Contribution to the definition of group.

By TIBOR FARAGÓ in Budapest.

Consider the usual four group axioms I—IV, which ensure a set G to be a group:

I. There is a single valued binary operation (called multiplication) defined in G, which associates with each pair of elements a, b of G an element ab of G.

II. G contains a left unit element, i. e. an element e such that $ea=a$ for every element a of G.

III. For each element a of G there exists a left inverse element, i. e. an element a^{-1} such that $a^{-1}a=e$.

IV. The multiplication is associative, i. e. if a, b, c are arbitrary elements of G, then $(ab)c=a(bc)$ holds.

It is well-known that each of the axioms I—IV is independent of the other three. In particular IV is no consequence of I—III. In what follows, we investigate the question what sort of systems arise if axiom IV is replaced by some different but analogous postulate. More exactly, we consider all possible conditions which can be obtained by permutation of the elements and by another distribution of the parentheses occurring in the associative law. In such a way we get the following 15 possibilities disregarding the associative law itself:

1. $(ab)c=a(cb)$;	6. $a(bc)=a(cb)$;	11. $(ab)c=(ac)b$;
2. $(ab)c=b(ac)$;	7. $a(bc)=b(ac)$;	12. $(ab)c=(ba)c$;
3. $(ab)c=b(ca)$;	8. $a(bc)=b(ca)$;	13. $(ab)c=(bc)a$;
4. $(ab)c=c(ab)$;	9. $a(bc)=c(ab)$;	14. $(ab)c=(ca)b$;
5. $(ab)c=c(ba)$;	10. $a(bc)=c(ba)$;	15. $(ab)c=(cb)a$.

We shall prove the following

Theorem. *If we replace the associative law by one of the above* 15 *requirements* (*while the axioms* I—III *retain their validity*), *then the resulting system will be* *a commutative group in the cases* 1., 2., 3., 8., 9., 10., 11., 13., 14.;

a commutative system not necessarily a group in the cases 4., 5., 6.,

and finally a system neither commutative nor associative in the cases 7., 12., 15.

In case 15. *the system is a quasigroup.*

We see that in most cases the above modification of the associative law leads to a group which is moreover commutative.

Proof. We start with the following remark:

If one of the above 15 requirements (e. g. 4., 5., 6., 12.) can be derived from the commutative law, then the corresponding system is not a group in general.

In fact, the system $S=\{e, u, v\}$ with the multiplication table

	e	u	v
e	e	u	v
u	u	e	v
v	v	v	e

satisfies axioms I—III and the commutative law, without being associative (i. e. a group).

Now we are going to investigate each of the 15 cases mentioned above separately.

1. $(ab)c=a(cb)$.

Putting $a=e$ we have $bc=cb$. Therefore the system is commutative and moreover associative, since, by 1. and the commutativity

$$(ab)c=a(cb)=a(bc).$$

2. $(ab)c=b(ac)$.

Putting $a=b^{-1}, c=b$ we have $(b^{-1}b)b=b(b^{-1}b)$, $b=be$. Thus it follows from 2. with $c=e$ that

$$ab=ba.$$

Hence the system is commutative, and so the associativity is a consequence of 2.:

$$(ab)c=(ba)c=a(bc).$$

3. $(ab)c=b(ca)$.

Putting $a=b=e$ we have $c=ce$. Hence from 3. with $c=e$ we infer again $ab=ba$. Therefore the system is commutative and associative:

$$(ab)c=(ba)c=a(cb)=a(bc).$$

4. $(ab)c = c(ab)$.

This equation is a consequence of the commutative law; thus, by the above remark, the system is not necessarily a group. However, it is commutative, since (in the case $a = e$) 4. implies $bc = cb$.

5. $(ab)c = c(ba)$.

Also this is a consequence of the commutative law, and so, as the above example S shows, the system is not necessarily a group. Nevertheless it is commutative, for in the case $a = b = e$ we have $c = ce$ and thus (with $c = e$) $ab = ba$.

6. $a(bc) = a(cb)$.

Since this is a consequence of the commutative law, the system is not necessarily a group. But it is commutative (put $a = e$).

7. $a(bc) = b(ac)$.

The system is neither commutative nor associative in general, as the following example shows:

	e	u
e	e	u
u	e	e

8. $a(bc) = b(ca)$.

Putting $b = e$ we have $ac = ca$. Hence the system is commutative. Consequently

$$a(bc) = a(cb) = c(ba) = c(ab) = (ab)c,$$

i. e., the system is a commutative group.

9. $a(bc) = c(ab)$.

