Math 417 Problem Set 8 Solutions

Starred (*) problems were due Friday, April 8.

(*) 61. (Gallian, p.202, # 37) If H is a normal subgroup in G and G is finite, and $g \in H$, show that the order of gH in G/H divides the order of g in G.

The quickest approach is to use the fact that if $x^n = e$ in a group then the order of x divides n. Translating that into the language of our problem, since what we want is that $|gH|$ divides $|g|$, this means tht we want gH to play the role of x, and $|g|$ to play the role of n. So it is enough to establish that $(gH)^{|g|} = e$ in G/H.

But this is true: since $g^{|g|} = e_G$, we have

$$(gH)^{|g|} = (gH)(gH)\cdots(gH) = (g\cdot g\cdots g)H = (g^{|g|})H = e_GH = H = e_{G/H}$$

in G/H. So the order of gH divides the order of g.

(*) 64. (Gallian, p.239, # 15) Show that if H and K are abelian, normal subgroups of the group G, and $H \cap K = \{e_G\}$, then the subgroup $N = HK$ is also abelian.

[Hint: if $a, b \in HK$, show that $aba^{-1}b^{-1} \in H \cap K$.]

What we wish to show is that if $h_1k_1, h_2k_2 \in HK$ (that is, $h_1, h_2 \in H$ and $k_1, k_2 \in K$), then $(h_1k_1)(h_2k_2) = (h_2k_2)(h_1k_1)$. Rewriting this, we want to show that $e_G = (h_1k_1)(h_2k_2)[(h_2k_2)(h_1k_1)]^{-1} = h_1k_1h_2k_2k_1^{-1}h_1^{-1}k_2^{-1}h_2^{-1} = x$. To show this, following the hint, we will show that x lies in both H and K. It then lies in their intersection, which is $\{e_G\}$, and so $x = e_G$.

Both assertions follow similiar lines. Because K is abelian, $x = h_1k_1h_2k_2k_1^{-1}h_1^{-1}k_2^{-1}h_2^{-1} = h_1k_1h_2k_1^{-1}k_2h_1^{-1}k_2^{-1}h_2^{-1} = h_1(k_1h_2k_1^{-1})(k_2h_1^{-1}k_2^{-1})h_2^{-1} = h_1(k_1h_2k_1^{-1})(k_2h_1k_2^{-1})^{-1}h_2^{-1}$. But because H is normal, $k_1h_2k_1^{-1} = h_3$ and $k_2h_1k_2^{-1} = h_4$ are in H, and so $x = h_1h_3h_4^{-1}h_2^{-1}$ is a product of elements of H, and so is in H.

On the other hand, since K is normal,
$x = h_1k_1h_2k_2k_1^{-1}h_1^{-1}k_2^{-1}h_2^{-1} = h_1k_1(h_1^{-1}h_1)h_2k_2k_1^{-1}h_1^{-1}(h_2^{-1}h_2)k_2^{-1}h_2^{-1}$
$= (h_1k_1h_1^{-1})h_1h_2k_2k_1^{-1}h_1^{-1}h_2^{-1}(h_2k_2^{-1}h_2^{-1}) = (h_1k_1h_1^{-1})h_1h_2k_2k_1^{-1}h_1^{-1}h_2^{-1}(h_2k_2h_2^{-1})^{-1}$, and we know that $h_1k_1h_1^{-1} = k_3$ and $h_2k_2h_2^{-1} = k_4$ are in K. Then, because H is abelian, $x = k_3h_1h_2k_2k_1^{-1}h_1^{-1}h_2^{-1}k_4 = k_3(h_1h_2)k_2k_1^{-1}(h_2h_1)^{-1}k_4 = k_3(h_1h_2)k_2k_1^{-1}(h_1h_2)^{-1}k_4$ and, again because K is normal, $(h_1h_2)[k_2k_1^{-1}](h_1h_2)^{-1} = k_5$ is in K. So $x = k_3k_5k_4$ is a product of elements of K, and so is in K.

