ЧЕБЫШЕВСКИЙ СБОРНИК
Том 16 Выпуск 3 (2015)

ONE CONSTRUCTION OF INTEGRAL REPRESENTATIONS OF p-GROUPS AND SOME APPLICATIONS

Dmitry Malinin (Kingston, Jamaica)
dmalinin@gmail.com

Department of Mathematics, University of the West Indies,
Mona, Kingston 7, Jamaica

Abstract

Some well-known classical results related to the description of integral representations of finite groups over Dedekind rings R, especially for the rings of integers $\mathbf{Z}$ and p-adic integers $\mathbf{Z_p}$ and maximal orders of local fields and fields of algebraic numbers go back to classical papers by S. S. Ryshkov, P. M. Gudivok, A. V. Roiter, A. V. Yakovlev, W. Plesken. For giving an explicit description it is important to find matrix realizations of the representations, and one of the possible approaches is to describe maximal finite subgroups of $GL_n(R)$ over Dedekind rings R for a fixed positive integer n.

The basic idea underlying a geometric approach was given in Ryshkov's papers on the computation of the finite subgroups of $GL_n(\mathbf{Z})$ and further works by W. Plesken and M. Pohst. However, it was not clear, what happens under the extension of the Dedekind rings R in general, and in what way the representations of arbitrary p-groups, supersolvable groups or groups of a given nilpotency class can be approached.

In the present paper the above classes of groups are treated, in particular, it is proven that for a fixed n and any given nonabelian p-group G there is an infinite number of pairwise non-isomorphic absolutely irreducible representations of the group G. A combinatorial construction of the series of these representations is given explicitly.

In the present paper an infinite series of integral pairwise inequivalent absolutely irreducible representations of finite p-groups with the extra congruence conditions is constructed.

We consider certain related questions including the embedding problem in Galois theory for local faithful primitive representations of supersolvable groups and integral representations arising from elliptic curves.

Keywords: finite nilpotent groups, integral domain, Dedekind ring, elliptic curves.

Bibliography: 27 titles.

ОБ ОДНОЙ КОНСТРУКЦИИ ЦЕЛОЧИСЛЕННЫХ ПРЕДСТАВЛЕНИЙ p-ГРУПП И ЕЁ ПРИЛОЖЕНИЯ

Д. А. Малинин (Кингстон, Ямайка)
dmalinin@gmail.com

Аннотация

Некоторые хорошо известные классические результаты, относящиеся к описанию целочисленных представлений конечных групп над дедекиндовыми кольцами R, в частности, для колец целых чисел $\mathbf{Z}$ и p-адических чисел $\mathbf{Z_p}$ и максимальных порядков локальных полей и полей алгебраических чисел берут начало в классических работах С. С. Рышкова, П. М. Гудивка, А. В. Ройтера, А. В. Яковлева, В. Плескена. Для их явного описания важно найти матричные реализаций представлений, и один из возможных подходов состоит в описании максимальных конечных подгрупп $GL_n(R)$ над дедекиндовым кольцом R при фиксированном натуральном n.

Основная идея, лежащая в основе геометрического подхода, была приведена в работах С. С. Рышкова по вычислению конечных подгрупп из $GL_n(\mathbf{Z})$ и дальнейших работах М. Поста и В. Плескена. Тем не менее, было неясно, что происходит при расширении дедекиндова кольца R в общем случае, и в случаях представлений произвольных p-групп, сверхразрешимых групп или групп заданного класса нильпотентности.

В настоящей работе изучаются представления вышеуказанных классов групп, в частности, доказано, что при фиксированном n и любой заданной неабелевой p-группы G существует бесконечное число попарно неизоморфных абсолютно неприводимых представлений группы G. Комбинаторная конструкция серии этих представлений получена в явном виде.

В настоящей работе построена бесконечная цепочка целочисленных попарно неэквивалентных абсолютно неприводимых представлений конечных p-групп с дополнительными условиями сравнимости по модулю дивизоров простого числа p.

Мы рассматриваем некоторые связанные нашей конструкцией вопросы, включая задачи погружения в теории Галуа для локальных точных примитивных представлений сверхразрешимых групп и целочисленные представления, возникающие из эллиптических кривых.

Ключевые слова: конечные нильпотентные группы, целые области, Дедекиндовые кольца, эллиптические кривые.

Библиография: 27 наименований.

1. Introduction

Let K be a finite extension of the p-adic field $\mathbf{Q_p}$, and let O_K be its ring of integers. If K is fixed, the number of irreducible pairwise inequivalent representations of a given finite group group over O_K is finite. In this paper we do not fix K, we allow K to be extended via adjoining certain roots of 1, we construct an infinite number of absolutely irreducible pairwise inequivalent representations of a given p-group over O_K for different K, and we consider the possible realization fields of these representations.

We construct some infinite series of integral pairwise inequivalent absolutely irreducible representations of finite p-groups over the rings of integers of number fields and local fields, and we apply this construction to representations having the minimal possible degrees. We also prove the extra condition that the matrices of these representations are contained in the kernel of reduction modulo a prime divisor of p. By giving a complete combinatoric description of all irreducible representations of a finite p-group of class 2 we show that a nonabelian p-group possesses infinitely many absolutely irreducible integral representations which are not equivalent over the ring of integers.

Remark that the class of groups considered in the first section below can be extended to classification of absolutely irreducible primitive representations of some supersolvable groups (see [16]), and this can be applied to the classification of the primitive representations of the Galois groups of local fields.

