www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 7 No. 3 (2018), pp. 81-94.

www.ui.ac.ir

ON SOME INTEGRAL REPRESENTATIONS OF GROUPS AND GLOBAL IRREDUCIBILITY

DMITRY MALININ

Communicated by Patrizia Longobardi

Abstract. Arithmetic aspects of integral representations of finite groups and their irreducibility are considered with a focus on globally irreducible representations and their generalizations to arithmetic rings. Certain problems concerning integral irreducible two-dimensional representations over number rings are discussed. Let K be a finite extension of the rational number field and O_K the ring of integers of K. Let G be a finite subgroup of $GL(2, K)$, the group of (2×2)-matrices over K. We obtain some conditions on K for G to be conjugate to a subgroup of $GL(2, O_K)$.

1. Definitions and notation

We consider the arithmetic background of integral representations of finite groups over p-adic and algebraic number rings. Section 2 gives an exposition of the known results and the formulations of the new results of the paper in the end of the section, the proofs are given in section 3.

For the ring of integers O_K of an algebraic number field K, for which natural numbers is there a finite group $G \subset GL(n, O_K)$ such that $O_K G$, the O_K-span of G, coincides with $M(n, O_K)$, the ring of $(n \times n)$-matrices over ?O_K? The answer is known if n is an odd prime. In this paper we study the case $n = 2$ and some related questions; in the cases when the answer is positive for $n = 2$, for $n = 2m$ there is also a finite group $G \subset GL(2m, O_K)$ such that $O_K G = M(2m, O_K)$.

MSC(2010): Primary: 20C10; Secondary: 11R33.
Keywords: globally irreducible representations, arithmetic rings, number fields, class numbers, genera, Hilbert symbol, quaternions, Schur ring, torsion points of elliptic curves.
Received: 30 Nvember 2016, Accepted: 23 November 2017.

http://dx.doi.org/10.22108/ijgt.2017.100688.1402

.

We are interested in several aspects of integral representations. First of them is a generalization of the concept of global irreducibility for arithmetic rings (maximal orders of number fields or local fields), which has been introduced by F. Van Oystaeyen and A.E. Zalesskii. This generalization is formulated below. We are interested in further generalizations of this concept.

Let K be an algebraic number field and O_K its ring of integers. Let G be a finite subgroup of $GL(n, O_K)$ for some integer n; when does the O_K-span of G give the full matrix ring $M(n, O_K)$? More generally, for which rings $M(n, O_K)$ does such a group G exist? In the latter case we say that $M(n, O_K)$ is a Schur ring. For any commutative ring R, the matrix ring $M(n, R)$ is called a Schur ring if there exists a finite group $G \subset GL(n, R)$ such that G spans $M(n, R)$ over R. Again following notation used in [25] we write RG for the R-algebra spanned by G in $M(n, R)$ for given $G \subset GL(n, R)$. Using the terminology of [25] we say that a finite group $G \subset GL(n, F)$ over an algebraic number field F is globally irreducible if for every non-archimedian valuation v of F the reduction of $G \pmod v$ is absolutely irreducible. We refer to [4], chapters XI, XII for the theory of integral and modular representations and the concept of the reduction of representations. Let p be a prime positive integer. Then there is an appropriate finite extension K of $\mathbb{Q}$ such that the original representation $\rho : G \to GL(n, \mathbb{C})$ is equivalent to a representation in $GL(n, K)$. The ring R of p-integers in K is a principal ideal domain; let P be a maximal ideal in R containing p. Then ρ is equivalent to a representation $\rho' : G \to GL(n, R)$. Let $K_P = R/P$, then the representation ρ' determines modulo P another representation $\overline{\rho} : G \to GL(n, K_P)$, which is called a Brauer reduction of ρ modulo P, see [4, sect. 82]. The group $\overline{\rho}(G)$ is usually viewed as a subgroup of $GL(n, \overline{K}_P)$ where $\overline{K}_P$ is an algebraic closure of K_P. The map ρ' is not unique, however, according to the Brauer-Nesbitt theorem (cf. [4, Theorem 82.1]) the irreducible components of the image $\overline{\rho}(G)$ do not depend on the choice of ρ' as above. Hence the notion of globally irreducible representation is well defined. We are going to discuss this concept further in the next section. The term "globally irreducible representation" was introduced by B. Gross [12] for the case $R = \mathbb{Z}$, but the concept of global irreducibility in [12] is slightly different from one defined above.

Throughout the paper $\mathbb{C}$, $\mathbb{Q}$ and $\mathbb{Q}_p$ denote the fields of complex, rational and rational p-adic numbers, $\mathbb{Z}$ is the ring of rational integers .
$N_{E/F}(a)$ is the norm of $a \in E$ in the field extension E/F.

We denote by O_K the ring of integers of an algebraic number field K. C_K denotes the ideal class group of a number field K. I_K denotes the class number of a number field K, cl$M$ is a Steinitz class of a lattice M.

We write $GL(n, R)$ for the general linear group over a ring R, $SL(n, R)$ denotes the special linear group. $M(n, R)$ is the full $(n \times n)$-matrix algebra over a ring R. $[E : F]$ denotes the degree of the field extension E/F. Finite groups are usually denoted by capital letters G, H, and their elements by small letters, e.g. $g \in G$, $h \in H$, $\langle a, b \cdots \rangle$ denotes a group generated by $a, b, \ldots$, $Z = Z(G)$ is the center of G. We write ζ_t for a primitive t-root of 1. For a prime p $(\frac{a}{p})$ is the Legendre symbol.

http://dx.doi.org/10.22108/ijgt.2017.100688.1402

Let $G \subset GL(n, \mathbb{C})$; $F_\chi(G)$ denotes the field generated by the traces of all matrices in G over the field F, and $\langle G\rangle_R = RG$ denotes the R-span of G.

For a simple K-algebra KG, the Schur index of KG, is denoted by $s(K, G)$, but in the case $K = K_\chi(G)$ we denote by $s(G)$ the Schur index $s(KG, G)$ and speak about the Schur index of G.

2. Introduction and main results

Let K be an algebraic number field, and let O_K be its ring of integers.

Theorem 2.1. [25] *Let $G \subset GL(n, O_K)$. Then $\langle G\rangle_{O_K} = M(n, O_K)$ if and only if G is globally irreducible.*

One may expect that the existence of a globally irreducible subgroup $G \subset GL(n, K)$ should imply that $M(n, O_K)$ is a Schur ring. However, G is not always conjugate to a subgroup of $GL(n, O_K)$. Some examples are given by Cliff, Ritter, Weiss [2], Feit and Serre [29].

