ON AUTOMORPHISMS OF THE INTEGRAL GROUP RINGS OF FINITE GROUPS

A.M. Popova

Novosibirsk State Technical University,
K. Marx Avenue, 20, Novosibirsk, 630073, Russia
e-mail: popovaam1946@yandex.ru

1 Preliminaries

We study automorphisms of the integral group rings of finite groups with the use of representation theory. If $T_1(G), \cdots, T_s(G)$ are all irreducible nonequivalent representations of G then consider the representation

$$D(G) = \{\mathrm{diag}(T_1(g), T_2(g), ..., T_s(g)), g \in G\}.$$

Obviously, $\mathbb{Z}G \cong \mathbb{Z}[D(G)]$. If χ_i is the character of the representation $T_i(G)$, $\mathbb{Q}(\chi_i)$ is the field of χ_i, $\tau \in \mathrm{Aut}(\mathbb{Q}(\chi_i))$, τ' is an extension of τ to an automorphism of the field of $T_i(G)$ then, on the algebra $\mathbb{Q}[T_i(G)]$, one can define an authomorphism $\hat{\tau'}$ by the rule $\hat{\tau'}((a_{ij})) = (a_{ij}^{\tau'})$.

In the article [1], the authors obtained a factorization of automorphisms of the integral group rings of finite groups by considering the ring $\mathbb{Z}[D(G)]$. In particular, we introduced the notion of a stabilizing automorphism, which is the composition $\hat{\tau'} \circ \varphi_s$, where φ_s is the conjugation by some unit s of the algebra $\mathbb{Q}[D(G)]$. The natural question arises whether for every $\tau \in \mathrm{Aut}(\mathbb{Q}(\chi_i))$ there is a matrix s such that the composition $\hat{\tau'} \circ \varphi_s$ is an automorphism of the ring $\mathbb{Z}[D(G)]$.

Pass from the ring $\mathbb{Z}[D(G)]$ to the isomorphic ring $\mathbb{Z}[R(G)^t]$, where $R(G)$ is the right regular representation of the finite group $G = \{e, g_2, \cdots, g_n\}$ and the matrix $t \in GL_n(\mathbb{C})$ is such that the matrices $(R(G))^t$ have cell-diagonal form in which each regular representation $T_i(G)$ occurs exactly n_i times, where n_i is the degree of this representation.

Our nearest aim is to formulate conditions under which such s exists.

Observe first of all that a necessary condition for the existence of such s is the coincidence of the $\mathbb{Q}$-algebras $\mathbb{Q}[R(G)^t]$ and $\mathbb{Q}[(R(G)^t)^{\hat{\tau'}}]$.

Agree to refer to the rings $\mathbb{Z}[T_i(G)]$ as *cells* of the ring $\mathbb{Z}[D(G)]$.

Between different cells of $\mathbb{Z}[D(G)]$, we have the mappings

$$\mu_{ij} : \sum_{g\in G} \alpha_g T_i(g) \longleftrightarrow \sum_{g\in G} \alpha_g T_j(g), \alpha_g \in \mathbb{Z},$$

which are isomorphisms or not.

Concerning the family of those cells $\mathbb{Z}[T_i(G)], i = 1, ..., s$, between which the mappings μ_{ij} are isomorphisms, we say that they *constitute a block*. If for a cell $\mathbb{Z}[T_i(G)]$ none of the mappings μ_{ij} is an isomorphism then the cell constitutes a block. If for a mapping $\mathbb{Z}[T_i(G)]$ there are cells $\mathbb{Z}[T_j(G)]$ such that μ_{ij} are isomorphisms, we may assume without loss of generality that these cells are $\mathbb{Z}[T_{i+1}(G)]$,...,$\mathbb{Z}[T_{i+k-1}(G)]$. Put

