

Groups and size

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 3/4ths 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 I think sufficiently 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 now be stated:

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

and our demonstrandum relating to S is

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

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

Now, in order to be able to use (2), we have to have some idea of how we can use information about size in the context of finite groups. The only 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”. Is it sensible to think we could use this? Well, the only group mentioned in the context of the problem is G , so that for a start, we would have to use (4) in the form:

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

In this form, it is clear that if (5) is our only means of using givens about size, then we have to have a subgroup H in mind in order to apply (2)! And what about $\#H$? Well, the only other size besides $\#G$ we are told anything about is $\#S$, but we do not know that S is a group, and so we cannot apply (5) with $H := S$. However, since $\#S$ is the only other size we know, it certainly pays to see what we could derive if S were a group, and so we calculate:

$$\begin{aligned}
 & S \preceq G \\
 \equiv & \{ (5) \text{ with } H := S \} \\
 & S \preceq G \quad \wedge \quad \#S \sqsubseteq \#G \\
 \equiv & \{ (2), \text{ ie } \#S > (3/4) * \#G \} \\
 & S \preceq G \quad \wedge \quad \#S = \#G \\
 \equiv & \{ \#G \text{ is finite} \} \\
 & S = G \quad .
 \end{aligned}$$

And this is (3), one half of our demonstrandum. In fact, from this last calculation we can extract the essence:

$$(6) \quad H \preceq G \quad \wedge \quad \#H > (1/2) * \#G \quad \Rightarrow \quad H = G \quad ,$$

so that the condition (2) on the size of S more than suffices —provided we can apply (5) —.

So far so very good. We have seen that our next investigation should be whether S is a subgroup of G . To do this, we have to check that S is closed under \sim , and that S is closed under the group operation \bullet .

For closure under \sim , we calculate:

$$\begin{aligned}
 & \sim x \in S \\
 \equiv & \{ (1) \} \\
 & f.(\sim x) = \sim \sim x \\
 \equiv & \{ \text{morphism property} \} \\
 & \sim f.x = \sim \sim x \\
 \equiv & \{ \text{assuming } x \in S, \text{ so that } f.x = \sim x \} \\
 & \sim \sim x = \sim \sim x \\
 \equiv & \{ \text{equality} \} \\
 & \mathbf{true} \quad .
 \end{aligned}$$

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

For closure under \bullet , we calculate:

$$\begin{aligned}
 & x \bullet y \in S \\
 \equiv & \{ (1) \} \\
 & f.(x \bullet y) = \sim(x \bullet y) \\
 \equiv & \{ \text{morphism property} \} \\
 & f.x \bullet f.y = \sim(x \bullet y) \\
 \equiv & \{ \text{assuming } x, y \in S \} \\
 & \sim x \bullet \sim y = \sim(x \bullet y) \\
 \equiv & \{ \text{a few steps of algebra} \} \\
 & x \bullet y = y \bullet x \quad .
 \end{aligned}$$

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:

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

Formula (7) is in fact so important at this stage of our design, we should stop and really explore what it means to us. First of all, one half of our demonstrandum is about commutativity, and finally commutativity has entered the picture via (7). In fact, we see that if we succeed in proving closure of S under \bullet , then by (7), S is commutative. But by (5) we will also have proved $S = G$, so that the commutativity of G comes for free. In other words, commutativity is not a separate proof obligation, but a consequence of the proof obligation we are currently investigating.

But formula (7), by relating closure to commutativity, tells us even more. The crux of our proof strategy, as expressed in (6), is to use Lagrange's theorem to show that a sufficiently large subgroup of G is in fact G . As we have seen, S is useful for calculations concerning size, thanks to (2), but is no good yet as a candidate for a subgroup. On the other hand, thanks to (7), commutativity has entered the picture, and while commutativity doesn't directly relate to size, it *does* bring groups into the picture for free, via so-called centralizer groups. (The centralizer group C_x is defined by

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

The reader may check that C_x is indeed a subgroup of G .)