There are 3 natural questions:

Question 2.2. *Let R be an arithmetic ring and $M(n, R)$ the matrix ring over R. For which n there exists a finite group $G \subset GL(n, R)$ such that the R-span of G is just ?$M(n, R)$??*

Question 2.3. *Let G be a finite irreducible linear group over $\mathbb{C}$, and let R be the ring spanned by the traces of the elements of G. Under what conditions $\langle G\rangle_R \cong M(n, R)$??*

Question 2.4. *Is it possible to determine globally irreducible finite subgroups of $GL(n, \mathbb{C})$??*

In his recent publication [29] J.-P. Serre emphasized remarkable connections between integral irreducible representations of the group of quaternions and genus theory of Gauss and Hilbert, and the theory of Hilbert's symbol. The following question was considered by W. Feit and J.-P. Serre with a focus on the case $n = 2$, though in general it appeared much earlier, see [4, section 75], in particular, in [4, Theorem 75.5], where a positive answer is given in the case when the order of G is relatively prime to the class number of O_K:

Let $\rho : G \to GL(n, K)$ be a linear representation of a finite group G over a number field K. Is it possible to realize ρ over O_K, i.e. is ρ conjugate to a homomorphism of G into $GL(n, O_K)$??

This question was also considered in our recent paper [22] as an application to the description of globally irreducible representations over arithmetic rings which was earlier introduced by F. Van Oystaeyen and A. E. Zalesskii, see [25]. This is also motivated by the following question considered by J.-P. Serre, W. Feit and other mathematicians (see also [2], [29]).

Let $G = Q_8$ be the group of quaternions of order 8. Given a linear representation $\rho : G \to GL_(2, K)$ of finite group G over a number field $K/\mathbb{Q}$, is it conjugate to a representation $\rho : G \to GL_(2, O_K)$ over O_K, and if it is not for some fields K, is it possible to find a reasonable description of such fields K??

Another approach to generalization of integral representations of finite groups was proposed by D. K. Faddeev in [10] (see also [11]) where a generalization of the theory of Steinitz and Chevalley has been suggested.

Using Atlas [3] and the classification of finite primitive irreducible subgroups $G \subset GL(p, K)$ in [8] the following result has been proven:

Theorem 2.5. [25] *Let p be an odd prime and G a primitive finite irreducible subgroup of $GL(p, \mathbb{C})$. Then G is globally irreducible exactly in the following cases:*

1. *$G \cong 3^+Alt(6)$, 3-fold cover of the alternating group, $p = 3$;*
2. *$G \cong PSL(2, q)$, $p = (q-1)/2$ with q prime or*
3. *$G \cong PSp(2l, 3)$, $p = (3^l - 1)/2$ and $l > 1$ is an odd prime. The fields of traces $\mathbb{Q}_\chi(G)$ in the cases (1), (2) and (3) are $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-q})$ and $\mathbb{Q}(\sqrt{3})$ respectively.*

Given the ring of integers O_K of an algebraic number field K, for which natural numbers is there a finite group $G \subset GL(n, O_K)$ such that $\langle G \rangle_{O_K}$, coincides with $M(n, O_K)$?? The answer is given by Theorem 2.6 if n is an odd prime:

Theorem 2.6. [25] *Let $p > 2$ be an odd prime. Let K_π denote the torsion subgroup of K^*, the multiplicative group of K. Then $M(p, R)$ is a Schur ring if and only if one of the following holds:*

- (i) *K contains an odd root of 1;*
- (ii) *there exists a field extension L of K such that $[L : K] = p$ and L_π/K_π contains a cyclic group of order st where s, t are distinct primes;*
- (iii) *$q = 2p + 1$ is a prime and K contains $\sqrt{-q}$.*

Below we are interested mainly in the case $n = 2$; in the cases when the answer is affirmative for $n = 2$, for $n = 2m$ it is also affirmative: there exists a finite group $G \subset GL(2m, O_K)$ such that $O_K G = M(2m, O_K)$. Globally irreducible subgroups $G \subset GL(2, \mathbb{C})$ are known, see below. Therefore, our task is to describe fields K such that G is conjugate to a subgroup of $GL(2, K)$ (which reduces to describing splitting fields for $\langle G \rangle_{\mathbb{Q}}$) and next to decide whether G is conjugate to a subgroup of $GL(2, O_K)$, which is a classical problem. The known results are: in [4, Theorem 75.2], saying that G is conjugate to a subgroup of $GL(2, O_K)$ if n is relatively prime to the number of ideal classes of K. For $n = 2$ this reduces to saying that the number of ideal classes of K is odd. In his recent paper [29] J.-P. Serre found the conditions for realizability of the group of quaternions over the ring of integers $O_{\mathbb{Q}(\sqrt{-d})}$ of imaginary quadratic fields and asked whether is it posible to construct the corresponding lattice explicitly; there are related results proven in [22], [2].

Theorem 2.7. *(Serre). Let $G = Q_8$, $K = \mathbb{Q}(\sqrt{-d})$, and $d > 0$. Then*

1. *G is realizable over K, $\rho : G \to GL(2, K)$, if and only if $d = a^2 + b^2 + c^2$ for some integers a, b, c.*
2. *G is realizable over O_K, $\rho : G \to GL(2, O_K)$, if and only if $d = a^2 + b^2$ for some integers a, b or $d = a^2 + 2b^2$ for some integers a, b.*

Every O_KG-lattice Λ has an invariant $cl\Lambda$, called the Steinitz class of Λ. $cl\Lambda$ is an element of I_K, the ideal class group of K. Moreover, the argument in [4, Theorem 75.2], shows that the Steinitz class of Λ has to be defined as an element of I_K/I_K^n, where n is the rank of Λ. Below we only consider the case $n = 2$ so the Steinitz class of Λ will be defined as an element of I_K/I_K^2.

The following propositions 2.8 and 2.9 list globally irreducible finite subgroups G in $GL(2,\mathbb{C})$, their character fields $F_\chi(G)$ and Schur indices $s(G)$.

For $G \subset GL(2,\mathbb{C})$ let $F_\chi(G)$ denote the field generated by the traces of all matrices in G over the field F.

