150. *On the Character Rings of Finite Groups*

By Shoichi KONDO
Department of Mathematics, Waseda University, Tokyo

(Comm. by Kenjiro SHODA, M. J. A., Nov. 12, 1973)

Introduction. Let G be a finite group. In this paper all groups are finite and all characters are assumed to be characters of representations over the complex field. As is well known, every character of G is the sum of irreducible characters of G and the set of characters of G is closed under addition and multiplication. It is often convenient to consider also the difference of two characters (see [1, Chapter 6]). From this fact we shall be concerned with the ring generated by the irreducible characters χ_k of G over the ring Z of rational integers. The ring thus obtained we denote by $R(G)$, and call it the character ring of G. In this paper we deal with this character ring $R(G)$.

Clearly, $R(G)$ is a commutative Z-algebra. Its unity element is the principal character of G. Moreover every element of $R(G)$ is uniquely expressible as a Z-linear combination of the χ_k. If G is abelian, it is known that $R(G)$ is isomorphic to the group ring ZG (see e.g. [5] or [6]). However, in general, it is difficult to give a characterization of character rings. On the other hand, it is possible to state a little further the structure of the ring $Q\otimes_Z R(G)$, where Q denotes the rational field. We note that the character ring $R(G)$ has non-zero nilpotents. This implies that the ring $Q\otimes_Z R(G)$ is semi-simple (cf. [3], [4]). Therefore $Q\otimes_Z R(G)$ is isomorphic to a direct sum of a finite number of fields K_i. In [6], Thompson showed this fact using the decomposition of unity element into a sum of orthogonal primitive idempotents. On the basis of these results we obtain some properties of the ring $Q\otimes_Z R(G)$.

In the first section of this paper we observe prime ideals of $R(G)$ and determine the minimal prime ideals. Next we discuss the structure of the field K_i This argument leads to the result that $Q\otimes_Z R(G)$ is determined by a permutation group on the set of conjugate classes of G. In particular, if G is a p-group, where p is an odd prime integer, then there is the set of integers which determines the ring $Q\otimes_Z R(G)$.

§1. Prime ideals of the character ring $R(G)$.

Suppose m is a multiple of the exponent of G. Let ε_m be a primitive m-th root of 1 over Q, and A the integral closure of Z in the cyclotomic field $F_m=Q(\varepsilon_m)$. Let $Cl(G)$ denote the set of all conjugate classes of G. Then the direct product $A^{Cl(G)}$ is the ring of all class functions of G which take their values in A, and $R(G)$ is regarded as a subring of $A^{Cl(G)}$. Since $A^{Cl(G)}$ is integral over $R(G)$ (in fact, integral over Z), any prime ideal P of $R(G)$ is the contraction of some prime ideal of $A^{Cl(G)}$. This shows that P is of the form $\{\zeta \in R(G) \mid \zeta(c) \in \mathfrak{p}\}$ for some $c \in Cl(G)$ and some prime ideal $\mathfrak{p}$ of A. In particular, minimal prime ideals are obtained by putting $\mathfrak{p}=0$ (see [5, § 11.4]).

In order to determine the minimal prime ideals of $R(G)$, it is convenient to consider the Galois group $\mathfrak{G}_m$ of F_m over Q. Since $\mathfrak{G}_m$ is isomorphic to the group of units of Z/mZ, each automorphism σ of $\mathfrak{G}_m$ is given by a map $\sigma(\varepsilon_m)=\varepsilon_m^{t(\sigma)}$, where $t(\sigma)$ is an integer relatively prime to m and satisfies the condition $t(\sigma)t(\tau)\equiv t(\sigma\tau) \pmod m$. Each σ yields a permutation of $Cl(G)$; if a conjugate class c contains an element x of G, then we define c^σ as the conjugate class containing $x^{t(\sigma)}$. When $\mathfrak{G}_m$ is regarded as a permutation group on $Cl(G)$, we denote it by $S_m(G)$. Then $S_m(G)$ is abelian and isomorphic to the factor group $\mathfrak{G}_m/\mathfrak{H}$, where $\mathfrak{H}=\{\sigma \in \mathfrak{G}_m \mid c^\sigma=c \text{ for all } c \in Cl(G)\}$. If n is the exponent of G, then $S_m(G)$ is the same as $S_n(G)$. Indeed, for each element τ of $\mathfrak{G}_n$, there is an element σ of $\mathfrak{G}_m$ such that τ is the restriction of σ to F_n. Thus $S_m(G)$ is determined only by G not depending on the choice of a multiple m of the exponent. Hence we shall denote it by $S(G)$.

