

Groups and size (revised)

In what follows, x and y are of type “element of G ”.

Given a finite group G with an automorphism f satisfying:

$$(0) \quad f.x = \sim x \quad , \quad \text{where } \sim \text{ is the inverse operation } \quad ,$$

for more than three-fourths of the elements of G . Show that f satisfies (0) for all elements of G , and that G is commutative.

In this note I present a design of a solution to this problem. I think it is quite nice, and easy to reconstruct by heart. It is not completely naive in that it uses more than just the bare axioms of group theory, but it is simple nonetheless.

* *

 *

The crux of this problem is the given about size. We are not given a name for the measured quantity, but it doesn't hurt us to provide such a name, and it may help tremendously to do so. Thus we define set S by:

$$(1) \quad x \in S \quad \equiv \quad f.x = \sim x \quad ,$$

so that our given about size can be written:

$$(2) \quad \#S > \frac{3}{4}.\#G \quad , \quad \text{where } \# \text{ is the size function } \quad ,$$

and so that our demonstrandum relating to S can be written:

$$(3) \quad S = G \quad .$$

So far so good: notice how naming has allowed us to compactly and clearly represent our givens and demonstrandum. We do not yet formalize the demonstrandum about commutativity, by the principle of “First things first.” We will deal with commutativity once we have more fully explored the notion of size.

Now, in order to use (2), we need some idea of how we can use information about size in the context of finite groups. The only relevant property I know of is Lagrange's theorem:

$$(4) \quad H \preceq K \quad \Rightarrow \quad \#H \sqsubseteq \#K \quad , \quad \text{for all } H \text{ and } K \quad ,$$

where \preceq is the subgroup relation, and \sqsubseteq is “divides”. Our hand is slightly forced in using Lagrange's theorem, as the only group mentioned in the problem is G . Hence we use (4) in the form:

$$(5) \quad H \preceq G \quad \Rightarrow \quad \#H \sqsubseteq \#G \quad , \quad \text{for all } H \quad .$$

JAW37a-1

Next we consider potential instantiations for H . Since the only size we know anything about is $\#S$, the obvious instantiation is $H := S$. Thus we calculate:

$$\begin{aligned}
 & S \preceq G \\
 \equiv & \{ (5) \text{ with } H := S \} \\
 & S \preceq G \quad \wedge \quad \#S \subseteq \#G \\
 \equiv & \{ (2), \text{ ie } \#S > \frac{3}{4} \cdot \#G, \text{ and arithmetic} \} \\
 & S \preceq G \quad \wedge \quad \#S = \#G \\
 \equiv & \{ \#G \text{ is finite} \} \\
 & S = G \quad ,
 \end{aligned}$$

which is (3), one half of our demonstrandum. The essence of this calculation is:

$$(6) \quad H \preceq G \quad \wedge \quad \#H > \frac{1}{2} \cdot \#G \quad \Rightarrow \quad H = G \quad ,$$

so we see that the condition (2) on the size of S more than suffices.

So far so very good: We have shown that (3) equivaless $S \preceq G$, so our focus now turns to investigating whether S is a subgroup of G . To do this, we have to check S for closure under \sim , and for closure under the group operation \bullet .

As for closure under \sim , we calculate:

$$\begin{aligned}
 & \sim x \in S \\
 \equiv & \{ (1) \} \\
 & f.(\sim x) = \sim \sim x \\
 \equiv & \{ \text{morphism property} \} \\
 & \sim f.x = \sim \sim x \\
 \equiv & \{ \text{algebra} \} \\
 & f.x = \sim x \\
 \equiv & \{ (1) \} \\
 & x \in S \quad .
 \end{aligned}$$

That is, we have shown $x \in S \equiv \sim x \in S$ for all x , and so we are done.

As for closure under \bullet , we calculate:

$$\begin{aligned}
 & x \bullet y \in S \\
 \equiv & \{ (1) \} \\
 & f.(x \bullet y) = \sim(x \bullet y)
 \end{aligned}$$

$$\begin{aligned}
&\equiv \{ \text{morphism property} \} \\
&\quad f.x \bullet f.y = \sim(x \bullet y) \\
&\equiv \{ \text{assuming } x, y \in S \} \\
&\quad \sim x \bullet \sim y = \sim(x \bullet y) \\
&\equiv \{ \text{a few steps of algebra} \} \\
&\quad x \bullet y = y \bullet x \quad .
\end{aligned}$$