Proposition 2.8. [24]. *Let G be a finite subgroup of $SL(2,\mathbb{C})$. Then G is one of the following cases:*

- *a cyclic group, of the form $\mathbb{Z}/n\mathbb{Z}$, with a positive integer n;*
- *a generalized quaternion group (binary dihedral group), of the form BD_{4n}, with a positive integer n;*
- *a binary group corresponding to one of the Platonic solids, that is BT_{24}, $G = E_{48}$, the binary octahedral group, or $G = SL(2,5) = BI_{120}$, the binary icosahedral group.*

Proposition 2.9. [22, Lemma 2.1]. *Let $G \subset GL(2,\mathbb{C})$ be a globally irreducible group, and $s(G)$ denote the Schur index of G (over $\mathbb{Q}$). Then one of the following holds:*

(i) *G is an extention of quaternion group by $S_3 \times C_2$ with $\mathbb{Q}_\chi(G) = \mathbb{Q}(\sqrt{-1})$; $s(G) = 1$.*
(ii) *$G = GL(2,3)$ with $\mathbb{Q}_\chi(G) = \mathbb{Q}(\sqrt{-2})$; $s(G) = 1$.*
(iii) *$G = E_{48}$, the binary octahedral group, with $\mathbb{Q}_\chi(G) = \mathbb{Q}(\sqrt{2})$; $s(G) = 2$.*
(iv) *$G = SL(2,5)$ with $\mathbb{Q}_\chi(G) = \mathbb{Q}(\sqrt{5})$; $s(G) = 2$.*
(v) *G has a non-trivial abelian normal subgroup A such that $|A/Z(G)|$ is not a prime power; $s(G) = 2$.*

In this paper we consider the realization of absolutely irreducible representations for dihedral groups and generalized quaternion groups over the rings of integers and give a description of the realization fields for Schur rings in the two-dimensional case.

In order to show that $M(2,O_K)$ is a Schur ring, according to [25], we need to find a globally irreducible finite subgroup in $GL(2,O_K)$. If the Schur index of G over $\mathbb{Q}_\chi(G)$ is equal to 1, then $\mathbb{Q}_\chi(G)$ is the minimal field of realization of G. If this is the case, we need to decide whether G can be realized over O_K. If the ideal class number is odd (in particular, is equal to 1) then this is the case, and if so, $\langle G\rangle_{O_K} = M(2,O_K)$. Thus, in these cases the condition $\mathbb{Q}_\chi(G) = 1$ is sufficient to conclude that $M(2,O_K)$ is a Schur ring.

In the case where G contains the group of quaternions $H = G = Q_8$, in the next section we introduce the arithmetic properties relating representations of G and H. We can summarize our results to describe the minimal realization fields for $G = Q_{4m}$ in the theorem below and the remark concerning the binary octahedral group $G = E_{48}$ and the binary icosahedral group $G = SL(2,5)$ following this theorem:

Main theorem. *1) Let $G = Q_{4m}$ be the group of generalized quaternions, and let $H = G = Q_8$ be the group of quaternions. Then there is a quadratic subfield $K_1 \subset K$ and an $O_{K_1}H$-module I which is an ideal in an extended field $L_1 = K_1(i)$, such that: $G = Q_{4m}$ is realizable over O_K if and only if H is realizable over O_{K_1}, and all Hilbert symbols $\left(\frac{-d, N_{L_1/\mathbb{Q}}(I)}{p}\right) = 1$ for all $p|d$.*
2) If $G = Q_{4m}$ is not realizable over O_K, the minimal realization field such that H is realizable over its ring of integers is a biquadratic extension $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where $d = d_1 d_2$ and d_1, d_2 are integers not equal to ± 1 or to $\pm d$.
3) The explicit computation of the above ideal I in the extended field $L_1 = K_1(i)$ is relevant to a representation of the integer $d = a^2 + b^2 + c^2$ as a sum of squares of integers. In particular, in the following 2 cases the norm N_{L_1/K_1} of either of these ideals is a principal ideal in O_{K_1} :

(1) $b = c$; then $d = a^2 + 2b^2$ (a and b are coprime) or equivalently, d has no prime factors $p \equiv 5 (\mathrm{mod} 8)$ and $p \equiv 7 (\mathrm{mod} 8)$,
(2) $c = 0$; then $d = a^2 + b^2$ (a and b are coprime) or equivalently, d has no prime factors $p \equiv 3 (\mathrm{mod} 4)$.

The proof of this theorem is given in section 3 using the theory of genera (propositions 3.7 and 3.9). The proofs of Theorem 2.7 and the Main theorem are independent, but the Main theorem gives an explicit construction the module of representation of G using ideals in Dirichlet's fields which clarifies answering the question on constructioning a Q_8-stable lattice in [29] (see [29, p. 556]) in a more general situation.

The binary octahedral group $G = E_{48}$ and the binary icosahedral group $G = SL(2,5)$ are realizable in $GL(2, O_K)$ over the rings of integers of some number fields (proposition 3.1, section 3). Note that it is still interesting to study the cases (iii) and (iv) of Proposition 2.9 for arbitrary number fields.

We would like to make one general remark. Let R be a Dedekind domain with quotient field K, let H be an R-order, L absolutely irreducible H-representation module (i.e., a finitely generated H-module that is torsion free as an R-module and such that $K \otimes_R L$ is an absolutely irreducible $K \otimes_R H$-module).

The most interesting case is the case where $H = RG$, G a finite group and $char K \nmid |G|$, it was treated in many classical papers by C. Jordan, H. Zassenhaus, K. Roggenkamp, D. K. Faddeev, A. V. Roiter, L. A. Nazarova, W. Plesken and G. Nebe. We can formulate the following classical theorem, see e.g. [4]:

Jordan-Zassenhaus Theorem. *Every isomorphism class of KH-representa- tion modules splits in a finite number of isomorphism classes of RH-representa- tion modules if the ideal class group of R is finite.*

However, though there were classes of isomorphism explicitly described by W. Plesken and M. Pohst for small dimensions n, it would be hard to expect estimates of class numbers in the case of globally irreducible representations; for this reason the existence of globally irreducible representations for a given dimension n is a more important question, and investigation of possible n is more flexible if representations are considered over a field extension, this can be observed from theorem 2.6 above.

http://dx.doi.org/10.22108/ijgt.2017.100688.1402

3. Quadratic and Dirichlet's fields, genera and globally irreducible subgroups of $GL(2,\mathbb{C})$

In this section we establish further arithmetic properties of globally irreducible finite subgroups of $GL(2,\mathbb{C})$ and their relationship to the arithmetic of quaternions.

There are simple examples of globally irreducible groups $G \subset GL(n,R)$ such that $\langle G\rangle_R \neq M(n,R)$, especially, for $n=2$. Let $R=\mathbb{Z}(\sqrt{2})$ (resp., $R=\mathbb{Z}(\sqrt{5})$). Then $GL(2,R)$ contains a globally irreducible group of order 48 (resp., 120, isomorphic to $SL(2,5)$) such that $\langle G\rangle_R$ is a quaternion algebra over R.

