International Journal of Pure and Applied Mathematics
Volume 35 No. 3 2007, 293-298

A PARTICULAR AUTOMORPHISM OF A FINITE GROUP

Abdulrasool Azizi
Department of Mathematics
College of Sciences
Shiraz University
Shiraz, 71454, IRAN
e-mails: a_azizi@yahoo.com, razizi@susc.ac.ir

Abstract: In this paper we will find some properties of an automorphism f of a finite group G such that f^3 is the identity automorphism and the equation $f(x) = x$ implies that $x = e$.

AMS Subject Classification: 14G15
Key Words: group, Sylow subgroup, automorphism of a group

1. Introduction

The following Exercise is in [1], Page 103, Problem 19.

Problem. *If G is a finite group and if f is an automorphism of G such that f^3 is the identity automorphism and the equation $f(x) = x$ implies that $x = e$, then every Sylow subgroup of G is normal in G.*

In this article in addition to a proof of the above problem, we will find some more properties of the above automorphism and groups having such automorphisms as well.

Firs notice to the following key lemmas. Lemma 1, is a problem in [1], Section 2.8.

Lemma 1. *If G is a finite group and if f is an automorphism of G such that $f(x) = x$ implies that $x = e$, then $G = \{x^{-1}f(x) \mid x \in G\}$.*

Proof. Consider the function $h : G \to G$, $h(x) = x^{-1}f(x)$. It is easy to see that h is a one-to-one function and since G is a finite set, then h is onto on G. □

Received: May 20, 2005

In the rest of this work, we suppose that G is a finite group and f is an automorphism of G such that f^3 is the identity automorphism and $f(x) = x$ implies that $x = e$.

Lemma 2. *i)* $f(g.f(g)) = g^{-1}$, *for each* $g \in G$.
ii) $g.f(g) = f(g).g$, *for each* $g \in G$.
iii) $G = \{xf(x)|\ x \in G\}$.

Proof. i) By Lemma 1, we have

$$G = \{x^{-1}f(x)\ |x \in G\}\,.$$

Then there exists an $x \in G$ such that $g = x^{-1}f(x)$. So

$$\begin{aligned} f(g.f(g)) = f(x^{-1}f(x)f(x^{-1}f(x))) &= f(x^{-1}f(x)(f(x))^{-1}f^2(x)) \\ &= f(x^{-1})f^3(x) = f(x^{-1})x = (x^{-1}f(x))^{-1} = g^{-1}. \end{aligned}$$

ii) In Lemma 1, if we put f^2 instead of f, we will get

$$G = \{x^{-1}f^2(x)\ |x \in G\}\,.$$

Then there exists an element $y \in G$, such that $g = y^{-1}f^2(y)$. Hence

$$\begin{aligned} f(f(g).g) &= f(f(y^{-1}f^2(y))y^{-1}f^2(y)) = f((f(y))^{-1}f^3(y)y^{-1}f^2(y)) \\ &= f((f(y))^{-1}yy^{-1}f^2(y)) = f((f(y))^{-1}f^2(y)) = (f^2(y))^{-1}f^3(y) \\ &= (f^2(y))^{-1}y = (y^{-1}f^2(y))^{-1} = g^{-1}. \quad (1) \end{aligned}$$

Now by part i) and (1), we have $f(gf(g)) = f(f(g)g)$, and since f is one-to-one then,

$$gf(g) = f(g)g \qquad \forall\, g \in G\,.$$

iii) Consider the function $h : G \to G,\ \ h(x) = xf(x)$. The function h is one-to-one, since if $h(g_1) = h(g_2)$, then by part i), we have $g_1^{-1} = f(g_1f(g_1)) = f(h(g_1)) = f(h(g_2)) = f(g_2f(g_2)) = g_2^{-1}$, hence $g_1 = g_2$. Therefore h is a one-to-one function and since G is a finite set, then h is onto on G as well. Consequently, $G = \{xf(x)\ |x \in G\}$. □

Proposition 3. *If* H *is a subgroup of* G, *then*

$$f^2(H) = \{zf(z)|z \in H\}\,.$$

Proof. Define the function $L : H \to \{zf(z)|z \in H\}$, $L(z) = zf(z)$, obviously L is onto on $\{zf(z)|z \in H\}$. Furthermore L is one-to-one, since if $L(z_1) = L(z_2)$, then by Lemma 2, i), we have

$$z_1^{-1} = f(z_1 f(z_1)) = f(z_2 f(z_2)) = z_2^{-2},$$

that is, $z_1 = z_2$. Since L and f^2 are bijective functions, then

$$|f^2(H)| = |H| = |\{zf(z)|z \in H\}|. \tag{2}$$

Let $z \in H$. By Lemma 2, i),

$$zf(z) = f^{-1}(z^{-1}) = f^2(z^{-1}) \in f^2(H)\,.$$

That is, $\{zf(z)|z \in H\} \subseteq f^2(H)$, and by (2), we get $|f^2(H)| = |\{zf(z)|z \in H\}|$. Consequently $f^2(H) = \{zf(z)|z \in H\}$. □

