# ON SOME INTEGRAL RINGS ASSOCIATED WITH A FINITE GROUP

MATHEMATICS

1966

SovietRxiv

## Abstract

## Full Text

UDC 519.4

**MATHEMATICS**

A. I. SAKSONOV

# ON SOME INTEGRAL RINGS ASSOCIATED WITH A FINITE GROUP

*(Presented by Academician A. I. Mal' tsev on 1 II 1966)*

Let $Z$ be the ring of rational integers, and let $R$ be the ring of integers of a finite extension of the field of rational numbers. By an **integral ring** we shall mean an algebra over the ring $R$, so that, for example, an isomorphism of two integral rings is always understood to mean an isomorphism over $R$. With an arbitrary finite group $G$ there is associated a number of integral rings; among these we consider here the integral ring of characters and the integral group ring. The study of these rings gives certain information about the structure of the group $G$. At least for some classes of finite groups this information turns out to be complete. In what follows, $G$ and $\widetilde{G}$ will everywhere denote finite groups.

§ 1. Since the multiplication table of the irreducible complex characters of a group $G$ is rational and integral, the $R$-linear combinations of these characters form, with respect to the usual operations, a commutative ring–the integral character ring $RX(G)$ of the group $G$. In particular, for $R = Z$ we obtain the ring of generalized characters of the group $G$.

The periodic part of the multiplicative group of the ring $RX(G)$ has a rather simple structure, as the following shows.

**Theorem 1.** *The only units of finite order in the ring $RX(G)$ are the elements of the form $\varepsilon X$, where $\varepsilon$ is a root of 1 in $R$, and $X$ is a linear character of the group $G$.*

**Corollary 1.1.** *If $RX(G) \cong RX(\widetilde{G})$, then $G/G' \cong \widetilde{G}/\widetilde{G}'$. In particular, if G is abelian, then from $RX(G) \cong RX(\widetilde{G})$ it follows that $G \cong \widetilde{G}$.*

Since an abelian group is isomorphic to the group of its absolutely irreducible characters, Theorem 1 may be interpreted as a generalization of the corresponding result of G. Higman ([1]) for the integral group ring of an abelian group.

If $G$ and $\widetilde{G}$ have identical character tables, then, of course, $RX(G) \cong RX(\widetilde{G})$. It turns out that conversely the structure of the ring $RX(G)$ determines the character table of the group $G$. Denote by $X_\rho$ ($\widetilde{X}_\rho$), $\rho = 1, \dots, k$, the absolutely irreducible characters of the group $G$ ($\widetilde{G}$). The basis $\{X_\rho\}_1^k$ of the ring $RX(G)$ is distinguished in the following sense.

**Theorem 2.** *Suppose that $RX(G) \cong RX(\widetilde{G})$, and let $\varphi$ be an isomorphism of $RX(\widetilde{G})$ onto $RX(G)$. Then $\varphi(\widetilde{X}_\rho) = \varepsilon X_{\varphi(\rho)}$, where $\varepsilon$ is a root of 1 in $R$, and $\varphi(\rho)$ is a certain permutation of the symbols $1, \dots, k$, induced by the automorphism $\varphi$.*

**Corollary 2.1.** *If $RX(G) \cong RX(\widetilde{G})$, then the character tables of the groups $G$ and $\widetilde{G}$ coincide (up to the numbering of rows and columns).*

Following E. M. Zhmud', we shall call an isomorphism of the structures of normal divisors of the groups $G$ and $\widetilde{G}$ that preserves indices a **strong $N$-structural isomorphism** of the groups $G$ and $\widetilde{G}$. With respect to a strong $N$-structural isomorphism, such group-theoretic properties as solvability, supersolvability, and nilpotency are evidently invariant. A necessary and suffi-

an exact condition for strong $N$-structural isomorphism of two finite groups was obtained in [4]. This condition is certainly satisfied for the groups $G$ and $\widetilde{G}$ if $RX(G) \cong RX(\widetilde{G})$. In the latter case, however, one can assert more.

Denote by $Z_i(G)$ the $i$-th center of the group $G$, and by $G_j$ its $j$-th mutual commutant.

**Theorem 3.** If $RX(G) \cong RX(\widetilde{G})$, then there exists a strong $N$-structural isomorphism $\psi$ of the groups $G$ and $\widetilde{G}$ such that:

1) for any $N \lhd G$, among $L \lhd G$, and $L/N = Z_1(G/N)$, it follows that

$$\psi(L)/\psi(N) = Z_1(\widetilde{G}/\psi(N))$$

and

$$L/N \cong \psi(L)/\psi(N);$$

2) $\psi(Z_i(G)) = Z_i(\widetilde{G})$ and

$$Z_{i+1}(G)/Z_i(G) \cong Z_{i+1}(\widetilde{G})/Z_i(\widetilde{G});$$

3) $\psi(G_j) = \widetilde{G}_j$ and

$$G_j/G_{j+1} \cong \widetilde{G}_j/\widetilde{G}_{j+1}.$$

In particular, if $G$ is nilpotent of class $c$, then $\widetilde{G}$ is nilpotent of the same class.