Proposition 3.1. *The binary octahedral group $G=E_{48}$ and the binary icosahedral group $G=SL(2,5)$ are realizable in $GL(2,O_K)$ over the rings of integers O_K of $K=\mathbb{Q}(\sqrt{2},\sqrt{-1})$ and $K=\mathbb{Q}(\sqrt{5},\sqrt{-1})$ respectively, i.e. any representation $\rho: G\to GL(2,K)$ of the group G over the field $K/\mathbb{Q}$ is conjugate in $GL(2,K)$ to a representation $\rho: G\to GL(n,O_K)$ over O_K.*

Proof. We use the Dirichlet formula for the class numbers of biquadratic extensions $\mathbb{Q}(\sqrt{d},\sqrt{-d}) = \mathbb{Q}(\sqrt{d},\sqrt{-1})$: let h_1, h_2 be the class numbers of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ respectively, then the class number of $\mathbb{Q}(\sqrt{d},\sqrt{-d})$ is equal to h_1h_2 if 2 is ramified in K and $h_1h_2/2$ if 2 is unramified in K. Since class numbers of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-2})$ are 1, and the class number of $\mathbb{Q}(\sqrt{-5})$ is 2, we can see that the class numbers of both $K=\mathbb{Q}(\sqrt{2},\sqrt{-1})$ and $K=\mathbb{Q}(\sqrt{5},\sqrt{-1})$ are 1. This implies that the Steinitz class of any O_KG-lattice is trivial, and since K is a splitting field for G, G is realizable over O_K. □

Proposition 3.2. *Let $R\subset K$ be a maximal order in a number field K. Let G be globally irreducible, and let M, N be full-dimensional RG-lattices in K^2. Then there is a fractional ideal k of K such that $M=kN$.*

Proof. Let G be a finite globally irreducible subgroup of $GL(2,\mathbb{C})$. Then the Brauer reduction $\rho(G)$ modulo all primes I of the maximal order R of a number field K are absolutely irreducible. By Nakayama's lemma it follows that $R_IG = M(2,R_I)$ for all localizations R_I of R (see the argument of [25, Proposition 2.5]). Let M, N be any 2-dimensional RG-lattices. Since $R_IG = M(2,R_I), R_I$ is a maximal order in $M(2,K)$, and by [27, (18.7), (i)], the localizations $M_I = M\otimes R_I$ and $N_I = M\otimes R_I$ are isomorphic as R_IG-lattices, and this isomorphism can be extended to a KG-endomorphism of K^2. Since $\mathrm{End}_{KG}(K^2)\simeq K$, this implies the existence of elements $k_I\in K$ such that $M_I = k_IN_I$ (and $k_I\neq 1$ only for finitely many I). So $M=kN$ for an ideal k of R which can be determined as $k=\cap_I R_Ik_I$ (see [27], (14.22)). Since the Steinitz class can be considered as an element of I_K/I_K^2 (where I_K is the ideal class group of K) for M and N, for Steinitz classes of M and N we have $\mathrm{cl}M = k^2\mathrm{cl}N = \mathrm{cl}N$ for any 2-dimensional RG-lattices M and N. □

Remark 3.3. *The above argument holds also for any globally irreducible subgroup $G\subset GL(n,K)$ and for full RG-lattices M, N in K^n, and there is a fractional ideal J of K such that $M=JN$, in other words, M and N are in the same genus. For a more general assertion (in comparison with this remark) see* [20, p. 30, line 1], *and* [20, p.3, Prop. 1.1.], *See also* [1].

The character fields of groups Q_{4k}, the generalized quaternion group of order $4k$, and D_m, the dihedral group of order $2m$, are $\mathbb{Q}(\zeta_{2k}+\zeta_{2k}^{-1})$ and $\mathbb{Q}(\zeta_m+\zeta_m^{-1})$, respectively ($\zeta_m$ denotes a primitive m-root of 1), so any character field of Q_{4k} can be obtained as a character field of D_m for $m = 2k$. In the case when m is divisible by 2 different odd primes the representation of the group D_m with generators and relations $\langle a, b | a^2 = b^m = 1, aba = b^{-1}\rangle$ given by

$$a \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, b \begin{vmatrix} 0 & -1 \\ 1 & \theta \end{vmatrix}$$

where $\theta = \zeta_m + \zeta_m^{-1}$ is an integer of $O_F, F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, and it is globally irreducible. Since $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ coincides with the character field of D_m, it is minimal possible as a realization field, according to [8], $\langle G\rangle_{O_K} = M(2, O_F)$, and $M(2, O_F)$ is a Schur ring. Below for a given number field K we consider the generalized quaternion group $G = Q_{4k}$ containing a quaternion subgroup $H \subset G$, in order to determine the conditions for $M(2, O_K) = O_K G$, and also to clarify the role of the quaternion subgroup $H \subset G$.

The necessary condition for $M(2, O_K)$ to be a Schur ring for a number field K is that the field K splits the algebra $\mathbb{Q}G$. First let us consider quadratic fields $K = \mathbb{Q}(\sqrt{-d})$. It is necessary that $d > 0$ for K to split $\mathbb{Q}G$ at the infinite place. The equation $x^2 + y^2 = -1$ must have a solution in K to provide the condition that the K-span of $G, KG \simeq M(2, K)$ or equivalently, the Hilbert symbol $\left(\frac{-1,-1}{K}\right) = 1$. This is equivalent to the existence of $\alpha \in L = K(i)$ such that $-1 = N_{L/K}(\alpha)$. By the Hasse-Brauer-Noether-Albert theorem, the necessary and sufficient condition for algebra KG to split is that $K_v G$ splits over all v-adic completions K_v of K. Equivalently, all local Hilbert symbols $\left(\frac{-1,-1}{K_v}\right) = 1$. Since $\left(\frac{-1,-1}{K_v}\right) = 1$ for all divisors v of odd primes and $\left(\frac{-1,-1}{\mathbb{C}}\right) = 1$ for infinite v, only prime divisors v of 2 should be checked. If $d \equiv 7 \pmod 8$, then $-d$ is a square in the field of 2-adic rationals (in [28, Theorem 4], sect. 3.3. of ch. 2), and $\left(\frac{-1,-1}{K_v}\right) = 1$. Furthermore, 2 is ramified in K if $d \equiv 2 \pmod 4$ or $d \equiv 1 \pmod 4$. If the prime $p = 2$ is not ramified in K, it is inert iff the Legendre symbol $\left(\frac{-d}{2}\right) = -1$, which happens for $d \equiv 3 \pmod 8$. Therefore in the cases $d \equiv 1, 2, 3, 5, 6 \pmod 8$ there is only one prime divisor v of $p = 1$ in K. By the reciprocity law for Hilbert symbols $\prod_v \left(\frac{-1,-1}{K_v}\right)$, and the number of v for which $\left(\frac{-1,-1}{K_v}\right) = -1$ is even, so $\left(\frac{-1,-1}{K_v}\right) = 1$ if v is the only prime divisor of 2 in K. For a globally irreducible subgroup $G \subset GL(2, \mathbb{C})$ containing the quaternion subgroup $H = \langle a, b | a^2 = b^2, b^{-1}ab = a^{-1}, b^4 = 1\rangle$ we intend to construct a full $O_K G$-modules and to calculate its Steinitz class. By Proposition 2.8, all $O_K G$-modules are in the same genus, and their Steinitz classes are the same modulo a square of an ideal of O_K. Therefore, it suffices to consider only one $O_K G$-module M. Let $G = Q_{4m} \subset GL(n, K)$ be a generalized quaternion group with generators and relations given by $\langle b, c | b^{-1}cb = c^{-l}, c^m = b^2, b^4 = 1\rangle$ of order $4m$, and let K be a number field containing the character field $F = \mathbb{Q}(\zeta_{2m} + \zeta_{2m}^{-1})$ of Q_{4m} and $\sqrt{-d}$ for some square-free positive integer d but not containing $\zeta_{2m}, m = 2r$.