Well! We did not manage to prove closure under \bullet , but we did manage to prove an interesting equivalence for the elements of S , which we state explicitly:

$$(7) \quad x, y \in S \quad \Rightarrow \quad (x \bullet y \in S \quad \equiv \quad x \bullet y = y \bullet x) \quad .$$

Formula (7) is the crux of our design. First of all, one half of our demonstrandum is about commutativity, and finally commutativity has entered the picture via the expression $x \bullet y = y \bullet x$. In fact, observe that if we succeed in proving closure of S under \bullet , then from (7) we may conclude that S is commutative. But also recall that proving closure of S under \bullet proves $S = G$, so we may conclude that G is commutative, as desired. Thus we see that commutativity is not a separate proof obligation at all, but a consequence of the proof obligation we are currently investigating.

More importantly, formula (7) represents a crucial mathematical interface between size and grouphood. Recall that in order to use (6), we need a subgroup of G of at least a certain size. While S is useful for reasoning about size, it is no good yet as a candidate for a subgroup. Formula (7) relates S to commutativity, which is no good for reasoning about size, but *does* bring groups into the picture for free, via so-called centralizer groups. The centralizer group C_x is defined by

$$(8) \quad y \in C_x \quad \equiv \quad x \bullet y = y \bullet x \quad .$$

(The reader may check that C_x is indeed a subgroup of G .) With all this in mind, we can envision the proof shape of S 's closure under \bullet :

$$\begin{aligned}
&x \bullet y \in S \\
&\equiv \{ (7), \text{ assuming } x, y \in S \} \\
&\quad x \bullet y = y \bullet x \\
&\equiv \{ (8) \} \\
&\quad y \in C_x \\
&\equiv \{ \text{assuming } C_x = G, \text{ for } x \in S \text{ (see below)} \} \\
&\quad y \in G \\
&\equiv \{ \} \\
&\quad \text{true} \quad .
\end{aligned}$$

The final step is to prove $C_x = G$, where we assume $x \in S$ for the remainder. As planned, we accomplish this by showing $\#C_x > \frac{1}{2} \cdot \#G$. Also, as mentioned, we need to exploit (7) once more to bring S back into the picture, since $\#S$ is the only size we know anything about. In preparation for the calculation, we convert (7) into set terminology:

$$\begin{aligned}
& y \in S \quad \Rightarrow \quad (x \bullet y \in S \quad \equiv \quad x \bullet y = y \bullet x) \\
& \equiv \quad \{ \text{algebra} \} \\
& y \in S \quad \Rightarrow \quad (y \in \sim x \bullet S \quad \equiv \quad y \in C_x) \\
& \equiv \quad \{ \text{predicate calculus} \} \\
& y \in S \quad \wedge \quad y \in \sim x \bullet S \quad \equiv \quad y \in S \quad \wedge \quad y \in C_x \\
& \equiv \quad \{ \text{set calculus} \} \\
& y \in (S \cap \sim x \bullet S) \quad \equiv \quad y \in (S \cap C_x) \quad ,
\end{aligned}$$

and thus we have:

$$(9) \quad S \cap \sim x \bullet S = S \cap C_x \quad .$$

Finally, we calculate:

$$\begin{aligned}
& \#C_x \\
& \geq \quad \{ \text{property of } \# \text{ , preparing to appeal to (9)} \} \\
& \#(S \cap C_x) \\
& = \quad \{ (9) \} \\
& \#(S \cap \sim x \bullet S) \\
& = \quad \{ \text{property of } \# \text{ , so as to extract } \#S \} \\
& \#S + \#(\sim x \bullet S) - \#(S \cup \sim x \bullet S) \\
& > \quad \{ \#S = \#(\sim x \bullet S) \text{ and (2) ; } S \cup (\sim x \bullet S) \subseteq G \} \\
& \frac{3}{4} \cdot \#G + \frac{3}{4} \cdot \#G - \#G \\
& = \quad \{ \text{arithmetic} \} \\
& \frac{1}{2} \cdot \#G \quad .
\end{aligned}$$

That concludes our proof. Note that nowhere did we use that f was an automorphism, just that it was a homomorphism. (The reader may prove that it is an automorphism, using $S = G$ and the defining property (0) of f .)

* * *

Thanks to Sandy Zabell for this problem, and Tom Verhoeff, who helped me design its solution. I consider this revision to be a pleasant improvement on the original.

Santa Cruz, 21 November 2006

Jeremy Weissmann
11260 Overland Ave. #21A
Culver City, CA 90230
USA
jeremy@mathmeth.com