A SIMPLIFIED SET OF POSTULATES FOR
A GROUP*

BY R. M. FOSTER

Let there be given a class of elements $(a, b, c, \cdots)$ denoted by G, and an operation by which any two ordered elements determine a unique result which may or may not be an element of the class G. For convenience, this operation may be called multiplication, and the result determined by a and b called the product and written ab. It is the purpose of the present note to show that this system then forms a group if it satisfies the following set of three postulates:

I. *If a, b, c, ab, bc, $(ab)c$, and $a(bc)$ are all elements of G, then $(ab)c = a(bc)$.*

II. *If a and b are elements of G, there exists an element x of G such that $ax = b$.*

III′. *There exists an element g of G with the property that, if b is an element of G, there exists an element y of G such that $yg = b$.*

It has been shown by Garver† that a finite group may be defined by these three postulates together with a fourth:

IV. *The number of elements of G is finite.*

To define a general group, however, Garver in an earlier paper‡ had required a set of three postulates consisting of I, II, and a stronger form of III′, namely,

III. *If a and b are elements of G, there exists an element y of G such that $ya = b$.*

Whereas Garver showed that in defining a finite group by the four postulates I, II, III, and IV, a part of III is redundant and that a considerable simplification can be effected upon re-

---

placing III by III′, it is shown in the present note that the same simplification can be effected in the set of postulates for a general group—that Garver's simplification is not essentially limited to the special case of finite groups. In other words, postulates I, II, and III′ suffice to define a group; and thus, without any revision, I, II, III′, and IV define a finite group.

The method of proof consists in establishing the existence of an identity element, and then of an inverse for each element; thereupon it is shown that the system has the closure property (if a and b are elements of G, then ab is an element of G). It is convenient to arrange the first part of this proof as the deduction of the three following lemmas.

LEMMA 1. *There exists an element e of G such that $ea = a$ for every element a of G.*

By III′ there exist elements g and e of G such that $eg = g$. If a is an element of G, then, by II, there exist elements m and n of G such that $em = a$ and $gn = m$. Thus $m = gn = (eg)n$, and $a = em = e(gn)$. Hence by I, $m = a$; and upon substituting in $em = a$, we have $ea = a$ for every element a.

LEMMA 2. *If e is the element of G having the property of Lemma 1, then $ae = a$ for every element a of G.*

By III′ there exists an element p of G such that $pg = e$. If a is an element of G, then, by II, there exist elements q, r, and s of G such that $aq = a$, $pr = q$, and $gs = r$. By Lemma 1, $s = es$. Thus $s = (pg)s$, and $q = pr = p(gs)$. Hence by I, $s = q$, and upon substituting in $gs = r$, we have $gq = r$.

By III′ there exists an element t of G such that $tg = a$. By II, there exist elements u and v of G such that $tu = e$ and $uv = g$. By Lemma 1, $v = ev$. Thus $v = (tu)v$, and $a = tg = t(uv)$. Hence, by I, $v = a$; and upon substituting in $uv = g$, we have $ua = g$.

We now have $r = gq = (ua)q$, and $g = ua = u(aq)$. Hence by I, $r = g$, and thus $gq = g$.

By Lemma 1, $q = eq$. Thus $q = (pg)q$, and $e = pg = p(gq)$. Hence by I, $q = e$, and upon substituting in $aq = a$, we have $ae = a$ for every element a of G.

LEMMA 3. *If e is the element of G having the properties of Lemmas 1 and 2, and if a is an element of G, there exists an element a^{-1} of G such that $aa^{-1} = a^{-1}a = e$.*

By II there exist elements a^{-1} and w of G such that $aa^{-1} = e$ and $a^{-1}w = e$. By Lemma 1, $w = ew$; and by Lemma 2, $a = ae$. Thus $w = (aa^{-1})w$, and $a = a(a^{-1}w)$. Hence by I, $w = a$, and, upon substituting in $a^{-1}w = e$, we have $a^{-1}a = e$.

We are now in a position to establish the following closure property.

V. *If a and b are elements of G, there exists an element z of G such that $ab = z$.*

By II and the lemmas, there exist elements e, a^{-1}, z, and k such that $aa^{-1} = e$, $a^{-1}z = b$, and $ak = z$. Then by Lemma 1, $k = ek$; and by Lemma 3, $e = a^{-1}a$. Thus $k = (a^{-1}a)k$, and $b = a^{-1}z = a^{-1}(ak)$. Hence by I, $k = b$, and upon substituting in $ak = z$, we have $ab = z$, thus establishing the closure property.

The proof of III then follows by a familiar derivation from closure and the lemmas established above. Since I, II, and III define a group, as shown by Garver in his 1934 paper, it thus follows that I, II, and III' define a group.

It is ordinarily assumed that multiplication is unique, and this assumption is not made one of the explicit postulates. For some purposes it might be better to incorporate uniqueness as one of the postulates of the set; in this case certain modifications would be desirable in the statement of the associative law. This procedure was followed by Baer and Levi* in a comprehensive study of group postulates. Their paper also gives an answer to the question raised by Garver at the end of his 1936 paper, showing by means of an example that it is not possible to define a commutative group by means of postulates I and II and the weak form of the commutative law (if a, b, ab, and ba are all elements of G, then $ab = ba$).

BELL TELEPHONE LABORATORIES

---

* Reinhold Baer and Friedrich Levi, *Vollständige irreduzibele Systeme von Gruppenaxiomen*, Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Mathematisch-naturwissenschaftliche Klasse, Beitrag zur Algebra, Nr. 18 (1932), pp. 3–12.