SEMI-HOMOMORPHISMS OF GROUPS

I. N. HERSTEIN

A mapping ϕ from one group, G, into another, H, is said to be a *semi-homomorphism* of G if $\phi(aba) = \phi(a)\phi(b)\phi(a)$ for all $a, b \in G$. Clearly any homomorphism or anti-homomorphism is a semi-homomorphism; the converse, however, need not be true in general. It is perfectly clear what one intends by a semi-isomorphism or semi-automorphism.

Our purpose here is to show that for a rather general situation a semi-homomorphism turns out to be a homomorphism or an anti-homomorphism. In **(2)** we proved that any semi-automorphism of a simple group which contains an element of order 4 must automatically be either an automorphism or an anti-automorphism. As a special case of the results that we prove in the present note, this above-mentioned theorem holds true merely in the presence of an element of order 2. In particular, in the light of the famous theorem of Feit and Thompson **(1)** the result is true for all finite simple groups. Another consequence of our results is that for a large family of simple groups semi-homomorphisms turn out to be one-to-one. Of course when we say simple we always exclude the trivial case of a cyclic group of prime order.

In all that follows ϕ will denote a semi-homomorphism of a group G into a group H. We shall progressively condition G and H as we go along. We begin with

LEMMA 1. *Suppose that the centralizer of $\phi(G)$ in H is (1), (that is, if $x \in H$ satisfies $x\phi(g) = \phi(g)x$ for all $g \in G$, then $x = 1$); then*

(a) $\phi(1) = 1$,

(b) $\phi(a^n) = \phi(a)^n$ *for all integers n and all $a \in G$.*

Proof. If $a \in G$, then $\phi(a) = \phi(aa^{-1}a) = \phi(a)\phi(a^{-1})\phi(a)$; cancelling we obtain that $\phi(a^{-1}) = \phi(a)^{-1}$. In particular, for $a = 1$ we get $\phi(1)^2 = 1$. Now for any $g \in G$, $\phi(g) = \phi(1g1) = \phi(1)\phi(g)\phi(1)$, which, together with the above, yields $\phi(1)\phi(g) = \phi(g)\phi(1)$ for all $g \in G$. By our hypothesis we see that $\phi(1) = 1$.

We show that $\phi(a^n) = \phi(a)^n$ for $n \geqslant 0$. For $n = 0$ we have just proved it; the case $n = 1$ is trivial. For $n = 2$, $\phi(a^2) = \phi(a1a) = \phi(a)\phi(1)\phi(a) = \phi(a)^2$.

Original received June 27, 1966, and revised version November 1, 1966. In the first version of this paper the results were proved for the case of semi-automorphisms of simple groups. The results were generalized to the present situation while the author was a guest at the Mathematics Research Institute of the E.T.H. in Zürich.

This work was supported by a grant from the Army Research Office, ARO(D), at the University of Chicago.

For $n = 3$ it is automatic from the definition of semi-homomorphism.

We proceed by induction on n, assuming that $n \geqslant 3$. Now

$$\phi(a^n) = \phi(aa^{n-2}a) = \phi(a)\phi(a^{n-2})\phi(a) = \phi(a)\phi(a)^{n-2}\phi(a) = \phi(a)^n$$

by the induction. The result is thus established for $n \geqslant 0$. Since $\phi(a^{-1}) = \phi(a)^{-1}$, we immediately get that $\phi(a^n) = \phi(a)^n$ for n a negative integer. This proves the lemma.

LEMMA 2. *Let G, H, ϕ be as in Lemma 1. If for $a, b, c, d \in H$, $a\phi(g)b = c\phi(g)d$ for all $g \in G$, then $a = c$ and $b = d$.*

Proof. Putting $g = 1$ in the given relation and using $\phi(1) = 1$ gives us $ab = cd$ and so $c^{-1}a = db^{-1}$. But $a\phi(g)b = c\phi(g)d$ leads to

$$c^{-1}a\phi(g) = \phi(g)db^{-1} = \phi(g)c^{-1}a$$

for all $g \in G$. By our hypothesis we obtain $c^{-1}a = 1$ and so $a = c$. This immediately implies that $b = d$ and so the lemma is proved.

