韓國數學敎育學會誌 <數學敎育>
1981. 12. Vol. XX. No. 1

Journal of the Korea Society of Mathematical Education
Dec. 1981. Vol. XX No. 1

Involutions in A Finite Group

By Eung Tai Kim

Seoul National University, Seoul, Korea

1. Introduction

An element of order 2 in a group is called *involution*. An important insight into the structure of a finite group is obtained by studying its involutions and their centralizers.

Richard and Suzuki [1] proved that a finite 2-group containing only one involution is cyclic or generalized quaternion group.

Dieudonne [2] and McDonald [3] characterized the automorphisms of linear group $GL(V)$ of finite dimensional R-space V over a ring R by the method of involutions.

The symmetric group Σ_5 contains exactly two conjugacy classes of involutions which are the set S_1 of all transpositions and the set S_2 of all products of two disjoint transpositions. If $a_1 \in S_1$ and $a_2 \in S_2$ are representatives of these conjugacy classes, then the centralizer $C_{\Sigma_5}(a_1) \cong \langle a_1 \rangle \times \Sigma_3$ and the centralizer $C_{\Sigma_5}(a_2)$ is a dihedral group of order 8.

In this paper, we shall study some properties of involutions in a group and prove the following main theorem, which is the converse of the above statement, by utilizing the properties of involutions.

Theorem. *Let the finite group G contain exactly two conjugacy classes of involutions and let a_1, a_2 be representatives of these classes. Suppose $C_G(a_1) \cong \langle a_1 \rangle \times \Sigma_3$ and $C_G(a_2)$ is a dihedral group of order* 8. *Then $G \cong \Sigma_5$.*

2. Involutions

In this paper, G is a finite group.

Lemma 2.1. *If a and b are distinct involutions in group G, then $\langle a, b \rangle$ is isomorphic to a dihedral group.*

Proof. Let $u = ba$ and let u be of order n. Then,

$$\langle a, b \rangle = \{x \mid x = u^k \text{ or } x = au^k a,\ k = 0, \pm 1, \pm 2, \cdots\} = \langle u, a \mid u^n = 1, ua = au^{-1} \rangle,$$

which is a dihedral group.

Lemma 2.2. *Let a and b be involutions in G.*

(1) *If ab is of odd order, then a and b are conjugate in G.*

(2) *If ab is of even oder 2m, then $v = (ab)^m$ is an involution and $a, b \in C_G(v)$.*

Proof. (1) Let order of ab be $2m+1$, then $(ab)^{2m+1}=1$ and

$$1=(ab)^m a(ba)^m b,\ b=(ab)^m a(ab)^{-m}.$$

Therefore a and b are conjugate in G.

(2) Clearly, $v=(ab)^m$ is an involution in G, and

$$a^{-1}va=a(ab)^m a=(ba)^m=(a^{-1}b^{-1})^{-m}=(ab)^{-m}=(ab)^m=v,$$

$$b^{-1}vb=b(ab)^m b=(ba)^m=(ab)^{-m}=(ab)^m=v.$$

Therefore $a, b\in C_G(v)$.

Lemma 2.3. *Suppose G contains a subgroup H of even order which does not contain all involutions of G. If $C_G(a)\subset H$ for any involution $a\in H$, then any two involutions in G are conjugate.*

Proof. Let a and b be involutions in G.

(case 1). $a\in H,\ b\notin H$. Suppose a and b are not conjugate. Then ab is of even order by LEMMA 2.2, (1). Therefore there is an involution v such that $a, b\in C_G(v)$. Then,

$$H\supset C_G(a)\supset C_G(a)\cap C_G(b)\ni v.$$

Therefore $a, b\in C_G(v)\subset H$. This leads to the contradiction that $b\in H$. Hence if $a\in H$ and $b\notin H$, then a and b are conjugate.

(case 2). $a\in H,\ b\in H$. There exists an involution $c\notin H$ by the assumption. Then a, c are conjugate, and b, c are conjugate by case 1, so a and b are conjugate.

(case 3). $a\notin H,\ b\notin H$. The subgroup H contains an involution c, since H is of even order. Then a, c are conjugate, and b, c are conjugate, so a and b are conjugate.

3. Proof of the Theorem

We shall now prove the main theorem according to the following lemmas. In this paragraph, let G be the finite group which contains exactly two conjugacy classes F_1, F_2 of involutions, and let $a_1\in F_1$ and $a_2\in F_2$ be representatives of these classes, and suppose $C_1=C_G(a_1)\cong\langle a_1\rangle\times\Sigma_3$ and $C_2=C_G(a_2)$ is a dihedral group of order 8.

Let $c_i=|C_G(a_i)|,\ i=1, 2$. Let $S_i,\ i=1, 2$, be the set of ordered pairs (x, y) with x conjugate to a_1, y conjugate to a_2 and $(xy)^m=a_i$ for some m. Let $|S_i|=s_i$.

Lemma 3.1. $|G|=c_1s_2+c_2s_1$.

