Groups Acting on a Set whose Orbits are all Singleton

M. R. Pournaki*

Abstract

In this article using techniques which appeared in Witt's proof of Wedderburn's theorem, an arithmetical characterisation of groups acting on a set whose orbits are all singleton is given. This can then be used to obtain a new proof of Wedderburn's theorem.

Keywords: Cyclotomic polynomial, Wedderburn's theorem, Division ring, Action of a group.

2000 Mathematics Subject Classification: Primary 20D60, 20B05; Secondary 16K20.

1 Introduction

In 1905 Wedderburn [4] proved that every finite division ring is a field. He used a somewhat complicated number theoretical result due to Birkhoff and Vandiver; and in fact, two proofs are given for this theorem in his paper. After that, several proofs were presented for this famous theorem, for example see [1, 2, 3]. But Witt [5] gave a now famous short and elegant argument, using the cyclotomic polynomials over $\mathbb{C}$, the field of complex numbers, which shows the commutativity of finite division rings.

In this article, by a slight modification of Witt's proof, we obtain a characterisation, in terms of the order of stabilizer subgroups, for groups acting on a set whose orbits are all singleton. Since groups acting on themselves by conjugation with the above property, are exactly Abelian groups, we obtain a characterisation for such groups in terms of the order of centralisers. Finally we derive the Wedderburn theorem from this purely group theoretical result.

2 Some Preliminaries

Throughout the article, we suppose that G is a finite group and Ω is a finite G-set. Also we let Δ be the set of representatives of distinct orbits of G such that Δ_1 and

*The research of the author was in part supported by grant no. 83-2216 from research council of Sharif University of Technology.

Δ_2 are the sets of representatives for non-trivial and trivial orbits, respectively. The following lemma has an important role in the proof of our main result.

Lemma 2.1 *Let G be a finite group and Ω a finite G-set. Suppose $|G|$ divides $|\Omega|$ and for each $\omega \in \Delta_1$, $\mathrm{Fix}(G)$ divides $|G_\omega|$. Then $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ is an integer, and divides $\gcd\{|G_\omega| : \omega \in \Delta_1\}$.*

Proof. Note that for each $\omega \in \Delta_1$, $|G_\omega|$ divides $|G|$, and we therefore have $\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ divides $|G|$. Hence $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ is an integer. Now the class equation of the action on Ω becomes

$$|\Omega| = \sum_{\omega\in\Delta_1} |\mathcal{O}(\omega)| + \sum_{\omega\in\Delta_2} |\mathcal{O}(\omega)|. \tag{1}$$

Each orbit has its size equal to the index in G of the stabilizer of a point in the orbit. On the other hand, each fixed point is in an orbit by itself, so the sum over these singleton orbits is precisely the number of fixed points. Therefore, by equation (1), we obtain

$$|\Omega| = \sum_{\omega\in\Delta_1} |G : G_\omega| + \mathrm{Fix}(G). \tag{2}$$

Obviously for each $\omega \in \Delta_1$, $|G_\omega|$ divides $\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$. Therefore, there is a positive integer l_ω such that $\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\} = l_\omega |G_\omega|$. So

$$|G|/|G_\omega| = l_\omega\big(|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}\big),$$

and hence $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ divides $|G|/|G_\omega| = |G : G_\omega|$. This implies that $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ divides $\sum_{\omega\in\Delta_1} |G : G_\omega|$. On the other hand, $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ divides $|G|$, which by assumption, divides $|\Omega|$. Therefore, equation (2) implies that $|G|/\mathrm{lcm}\{|G_\omega| : \omega \in \Delta_1\}$ divides $\mathrm{Fix}(G)$, which by assumption again, divides $\gcd\{|G_\omega| : \omega \in \Delta_1\}$. $\square$

We also need something about the polynomial $x^n - 1 \in \mathbb{C}[x]$ and its irreducible factors in $\mathbb{Z}[x]$. For any positive integer d, the dth *cyclotomic polynomial*, $\phi_d(x)$, is defined by

$$\phi_d(x) = \prod (x - \xi),$$

where ξ runs through all dth primitive roots of unity. It is a classical result that $\phi_d(x)$ is an irreducible polynomial of degree $\varphi(d)$ in $\mathbb{Z}[x]$ for all positive d's, where φ is the Euler function. It is easy to see that

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

holds for any positive integer n.

We need the following well known result for which we give a proof here for the convenience of the reader.

Lemma 2.2 *Let n and a be positive integers. If $n > 1$, then $|\phi_n(a)| > a - 1$.*

Proof. We know that $|\phi_n(a)| = \prod |a - \xi|$, where the product is taken over all complex roots $\xi = e^{i\theta}$ of unity of order n. We have $|a - \xi|^2 = a^2 - 2a\cos\theta + 1$ and $|a - 1|^2 = a^2 - 2a + 1$. Since $n > 1$, $\xi \neq 1$ and so $\cos\theta < 1$. Therefore, we have $|a - \xi| > |a - 1| = a - 1$ for each factor. This implies that $|\phi_n(a)| > a - 1$. □

Finally we need the following straightforward fact from number theory.

Remark 2.3 Let $a > 1$, s and t be positive integers. Then $\gcd\{a^s - 1, a^t - 1\} = a^{\gcd\{s,t\}} - 1$. In particular, if $a^s - 1$ divides $a^t - 1$, then s divides t.