2. Notation

We denote $\mathbf{C}$, $\mathbf{Q}$ *and* $\mathbf{Q_p}$ *the fields of complex, real, rational and rational p-adic numbers.* $\mathbf{Z}$ *and* $\mathbf{Z_p}$ *are the rings of rational and p-adic integers.* $N_{E/F}(a)$ *denotes the norm of* $a \in E$ *in the field extension* E/F.

We denote $GL_n(R)$ *the general linear group over a ring* R, $SL_n(R)$ *denotes the special linear group.*

$[E : F]$ *denotes the degree of the field extension* E/F.

$M_n(R)$ *is the full matrix algebra over a ring* R.

Finite groups are usually denoted by capital letters G, H, *and their elements by small letters, e.g.* $g \in G$, $h \in H$, $\langle a, b... \rangle$ *denotes a group generated by* $a, b, ...$, $Z = Z(G)$ *is the center of* G, $[a, b] = aba^{-1}b^{-1}$ *denotes the commutator of* a, b.

We write ζ_t *for a primitive t-root of 1.*

Diagonal matrices are denoted by $diag(d_1, \ldots, d_n)$, I *(and* I_m*) stands for a unit* $(m \times m$*-matrix).*

Binomial coefficients are denoted by $\begin{pmatrix} n \\ m \end{pmatrix}$.

3. The construction

Let us consider a nonabelian group G_0 generated by two elements a and b of order $t = p^m$, $a^t{=}b^t{=}1$ such that the commutator $c = [a, b] \neq 1$ is contained in the center of G_0, and $c^t{=}1$, t is the minimal positive integer having this property. Let ζ be a primitive root of 1 of degree t. The following representation of G_0 is faithful and absolutely irreducible.

$$A = \Delta(a) = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \dots & \ddots & \dots \\ 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix},$$

$$B = \Delta(b) = diag(1, \zeta, \dots, \zeta^{t-1})$$

Indeed, all matrices of this representation are unitary, and any matrix in $GL_t(\mathbf{C})$ commuting with all matrices of this representation is a scalar matrix; it follows from [8], p. 8 that $\Delta(G_0)$ is absolutely irreducible.

Proposition 1. *(see e.g. theorem (2.32), p. 29 [11]. A p-group has a faithful irreducible representation if and only if its center is cyclic.*

For the $n \times n$-matrices e_{ij} having precisely one nonzero entry in the position (i, j) equal to 1 we can define a $n \times n$-matrix using the binomial coefficients $\begin{pmatrix} n-j \\ i-j \end{pmatrix}$; in the case $i = j = n$ we replace the above coefficients with 1. Let us consider $n = t$ and the following triangular matrices:

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

$$C_1 = \sum_{n \geq i \geq j \geq 1} \begin{pmatrix} n-j \\ i-j \end{pmatrix} e_{ij}.$$

Let $X = diag(1, x, x^2, \dots, x^{t-1})$, then

$$C_1 X C = \sum_{n \geq i \geq j \geq 1} \begin{pmatrix} n-j \\ i-j \end{pmatrix} x^{j-1}(1-x)^{i-j} e_{ij},$$

and if we take $x = 1$, this will imply $C^{-1} = C_1$.
If we take $x = \zeta$, we will obtain:

$$\Delta'(b) = C_1 \Delta(b) C = C_1 B C = \sum_{n \geq i \geq j \geq 1} \begin{pmatrix} n-j \\ i-j \end{pmatrix} \zeta^{j-1}(1-\zeta)^{i-j} e_{ij},$$

We can see that all matrix entries below the main diagonal are divisible by powers of $\zeta - 1$, and the exponents of the powers are growing proportionally to the distance from the main diagonal. An elementary computation shows that

$$\Delta'(a) = C^{-1}AC = \begin{pmatrix} 1-t & 1 & 0 & \dots & 0 & 0 \\ -\binom{t}{2} & 1 & 1 & \dots & 0 & 0 \\ \dots & \dots & \ddots & \ddots & \dots & \dots \\ -\binom{t}{t-1} & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

Let K be (as earlier in Introduction) a finite extension of the p-adic field $\mathbb{Q}_p$. Let us assume that K contains ζ. For a positive integer h let us consider a finite extension $L_h \subset K(\zeta_{p^r})$ of degree h over $\mathbf{Q_p}$ for an appropriate integer r and a primitive p^r-root of 1 ζ_{p^r}; its maximal order O_{L_h}, a prime divisor $\mathcal{P}$ of p and its prime element π_h, this prime element may be chosen as $\zeta_{p^r} - 1$ in the case if L_h is a cyclotomic field $\mathbf{Q_p}(\zeta_{\mathbf{p^r}})$. Let $D_h = diag(1, \pi_h, \pi_h^2, \dots, \pi_h^{t-1})$, then

$$A_h = \Delta_h(a) = D_h^{-1}\Delta'(a)D_h = \begin{pmatrix} 1-t & \pi_h & 0 & \dots & 0 & 0 \\ -\binom{t}{2}\pi_h^{-1} & 1 & \pi_h & \dots & 0 & 0 \\ \dots & \dots & \ddots & \ddots & \dots & \dots \\ -\binom{t}{t-1}\pi_h^{2-t} & 0 & 0 & \dots & 1 & \pi_h \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

$$B_h = \Delta_h(b) = D_h^{-1}\Delta'(b)D_h = \sum_{n \geq i \geq j \geq 1} \begin{pmatrix} n-j \\ i-j \end{pmatrix} \zeta^{j-1}(1-\zeta)^{i-j}\pi_h^{j-i}e_{ij}.$$