http://dx.doi.org/10.22108/ijgt.2017.100688.1402

Proposition 3.4. *(1) An algebraic number field K is a splitting field for the group G of quaternions if and only if K is totally imaginary and for all localizations K_v for all prime divisors v of 2 the local degree $[K_v : \mathbb{Q}_2]$ is even.*

(2) If K is a splitting field for the group G of quaternions, then $[K : \mathbb{Q}]$ is even.

(3) K is a splitting field for the group G of quaternions and $K/\mathbb{Q}$ is abelian, then K has a quadratic subfield $\mathbb{Q}(\sqrt{d})$.

Proof. By the theorem of Hasse-Brauer-Noether, K is a splitting field for $\langle G\rangle_{\mathbb{Q}}$ if and only if the localization K_v is a splitting field locally for $\langle G\rangle_{\mathbb{Q}_p} = \mathbb{Q}_p G$ for all prime divisors v of p. Since the quaternion algebra has invariants $1/2$ at 2 and ∞ in the Brauer group, and 0 at all other primes p, K is a splitting field for G if and only if K is totally imaginary and for all localizations K_v for all prime divisors v of 2 the local degree $[K_v : \mathbb{Q}_2]$ is even [7, Satz 2, ch. VII, sect. 5].

Since $[K : \mathbb{Q}]$ is the sum of $[K_v : \mathbb{Q}_2]$, it must be even, and this implies (2).

If $K/\mathbb{Q}$ is abelian, its degree is even, and its Galois group has a subgroup of index 2, therefore, the fixed subfield of this subgroup is a quadratic extension of $\mathbb{Q}$.

This completes the proof of proposition 3.4. □

Below we consider realization fields for the group $G = Q_{4m}$, and we are interested in the case when realization field contains a quadratic subfield over $\mathbb{Q}$. However, as an example, we can show that a minimal splitting field of H, the group of quaternions, may not contain any quadratic subfields $F/\mathbb{Q}$.

Example 3.5. *Consider splitting field K over $\mathbb{Q}$ of the polynomial $f(x) = x^4+24x+36$. The polynomial $f(x)$ has discriminant $3^6 2^{12}$, and it is a square of an integer; the resolvent of $f(x)$ is $y^3-144y-576$, and it is irreducible over $\mathbb{Q}$. It follows from Galois theory that K has the Galois group A_4, the alternating group, so it can not contain any quadratic subfields $F/\mathbb{Q}$.*

From the other part, K has no real roots, and K is a splitting field for the group of quaternions: indeed, $\left(\frac{-1,-1}{K_v}\right) = 1$ for all completions K_v, and by the Theorem of Hasse-Minkowski we have $\left(\frac{-1,-1}{K}\right) = 1$.

However, the splitting field of G contains $F = \mathbb{Q}(\zeta_{2m} + \zeta_{2m}^{-1})$, and below we assume that a splitting field K of G contains $\sqrt{-d}$ for some positive integer d and $\mathbb{Q}(\sqrt{-d})$ is a splitting field for H (see proposition 3.4 above). We will establish a relationship between the realizability of $G = Q_{4m}$ over O_K and the realizability of its quaternion subgroup $H \subset G$ over the integers of a smaller field $K_1 = \mathbb{Q}(\sqrt{-d}) \subset L_1 = \mathbb{Q}(\sqrt{-d}, i)$. Further, for $Q_{4m} \supset H$ we can extend an O_{K_1}-character from $H = Q_8$ in the appropriate CM-field $\mathbb{Q}(\sqrt{-d}, \zeta_{2m} + \zeta_{2m}^{-1})$ containing the field $\mathbb{Q}(\zeta_{2m} + \zeta_{2m}^{-1})$ of characters of Q_{4m}, so that $\mathbb{Q}(\sqrt{-d}, \zeta_{2m} + \zeta_{2m}^{-1})$ is the minimal realization field according to proposition 3.4.

Below we will show that a representation of $G = Q_{4m}$ can be realized over O_K if and only if M is realizable over O_K, and if this is the case, we will construct an $O_K G$-module M and the related $O_{K_1} H$-module I. This can be also formulated as a necessary and sufficient condition for Hilbert symbols.

Let us consider the $O_K G$-module $M_1 = O_K[1, \alpha, \zeta_{2m}, \zeta_{2m}\alpha] \subset K(\zeta_{2m})$ determined by the action on the generators of G as follows : $bl = l\zeta_{2m}, cl = \alpha l^{\sigma}$, where $l \in K(\zeta_{2m}), \alpha \in L_1$ is an element whose norm

http://dx.doi.org/10.22108/ijgt.2017.100688.1402

in $L_1/\mathbb{Q}(\sqrt{-d})$ is equal $-1, \sigma$ is the generator of the Galois group of $K(\zeta_{2m})/K$. We are interested to find a minimal possible K. In order to determine certain necessary conditions for all possible K we restrict the action of G to $H \subset G$, the quaternion subgroup. It is also convenient to find a minimal realization field K_1 for H, it can be chosen as $K_1 = \mathbb{Q}(\sqrt{-d})$ or a quadratic extension of $\mathbb{Q}(\sqrt{-d})$.

