Volume 243

A Series of Lecture Notes in Pure and Applied Mathematics

Noncommutative Algebra and Geometry

Edited by

Corrado De Concini

Freddy Van Oystaeyen

Nikolai Vavilov

Anatoly Yakovlev

Chapman & Hall/CRC
Taylor & Francis Group

Noncommutative Algebra and Geometry

PURE AND APPLIED MATHEMATICS

A Program of Monographs, Textbooks, and Lecture Notes

LECTURE NOTES IN PURE AND APPLIED MATHEMATICS

Recent Titles

G. Lumer and L. Weis, Evolution Equations and Their Applications in Physical and Life Sciences

J. Cagnol et al., Shape Optimization and Optimal Design

J. Herzog and G. Restuccia, Geometric and Combinatorial Aspects of Commutative Algebra

G. Chen et al., Control of Nonlinear Distributed Parameter Systems

F. Ali Mehmeti et al., Partial Differential Equations on Multistructures

D. D. Anderson and I. J. Papick, Ideal Theoretic Methods in Commutative Algebra

Á. Granja et al., Ring Theory and Algebraic Geometry

A. K. Katsaras et al., p-adic Functional Analysis

R. Salvi, The Navier-Stokes Equations

F. U. Coelho and H. A. Merklen, Representations of Algebras

S. Aizicovici and N. H. Pavel, Differential Equations and Control Theory

G. Lyubeznik, Local Cohomology and Its Applications

G. Da Prato and L. Tubaro, Stochastic Partial Differential Equations and Applications

W. A. Carnielli et al., Paraconsistency

A. Benkirane and A. Touzani, Partial Differential Equations

A. Illanes et al., Continuum Theory

M. Fontana et al., Commutative Ring Theory and Applications

D. Mond and M. J. Saia, Real and Complex Singularities

V. Ancona and J. Vaillant, Hyperbolic Differential Operators and Related Problems

G. R. Goldstein et al., Evolution Equations

A. Giambruno et al., Polynomial Identities and Combinatorial Methods

A. Facchini et al., Rings, Modules, Algebras, and Abelian Groups

J. Bergen et al., Hopf Algebras

A. C. Krinik and R. J. Swift, Stochastic Processes and Functional Analysis: A Volume of Recent Advances in Honor of M. M. Rao

S. Caenepeel and F. van Oystaeyen, Hopf Algebras in Noncommutative Geometry and Physics

J. Cagnol and J.-P. Zolésio, Control and Boundary Analysis

S. T. Chapman, Arithmetical Properties of Commutative Rings and Monoids

O. Imanuvilov, et al., Control Theory of Partial Differential Equations

Corrado De Concini, et al., Noncommutative Algebra and Geometry

Alberto Corso, et al., Commutative Algebra: Geometric, Homological, Combinatorial and Computational Aspects

Giuseppe Da Prato and Luciano Tubaro, Stochastic Partial Differential Equations and Applications – VII

Noncommutative Algebra and Geometry

Edited by

Corrado De Concini
University of Rome
Rome, Italy

Freddy Van Oystaeyen
University of Antwerp/UIA
Antwerp, Belgium

Nikolai Vavilov
St. Petersburg State University
St. Petersburg, Russia

Anatoly Yakovlev
St. Petersburg State University
St. Petersburg, Russia

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150309

International Standard Book Number-13: 978-1-4200-2810-2 (eBook - PDF)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Introduction

The international meeting at St. Petersburg was organized in honor of Prof. Dr. Z. Borevich, but there was no restriction on the topics of the lectures. A proceedings covering all subjects of the meeting would therefore constitute a rather inhomogeneous collection. The present volume, however, is mainly devoted to the contributions related to the ESF workshop organized in the framework of the scientific program "Noncommutative Geometry" of the European Science Foundation and integrated in the Borevich meeting. The topics dealt with here may be classified as noncommutative algebra.

The congenial atmosphere at the meeting combined with the city's preparations for the anniversary festivities provided the perfect setting for a very fruitful meeting. Moreover, the combination of the ESF workshop and the Borevich meeting brought together many participants from East and West (now perhaps old-fashioned terminology) engaging in open discussions, hard work, and the occasional party. Most of this may be blamed on the local organizers, Vavilov and Yakovlev, whom we thank for their great hospitality.

Contributors

Hans-Jochen Bartels
Universitat Mannheim
Mannheim, Germany

Igor Burban
Fachbereich Mathematik
Kaiserslautern, Germany

Eloisa Detomi
Dipto di Matematica Universit
Padova, Italy

Yuriy Drozd
Kyiv Taras Shevchenko University
Department of Mechanics and Mathematics
Kyiv, Ukraine

G. Griffith Elder
University of Nebraska/Omaha
Department of Mathematics
Omaha, Nebraska

Eivind Eriksen
University of Warwick
Institute of Mathematics
Coventry, United Kingdom

Michiel Hazewinkel
CWI
Amsterdam, The Netherlands

Lieven Le Bruyn
Universiteit Antwerpen
Department of Wiskunde and Informatica
Antwerpen, Belgium

Lucchini, Andrea
Dipto di Matematica University
Brescia, Italy

Dmitry A. Malinin
Belarusian State Pedag. University
Minsk, Belarus

Janvière Ndirahisha
University of Antwerp (UIA)
Department of Math and Computer Science
Wilrijk, Belgium

Toukaiddine Petit
University of Antwerp
Department of Math and Computer Science
Antwerp, Belgium

Tsetska G. Rashkova
University of Rousse
Center of Applied Math and Information
Rousse, Bulgaria

Wolfgang Rump
Universitat Stuttgart
Institut f'ur Algebra und Zah
Stuttgart, Germany

Freddy Van Oystaeyen
University of Antwerp/UIA
Department of Mathematics
Antwerp/Wilrijk, Belgium

Table of Contents

FINITE GALOIS STABLE SUBGROUPS OF GL_n

H. -J. BARTELS[1] AND D. A. MALININ[2]

Abstract. Let $K/\mathbb{Q}$ be a finite Galois extension with maximal order $\mathcal{O}_K$ and Galois group Γ. We consider finite Γ-stable subgroups $G \subset GL_n(\mathcal{O}_K)$ and prove that they are generated by matrices with coefficients in $\mathcal{O}_{K_{ab}}, K_{ab}$ the maximal abelian subextension of K over $\mathbb{Q}$. This implies in particular a positive answer to a conjecture of J. Tate on the classification of p-divisible groups over $\mathbb{Z}$ and answers also a longstanding question of Y. Kitaoka on totally real scalar extensions of positive definite integral quadratic lattices.

Introduction

The starting point of our investigations was the following problem studied by Y. Kitaoka and the first named author around 1978 on the behaviour of the automorphism groups of positive definite quadratic $\mathbb{Z}$-lattices under totally real scalar extensions. There was the

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

Closely connected with this question was the following

Conjecture 1. *Let $K/\mathbb{Q}$ be a finite totally real Galois extension and denote by $\mathcal{O}_K$ the corresponding ring of integers and let $G \subset GL_n(\mathcal{O}_K)$ be a finite subgroup stable under the operation of the Galois group $\Gamma = Gal(K/\mathbb{Q})$, then $G \subset GL_n(\mathbb{Z})$ holds, $\mathbb{Z}$ the ring of rational integers.*

There are several reformulations and generalizations of the above mentioned conjecture. One generalization is the following:

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

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

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

Partial answers to these questions are given in [2], [3], [4], [8], [9], [10], [14], [16], [17], [19] (compare also the references in mentioned articles).