In the field $\mathbf{Q_p}$ the prime p factorizes as $(1-\zeta)^{p^{m-1}(p-1)}$. The entries of the first column of $\Delta'(a)$ (except the first one) are divisible by p, all of them lower than $-\binom{t}{p^{m-1}(p-1)}$ are even divisible by p^2, and π_h divides $(1-\zeta)$, therefore, all subdiagonal entries of $\Delta_h(a)$ (except the first one) are divisible by π_h^{i-j}. The same is true for the matrix $\Delta'(b)$, and the representations Δ_h are integral in O_K, and they are contained in the kernel of reduction $(mod\pi_h)$. Moreover, the matrices $\Delta_h(a) \equiv I_t(mod\pi_h)$, but $\Delta_h(a) \not\equiv I_t(mod\pi_h^2)$. Thus Δ_h and Δ_r are not equivalent over O_K if $h \neq r$. This gives an explicit construction of an infinite series of pairwise integrally inequivalent representations over O_K. Thus we have the following theorem:

THEOREM 1. *Let L denote $\mathbf{Q_p}(\zeta_{\mathbf{p}^\infty})$, the extension of $\mathbf{Q_p}$ obtained by adjoining all roots $\zeta_{p^i}, i = 1, 2, 3, ...$ of p-primary orders of 1. Let G be a finite nonabelian two-generator p-group admitting representations by matrices $\Delta(a), \Delta(b)$ above, and let O_L be the ring of integers of L. Then there is an infinite number of integral pairwise inequivalent absolutely irreducible representations of G over O_L.*

We shall extend the construction of Δ_h from theorem 1 above first to the case of a nonabelian p-group G_1 generated by its center Z and elements a, b with central nontrivial commutator $c = [a, b] = aba^{-1}b^{-1}$. Let χ be a character of Z such that $\chi(c) = \zeta \neq 1$ for a primitive root of 1 of some degree $t = p^m$. There is an absolutely irreducible representation of G_1 extending χ; the central elements z correspond to scalar matrices $\chi(z)I$, and let us denote by C_χ the kernel of χ. Let us denote by C_χ the kernel of χ. Then we have a representation of the factorgroup $G_\chi = G_1/C_\chi$. Let $Z_\chi \subset G_1$ be the preimage of the center of G_χ; it consists of the elements $x \in G_1$ such that $\chi(xax^{-1}a^{-1}) = \chi(xax^{-1}a^{-1}) = 1$. It is also clear that $a^t \in Z_\chi$ and $b^t \in Z_\chi$, since $\chi(a^taa^{-t}a^{-1}) = \chi(xax^{-1}a^{-1}) = 1, \chi(a^tba^{-t}b^{-1}) = \chi(c) = 1$ and $\chi(b^tbb^{-t}b^{-1}) = \chi(b^tab^{-t}a^{-1}) = 1$. The same computation shows that powers of a and b lower than t^{th} powers are not contained in Z_χ. Further, Z_χ/C_χ is an abelian group containing Z/C_χ, and we can extend the character χ of Z/C_χ to Z_χ/C_χ, and thereby to a linear character of Z_χ. In the absolutely irreducible representation Δ of G_1 such that $\Delta(z) = \chi(z)I$, the elements x correspond to scalar matrices $\chi_1(z)I$ for the extension χ_1 of the character $\chi(z)$ to Z_χ.

Denote $\zeta_1 = \sqrt[t]{\chi_1(a^t)}$ and $\zeta_2 = \sqrt[t]{\chi_1(b^t)}$. The matrices $\Delta_h(z) = \chi(z)I$, for $z \in Z_\chi$, together with $\Delta_h(a) = \zeta_1 A_h$ and $\Delta_h(b) = \zeta_2 B_h$ determine a representation of G_1, and since $\zeta_1 = \zeta_2 (mod \pi_h)$ for sufficiently large n, for large enough distinct n and n' the integral representations Δ_h and $\Delta_{h'}$ are integrally inequivalent.

Now let us consider an arbitrary p-group G of the nilpotency class 2 having the center Z. For every character χ of the center let us denote its kernel by C_χ. Denote by $Z_\chi \subset G$ be the preimage of the center of G/C_χ. Then Z_χ is the set of of the elements $x \in G$ such that $\chi(xyx^{-1}y^{-1}) = 1$ for all $y \in G$. Let χ_1 be an extension of χ from Z/C_χ to Z_χ/C_χ. In the absolutely irreducible representation of G extending the representation $\chi(z)I_n$ of the center, the elements $y \in Z_\chi$ correspond to scalar matrices $\chi(y)I_n$. Let us assume that the commutator subgroup G' of G is not 1, and $G \neq Z_\chi$.

Let us define an "inner product" $(x, y) = \chi([x, y])$, where $x, y \in G$ and $[x, y] = x^{-1}y^{-1}xy$.

The following lemma is well known in the theory of nilpotent groups and can be checked by a direct calculation of commutators $[x, y]$.

LEMMA 1. *Suppose G is a nilpotent group of nilpotency class is two. Then, for any element $x \in G$, the map*

$$y \mapsto [x, y]$$

is an endomorphism of G.

The image of these endomorphism lie in the commutator subgroup G' of G, hence in the center of G, so it is abelian. The kernel of this endomorphism contains the center of the group, more specifically, it is the centralizer of x in G.

PROOF. Consider an element $x \in G$. Since G has nilpotency class two, the commutator $[x, y] = xyx^{-1}y^{-1}$ is in the center Z of G, and hence it commutes with any $y \in G$.