LEMMA 3. *Suppose that G is generated by its elements of order 2 and that the centralizer of $\phi(G)$ in H is (1). Then there exists a homomorphism $\lambda: G \rightarrow H$ such that for all $a, b \in G$, $\phi(aba^{-1}) = \lambda(a)\phi(b)\lambda(a)^{-1}$.*

Proof. Let $a \in G$; since G is generated by its elements of order 2, $a = u_1 u_2 \ldots u_n$ where each $u_i^2 = 1$. Therefore

$$\phi(aba^{-1}) = (u_1 u_2 \ldots u_n b u_n u_{n-1} \ldots u_1) = \phi(u_1) \ldots \phi(u_n)\phi(b)\phi(u_n) \ldots \phi(u_1)$$

for all $b \in$ G. By Lemma 2, this element $\phi(u_1) \ldots \phi(u_n)$ is unique and it is determined by *any* factorization of a as a product of elements of order 2. Define $\lambda(a)$ as $\phi(u_1) \ldots \phi(u_n)$.

It is clear from its construction that $\phi(aba^{-1}) = \lambda(a)\phi(b)\lambda(a)^{-1}$ for all $a, b \in G$. We now show that λ is indeed a homomorphism of G into H. For $a, c \in G$ we have that for all $b \in G$, $\phi((ac)b(ac)^{-1}) = \lambda(ac)\phi(b)\lambda(ac)^{-1}$. But $\phi(acb(ac)^{-1}) = \phi(acbc^{-1}a^{-1}) = \lambda(a)\phi(cbc^{-1})\lambda(a)^{-1} = \lambda(a)\lambda(c)\phi(b)\lambda(c)^{-1}\lambda(a)^{-1}$. Invoking Lemma 2 for the comparison of these calculations yields

$$\lambda(ac) = \lambda(a)\lambda(c)$$

as desired.

We now want to limit somewhat further the groups whose semi-homomorphisms will be considered. Let G, H, ϕ have the same meaning as earlier in the paper. We further insist that:

(1) the centralizer of $\phi(G)$ in H is (1),

(2) G is generated by its elements of order 2,

(3) G is generated by its squares; that is, given $g \in G$, then $g = a_1^2 \ldots a_n^2$ for $a_i \in G$.

Clearly any simple group satisfies (3): moreover, any simple group having an element of order 2 satisfies (2). If H is simple and $\phi(G)$ is thick enough in H to generate H, then (1) is satisfied. In particular, if G is a simple group having an element of order 2 and ϕ is a semi-homomorphism of G onto H, where H is simple, then all our conditions will be satisfied.

We *assume throughout the rest of this paper that our* G, H, *and* ϕ *satisfy the properties* (1), (2), *and* (3).

LEMMA 4. *There exist a homomorphism* g *and an anti-homomorphism* f *of* G *into* H *such that, given* $a \in G$, *then for all* $x \in G$ $\phi(xa) = f(a)\phi(x)g(a)$. *Consequently, for all* $a \in G$ $\phi(a) = f(a)g(a)$.

Proof. Let $a, x \in G$; thus $\phi(axa) = \phi(a)\phi(x)\phi(a)$. However, by Lemma 3, $\phi(axa) = \phi(axa^2a^{-1}) = \lambda(a)\phi(xa^2)\lambda(a)^{-1}$. The net outcome of this is that $\phi(xa^2) = \lambda(a)^{-1}\phi(a)\phi(x)\phi(a)\lambda(a)$ for all $x \in G$.

Let $y \in G$; since G is generated by its squares, $y = a_1^2 \ldots a_n^2$. Thus, for any $x \in G$, $\phi(xy) = \phi(xa_1^2 \ldots a_n^2)$. By what was done above we get that

$$\begin{aligned}\phi(xy) &= \lambda(a_n)^{-1}\phi(a_n)\phi(xa_1^2 \ldots a_{n-1}^2)\phi(a_n)\lambda(a_n) = \ldots \\ &= \lambda(a_n)^{-1}\phi(a_n)\lambda(a_{n-1})^{-1}\phi(a_{n-1}) \ldots \lambda(a_1)^{-1}\phi(a_1)\phi(x)\phi(a_1)\lambda(a_1) \\ &\qquad \times \ldots \phi(a_n)\lambda(a_n).\end{aligned}$$

Let us denote $\lambda(a_n)^{-1} \ldots \lambda(a_1)^{-1}\phi(a_1)$ by $f(y)$ and $\phi(a_1)\lambda(a_1) \ldots \phi(a_n)\lambda(a_n)$ by $g(y)$. These have been determined by a representation of y as a product of squares. However, by Lemma 2 these elements are *unique* (and so are independent of the particular factorization of y as a product of squares) and so define functions f and g from G to H. As we see by inspection,

$$\phi(xy) = f(y)\phi(x)g(y)$$

for all $x, y \in G$. Putting $x = 1$ we see that $\phi(y) = f(y)g(y)$.