1991 *Mathematics Subject Classification.* Primary 20C10, 11R33, 11S23, 11R29.

In an earlier version of this paper (see [4]) it is shown that conjecture 2 is true in the case of Galois field extension $K/\mathbb{Q}$ with odd discriminant. Also some partial answers are given in the case of field extensions $K/\mathbb{Q}$ which are un-ramified outside 2. The proof of the main part is essentially already contained in the article [17] of the second named author in slightly different formulation. While [17] focusses mainly on the proofs of conjecture 1 and contains also some other related results, we observed that the proofs of conjecture 1 can immediately be transfered in order to proof conjecture 2 in the mentioned cases. Using the methods of [2], [3] and discriminant estimations of A. Odlyzko [23] in order to exclude the existence of certain Galois extensions having low ramification, the first named author proved in an unpublished note eighteen years ago, that conjecture 1 is true in the following cases:

i) $\Gamma = \mathrm{Gal}(K/\mathbb{Q}) = PSL_2(5) \cong A_5$ the alternating group of order 60,
ii) $\Gamma = \mathrm{Gal}(K/\mathbb{Q}) = PSL_2(7)$ the simple group of order 168,
iii) $K/\mathbb{Q}$ is tamely ramified of degree ≤ 131
iv) $K/\mathbb{Q}$ is tamely ramified of degree ≤ 233 assuming a generalized Riemann hypothesis to be true.

The combination of this approach using discriminant estimations with the far reaching results of [17] and [7] gave us the the following better results:

Conjecture 1 is true in the following cases:

i) $[K : \mathbb{Q}] \leq 960$ assuming the generalized Riemann hypothesis for the zeta function of the number field K, or if
ii) $[K : \mathbb{Q}] \leq 480$ unconditionally.

Conjecture 2 is true if $[K : \mathbb{Q}] < 288$ unconditionally. See [4] for the details.

After finishing the first version of our paper [4] we became aware of the recent work [20] of M. Mazur on the same topic. It turned out that in a certain sense the partial results of M. Mazur are complementary to our partial results. Using the the classification of finite flat group schemes over $\mathbb{Z}$ annihilated by a prime p for primes $p \leq 17$ due to V. A. Abrashkin [1] and J.-M. Fontaine [6] the particular case of field extensions $K/\mathbb{Q}$ which are unramified outside 2 follows in full generality from [20]. In this revised version of our paper we restrict therefore ourselves to the case of ramified primes $p \neq 2$. It should be noted that conversely our Main Theorem in combination with the work of M. Mazur has interesting consequences for the classification of finite flat commutative group schemes over $\mathbb{Z}$ annihilated by a prime p: It answers a question of J. Tate [28] also for primes $p \geq 17$ completing the partial results of Abrashkin [1] and Fontaine [6].

It is interesting to notice that the methods used in the proofs, namely the detailed study of the operation of the higher ramification groups of the Galois group on the given Galois stable group G for the ramified primes in the field extension K over $\mathbb{Q}$ together with discriminant estimations, in order to eliminate ramification with large depth using trivial action of higher ramification groups (compare [2] section 1), are similar to the methods used by [1] and [6].

This paper is organized as follows: Section I contains the results and the propositions and lemmata used in the proofs. The proofs themselves are presented in Section II. As far as it is needed the necessary parts of the proofs from [17] are reproduced only slightly changed in this paper for the convenience of the reader.

Acknowledgement: The second author is grateful to DAAD for support. Helpful comments from an anonymous referee to an earlier version of this paper are also gratefully acknowledged.

Notation

$\mathbb{Q}, \mathbb{Q}_p, \mathbb{Z}, \mathbb{Z}_p, \mathcal{O}_K$ denote the field of rationals and p-adic rationals, the ring of rational and p-adic rational integers respectively, and the ring of integers of an algebraic number field K. We consider $\mathcal{O}'_K$ to be the intersection of valuation rings of all ramified prime ideals $\mathfrak{p} \in \mathcal{O}_K$ (if $K \neq \mathbb{Q}$). $Tr_{K/L}$ denotes the trace map from K to L. $\mathrm{GL}_n(R)$ denotes the general linear group over R. $[E : F]$ denotes the degree of the field extension E/F. I_m denotes the unit $m \times m$-matrix, $0_{n,m}$ and 0_m are zero $n \times m$ and $m \times m$-matrices, $e_{i,j}$ are square matrices having the only nonzero element 1 in the position (i,j), rank$M$ and det$M$ are rank and determinant of a matrix M. ${}^tM$ denotes a transposed matrix for M, $diag(d_1, d_2, \dots, d_m)$ is a block-diagonal matrix having diagonal components $d_1, d_2, \dots, d_n$. We suppose that K is a Galois extension of the rationals $\mathbb{Q}$. 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, e_i is the order of $\Gamma_i(\mathfrak{p})$ for $i \geq 1$, while $e = e_0$ is the order of the inertia group. 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 $g \in G$. Throughout this paper ζ_m denotes a primitive m-th root of unity.

1. Statement of the main results

1.1. Let E/F be a normal extension of algebraic number fields, and let $\Gamma_{E/F} = \mathrm{Gal}(E/F)$ be its Galois group. We consider the problem of integral realizations of finite subgroups G of the general linear group $\mathrm{GL}_n(E)$ that are stable under the natural action of $\Gamma_{E/F}$ on the matrices of the group G.

Let $\mathcal{O}_F$ and $\mathcal{O}_E$ denote the maximal orders of the number fields F and E respectively. Let us introduce the class $C(F)$ of fields normal over F that are obtained by adjoining to F all coefficients of matrices contained in some finite $\Gamma_{E/F}$-stable group $G \subset \mathrm{GL}_n(\mathcal{O}_E)$.

In [3] it is shown that if $F = \mathbb{Q}$ and the class $C(\mathbb{Q})$ contains some field $K \neq \mathbb{Q}$, then $C(\mathbb{Q})$ will also contain some field $K_1 \neq \mathbb{Q}$, $K_1 \subset K$ such that there exists only one prime p ramified in K_1. In this paper we use some properties of Galois groups for fields having restricted ramification. In general, the existence of global fields with a given Galois group and prescribed local properties for ramification is a rather subtle question. L. Moret-Bailly proved the existence of extensions of number fields that have prescribed local structure of ramification over a given set of prime divisors and unramified elsewhere for certain relative extensions [22]. In our case we deal with absolute extensions of the rationals $K/\mathbb{Q}$, and we fix the only ramified prime p. Let $C_p(\mathbb{Q})$ denote the class of fields in $C(\mathbb{Q})$ with the unique ramified prime p. Nilpotent extensions of $\mathbb{Q}$ having this property were described by Markshaitis in [18], but there are many examples of extensions in $C_p(\mathbb{Q})$ that are not nilpotent, and also nonsolvable extensions unramified outside p; for this and also for non-existence theorems compare [27], [7]. Both conjectures 1 and 2 are true for nilpotent extensions $K/\mathbb{Q}$ (see [3], [8]), and the proof of this fact uses the special structure of the Galois group of nilpotent extensions unramified outside a prime p [18].

1.2. It is well known, that the problem of description of fields $\mathbb{Q}(G)$ can be reduced to the case of commutative groups G of exponent p. Compare Proposition 1 in [17] and section 3 of [19] and [20] chapter 4. The idea of this reduction appears already in [14], [15], [13] and [10] where it was used, in particular, to study conditions for coefficients of the representations of nilpotent groups over integral rings providing their diagonalizability.

Hence, if there would be a counterexample to conjecture 1 or conjecture 2, there would exist also an elementary abelian p group G as a counterexample.