Proof. Let $S=\{(x, y)\,|\,x$ is conjugate to a_1, and y is conjugate to $a_2\}$. Then $|S|=(|G|/c_1)(|G|/c_2)$. On the other hand, since for any $(x, y)\in S$, x is not conjugate to y, LEMMA 2.2 implies that for $m=o(xy)/2$, where $o(xy)$ is the order of xy, $(xy)^m$ is an involution. Therefore $(xy)^m$ is conjugate to either a_1 or a_2, since G contains exactly two conjugacy classes of involutions.

Let $T_i=\{(x, y)\in S\,|\,(xy)^m$ is conjugate to a_i for some $m\}$, $i=1, 2$. Then $S=T_1\cup T_2$, $T_1\cap T_2=\phi$, $|T_i|=(|G|/c_i)s_i$. Therefore,

$$(|G|/c_1)(|G|/c_2)=(|G|/c_1)s_1+(|G|/c_2)s_2,\ |G|=c_1s_2+c_2s_1.$$

Lemma 3.2. *C_2 is a Sylow 2-subgroup of G.*

Proof. Let P be a Sylow 2-subgroup of G containing C_2. Then there exists an involution c in the center of P. Suppose c be conjugate to a_1, then $|C_G(c)|=|C_G(a_1)|=12$. But

$8 \mid |C_G(c)|$, since $C_G(c) \supset C_2$ and $|C_2|=8$. This leads to the contradiction. Therefore c is conjugate to a_2. Hence $|C_2| \leq |P| \leq |C_G(c)| = |C_2|$.

Therefore $C_2=P$, that is, C_2 is a Sylow 2-subgroup of G.

Lemma 3.3. *There is an involution $a \in C_2$, which is conjugate to a_1 and $a_2 \in C_G(a)$.*

Proof. Let P be a Sylow 2-subgroup containing a_1. Then $g^{-1}Pg=C_2$ for some $g \in G$, since C_2 is a Sylow 2-subgroup of G. So, $g^{-1}a_1g=a \in C_2$. Then $a_2 \in C_G(a)$, clearly.

In the following lemmas, replacing a_1 by a conjugate element, we assume $a_1 \in C_2$ and $a_2 \in C_1$ by LEMMA 3.3.

Lemma 3.4. (1) *C_1 contains three classes of involutions, and if x is an involution in C_1, $x \neq a_1$, then x is not conjugate to xa_1 in C_1.*

(2) *For any involution x in C_1, $x \neq a_1$, exactly one of x and xa_1 is conjugate to a_1 in G.*

(3) $s_i=9$.

Proof. (1) Since $C_1 \cong \langle a_1 \rangle \times \Sigma_3 = \langle a_1 \rangle \times \langle u, v \mid u^3=v^2=1,\ vu=u^2v \rangle$, we shall denote

$$C_1=\{1,\ u,\ u^2,\ v,\ uv,\ u^2v,\ a_1,\ ua_1,\ u^2a_1,\ va_1,\ uva_1,\ u^2va_1\}$$

Then C_1 contains the following three classes of involutions,

$$F_1=\{a_1\},\quad F_2=\{v, uv, u^2v\},\quad F_3=\{va_1,\ uva_1,\ u^2va_1\}$$

Clearly, if x is an involution in C_1, $x \neq a_1$, then x is not conjugate to xa_1 in C_1.

(2) Since $x \in C_1$ *and* $x \neq a_1$, $x \in F_2$ or $x \in F_3$. If $x \in F_2$, then $xa_1 \in F_3$, and conversely if $x \in F_3$, then $xa_1 \in F_2$. Suppose both of x and xa_1 are conjugate to a_1 in G. Then all involutions in C_1 are conjugate to a_1. But, since $a_2 \in C_1$, this leads to the contradiction. So, at most one of x and xa_1 is conjugate to a_1. Since G contains two conjugacy classes, exactly one of x and xa_1 is conjugate to a_1.

(3) Since $a_2 \in C_2$ and $a_1 \neq a_2$, $a_2 \in F_2$ or $a_2 \in F_3$. Suppose $a_2 \in C_2$. Then a_1 is conjugate to elements of F_3 in G. Therefore

$$S_1=\{(x,y) \mid x \in F_2,\ y \in F_3,\ (xy)^m=1 \text{ for some } m\},$$

hence $s_1=|S_1|=3 \cdot 3=9$.

Lemma 3.5. (1) *C_2 contains three conjugacy classes of involutions, and if x is an involution in C_2, $x \neq a_2$, then x is conjugate to xa_2.*

(2) $s_2=4$.

(3) $|G|=120$.

Proof. (1) Since $C_2=\langle u, v \mid u^4=v^2=1,\ vu=u^3v \rangle = \{1, u, u^2, u^3, v, uv, u^2v, u^3v\}$, C_2 contains the following three conjugacy classes of involutions,

$$F_1=\{u^2\}=\{a_2\},\quad F_2=\{v, u^2v\},\quad F_3=\{uv, u^3v\}$$

If x is an involution in C_2, $x \neq a_2$, then x is conjugate to $xa_2=xu^2$.