So we can see now the overall shape of the proof of S 's closure under \bullet : Via (7), we relate closure to commutativity, and then bring in an as-yet undetermined centralizer group. Using Lagrange's theorem, we show that group to be G , but in order to measure the size of that group, we will have to use (7) again to relate it back to S , which is the only thing we can measure. This is a lovely shape, but let's see whether it is supported by the details:

S is closed under \bullet
 \equiv { definition of closed }
 $\langle \forall x, y : x, y \in S : x \bullet y \in S \rangle$
 \equiv { (7) }
 $\langle \forall x, y : x, y \in S : x \bullet y = y \bullet x \rangle$
 \equiv { introducing C_x via (8) }
 $\langle \forall x, y : x, y \in S : y \in C_x \rangle$
 \equiv { predicate calculus }
 $\langle \forall x : x \in S : \langle \forall y : y \in S : y \in C_x \rangle \rangle$
 \equiv { definition of \subseteq }
 $\langle \forall x : x \in S : S \subseteq C_x \rangle$
 \equiv { given our goal to apply Lagrange's theorem, assume $\langle \forall x : x \in S : C_x = G \rangle$ }
 $\langle \forall x : x \in S : S \subseteq G \rangle$
 \equiv { $S \subseteq G$, vacuous quantification over nonempty range }
true .

Well, that is terrific, if a little heavy on the semantically null steps —more on that in the Afterword—. The last remaining step is to prove $\langle \forall x : x \in S : C_x = G \rangle$, and we have already planned to do that by showing $\#C_x > (1/2) * \#G$ for all $x \in S$. Also, as we said before, to do this we will need to exploit (7) once more to bring S back into the picture, since $\#S$ is the only size we know anything about. For all $x \in S$, we have:

$\#C_x$
 $=$ { property of $\#$ }
 $\langle \#y :: y \in C_x \rangle$
 $=$ { (8) }
 $\langle \#y :: x \bullet y = y \bullet x \rangle$
 \geq { In order to apply (7) , we need the conjunct $y \in S$ in the range; this is all right, from the monotonicity of $\#$. }
 $\langle \#y : y \in S : x \bullet y = y \bullet x \rangle$
 $=$ { (7) }
 $\langle \#y : y \in S : x \bullet y \in S \rangle$
 $=$ { simplifying }
 $\langle \#y : y \in S : y \in (\sim x \bullet S) \rangle$

$$\begin{aligned}
&= \{ \text{property of } \# , \text{ so as to extract } \#S \} \\
&\quad \#S + \#(\sim x \bullet S) - \#(S \cup (\sim x \bullet S)) \\
&> \{ \#(\sim x \bullet S) = \#S \text{ and (2)} \} \\
&\quad (3/2) * \#G - \#(S \cup (\sim x \bullet S)) \\
&\geq \{ \} \\
&\quad (1/2) * \#G .
\end{aligned}$$

The last step is equivalent by algebra to:

$$\#(S \cup (\sim x \bullet S)) \leq \#G ,$$

which is of course **true** , since the set on the lefthand side is a subset of G . This calculation settles the entire proof. Again, very heavy on the semantically null steps, but quite straightforward.

Note that nowhere did we use that f was an automorphism, just that it was a homomorphism. (That it is an automorphism follows easily from $S = G$ and the defining property (0) of f .)

* *

 *

Afterword. As I hope the reader can see, the proof and its design are entirely straightforward, following only from the basic manipulative knowledge of group theory, and the calculational style in general. But what constitutes the difficulty and length of the above proofs? The answer is clear: it's the notation the proof is carried out in; the beauty and simplicity of the meat of the proof is obscured by meaningless shuntings which do nothing but put things into the appropriate forms to apply more manipulations.

I think (7) expresses the problem nicely. This crucial property —which we derived from trying to fulfil proof obligations, recall— told us that there was a symmetry in S between closure and commutativity. Both of these properties are expressed nicely as quantifications over two variables in S . But our next observation was to use centralizer groups, so we could have something to apply Lagrange's theorem to, and that destroyed the symmetry by forcing us to rewrite $x \bullet y = y \bullet x$ as the ugly $y \in C_x$. That shift to a single quantification later had to be undone, but as far as I can see, there's no way in the present notation to avoid it. (It wouldn't have helped to write

$$y \in C_x \wedge x \in C_y \quad ;$$

symmetry is not just redundant asymmetry!) So it was this problem with notation that contributed to the length of the main calculation, and the subcalculation of the size of C_x .

Naturally, suggestions on how things could be improved —without sacrificing detail of course!— are greatly welcomed.

JAW37-5

Thanks to Sandy Zabell for this problem, and Tom Verhoeff, who helped me design its solution.

Eindhoven, 14 September 2005

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