Theorem 4. *If H is a subgroup of G, then $Hf(H)$ is a subgroup of G.*

Proof. To prove this result we will show that $Hf(H) = f(H)H$.

Let $y,\ t \in H$. By Lemma 2, iii), we have $y = y_1 f(y_1)$, where $y_1 \in G$, and by Lemma 2, i), $f(y) = f(y_1 f(y_1)) = y_1^{-1}$. Then, $y_1 = (f(y))^{-1} = f(y^{-1}) \in f(H)$. Similarly, $t = t_1 f(t_1)$, where $t_1 \in f(H)$. Thus,

$$yf(t) = y_1 f(y_1) f(t_1 f(t_1)) = y_1 f(y_1 t_1) f^2(t_1). \tag{3}$$

Since $y_1 t_1 \in f(H)$, then by Proposition 3, and Lemma 2, ii), we have

$$f(y_1 t_1) \in f^2(H) = \{zf(z)|z \in H\} = \{f(z)z|z \in H\}\,.$$

Let $f(y_1 t_1) = f(t_0)t_0$, where $t_0 \in H$. Then by (3),

$$yf(t) = (y_1 f(t_0))(t_0 f^2(t_1)). \tag{4}$$

Since $y_1 \in f(H)$ and $t_0 \in H$, then obviously $y_1 f(t_0) \in f(H)$, and since $t_1 \in f(H)$, then $f^2(t_1) \in f^3(H) = H$. Also $t_0 \in H$, then $t_0 f^2(t_1) \in H$. Hence by (4), we will get $yf(t) \in f(H)H$. That is, $Hf(H) \subseteq f(H)H$, and obviously $|Hf(H)| = \frac{|H||f(H)|}{|H \cap f(H)|} = |f(H)H|$. Then, $Hf(H) = f(H)H$. □

Remark. Proposition 3 and Theorem 4, does not hold for every arbitrary automorphism of a group. For example in the permutation group S_3, $f : S_3 \to S_3$, $f(1\ 2) = (1\ 3)$, $f(1\ 2\ 3) = (1\ 3\ 2)$, induces an automorphism of S_3, and if $H = \{(I),\ (1\ 2)\}$, then it is easy to see that

$$f(H) = \{(I), (1\ 3)\}, \quad f^2(H) = \{(I),\ (1\ 2)\}\,.$$

Then

$$\{zf(z)|\ z \in H\} = \{(I),\ (1\ 3\ 2)\},\ Hf(H) = \{(I),\ (1\ 3), (1\ 2),\ (1\ 3\ 2)\}.$$

Consequently, $f^2(H) \neq \{zf(z)|\ z \in H\}$, and since $4 \not| 6$, then $Hf(H)$ is not a subgroup of S_3.

Theorem 5. *If P is a p-Sylow subgroup of G, then,*
i) $f(P) = P$.
ii) P is normal in G.

Proof. i) Since f is a bijective function, then

$$|Pf(P)| = \frac{|P||f(P)|}{|P \cap f(P)|} = \frac{|P|^2}{|P \cap f(P)|}. \tag{5}$$

By Theorem 4, $Pf(P)$ is a subgroup of G, then by (5), $Pf(P)$ is a p-subgroup of G, and obviously $P \subseteq Pf(P)$, therefore $Pf(P) = P$. Also $f(P) \subseteq Pf(P) = P$, then $f(P) \subseteq P$, and $|f(P)| = |P|$. Then $P = f(P)$.

ii) Let x be an arbitrary element of G. Obviously $Q = xPx^{-1}$ is a p-Sylow subgroup of G. Therefore, by part i), we have

$$xPx^{-1} = Q = f(Q) = f(xPx^{-1}) = f(x)f(P)f(x^{-1}) = f(x)Pf(x^{-1}).$$

So $P = (x^{-1}f(x))P(f(x^{-1})x) = (x^{-1}f(x))P(x^{-1}f(x))^{-1}$. That is, $x^{-1}f(x) \in N(P)$, for each $x \in G$. Hence by Lamma 1, we have $N(P) = G$. Consequently the p-Sylow subgroup P is normal in G. □

Corollary 6. *i) In the prime factorization of $|G|$, the power of every prime of the form $3k + 2$ is an even number.*
ii) $|G| \equiv 1(mod\ 3)$.