We use also reduction to the case of a $GL_n(\mathbb{Q})$-irreducible group G. Here a matrix group G is reducible in $GL_n(R)$ or simply R-reducible (R a ring or a field) if there exist $h \in GL_n(R)$ such that

$$h^{-1}Gh \subset \begin{vmatrix} G_1 & * \\ 0 & G_2, \end{vmatrix},$$

and G is irreducible otherwise.

We note that the reduction to the case of an irreducible group G can be done using the following lemma:

Lemma 1.2.1. *Let E/F be a normal extension of algebraic number 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 $G_1, G_2, \ldots, G_r$, then $F(G)$ is the composite of the fields $F(G_1), F(G_2), \ldots, F(G_r)$.*

The proof of this Lemma is given at the beginning of section II.

1.3. The essential results of this note can be summarized as follows:

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

Let μ_p denote the multiplicative group scheme over $\mathbb{Z}$ of order p and α_p the constant group scheme of order p (see [28] and [1]). Due to the results of [1] and [6] in conjunction with [20] one gets immediately the following

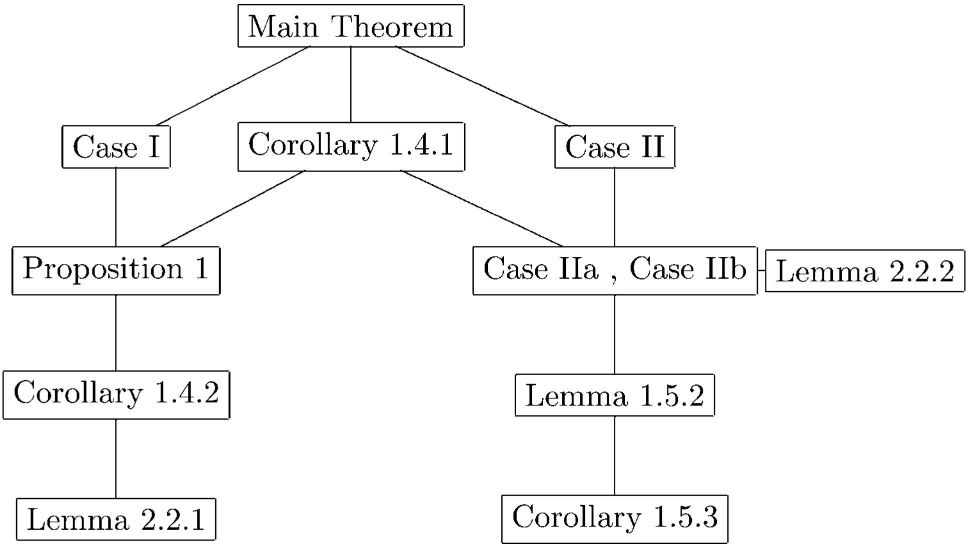
Corollary 1. *If G is a finite flat commutative group scheme over $\mathbb{Z}$ annihilated by a prime p, then it is a direct sum of copies of μ_p, α_p and, if $p = 2$, the nontrivial element in $Ext(\alpha_2, \mu_2)$.*

We can also express the result of the Main Theorem in the following form:

Corollary 2. *A finite flat group scheme $\mathfrak{G}$ over $\mathbb{Z}$ satisfies $\mathfrak{G}(\overline{\mathbb{Q}}) = \mathfrak{G}(\overline{\mathbb{Q}}_{ab}), \overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ and $\overline{\mathbb{Q}}_{ab}$ the maximal abelian (over $\mathbb{Q}$) subextension of $\overline{\mathbb{Q}}$.*

For the proof of the Main Theorem we distinguish essentially two cases and for their treatment we need several results which are recorded in the subsequent sections 1.4 and 1.5. The first Proposition 1 gives a criterion for the existence of integral realizations of an abelian matrix group. It shows that the existence of G in question is possible only if certain determinants d_k are divisible by the root of the discriminant D of a certain extension of number fields (for the details see section 1.4 below). In the proof of the Main Theorem in section II we use this for a certain cyclic extension E/F which is tame with respect to a fixed prime ideal (case I). Assume that $E/\mathbb{Q}$ is not abelian. Then we can make E/F to be a Kummer extension via adjoining appropriate roots of 1. We use the explicit Kummer basis to find an index k for which $\sqrt{D}$ does not divide d_k. The proof of the Main Theorem is divided in to two parts depending on the ramification index $e = e_0$ of $\mathbb{Q}(G)$. In the first part we use Proposition 1. In the second part we use lemma 1.5.2 and the Corollary 1.5.3 of section 1.5.

We can sketch the scheme of the proof of the Main Theorem:



Let us outline the idea of the proof of the Main Theorem in more detail for the convenience of the reader.

The outline of the proof of the Main Theorem.

In virtue of the argument of [3], lemmata 1 and 2 (compare also Theorem 2 in [19]), we can assume that K is unramified outside a prime p, so we can fix this prime. Since as already remarked in the introduction the particular case of field extensions $K/\mathbb{Q}$ which are unramified outside 2 follows in full generality from [20], we can restrict ourself to the case $p > 2$. We can also assume that G is an abelian group of exponent p, and we can consider G to be irreducible under conjugation in $GL_n(\mathbb{Q})$ by Corollary 1.4.1. The proof of the Main Theorem consists of a reduction to special cases, and these special cases are treated with different methods.

For number fields E, L be let $\mathcal{O}'_E, \mathcal{O}'_L$ denote the semilocal rings that are obtained by intersection of the valuation rings of all ramified prime ideals in the rings $\mathcal{O}_E, \mathcal{O}_L$ respectively. These semilocal rings are known to be principal ideal domains. Denote $G_0 = G^{\Gamma_1(\mathfrak{p})}$ 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. Let e'_0 be the ramification index of $\mathbb{Q}(G_0)$ over $\mathbb{Q}$ with respect to $\mathfrak{p}$. Then $e'_0 \leqslant e_0/e_1$ (= the index of $\Gamma_1(\mathfrak{p})$ in $\Gamma_0(\mathfrak{p})$.)

Case I.

Assume that e'_0 does not divide $p-1$. In this case we apply Proposition 1 to a certain subgroup $\overline{G_0} \subset G^{\Gamma_1(\mathfrak{p})} \subset GL_n(\mathcal{O}'_E)$ for a certain cyclic Kummer extension E/F with a convenient power basis $\pi^i, i = 0, \dots, t-1$ and with the explicit action of the generating element σ of order t of the Galois group on the uniformizing element π of O'_E, namely $\pi^\sigma = \pi\zeta_t$, which is convenient for applying Proposition 1 explicitly. Here E and F are the ramification field and the inertia field for some prime divisor $\mathfrak{p}$ of p adjoined by a primitive t-root of 1, $t = e'_0$.

Denote Γ_E/F the Galois group of E/F. In case I we determine a Γ_E/F-stable subgroup $\overline{G_0} \subset G_0$ which is generated by all conjugates $h^\gamma, \gamma \in \Gamma_E/F$ of some element $h \in G_0$. $\overline{G_0}$ can not be cyclic provided $t = e'_0$ does not divide $p-1$, and this is just the case where the arguments in case II (see below) can not be applied. So we start the proof of the Main Theorem just from this most difficult case, and apply Proposition 1 to a subgroup $\overline{G_0} \subset G$. We show that case I is impossible since the conditions of Proposition 1 never hold true for $\overline{G_0}$ and the extension E/F. In particular, if e_0' does not divide $p-1$ we have a contradiction with the condition $G \subset GL_n(\mathcal{O}_E)$ which can not hold true since $\overline{G_0} \not\subset GL_n(\mathcal{O}_E')$.