Theorem 1. *Any finite group G determines $(S(G); Cl(G))$, an abelian permutation group $S(G)$ on $Cl(G)$.*

Now we need the following known result (see e.g. [2]).

Lemma 1. *Let $\zeta \in R(G)$, and let $\sigma \in \mathfrak{G}_m$. Then we have*

$$\sigma(\zeta(c))=\zeta(c^\sigma), \qquad c \in Cl(G). \tag{1.1}$$

Proof. Let c contain an element x of order n', and H the cyclic subgroup of G generated by x. Then the restriction of ζ to H lies in $R(H)$, hence it is sufficient to show (1.1) for any irreducible character ξ of H. Since ξ is a linear character and the order n' of H is a divisor of m, ξ is given by $\xi(x)=\varepsilon_m^l$ for some positive integer l. Then we have

$$\sigma(\xi(x))=\sigma(\varepsilon_m^l)=\varepsilon_m^{l\cdot t(\sigma)}=(\xi(x))^{t(\sigma)}=\xi(x^{t(\sigma)}).$$

This shows that $\sigma(\zeta(x))=\zeta(x^{t(\sigma)})$, and completes the proof.

As previously stated, each minimal prime ideal of $R(G)$ is of the form $\{\zeta \in R(G) \mid \zeta(c)=0\}$ for some $c \in Cl(G)$. It is easy to see by Lemma 1 that if $\zeta(c)=0$, then $\zeta(c^\sigma)=0$ for all $\sigma \in \mathfrak{G}_m$. Therefore minimal prime ideals are determined by the orbits O_i $(1\leqq i\leqq r)$ in $Cl(G)$ relative to $S(G)$. Let

$$P_i=\{\zeta \in R(G) \mid \zeta(c)=0 \text{ for all } c \in O_i\}, \qquad 1\leqq i\leqq r.$$

Then we shall show that the P_i are all distinct. By the orthogonality relations, we have

$$(1.2) \qquad \sum_k \overline{\chi_k(c)}\chi_k(c') = \begin{cases} n_c, & \text{if } c'=c \\ 0, & \text{otherwise,} \end{cases} \qquad c, c' \in Cl(G),$$

where $\overline{\chi_k(c)}$ is the complex conjugate of $\chi_k(c)$ and n_c is the order of the normalizer of $x \in c$ in G. We note that n_c depends only upon the orbit to which c belongs. For convenience we write n_i for n_c when $c \in O_i$. For each orbit O_i, define a class function d_i on G by $d_i = \sum_k a_{ik}\chi_k$, where $a_{ik} = \sum_{c \in O_i} \overline{\chi_k(c)}$. Then for $\sigma \in \mathfrak{G}_m$ we have

$$\sigma(a_{ik}) = \sum_{c \in O_i} \overline{\sigma(\chi_k(c))} = \sum_{c \in O_i} \overline{\chi_k(c^\sigma)} = \sum_{c \in O_i} \overline{\chi_k(c)} = a_{ik},$$

by Lemma 1. This shows that $a_{ik} \in Q \cap A = Z$, and so $d_i \in R(G)$. By (1.2), we have also

$$d_i(c) = \begin{cases} n_i, & \text{if } c \in O_i \\ 0, & \text{otherwise.} \end{cases}$$

Hence we find $d_i \notin P_i$ and $d_j \in P_i$ $(i \neq j)$. We conclude that the P_i $(1 \leqq i \leqq r)$ are all distinct minimal prime ideals of $R(G)$.

