the reduction of $GL_n(O_K)$ $(mod\mathfrak{p})$ 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 [32], 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 $GL_n(O_K)$ having the maximal possible order with some modifications in the case $p = 2$. The theorems describing the maximal p-subgroups of $GL_n(K)$ over fields can be found in [24], in particular, it is proven that there is only one conjugacy class of maximal p-subgroups of $GL_n(K)$ for $p > 2$. However, equivalence of subgroups in $GL_n(O_K)$ over O_K is a more subtle question. See [49], chapter 3, [50], [51] for the structure of finite linear groups (including the groups of small orders). See [8] for more details, proofs and applications to determining torsion elements in the reduced projective class group.

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

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

Let us consider an integer $h = [\frac{n}{\phi_K(q)}]$ and a semidirect product $H = M \rtimes S_h$ of the symmetric group S_h and the matrix group $M = \mathrm{diag}(g_1, g_2, \ldots, g_h, I_k)$ for $k = n - h\phi_K(q)$ and $g_i \in C_{q^j}$ for a cyclic group $C_{q^j} \subset GL_{\phi_K(q)}(O_K)$ with the operation of S_h (which can be identified with a subgroup P_h of block-permutation matrices $P \in GL_n(O_K)$) on M determined by permutations of diagonal blocks g_1: $P \cdot \mathrm{diag}(g_1, g_2, \ldots, g_h, I_k) = \mathrm{diag}(g_{P(1)}, g_{P(2)}, \ldots, g_{P(h)}, I_k), P \in P_h$. H is naturally isomorphic to the group consisting of matrices $mp \in GL_n(O_K)$ 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 $H = M \rtimes S'_h$, where

$$M = \mathrm{diag}(g_1, g_2, \ldots, g_h, I_k), \;\; g_i \in C_{q^m},$$

C_{q^m} is a cyclic subgroup of order q^m in $GL_{\phi_K(q^m)}(O_K)$ and S'_h is a Sylow q-subgroup of S'_h, and the order $|H|$ of the q-subgroup H is equal to

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

There are no q-subgroups in $GL_n(O_K)$ of order greater than $|H|$.

2) For $q = 2$ let $L = K(\sqrt{-1})$. There is a 2-subgroup of $H = M \rtimes S'_h$, where

$$M = \mathrm{diag}(g_1, g_2, \ldots, g_h, I_k), \;\; g_i \in C_{2^m},$$

C_{q^m} is a cyclic subgroup of order q^m in $GL_{\phi_L(q^m)}(O_L)$ and S'_h is a Sylow q-subgroup of S'_h, and the order $|H|$ of the group H is equal to

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

There are no 2-subgroups in $GL_n(O_L)$ (and therefore in $GL_n(O_K)$) of order greater than $|H|$.

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

The order of any finite subgroup of $GL_n(O_K)$ can be bounded by the constant

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

where the product is taken for all primes $q = 2, 3, 5, 7, \ldots$. This is a generalization of the above result by H. Minkowski [36].

Acknowledgments

The author is grateful to the referee for good remarks and helpful suggestions. The support of the DFG (BA 784/5-1) is gratefully acknowledged.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Second Edition, AMS Chelsea Publishing, 2009.

[2] M. Asada, On unramified Galois extensions over maximum abelian extensions of algebraic number fields, *Math. Ann.*, **270** no. 4 1985 477-487.

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

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

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

[6] H.-J. Bartels and D. A. Malinin, Finite Galois stable subgroups of GL_n over local fields, preprint.

[7] A. Borel, *Introduction aux groupes arithmetiques*, Publications de l'Institut de Mathmatique de l'Universit de Strasbourg, XV. Actualits Scientifiques et Industrielles, Hermann, Paris, no. 1341 1969 125 pp.

[8] B. Bürgisser, On the Projective Class Group of Arithmetic Groups, *Math. Z.*, **184** (1983) 339–357.

[9] G. Cardona, Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$, *J. Algebra*, **303** (2006) 707–721.

