Math 417 Problem Set 3

Starred (*) problems are due Friday, September 14.

(*) 15. (Gallian, p.58, #51) Show that, if we had 'weakened' the definition of a group G to (1) there is an $e \in G$ with $ge = g$ for every $g \in G$, (2) inverses exist, and (3) the group operation is associative, then we can prove that $eg = g$ for every $g \in G$ (i.e, the other half of the definition of an identity automatically holds).

We want to show that, for any $g \in G$, we have $eg = g$. But by property (2), we know that g^{-1} exists, so we know that $gg^{-1} = g^{-1}g = e$. So then $eg = (gg^{-1})g = g(g^{-1}g) = ge = g$, where we used associativity (3) for the second equality and our modified property (1) for the fourth equality.

So we have shown that if (1),(2), and (3) are true, then $eg = g$ for every $g \in G$.

(*) 17. (Gallian, p.57, #39) If G is a group, and for every $a, b, c, d, x \in G$ we have $axb = cxd$ implies that $ab = cd$, show that then for every $u, v \in G$ we have $uv = vu$. ('A middle cancellation law implies commutativity.')

[Hint: Find an x so that $uxv = vxu$!]

Following the hint, we look for an $x \in G$ so that $uxv = vxu$. We only 'know' about the elements u and v, so we probably want to build x out of them. If we just try a few possibilities, $x = u$ doesn't seem to work ($u^2v = vu^2$? why should u^2 and v commute?), and neither does $x = v$ ($uv^2 = v^2u$ has the same problem). But trying $x = u^{-1}$, we get $uxv = uu^{-1}v = ev = v$, while $vxu = vu^{-1}u = ve = v$, so $uxv = vxu$ is actually true. [N.B.: $x = v^{-1}$ also works, as does $x = v^{-1}uv^{-1}$:

$$uxv = u(v^{-1}uv^{-1})v = uv^{-1}u(v^{-1}v) = uv^{-1}u = vv^{-1}(uv^{-1}u) = v(v^{-1}uv^{-1})u = vxu \ .$$

There are many others that also work!]

Having done this, we know that for any $u, v \in G$ there is an $x \in G$ so that $uxv = vxu$. So by our hypothesis we have that, for any $u, v \in G$, $uv = vu$. That is, G is abelian.

(*) 19. If G is a group and $a \in G$, and if $|a| < \infty$ and $\gcd(k, |a|) = 1$, show that then $|a^k| = |a|$.

There is more than one way to proceed with this problem; here are two.

Viewing $|a|$ as $|\{a\}|$, what we want to show is that $|\{a^k\}| = |\{a\}|$. But since $a^k \in \{a\}$, we know that $\{a^k\} \subseteq \{a\}$; $g \in \{a^k\}$ means that $g = (a^k)^s = a^{ks}$ for some $s \in \mathbb{Z}$, so $g \in \{a\}$. Therefore, $|a^k| = |\{a^k\}| \leq |\{a\}| = |a|$ (a subset has fewer elements!).

To establish the opposite inequality ($|a|leq|a^k|$), based on what we just showed, it is enough to show that $a \in \{a^k\}$, since then $\{a\} \subseteq \{a^k\}$.

We need our hypothesis, $\gcd(k, |a|) = 1$, in order to show this. This hypothesis tells us that we can write $1 = rk + s|a|$ for some integers r, s. Therefore, $a = a^1 = a^{rk+s|a|} = a^{rk}a^{s|a|} = (a^k)^r(a^{|a|})^s$. But! $a^{|a|} = e$ (from class; $|a| < \infty$ implies that this is true). So: $a = (a^k)^s \in \{a^k\}$, as desired. This gives $|a| \leq |a^k|$, and so together with $|a^k| \leq |a|$ we get $|a^k| = |a|$.

If we view, instead, $|a|$ as the smallest $n \in \mathbb{N}$ with $a^n = e$, then we know that $(a^k)^{|a|} = a^{k|a|} = (a^{|a|})^k = e^k = e$, and so $|a^k|$, the smallest n with $(a^k)^n = e$, must be at most $|a|$, and so $|a^k| \le |a|$.