We need to determine an integral basis for special biquadratic fields (Dirichlet's fields) $L_1 = \mathbb{Q}(\sqrt{-d}, i)$, where $i = \sqrt{-1}$. Dirichlet's fields $L_1 = \mathbb{Q}(\sqrt{\delta}, i)$ for a square-free element $\delta \in \mathbb{Z}[i]$ were investigated by D. Hilbert in [17], and the basis of O_{L_1} is given explicitly in [17, sect. 1], as $1, \omega, i, i\omega$ for $\omega \in L_1$ depending on δ. We need only the following particular cases: if $\delta = -d \equiv 3(\text{mod}4)$, then we can take $\omega = \frac{1-i\sqrt{-d}}{2} = \frac{1+\sqrt{d}}{2}$; if $d \equiv 2(\text{mod}4)$, then we can take $\omega = \sqrt{\delta} = \sqrt{-d}$; if $-d \equiv 1(\text{mod}4)$, then $\omega = \frac{1-i\sqrt{-d}}{2} = \frac{1+\sqrt{d}}{2}$. Let $K_1 = \mathbb{Q}(\sqrt{-d})$ for a square-free positive integer d. We distinguish the cases $d \equiv 3(\text{mod}4), d \equiv 1(\text{mod}4)$ and $d \equiv 2(\text{mod}4)$ in our construction of an $O_{K_1}H$-module I. Consider an $O_{K_1}H$-module $I_1 = O_{K_1}[1, \alpha, i, i\alpha] \subset L_1 = K_1(i)$ determined by setting $la = il, lb = dl^\gamma$ for the generator γ of the Galois group of L_1/K_1. Since for $d \equiv 3(\text{mod}4), O_{L_1} = O_{K_1}[i]$ we can set $I = I_1$ in this case and consider I as a fractional O_{K_1} -ideal in L_1. If $d \equiv 3(\text{mod}4)$ we can take $I = I_1 + \omega I_1$. In all cases the O_{K_1}-module I becomes an O_{L_1}-module in a natural way, therefore I can be regarded as an O_{L_1}-ideal in L_1. Likewise, take the $O_K G$-module $M = M_1$ if $d \equiv 3(\text{mod}4)$ and $M = M_1 + \omega M_1$ if $d \not\equiv 3(\text{mod}4)$.

As it was pointed out before, we consider generalized quaternion groups $G = Q_{4m}$ containing a quaternion subgroup H, but we know that such G is globally irreducible if and only if m is not a 2-power. Thus in the foregoing considerations we could restrict attention to G not of 2-power order but containing the quaternion group of order 8. Below we reduce the question concerning the realizability of $G = Q_{4m}$ over O_K to a special question about the realizability of its quaternion subgroup $H \subset G$ over the integers of a smaller field $K_1 = \mathbb{Q}(\sqrt{-d})$ as earlier, and the constructed ideal I is the $O_{K_1}H$-module of the latter representation.

The following proposition describes the possible quadratic subfields of cyclotomic fields which can serve as realization fields for H. Let $n > 4$ be an integer, and let for every prime p $\chi_p = (\frac{-1}{p})$ ($(\frac{-1}{p})$ is the Legendre symbol) be the quadratic residue character $\chi_p : \mathbb{Z}/p\mathbb{Z} \to \{\pm 1\}$.

Proposition 3.6. *Let S be the set of integers containing -1 if $n = 4k$, 2 if $n = 8t$ (t, k are integers), and $\chi_p(-1)p$ for odd prime divisors p of n. Let $S = S_1 \cup S_2$, subsets having s_1 and s_2 elements resp., where S_1 contains all s_1 negative, and S_2 contains all positive integers of S. Then*

(1) *The maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of n-cyclotomic field $\mathbb{Q}(\zeta_n)$ contains $2^{s_1+s_2-1} - 1$ real quadratic subfields $\mathbb{Q}(\sqrt{d})$, where d is any positive product of distinct elements of S,*

(2) *$\mathbb{Q}(\zeta_n)$ contains $2^{s_1+s_2-1}$ imaginary quadratic subfields $\mathbb{Q}(\sqrt{d})$, where d is any negative product of distinct elements of S.*

Proof. By Galois theory, the quadratic extensions of $\mathbb{Q}$ correspond to subgroups of index 2 of $(\mathbb{Z}/n\mathbb{Z})^*$ which is the Galois group of the n-th cyclotomic field. From the other part, $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to a direct product of $(\mathbb{Z}/p^i\mathbb{Z})^*$ for primes p, $(\mathbb{Z}/2\mathbb{Z})^* = 1$, $(\mathbb{Z}/4\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$, and $(\mathbb{Z}/2^k\mathbb{Z})^*$ is a product of $(\mathbb{Z}/2\mathbb{Z})$ and $(\mathbb{Z}/2^{k-2}\mathbb{Z})$. The total number of quadratic subfields is $2^{s_1+s_2} - 1$, since there are $2^{s_1+s_2}$ homomorphisms from $(\mathbb{Z}/n\mathbb{Z})^*$ to $(\mathbb{Z}/2\mathbb{Z})$, one of which is trivial. Thus we can take a positive or negative product d of elements from sets S_1 and S_2 by the number of ways given in (1) and (2) for obtaining the field $\mathbb{Q}(\sqrt{d})$ which is trivial for $d = 1$. □

Let F be an algebraic number field and K a finite abelian extension of F having the Galois group $Gal(K/F)$. Let K' be the Hilbert class field of K and let C_K be the ideal class group of K. By class field theory the fields lying between K and K' are in one-one correspondence with the subgroups of C_K. Let L be the genus field of K/F. Then L is the maximal abelian extension of F contained in K. The subgroup of C_K corresponding to L is the principal genus and the quotient of C_K modulo the principal genus is the group of genera. H. Hasse has shown that for $F = \mathbb{Q}$ in the absolutely abelian case, the principal genus can be determined by arithmetic characters.

Proposition 3.7. *$G = Q_{4m}$ is realizable over O_K if and only if H is realizable over O_{K_1} the corresponding O_KG-module is M, and $O_{K_1}H$-module is I. This happens if and only if all Hilbert symbols $\left(\frac{-d, N_{L_1/\mathbb{Q}}(I)}{p}\right) = 1$ for all $p|d$. If the above condition is not true, the minimal realization field such that H is realizable over its ring of integers is a biquadratic extension $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where $d = d_1d_2$ and d_1, d_2 are integers not equal to $\pm\, 1$ or to $\pm\, d$.*

Proof. We refer to [14], [16], ch. 7 sect. 45, [13], ch. 26, sect. 8, ch. 29, sect. 3 for the theory of genera in quadratic number fields. It follows from [14], sect. 45, that any $t-1$ of t prime divisors $\mathbf{q}_i|q_i$ for primes $q_i|d$ ramified in $K_1/\mathbb{Q}$ can be selected as generators of the genus group. In fact, $\mathbf{q}_i$ represent cosets of the ideal class group C_{K_1} modulo $C_{K_1}^2$, and the number of different genera is 2^{t-1} since for an imaginary field $K_1 = \mathbb{Q}(\sqrt{-d})$ ideal classes coincide with narrow classes. Besides, all squares $\mathbf{q}_i^2 = q_i$ are principal divisors, and any non-principal genus is represented by $\mathbf{q}_{i_1}\mathbf{q}_{i_2}\cdots\mathbf{q}_{i_t}C_{K_1}^2$.