To finish the proof we must still show that f is an anti-homomorphism and g a homomorphism of G into H. Now $\phi(x(yz)) = f(yz)\phi(x)g(yz)$ by the properties of f and g. On the other hand,

$$\phi(x(yz)) = \phi((xy)z) = f(z)\phi(xy)g(z) = f(z)f(y)\phi(x)g(y)g(z)$$

for all $x, y, z \in G$. Comparing these two evaluations of $\phi(xyz)$ and invoking Lemma 2 gives us that $f(yz) = f(z)f(y)$ and $g(yz) = g(y)g(z)$ as required.

COROLLARY 1. *For* $a \in G$, $f(a)g(a) = g(a)f(a)$.

Proof. Since ϕ is a semi-homomorphism, $\phi(a^{-1}) = \phi(a)^{-1}$; consequently $f(a^{-1})g(a^{-1}) = (f(a)g(a))^{-1}$. Since $f(a^{-1}) = f(a)^{-1}$ and $g(a^{-1}) = g(a)^{-1}$ we immediately deduce from this that $f(a)g(a) = g(a)f(a)$.

COROLLARY 2. *For* $a \in G$, $g(a) = \lambda(a)f(a) = f(a)\lambda(a)$.

Proof. In the course of proving Lemma 4 we established that

$$\phi(xa^2) = \lambda(a)^{-1}\phi(a)g(x)\phi(a)\lambda(a).$$

By the definitions of f and g we then have that

$$g(a^2) = \phi(a)\lambda(a) = f(a)g(a)\lambda(a) = g(a)f(a)\lambda(a)$$

(using Corollary 1 above). But $g(a^2) = g(a)^2$; hence we get $g(a) = f(a)\lambda(a)$. Since $f(a)$ commutes wth $g(a)$, it follows that it must also commute with $\lambda(a)$, thereby yielding the corollary.

LEMMA 5. *For all $a, b \in G$, $f(a)g(b) = g(b)f(a)$.*

Proof. By Corollary 2 to Lemma 4, $g(ab) = \lambda(ab)f(ab)$ and $g(a) = \lambda(a)f(a)$. Now $g(ab) = g(a)g(b) = \lambda(a)f(a)g(b)$; hence $\lambda(ab)f(ab) = \lambda(a)f(a)g(b)$. However, by Lemma 3, λ is a homomorphism and, by Lemma 4, f is an anti-homomorphism of G. Therefore $\lambda(ab)f(ab) = \lambda(a)\lambda(b)f(b)f(a)$. Thus we see that $\lambda(a)\lambda(b)f(b)f(a) = \lambda(a)f(a)g(b)$, and so $\lambda(b)f(b)f(a) = f(a)g(b)$. Making use of the fact that $\lambda(b)f(b) = g(b)$, we obtain $g(b)f(a) = f(a)g(b)$ as desired.

LEMMA 6. $f(G) \cap g(G) = 1$.

Proof. Let $u \in f(G) \cap g(G)$. Being of the form $g(b)$ for some $b \in G$, u must centralize all of $f(G)$. (Lemma 5); being of the form $f(a)$ for some $a \in G$, u must centralize all of $g(G)$. Hence u centralizes $f(G)g(G)$. However, for any $x \in G$, $\phi(x) = f(x)g(x) \in f(G)g(G)$, whence u centralizes all $\phi(x)$'s. By our basic hypothesis u must therefore be 1.

The lemmas obtained contain the essential information from which we obtain the principal results of this paper. We begin with

THEOREM 1. *Let G be a simple group having an element of order 2 and let ϕ be a semi-homomorphism of G into $H \neq (1)$ so that the centralizer of $\phi(G)$ in H is (1). Then ϕ is a one-to-one mapping.*

Proof. As we pointed out earlier, as a simple group with an element of order 2 G satisfies our conditions (2) and (3) so that all the lemmas proved pertain to the situation at hand.

