Math 417 Problem Set 10 Solutions

Starred (*) problems were due Friday, November 16.

(*) 67. (Gallian, p.191, #) If G is a group, $H \lhd G$ is a normal subgroup, and $K \leq G$ is a subgroup, then $HK = \{hk \ : \ h \in H, k \in K\}$ is a subgroup of G. (See Example 5 on p.175 for an explanation why.) Show that if, in addition, K is a <u>normal</u> subgroup of G, then HK is a normal subgroup.

$HK = \{hk \ : \ h \in H, k \in K\}$, and we wish to show that if $x \in HK$ and $g \in G$, then $gxg^1 \in HK$. We start by knowing that both H and K are normal subgroups of G. So we write $x = hk$ with $h \in H$ and $k \in K$. Then $gxg^{-1} = g(hk)g^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1})$. But since H is normal, $ghg^{-1} = h' \in H$, and since K is normal, $gkg^{-1} = k' \in K$. So $gxg^{-1} = h'k' \in HK$, as desired. So $HK \lhd G$ is a normal subgroup of G.

(*) 70. 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, $2^5 = 32 \equiv 1$ mod 31, so the order of 2 is actually 5.

On the other hand, to show that the order of 3 <u>is</u> 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 $(26)^{11} = (13)^5$ mod 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 .

(*) 73. Find a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}_7)$ so that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 5 & 4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in the group $GL(2, \mathbb{Z}_7)$.

[Note that we can multiply a, b, c, and d, in a solution, by $u \in \mathbb{Z}_7^*$, and still have a solution. This allows you to <u>assume</u> that, for example, either $a = 0$ or $a = 1$. This can lower your work factor....]

Multiplying the matrices out and equating corresponding entries, we find that we want to solve the linear equations

$$2a + 4b = 3a + 0c\ ,\ 3a + 5b = 3b + 0d\ ,\ 2c + 4d = 5a + 4c\ ,\ 3c + 5d = 5b + 4d,$$

where $a, b, c, d \in \mathbb{Z}_7$ and $ad - bc \in \mathbb{Z}_7^*$, and all equations hold modulo 7. We could turn this into a matrix system and solve by row reduction (mod 7), or we can just fiddle with the equations, adding multiples of one to another (which is really what row reduction is, anyway...) Rewriting the equations (mod 7) as

$-a + 4b = 0\ ,\ 3a + 2b = 0\ ,\ -5a - 2c + 4d = 0\ ,\ -5b + 3c + d = 0$, or

$a = 4b\ ,\ 3a + 2b = 0\ ,\ 2a + 5c + 4d = 0\ ,\ 2b + 3c + d = 0$, so $a = 4b$; note that $3a + 2b = 12b + 2b = 14b = 0$ is then correct. Substituting, we have

$a = 4b$, $2(4b) + 5c + 4d = 0\ ,\ 2b + 3c + d = 0$, which means $b + 5c + 4d = 0$, so $b = -5c - 4d = 2c + 3d$. Substituting, we have

$0 = 2(2c + 3d) + 3c + d = 4c + 6d + 3c + d = 7c + 7d = 0$, which is true! So we "really" only have two equations:

$a = 4b$, $b = 2c + 3d$, so $a = 8c + 12d = c + 5d$. But $a = c + 5d$ and $b = 2c + 3d$ means that $ad - bc = (c + 5d)d - (2c + 3d)c = cd + 5d^2 - 2c^2 - 3cd = 5c^2 + 5cd + 5d^2$. So, so long as $5(c^2 + cd + d^2)$ is not a multiple of 7, that is $c^2 + cd + d^2 \neq 0$ in $\mathbb{Z}_7$, we can construct a solution using $a = c + 5d$ and $b = 2c + 3d$. So, for example, we have the solutions

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$ (for $c = 1, d = 0$), or $\begin{pmatrix} 5 & 3 \\ 0 & 1 \end{pmatrix}$ (for $c = 0, d = 1$), or $\begin{pmatrix} 6 & 5 \\ 1 & 1 \end{pmatrix}$ (for $c = 1, d = 1$), or $\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}$ (for $c = 1, d = 3$).

Note, though, that $(c, d) = (1, 2)$, or $(2, 1)$, or $(2, 4)$, or several other choices, will not result in a matrix in $GL(2, \mathbb{Z}_7)$; they will have determinant 0.

A selection of further solutions.

68. (Gallian, p.168, # 17) Show that if $G \oplus H$ is a cyclic group, then G and H are both cyclic. [Hint: A group <u>isomorphic</u> to a cyclic group is cyclic!]

Suppose that $G \oplus H = \langle g \rangle$ is a cyclic group. We can build a homomorphism $\varphi : G \to G \oplus H$ by $\varphi(g) = (g, e_H)$; this is a homomorphism because $\varphi(g_1 g_2) = (g_1 g_2, e_H) = (g_1 g_1, e_H e_H) = (g_1, e_H)(g_2, e_H) = \varphi(g_1)\varphi(g_2)$. This map is also one-to-one, since $(g_1, e_H) = (g_2, e_H)$ implies that $g_1 = g_2$. Therefore, the image of G, $\varphi(G) = K \leq G \oplus H$, is isomorphic to G; the map $\varphi : G \to \varphi(G)$ is a bijective homomorphism. Therefore, $G \oplus H$ contains a subgroup isomorphic to G. But every subgroup of a cyclic group is cyclic, and a group isomorphic to a cyclic group is cyclic (if $\phi : \langle g \rangle \to G$ is an isomorphism, then every element of G is the image of a power of g, and so is a power of the image, $\phi(g)$, of g). Therefore, G is isomorphic to the subgroup of a cyclic group, and is therefore cyclic! A completely analogous argument establishes that H is cyclic, as well.

71. 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:

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