Proof. Let p be a prime number, where $p \equiv 2(mod\ 3)$, $p^\alpha \mid |G|$ and $p^{\alpha+1} \not| |G|$. Also Let P be a p-Sylow subgroup of G, and $x \in P$. By Theorem 5, we have $f(x) \in f(P) = P$, then $f(x) \in P$, and $f^2(x) \in P$. Easily one can see that the following relation is an equivalent relation on P.

$$x \sim y \text{ if and only if } (y = x \vee y = f(x) \vee y = f^2(x)). \tag{6}$$

Obviously for each class $[a]$, where $a \neq e$ of the above relation, we have

$$[a] = \{a,\ f(a),\ f^2(a)\}.$$

Then each class $[a]$, where $a \neq e$ has exactly three elements, and since $P = \bigcup_{a \in P}[a]$, then, $p^\alpha = |P| \equiv 1(mod\ 3)$. Also $p \equiv 2(mod\ 3)$, hence α must be an even number.

ii) It is easy to see that the relation defined in (6) is also an equivalent relation on G, and if $e \neq a$, then $|[a]| = 3$. Also $|[e]| = 1$. We know that $G = \bigcup_{a \in G}[a]$, then, $|G| \equiv 1(mod\ 3)$. □

Remark. By Corollary 6, if a finite group G has an automorphism f such that $f^3 = I$, and the equation $f(x) = x$ implies that $x = e$, then $|G| \equiv 1(mod\ 3)$. Now let $G = Z_p$, where p is a prime number. Then $p = |Z_p| \equiv 1(mod\ 3)$. Let f be an automorphism of Z_p such that $f(\bar{1}) = \bar{k}$, where $k \in Z,\ 0 \leq k \leq p-1$. Since $f(x) = x$ implies that $x = \bar{0}$, then $k \neq 1$. The condition $f^3 = I$ implies that $\bar{1} = f(f(f(\bar{1}))) = \bar{k^3}$. Then, $p|k^3 - 1$, that is $k^3 \equiv 1(mod\ p)$.

The condition $f(\bar{m}) = \bar{m}$, implies that, $\bar{m} = f(\bar{m}) = \bar{mk}$, then $p|m(k-1)$. Since $(p, k-1) = 1$, then $p|m$. That is, $\bar{m} = 0$, in Z_p. So the second condition always holds for every non trivial automorphism of Z_p.

Corollary 7. *If p is a prime number, then the equation $x^3 \equiv 1(mod\ p)$, has a non trivial integer solution (that is, $x \not\equiv 1(mod\ p)$) if and only if $p \equiv 1(mod\ 3)$.*

Proof. If x_0 is a non trivial solution of the equation $x^3 \equiv 1(mod\ p)$, and $x_0 \equiv k(mod\ p)$, where $0 \leq k \leq p-1$. Obviously, k is a solution of the equation $x^3 \equiv 1(mod\ p)$. Now by the previous remark, $f : Z_p \longrightarrow Z_p$, $f(\bar{1}) = \bar{k}$, defines an automorphism such that such that $f^3 = I$, and the equation $f(x) = x$, implies that $x = 0$. Thus $p = |Z_p| \equiv 1(mod\ 3)$.

Conversely let p is a prime number such that $p \equiv 1(mod\ 3)$. Since Z_p is a cyclic group of order p, then, $3|p - 1 = \varphi(p) = |\mathrm{Aut}(Z_p)|$. Now by Cauchy's Theorem $\mathrm{Aut}(Z_p)$ has an element f of order 3. That is, $f^3 = I$, and $f \neq I$. Let $f(\bar{1}) = \bar{k}$, where $0 \leq k \leq p-1$. Since $f \neq I$, then $k \neq 1$. Also $\bar{1} = f(f(f(\bar{1}))) = \bar{k^3}$, then k is a non trivial solution of the equation $x^3 \equiv 1(\ mod\ p)$. □

Acknowledgments

The author would like to thank Y. Sharifi for some comments to this work.

References

[1] I.N. Herstein, *Topics in Algebra*, Second Edition, John Wiley and Sons Inc., New York (1975).

[2] T.W. Hungerford, *Algebra*, Springer-Verlog, New York Inc. (1989).

[3] J. Rotman, *The Theory of Groups*, Second Edition, Allyn and Bacon, Inc., Boston (1973).