The quaternion group $H \subset G$ acts on the $O_{K_1}H$-module I generated by $1, i, \alpha$ and $i\alpha$ if $d \equiv 3(\mathrm{mod}4)$ (and all these elements multiplied by ω in the case $d \not\equiv 3(\mathrm{mod}4)$) over O_{K_1} as follows : $la = il, lb = \alpha l^\sigma$, where σ is a generator of the Galois group of L_1/K_1, and this action can be extended to the O_KG-module M in a natural way taking into account that the generators b and c of G can be chosen in such a way that $a = c^{\frac{m}{2}}$ and b are the generators of H. Therefore, the action of G on M agrees with the action of H on I, and M can be obtained from I by extending the ground ring adjoining ζ_{2m}. This implies that the O_KG-module M is free if the O_{K_1}-module I is free.

Note that in the case $K_1 = \mathbb{Q}(\sqrt{-d})$ and $-d \equiv 1(\mathrm{mod}4)$, 2 is unramified K_1, and $O_{L_1} = O_{K_1}[i]$ for $L = K(i)$, so M is a fractional ideal in L. $^{S}incetheSteinitzclassofthe$ O_{K_1}-module I is just the class of $N_{L_1/K_1}(I)$, we need to find whether or not the Steinitz class of N_{L_1/K_1} is contained in the principal genus. If not, $N_{L_1/K_1}(I)$ is contained in some non-principal genus $\mathbf{q}_{i_1}\mathbf{q}_{i_t}\cdots\mathbf{q}_{i_t}C_{K_1}^2$. The minimal extension of K_1 where $N_{L_1/K_1}(I)$ becomes a square is a quadratic extension $K_1(\sqrt{q_{i_1}q_{i_2}\cdots q_{i_t}}) = K_1(\sqrt{d_1})$ for $d_1|d$, and since the ideal $\mathbf{q}_{i_1}\mathbf{q}_{i_2}\cdots\mathbf{q}_{i_t}$ is not principal, it cannot be a unit ideal or $(\sqrt{-d})$. Therefore, the

Steinitz class of I in $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ becomes trivial, and H is realizable over the ring of integers of $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ for $d = d_1 d_2$ as it was claimed.

The necessary and sufficient condition for an ideal J to belong to the principal genus is given in [14, p. 49], and [13, p. 513–514], and [13, p. 516]. For $K_1 = \mathbb{Q}(\sqrt{-d})$ and $J = N_{L_1/K_1}(I)$ it can be written as follows : $\left(\frac{-d, \pm N_{K_1/Q}(J)}{p}\right) = \left(\frac{-d, \pm N_{L_1/Q}(I)}{p}\right) = 1$ for all $p|d$ or $r = \infty$. For $r = \infty$ this condition implies that the plus sign must be taken. This completes the proof. □

Remark 3.8. *The $O_{K_1}H$-module I constructed above certainly has an O_{K_1}-basis $1, \alpha$ if $\alpha \in O_L$ but this depends strongly on the solvability of the equation in $\mathbb{Q}(\sqrt{-d})$ and on the Hasse index Q of units in L_1. By definition, $Q = [E : WE^+] (Q = 1$ or $2)$ where E is the unit group of a CM-field Λ, E^+ is the unit group of the maximal totally real subfield of Λ, and W is the subgroup of all roots of 1 in Λ. If $s \equiv 1 (\mathrm{mod} 4)$, we have $Q = 1$, and $\alpha \in O_{L_1}$ iff the corresponding Pellian equation $x^2 - dy^2 = -4$ has an integral solution (x, y). If $d \equiv 3 (\mathrm{mod} 4)$, $Q = 2$ or 1 depending on whether or not the equation $x^2 - dy^2 = \pm 2$ has an integral solution (x, y), the necessary condition for this is $\left(\frac{\pm 2}{p}\right) = 1$ (see [15], [17, p. 77]). In the case $d \equiv 3 (\mathrm{mod} 4)$ we have $\alpha \notin O_{L_1}$ if $Q = 1$ since the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm -1 iff the Pellian equation $x_2 - dy^2 = -1$ has an integral solution (x, y) which is possible only if d has no prime factors $p \equiv 3 (\mathrm{mod} 4)$.*

According to Theorem 2.1, the realizability of G over the ring of integers of K depends on the realizability of the $O_{K_1}H$-module I introduced above. I is an ideal in O_{L_1}, and it can be calculated more explicitly if a square-free integer d is a sum $a^2 + b^2 + c^2$ for some rational integers a, b, c. By the well-known theorem of Gauss (see e.g [28], appendix to ch. 3) this happens for $d \equiv 1, 2, 3, 5, 6 (\mathrm{mod} 8)$. As it was mentioned above, for $d \equiv 7 (\mathrm{mod} 8)$ we have $K_1 G \not\simeq M(2, K_1)$, so in this case the field K_1 should be extended, and we exclude this case.

Some interesting results in Galois theory reflect interplay between seemingly unrelated arithmetic topics, and we will formulate one of them after the following proposition.

In the following proposition the group G is the same as in proposition 3.7.

Proposition 3.9. *If for $K_1 = \mathbb{Q}(\sqrt{-d})$, d is square-free, and $L_1 = K_1(i)$ the algebra $K_1 G$ splits, then $d = a^2 + b^2 + c^2$ for some rational integers a, b, c, and the above O_{L_1}-ideal I is equivalent in I_{L_1}, the ideal class group of L_1, to the O_{L_1}-ideal $(a - \sqrt{-d} i, b + ic)$, and it is also equivalent to the O_{L_1}-ideal $(b^2 + c^2, (b + ci)(a - \sqrt{-d} i))$. In particular, in the following 2 cases the norm N_{L_1/K_1} of either of these ideals is a principal ideal in O_{K_1} :*

(a) *$b = c$; then $d = a^2 + 2b^2$ (a and b are coprime) or equivalently, d has no prime factors $p \equiv 5 (\mathrm{mod} 8)$ and $p \equiv 7 (\mathrm{mod} 8)$,*
(b) *$c = 0$; then $d = a^2 + b^2$ (a and b are coprime) or equivalently, d has no prime factors $p \equiv 3 (\mathrm{mod} 4)$.*

