Math 417 Problem Set 4 Solutions

Starred (*) problems were due Friday, September 21.

(*) 23. (Gallian, p.71, #46) Suppose that G is a group and $g \in G$ has $|g| = 5$. Show that the centralizer of g, $C(g) = C_G(g) = \{x \in G \ : \ xg = gx\}$, is equal to the centralizer of g^3, $C_G(g^3)$.

[Hint: show that anything that commutes with g must commute with g^3, and vice versa! What, if anything, is special about the numbers 5 and 3 in this problem?]

What we need to show is that both $C_G(g) \subseteq C_G(g^3)$ and $C_G(g^3) \subseteq C_G(g)$. That is, if an element $x \in G$ satisfies $xg = gx$ then we also have $xg^3 = g^3x$, and, conversely, if $xg^3 = g^3x$ then we must also have $xg = gx$.

For the first, if $x \in C_G(g)$, then $xg = gx$, and so

$xg^3 = x(ggg) = (xg)gg = (gx)gg = g(xg)g = g(gx)g = gg(xg) = gg(gx) = (ggg)x = g^3x$,

so $x \in C_G(g^3)$. Conversely, if $y \in C_G(g^3)$, then $yg^3 = g^3y$, and so

$yg = yg(e) = yg(g^5) = yg^6 = y(g^3g^3) = (yg^3)g^3 = g^3y)g^3 = g^3(yg^3) = g^3(g^3y) = (g^3g^3)y = g^6y = (g^5)gy = (e)gy = gy$,

so $y \in C_G(g)$. Here we have used that we were told that $|g| = 5$, so $g^5 = e$. So we have found that $C_G(g)$ and $C_G(g^3)$ contain the same elements, when $|g| = 5$, and so $C_g(g) = C_G(g^3)$.

(*) 25. If G is an abelian group and $n \in \mathbb{Z}$, show that $H_n = \{g \in G \ : \ g = x^n \text{ for some } x \in G\}$ (i.e., the set of n-th powers of elements of G) is a subgroup of G. Give an example where this fails if G is not abelian.

We show the three needed properties:

Since for $e \in G$, $e = e^n$ (by induction!), we have $e \in H_n$.

If $g, h \in H_n$, then $g = x^n$ and $h = y^n$ for some elements $x, y \in G$. Then, since G is abelian, $gh = x^ny^n = x \cdots x \cdot y \cdots y = xy \cdots xy = (xy)^n$ (by induction!), so $gh \in H_n$.

If $g \in H_n$, then $g = x^n$ for some $x \in g$, and then $g^{-1} = (x^n)^{-1} = x^{-n} = (x^{-1})^n = y^n$ for $y = x^{-1} \in G$, and so $g^{-1} \in G$.

Having established the three needed properties, we have shown that H_n is a subgroup.

This does not work, however, when G is not abelian. An example can be found using symmetry groups of polygons. In D_3, for example, with $n = 3$, the three reflections have $x^2 = e$, so $x^3 = x$. But all of the rotations have $x^3 = e$. So $H = \{g \in D_3 \ : \ g = x^3 \text{ for some } x \in D_3\}$ is equal to the three reflections, together with e; these are the cubes in D_3. But these do not form a (sub)group, since the product of two distinct reflections is a rotation by a non-trivial angle, which is not in H.

(*) 26. (Gallian, p.72, #53) Consider the element $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2, \mathbb{Z})$ What is the order of A ? If we instead view $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2, \mathbb{Z}_n)$ for an integer $n \geq 2$, what is the order of A ?

We can compute $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$
and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$,
which leads us to believe that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$.

This can be verified by induction on m; the case $m = 1$ is immediate, while $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ implies that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{m+1} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+1 \\ 0 & 1 \end{pmatrix}$, establishing the inductive step.

Since, in $SL(2\mathbb{Z})$, none of these matrices, for $n \in \mathbb{N}$ is the identity element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of the group, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order in $SL(2, \mathbb{Z})$.

On the other hand, since $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in $SL(2, \mathbb{Z}_n)$ precisely when $m \equiv 0 \pmod{n}$, so $n|m$, the smallest $m \in \mathbb{N}$ with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is n, so the order of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $SL(2, \mathbb{Z}_n)$ is n.

A selection of further solutions.

21. If G is a group, and $H \subseteq G$ is a subset of G so that, whenever $a, b \in H$ we have $a^{-1}b^{-1} \in H$, is this enough to guarantee that H is a subgroup of G? If yes, explain why! If not, give an example which shows that it doesn't work.

[Hint: if $a \in H$, start listing other elements that you can guarantee are in H ...]

Taking our cue from the hint, if we know that $a \in H$, then $a, a \in H$ and so $a^{-1}a^{-1} = a^{-2} \in H$. Then we know that $a, a^{-2} \in H$, and so $a^{-1}(a^{-2})^{-1} = a^{-1}a^2 = a \in H$, which tells us nothing new.... But $a^{-2}, a^{-2} \in H$, so $(a^{-2})^{-1}(a^{-2})^{-1} = a^2a^2 = a^4 \in H$. Then $a, a^4 \in H$, and so $a^{-1}(a^4)^{-1} = a^{-1}a^{-4} = a^{-5} \in H$.

We can keep this up for awhile; so far we have showwn that if $a \in H$, then $a^{-5}, a^{-2}, a, a^4 \in H$. Even with this list we might get suspicious; the exponents differ by (multiples of) 3. This pattern will continue; the only powers of a we will discover in H are of the form $1 + 3k$ for some $k \in \mathbb{Z}$. This suggests that

$H = \{a^{3k+1} : k \in \mathbb{Z}\}$

is in fact a set satisfying the condition we have imposed. And we can show this: $(a^{3k+1})^{-1}(a^{3\ell+1})^{-1} = a^{-3k-3\ell-2} = a^{3(-k-\ell-1)+1} = a^{3m+1}$ for $m = -k - \ell - 1$. But! If $|a| = \infty$, then $e \notin H$, since the only power of a which is equal to e is a^0, and a^0 is not in H. [Actually, all of the conditions for a group fails for this example!] We can get the same result if we choose our favorite group G and element $a \in G$ having $|a| = 3n$ for some k (like, for example, $\mathbb{Z}_{3n}$?), since then the set H we have built has exactly n elements, none of which are e.

[It is in fact true that the property that $a, b \in H$ implies $a^{-1}b^{-1} \in H$ together with $e \in H$ does imply that H is a subgroup.]

24. (Gallian, p.73, #66) Let $G = GL_2(\mathbb{R})$ = the 2×2 invertible matrices, under matrix multiplication, and let $H = \{A \in GL_2(\mathbb{R}) \ : \ \det(A) = 2^k \text{ for some } k \in \mathbb{Z}\}$. Show that H is a subgroup of G.

    We wish to show that H contains the identity (matrix), and is closed under both matrix multiplication and matrix inversion. This we can do, following the two step model, if we wish. Here we will instead, for fun, apply our one-step approach: H is a subgroup of G so long as whenever $A, B \in H$ we have $AB^{-1} \in H$ But since we have $A \in H$ and $B \in H$, we know that $\det(A) = 2^k$ for some integer k, and $\det(B) = 2^\ell$ for some integer ℓ. But then

    $$\det(AB^{-1}) = \det(A)(\det(B^{-1})) = \det(A)(\det(B))^{-1} = 2^k \cdot (2^\ell)^{-1} = 2^k \cdot 2^{-\ell} = 2^{k-\ell},$$

    for the integer $k - \ell$, using the properties of determinants which we learn in linear algebra, and so $AB^{-1} \in H$. So H is a subgroup of G.