Let $y_1, y_2 \in G$. Since $[x, y_2] \in Z$, we have
$[x, y_1][x, y_2] = [x, y_1]y_1[x, y_2]y_1^{-1} = xy_1x^{-1}y_1^{-1}y_1xy_2x^{-1}y_2^{-1}y_1^{-1}$
$= xy_1y_2x^{-1}y_2^{-1}y_1^{-1} = [x, y_1y_2]$. This completes the proof of lemma 1. □

The above inner product $(x, y) = \chi([x, y])$ is multiplicative in both arguments and antisymmetric, since $(x, x) = 1$. The value of (x, y) depends only on cosets containing x and y modulo Z_χ. Thus we can view (x, y) as being defined on $G_\chi = G/Z_\chi$. The product (x, y) is nondegenerate on this group by the definition of Z_χ. Now G_χ is an abelian p-group. Let $a, b, ...$ be the generators of its cyclic direct factors. The values of (x, y) are roots of 1 of degrees that are powers of p. They are generated by the values of the symbol (x, y) on the generators. Therefore, there is a pair of generators on which the value of the symbol is a root of 1 of the highest possible degree $t = p^m$. Let a and b be such generators, and let $(a, b) = \zeta = \sqrt[t]{1}$. Thus $a^t = b^t$ in G_χ.

LEMMA 2. *G_χ is the direct product of the group H generated by 2 elements a and b and its orthogonal product $H^\perp$. In particular, the number of generators is even, and they are divided to pairs a_i, b_i such that the generators from different pairs are orthogonal, the orders of a_i and b_i are equal, and the degrees of the roots (a_i, b_i) of 1 are equal.*

PROOF. Suppose that $x \in G_\chi$. Then $(x, a) = \zeta^{k_1}$ and $(x, b) = \zeta^{k_2}$. for some integers k_1, k_2. Then we have $(x \cdot a^{-k_2}b^{k_1}, b) = 1$, thus $x \cdot a^{-k_2}b^{k_1} \in H^\perp$, and $H \cdot H^\perp = G_\chi$. Any element $u \in H \bigcap H^\perp$ is orthogonal to both H and $H^\perp$, and thus to all $G_\chi = H \cdot H^\perp$ and since the symbol (x, y) is nondegenerate, $u = 1$. This argument implies that G_χ is a direct product of H and $H^\perp$. We can apply the same argument to $H^\perp$ and use induction on the number of generators G. Finally we find that G can be expressed as a direct product of pairwise orthogonal two-generator subgroups.

Let A_i and B_i be representatives in G of the classes of a_i and b_i from the constituents of G/Z_χ. Then both $A_i^{t_i} = B_i^{t_i}$ are contained in Z_χ, and

$$\chi(a_ib_ia_i^{-1}b_i^{-1})\zeta_{t_i} = \sqrt[t_i]{1},$$

and the values of χ on commutators of elements from different pairs are all equal 1.

The representation of G extending the character χ_1 of Z_χ is also a representation of an algebra over K (K is $Q_p(\zeta)$) with generators $u_1, v_1, \ldots, u_s, v_s$ with multiplication given by $u_i^{t_i} = \chi_1(A_i^{t_i}), v_i^{t_i} = \chi_1(B_i^{t_i}), u_iv_i = v_iu_i\zeta_{t_i}$, and the generators from different pairs commute. This algebra is a tensor product over K of the algebras generated by the pairs u_i, v_i, and representations of these algebras are representations of groups of type G_1 as considered above. These algebras determine symbols $K[u, v]$ satisfying the properties of Hilbert symbol which can be identified with an element

of the Brauer group (see [12], theorem A.2.3, p. 142). Note that the degree of the irreducible representation of each two-generator group $\langle u_i, v_i\rangle$ described above is equal to p^{t_1}. Compare section 2 in [10].

LEMMA 3. *Let G be a two-generator group $\langle u, v\rangle$ as above with cyclic center $Z = \langle c\rangle$ of order p^n, and the order of $(u, v) = d$ is p^t. For $p \neq 2$ we can find the generators u, v of the group G above in such a way that either $u^{p^t} = 1$ or $v^{p^t} = 1$ for $p \neq 2$.*

PROOF. We can use our previous remarks and replace the generators in the following way: if neither of the conditions $u^{p^t} = 1$ or $v^{p^t} = 1$ is true, and the order of u does not exceed the order of v, then we can change v: consider $v_0 = u^r v$, then $[u, v] = S$ is in Z, the order of $[u, v]$ is d, and computations of the commutators show that $v_0 = (u^r v)^{p^t} = u^{rp^t} v p^t S^{-\frac{rp^t(p^t-1)}{2}}$, and $v_0 = 1$ for an appropriate choice of an integer r if $p \neq 2$, and we can take the generators u, v_0 instead of u, v; this replacement will not change the group $\langle u, v\rangle$. □

This implies that the number of O_K-inequivalent representations of G is infinite.

The constructed representations are contained in the kernel of reduction modulo some prime divisor $\mathcal{P}$ of p.

Further let us formulate the following propositions based on results. Note that there are some general results on the classification of two-generator p-groups G of the nilpotency class 2, see [2], [25], see also earlier papers: [1], theorem 2.6, [14], theorem 2.5.

PROPOSITION 2. *[21] or [22], Satz 6.1, p. 291. Let G be a minimal nonabelian p-group. Then $G = \langle a, b\rangle$ and one of the following holds:*
(a) $A^{p^m} = B^{p^n} = C^p = 1, [A, B] = C, B_h^2 = A_h^{-m}, [A, C] = [B, C] = 1$ is not metacyclic. Furthermore, this group is not metacyclic and in the case $p = 2$, we have $m \geq n; m \geq 2$.
Also, $|G| = p^{m+n+1}; G' = \langle C\rangle$ and $Z(G) = \langle A^p\rangle \times \langle B^p\rangle \times \langle C\rangle$;
(b) $G = Q_8$ is the group of quaternions of order 8;
(c) $G = \langle A, B | A^{p^m} = B^{p^n} = C^p = 1, [A, B] = A^{p^{m-1}}\rangle$ is metacyclic.