(2) Since $a_1 \in C_2$ and $a_1 \neq a_2$, $a_1 \in F_2$ or $a_1 \in F_3$. For any $x \in F_2$ and $y \in F_3$, x and y are not conjugate in G. For, if x and y were conjugate in G, then every $z \in F_2 \cup F_3$ would be conjugate to a_1 and $(za_2)^m=a_2$ or $(za_2)^m=a_1$ for some m. It is impossible in C_2.

Suppose $a_1 \in F_2$. Then every element of F_3 is conjugate to a_2 in G. Therefore $S_2=\{(x,y) \mid x \in F_2,\ y \in F_3,\ (xy)^m=a_2 \text{ for some } m\}$, hence $s_2=|S_2|=2 \cdot 2=4$.

(3) By using LEMMA 3.1, we have $|G|=120$.

Lemma 3.6. (1) *C_2 contains a non-cyclic group K of order 4 such that $a_2 \in K$ and all the involutions in K are conjugate in G.*

(2) $C_G(K)=K$.

(3) *$N_G(K)$ contains at least two Sylow 2-subgroups of G.*

Proof. (1) If we use the notations in the proof of LEMMA 3.5, we know that C_2 contains a non-cyclic group K of order 4 such that $a_2 \in K$, that is, $K=\{1, a_2, uv, uva_2\}$, and all the involutions in K are conjugate in G.

(2) Let $x \in C_G(K)$, then $x^{-1}a_2x=a_2$, hence $x \in C_2$. Therefore $C_G(K)=C_{C_2}(K)=K$.

(3) There exists an element x of G such that $x^{-1}a_2x \neq a_2$ and $x^{-1}a_2x \in K$, since the three elements of K different from identity are conjugate in G. Then $x^{-1}C_2x \neq C_2$, since $u \in C_2$ but $u \notin x^{-1}C_2x$, and $a_2 \in C_G(x^{-1}a_2x)$. So, $x^{-1}Kx$ contains a_2 and $x^{-1}a_2x$ which are elements of K. Therefore $x^{-1}Kx=K$, hence $x \in N_G(K)$. Since $N_G(K) \supset C_2$, $N_G(K)=x^{-1}N_G(K)x \supset x^{-1}C_2x$. That is $N_G(K)$ contains at least two Sylow 2-subgroups of G.

Lemma 3.7. $N_G(K)/K \cong \mathrm{Aut}\,K \cong \Sigma_3$, $|N_G(K)|=24$.

Proof. Let the mapping $f: N_G(K) \to \mathrm{Aut}\,K$ be defined by $f(g)(x)=g^{-1}xg$ for $g \in N_G(K)$ and $x \in K$. Then f is a group homomorphism.

Let $S=\{x\} \cup C_2 \cup x^{-1}C_2x$ where x is an element of $N_G(K)$ and C_2, $x^{-1}C_2x$ are Sylow 2-subgroups contained in $N_G(K)$, which were obtained in the proof of LEMMA 3.6, (3). Then we can show that $f(S)=\mathrm{Aut}\,K$ easily.

Therefore f is surjective homomorphism. Since $C_G(K)=K$, $\ker f=K$. Therefore $N_G(K)/K \cong \mathrm{Aut}\,K \cong \Sigma_3$. Hence $|N_G(K)|=|\Sigma_3| \cdot |K|=6 \cdot 4=24$.

Lemma 3.8. $[G:N_G(K)]=5$, $|G| \cong \Sigma_5$.

Proof. Since $|G|=120$ and $|N_G(K)|=24$, $[G:N_G(K)]=5$.

Let X be the coset space $\{N_G(K)g_i \mid i=1,2,\cdots,5\}$, and let $\Sigma(X)$ be the group of all permutations on X. Then $\Sigma(X) \cong \Sigma_5$.

Let the mapping $f: G \to \Sigma(X)$ be defined by $f(g)(N_G(K)g_i)=N_G(K)g_ig$. Then f is a group homomorphism, and $\ker f=\bigcap_{X \in G} x^{-1}N_G(K)x$.

Now, there is an element $x \in G$ such that $x^{-1}a_2x \notin K$, since number of elements of the conjugacy class containing a_2 is $c_2=|G|/8=15$. For this x, $N_G(x^{-1}Kx) \cap N_G(K)=\{1\}$. Then $\ker \mathrm{f}=\bigcap_{X \in G} x^{-1}N_G(K)x=\{1\}$, since $N_G(x^{-1}Kx)=x^{-1}N_G(K)x$.

Therefore f is injective and surjective, since $|G|=120=|\Sigma(X)|$. So, $G \cong \Sigma(X) \cong \Sigma_5$.

References

1. Brauer, Richard; Suzuki, Michio, On finite groups of even order whose Sylow 2-subgroup is a quaternion group, *Proc. Nat. Acad. Sc. U.S.A.*, 45 (1959).
2. Dieudonne, J., On the automorphisms of classical groups, *Memories of A.M.S.*, 2 (1950).
3. McDonald, B.R., Automorphisms of $GL_n(R)$, *Trans. A.M.S.*, 215(1976), 145—159.