Theorem 2 can be applied to the study of the automorphism group $A$ of the ring $RX(G)$. The group $A$ is, obviously, finite, and it is easy to see that for a given group $G$ the order of $A$ is bounded for all $R$. The following theorem shows that, with respect to automorphisms of the ring $RX(G)$, the basis $\{X_\rho\}_1^k$ is a closed set (up to some roots of 1 contained in $R$).

**Theorem 4.** Every automorphism $\alpha$ of the ring $RX(G)$ induces a monomial permutation on the set of absolutely irreducible characters of the group $G$:

$$\alpha(X_\rho) = \varepsilon X_{\alpha(\rho)},$$

where $\varepsilon$ is a root of 1 in $R$. Let $U_0(R)$ denote the periodic part of the group of units of the ring $R$. If $(|Z_1(G)|,\ |U_0(R)|) = 1$, then the permutation induced by the automorphism $\alpha$ is ordinary.

Since every automorphism $\alpha \in A$ leaves the principal character of the group $G$ fixed, the group $A$ is faithfully represented by monomial matrices of degree $k-1$. As a linear group, $A$ is a semidirect product of its diagonal part $D$ (the structure of which depends not only on $G$, but also on $U_0(R)$) by a certain subgroup $T$ of the symmetric group of degree $k-1$. The structure of $T$ is completely determined by the group $G$.

Let $T_1$ (respectively $T_2$) denote the subgroup of all automorphisms of the ring $RX(G)$ induced by automorphisms of the group $G$ (respectively by automorphisms of the character field of the group $G$ over the field of rational numbers). It is easy to verify that $T_2$ lies in the center of $T$, and $T \supset T_1T_2$. The structure of the group $T$ as a permutation group is closely connected with the structure of the ring $RX(G)$. In this connection one may state the following

**Conjecture.** If some automorphism $\tau \in T$ acts regularly on the set of nonprincipal absolutely irreducible characters of the group $G$, then the multiplicative group of the ring $RX(G)$ contains a nontrivial periodic part.

Here we regard the periodic part of the multiplicative group of the ring $RX(G)$ as trivial if it coincides with $U_0(R)$.

It can be shown that, if the formulated conjecture is false, then a counterexample must be found among simple nonabelian groups. The series of simple groups checked by the author—$LF(2,p)$, $p > 3$ prime, the Suzuki groups, the Ree groups, and also the Mathieu groups of degrees 12 and 24—do not yield a counterexample.

Let us note, on the other hand, some consequences of our conjecture.

**1. Solvability of groups of odd order.** All nonprincipal absolutely irreducible characters of a group $G$ of odd order are, as is known, complex, and it is easy to see that the mapping of each such character to its complex conjugate extends to an automorphism of the ring $RX(G)$ satisfying the condition of our conjecture. But

then, by the conclusion of the assumption and Theorem 1, $G \neq G'$, whence by induction the solvability of the group $G$ follows.

**2. Solvability of groups admitting a regular automorphism of arbitrary order *n*.** If $\sigma$ is a regular automorphism of a group $G$, then it induces a regular permutation on the set of nonidentity classes of conjugate elements of the group $G$ and, by the well-known lemma of R. Brauer, on the set of nonlinear absolutely irreducible characters of the group $G$. Consequently, we can apply our assumption; in view of Theorem 1, we again obtain that $G \neq G'$ and, by induction, the solvability of the group $G$.

Let us note that the question of the solvability of a finite group with a regular automorphism of composite order has not been solved at the present time.

§ 2. The integral group ring $RG$ gives, generally speaking, more information about the group $G$ than the ring $RX(G)$. If $RG \cong R\widetilde{G}$, then, by Corollary 5.1, $RX(G) \cong RX(\widetilde{G})$. At the same time the example of two nonisomorphic nonabelian groups of order $p^3$, $p$ prime, shows that the converse is false. One of the main unsolved questions in the theory of the integral group ring is the following: does the ring $RG$ completely determine the structure of the group $G$, i.e. will $RG \cong R\widetilde{G}$ always imply $G \cong \widetilde{G}$? A positive answer to this question has been obtained only for rather narrow classes of finite groups (abelian ([1]), Hamiltonian ([1,3]), and some types of $p$-groups ([7])*).

Theorems 5–7 given below provide necessary conditions for an isomorphism of integral group rings. Moreover, as some corollaries of the main Theorem 7, all known results of this kind are obtained.

Denote by $K_i$ (respectively $\widetilde{K}_i$) the sum of the elements of the $i$-th class of conjugate elements of the group $G$ (respectively of the group $\widetilde{G}$).