So $x = (h_1k_1)(h_2k_2)[(h_2k_2)(h_1k_1)]^{-1}$ is in $H \cap K = \{e_G\}$, so $x = e_G$ as desired, and the elements of HK all commute with one another. So HK is abelian.

(*) 65. Show that 2 is <u>not</u> a generator for the group $\mathbb{Z}_{31}^*$ of units modulo 31, but that 3 <u>is</u>. If, using $\mathbb{Z}_{31}^*$ and $a = 3$ as the basis for a (very weak!) Diffie-Hellman key exchange, if Alice chooses $n = 5$ and Bob chooses $m = 11$ to build a shared key, what information do they send to one another and what is that key?

$|\mathbb{Z}_{31}^*| = 30 = 2\cdot 3\cdot 5$, and so to show that $|2| \neq 30$ it is enough to show that $2^n \equiv 1$ mod 31 for some $n < 30$. Fermat's Little Theorem tells us that the order must <u>divide</u> 30, so if it is less than 30 it must in fact divide one of $30/2 = 15$. $30/3 = 10$, or $30/5 = 6$. In fact, $2^5 = 32 \equiv 1 \bmod 31$, so the order of 2 is actually 5.

On the other hand, to show that the order of 3 is 30, it is enough (by Fermat's Little Theorem) to show that it is not a proper factor of 30 (which would then have to divide one of 15, 10, or 6), and so it is enough to show that 3^n is not congruent to 1 mod 31 for $n = 6, 10$, and 15. And so we check: $3^3 = 27 \equiv -4$, so $3^6 \equiv (-4)^2 = 16 \not\equiv 1$. $3^5 = 243 = 31(8) - 5 \equiv -5$, so $3^{10} \equiv (-5)^2 = 25 \equiv -6 \not\equiv 1$, and $3^{15} \equiv (-5)^3 = (-5)^2(-5) \equiv (-6)(-5) = 30 \equiv -1 \not\equiv 1$. So the order of 3 does not divide any proper factor of 30, while $3^{30} \equiv 1$, so the order of 3, mod 31, is 30.

This makes 3 a candidate for the generator of a Diffie-Hellman construction mod 31. Then with Alice using $n = 5$, she computes $3^5 \equiv -5 \equiv 26$, and so she transmits 26. With Bob using $m = 11$, he computes $3^{11} = 3^{10} \cdot 3 \equiv (-6)(3) = -18 \equiv 13$, and so he transmits 13. Then the shared key is $(26)^{11} = (13)^5 \bmod 31$, which is (although neither of them can compute it this way!) equal to $3^{5\cdot 11} = 3^{55} = 3^{30} \cdot 3^{25} \equiv 3^{25} = (3^5)^5 \equiv (-5)^5 = -5^5 = (-5)(25)(25) \equiv (-5)(-6)(-6) = (-5)(36) \equiv (-5)(5) = -25 \equiv 6$. So their shared secret is 6 .

A selection of further solutions.

62. If $\varphi : G \to H$ is a surjective homomorphism and $N \leq G$ is a normal subgroup of G, show that $\varphi(N) \leq H$ is a normal subgroup of H. Show, on the other hand, that if φ is not surjective, then $\varphi(N)$ need not be a normal subgroup.

If $h \in H$ and $x \in \varphi(N)$, we need to show that $hxh^{-1} \in \varphi(N)$. Since $x \in \varphi(N)$, we know that $x = \varphi(y)$ for some $y \in N$. And since φ is surjective, we know that there is $g \in G$ so that $\varphi(g) = h$. Then $hxh^{-1} = \varphi(g)\varphi(y)\varphi(g)^{-1} = \varphi(g)\varphi(y)\varphi(g^{-1}) = \varphi(gyg^{-1})$. But! Since $y \in N$ and $g \in G$, we have $gyg^{-1} \in N$, since N is normal. This means that $hxh^{-1} = \varphi(gyg^{-1})$ is the image under φ of something in N, and so $hxh^{-1} \in \varphi(N)$. So the conjugate of anything in $\varphi(N)$ lies in $\varphi(N)$, so $\varphi(N)$ is a normal subgroup of H.