Case II.

Let us suppose that e_0' divides $p-1$. In this case we can suppose without loss of generality, that K contains a p-th root of unity ζ_p (see Lemma 2.2.2 below). Using a local argument on the diagonalization of matrices which are congruent to I_n modulo the prime ideal $\mathfrak{p}$ (see Corollary 1.5.3 below) a certain subgroup G_1' in G is constructed such that $K^{\Gamma_1(\mathfrak{p})}(G_1')$ is an extension of $K^{\Gamma_1(\mathfrak{p})}$ with $\zeta_p \in K^{\Gamma_1(\mathfrak{p})}(G_1')$, tame ramification index $p-1$ and $K^{\Gamma_1(\mathfrak{p})}(G_1')/K^{\Gamma_1(\mathfrak{p})}$ is an elementary abelian Kummer extension. In a second step a careful study of the Galois-action of $\Gamma_0(\mathfrak{p})$ on G_1' shows that the constructed group G_1' can not exist. This gives then the desired contradiction.

1.4. In this section we formulate the mentioned criterion for the existence of an integral realization of an abelian group G with the properties mentioned above.

Let E, L be finite Galois extensions of the number field F that are different from F with Galois groups $\Gamma_{E/F}$ and $\Gamma_{L/F}$ respectively. As above let $\mathcal{O}_E'$, $\mathcal{O}_L'$ be the semilocal rings that are obtained by intersection of the valuation rings of all ramified prime ideals in the rings $\mathcal{O}_E$, $\mathcal{O}_L$, and let $\mathcal{O}_F' = F \cap \mathcal{O}_E'$. Let $w_1, w_2, \dots, w_t$ be a basis of $\mathcal{O}_E'$ over $\mathcal{O}_F'$, and let D be the discriminant of this basis. Suppose that some matrix g of prime order p has coefficients in E and all $\Gamma_{E/F}$-conjugates $g^\gamma, \gamma \in \Gamma_{E/F}$ 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 $L = E(\zeta_p), \zeta_p$ 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 a numberfield containing $F(G)$ which is 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 can prove the following

Proposition 1. *1) 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 $GL_n(\mathcal{O}_E')$ if and only if all determinants*

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

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

2) If any of the three sets of conjugates $\{g^\gamma, \gamma \in \Gamma_{E/F}\}, \{h^\gamma, \gamma \in \Gamma_{E/F}\}, \{(gh)^\gamma, \gamma \in \Gamma_{E/F}\}$ generates G and the corresponding eigenvalues of g and h given in 1) are $\zeta_{(1)}^g, \zeta_{(2)}^g, \dots, \zeta_{(t)}^g$ and $\zeta_{(1)}^h, \zeta_{(2)}^h, \dots, \zeta_{(t)}^h$ respectively, then the eigenvalues for the matrix gh in 1) can be chosen as products $\zeta_{(1)} = \zeta_{(1)}^{gh} = \zeta_{(1)}^g \zeta_{(1)}^h, \zeta_{(2)} = \zeta_{(2)}^{gh} = \zeta_{(2)}^g \zeta_{(2)}^h, \dots, \zeta_{(t)} = \zeta_{(t)}^{gh} = \zeta_{(t)}^g \zeta_{(t)}^h$.

Note that the conditions of Proposition 1 are always true if E is unramified over F since $D\mathcal{O}_E' = \mathcal{O}_E'$ in this case.

Corollary 1.4.1. *If there is an abelian $\Gamma_{E/F}$-stable subgroup $G \subset GL_n(O'_E)$ of exponent p generated by $g^\gamma, \gamma \in \Gamma_{E/F}$ 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 1 hold true even if G is not irreducible.

Corollary 1.4.2. *Let E/F be a normal extension of number fields with Galois group $\Gamma_{E/F}$. Let $G \subset GL_n(E)$ be an abelian $\Gamma_{E/F}$-stable subgroup of exponent p generated by g and all matrices $g^\gamma, \gamma \in \Gamma_{E/F}$, and let $E = F(G)$. Then G is conjugate in $GL_n(F)$ to $G' \subset GL_n(\mathcal{O}'_E)$ if and only if all eigenvalues of matrices $B_i, i = 1, \dots, t$ are contained in $\mathcal{O}'_L$, where $L = E(\zeta_p)$. The latter happens if and only if the criterion of Proposition 1, 1) holds true, i.e. all determinants*

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

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

Corollary 1.4.3. *Let $F = \mathbb{Q}$. If there is an abelian $\Gamma_{E/\mathbb{Q}}$-stable subgroup $G \subset GL_n(O_E)$ of exponent p generated by $g^\gamma, \gamma \in \Gamma_{E/\mathbb{Q}}$ such that $E = \mathbb{Q}(G) \neq \mathbb{Q}$, then the $GL_n(\mathbb{Q})$-irreducible components $G_i \subset GL_{n_i}(E), i = 1, \dots, k$ of G are conjugate in $GL_{n_i}(\mathbb{Q})$ to subgroups $G'_i \subset GL_{n_i}(O_E)$ such that $E = \mathbb{Q}(G_1)\mathbb{Q}(G_2)\dots\mathbb{Q}(G_k)$. In particular, $\mathbb{Q}(G_i) \neq \mathbb{Q}$ for some indices i.*

1.5. For the proof of the Main Theorem (more precisely for the part of the proof dealing with case II) we use a lemma which is a variation on a theme of Minkowski [21] and is – like in the earlier related work [2], [3] - the key ingredient in the proofs of Lemma 1.5.2 and the Main Theorem. For the proof see [11]. Compare also [19], Proposition 1.

Lemma 1.5.1. *Let J be an ideal in Dedekind ring S of characteristic $\chi, 0 \neq J \neq S$, let g be an $n \times n$-matrix of finite order congruent to $I_n(\mathrm{mod}\ J)$.*

(i) If $\chi = p > 0$, then $g^{p^j} = I_n$ for some integer j. If $\chi = 0$, then J contains a prime number p and $g^{p^j} = I_n, i \in \mathbb{Z}$. In particular, any finite group of matrices congruent to $I_n(\mathrm{mod}\ J)$ is a p-group.

(ii) Let $\chi = 0, J = \mathfrak{p}$ be a prime ideal having the ramification index e with respect to $p, g \equiv I_n(\mathrm{mod}\ \mathfrak{p}^r)$ and $mp^{i-1}(p-1) \leq e/r < p^i(p-1), i \geq 0, m = min\{1, i\}$. Then $g^{p^i} = I_n$. In particular, any finite group of matrices congruent to $I_n(\mathrm{mod}\ \mathfrak{p}^t)$ is trivial if $e < t(p-1)$.