Proof. We can use the theory of Pfister forms (see [21], [26]) to determine explicitly the form of $a \in L_1$ such that $N_{L_1/K_1} \alpha = -1$. By definition, the level $s(K)$ of a field K is the minimal natural number for which -1 is a sum of $s(K)$ squares in K or ∞ if K is formally real. By in [21, Theorem 5.4] (or [26, Satz 5, p. 164]), if for a formally real field K an integer d is a sum of n squares, but not $n-1$ squares, where $2^k \le n < 2^{k+1}$, then for a field $L = K(\sqrt{-d})$ the level of L is 2^k. The proof of the above claim is constructive, and since $-1 = (\frac{a}{\sqrt{-d}})^2 + (\frac{b}{\sqrt{-d}})^2 + (\frac{c}{\sqrt{-d}})^2$, it allows to find explicitly a way to represent -1 as a sum of 2 squares : $-1 = x^2 + y^2$. We need to determine $\alpha = x + iy$ having the same property. Omitting some auxiliary calculations, finally we obtain :

$$\alpha = \frac{ab + c\sqrt{-d}}{b^2 + c^2} + i\frac{(ac - b\sqrt{-d})}{b^2 + c^2} = \frac{(b + ci)(a - i\sqrt{-d})}{b^2 + c^2}$$

Taking an O_{L_1}-ideal $(1, \alpha)$ and multiplying it by $b^2 + c^2$ or multiplying by $b - ic$ and replacing simultaneously c by $-c$ we obtain the first assertion of Proposition 3.9. The part (b) of proposition 3.9 can be checked by a direct calculation. □

Remark 3.10. *In* [6] *some integral representations arising from torsion points of elliptic curves were considered. For the following finite extension $K/\mathbb{Q}_p$ of local fields obtained via adjoining torsion points of elliptic curves, let O_K be the ring of integers of K with the maximal ideal $\mathcal{P}$. Consider an elliptic curve E over $\mathbb{Z}_p$ with supersingular good reduction (see* [29, sect. 1.11]*). Let $K/\mathbb{Q}_p$ be the field extension obtained by adjoining p-torsion points of E, then the formal group associated to E has height 2, its Hopf algebra O_A is a free module of rank p^2 over $\mathbb{Z}_p$, and for the kernel E_p of multiplication by p $|E_p| = p^2$ (see* [5, 1.3 and sect. 2]*). Note that for some E the ramification index $e = e(K/\mathbb{Q}_p) = p^2 - 1$ (*[30, p. 275, Proposition 12]*).*

Acknowledgments

The author is grateful to the referee for helpful suggestions, corrections and remarks, and for a deep insight into the subject.

References

[1] M. Auslander and O. Goldman, Maximal Orders, *Trans. Amer. Math. Soc.*, **97** (1960) 1–24.

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

[3] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[4] Ch. Curtis and I. Reiner, Represenation theory of finite groups and associative algebras, Pure and Applied Mathematics, **11**, Interscience Publishers, a division of John Wiley Sons, New York-London, 1962.

[5] F. Destrempes, Deformations of Galois representations: the flat case, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), *Canad. Math. Soc. Conf. Proc.*, Amer. Math. Soc., Providence, RI, **17** (1995) 209–231.

[6] F. Destrempes and D. Malinin, *The maximal tamely ramified extension over a local field with applications to torsion points of formal groups or elliptic curves*, a preprint.

[7] M. Deuring, *Algebren*, Springer-Verlag, Berlin-New York, 1968.

[8] J. D. Dixon and A. E. Zalesskii, Finite primitive linear groups of prime degree, *J. London Math. Soc. (2)*, **57** (1998) 126–134, errata: in *J. London Math. Soc. June*, **77** (2008) 808–812.

[9] D. K. Faddeev, On generalized integral representations over Dedekind rings, (Russian) *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, **227**, 1995, Voprosy Teor. Predstav. Algebr i Grupp. 4, 113–118; English translation in *J. Math. Sci.*, (New York), **89** (1998) 1154–1158.

[10] D. K. Faddeev, Tables of the fundamental unitary representations of the Fedorov groups, *Trudy Mat. Inst. Steklov*, **56** (1961) pp. 174.

[11] D. K. Faddeev, An introduction to the multiplicative theory of modules of integral representations, (Russian) *Trudy Mat. Inst. Steklov*, **80** (1965) 145–182.

[12] B. H. Gross, Group representations and lattices, *J. Amer. Math. Soc. (3)*, **2** (1990) 929–960.

[13] H. Hasse, *Number Theory*, Translated from the third German edition of 1969 by H. Gnter Zimmer, Akademie-Verlag, Berlin, 1979.

[14] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörpern, *J. Math. Soc. Japan*, **3** (1951) 45–51.

[15] H. Hasse, *Über die Klassenzahl Abelscher Zahlkörper*, Berlin, Akademie Verlag, Berlin, 1952.

[16] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, Akademische Verlagsgesellschaft, 1923.

[17] D. Hilbert, Über den Dirichletischen Zahlkörper, *Math. Ann.*, **45** (1894) 309-340.

[18] I. M. Isaacs, *Character Theory of finite groups*, Academic Press, 1976.

[19] V. V. Ishkhanov, B. B. Lurje and D. K. Faddeev, The Embedding Problem in Galois Theory, Translations of Mathematical Monographs, **165**, American Mathematical Society, Providence, 1997.

[20] H. Jacobinski, Genera and decompositions of lattices over orders, *Acta Math.*, **121** (1968) 1–29.

[21] M. Knebusch and W. Scharlau, *Algebraic theory of quadratic forms: Generic methods and Pfister Forms*, DMV Seminar 1, Birkhauser, 1980.

[22] D. Malinin and F. Van Oystaeyen, Realizability of two-dimensional linear groups over rings of integers of algebraic number fields, *Algebr. Represent. Theory*, **14** (2011) 201–211.

[23] D. Malinin, Integral representations of p-groups of given nilpotency class over local fields, *St. Petersburg Math. J.*, **10** (1999) 45–52.

[24] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and applications of nite groups*, Dover, New York, 1916.

[25] F. Van Oystaeyen and A. E. Zalesskiĭ, Finite groups over arithmetic rings and globally irreducible representations, *J. Algera*, **215** (1999) 418–436.

[26] A. Pfister, Zur Darstellung von-1 als Summe von Quadraten in einem Korper, *J. London Math. Soc.*, **40** (1965) 159–165.

[27] I. Reiner, *Maximal Orders*, Academic Press, 1975.

[28] J.-P. Serre, *Cours d'arithmétique*, Paris, 1970.

[29] J.-P. Serre, Three letters to Walter Feit on group representations and quaternions, *J. Algebra*, **319** (2008) 549–557.

[30] J.-P. Serre, Propriétés galoisiennes des points dordre fini des courbes elliptiques, *Invent. Math.*, **15** (1972) 259–331.

[31] M. F. Vigneras, Arithmetique des algebres de quaterniones, Springer Lect. Notes in Math., **397**, 1974.

Dmitry Malinin

Dipartimento di Matematica e Informatica U. Dini, Universita‘ degli Studi di Firenze, viale Morgagni 67/a, 50134 Firenze, Italy.

Email: dmalinin@gmail.com

http://dx.doi.org/10.22108/ijgt.2017.100688.1402