Suppose that for $x, y \in G$ $\phi(x) = \phi(y)$. Therefore $f(x)g(x) = f(y)g(y)$ and so $f(y^{-1})f(x) = g(y)g(x^{-1})$, which is to say that $f(xy^{-1}) = g(yx^{-1})$. This implies that $f(xy^{-1}) \in f(G) \cap g(G) = (1)$; in short $f(xy^{-1}) = 1$. Consequently $g(yx^{-1}) = 1$. Since G is simple and f is an anti-homomorphism of G, if $x \neq y$, then $\operatorname{Ker} f \neq (1)$ so $\operatorname{Ker} f = G$ is forced. Hence $f(a) = 1$ for all $a \in G$. Similarly, if $x \neq y$, then $\operatorname{Ker} g \neq (1)$; hence $\operatorname{Ker} g = G$ and so $g(a) = 1$ for all $a \in G$. But then $\phi(a) = f(a)g(a) = 1$ for all $a \in G$. Since $H \neq (1)$ and the centralizer of $\phi(G)$ in H is (1), which is simply not possible. We therefore conclude that $x = y$ and so ϕ is one-to-one.

One should point out that the conditions in Theorem 1 are not enough to force the conclusion that ϕ is an isomorphism or anti-isomorphism. The simplest counter-example—G simple, $H = G \times G$, $\phi(a) = (a^{-1}, a)$—shows this to be the case. The hypothesis of the next few results is to preclude the presence of the phenomenon of this example.

THEOREM 2. *Let G be a group generated by its elements of order 2 and also by its squares, and let H be a simple group. Suppose that ϕ is a semi-homomorphism of G into H such that $\phi(G)$ generates H. Then ϕ is either a homomorphism or an anti-homomorphism of G onto H.*

Proof. Since f is an anti-homomorphism of G into H, $f(G)$ is a subgroup of H. We claim that it is normal in H. To see this note that, for $x \in G$, $\phi(x)f(G)\phi(x)^{-1} = f(x)g(x)f(G)g(x)^{-1}f(x)^{-1}$. However, $g(x)$ centralizes $f(G)$; hence $\phi(x)f(G)\phi(x)^{-1} = f(x)f(G)f(x)^{-1} = f(G)$. Since $\phi(G)$ is contained in the normalizer of $f(G)$ and $\phi(G)$ generates H, we have that $f(G)$ is normal in H. Similarly $g(G)$ is normal in H. But $f(G) \cap g(G) = (1)$; hence, by the simplicity of H, either $f(G) = (1)$ or $g(G) = (1)$. If $f(G) = (1)$, then $\phi(x) = f(x)g(x) = g(x)$ for all $x \in G$, whence ϕ would be a homomorphism of G; if $g(G) = (1)$, then ϕ would be an anti-homomorphism of G. Because $\phi(G)$ generates H and $\phi(G) = g(G)$ or $\phi(G) = f(G)$ respectively, we see that ϕ is indeed onto.

COROLLARY 1. *If G is a simple group having an element of order 2 and if H is simple, then any semi-homomorphism ϕ of G into H such that $\phi(G)$ generates H is an isomorphism or anti-isomorphism of G onto H.*

COROLLARY 2. *If G is simple having an element of order 2, then any semi-homomorphism ϕ of G into G such that $\phi(G)$ generates G is an automorphism or anti-automorphism of G.*

COROLLARY 3. *If G is a simple group having an element of order 2, then any semi-automorphism of G is either an automorphism or anti-automorphism of G.*

If one checks the proofs given one sees that we have actually proved a slightly stronger result than that stated in Theorem 2, namely

THEOREM 3. *Let G be a group which is generated by its elements of order 2 and also by its squares and suppose that ϕ is a semi-homomorphism of G into H such that:*

(1) *the centralizer of $\phi(G)$ in H is (1).*

(2) *$\phi(G) \not\subset A \times B$ where A, B are non-trivial subgroups invariant under conjugation by the elements of $\phi(G)$.*

Then ϕ is either a homomorphism or an anti-homomorphism of G.

REFERENCES

1. Walter Feit and John Thompson, *Solvability of groups of odd order*, Pacific J. Math., *13* (1963), 775–1029.

2. I. N. Herstein and M. F. Ruchte, *Semi-automorphisms of groups*, Proc. Amer. Math. Soc., *9* (1958), 145–150.

University of Chicago,
Chicago, Ill.