Putting $a = e$ we have $bc = cb$, i. e., the system is a commutative group since

$$a(bc) = c(ab) = (ab)c.$$

10. $a(bc) = c(ba)$.

Putting $b = e$ we have $ac = ca$, i. e. the system is a commutative group, since

$$a(bc) = c(ba) = (ba)c = (ab)c.$$

11. $(ab)c = (ac)b$.

Putting $a = e$ we have $bc = cb$ i. e. the system is a commutative group since

$$(ab)c = (ba)c = (bc)a = a(bc).$$

12. $(ab)c = (ba)c$.

This is a consequence of the commutative law, i. e., the system is not necessarily a group. Moreover it is not necessarily commutative, as the following example shows:

	e	u	v
e	e	u	v
u	u	e	e
v	u	e	e

13. $(ab)c=(bc)a$.

Putting $a=b=e$ we get $c=ce$. Hence (with $c=e$)

$$ab=ba.$$

Thus the system is a commutative group since

$$(ab)c=(bc)a=a(bc).$$

14. $(ab)c=(ca)b$.

Putting $a=c=e$ we get $be=b$. Hence (with $b=e$)

$$ac=ca,$$

i. e., the system is a commutative group since

$$(ab)c=(ba)c=(cb)a=a(cb)=a(bc).$$

15. $(ab)c=(cb)a$.

The system is neither commutative nor associative in general as the following example shows:

	e	u	v
e	e	u	v
u	v	e	u
v	u	v	e

We can prove, however, that such a system is a quasigroup, i. e., the equations $xa=b, ay=b$ have always a unique solution x resp. y. First we show that for each element b of the system $bb^{-1}=e$ holds. In fact, putting $a=e$ and $c=b^{-1}$ in $(ab)c=(cb)a$ we get

$$bb^{-1}=(b^{-1}b)e=ee=e.$$

Now we state that $x=ba^{-1}$ is a solution of the equation $xa=b$. Indeed, by 15., we have

$$xa=(ba^{-1})a=(aa^{-1})b=eb=b.$$

On the other hand, $y=(be)a^{-1}$ is a solution of $ay=b$. As a matter of fact,

$y=(be)a^{-1}$ satisfies the equation

$$(1) \qquad (ay)e=be,$$

for (making use repeatedly of 15.) we obtain

$$(ay)e=(ey)a=ya=((be)a^{-1})a=(aa^{-1})be=e(be)=be.$$

Now, it follows from (1) by multiplication with e on the right:

$$((ay)e)e=(be)e,$$
$$(ee)ay=(ee)b,$$
$$ay=b.$$

The solution of $xa=b$ resp. $ay=b$ is uniquely determined by the elements a, b since $xa=x'a$ implies

$$(xa)a^{-1}=(x'a)a^{-1}, \quad (a^{-1}a)x=(a^{-1}a)x', \quad ex=ex', \quad x=x'.$$

Furthermore $ay=ay'$ implies

$$(ay)e=(ay')e, \quad (ey)a=(ey')a, \quad ya=y'a,$$

i. e., (as before) $y=y'$. Thus we have completed the proof of our theorem.

Remarks. It is easy to show that if we drop axioms II and III, none of the above 15 requirements implies the associativity of the resulting system. — It is worth while to note that in the cases 4., 5., 6., the left unit element of the system under consideration is at the same time a right unit element too. This follows from the fact that in these cases the system is necessarily commutative. A similar statement does not hold in the cases 7., 12., 15. as the above examples illustrate. — In cases 4., 5., 6., 12., 15. any left inverse of an arbitrary element of the system is at the same time a right inverse. (The above example shows that this is not true in the case 7.) The validity of this statement follows in the cases 4., 5., 6. from the commutativity of the system, and in the case 15. from the proof given above. In the case 12. one proceeds as follows. Obviously it is sufficient to show that the system contains only one left unit element, since then 12. implies $c=ec=(a^{-1}a)c=(aa^{-1})c$ for arbitrary elements a, c of the system, i. e., $aa^{-1}=e$. Now let e and e' be left unit elements in our system and let d be a left inverse of e' relative to e, i. e., $de'=e$. Then we have by 12:

$$e'=ee'=(de')e'=(e'd)e'=de'=e.$$

Remark (added October 14, 1953). That the modification 8. and 13. of the assiciative law implies the commutativity of the groups is stated in the paper: RAFAEL SÁNCHEZ—DIAZ, Definitions of group involving quasi-inverse elements, *Proc. Amer. Math. Soc.*, **4** (1953), 424—428.

(*Received April 16, 1953.*)