Math 417 Problem Set 5 Solutions

Starred (*) problems were due Friday, September 28.

(*) 28. (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 $b^0 a = ea = a = ae = ab^0$, we find that $b^n a = ab^n$, i.e., $b^n \in C_G(a)$, for every $n \in \mathbb{Z}$. In other words, $\langle b \rangle \leq C_G(a)$, as desired.

(*) 30. (Gallian, p.86, #17) If $a \in G$ and $|a| < \infty$, then complete the following statement:

"$|a^2| = |a^{12}|$ if and only if ________ ."

Explain why your statement is true.

First, we note that $a^{12} \in \langle a^2 \rangle$, since $a^{12} = (a^2)^6$. So we can write $a^2 = b$ and then $a^{12} = b^6 \in \langle b \rangle$. And in this context, $|b^6| = |b|/gcd(|b|, 6)$. So $|a^{12}| = |b^6| = |b| = |a^2|$ precisely when $gcd(6, |a^2|) = 1$. So $|a^{12}| = |a^2|$ precisely when $|a^2|$ is not a multiple of 2 or 3.

If you would prefer an answer in terms of $|a|$, we know that $|a^2| = |a|/gcd(2, |a|)$. So $|a^{12}| = |a^2|$ if and only if $gcd(6, |a|/gcd(2, |a|)) = 1$. Multiplying through by $gcd(2, |a|)$ this becomes $gcd(6 \cdot gcd(2, |a|), |a|) = gcd(2, |a|)$. [This is because $gcd(a, b) = k$ implies that $gcd(na, nb) = nk$.]

So: if $|a|$ is odd, $gcd(2, |a|) = 1$, so this becomes $gcd(6, |a|) = 1$. When $|a|$ is even, $gcd(2, |a|) = 2$, so this becomes $gcd(12, |a|) = 2$. So, $|a^{12}| = |a^2|$ if and only if $gcd(6, |a|) = 1$ when $|a|$ is odd, or $gcd(12, |a|) = 2$ when $|a|$ is even.

(*) 34. Show that if $\alpha \in S_n$ has $|\alpha|$ <u>odd</u>, then α is an <u>even</u> permutation!

[Hint: Imagine that you have expressed α as a product of disjoint cycles...]

Since $|\alpha|$ is odd, when we write α as a product of disjoint cycles

$$\alpha = (a_{1,1}, \ldots, a_{1,k_1}) \cdots (a_{m,1}, \ldots, a_{m,k_m}) \ ,$$

the lcm of $k_1, \ldots k_m$ must be odd. But this implies that each k_i is odd; if one of the k_i were even then all of its multiples would be even, and so the lcm would be even.

But this means that α is a product of (disjoint) cycles of odd length. But an odd-length cycle is an even permutation! So each cycle can be written as a product of an even number of 2-cycles. This means that their product, α can be written as a product of even numbers of 2-cycles, and so can be written as the product an even number of 2-cycles. So α is even.

[N.B.: Note that this means that the alternating group A_n contains all of the elements of S_n with odd order...]

A selection of further solutions.

31. (Gallian, p.87, #14) Suppose that G is a cyclic 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 (!)). So k must be 7, otherwise there would be another 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 more 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.

33. (Gallian, p.114, #32) If $\beta = (1\ 2\ 3)(1\ 4\ 5)$, express β^{99} as a product of disjoint cycles.

    We can write β as a product of disjoint cycles, by starting from 1 and following them through the permutation:

    $\beta = (1\ 2\ 3)(1\ 4\ 5) = (1\ 4\ 5\ 2\ 3)$.

    So β is in fact a 5-cycle, which means that β has order 5. So $\beta^5 = e$. Since $99 = 5 \cdot 19 + 4$, we then have $\beta^{99} = \beta^4 = \beta^{-1} = (3\ 2\ 5\ 4\ 1) = (1\ 3\ 2\ 5\ 4)$.