3 Main Results

In this section, by a slight modification of Witt's proof of Wedderburn's theorem, we obtain a characterisation, in terms of order of stabilizer subgroups, for groups acting on a set whose orbits are all singleton. Our main result is:

Theorem 3.1 *Let G be a finite group and Ω a finite G-set. Suppose $|G|$ divides $|\Omega|$ and for each $\omega \in \Delta_1$, $\mathrm{Fix}(G)$ divides $|G_\omega|$. Then all orbits of G are singleton if, and only if, there is a positive integer a and for each $\omega \in \Delta$, a positive integer $n(\omega)$ such that $|G_\omega| = a^{n(\omega)} - 1$.*

Proof. ($\Rightarrow$) If all orbits of G are singleton, it is enough to consider $a = |G| + 1$ and put $n(\omega) = 1$, for each $\omega \in \Delta$.

($\Leftarrow$) Suppose $\Delta_1 \neq \emptyset$. Since for $\omega \in \Delta_1$, $|G_\omega| \geq 1$, so $a > 1$. Therefore, by Remark 2.3, we obtain that

$$\gcd\{a^{n(\omega)} - 1 : \omega \in \Delta_1\} = a^{\gcd\{n(\omega)\ :\ \omega \in \Delta_1\}} - 1.$$

Without loss of generality we can assume $\gcd\{n(\omega) : \omega \in \Delta_1\} = 1$, because in other cases we can replace a by $a^{\gcd\{n(\omega)\ :\ \omega \in \Delta_1\}}$. Therefore, we get

$$\gcd\{a^{n(\omega)} - 1 : \omega \in \Delta_1\} = a - 1.$$

Since for $\omega \in \Delta_1$, $\mathrm{Fix}(G)$ divides $|G_\omega|$, so $\mathrm{Fix}(G) \neq 0$ and therefore $\Delta_2 \neq \emptyset$. Fix $\omega_0 \in \Delta_2$, and consider $n := n(\omega_0)$. For each $\omega \in \Delta_1$, $|G_\omega|$ is a proper divisor of

$|G|$. Therefore the integer $a^{n(\omega)}-1$ is a proper divisor of a^n-1. The second part of Remark 2.3 now implies that $n(\omega)$ is a proper divisor of n and so we have $n>1$. On the other hand, $x^k-1=\prod_{d|k}\phi_d(x)$ holds for any positive integer k. Therefore, the integer $\phi_n(a)$ divides

$$a^n-1/\mathrm{lcm}\{a^{n(\omega)}-1:\omega\in\Delta_1\}=|G|/\mathrm{lcm}\{|G_\omega|:\omega\in\Delta_1\},$$

which in turn divides

$$\gcd\{|G_\omega|:\omega\in\Delta_1\}=\gcd\{a^{n(\omega)}-1:\omega\in\Delta_1\}=a-1$$

according to the Lemma 2.1. As $a>1$, we conclude that $|\phi_n(a)|\leq a-1$. Therefore Lemma 2.2 implies that $n=1$. This is a contradiction and thus $\Delta_1=\emptyset$. Therefore, $\Delta=\Delta_2$ and so all orbits of G are singleton. $\square$

Since groups acting on themselves by conjugation whose orbits are all singleton, are exactly Abelian groups, Theorem 3.1 gives us an arithmetical characterisation for such groups in terms of order of centralisers. Below we make this fact explicit, where Δ now denotes the set of distinct representatives of conjugacy classes of G. Note that the fixed points form the centre of G, and so $\mathrm{Fix}(G)$ divides $|G_\omega|$.

Corollary 3.2 *Let G be a finite group. Then G is Abelian if, and only if, there is a positive integer a and for each $g\in\Delta$, a positive integer $n(g)$ such that $|C_G(g)|=a^{n(g)}-1$.*

By applying Corollary 3.2 to the multiplicative group $F^\times$ of a finite division ring F, we obtain the following corollary due to Wedderburn.

Corollary 3.3 *Let F be a finite division ring. Then F is a field.*

Proof. For each element x in F, the centraliser $C_F(x)$ of x can be regarded as a finite dimensional vector space over the centre $Z(F)$ of F. Denote the dimension of this vector space by $n(x)$. Therefore, we obtain $|C_{F^\times}(x)|=|Z(F)|^{n(x)}-1$ and so Corollary 3.2 implies that $F^\times$ is Abelian, that is, F is a field. $\square$

References

[1] E. Artin, *Über Einen Satz von Herrn J. H. Maclagan Wedderburn*, Abh. Math. Sem. Hamburg **5** (1927), 245-250.

[2] L. E. Dickson, *On Finite Algebras*, Göttingen Nachr. (1905), 358-393.

[3] B. L. van der Waerden, "*Modern Algebra*", Ungar, New York, 1949.

[4] J. H. M. Wedderburn, *A Theorem on Finite Algebras*, Trans. Amer. Math. Soc. **6** (1905), no. 3, 349-352.

[5] E. Witt, *Über die Kommutativität Endlicher Schiefkörper*, Abh. Math. Sem. Hamburg **8** (1931), 413.

The Author's Address

M. R. Pournaki, Department of Mathematical Sciences, Sharif University of Technology, P.O. Box 11365-9415, Tehran, Iran.

E-mail address: pournaki@ipm.ir