Related to these properties is the following

Lemma 1.5.2. *Let $\mathcal{O}$ be a Dedekind ring in an algebraic number field, and let $\zeta_p \in \mathcal{O}$. Let $p = \mathfrak{p}^e, e = p-1$. Let G be a finite subgroup of $GL_n(\mathcal{O})$ and $g \equiv I_n(mod\ \mathfrak{p})$ for all $g \in G$. Then G is conjugate in $GL_n(\mathcal{O})$ to an abelian group of diagonal matrices of exponent p.*

Corollary 1.5.3. *Let L be an extension of $\mathbb{Q}$ and $\mathfrak{p}$ a prime ideal in the field $L(\zeta_p)$. Suppose that L is unramified at $\mathfrak{p}$ and let $\mathcal{O}_{\mathfrak{p}}$ denote the valuation ring of the ramified prime ideal $\mathfrak{p}$ in $L(\zeta_p)$. Let Γ denote the Galois group of $L(\zeta_p)$ over L. If G is a finite Γ-stable subgroup of $GL_n(\mathcal{O}_{\mathfrak{p}})$ consisting of matrices $g, g \equiv I_n (\mathrm{mod}\ \mathfrak{p})$, then G is conjugate in $GL_n(L \cap \mathcal{O}_{\mathfrak{p}})$ to an abelian group of diagonal matrices of exponent p.*

2. Proofs

2.1. **Proof of Lemma 1.2.1.** Let

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

for $h \in GL_n(F_1)$. If there exists $g \in G$ such that $g^\gamma \neq g$ for some automorphism γ of $F(G)$ over $F(G_1)F(G_2)\dots F(G_r)$, then $g' = g^\gamma g^{-1} \neq I_n$. The blocks G_i in $h^{-1}Gh$ are stable under the action of γ, since $h \in GL_n(F_1)$ and the elements of $F(G_i)$ are fixed by γ. Because

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

and

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

are matrices having the same diagonal components, all eigenvalues of the matrix $g' = g^\gamma g^{-1}$ of finite order are 1 and hence $g' = I_n$. This contradiction completes the proof of Lemma 1.2.1. □

Proof of Proposition 1. One proof (namely of the first part) is given in the paper [17]. The second part of proposition 1, which is important for the proof of the Main Theorem, follows from the construction given in [17]. But for convenience we give here a proof for the proposition, which is shorter than in [17].

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

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

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 $g^{\sigma_j}, i, j = 1, 2, \dots, t$:

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

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 [26], page 8, Corollary 3 for example). So if one of the eigenvalues of B_i is in $\mathcal{O}'_L$ then all of them are since they are Galois conjugate. Using the dual basis $w_1^*, \dots, w_t^*$ to $w_1, \dots, w_t$ with respect to the traceform 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 $B_i, i = 1, \dots, t$ are conjugate in $GL_n(F)$ to matrices $B'_i \in M_n(\mathcal{O}'_F)$, since for the generator g of G the equation

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

holds with $B_i \in M_n(F)$ and $w_1, \dots, w_t$ a basis of $\mathcal{O}'_E$ over $\mathcal{O}'_F$. In fact each semisimple matrix $B_i \in M_n(F)$ is conjugate in $\mathrm{GL}_n(F)$ to a matrix from $M_n(\mathcal{O}'_F)$ if and only if all its eigenvalues are contained in $\mathcal{O}'_L$ (see Lemma 2.1.1 below).

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

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

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

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

The cofactor expansion for determinants implies $\lambda_k = d_k / detW$ and therefore the eigenvalues of B_k are in $\mathcal{O}'_L$ iff $detW$ divides d_k, which proves the criterion of Proposition 1 and - by definition of the eigenvalues t_i - also the second statement modulo the proof of the following

Lemma 2.1.1. *i) Let all eigenvalues $\lambda_j, j = 1, 2, \dots, k$ of the semisimple matrices $B_i \in M_n(F), i = 1 \dots, t$ be contained in the ring $\mathcal{O}'_L$ for some field $L \supset F$. Then B_i are conjugate in $GL_n(F)$ simultaneously to matrices that are contained in $M_n(\mathcal{O}'_F)$.*

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

Proof of Lemma 2.1.1. i) By the virtue of [26], chapter 1, sect. 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 $\mathcal{O}'_A$ over $\mathcal{O}'_F$. Then for any $B \in A$ we have $B = b_1 a_1 + \cdots + b_n a_n$, and the elements $b_i \in F$ are contained in $\mathcal{O}'_F$ iff $B \in \mathcal{O}'_A$. But all coefficients k_{ij} of the characteristic polynomials $f_i(x) = k_{i0} + k_{i1} x + \cdots + k_{in} x^n$ of the matrices B_i are contained in $\mathcal{O}'_L$, and $k_{in} = 1$, so $B_i \in A$ are integral over F. It follows that $B_i = b_{i1} a_1 + \cdots + b_{in} a_n$, and $b_{ij} \in \mathcal{O}'_F$. If $v \in F^n$ is a non-zero vector in F^n, then $a_1 v, a_2 v, \dots, a_n v$ is a basis of F^n, and $B_i a_j v = \Sigma_k c_{ijk} a_k v$, where $c_{ijk} \in \mathcal{O}'_F$. It follows that for any i the matrix $C_i = [c_{ijk}]_{k,j}$ belongs to $GL_n(\mathcal{O}'_F)$, and C_i is the matrix of the operator B_i in the basis $a_1 v, a_2 v, \dots, a_n v$ 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 $f_i(x) = k_{i0} + k_{i1} x + \cdots + k_{in} x^n$ of the matrices B_i. Since $k_{in} = 1$ and all k_{ij} are in $\mathcal{O}'_F$ all roots of $f(x)$ are in $\mathcal{O}'_L$. This completes the proof of Lemma 2.1.1. □

Remark. *In the situation of Lemma 2.1.1, i) the F-algebra $A = F[B_1, \ldots, B_t]$ is isomorphic to the field $L = F[\lambda_1, \ldots, \lambda_k]$ where $\lambda_j,\ j = 1, 2, \ldots, k$ are all eigenvalues of the matrices $B_i, i = 1 \ldots, t$.*

Proof of Corollary 1.4.1. If $G \subset GL_n(\mathcal{O}'_E)$ is a group of exponent p and $g = B_1w_1 + B_2w_2 + \cdots + B_tw_t$ for a basis $w_1, \ldots, w_t$ of $\mathcal{O}'_E$ over $\mathcal{O}'_F$, then $B_i \in M_n(\mathcal{O}'_F)$, and it follows from Lemma 2.1.1 that the eigenvalues of B_j are contained in $\mathcal{O}'_L$. But eigenvalues are preserved under conjugation, so the latter claim is also true for all components G_i. We can apply Proposition 1 to $G_i, i = 1, \ldots, k$. It follows that G_i are conjugate to subgroups $G'_i \subset GL_{n_i}(O'_E)$. Now, Lemma 1.2.1 implies $E = F(G_1)F(G_2)\ldots F(G_k)$. This completes the proof of Corollary 1.4.1. □

Proof of Corollary 1.4.2. Let

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

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

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

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

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

are divisible by $\sqrt{D}$ in the ring $\mathcal{O}'_L$. But $F(G) = F(G_1)F(G_2)\ldots F(G_k)$ by the Lemma in section 1.2, and so $L = L_1L_2\ldots L_k$. This completes the proof of Corollary 1.4.2. □

Proof of Corollary 1.4.3. The argument of the proof of Corollary 1.4.1 remains true for the rings of integers $\mathcal{O}_E$ and $\mathbb{Z}$ in E and $F = \mathbb{Q}$ since $\mathbb{Z}$ is a principal ideal domain and $\mathcal{O}_E$ has a free basis over $\mathbb{Z}$. Therefore, the rest of the proof of Corollary 1.4.3 reproduces the proof of Corollary 1.4.1 with $\mathcal{O}_E$ and $\mathbb{Z}$ instead of $\mathcal{O}'_E$ and $\mathcal{O}'_F$ respectively. □