[10] J. W. S. Cassels, A. Frohlich and (ed.), *Algebraic Number Theory*: Proceedings of an Instructional Conference Organized by the London Mathematical Society (Nato Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich Academic Press, London, Thompson Book Co., Inc., Washington, D. C. 1967.

[11] G. Cliff, J. Ritter and A. Weiss, Group representations and integrality, *J. Reine Angew. Math.*, **426** (1992) 193–202.

[12] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, **13**, Academic Press, Inc. Harcourt Brace Jovanovich, Publishers, London–New York, 1978.

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

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

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

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

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

[18] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo. 1972), *Amer. Math. Soc.*, Providence, R.I., 1973 91–101.

[19] F. R. Gantmakher, *The theory of matrices*, Translated from the Russian by K. A. Hirsch, translation. AMS Chelsea Publishing, Providence, RI, **1** 1959.

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

[21] W. Knapp and P. Schmidt, An extension theorem for integral representations, *J. Austral. Math. Soc. Ser. A*, **63** (1997) 1–15.

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

[23] H. W. Knobloch, Die Seltenheit der reduziblen Polynome, *Jber. Deutch. Math. Verein.*, **59** Abt. 1 (1956) 12–19.

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

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

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

[27] D. A. Malinin, Galois stability for integral representations of finite groups, (Russian) *Algebra i Analiz*, (2000) 106–145, translation in *St. Petersburg Math. J.*, **12** no. 3 (2001) 423–449.

[28] D. A. Malinin, On the existence of finite Galois stable groups over integers in unramified extensions of number fields, *Publ. Mathem. Debrecen*, **60** no. 1-2 (2002) 179–191.

[29] D. A. Malinin, Galois stability, integrality and realization fields for representations of finite Abelian groups, *Algebr. Represent. Theory*, **6** no. 2 (2003) 215–237.

[30] D. A. Malinin, *Some integral representations of finite groups and their arithmetic applications*, In: Algebraic Geometry and Its Applications, World Sci. Publ., Hackensack, NJ, 2008 467–480.

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

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

[33] D. A. Malinin, Integral representations of p-groups of a given class of nilpotency over local fields, (Russian) *Algebra i Analiz* **10** no. 1 (1998) 58–67, translation in *St. Petersburg Math. J.*, **10** no. 1 (1999) 45–52.

[34] 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) 619–622.

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

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

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

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

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

[40] J. Ritter and A. Weiss, Regulators and Galois stability, *Math. Nachr.*, **158** (1992) 27–41.

[41] P. Roquette, Realisierung von Darstellungen endlicher nilpotenter Gruppen, *Arch. Math. (Basel)*, **9** (1958) 241-250.

[42] J.-P. Serre,*Corps locaux*, (French) Publications de l'Institut de Mathmatique de l'Universit de Nancago, VIII Actualits Sci. Indust., Hermann, Paris, no. 1296 (1962) 243 pp.

[43] J.-P. Serre, *Bounds for the orders of the finite subgroups of* $G(k)$, Group representation theory, EPFL Press, Lausanne, 2007 405-450.

[44] C. Soulé, *An introduction to arithmetic groups*, Frontiers in number theory, physics, and geometry. II, Springer, Berlin, 2006 247-276.

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

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

[47] L. C. Washington, *Introduction to Cyclotomic Fields*, second edition, **83**, Springer-Verlag, New York, Berlin, Heidelberg, 1997.

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

[49] A. E. Zalesskii, Linear groups, *Russ. Math. Surv.*, **36** (1981) 63-128.

[50] A. E. Zalesskii, Linear groups, Algebra. Topology. Geometry, Itogi Nauki i Tekhniki, *Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform.*, Moscow, **21** (1983) 135-182.

[51] P. H. Tiep and A. E. Zalesskii, Some aspects of finite linear groups: A survey, *J. Math. Sci.*, **100** (2000) 1893-1914.

Dmitry Malinin

Institut des Hautes Études Scientifiques, Le Bois-Marie 35, route de Chartres 91440 Bures-sur-Yvette, France

Email: dmalinin@ihes.fr

Email: dmalinin@gmail.com