$$D_l(G) = \{\mathrm{diag}(T_i(g), ..., T_{i+k-1}(g)), g \in G\}.$$

Refer to the ring $O_l = \mathbb{Z}[D_l(G)]$ as a *block*. In such notations,

$$D(g) = \mathrm{diag}(D_1(g), ..., D_t(g)).$$

Lemma 1. *Suppose that cells $\mathbb{Z}[T_i(G)], \mathbb{Z}[T_{i+1}(G)], \ldots, \mathbb{Z}[T_{i+k-1}(G)], k \geqslant 1$, with the respective characters $\chi_i, ..., \chi_{i+k-1}$ constitute a block O. Then the degrees of the representations $T_i(G), \ldots, T_{i+k-1}(G)$ coincide, $k = |\mathrm{Aut}(\mathbb{Q}(\chi_i))|$, and the representation $T_{i+j}(G)$ is equivalent to the representation $\hat{\tau'}(T_i(G))$, where $\tau' \in \mathrm{Aut}(\mathbb{Q}(T_i(G)))$ is an extension of some automorphism $\tau \in \mathrm{Aut}(\mathbb{Q}(\chi_i))$ depending on j, $j = 0, ..., k-1$.*

Доказательство. All the cells $\mathbb{Z}[T_i(G)], \mathbb{Z}[T_{i+1}(G)], \ldots, \mathbb{Z}[T_{i+k-1}(G)]$ in the block O are isomorphic between each other.

In each cell $\mathbb{Z}[T_j(G)], j = i, \ldots, i+k-1$, consider the subring generated by the *class sums*

$$\sum_{g\in g_0^G} T_j(g) = \frac{|g_0^G|\chi_j(g_0)}{n_j} e_{n_j},$$

where g_0^G is the conjugacy class of an element $g_0 \in G$. Obviously, the mappings μ_{ij} define isomorphisms between the corresponding subrings. The quotient fields of these subrings are isomorphic, and each of them is isomorphic to its corresponding character field $\mathbb{Q}(\chi_j)$; therefore, the character fields are also isomorphic. Thus, every cell isomorphism induced by the mapping μ_{ij} is extendable to an isomorphism of the corresponding fields $\mathbb{Q}(\chi_i)$ and $\mathbb{Q}(\chi_j)$. Further, this isomorphism can be extended to some automorphism of a finite algebraic extension $K = \mathbb{Q}(\omega_l)$ containing the fields under consideration ([3]). The automorphisms of the represnetation field K of G take each character field $\mathbb{Q}(\chi_j) \subseteq K$ into itself, which yields the equalities $\mathbb{Q}(\chi_i) = \cdots = \mathbb{Q}(\chi_{i+k-1})$. Consequently, the mappings $\mu_{ij}, j = i+1, \ldots, i+k-1$, induce automorphisms of the character field $\mathbb{Q}(\chi_i)$.

Let $\tau_{ij} \in \mathrm{Aut}(\mathbb{Q}(\chi_i))$ be the automorphism induced by μ_{ij}, then

$$\frac{|g_0^G|(\chi_i(g_0))^{\tau_{ij}}}{n_i} = \left(\frac{|g_0^G|\chi_i(g_0)}{n_i}\right)^{\tau_{ij}} = \frac{|g_0^G|\chi_j(g_0)}{n_j}.$$

Consequently, the image of the irreducible character $\chi_i^{\tau_{ij}} = \dfrac{n_i}{n_j}\chi_j$. Since all irreducible characters are linearly independent over $\mathbb{C}$, we have $n_i = n_j$. Obviously, to disctinct mappings μ_{ij} there correspond different automorphisms $\tau_{ij} \in \mathrm{Aut}(\mathbb{Q}(\chi_i))$; therefore, $k \leqslant |\mathrm{Aut}(\mathbb{Q}(\chi_i))|$.

