One construction of integral representations of p-groups

Dmitry Malinin

Department of Mathematics
UWI

ISCHIA GROUP THEORY 2014

The construction for 2-generated p-groups

Let K be a finite extension of either the rational p-adic field $\mathbb{Q}_p$, or the field $\mathbb{Q}$ of rationals, and let O_K be its ring of integers. Consider a group G_0 generated by two elements a and b of order $t = p^m$, a^t=b^t=1 such that the commutator $c = [a, b]$ is contained in the center of G_0, and c^t=1. Let ζ be a primitive root of 1 of degree t.

A combinatorial construction

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

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

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

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

and if we take $x = 1$, this will imply $C^{-1} = C_1$.

A combinatorial construction

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

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

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

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

and if we take $x = 1$, this will imply $C^{-1} = C_1$.

The construction for 2-generated p-groups

The following representation of G_0 is faithful and absolutely irreducible.

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

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

The construction for 2-generated p-groups

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

$$C^{-1}XC = \sum_{n \geq i \geq j \geq 1} \binom{n-j}{i-j} x^{j-1}(1-x)^{i-j} e_{ij},$$

If we take $x = \zeta$, we will obtain:

$$\Delta'(b) = C^{-1}\Delta(b)C = C^{-1}BC = \sum_{n \geq i \geq j \geq 1} \binom{n-j}{i-j} \zeta^{j-1}(1-\zeta)^{i-j} e_{ij},$$

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

The construction for 2-generated p-groups

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

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

If we take $x = \zeta$, we will obtain:

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

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

The construction for 2-generated p-groups

Consider a finite extension $L_h = K(\zeta)$ of K, 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 $\zeta_{p^m} - 1$ in a cyclotomic field $K = \mathbb{Q}(\zeta_{p^m})$ or $K = \mathbb{Q}_p(\zeta_{p^m})$, where ζ_{p^m} is a primitive p-root of 1. Let $D = diag(1, \pi_h, \pi_h^2, \dots, \pi_h^{t-1})$, then

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

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

The construction for 2-generated p-groups

Consider a finite extension $L_h = K(\zeta)$ of K, 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 $\zeta_{p^m} - 1$ in a cyclotomic field $K = \mathbb{Q}(\zeta_{p^m})$ or $K = \mathbb{Q}_p(\zeta_{p^m})$, where ζ_{p^m} is a primitive p-root of 1. Let $D = diag(1, \pi_h, \pi_h^2, \ldots, \pi_h^{t-1})$, then

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

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

The construction of a representation of p-groups

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 construction of a representation of p-groups

This 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 $a, b, \ldots$ 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. *G_χ is the direct product of the group H generated by 2 elements a and b and its orthogonal complement $H^\perp$. 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.*

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 $\chi(a_i b_i a_i^{-1} b_i^{-1}) = \zeta_{t_i} = \sqrt[t_i]{1}$, and the values of χ on commutators of elements from different pairs are all equal 1.

Lemma. *G_χ is the direct product of the group H generated by 2 elements a and b and its orthogonal complement $H^\perp$. 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.*

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 $\chi(a_i b_i a_i^{-1} b_i^{-1}) = \zeta_{t_i} = \sqrt[t_i]{1}$, and the values of χ on commutators of elements from different pairs are all equal 1.

The construction of a representation of p-groups

K – $\mathbb{Q}_p(\zeta_{p^\gamma})$ or $\mathbb{Q}(\zeta_{p^\gamma})$. The representation of G extending the character χ_1 of Z_χ is also a representation of the algebra over K on generators $u_1, v_1, \ldots, u_s, v_s$ with multiplication given by $u_i^{t_i} = \chi_1(A_i^{t_i}), v_i^{t_i} = \chi_1(B_i^{t_i}), u_i v_i = v_i u_i \zeta_{t_i}$, 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 2-generated groups of type considered above. These algebras determine symbols $(u, v)_K$ satisfying the properties of Hilbert symbol which can be identified with an element of the Brauer group. Note that the degree of the irreducible representation of each two-generator group $< u_i, v_i >$ described above is equal to p^{t_1}.

Some related problems

D.K. Faddeev,1965,1995– Generalized integral representations

Problem 1. (W. Feit, J.-P. Serre). Given a linear representation $\rho : G \to GL_n(K)$ of finite group G over a number field $K/\mathbb{Q}$, is it conjugate to a representation $\rho : G \to GL_n(O_K)$ over O_K?