PROPOSITION 3. *[3]. Let G be a 2-generated finite 2-group and $|G'| = 2$. Then G is minimal nonabelian.*

Now we can extend theorem 1 to representations (which are not always faithful) of an arbitrary p-group G. First, let us observe that among the representations of G there occur the absolutely irreducible representations of the factor-group by the third term of the lower central series, and this is nilpotent of class 2. We can also observe that the absolutely irreducible representations of the factor-group by the

orthogonal complement $H^{\perp}$ to any two-generator subgroup $H = \langle u, v\rangle \subset G$ are also the representations of G. If H is not abelian, any its faithful absolutely irreducible representation will be an absolutely irreducible representation of G. Using lemma 3, we can start from the representation determined by matrices A and B together with scalar $p^k \times p^k$-matrices composing the centre $Z = \langle c\rangle$ of G:

$$A' = \Delta(a) = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \dots & \ddots & \dots \\ 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix},$$

$$B' = \Delta(b) = diag(1, \zeta, \dots, \zeta^{t-1})$$

Let the order of Z be p^m, and let ϵ be a primitive p^m-root of 1. Let $u^{p^k} = 1$, $v^{p^k} = c^f$, $\zeta = \epsilon^{p^{m-k}}$, $\theta = \epsilon^{c^f}$ Then the representation Δ_h of H determined by

$u \to A$, $v \to \theta B' = B$, $c \to \epsilon I' = C$ is absolutely irreducible and faithful. As earlier, we can obtain the integral representation by matrices congruent to the unit matrix $I \pmod{\mathcal{P}}$:

$$A_h = \Delta_h(a) = D_h^{-1}C^{-1}A'CD_h = \begin{pmatrix} 1-t & \pi_h & 0 & \dots & 0 & 0 \\ -\binom{t}{2}\pi_h^{-1} & 1 & \pi_h & \dots & 0 & 0 \\ \dots & \dots & \ddots & \ddots & \dots & \dots \\ -\binom{t}{t-1}\pi_h^{2-t} & 0 & 0 & \dots & 1 & \pi_h \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

$$B_h = \Delta_h(b) = D_h^{-1}C^{-1}B'CD_h = \sum_{n\geq i\geq j\geq 1} \begin{pmatrix} t-j \\ i-j \end{pmatrix} \zeta^{j-1}(1-\zeta)^{i-j}\pi_h^{j-i}e_{ij}.$$

In the case $p = 2$ we can consider a character χ of $Z \subset G = \langle u, v\rangle$ as earlier, and for the subgroup $\langle [u, v]\rangle = C \subset Z$ generated by the commutator $c = [u, v]$. Let $\chi(c) = \gamma \neq 1$ be an element of of order 2^x; then and for $\chi^{2^{x-1}}$ the image of the commutator subgroup $G' \subset G$ is a group of order 2, the image $\chi^{2^{x-1}}(G)$ is nonabelian, we can apply Propositions 2 and 3 together with examples 1) - 3) for constructing an infinite series of pairwise inequivalent representations of G of the minimal degree. Alternatively, we can use our construction from theorem 1.

Thus we have the following

THEOREM 2. *Let L denote $\mathbf{Q_p}(\zeta_{\mathbf{p}^\infty})$, the extension of $\mathbf{Q_p}$ obtained by adjoining all roots $\zeta_{p^i}, i = 1, 2, 3, \dots$ of p-primary orders of 1. Let us fix the degree t of matrix representations. Let G be any finite nonabelian p-group, and let O_L be the ring of*

integers of L. Then there is an infinite number of integral pairwise inequivalent absolutely irreducible representations of finite groups G in $GL_n(O_L)$.

The constructed representations are contained in the kernel of reduction $I_t \pmod{\mathcal{P}}$ modulo some prime divisor $\mathcal{P}$ of p.

Remark. *Our construction applied to two-generator nonabelian subgroups gives the representations of G having minimal possible degrees.*

The results above preceding theorem 2 (in particular, lemma 2) can be reformulated for some supersolvable groups and used for classification of absolutely irreducible primitive representations of the absolute Galois groups of local fields, see (see [16], theorem 2.2), see also [26], [27] and [23].

4. Some related topics and applications

PROPOSITION 4. *Let G be a finite group, H – its normal p-subgroup, let G/H be supersolvable, $\rho : G \to GL_n(\mathbf{C})$ – a faithful primitive representation. Then:*

- *$n = p^d$. The center $Z = Z(H)$ is cyclic of order p^z, and for $c \in Z$ of order p there are elements $u_1, v_1, \ldots, u_d, v_d$ which together with Z generate H and satisfy the generating relations: $[u_i, u_j] = [v_i, v_j] = 1$, $[u_i, v_j] = c^{\delta_{i,j}}$, where $\delta_{i,j}$ is the Kronecker's delta, $(i, j = 1, \ldots, d)$, and the generators from different pairs commute.*

- *There are 2 possibilities:*

  1) $u^p = v^p = 1$ for $p \neq 2$

  2) $u^p = v^p = c$ (quaternion type), or $u^p = v^p = 1$ (dihedral type) for $p = 2$.

- *H/Z is p-elementary abelian of order p^{2d}*

- *H has $(p-1)p^{z-1}$ inequivalent faithful absolutely irreducible representations*

This result is closely related to the embedding problem with a nonabelian kernel for local fields which has been studied in [12] and [10].