On the other hand, automorphisms of the field $\mathbb{Q}(\chi_i)$ extend to automorphisms of the field $\mathbb{Q}(T_i(G))$ and then to automorphisms of the field K (see [2]). Any automorphism of the representation field of G maps an irreducible character to an irreducible character ([3]). This gives that any automorphism of the field $\mathbb{Q}(\chi_i)$ takes χ_i to some irreducible character χ_j. If we extend this automorphism to an automorphism of the field $\mathbb{Q}(T_i(G))$ and apply it to the entries of the matrix $T_i(G)$ then, up to equivalence, we obtain the representation $T_j(G)$ due to the coincidence of the characters. Obviously, the mapping μ_{ij} induced by an automorphism of the field $\mathbb{Q}(T_i(G))$ and the conjugation by a matrix from $\mathrm{GL}_{n_i}(\mathbb{C})$ defines an isomorphism. Thus, the cell $\mathbb{Z}[T_j(G)]$ gets into the block O and $k \geqslant |\mathrm{Aut}(\mathbb{Q}(\chi_i))|$.

The above arguments imply that if $\mathrm{Aut}(\mathbb{Q}(\chi_i)) = \{\tau_1 = id, \tau_2, ..., \tau_r\}$ then $k = r$ and the representation $T_{i+j}(G)$ is equivalent to the representation $\hat{\tau'}_{j+1}(T_i(G))$, $j = 0, ..., r-1$, τ'_{j+1} is an extension of τ_{j+1} up to an automorphism of the field $\mathbb{Q}(T_i(G))$. Thus, the lemma is proved. □

2 Description of the algorithm and the main theorem

Lemma 1 implies that each block contains $k_i n_i^2$ linearly independent matrices and a matrix in a block is uniquely defined by its first cell. Therefore, if the *Schur index* (see [2]) is equal to 1 then from an additive basis of the block one can "compose" any matrix in the algebra $(\mathbb{Q}(\chi_i))_{n_i}$, which implies the coincidence of the $\mathbb{Q}$-algebras of the block under the action of $\hat{\tau}'$. Hence, in the particular case when all the representations $T_i(G)$ have Schur index 1, the necessary condition for the existence of a matrix s is fulfilled.

If for some representations $T_i(G)$ the Schur index is greater than 1 then the coincidence of the $\mathbb{Q}$-algebras may fail. So, let τ' be an automorphism of the representation field of G.

For convenience of the exposition, enumerate the steps of our considerations.

1. Suppose the coincidence of the $\mathbb{Q}$-algebras $\mathbb{Q}[R(G)^t]$ and $\mathbb{Q}[(R(G)^t)^{\hat{\tau}'}]$.

2. The coincidence of the $\mathbb{Q}$-algebras implies that the elements $((R(g_i))^t)^{\hat{\tau}'}$ are $\mathbb{Q}$-linear combinations of the elements $(R(g_i))^t$.

3. Item 2 implies that the elements $((R(G))^t)^{\hat{\tau}'}$ in the $\mathbb{Q}$-algebra of the left regular representation of G have the form

$$L(g_i) = \frac{p_1^i}{q_1^i} R_l(e) + \cdots + \frac{p_n^i}{q_n^i} R_l(g_n), g_i \in G, i = 1, \cdots, n.$$

We obtain a representation $L(G)$ of the group G in the algebra $\mathbb{Q}[R_l(G)]$.

4. Observe that by $\mathbb{Z}^n$ we mean the set of integral vectors of length n written as a row or a column. It is always clear from the context which of the cases is being considered. The same applies to the canonical basis $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$.

Consider the algebra $\mathbb{Q}[R_l(G)]$. The first columns of the matrices $R_l(e)$, $\ldots$, $R_l(g_n)$ constitute the canonical basis of $\mathbb{Z}^n$, and each matrix $R_l(g_i)$ is uniquely determined by its first column. Namely, the first column of this matrix is the vector e_i of the canonical basis of $\mathbb{Z}^n$, the second column equals $R(g_2)e_i$, where $R(G)$ is the right regular representation of G, etc. Thus, $R_l(g_i) = (e_i \ R(g_2)e_i \ \cdots \ R(g_n)e_i)$. It is now clear that if $a = u_1 R_l(e) + \cdots + u_n R_l(g_n)$, $u = (u_1, \ldots, u_n)$ then $a = (u^T \ R(g_2)u^T \ \ldots \ R(g_n)u^T)$.