2.2. **Proof of the Main Theorem.** Let us suppose that there exist a counterexample G to the Main Theorem with corresponding Galois extension $K/\mathbb{Q}, K = \mathbb{Q}(G)$ with Galois group $\Gamma := \Gamma_{K/\mathbb{Q}}$. In virtue of Lemmas 1 and 2 in [3] or Theorem 2 in [19] we can assume the field K to be unramified outside the fixed prime p. Since as already remarked above the particular case of field extensions $K/\mathbb{Q}$ which are unramified outside 2 follows in full generality from [20], we can restrict our self to the case $p > 2$. Because of the Proposition in section 1.2 we can also suppose that G is an abelian group of exponent p and we can consider G to be irreducible under conjugation in $GL_n(\mathbb{Q})$ by Corollary 1.4.3. Let us assume that G is a counterexample of minimal order of this kind. With the notation of the beginning of this note let $\Gamma_i(\mathfrak{p}) \subset \Gamma$ denote the i-th ramification groups of the prime divisor $\mathfrak{p}$ for $i \geq 1$ and $\Gamma_0(\mathfrak{p})$ the inertia group in Γ. Let $G_0 = G^{\Gamma_1(\mathfrak{p})}$ denote 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. Let e_0' be the ramification index of $\mathbb{Q}(G_0)$ over $\mathbb{Q}$ with respect to $\mathfrak{p}$. Then $e_0' \leqslant e_0/e_1$(= the index of $\Gamma_1(\mathfrak{p})$ in $\Gamma_0(\mathfrak{p})$.) We distinguish two cases: Case I : e_0' does not divide $p-1$ and Case II : e_0' is a divisor of $p-1$.

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

1) In this case, where e_0' does not divide $p-1$, let us fix p and one of its ramified prime divisors say $\mathfrak{p}$. Let E_1 and F_1 denote the subfields of $\Gamma_1(\mathfrak{p})$-fixed elements and $\Gamma_0(\mathfrak{p})$-fixed elements of K respectively. We will prove that for $p \neq 2$ and a field K which has discriminant p^j, $j \in \mathbb{Z}$, all $\Gamma_0(\mathfrak{p})/\Gamma_1(\mathfrak{p})$-stable finite subgroups G of $\mathrm{GL}_n(\mathcal{O}_{E_1'})$ are already in $\mathrm{GL}_n(\mathcal{O}_{F_1})$ for $E_1' = F_1(G^{\Gamma_1(\mathfrak{p})}) = F_1(G_0) \subset K^{\Gamma_1(\mathfrak{p})}$ and $F_1 = K^{\Gamma_0(\mathfrak{p})}$. We can extend the ground field F_1 by adjoining ζ_t, $t = e_0'$. Set $E = E_1(\zeta_t)$ and $F = F_1(\zeta_t)$. We obtain a cyclic extension E/F such that $\zeta_t \in F$ for $t = e_0'$. Since K is unramified outside $p, \mathbb{Q}(\zeta_t)$ and K have intersection $\mathbb{Q}$ and therefore we can identify the Galois group $\Gamma_{E/F} = Gal(E/F)$ with the Galois group $Gal(E_1/F_1)$. With respect to this extension of the corresponding Galois action to E/F we obtain a $\Gamma_{E/F}$-stable group $G_0 \subset \mathrm{GL}_n(\mathcal{O}_E)$. E/F is a tame extension with respect to $\mathfrak{p}, t = e_0'$ is its ramification index and $p-1 \geq 2$. We have the following conditions for local ramification: $\mathfrak{p}_E^{e_0'} = (p) = (\zeta_p - 1)^{p-1}$ as ideals of the ring $\mathcal{O}_{E_\mathfrak{p}(\zeta_p)}$, where $\mathfrak{p}_E$ is the prime divisor of p in $\mathfrak{p}$-adic completion $E_\mathfrak{p}$ of E. It is clear that $\left(\left[\frac{e_0'}{2}\right] + 1\right)(p-1) > e_0'$. Hence $\mathfrak{p}^{[t/2]+1}$ does not divide $(\zeta_p - 1)$ as ideals of $\mathcal{O}_{E(\zeta_p)}$. We can also assume that G is an abelian p-group of exponent p, and $E \neq F$ because $e_0' > 1$ in the case I. We use the statement of Proposition 1 and its Corollary 1.4.2 for the rings $\mathcal{O}_E'$ and $\mathcal{O}_F'$ and a basis $1, \pi, \ldots, \pi^{t-1}$, such that $\pi^t \in F$. If $\Gamma_{E/F}$, the Galois group of E/F, is generated by an element σ of order t, we can consider the action of $\Gamma_{E/F}$ on the basis $1, \pi, \ldots, \pi^{t-1}$ in the following way: $(\pi^i)^\sigma = \pi^i \zeta_t^i$. Then

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

Let us consider the determinants of the matrices W_j that are obtained from W by changing elements of j-th column of $W = [(\pi^i)^{\sigma^j}]_{i,j}$ to appropriate p-roots $\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(t)}$ of 1 that are the eigenvalues of the matrices $g^{\sigma^i}, i = 1, 2, \ldots, t$ for some $g \in G$, according to Proposition 1. For simplicity let $\zeta = \zeta_t$, but reserve previous notation for ζ_p for the rest of this proof.

Recall, that G is supposed to be a minimal counterexample to the Main Theorem and that K is unramified outside p. In the proof of the Case I we pick $g \in G_0 = G^{\Gamma_1(\mathfrak{p})}$ and a generator σ of the Galois group of E over F; by our assumption, the order t of σ does not divide $p-1$. There is a matrix $g \in G_0$ such that matrices $g^\gamma, \gamma \in \Gamma$ generate G. Indeed, if matrices $g^\gamma, \gamma \in \Gamma$ generated a proper subgroup G_1 of G for any $g \in G_0$, then G_1 would be a group of A-type, since G is a minimal counterexample, and the order of e_0' would divide $p-1$ (because $\mathbb{Q}(G_1)/\mathbb{Q}$ is unramified outside p and tamely ramified at $\mathfrak{p}$), contrary to the assumption of the Case I. Let us fix the above G and σ. We need the following auxiliary lemma which specifies the option of g for our proof of the case I:

Lemma 2.2.1. *Let k be an integer such that $0 < k < p$. There is a matrix $g \in G_0$ such that matrices $g^\gamma, \gamma \in \Gamma$ generate G, and the group G is generated by all $h^\gamma, \gamma \in \Gamma$, where $h := g^k g^\sigma$.*

Proof of Lemma 2.2.1. Take a matrix $g \in G_0$ such that matrices $g^\gamma, \gamma \in \Gamma$ generate G. If a group H generated by all $h^\gamma, \gamma \in \Gamma$ is a proper subgroup of G, it is a group of A-type, and it is fixed elementwise by the commutator subgroup Γ' of Γ. Then $g^\sigma = g^{-k}h = g^l h$ for $l \equiv -k (mod p)$. We have $g^{\sigma^2} = g^{l^2} h^l h^\sigma, \ldots, g^{\sigma^{p-1}} = g^{l^{p-1}} h_0 = g h_0$ for some matrix h_0 having coefficients fixed by Γ'. Since $h \in G_0, G_0$ is fixed by $\Gamma_1(\mathfrak{p})$ and K is unramified outside p, we have $h \in GL_n(\mathbb{Q}(\zeta_p))$. But $\zeta_p^{\sigma^{p-1}} = \zeta_p$, and we also have $g^{\sigma^{i(p-1)}} = g h_0^i$, so for $i = p$ we obtain $g^{\sigma^{p(p-1)}} = g$. The same argument is true for elements g_1, h_1 such that $g_1 = g^\tau \in G_0 (\tau \in \Gamma)$ and $h_1 = g_1^k g_1^\sigma$ taken instead of g, h. We have $g_1^{\sigma^{p(p-1)}} = g_1$. But G_0 is covered by subgroups generated by all elements $g_1 = g^\tau$ since G is generated by elements $g_1 = g^\gamma, \gamma \in \Gamma$. Therefore, $\sigma^{p(p-1)}$ acts trivially on G_0. But the order of σ is coprime to p. We conclude that the order of σ divides $p-1$, which contradicts the assumption of the Case I. It follows that either the group H or the group H_1 generated by all $h_1^\gamma, \gamma \in \Gamma$ coincides with G. In the latter case we can rename matrix g_1 to g. This completes the proof of Lemma 2.2.1.