Let

$$1 \to B \to G \xrightarrow{\varphi} F \to 1$$

be an exact sequence of p-groups, K/k be a Galois extension of a local field with the Galois group F, and $p > 2$ be the characteristic of the residue field $\mathbf{Q_p}$ of k. The embedding problem consists in constructing an extension L of K having the Galois group G over k, such that the automorphisms $g \in G$, being restricted on K, coincide with $\varphi(g)$. The associated abelian problem is a similar problem for the sequence

$$1 \to B/B' \to G/B' \to F \to 1$$

where B' is the commutator subgroup of B; the solution of the abelian embedding problem is well known. Let $\overline{F}$ be the Demushkin group of k, that is, the Galois group of the maximal p-extension of k. The number $d(\overline{F})$ of generators of the group $\overline{F}$ is equal to $[k\colon \mathbf{Q_p}]+\mathbf{2}$. Let $d(F)$ be the number of generators of F. In [10] the authors prove that if $d(\overline{F}) \geqslant d(F)+3$ then the embedding problem is equivalent to the associated abelian problem. In the proof they used the generalized Hilbert symbol and orthogonality of elements of k^*/k^{*p} for an option of a basis k^*/k^{*p} and abelian radical extensions of k and for the fulfillment of the Faddeev-Hasse compatibility conditions. In our argument above we used similar techniques.

In his recent publication [24] 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. This was also considered in our recent paper [17] 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 [20].

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, the ring of integers of K, i. e. is ρ conjugate to a homomorphism of G into $GL_n(O_K)$?

Another approach to generalization of integral representations of finite groups was proposed by D. K. Faddeev in [8] (see also [9]) where a generalization of the theory of Steinitz and Chevalley has been suggested.

Remark that in the paper by Serre [24] only imaginary quadratic fields $\sqrt{\mathbf{Q}(-\mathbf{d})}$, $\mathbf{d} > \mathbf{0}$, were considered as realization fields for representations of the group G of quaternions.

It would be interesting to find the conditions for realizations of $G \subset GL_2(O_K)$ for any algebraic number field. The necessary condition is that K should be a splitting field of G, or in the terms of Hilbert symbol,

$$\left(\frac{-1,-1}{K}\right) = 1.$$

PROPOSITION 5. *(1) An algebraic number field K is a splitting field for 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 $[K_v : \mathbf{Q_2}]$ is even.*

(2) If (1) is true, then $[K : \mathbf{Q}]$ is even.

(3) If (1) is true and $K/\mathbf{Q}$ is abelian, then K has a quadratic subfield $\mathbf{Q}(\sqrt{\mathbf{d}})$.

PROOF. By Hasse-Brauer-Noether theorem, K is a splitting field for $\langle G\rangle_{\mathbf{Q}} = \mathbf{QG}$, $\mathbf{Q}$-span of G, if and only if K_v is a splitting field for $\langle G\rangle_{\mathbf{Q}_p} = \mathbf{Q_p}G$ locally 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 $[K_v : \mathbf{Q_2}]$ is even [6], Satz 2, ch. VII, sect. 5.

Since $[K : \mathbf{Q}]$ is the sum of $[K_v : \mathbf{Q_2}]$, it must be even, and this implies (2).

If $K/\mathbf{Q}$ 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 $\mathbf{Q}$.

This completes the proof of Proposition 5. □

Let us consider two examples.

1) We can use our construction in the case of the generalized quaternion group G generated by A_h and B_h, $A_h^{2m} = 1, [A_h, B_h] = B_h A_h B_h^{-1} A_h^{-1} = A_h^{-2}, B_h^2 = A_h^{-m}$ we can use the following construction of an infinite series of pairwise integrally inequivalent over O_K representations in $GL_2(O_K)$:

$$A_h = \Delta_h(b) = \begin{pmatrix} \zeta^{-1} & \pi_h \\ 0 & \zeta \end{pmatrix},$$

where ζ is a primitive $2m$-root of 1,

$$B_h = \Delta_h(a) = \begin{pmatrix} 1 & \frac{-2\pi_h\zeta}{\zeta^2-1} \\ \frac{\zeta^2-1}{\zeta\pi_h} & -1 \end{pmatrix}.$$

2) For the following finite extension $K/\mathbf{Q_p}$ 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 $\mathbf{Z_p}$ with supersingular good reduction (see [24], sect. 1.11). Let $K/\mathbf{Q_p}$ 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 $\mathbf{Z_p}$, 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 $e = e(K/\mathbf{Q_p}) = \mathbf{p^2 - 1}$ ([24], p. 275, Proposition 12).

We can consider the group G of p-torsion points as $\mathbf{Z_p}$-algebra homomorphisms from the Hopf algebra O_A to the $\mathbf{Z_p}$-algebra O_K, then
$G = Hom_{\mathbf{Z_p}}(O_A, O_K)$, and the algebra O_A is isomorphic to $\mathbf{Z_p}[\mathbf{X}]/(\mathbf{c_1 X} + \mathbf{c_2 X^2} + ... + \mathbf{X^{p^2}})$, see [5], sect.2 and [15]. So there is a representation $v : G \to GL_{p^2}(O_K)$, and since E is supersingular, the image of v is contained in the kernel of reduction modulo $\mathcal{P}$.

