SEMI-AUTOMORPHISMS OF GROUPS

I. N. HERSTEIN1 AND M. F. RUCHTE

A semi-automorphism of a group $G$ is a 1–1 mapping, $\phi$, of $G$ onto itself such that $\phi(aba) = \phi(a)\phi(b)\phi(a)$ for all $a, b \in G$. The nature of such mappings, in the special cases when $G$ is the symmetric or alternating group (finite or infinite) and in a few other examples, was determined by Dinkines [1], who showed they must be automorphisms or anti-automorphisms. Her proof was rather computational in character. In her paper she conjectured that a semi-automorphism of a simple group is either an automorphism or an anti-automorphism.

In this paper we prove this result for a wide class of simple groups, finite or infinite. In the process of doing so we are led to a simplified, and somewhat more conceptual, proof of Dinkines’s results.

In the body of this paper $\phi$ will denote a semi-automorphism of the group $G$.

We begin with

**Lemma 1.** If $G$ has no elements of order 2 in its center, then:
1. $\phi(e) = e$ where $e$ is the identity of $G$,
2. $\phi(a^{-1}) = \phi(a)^{-1}$,
3. $\phi(a^n) = \phi(a)^n$
for all $a \in G$ and all integers $n$

The proof of this lemma is straightforward and will be omitted. Suppose that $G$ has no elements of order 2 in its center. Suppose further that there are $c, d \in G$ so that $cxc = dxd$ for all $x \in G$. In particular, putting $x = e$, we obtain $c^2 = d^2$. If we put $x = c$ in the above relation we arrive at $c^3 = dcd$, which, together with $c^2 = d^2$, yields $cd = dc$. Thus $(cd^{-1})^2 = e$. But, by assumption, $d^{-1}cxcd^{-1} = x$, and so, by the above remarks, $(cd^{-1})^{-1}x(cd^{-1}) = x$, for all $x \in G$. But then $cd^{-1}$ is an element in the center of $G$ whose square is $e$, so $cd^{-1} = e$; hence we have proved

**Lemma 2.** If $G$ has no elements of order 2 in its center and if for $c, d \in G$, $cxc = dxd$ for all $x \in G$, then $c = d$.

We proceed to

Presented to the Society January 28, 1958; received by the editors June 8, 1957.

1 The first author was partially supported in the research for this paper by an ONR contract with Yale University and by an NSF grant to him.
**Lemma 3.** If $G$ has only $(e)$ as its center and if for $a, b \in G$, $ab = ba$ then $\phi(ab) = \phi(a)\phi(b)$.

**Proof.** By the definition of semi-automorphism and Lemma 1, $\phi(ab^2a) = \phi(a)\phi(b)^2\phi(a)$. Since $ab = ba$,

$$\phi(ab^2a) = \phi(ba^2b) = \phi(b)\phi(a)^2\phi(b).$$

If we let $u = \phi(a)\phi(b)$ and $v = \phi(b)\phi(a)$, the above discussion leads us to $uv = vu$.

Let $x \in G$. Then

$$\phi(abxba) = \phi(a)\phi(b)\phi(x)\phi(b)\phi(a) = u\phi(x)v.$$ 

But

$$\phi(abxba) = \phi(baxab) = \phi(b)\phi(a)x\phi(a)\phi(b) = v\phi(x)u.$$ 

Thus $u\phi(x)v = v\phi(x)u$, and since $uv = vu$, we conclude that $v^{-1}u\phi(x) = \phi(x)v^{-1}u$. Since $\phi$ is onto, this means that $v^{-1}u$ is in the center of $G$, so is equal to $e$. That is, $u = v$; equivalently $\phi(a)\phi(b) = \phi(b)\phi(a)$.

Now

$$\phi(a)\phi(b)\phi(x)\phi(a)\phi(b) = \phi(a)\phi(b)\phi(x)\phi(b)\phi(a) = \phi(abxba) = \phi(abxab) = \phi(ab)\phi(x)\phi(ab).$$

Invoking Lemma 2 we now arrive at $\phi(ab) = \phi(a)\phi(b)$ which is the contention of Lemma 3.