5. If $a = \alpha_1 R_l(e) + \cdots + \alpha_n R_l(g_n) \in \mathbb{Q}[R_l(G)] \cap M_n(\mathbb{Z})$ then item 4 implies that $a \in \mathbb{Z}[R_l(G)]$.

6. By Burnside's theorem (see [4, p. 68]), for the group $L(G)$ there exists a matrix $s \in GL_n(\mathbb{Q})$ such that $(L(G))^s \subseteq GL_n(\mathbb{Z})$. In our case, the positive answer to the above-posed question means that that there is a unit s_l of the algebra $\mathbb{Q}[R_l(G)]$ such that $(L(G))^{s_l} \subseteq GL_n(\mathbb{Z})$. Obviously, the existence of s_l implies the existence of s.

7. Following the idea of the proof of Burnside's theorem, we must find a submodule N in $\mathbb{Z}^n$ invariant under $L(G)$ and such that the transition matrix from the basis of N to the canonical basis of $\mathbb{Z}^n$ be from $\mathbb{Q}[R_l(G)]$. Then the matrices of $\mathbb{Z}[L(G)]$ conjugated by such a transition matrix remain in $\mathbb{Q}[R_l(G)]$ and become integral, i.e., the ring $\mathbb{Z}[L(G)]$ under such conjugation gets into the ring $\mathbb{Z}[R_l(G)]$, which implies the existence of the matrix s_l and hence of the matrix s. We will consider right modules. Then the coordinated of the basis of N in the canonical basis of $\mathbb{Z}^n$ are the rows of the transition matrix. If we recall that transposition is an anti-isomorphism of the algebra

$\mathbb{Q}[R_l(G)]$ and $(R(g_i))^T = R(g_i^{-1})$ then the transition matrix must have the form

$$S(u) = \begin{pmatrix} u \\ uR(g_2^{-1}) \\ \vdots \\ uR(g_n^{-1}) \end{pmatrix},$$

or, equivalently, N must have the basis $u, uR(g_2^{-1}), \cdots, uR(g_n^{-1})$, i.e., $N = u\mathbb{Z}[R(G)]$.

8. Invariance of N under $L(G)$. Put $p_i = (\frac{p_1^i}{q_1^i}, \cdots, \frac{p_n^i}{q_n^i})$. Then, by item 4,

$$L(g_i) = (p_i^T \; R(g_2)p_i^T \; \cdots \; R(g_n)p_i^T),$$

$$uL(g_i) = (up_i^T, uR(g_2)p_i^T, \cdots, uR(g_n)p_i^T) =$$

$$= (p_i u^T, \ldots, p_i R(g_n^{-1})u^T) = p_i(u^T \cdots R(g_n^{-1})u^T) = p_i\widetilde{S}(u),$$

where $\widetilde{S}(u) = (u^T \cdots R(g_n^{-1})u^T)$.

The invariance of N under $L(G)$ implies that $p_i\widetilde{S}(u) = (z_1^i, \cdots, z_n^i)S(u)$. Consider the matrix $L' = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$. The last equality implies that

$$L'\widetilde{S}(u) = AS(u), \text{ where } A \in M_n(\mathbb{Z}) \qquad (*)$$

The automorphism $\widehat{\tau}'$, defined on the algebra $\mathbb{Q}[(R(G))^t]$, induces an automorphism $\sigma : R_l(G) \to L(G)$ on the algebra $\mathbb{Q}[R_l(G)]$. L' is the matrix of σ in the basis $R_l(e), \cdots, R_l(g_n)$ of the algebra $Q[R_l(G)]$, which implies that $|L'| = \pm 1$ since σ has finite order. Then condition (*) gives $|A| = \pm 1$ because $|\widetilde{S}(u)| = \pm|S(u)|$. Since $uL(g_i) = p_i\widetilde{S}(u)$, the rows of the matrix $L'\widetilde{S}(u)$ are the coordinates of the basis of the module $u\mathbb{Z}[L(G)]$. Therefore, condition (*) for $|A| = \pm 1$ means that the modules $u\mathbb{Z}[L(G)]$ and $u\mathbb{Z}[R(G)]$ coincide. Thus, condition $(*)$ determines the invariance of the module $N = u\mathbb{Z}[R(G)]$ under $L(G)$ since the module $u\mathbb{Z}[L(G)]$ is obviously invariant under $L(G)$.

