Research Journal of Applied Sciences 3 (1): 88-89, 2008
ISSN: 1815-932X

Application of Character Theory of Finite Group

H.S. Ndakwo, M.A. Umar and A.M. Yau
Department of Mathematical Sciences, Nasarawa State University, Keffi, Nigeria

Abstract: One of the most celebrated applications of character theory to pure group theory is Burnside's theorem which states that a group with order divisible by at most two primes is solvable. The proof of this theorem depends on the properties of algebraic integers.

Key words: Pure group, prime, solvable, algebraic integers, character theory, burnside's theorem, celebrated

INTRODUCTION

An algebraic integer is a complex number which is a zero of a polynomial of the form,

$$X^n+a_{n-1}X^{n-1}+...+a_0,$$

where, $a_i \in Z$ for $0 \leq i \leq n-1$ (Burnsides, 1955).

And also a group G is solvable if and only if it has a chain of normal subgroups (Feit, 1971).

Frequently, the word integer is used to mean an algebraic integer and the elements of Z are referred to as rational integers. One of the most important properties of the set of algebraic integers is that it is a ring. In order words, sums and products of integers are integers (Dornhoff, 1971).

Lemma 1: The rational algebraic integers are precisely the elements of Z.

Proof: If $\alpha \in Z$, then α is a root of the polynomial $X-\alpha$ and thus is an algebraic integer.

Conversely, let r/s be an algebraic integer with r, s$\in$Z. We may assume that (r, s) = 1. We have,

$$(r,s)^n + a_{n-1}(r/s)^{-1} + ... + a_0 = 0 \quad (1)$$

Now multiplying (1) by S^n and rearrange terms to obtain,

$$r^n = -S(a_{n-1}r^{n-1} + a_{n-2}Sr^{n-2} + ... + a_0S^{n-1}) \quad (2)$$

We conclude that S/r^n. However, since (r, s) = 1 this yields, S = ±1 and r/s$\in$Z as required.

Lemma 2: Let X = $\{\alpha_1,...,\alpha_k\}$ be a finite set of algebraic integers. There exists a ring satisfying

(a) $Z \subseteq S \subset C$
(b) $X \subseteq S$
(c) There exists a finite subset, Y of S such that every element of S is a Z-linear combination of element of Y.

Proof: The integer α_i satisfies an equation of the form,

$$\alpha^{ni} = f_i(\alpha_i) \quad (3)$$

where, f_i is a polynomial of degree n-i with coefficient in Z. Let,

$$Y = \{\alpha_1, \alpha_2, ..., \alpha_k : 0 \leq r_i \leq n_{i-1}\}$$

and Let S be the set of all Z- linear combination of elements of Y. Using Eq. 3 and the power of α_i may be written as Z- linear combinations of 1, α,..., α_i^{n-i}.

It follows from this fact that the product of any two elements of Y lies in S and hence S is a ring. All of the properties claimed for S are now clear.

Note that condition (c) of the above Lemma may be paraphrased by saying that S is finitely generated as Z-module.

Theorem 3: Let S be a ring with $Z \subseteq S \subset C$. Suppose that S is finite generated as a Z-module, then every element of S is an algebraic integer.

Proof: Let s$\in$S and Let

$$Y = \{y_1,...,y_n\} \subseteq S$$

Have the property that every element of S is a Z-linear combination of elements of Y we then have

Corresponding Author: H.S. Ndakwo, Department of Mathematical Sciences, Nasarawa State University, Keffi, Nigeria

$$SY_i = \sum a_{ij} y_j$$

For all i with $\alpha_{ij} \in Z$.

Let A be the matrix (α_{ij}) and Let v be the column, col $(y_i, ..., y_n)$ then
$A_v = S_v$ and thus S is a root of the polynomial.

$$F(x) = \det(XI-A)$$

It follows that S is an algebraic integer and the proof is complete.

Corollary 4: Sums and products of algebraic integers are algebraic integers by Isaacs (1956).

Proof: Let α and β be algebraic integers by Lemma 2, there exists a ring S with $Z \subseteq S \subset C$ such that $\alpha, \beta \in S$ and S is finitely generated as a Z-module.

Since, $\alpha + \beta$ and $\alpha\beta \in S$, it follows from theorem (3) that they are algebraic integers as required.

RESULTS

Theorem 5 (Burnside, 1955): Let $\chi \in \mathrm{Irr}(G)$ and Let $\Re$ be conjugacy class of G with $g \in \Re$. Suppose that $\{\chi(1), |\Re|\} = 1$. Then either $g \in Z(\chi)$ or else $\chi(g) = 0$

Proof: We know that

$$\frac{\chi(g)|\Re(g)|}{\chi(1)}$$

is an algebraic integer. Since, $(\chi(1), |\Re|) = 1$ we may choose rational integers u and v so that $u\chi(1) + v|\Re| = 1$. Thus is an algebraic integer. Since $u\chi(g)$ is also integral, it follows that $\alpha = \chi(g)$ is an algebraic integer.
Supposed that $g \in Z(\chi)$, so that $|(g)| < \chi(1)$ and $|\alpha| < 1$.

Let $n = o(g)$ and Let E be the splitting field for the polynomial X^n-1 over Q in C so that $\alpha \in E$.

Let Ψ be the Galoise group of E over Q. Since $\chi(g)$ is a sum of $\chi(l)$ roots of unity, so is $\chi(g)$ for each $\sigma \in \Psi$. It follows that $|\chi(g)^\sigma| \leq (\chi)$ and $|\alpha^\sigma| \leq 1$ for $\sigma \in \Psi$. We have by (Reiner, 1962) that $|\prod \alpha^\sigma|$. For each $\sigma \in \Psi$, α^σ satisfies the same rational polynomials that α satisfies and hence is integral. Therefore,

$$\beta = \prod \alpha^\sigma \tag{5}$$

Is an algebraic integer. However, β is clearly fixed by all $\sigma \in \Psi$ and therefore $\beta \in Q$ by elementary Galois Theory. It follows from Lemma1 that $\beta \in Z$. Since, $|\beta| = 0$ and hence $\alpha^\sigma = 0$ for some σ. Therefore,

$$0 = \alpha = \frac{\chi(g)}{\chi(1)}$$

and $\chi(g) = 0$. The proof is complete.

Theorem 6: Let $|G| = P^a q^b$ where P and q are primes then G is Solvable (Burnsides, 1955).

Proof: We use induction on $|G|$. We may assume $|G|>1$ and choose a maximal proper normal subgroup N. If N>1, then by the inductive hypothesis, N and G/N are solvable and thus G is solvable and the subgroup of G. We may choose $g \in Z(p)$, $g \neq 1$. Then $(C|g|) = |G: C(g)|$ Divides $|G:P|$,

Which is the simple group G is abelian and the proof is complete.

CONCLUSION

It should be emphasized the fact that

$$\frac{\chi(g)(C|(g)|)}{\chi(1)}$$

is an algebraic integer does not follow from the fact that $\chi(g)$ is integral, since division of an integer by an integer does not usually result in an integer.

REFERENCES

Burnside, W., 1955. Theory of groups of finite order. 2nd Edn.1911. Represented by Dover, Dekker, New York.

Dornhoff, L., 1971. Group representation Theory. Dekker, New York.

Feit, W., 1971. Characters of finite groups. New York.

Isaacs, I.M., 1956. Character theory of finite groups. Academic Press New York.

Reiner, I., 1962. Representation theory of finite group and associative algebras. Wiley (interscience), New York.