The following theorem is the key to our approach to the problem, affording us a reduction from a general semi-automorphism to a very particular one. It is

**Theorem 1.** If $G$ is generated by its elements of order 2 and has a trivial center then there exists a semi-automorphism $\psi$ such that:

1. $\psi(axa^{-1}) = a\psi(x)a^{-1}$ for all $a, x \in G$.
2. $\psi^{-1}$ is an automorphism of $G$.
3. $a\psi(a) = \psi(a)a$ for all $a \in G$.
4. if $a^2 = e$ then $\psi(a) = a$.

**Proof.** Let $W = \{ u \in G \mid \exists c_u \in G, \phi(uxu^{-1}) = \phi(c_u)\phi(x)\phi(c_u)^{-1} \text{ for all } x \in G \}$. Since $\phi$ is a semi-automorphism, $W$ clearly contains all elements $a$, of order 2 (with $c_a = a$). We claim that $W$ is a subgroup of $G$. For if $a, b \in W$, then

$$\phi(abxb^{-1}a^{-1}) = \phi(c_a)\phi(c_b)\phi(x)\phi(c_b)^{-1}\phi(c_a)^{-1},$$

and since $\phi$ is onto, $\phi(c_a)\phi(c_b) = \phi(t)$ for some $t \in G$. So $ab \in W$. Similarly, one shows that $\phi(a^{-1}xa) = \phi(c_a)^{-1}\phi(x)\phi(c_a)$ for $a \in W$. Thus
$W$ is indeed a subgroup of $G$. Because it contains all elements of order 2, which generate $G$, $W = G$ follows. Thus for any $a \in G$ there is a $c_a \in G$ so that $\phi(axa^{-1}) = \phi(c_a)\phi(x)\phi(c_a)^{-1}$ for all $x \in G$. Since $G$ has a trivial center it is clear that $c_a$ is unique. We define $\psi^{-1}$ by $\psi^{-1}(a) = c_a$. In showing that $W$ was closed we actually showed that $\phi(c_{ab}) = \phi(c_a)\phi(c_b)$ and that $\phi(c_{a^{-1}}) = \phi(c_a)^{-1}$, so that $\phi\psi^{-1}$ is an isomorphism of $G$ into itself. Also if $x^2 = e$ then $\phi\psi^{-1}(x) = \phi(x)$ so every element of order 2 is in the image of $\phi\psi^{-1}$ which is now a subgroup of $G$, so the image must be all of $G$ by our assumptions; hence $\phi\psi^{-1}$ is onto so is an automorphism of $G$, from which it follows that $\psi^{-1}$ is a semi-automorphism of $G$. Thus $\psi$ is also a semi-automorphism of $G$.

By its very definition,

$$\phi(axa^{-1}) = \phi\psi^{-1}(a)\phi(x)\phi\psi^{-1}(a)^{-1}$$

for all $a, x \in G$.

Since $(\phi\psi^{-1})^{-1} = \psi\phi^{-1}$ is an automorphism of $G$, applying it to this identity we obtain that $\psi(axa^{-1}) = a\psi(x)a^{-1}$ for all $a, x \in G$. If we put $x = a$ in this we see that $a\psi(a) = \psi(a)a$.

Finally, in its very definition we saw that if $a^2 = e$ then $c_a = a$ and so $\psi(a) = a$. The theorem is now completely proved.

**Corollary.** If $\psi$ is an automorphism or an anti-automorphism of $G$ then so is $\phi$.

This is immediate from part (2) of the theorem.

Our aim is to prove that for a wide class of groups (in particular, these are generated by their elements of order 2 and have trivial centers), a semi-automorphism is either an automorphism or an anti-automorphism. To do so, as we have just seen, it is enough to do so for a particular class of semi-automorphisms, namely such $\psi$'s so that:

1. $\psi(axa^{-1}) = a\psi(x)a^{-1}$,
2. $a\psi(a) = \psi(a)a$,
3. $a^2 = e$ implies that $\psi(a) = a$.

