Math 417 Problem Set 10

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

66. (Gallian, p209, # 51) Let N be a normal subgroup of a group G. Show that every subgroup K of G/N has the form H/N, where H is a subgroup of G. [Hint: Think about the homomorphism $\varphi : G \to G/N$.

(*) 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 normal subgroup of G, then HK is a normal subgroup.

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 isomorphic to a cyclic group is cyclic!]

69. (Gallian, p.170, # 59) Let p be a prime. Prove that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has exactly $p+1$ distinct subgroups of order p.

(*) 70. Show that 2 is not a generator for the group $\mathbb{Z}_{31}^*$ of units modulo 31, but that 3 is. 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?

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 $xa = bx$).

72. Find a matrix $X \in GL(2,\mathbb{Z})$ so that $X \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} X$.

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

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

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 assume that, for example, either $a = 0$ or $a = 1$. This can lower your work factor....]