9. We infer that the existence of the matrix s is equivalent to the existence of a vector $u = (u_1, ..., u_n) \in \mathbb{Z}^n$ satisfying the following conditions:

(1) $uL(g_i) \in \mathbb{Z}^n, i = 1, ..., n$;

(2) the matrix $s_l = u_1R_l(e) + \cdots + u_nR_l(g_n)$ is invertible;

(3) condition $(*)$ is fulfilled.

Theorem 1. *If* $\mathbb{Q}[(R(G))^t] = \mathbb{Q}[((R(G))^t)^{\hat{\tau'}}]$ *then, given* $\tau \in Aut\mathbb{Q}(\chi_i)$, *there exists a unit* s *of the algebra* $\mathbb{Q}[(R(G))^t]$ *such that the composition* $\hat{\tau'} \circ \varphi_s$ *is an automorphism of the ring* $\mathbb{Z}[(R(G))^t]$ *if and only if the following conditions hold: there exists a vector* $u = (u_1, ..., u_n) \in \mathbb{Z}^n$ *such that*

(1) $uL(g_i) \in \mathbb{Z}^n, i = 1, ..., n$;

(2) the matrix $s_l = u_1 R_l(e) + \cdots + u_n R_l(g_n)$ *is invertible;*

(3) $L'\widetilde{S}(u) = AS(u)$, *where* $A \in M_n(\mathbb{Z})$.

Доказательство. Necessity. Suppose that s exists. Then the $\mathbb{Q}$-algebras coincide and there exists a unit $s' \in \mathbb{Q}[R_l(G)]$ such that $\mathbb{Z}[L(G)]^{s'} = \mathbb{Z}[R_l(G)]$. By item 4,

$$s' = (v^T \ R(g_2)v^T \ \cdots \ R(g_n)v^T),$$

where $v = (\frac{p_1}{q_1}, \cdots, \frac{p_n}{q_n})$. Assume that

$$q = \text{l.c.m.}(q_1, \cdots, q_n), \ u = qv, \ qs' = (u^T \ R(g_2)u^T \ \cdots \ R(g_n)u^T),$$

and we can take qs' instead of s'. In this case, the vector $u \in \mathbb{Z}^n$ satisfies conditions (1),(2),(3). Indeed, the vectors $u, uR(g_2^{-1}), \cdots, uR(g_n^{-1})$ are linearly independent, i.e., (2) holds. In this basis, the matrices $L(g_i)$ are integral. Then $uL(g_i) = z_1 u + \cdots + z_n u(R(g_n^{-1}) \in \mathbb{Z}^n$, i.e., (1) is fulfilled. Moreover, the module N with basis $u, uR(g_2^{-1}), \cdots, uR(g_n^{-1})$ is invariant under $L(G)$, i.e., the matrices $L(G)$ become integral, and this means the fulfillment of condition (3).

Sufficiency. Note that conditions (1),(2),(3) coincide with conditions (1)-(3) of item 9, which is equivalent to the existence of s. The theorem is proved. □

References

[1] A. M. Popova, E. V. Grachev. The Factorization Problem for Automorphisms of Group Rings of Finite Groups // Algebra and Model Theory 11, Novosibirsk 2017, 75–80.

[2] Ch. W. Curtis, I. Reiner. Representation Theory of Finite Groups and Associative Algebras. Interscience Publishers, New York–London, 1962, 685 pp. [Nauka, Moscow, 1969, 668 pp.].

[3] V. A. Belonogov. Representations and Characters in the Theory of Finite Groups. Akad. Nauk SSSR Ural. Otdel., Sverdlovsk, 1990. 380 pp. [in Russian].

[4] D. A. Suprunenko. Matrix Groups. Nauka, Moscow, 1972, 351 pp. [AMS, Providence, R.I., 1976. viii+252 pp.]