# HOMEWORK 4, DUE THU FEB 25TH

*All solutions should be with proofs, you may quote from the book or from previous home works*

(1) Let $G$ be a finite abelian group.
  (a) Let $H, K$ be subgroups of $G$ with $\gcd(o(H), o(K)) = 1$. Show that the natural map $f : H \times K \to G$, $f(a, b) = ab$ is a one-to-one group homomorphism.

  (b) Show that $G$ is isomorphic to $H_1 \times H_2 \times \cdots \times H_n$ with all $H_i$ cyclic and $o(H_{i+1})$ dividing $o(H_i)$.

(2) We write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$, since we wish to use the fact that it has addition, multiplication and inverses for all non-zero elements, called a *field*.
  (a) Let $G = GL(n, \mathbb{F}_p)$. Then, we can let $G$ act on $\mathbb{F}_p^n = \mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ ($n$ times) as usual (recall from Math 429 how this works). If $A$ is any $n \times n$ matrix with entries from $\mathbb{F}_p$ and $\underline{a} \in \mathbb{F}_p^n$ (written as column vectors) then $A\underline{a} \in \mathbb{F}_p^n$ makes sense. Show that such an $A$ is in $G$ if and only if the columns (or rows) are linearly independent. That is, if $A = [\underline{a}_1, \underline{a}_2, \cdots, \underline{a}_n]$ and $c_1\underline{a}_1 + c_2\underline{a}_2 + \cdots + c_n\underline{a}_n = \underline{0}$, with $c_i \in \mathbb{F}_p$, then $c_i = 0$ for all $i$.

  (b) Calculate the order of $G$ for a prime $p$.

(3) These are some problems on automorphisms.
  (a) Let $G$ be a finite group and $\phi \in \mathrm{Aut}(G)$. Assume that if $\phi(g) = g$ for $g \in G$ then $g = e$. Show that every element in $g \in G$ is of the form $g = x^{-1}\phi(x)$ for some $x \in G$. Deduce that, if in addition $\phi^2 = \mathrm{Id}$, then $G$ is abelian.

  (b) Show that a finite group with order greater than two has a non-trivial (not equal to identity) automorphism.

(c) Let $\phi(n)$ be the Euler function (the number of integers $k$, $1 \leq k < n$ with $\gcd(k, n) = 1$). For any integer $a > 1$, show that $n$ divides $\phi(a^n - 1)$. (Hint: For any $m > 1$, $\phi(m)$ is the order of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.)

(4) These are some problems on semi-direct products.
   (a) Construct a non-abelian group of order 55 and one of order 203.

   (b) Can you do the same for 35?

(5) Show that $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group for any prime $p$.