Math 417 Problem Set 8 Solutions

Starred (*) problems were due **either** Friday, October 19, if you wanted to get your graded worked back before the midterm, **or** Monday, October 22, if you didn't care if you did or not.

(*) 51. (Gallian, p.209, #59) If $\varphi : G \to H$ is a homomorphism that is onto, show that if $g \in Z(G)$ then $\varphi(g) \in Z(H)$.

Suppose that $g \in Z(G)$, so that $gx = xg$ for every $x \in G$. now let $h = \varphi(g) \in H$, and suppose that $y \in H$. Then since φ is onto, there is an $x \in G$ with $\varphi(x) = y$. Then we have $gx = xg$, and so $\varphi(gx) = \varphi(xg)$, since φ is a function. But then

$$hy = \varphi(g)\varphi(x) = \varphi(gx) = \varphi(xg) = \varphi(x)\varphi(g) = yh,$$

since φ is a homomorphism. So $hy = yh$ for every $y \in H$, and so $\varphi(g) = h \in Z(H)$, as desired.

(*) 54. (Gallian p.151, #10) Let a and b be elements of a group G, and let H and K be subgroups of G. If $aH = bK$, show that $H = K$.

[One approach: show, first, that $aH = bH$!]

Since $aH = bK$, and $e_g \in K$ (since K is a subgroup of G), we have $be_G = b \in bK = aH$, so $b \in aH$, and so $a^{-1}b \in H$, and so $aH = bH$ (from work in class). So $bH = aH = bK$, and so $bH = bK$. This means that for any $h \in H$ we have $bh \in bH = bK$, so $bh = bk$ for some $k \in K$, and so by cancellation we have $h = k \in K$. So $h \in H$ implies $h \in K$, meaning that $H \subseteq K$. By a symmetric argument, $k \in K$ implies that $bk \in bK = bH$, so $bk = bh$ for some $h \in H$, so $k = h \in H$, so $K \subseteq H$.

Having both inclusions $H \subseteq K$ and $K \subseteq H$, we can conclude that $H = K$.

(*) 55. (Gallian p.152, #33) Let H and K be subgroups of a finite group G with $K \subseteq H \subseteq G$. Prove that $[G : K] = [G : H] \cdot [H : K]$.

The quick way: we know by Lagrange's Theorem that $|G| = |H| \cdot [G : H]$, since H is a subgroup of G, and $|G| = |K| \cdot [G : K]$ since K is a subgroup of G. We also know that, since K is a (sub)group (of G) and $K \subseteq H$, that K is a subgroup of H, so $|H| = |K| \cdot [H : K]$. Substituting the third equation into the first, we have $|G| = (|K| \cdot [H : K]) \cdot [G : H] = ([G : H] \cdot [H : K]) \cdot |K|$. Equating the right-hand side of this with the right-hand side of $|G| = [G : K] \cdot |K|$, we have

$([G : H] \cdot [H : K]) \cdot |K| = [G : K] \cdot |K|$. Since everything in this equation, including $|K|$ is finite (all of the indices are at most $|G| < \infty$), we can cancel $|K|$ to yield $[G : H] \cdot [H : K] = [G : K]$, as desired.

The less quick, but equally valid, way would be to count the number of left cosets of K in G in two ways, by noting that the cosets a_ib_jK, where the a_i are coset representatives of K in H, and the b_j are coset representatives of H in G, are in fact all disjoint and have union G, so the a_ib_j are coset representatives for K in G.

A selection of further solutions.

51. We showed that for $G = \mathbb{Z}[x] =$ the integer polynomials under addition, and $a \in \mathbb{Z}$, the function $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\varphi(p) = p(a)$ is a homomorphism. Describe the kernel of this homomorphism.

The kernel of φ is $\{p(x) \ : \ p(a) = 0\}$. But from (pre?)calculus, we know that $p(a) = 0$ precisely when we can write $p(x) = (x - a)q(x)$ for some other polynomial $q \in \mathbb{Z}[x]$. (Maybe this is really a Math 310 result? We can write any polynomial as $p(x) = (x - a)q(x) + r(x)$ for some $r(x)$ wwith degree less than 1, so $r(x)r \in \mathbb{Z}$, and then $p(a) = r = 0$.)

Therefore, the kernel of φ is the collection $\{(x - a)q(x) \ : \ q(x) \in \mathbb{Z}[x]\}$ of all multiples of the polynomial $(x - a)$.

56. (Gallian p.153, #47) Show that in a finite group G with $|G|$ odd, for every $a \in G$ the equation $x^2 = a$ has exactly one solution.

[Hint: show that the function (not a homomorphism!) $f : G \to G$ given by $f(x) = x^2$ is <u>onto</u> !]

Since $|G|$ is odd, then for every $a \in G$, we have $|a|$ divides $|G|$, so $|a|$ is odd. If we then write $|a| = 2n + 1$ for some $n \in \mathbb{Z}$, then $a^{2n+1} = e = a(a^n)^2$, so $a = ((a^n)^2)^{-1} = ((a^n)^{-1})^2 = (a^{-n})^2$. So setting $x = a^{-n}$ we have $x^2 = a$. So for every $a \in G$ there is an $x \in G$ so that $x^2 = a$. This means that the function $f(x) = x^2$ is a surjective function from G to G. But since G is finite, any surjective function from G to G is automatically injective as well, by the pigeonhole principle. So for every $a \in G$ there is <u>at</u> <u>most</u> one $x \in G$ with $x^2 = a$. Since we have shown there is also at least one, we conclude that for every $a \in G$, the equation $x^2 = a$ has exactly one solution $x \in G$.

[Note that since $|a|$ divides $|G| = 2N + 1$, we in fact have $a^{|G|} = a^{2N+1} = e$, and so there is in fact a single exponent $-N$ so that $(a^{-N})^2 = a$ for <u>every</u> $a \in G$ ...]