5. Conclusion

There are many classical results related to the description of integral representations of finite groups over Dedekind rings R, especially for the rings of integers $\mathbf{Z}$ or p-adic integers $\mathbf{Z_p}$ and maximal orders of local fields or fields of algebraic numbers. Some of them given by P. M. Gudivok, A. V. Roiter, A. V. Yakovlev, W. Plesken go back to the classification of irreducible and indecomposable representations that can give an explicit description only for certain classes of groups and rings R. There are classification results for finite, wild and tame representation types, including the classification of arbitrary commutative R-rings having finitely many non-isomorphic

indecomposable integral representations. For an explicit description it is important to find matrix realizations of the representations, and one of possible approaches is to describe maximal finite subgroups of $GL_n(R)$ over Dedekind rings R for a fixed positive integer n. The basic idea underlying a geometric approach was given in Ryshkov's papers on the computation of the finite subgroups of $GL_n(\mathbf{Z})$ and further papers by W. Plesken and M. Pohst. However, it was not clear, what happens under the extension of the Dedekind rings R in general, and in what way the representations of arbitrary p-groups, supersolvable groups or groups of a given nilpotency class can be approached. In this paper the above classes of groups are treated, in particular, it is proven that for a fixed n and any given nonabelian p-group G there is an infinite number of pairwise non-isomorphic absolutely irreducible representations of G. The series of these representations is constructed explicitly. We study group representations with extra properties of congruences, and we give some links to representations arising from elliptic curves. The integral representations in question are very sensitive to changing the ground ring and the ramification index. Besides, the group of units of the Dedekind rings R, especially its torsion subgroup, plays an important role.

There are some applications to the embedding problem in Galois theory, globally irreducible representations and Schur rings which are discussed in proposition 4 and section 2 of the paper. Throughout the paper we give examples of particular representations. There are some more applications, which can be considered for the group representations with extra properties of congruences in our construction, arising from the class of Galois stable subgroups of $GL_n(R)$ and considered earlier in [18]. Besides a score of generalizations, finite groups that are stable under Galois action have some interaction with seemingly unrelated results in the theory of definite quadratic forms and Galois cohomologies of certain arithmetic groups.

Acknowledgement: The author is grateful to the referees for many useful remarks and suggestions which improved the paper essentially.

REFERENCES

1. Bacon, M. & Kappe, L. C. 1993, "The nonabelian tensor square of a 2-generator p-group of class 2" , *Arch. Math.*, vol. 61, pp. 508–516.

2. Ahmad, A., Magidin, A. & Morse, R. 2012, "Two generator p-groups of nilpotency class 2 and their conjugacy classes" , *Publ. Math. Debrecen*, vol. 81, no. 1-2, pp. 145–166.

3. Cepulic, V. & Pyliavska, O. S. 2006, "A class of nonabelian nonmetacyclic finite 2-groups" , *Glasnik matematicki*, vol. 41(61), pp. 65–70.

4. Curtis, Ch. W. & Reiner, I. 1962, "Representation theory of finite groups and associative algebras" , Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006. xiv+689 pp. ISBN: 0-8218-4066-5

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

6. Deuring, Max 1968, "Algebren." , (German) Zweite, korrigierte auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, *Springer-Verlag, Berlin-New York*, B. 41, viii+143 pp.

7. Faddeev, D. K. 1998, "On generalized integral representations over Dedekind rings" , *J. Math. Sci. (New York)*, vol. 89, no. 2, pp. 1154–1158.

8. Faddeev, D. K. 1961, "Tables of the fundamental unitary representations of the Fedorov groups" , *Trudy Mat. Steklov Inst.*, vol. 56, pp. 3–174. (Russian)

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

10. Ishkhanov, V. V. & Lur'e, B. B. 2009, "An embedding problem with a nonabelian kernel for local fields" , *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, vol. 365, Voprosy Teorii Predstavlenii Algebr i Grupp. 18, pp. 172–181, 264 (Russian); translation in *J. Math. Sci. (N. Y.)*, vol. 161 (2009), no. 4, pp. 553–557.

11. Isaacs, I. 1976, "Martin Character theory of finite groups." Pure and Applied Mathematics, No. 69. *Academic Press* [Harcourt Brace Jovanovich, Publishers], *New York-London*, xii+303 pp.

12. Ishkhanov, V. V., Lur'e, B. B. & Faddeev, D. K. 1997, "The embedding problem in Galois theory." Translated from the 1990 Russian original by N. B. Lebedinskaya. Translations of Mathematical Monographs, 165. *American Mathematical Society, Providence, RI*, xii+182 pp. ISBN: 0-8218-4592-6

13. Knapp, W. & Schmidt, P. 1997, "An extension theorem for integral representations" , *J. Austral. Math. Soc. (Ser. A)*, vol. 63, pp. 1–15.

14. Kappe, L. C., Sarmin, N. & Visscher, M. 1999, "Two-generator 2-groups of class two and their nonabelian tensor squares" , *Glasgow Math. J.*, vol. 41, pp. 417–430.

15. Kolyvagin, V. A. 1979, "Formal groups and the norm residue symbol" , *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 43, no. 5, pp. 1054–1120. (Russian) (=Math. USSR Izvestija, 1980, vol. 15(2), pp. 289–348.)

16. Koch, H. 1977, "Classification of the primitive representations of the Galois group of local fields." , *Inventiones Math.*, vol. 40, pp. 195–216.

17. Malinin, D. & Van Oystaeyen, F. 2011, "Realizability of two-dimensional linear groups over rings of Integers of algebraic number fields" , *Algebras and Representation Theory*, vol. 14, nr. 2, pp. 201–211.

18. Malinin, D. 2001, "Galois stability for integral representations of finite groups" , *Algebra i Analiz, St.-Petersburg Math. J.*, vol. 12, nr. 3, pp. 423–449.

19. Malinin, D. 1998, "Integral representations of p-groups of given nilpotency class over local fields" , *St.-Petersburg Math. J.*, vol. 10, nr. 1, pp. 45–52.

20. Van Oystaeyen, F. & Zalesskiĭ, A. E. 1999, "Finite groups over arithmetic rings and globally irreducible representations" , *J. Algera*, vol. 215, pp. 418–436.