However, if φ is not surjective, this need not be true. Probably the quickest way to show this is to use the identity map for φ (or more exactly, the inclusion map). For example, In $H = S_3$, $G = \{e_H, (1, 2)\}$ is a subgroup, but not a normal subgroup (since, e.g., $(1, 3)(1, 2)(1, 3) = (2, 3) \neq (1, 2)$). But the inclusion map $\iota : G \to H$ sending x to x is an injective homomorphism, but not a surjective one, and the normal subgroup $N = G \leq G$ is taken by φ to $G \leq H$, which is not a normal subgroup of H.

We can build more elaborate examples, as well. For example, the map $\mathbb{Z}_8 \to S_8$ sending k to $(1, 2, 3, 4, 5, 6, 7, 8)^k$ is a homomorphism, and $2\mathbb{Z}_8$ is a normal subgroup of $\mathbb{Z}_8$, but (you can check!) $\varphi(2\mathbb{Z}_8) = \langle(1, 2, 3, 4, 5, 6, 7, 8)^2\rangle = \langle(1, 3, 5, 7)(2, 4, 6, 8)\rangle$ is not a normal subgroup of S_8.

66. In the group S_{10} the elements $a = (1, 2, 3)(4, 5)(8, 9)$ and $b = (2, 4, 8)(1, 10)(3, 7)$ are conjugate. Find at least two distinct conjugating elements x (so that $xa = bx$).

Both elements are a product of disjoint cycles of length 2, 2, and 3. It is in fact the case that any elements of S_n that have the same 'disjoint cycle structure' are conjugate. This behaves kind of like 'change of basis' in linear algebra, we treat every element of $\{1, 2, \ldots, n\}$ as the basis elements. What we really need to do is to make a correspondence between the two sets of cycles and than send the elements of one cycle to the elements of the other. In order to make sure we build a permutation, though, we need to include the 1-cycles as part of this!

So, e.g., to conjugate $(1,2,3)$ to $(2,3,4)$ in S_5, we treat them as $(1,2,3)(4)(5)$ and $(2,3,4)(5)(1)$, and so we use the permutation $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 5$, and $5 \mapsto 1$, i.e., the permutation $(1,2,3,4,5)$. Then we can check that

$$(1,2,3,4,5)(1,2,3)(5,4,3,2,1) = (1)(2,3,4)(5) = (2,3,4).$$

So, in S_{10}, to conjugate $(1,2,3)(4,5)(8,9) = (1,2,3)(4,5)(8,9)(6)(7)(10)$ to

$(2,4,8)(1,10)(3,7) = (2,4,8)(1,10)(3,7)(5)(6)(9)$, we send $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 8$, $4 \mapsto 1$, $5 \mapsto 10$, $6 \mapsto 5$, $7 \mapsto 6$, $8 \mapsto 3$, $9 \mapsto 7$, and $10 \mapsto 9$, which is the permutation $(1,2,4)(3,8)(5,10,9,7,6)$. And we can check:

$$[(1,2,4)(3,8)(5,10,9,7,6)][(1,2,3)(4,5)(8,9)][(4,2,1)(8,3)(6,7,9,10,5)]$$
$$= (1,10)(2,4,8)(3,7)(5)(6)(9) = (1,10)(2,4,8)(3,7)\ .$$

On the other hand, writing the second element as $(2,4,8)(3,7)(1,10)(9)(5)(6)$, we send $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 8$, $4 \mapsto 3$, $5 \mapsto 7$, $6 \mapsto 9$, $7 \mapsto 5$, $8 \mapsto 1$, $9 \mapsto 10$, and $10 \mapsto 6$, which is the permutation $(1,2,4,3,8)(5,7)(6,9,10)$. And we can check:

$$[(1,2,4,3,8)(5,7)(6,9,10)][(1,2,3)(4,5)(8,9)][(8,3,4,2,1)(7,5)(10,9,6)]$$
$$= (1,10)(2,4,8)(3,7)(5)(6)(9) = (1,10)(2,4,8)(3,7)\ .$$