To get the opposite inequality, set $|a^k| = m$ (for notational convenience); what we want to show is that $a^m = e$ (so that $|a| \le m = |a^k|$). Again, we need to use our hypothesis that $\gcd(k, |a|) = 1$ in order to do this. And, again, we use that $1 = rk + s|a|$ for some integers r and s. Then:

$a^m = (a^1)^m = (a^{rk+s|a|})^m = a^{m(rk+s|a|)} = a^{mrk+ms|a|} = a^{mrk}a^{ms|a|} = ((a^k)^m)^r(a^{|a|})^{ms} = e^r e^{ms} = ee = e$,

since $m = |a^k|$ so $(a^k)^m = e$, and $a^{|a|} = e$. So $a^m = e$, so $|a^k| = m \le |a|$.

Putting together $|a^k| \le |a|$ and $|a| \le |a^k|$, we get $|a^k| = |a|$.

A selection of further solutions

14. Give an <u>example</u> of a group G and $a, b \in G$ so that $(ab)^4 = a^4b^4$, but $ab \ne ba$.

[Hint: Problem #11 might help? Slightly bigger challenge: try the same thing with the 4's replaced by 3's !]

The cheapest way to arrange this is to (first) try making $(ab)^4 = e = a^4 = b^4$, that is, find elements a and b with order (dividing) 4 whose product ab also has order (dividing) 4, and then check to see if $ab = ba$. Problem #11 suggests a way to do this: try $a = F(\theta)$ and $b = F(\psi)$ with ab <u>not</u> equal to $R(\pi)$ (which, we can note, has order 2), but (rather) having order 4. Note that in this case $a^2 = b^2 = e = R(0)$, and so $a^4 = b^4 = e^2 = e$, and so $a^4b^4 = e = (ab)^4$. And to get what we want, we set $\theta - \psi = \pi/4$, so $ab = R(2(\pi/4)) = R(\pi/2)$, which does have order 4. Specifically, we can choose $F_1 = R(\pi/4)$ and $F_2 = R(0)$. And we can choose any group G that contains these reflections, like the symmetries of a circle, or the symmetries of a square.

18. (Gallian, p.69, # 4) Show that if G is a group and $a \in G$, then $|a| = |a^{-1}|$.

There are at least two ways to approach this (and probably more?). If $|a| < \infty$, then setting $n = |a|$ for notational simplicity, we know that $a^n = e$, so $(a^{-1})^n = a^{-1} \cdots a^{-1} = (a \cdots a)^{-1} = (a^n)^{-1} = e^{-1} = e$ (where this 'used' that $(ab)^{-1} = b^{-1}a^{-1}$ and induction), and so we know that $|a^{-1}| \le n$ (by definition) or $|a^{-1}|$ divides n (from results from class), depending on your viewpoint. In particular, we have $|a^{-1}| < \infty$, as well.

But then , since $(a^{-1})^{-1} = a$ and we know that $m = |a^{-1}| < \infty$ (introducing the notation again for simplicity), the same argument above shows that $n = |a| = |(a^{-1})^{-1}| \le m$ (or n divides m, if you take that viewpoint). So we have established that $m \le n$ and $n \le m$ (or $m|n$ and $n|m$, with $m, n \ge 1$), which (both) imply that $n = m$. So $m = |a^{-1}| = |a| = n$, as desired.

For completeness, we should mention that if $|a| = \infty$ then we must also have $|a^{-1}| = \infty$, since otherwise $|a^{-1}| = m < \infty$, and then our argument above implies that $|a| = |(a^{-1})^{-1}|$ must be finite as well (and $|a| \le m$), a contradiction! So $|a^{-1}| = \infty$, and in particular $|a^{-1}| = |a|$. So whether $|a|$ is finite or infinite, we always have $|a| = |a^{-1}|$.