We distinguish the cases of odd and even t, the order of σ. If t is odd, we need a matrix g' having at least one eigenvalue $\theta_i = \zeta_{(i)} = 1$ (we use notations of Proposition 1) such that G is generated by all conjugates $g'^\gamma, \gamma \in \Gamma$. For an even t we have to choose $g' = g^k g^\sigma \zeta_p^s$. The choice of the eigenvalues $\zeta_{(i)}$ (see Proposition 1) ensures that the product of the corresponding eigenvalues are in accordance with the product of two matrices $h_1, h_2 \in G$ (compare the proof of Proposition 1).

Now, we intend to replace G_0 by a smaller subgroup $\overline{G}_0$ generated by a single element of G_0 which also satisfies the conditions of the Case I.

G_0 is covered by its $\Gamma_{E/F}$-stable subgroups G_γ, where G_γ are generated by elements $(\hat{g}^\gamma)^{\sigma^i}, i = 1, 2, \ldots, t$ for some $\gamma \in \Gamma$ and any $\hat{g}$ such that $\hat{g}^\gamma \in G_0$ and all $\hat{g}^\tau, \tau \in \Gamma$, generate G. By definition, G_γ is generated by the orbit of an element g having the above property. But if h satisfies the conditions of the above Lemma, the elements $\hat{g}^\tau, \tau \in \Gamma$ generate G for $\hat{g} = h^{\gamma^{-1}}$, so we can assume that G_γ is generated by elements $h^{\sigma^i}, i = 1, \ldots, t$ for a given γ and some $h \in G$ satisfying the conditions of the above Lemma. Since the ramification index with respect to $\mathfrak{p}$ of the composite of the fields $F(G_\gamma), \gamma \in \Gamma$, does not divide $p-1$, there is $\gamma \in \Gamma$ such that the ramification index $e(F(G_\gamma)/F)$ of $F(G_\gamma)$ does not divide $p-1$. Let us briefly explain this claim. The field $F(G_0)$ is a composite of fields $E_i = F(G_{\gamma_i})$, and $F(G_0)/F$ is a cyclic totally ramified extension whose Galois group is generated by an element $\overline{\sigma}$ of order $\overline{t}$ equal to the ramification index of $F(G_0)/F$ in $\mathfrak{p}$. So E_i/F are also cyclic totally ramified extensions, and their Galois groups are generated by elements σ_i of orders equal to the ramification indices t_i of E_i/F. Therefore, if all t_i divide $p-1$, then the order of $\overline{\sigma}$ must also divide $p-1$, because $\overline{\sigma}$ is a product of pairwise commuting elements of orders t_i. This completes the proof of our claim.

Let us fix γ and denote $\overline{G_0} = G_\gamma$. The group $\overline{G_0}$ is not cyclic since the order of σ does not divide $p-1$ in the case I. Using Proposition 1 or, alternatively, Corollary 1.4.1 or Corollary 1.4.2 of Proposition 1, we will prove that $\overline{G_0} \subset GL_n(\mathcal{O}'_F)$. Below we use $\Gamma_{E/F}$-stability of G_0 in order to apply Proposition 1 to $\overline{G_0} \subset G_0$ generated by all $(h^\gamma)^{\sigma^i}, i = 1, 2, \ldots, t$ for the fixed $\gamma \in \Gamma$. Since E/F is a cyclic Kummer extension, for $E' = F(\overline{G_0}) \subset E$ the extension E'/F is also a cyclic Kummer extension, and there are an integer $\bar{t}$ dividing $t, \bar{\sigma} \in \Gamma_{E/F}$ and a basis $1, \bar{\pi}, \bar{\pi}^2, \ldots, \bar{\pi}^{\bar{t}-1}$ such that $\bar{\pi}^{\bar{t}} \in F, \bar{\pi}^{\bar{\sigma}} = \bar{\pi}\zeta_{\bar{t}}$ and the Galois group $\Gamma_{E'/F}$ of E'/F is generated by $\bar{\sigma}$. Moreover, both extensions E/F and E'/F are totally ramified in $\mathfrak{p}$, and $\bar{t}$ is the ramification index of E'/F, so we have as earlier the following inequality: $\left(\left[\frac{\bar{t}}{2}\right] + 1\right)(p-1) > \bar{t}$, and $\mathfrak{p}^{[\bar{t}/2]+1}$ does not divide $(\zeta_p - 1)$.

Since p is odd and $\bar{t}$ does not divide $p-1$, we can assume that $\bar{t} > 2$. We will consider matrices

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

$j = 2, \ldots, \bar{t}$ that are obtained from W_j by subtracting first column of W_j from j-th column of W_j. For even $\bar{t}$ we may suppose that only $r \leqslant n-2$ elements from $\zeta_{(1)}, \zeta_{(2)}, \ldots, \zeta_{(\bar{t})}$, the eigenvalues of h, are distinct from 1. Indeed, we can choose two elements g_1 and g_2 of $\overline{G_0}$ generating a noncyclic subgroup of $\overline{G_0}$ in such a way that $\zeta_p^{\alpha_1}, \zeta_p^{\alpha_2}, \ldots$ and $\zeta_p^{\beta_1}, \zeta_p^{\beta_2}, \ldots$ compose the full set of eigenvalues of g_1 and g_2 respectively and $\alpha_1 \neq \alpha_2$. Set

$$k = \frac{-(\beta_1 - \beta_2)}{\alpha_1 - \alpha_2} \quad \text{and} \quad h = \zeta_p^s \cdot g_1^k g_2 \quad \text{for } s = -k\alpha_1 - \beta_1,$$

since we are calculating α_j, β_j and k modulo p we can find an integer k with this properties.

Then matrix h has two eigenvalues $\zeta_{(i)}$ for different i, and the group generated by $h^\gamma, \gamma \in \Gamma_{E'(\zeta_p)/F}$ ($\Gamma_{E'(\zeta_p)/F}$ denotes the Galois group of $E'(\zeta_p)/F$) is abelian of exponent p; we can still apply the criterion of Proposition 1 to the group $\overline{G_0}$ generated by matrices $h^\gamma, \gamma \in \Gamma_{E'/F}$. In other words, we can extend the group G_0, if it is needed, by adjoining some scalar matrices and naturally extending Galois action to them, and this does not change $\Gamma_{E/F}$-stability of G_0. For convenience we still preserve our previous notation. We can apply our construction to the matrix $h = \zeta_p^s \cdot g_0$ for some $g_0 \in G_0$ and if we show that this matrix is not contained in $GL_n(\mathcal{O}'_{E(\zeta_p)})$, then $g_0 \notin GL_n(\mathcal{O}'_E)$, and this contradiction is exactly the aim of our proof of the case 1). Denote $\Lambda = [\zeta^{(i-1)(j-1)}]_{i,j=1}^{\bar{t}}$. Note that Λ is a symmetric matrix. Let

