Math 417 Problem Set 4 Solutions

Starred (*) problems were due Friday, February 19.

(*) 28. If G is a group with $a, b \in G$, and $ab = b^2a$ and $a^2b = ba$, show that $a = b = e$.

[What <u>other</u> "words" in a and b are equal to one another?]

There are any number of posible ways to answer this question. What we essentially want to do is to show that from the two 'equations', other products of a and b are equal; then by left- and right-cancellation we can establish the $a = e$ and $b = e$. Here are two possible routes:

$ab = b^2a = bba$ means $aba = bbaa$. Then $aab = ba$ means $aaba = baa$, so $baaba = bbaa = aba$. But then right-cancellation gives $baab = ab$, so $baa = a$, so $ba = e$. But then $ab = bba = b(ba) = be = eb$, and so $a = e$ by right cancellation. But then $e = ba = be = b$. So $a = e$ and $b = e$, as desired.

Another: $ab = bba$ and $ba = aab$ means $ba = a(ab) = a(bba) = (ab)ba = (bba)ba = bbaba$ But then left-cancellation gives $a = baba$, and right-cancellation gives $e = aba$. Then $e = a^{-1}a = a^{-1}ea = a^{-1}(aba)a = (a^{-1}a)baa = ebaa = baa$, so $baa = e$. But since $baa = ab$, this means that $ab = e$. Then $ba = aab = ae = a$, and so $b = e$. Then $ab = baa$ means $a = ae = eaa = aa$, and so $e = a$. So $a = e$ and $b = e$, as desired.

(*) 29. (Gallian, p.87, #14) Suppose that G is a <u>cyclic</u> group that has exactly three subgroups: G, $\{e\}$, and a subgroup of order 7. What is $|G|$? Is there anything special about the number 7 ?

From work in class, we know that the subgroups of $G = \langle a \rangle$ are all of the form $H = \langle a^k \rangle$ for some k dividing $|a| = |G| = n$, and that the order of H is then n/k. Since every divisor of n gives a different subgroup (since they have different orders) this means that there are precisely three numbers that divide n: n (giving a subgroup of order 1 (i.e., $\{e\}$)), 1 (giving a subgroup of order n, i.e., G), and a k with $n/k = 7$. But this means that $n = 7k$, so 7 is a divisor of n (giving a subgroup of order k (!)). <u>So</u> k must <u>be</u> 7, otherwise there would be <u>another</u> subgroup, of order k (generated by a^7). So $n = 7k = 7 \cdot 7 = 49$.

What makes 7 special is that it is a prime. The argument above says that if you have exactly three subgroups of $\langle a \rangle$ of order 1, k , and n, then n must be k^2. But if k is not prime, there there will be <u>more</u> factors of $n = k^2$ than these three, meaning more than three subgroups will exist. So not only must n be a square, but it must be the square of a prime number.

(*) 34. Show that if is G is a group and $a, b \in G$ with $|a| = 5$ and $|b| = 7$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$. Use this to show that if, in addition, G is abelian, then $|ab| = 35$.

A previous homework problem (# 18) established that since $\langle a \rangle$ and $\langle b \rangle$ are subgroups of G, $H = \langle a \rangle \cap \langle b \rangle$ must also be a subgroup of G. But then H is a subgroup of $\langle a \rangle$, as well, and so $H = \langle a^k \rangle$ and $|H|$ divides $|\langle a \rangle| = |a| = 5$, so (since 5 is prime!) $|H| = 1$ or $|H| = 5$. But the same argument shows that H is a subgroup of $\langle b \rangle$, as well, and so has order dividing $|b| = 7$, and so $|H| = 1$ or $|H| = 7$. The only way for both of these statements to be true is if $|H| = 1$, and so (since H must contain e) $H = \{e\}$.

If, in addition, G is abelian, then $(ab)^n = a^n b^n$ for any n. Consequently, $(ab)^{35} = a^{35}b^{35} = (a^5)^7(b^7)^5 = e^7e^5 = ee = e$, and so (from class) $|ab|$ divides 35. On the other hand, if $(ab)^k = a^k b^k = e$ then $z = b^k = (a^k)^{-1} = a^{-k}$, and so z is a power of both a and b, so $z \in \langle a \rangle \cap \langle b \rangle = \{e\}$, so $z = e$. This means that $b^k = e$ (so k is a multiple of $|b| = 7$) and $a^{-k} = e$, so $a^k = e$, and so k is a multiple of $|a| = 5$. This means that k is divisible by 5 and 7, and so is divisible by their least common multiple, which is 35 [This is because the lcm is $5 \cdot 7 = 35$ divided by the gcd of 5 and 7 (which is 1).]

Consequently, since $(ab)^{|ab|} = e$, we have 35 divides $|ab|$ and $|ab|$ divides 35, so $|ab| = 35$.

A selection of further solutions

27. (Gallian, p.72, #49) If G is a group with $a, b \in G$, so that $|a| = 4$, $|b| = 2$, and $a^3b = ba$, find the value of $|ab|$.

Since $|b| = 2$¡ we have $b \neq e$ (otherwise $|b| = 1$) and $b^2 = e$, so $b^{-1} = b$. Also, since $|a| \neq |b| = |b^{-1}|$, we must have $a \neq b^{-1}$ (otherwise they would have the same order!), and so $ab \neq e$ an so $|ab| > 1$.

But now $(ab)^2 = abab = a(ba)b = a(a^3b)b = a^4b^2 = ee = e$, and so $|ab| \leq 2$. Consequently, $|ab| = 2$.

30. (Gallian, p.88, #24, sort of) Show that if G is a group with $a, b \in G$ and $ab = ba$, then $\langle b \rangle \leq C_G(a) =$ the centralizer of a in G.

If $x \in \langle b \rangle$, then $x = b^k$ for some $k \in \mathbb{Z}$, then since $ab = ba$, we have $b^{-1}a = b^{-1}(ab)b^{-1} = b^{-1}(ba)b^{-1} = ab^{-1}$. But then induction on n implies that

$b^n a = b^{n-1}(ba) = b^{n-1}(ab) = (b^{n-1}a)b = (ab^{n-1})b = ab^n$

(when $n \geq 1$; we applied the inductive hypothesis in the middle to complete the inductive step, and $ab = ba$ is the initial step). An identical argument shows $b^{-n}a = ab^{-n}$ for every $n \geq 1$. Since $b^0a = ea = a = ae = ab^0$, we find that $b^n a = ab^n$, i.e., $b^n \in C_G(a)$, for every $n \in \mathbb{Z}$. In oter words, $\langle b \rangle \leq C_G(a)$, as desired.

31. (Gallian, p.89, #31) If G is a <u>finite</u> group, show that there is an integer $n \geq 1$ so that $a^n = e$ for all $a \in G$.

[The smallest such n is called the *exponent* of the group G, and will divide any other value of n (Why?).]

Because G is finite, given an $a \in G$ we have $\langle a \rangle \leq G$ and so $\langle a \rangle$ is finite, so $|a| = |\langle a \rangle| = n(a) < \infty$. In particular, $a^{n(a)} = e$. Since we know that if $n(a)|N$ then $a^N = (a^{n(a)})^{N/n(a)} = e^{N/n(a)} = e$, if we take n to be the <u>product</u> of all of the $n(a)$, over all $a \in G$, then $n(a)|n$ for every $a \in G$¡ and so $a^n = e$ for every $a \in G$, as desired.

[This value of n, we will see, is far larger than it needs to be....!]