Thus we have

Theorem 2. *The number of minimal prime ideals of $R(G)$ is equal to the number of orbits of $(S(G); Cl(G))$.*

§ 2. On the ring $Q \otimes_Z R(G)$.

In the introduction, we stated that the ring $Q \otimes_Z R(G)$ is isomorphic to a direct sum of a finite number of fields. Here we give a proof of this.

Let R be a commutative ring with unity element, and $Z \subseteq R$. Suppose that R is finitely generated as a Z-module and has no non-zero nilpotents. Moreover we assume that no non-zero element of Z is a zero-divisor in R. (It is obvious that the character ring $R(G)$ satisfies these conditions.) Then R is Noetherian, hence has a finite number of minimal prime ideals, say $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$. Then we have $\bigcap_{i=1}^r \mathfrak{p}_i = 0$. Let $S = Z - \{0\}$. Then S is a multiplicatively closed subset of R, and we have $Q \otimes_Z R = S^{-1}R$. It is clear that $\mathfrak{p}_i$ does not meet S and $\bigcap_{i=1}^r S^{-1}\mathfrak{p}_i = 0$. Furthermore the $S^{-1}\mathfrak{p}_i$ $(1 \leqq i \leqq r)$ are all distinct maximal ideals of $S^{-1}R$ and are pairwise coprime. Therefore the canonical homomorphism $S^{-1}R = \bigoplus_{i=1}^r (S^{-1}R/S^{-1}\mathfrak{p}_i)$ is a ring isomorphism, where $S^{-1}R/S^{-1}\mathfrak{p}_i = S^{-1}(R/\mathfrak{p}_i)$ is the quotient field of $R/\mathfrak{p}_i$ $(1 \leqq i \leqq r)$.

Now let P_i $(1 \leqq i \leqq r)$ be the minimal prime ideals of $R(G)$. Then each P_i is the kernel of the map $R(G) \to F_m$ defined by $\zeta \mapsto \zeta(c)$, where $c \in O_i$. Hence there is a subfield K_i of F_m which is isomorphic to the quotient field of $R(G)/P_i$. It is clear that the field K_i is generated by $\{\chi_k(c)\}_k$ over Q. Thus we have the following decomposition which is unique up to isomorphism.

$$(2.1) \qquad Q \underset{Z}{\otimes} R(G) = K_1 \oplus \cdots \oplus K_r$$

Next we observe that the fields K_i are uniquely determined by the group $S(G)$. Let $O_1, \cdots, O_r$ be the distinct orbits in $Cl(G)$ relative to $S(G)$. Then we define subgroups S_i $(1 \leqq i \leqq r)$ of $S(G)$ as follows;

$$S_i = \{\sigma \in S(G) \mid c^\sigma = c \text{ for all } c \in O_i\}.$$

Moreover, for m a multiple of the exponent of G, let $\mathfrak{G}_m$ be the Galois group of the cyclotomic field F_m of order m over Q. As stated in § 1, $\mathfrak{G}_m$ is regarded as the permutation group on $Cl(G)$ which coincides with $S(G)$. Let $\mathfrak{H}_i$ be the inverse image of S_i in $\mathfrak{G}_m$, that is, $\mathfrak{H}_i = \{\sigma \in \mathfrak{G}_m \mid c^\sigma = c \text{ for all } c \in O_i\}$. Then we have that

$$S_i = \mathfrak{H}_i / \mathfrak{H}, \tag{2.2}$$

where $\mathfrak{H} = \mathfrak{H}_1 \cap \cdots \cap \mathfrak{H}_r$.

We show that K_i is the fixed field of $\mathfrak{H}_i$ (see [2] or [6]). Suppose $c \in O_i$. We note that K_i is generated by $\{\chi_k(c)\}$ over Q. If $\sigma \in \mathfrak{H}_i$, by Lemma 1 we have $\sigma(\chi_k(c)) = \chi_k(c^\sigma) = \chi_k(c)$. Conversely let $\sigma \in \mathfrak{G}_m$ such that $\sigma(a) = a$ for all $a \in K_i$. By (1.2) we have

$$\sum_k \overline{\chi_k(c)} \chi_k(c^\sigma) = \sum_k \overline{\chi_k(c)} \sigma(\chi_k(c)) = \sum_k \overline{\chi_k(c)} \chi_k(c) = n_c,$$

since $\sigma(\chi_k(c)) = \chi_k(c)$. This implies that $c^\sigma = c$, and so $\sigma \in \mathfrak{H}_i$. Our assertion has been settled.