Henceforth in this paper we restrict ourselves to such and $\psi$ will denote a semi-automorphism with properties (1), (2) and (3).

**Lemma 4.** If

$$M = \{a \in G \mid \psi(ax) = \psi(a)\psi(x)\text{ all } x \in G\}$$

and

$$N = \{a \in G \mid \psi(ax) = \psi(x)\psi(a)\text{ all } x \in G\}$$

then $M$ and $N$ are normal subgroups of $G$.

**Proof.** We show only that $M$ is normal in $G$, for the proof for $N$ is almost identical.
Let $a, b \in M, x \in G$. Then
\[ \psi(abx) = \psi(a)\psi(bx) = \psi(a)\psi(b)\psi(x) = \psi(ab)\psi(x), \]
so $ab \in M$. Similarly $a^{-1} \in M$. Thus $M$ is a subgroup of $G$. If $a \in M, x, y \in G$, then
\[
\begin{align*}
\psi(xax^{-1}y) &= \psi(xax^{-1}yx^{-1}) = x\psi(ax^{-1}yx)x^{-1} = x\psi(a)\psi(x^{-1}yx)x^{-1} \\
&= x\psi(a)x^{-1}\psi(y)xx^{-1} = \psi(xax^{-1})\psi(y)
\end{align*}
\]
from the fact that $\psi(wu^{-1}) = \psi(u)w^{-1}$.

So $xMx^{-1} \subseteq M$ for all $x \in G$. Thus $M$ is normal in $G$.

**Corollary.** If $G$ is simple and $\psi$ is neither an automorphism nor an anti-automorphism then $M = N = \{e\}$.

**Lemma 5.** If $G$ is simple and $\psi$ is neither an automorphism nor an anti-automorphism and if $\psi(a) = a$ or if $\psi(a) = a^{-1}$ then $a^2 = e$.

**Proof.** Suppose $\psi(a) = a$. For all $x \in G$,
\[ \psi(a^2x) = \psi(a(axa)a^{-1}) = a\psi(axa)a^{-1} = a\psi(a)\psi(x)\psi(a)a^{-1} = a^2\psi(x) = \psi(a^2)\psi(x). \]
Hence $a^2 \in M = \{e\}$, and so $a^2 = e$. Similarly if $\psi(a) = a^{-1}$, $a^2 \in N = \{e\}$.

**Lemma 6.** If $G$ is simple and if $\psi^2$ is an automorphism of $G$ then $\psi(x) = x$ for all $x \in G$ or $\psi(x) = x^{-1}$ for all $x \in G$.

**Proof.** If $\psi^2$ is an automorphism of $G$, since
\[ \psi^2(axa^{-1}) = a\psi^2(x)a^{-1} \]
and since
\[ \psi^2(axa^{-1}) = \psi^2(a)\psi^2(x)\psi^2(a)^{-1}, \]
we must conclude that $\psi^2(a) = a$ for all $a \in G$.

Now let $x \in G$. By the properties of $\psi$, $x\psi(x) = \psi(x)x$; thus by Lemma 3,
\[ \psi(x\psi(x)) = \psi(x)\psi^2(x) = \psi(x)x = x\psi(x). \]
Since $x\psi(x)$ is left fixed by $\psi$, by Lemma 5 we have that $(x\psi(x))^2 = e$. Thus $\psi(x^2) = x^{-2}$. If $\psi$ is neither an automorphism nor an anti-automorphism, by Lemma 5 again we are forced to $x^4 = e$. Thus $G$ is a simple group in which $x^4 = e$ for all $x \in G$. However, since the Burnside problem has been solved by Sanov for exponent 4, [3], we know $G$ is locally finite. Thus a finite set of elements generates a finite subgroup in which $x^4 = e$, so this subgroup is of order a power of 2, and
so is nilpotent. Thus $G$ is locally nilpotent. As is pointed out in [2, p. 222] a simple group cannot be locally nilpotent. Thus $\psi$ itself must be an automorphism or an anti-automorphism. Since

$$\psi(axa^{-1}) = a\psi(x)a^{-1} = \psi(a)\psi(x)\psi(a)^{-1} \text{ (or } = \psi(a)^{-1}\psi(x)\psi(a))$$

we obtain that $\psi(a) = a$ or $\psi(a) = a^{-1}$.