21. Redei, L. 1947, "Das schiefe Produkt in der Gruppentheorie" , *Comment. Math. Helvet.*, vol. 20, pp. 225–267.

22. Redei, L. 1989, "Endliche p-Gruppen" , *Budapest: Akademiai Kiado.*

23. Rigby, J. F. 1960, "Primitive linear groups containing a normal nilpotent subgroup larger than the centre of the group." , *J. London Math. Soc.*, vol. 35, pp. 389–400.

24. Serre, J.-P. 2008, "Three letters to Walter Feit on group representations and quaternions." , *J. Algebra*, vol. 319, nr. 2, pp. 549–557.

25. Song, Qiangwei 2013, "Finite two-generator p-groups with cyclic derived group" , *Communications in Algebra*, vol. 41, no. 4, pp. 1499–1513.

26. Yakovlev, A. V. 1964, "The embedding problem of fields" , *Izv. Akad. Nauk SSSR Ser. Mat.* vol. 28, no. 3, pp. 645–660. (Russian)

27. Demushkin, S. P. & Shafarevich, I. R. 1959, "The embedding problem for local fields" , *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 23, no. 6, pp. 823–840. (Russian)

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. M. Bacon, L. C. Kappe The nonabelian tensor square of a 2-generator p-group of class 2 // Arch. Math. 1993. Vol. 61. P. 508–516.

2. A. Ahmad, A. Magidin, R. Morse Two generator p-groups of nilpotency class 2 and their conjugacy classes // Publ. Math. Debrecen. 2012. Vol. 81, № 1-2. P. 145–166.

3. V. Cepulic, O. S. Pyliavska A class of nonabelian nonmetacyclic finite 2-groups // Glasnik matematicki. 2006. Vol. 41(61). P. 65–70.

4. Ch. Curtis, I. Reiner Representation theory of finite groups and associative algebras. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006. xiv+689 pp. ISBN: 0-8218-4066-5

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

6. Deuring, Max Algebren. (German) Zweite, korrigierte auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 41 Springer-Verlag, Berlin-New York 1968. viii+143 pp.

7. D. K. Faddeev On generalized integral representations over Dedekind rings // J. Math. Sci. (New York). 1998. Vol. 89, no. 2. P. 1154–1158.

8. Д. К. Фаддеев Таблицы основных унитарных представлений федоровских групп // Тр. МИАН СССР. 1961. Т. 56. С. 3–174.

9. Д. К. Фаддеев Введение в мультипликативную теорию модулей целочисленных представлений // Тр. МИАН СССР. 1965. Т. 80. С. 145–182.

10. В. В. Ишханов, Б. Б. Лурье Задача погружения с неабелевым ядром для локальных полей // Зап. научн. сем. ПОМИ. 2009. Т. 365. С. 172–181.

11. I. M. Isaacs Character Theory of finite groups. Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976. xii+303 pp.

12. V. V. Ishkhanov, B. B. Lurje, D. K. Faddeev The Embedding Problem in Galois Theory. Volume 7; Transl. Math. Monographs, AMS. 1997. Vol. 165.

13. W. Knapp, P. Schmidt An extension theorem for integral representations // J. Austral. Math. Soc. (Ser. A). 1997. Vol. 63. P. 1–15.

14. L. C. Kappe, N. Sarmin, M. Visscher Two-generator 2-groups of class two and their nonabelian tensor squares // Glasgow Math. J. 1999. Vol. 41. P. 417–430.

15. В. А. Колывагин Формальные группы и символ норменного вычета // Изв. АН СССР. Сер. матем. 1979. Т. 43, № 5. С. 1054–1120 (=Math. USSR Izvestija, 1980, vol. 15(2), p. 289–348.)

16. H. Koch Classification of the primitive representations of the Galois group of local fields // Inventiones Math. 1977. Vol. 40. P. 195–216.

17. D. A. Malinin, F. Van Oystaeyen Realizability of two-dimensional linear groups over rings of Integers of algebraic number fields // Algebras and Representation Theory. 2011. Vol. 14, nr. 2. P. 201–211.

18. Д. А. Малинин Целочисленные представления конечных групп, устойчивые при действии группы Галуа // Алгебра и анализ. 2000. Т. 12, № 3. С. 106–145.

19. Д. А. Малинин Целочисленные представления p-групп заданного класса нильпотентности над локальными полями // Алгебра и анализ. 1998. Т. 10, № 1. С. 58–67.

20. F. Van Oystaeyen, A. E. Zalesskiĭ Finite groups over arithmetic rings and globally irreducible representations // J. Algera. 1999. Vol. 215. P. 418–436.

21. L. Redei Das schiefe Produkt in der Gruppentheorie // Comment. Math. Helvet. 1947. Vol. 20. P. 225—267.

22. L. Redei Endliche p-Gruppen. Budapest: Akademiai Kiado. 1989.

23. J. F. Rigby Primitive linear groups containing a normal nilpotent subgroup larger than the centre of the group // J. London Math. Soc. 1960. Vol. 35. P. 389–400.

24. J.-P. Serre Three letters to Walter Feit on group representations and quaternions // J. Algebra. 2008. Vol. 319, nr. 2. P. 549–557.

25. Song Qiangwei Finite two-generator p-groups with cyclic derived group // Communications in Algebra. 2013. Vol. 41, no 4. P. 1499–1513.

26. А. В. Яковлев Задача погружения полей // Изв. АН СССР. Сер. матем. 1964. Т. 28, № 3. С. 645–660.

27. С. П. Демушкин, И. Р. Шафаревич Задача погружения для локальных полей // Изв. АН СССР. Сер. матем. 1959. Т. 23, № 6. С. 823–840.

Department of Mathematics, University of the West Indies, Mona, Kingston 7, Jamaica.
Received 10.07.2015