Collecting our results, we have established the following:

Theorem 3. *The ring $R \otimes_Z R(G)$ is uniquely determined (up to isomorphism) by the group $(S(G); Cl(G))$.*

In particular, let G be a p-group, where p is an odd prime. In this case, we assume that m is a power of p. Then the Galois group $\mathfrak{G}_m$ is cyclic, and so is $S(G)$. Therefore each subgroup S_i is uniquely determined by its order h_i which is a divisor of the order h of $S(G)$. Then we put

$$I(G) = \{h_1, \cdots, h_r\}, \qquad h_1 \geqq h_2 \geqq \cdots \geqq h_r.$$

Assume further that the orbit O_1 consists of the conjugate class containing unity element of G. Then it is clear that $S_1 = S(G)$, and so $h_1 = h$. Let K be the composite of the fields K_i $(1 \leqq i \leqq r)$. Then K is the fixed field of $\mathfrak{H}$, where $\mathfrak{H} = \mathfrak{H}_1 \cap \cdots \cap \mathfrak{H}_r$. It is easy to see by (2.2) that $h_i = (K : K_i)$. In particular, $K_1 = Q$, and hence $h = h_1$ is the dimension of K over Q.

Theorem 4. *Let p be an odd prime, and G a p-group. Then the ring $Q \otimes_Z R(G)$ is uniquely determined up to isomorphism by the set $I(G)$.*

Proof. It suffices to prove that if G and G' are p-groups, then $Q \otimes_Z R(G)$ is isomorphic to $Q \otimes_Z R(G')$ if and only if $I(G) = I(G')$. We assume that K'_i, S'_i, and so on, have the same meanings for G' as K_i, S_i, and so on, for G. Suppose that m be the least common multiple of orders of G and G'. Then the cyclotomic field F_m is a cyclic extension of Q. If $Q \otimes_Z R(G)$ is isomorphic to $Q \otimes_Z R(G')$, then (2.1) implies that the K_i are isomorphic to the K'_i in some order. Hence we may assume that $K_i=K'_i$ for all i. Then $K=K'$, so $h_i=(K:K_i)=(K':K'_i)=h'_i$ $(1\leqq i\leqq r)$. Thus we have $I(G)=I(G')$.

Conversely, let $I(G)=I(G')$. Then we may assume that $h_i=h'_i$ for all i. Obviously, $(K:Q)=h_1=h'_1=(K':Q)$, and hence $K=K'$. From this it follows at once that $(K:K_i)=h_i=h'_i=(K':K'_i)$, and so $K_i=K'_i$ $(1\leqq i\leqq r)$. Then we have, by (2.1), that $Q\otimes_Z R(G)$ is isomorphic to $Q\otimes_Z R(G')$. This completes the proof.

Acknowledgement. The author wishes to thank Professor Y. Hinohara for his helpful advice.

References

[1] C. W. Curtis and I. Reiner: Representation Theory of Finite Groups and Associative Algebras. Interscience, New York (1962).

[2] B. Fein and B. Gordon: Fields generated by characters of finite groups. J. London Math. Soc., (2) 4, 735–740 (1972).

[3] J. A. Green: The modular representation algebra of a finite group. Illinois J. Math., **6**, 607–619 (1962).

[4] I. Reiner: The integral representation ring of a finite group. Michigan Math. J., **12**, 11–22 (1965).

[5] J.-P. Serre: Représentations linéaires des groupes finis. Hermann Collection, Paris (1971).

[6] J. G. Thompson: A non-duality theorem for finite groups. J. Algebra, **14**, 1–4 (1970).