Global irreducibility, Schur rings – F. Van Oystaeyen and A.E. Zalesskii. R-span of a group $G \subset M(n, R) \Leftrightarrow$ Brauer reduction of $G(mod \mathfrak{p})$ is abs. irreducible for each prime ideal $\mathfrak{p}$ of R.

Problem 2. Describe the possible n and arithmetic rings R such that there is a globally irreducible $G \subset M(n, R)$. What happens for $n = 2$?

Theorem (Feit, Cliff, Ritter, Weiss). *If $G = Q_8$, $K = \mathbb{Q}(\sqrt{-35})$ and $\rho : G \to GL_2(K)$, Problem 1 has a negative answer.*

It is possible to describe the fields K where $G = Q_8$ is realizable in $GL_2(O_K)$, but Serre asked a question, whether it is possible to give the realization explicitly in the terms of lattices. Explicit constructions are recently given by D. M. and F. Van Oystaeyen

Some related problems

D.K. Faddeev,1965,1995– Generalized integral representations

Problem 1. (W. Feit, J.-P. Serre). Given a linear representation $\rho : G \to GL_n(K)$ of finite group G over a number field $K/\mathbb{Q}$, is it conjugate to a representation $\rho : G \to GL_n(O_K)$ over O_K?

Global irreducibility, Schur rings – F. Van Oystaeyen and A.E. Zalesskii. R-span of a group $G \subset M(n, R) \Leftrightarrow$ Brauer reduction of $G(mod \mathfrak{p})$ is abs. irreducible for each prime ideal $\mathfrak{p}$ of R.

Problem 2. Describe the possible n and arithmetic rings R such that there is a globally irreducible $G \subset M(n, R)$. What happens for $n = 2$?

Theorem (Feit, Cliff, Ritter, Weiss). *If $G = Q_8$, $K = \mathbb{Q}(\sqrt{-35})$ and $\rho : G \to GL_2(K)$, Problem 1 has a negative answer.*

It is possible to describe the fields K where $G = Q_8$ is realizable in $GL_2(O_K)$, but Serre asked a question, whether it is possible to give the realization explicitly in the terms of lattices. Explicit constructions are recently given by D. M. and F. Van Oystaeyen

Some related problems

D.K. Faddeev,1965,1995– Generalized integral representations

Problem 1. (W. Feit, J.-P. Serre). Given a linear representation $\rho : G \to GL_n(K)$ of finite group G over a number field $K/\mathbb{Q}$, is it conjugate to a representation $\rho : G \to GL_n(O_K)$ over O_K?

Global irreducibility, Schur rings – F. Van Oystaeyen and A.E. Zalesskii. R-span of a group $G \subset M(n, R) \Leftrightarrow$ Brauer reduction of $G(mod \mathfrak{p})$ is abs. irreducible for each prime ideal $\mathfrak{p}$ of R.

Problem 2. Describe the possible n and arithmetic rings R such that there is a globally irreducible $G \subset M(n, R)$. What happens for $n = 2$?

Theorem (Feit, Cliff, Ritter, Weiss). *If $G = Q_8$, $K = \mathbb{Q}(\sqrt{-35})$ and $\rho : G \to GL_2(K)$, Problem 1 has a negative answer.*

It is possible to describe the fields K where $G = Q_8$ is realizable in $GL_2(O_K)$, but Serre asked a question, whether it is possible to give the realization explicitly in the terms of lattices. Explicit constructions are recently given by D. M. and F. Van Oystaeyen

Classification of primitive representations of Galois Groups

Classification of absolutely irreducible primitive representations of the absolute Galois groups of local fields.

Theorem. G – a finite group, H – its normal p-subgroup, G/H supersolvable, $\rho : G \to GL_n(K)$ – faithful primitive. 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 $u_1, v_1, \dots, u_d, v_d$ which together with Z generate H and satisfy the generating relations: $[u_i, u_j] = [v_i, v_j] = 1$, $[u_i, v_j] = c^{\delta_{i,j}}$, $(i, j = 1, \dots, d)$, 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 irr. representations

Classification of primitive representations of Galois Groups

Classification of absolutely irreducible primitive representations of the absolute Galois groups of local fields.

Theorem. G – a finite group, H – its normal p-subgroup, G/H supersolvable, $\rho : G \to GL_n(K)$ – faithful primitive. 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: $[u_i, u_j] = [v_i, v_j] = 1$, $[u_i, v_j] = c^{\delta_{i,j}}$, $(i, j = 1, \ldots, d)$, 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 irr. representations