**Theorem 5** (for the case $R = Z$ see ([2])). *Let $\widetilde{G}$ be a finite subgroup of the multiplicative group of the ring $RG$, such that $RG \cong R\widetilde{G}$. Then, under a corresponding numbering of the classes of conjugate elements of the groups $G$ and $\widetilde{G}$,*

$$\widetilde{K}_i = \varepsilon K_i,$$

*where $\varepsilon$ is a root of 1 in $R$.*

**Corollary 5.1.** *If $RG \cong R\widetilde{G}$, then the groups $G$ and $\widetilde{G}$ have identical character tables.*

**Corollary 5.2** ([7]). *If $RG \cong R\widetilde{G}$, then all assertions of Theorem 3 hold.*

For any $w \in RG$ denote by $s_i(w)$ the sum of the coefficients at the elements of the $i$-th class of conjugate elements of the group $G$ in the expansion

$$w = \sum_{i=1}^{|G|} w_i x_i \quad (x_i \in G,\ w_i \in R).$$

**Theorem 6.** *Suppose that the condition of Theorem 5 is satisfied and that, in accordance with the numbering established by Theorem 5, $u \in \widetilde{G}$ belongs to the $j$-th class of conjugate elements of the group $\widetilde{G}$. Then*

$$s_i(u) = \delta_{ij}\varepsilon,$$

*where $\delta_{ij}$ is the Kronecker delta, and $\varepsilon$ is a root of 1 in $R$.*

Theorem 6 gives some information about the embedding of a group basis in the ring $RG$.

**Remark.** Obviously, the number of distinct ring homomorphisms $RG \to R$ is equal to the number of linear characters of the group $G$ over $R$. Let $\mu : RG \to R$ be the homomorphism that is induced by the identity representation of the group $G$. If $\widetilde{G}$ is a finite subgroup of the multiplicative group of the ring $RG$ generating the $R$-module $RG$, then the group

$$\widetilde{G}_0 = \{\mu^{-1}(u)u\},$$

where $u$ runs through $\widetilde{G}$, is isomorphic to $\widetilde{G}$ and also generates $RG$. Therefore, without loss of generality one may immediately assume that $\mu(u) = 1$ for all $u \in \widetilde{G}$. Under this condition, in the conclusions of Theorems 5 and 6 one must put $\varepsilon = 1$.

* The proof of Lemma 4.1 of paper ([7]) contains a substantial error. Nevertheless, this lemma and the results obtained in ([7]) with its aid are true (see the corollaries of our Theorem 7).

In 1963 R. Brauer ([5]) posed the question: will two finite groups $G$ and $G^*$ be isomorphic if there exists a one-to-one correspondence $K \leftrightarrow K^*$ between the classes of conjugate elements such that: 1) the class multiplication table is preserved; 2) if $K^{[m]}$ denotes the class containing the $m$-th powers of the elements of the class $K$, then $(K^{[m]})^* = (K^*)^{[m]}$. Although, as it turned out ([6]), such groups need not be isomorphic, they are nevertheless very close in structure. We shall call two groups $G$ and $G^*$ for which the above correspondence exists a **Brauer pair**.

With the aid of Theorems 5 and 6 the main result is proved.

**Theorem 7.** *If $RG \cong R\widetilde{G}$, then the groups $G$ and $\widetilde{G}$ form a Brauer pair.*

**Corollary 7.1.** *The structure of the ring $RG$ completely determines the structure of the group $G$, if $G$ is: a) abelian ([1]); b) Hamiltonian ([1,3]); c) a $p$-group containing a cyclic normal divisor of index $\leq p^2$ for odd $p$ and of index 2 for $p = 2$ ([7]).*

**Corollary 7.2.** *Let $RG \cong R\widetilde{G}$. Then there exists a strong $N$-structural isomorphism $\psi$ of the groups $G$ and $\widetilde{G}$ such that:*

a) *all assertions of Theorem 3 hold for it;*

b) *if $N \lhd G$, $L \lhd G$, $N \subseteq L$, then $L/N$ and $\psi(L)/\psi(N)$ have the same number of elements of any given order; in particular, $L/N$ and $\psi(L)/\psi(N)$ have the same exponents;*

c) ([7]) *if the factor $L/N$ is cyclic, then $L/N \cong \psi(L)/\psi(N)$;*

d) *if the factors $L/N$ and $\psi(L)/\psi(N)$ are abelian, then they are isomorphic.*

**Note added in proof.** After this note had been submitted for publication, the author became acquainted with the paper ([8]), which contains a theorem analogous to our Theorem 7.

Institute of Mathematics
Academy of Sciences of the BSSR

Received
20 XI 1965

## References

[1] G. Higman, Proc. Lond. Math. Soc., 2, 46, 3–4, 231 (1940).
[2] S. D. Berman, Dokl. USSR, 5 (1953).
[3] S. D. Berman, Ukr. Math. J., 7, 3, 253 (1957).
[4] E. M. Zhmud' , Mat. Sb., 44 (86), 3, 353 (1958).
[5] R. Brauer, *Lectures on Modern Mathematics*, 1, N. Y., 1963, p. 133.
[6] E. C. Dade, J. Algebra. 1, No. 1, 1-4 (1964).
[7] J. A. Cohn, D. Livingstone, Canad. J. Math., 17, 4, 583 (1965).
[8] D. S. Passman, Pacific J. Math., 15, 561 (1965).

*Note: Figure translations are in progress. See original paper for figures.*