$$\begin{aligned} \det W_j &= det\ M_j = \theta_{j1}(\zeta_{(1)} - 1) + \theta_{j2}(\zeta_{(2)} - 1) + \cdots + \theta_{j\bar{t}}(\zeta_{(\bar{t})} - 1), \quad \text{where} \\ \theta_{jk} &= (-1)^{j+k}\bar{\pi}^{\bar{t}(\bar{t}-1)/2-(j-1)} \cdot \frac{\zeta^{-(j-1)(k-1)}}{\bar{t}} \cdot c = \bar{\pi}^{\bar{t}(\bar{t}-1)/2-(j-1)} \cdot \frac{\lambda_{jk}}{\bar{t}}, \end{aligned}$$

for

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

and $\lambda_{jk} = (-1)^{k+j}\zeta^{-(j-1)(k-1)} = \lambda_{kj}$. Indeed, denote $\Lambda^{-1} = [\frac{\zeta^{-(j-1)(i-1)}}{\overline{t}}]_{i,j=1}^{\overline{t}}$, and so (ij)-th cofactor of W_j is $(-1)^{j+i} \cdot \frac{\zeta^{-(j-1)(i-1)}}{\overline{t}} \cdot c$. Let us consider the element δ from the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ such that $\delta : \zeta \to \zeta^{-1}$, and so $\delta \neq 1, \delta^2 = 1$. δ acts as a complex conjugation on t-th roots of 1. Note that for a $\overline{t}$-root η of 1 $\eta^\delta = \eta$ iff $\eta^{-1} = \eta$ or, equivalently, $\eta = \pm 1$. Let us determine some properties of the above elements λ_{ij} under δ-action. Since the number of rows in Λ that are permuted under δ-action is equal to $\phi(\overline{t})$, the Euler function, we have $c^\delta = c$ if $\phi(\overline{t})/2$ is even and $c^\delta = -c$ if $\phi(\overline{t})/2$ is odd. Furthermore, δ permutes i-th row and $(\overline{t} + 2 - i)$-th row of the matrix Λ for $1 < i < 1 + \overline{t}/2$, and $(-1)^{i+j} = (-1)^{\overline{t}-i+j} = (-1)^{\overline{t}}(-1)^{i+j}$. Therefore, if both $\overline{t}$ and $\phi(\overline{t})/2$ are even, or both $\overline{t}$ and $\phi(\overline{t})/2$ are odd, then $\lambda_{k,j}^\delta = \lambda_{k,\overline{t}-j+2} = \lambda_{\overline{t}-k+2,j}$ for $1 < j < 1 + \overline{t}/2$, otherwise $\lambda_{k,j}^\delta = -\lambda_{k,\overline{t}-j+2} = -\lambda_{\overline{t}-k+2,j}$. In the general case we can claim that $\lambda_{k,j}^\delta = s \cdot \lambda_{k,\overline{t}-j+2} = s \cdot \lambda_{\overline{t}-k+2,j}$ where $s = s(\overline{t}) = (-1)^{\overline{t}+\phi(\overline{t})/2} = \pm 1$ depends only on $\overline{t}$.

Let $\overline{t}$ be even, and let $\Lambda_1 = [\lambda_{ij}]_{i,j} = [(-1)^{i+j}\zeta^{-(i-1)(j-1)}]_{i,j}$. Then $\Lambda_1^{-1} = [\lambda_{i,j}]_{i,j}^{-1} = [(-1)^{i+j} \cdot \frac{\zeta^{(i-1)(j-1)}}{\overline{t}}]_{i,j}$, and it follows that cofactors of λ_{ij} are equal to $a_{ij} = \frac{\zeta^{(i-1)(j-1)}}{\overline{t}}$, and so all $a_{ij} \not\equiv 0(mod\mathfrak{q})$, in particular, $a_{1j} = \overline{t}^{-1}$. Let $C = [c_{ij}]$ be a $(\overline{t} - 1) \times (\overline{t} - 1)$- matrix obtained via eliminating the first row and the first column of Λ. Taking an expansion of a_{1i} by $\frac{\overline{t}}{2}$-th row of C we obtain: $\overline{t}^{-1} = c_{i1}A_{i1} + c_{i2}A_{i2} + \cdots + c_{i,\overline{t}-1}A_{i,\overline{t}-1}$ where A_{iu} are cofactors of the elements c_{iu} in the i-th row of C. It follows that for some m $A_{im} \not\equiv 0(mod\mathfrak{q})$. Now it is possible to fix integers $j = 1$ and m. We can use matrices $g_1 = g$ and $g_2 = g^\sigma$ for getting a matrix g' whose eigenvalues associated with j-th and m-th blocks are $\zeta_{(j)} = \zeta_{(m)} = 1$ (see Proposition 1, 2)) and the above Lemma. For this purpose take the eigenvalues $\zeta_p^{\alpha_1}$ and $\zeta_p^{\alpha_2}$ of g_1 and the eigenvalues '$\zeta_p^{\beta_1}$ and $\zeta_p^{\beta_2}$ of g_2 associated with j-th and m-th blocks respectively. If $\zeta_p^{\alpha_1} = \zeta_p^{\alpha_2}$, set $g' = \zeta_p^{\alpha_1}g$, otherwise set $g' = \zeta_p^s g_1^k g_2$ for $s = -k\alpha_1 - \beta_1$ and $k = \frac{-(\beta_1-\beta_2)}{\alpha_1-\alpha_2}$. Now we can apply Proposition 1 to the group $\overline{G_0}$ generated by all $h^{\sigma^i}, i = 1, \ldots, t$ for $h = g'$.

Let us consider a prime ideal $\mathfrak{q}$ in the ring of integers $\mathcal{O}$ of the field $\mathbb{Q}_p(\zeta_p, \zeta)$ such that $\mathfrak{q}$ divides p. Let us suppose that $\zeta_{(l)} \neq 1$ and the elements

$$\frac{(\zeta_{(1)} - 1)\lambda_{i1}}{\zeta_{(l)} - 1} + \frac{(\zeta_{(2)} - 1)\lambda_{i2}}{\zeta_{(l)} - 1} + \cdots + \frac{(\zeta_{(\overline{t})} - 1)\lambda_{i\overline{t}}}{\zeta_{(l)} - 1}, i = 1, 2, \ldots, \overline{t}$$

are divisible by $(\zeta_{(l)} - 1)$ in the ring $\mathcal{O}$, then the system of congruences

$$\begin{cases} x_1\lambda_{11} + x_2\lambda_{12} + \cdots + x_{\overline{t}}\lambda_{1\overline{t}} \equiv 0(\text{mod } \mathfrak{q}) \\ x_1\lambda_{21} + x_2\lambda_{22} + \cdots + x_{\overline{t}}\lambda_{2\overline{t}} \equiv 0(\text{mod } \mathfrak{q}) \\ \vdots \\ x_1\lambda_{\overline{t}1} + x_2\lambda_{\overline{t}2} + \cdots + x_{\overline{t}}\lambda_{\overline{t}\overline{t}} \equiv 0(\text{mod } \mathfrak{q}) \end{cases} \tag{S}$$

has a nontrivial solution

$$x_1 = 1, \quad x_2 = \frac{\zeta_{(2)} - 1}{\zeta_{(l)} - 1}, \quad x_3 = \frac{\zeta_{(3)} - 1}{\zeta_{(l)} - 1}, \ \cdots, \ x_{\overline{t}} = \frac{\zeta_{(\overline{t})} - 1}{\zeta_{(l)} - 1}.$$

Let us eliminate the first and the $(\overline{t}/2 + 1)$-th congruences from system (S), coefficients of which are equal to $(\lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{i\overline{t}}) = (1, 1, \ldots, 1)$ for $i = 1$ and $(1, -1, 1, -1, \ldots, 1, -1)$,