**Lemma 7.** If $G$ is simple and if $\psi^2(a) = a$ for some $a \in G$ such that $a^2 \neq e$ then either $\psi(x) = x$ for all $x \in G$ or $\psi(x) = x^{-1}$ for all $x \in G$.

**Proof.** $\psi^2$ is itself a semi-automorphism of $G$. Moreover it satisfies the properties (1), (2) and (3) that $\psi$ satisfies. If $\psi^2$ is an automorphism of $G$ then by Lemma 6 we would obtain Lemma 7. If $\psi^2$ is an anti-automorphism it is easy to see that $\psi^2(x) = x^{-1}$ for all $x$, but since $\psi^2(a) = a$ by assumption we obtain from the above remark that $a = a^{-1}$, violating the fact that $a^2 \neq e$. If $\psi^2$ is neither an automorphism nor an anti-automorphism then by Lemma 5 if $\psi^2(a) = a$ or $\psi^2(a) = a^{-1}$ then $a^2 = e$. Thus the lemma is proved.

We now turn to

**Lemma 8.** If $G$ is simple and has an element of order 4 then $\psi(x) = x$ for all $x \in G$ or $\psi(x) = x^{-1}$ for all $x \in G$.

**Proof.** Suppose $a^4 = e$, $a^2 \neq e$. Now, since $(a^2)^2 = e$, $\psi(a^2) = a^2 = a^{-2}$. Also, since $a\psi(a) = \psi(a)a$, we can go one step further and say that $(a\psi(a))^2 = e$. But then $\psi(a\psi(a)) = a\psi(a)$. Thus $\psi(a)\psi^2(a) = a\psi(a) = \psi(a)a$. So $\psi^2(a) = a$. By Lemma 7 the result follows.

The pieces are now all in place for us to prove the main result of this paper, namely

**Theorem 2.** Let $G$ be a simple group which has an element of order 4. Then any semi-automorphism of $G$ is either an automorphism or an anti-automorphism.

**Proof.** Let $\phi$ be a semi-automorphism of $G$. Since $G$ has an element of order 4, it has elements of order 2; these generate a nontrivial normal subgroup, so they must generate all of $G$. Also $G$ has a trivial center. Thus Theorem 1 applies to produce a $\psi$ for us with $\phi\psi^{-1}$ an automorphism of $G$. This $\psi$, by Lemma 8 is either the identity map or maps every element on its inverse; thus $\psi$ is an automorphism or anti-automorphism. Thus the same is true for $\phi$.

The theorem raises an interesting side question, namely, what simple groups (in particular, what finite simple groups of even order) fail to have elements of order 4. Finite simple groups whose orders are divisible by 4 but not by 8, have this property. Are there others?
The alternating groups of degree larger than 5 do have elements of order 4. (For the case $A_3, A_4, A_5$ we could adapt our argument.) So we have

**Corollary 1 (Dinkines).** A semi-automorphism of an alternating group is an automorphism or an anti-automorphism.

Let $S$ be a symmetric group. Let $\phi$ be a semi-automorphism of $S$, and let $\psi$ be constructed for $\phi$ as in Theorem 1. $\psi$ then induces a semi-automorphism on the alternating group, $A$, so there $\psi(x) = x$ or $\psi(x) = x^{-1}$ for all $x \in A$. We may assume, say, that $\psi(x) = x$. If $y \in S$, $x \in A$, then $yxy \in A$, so

$$\psi(yxy) = yxy = \psi(y)\psi(x)\psi(y) = \psi(y)x\psi(y),$$

so $y = \psi(y)$. So we have

**Corollary 2 (Dinkines).** A semi-automorphism of a symmetric group (of degree greater than 2) is an automorphism or anti-automorphism.

**Bibliography**


Yale University