HW 3, due 02.03

1. Let $f : \mathbb{C} \to \mathbb{C}$ be given by $f(a+bi) = a - bi$ (for all $a+bi \in \mathbb{C}$). (As you know, $a - bi$ is referred to as *conjugate* of $a+bi$, and $a-bi$ is denoted $\overline{a+bi}$).

   (a) Show f above is a ring automorphism of $\mathbb{C}$.

   (b) Let $Aut_{\mathbb{R}}(\mathbb{C})$ be the ring automorphisms of $\mathbb{C}$ that fix $\mathbb{R}$ pointwise, i.e., $g(x) \in Aut_{\mathbb{R}}(\mathbb{C})$ if $g(x) \in Aut(\mathbb{C})$ and for all $r = r + 0i \in \mathbb{C}$, $g(r) = r$. Show that the only non-identity member of $Aut_{\mathbb{R}}(\mathbb{C})$ is f above, the complex conjugation map.

2. For a finite group G, let $exp(G) = \min\{k \in \mathbb{N} : \forall g \in G \in \ \ g^k = e\}$. So $exp(G)$ is the least positive power that "kills off" each element of G. It is easy to see that if G is cyclic, then $exp(G) = |G|$. The converse holds for finite Abelian groups, as you'll prove.

   Let G be a finite Abelian group with $|G| = p_1^{r_1} \dots p_k^{r_k}$ a prime factorization.

   (a) Explain *briefly* why every Sylow-p_i subgroup in G is normal. Use the Sylow Theorem (be sure to cite which part of the Sylow Theorem you are using in your proof).

(b) For $i = 1, \ldots, k$, you've proven that's there a unique Sylow-p_i group. Let's call it P_i. Find the finite group theoretic cardinality result (*)– cite the result and the page number of (*) in the text—that can be used to show that $G = P_1 \ldots P_k$, briefly explaining how (*) is applied to show $G = P_1 \ldots P_k$.

(c) We proved that (**) if H is a group with normal subgroups A and B satisfying $A \cap B = \{e\}$ and $AB = G$, then $G \cong (A \times B)$. Use (b) and (**) to explain, briefly but convincingly, why $G \cong P_1 \times \cdots \times P_k$. You can use the phrase "inductively", or something like it.

(d) As you know, for $g \in P_1 \ldots P_k$ with $g = (g_1, \ldots, g_k)$, then $|g| = \text{lcm}(|g_1|, \ldots, |g_k|)$. Use this observation to show that $exp(G) = exp(P_1) \times \ldots exp(P_k)$. (This is easy since for each i, $exp(P_i)$ is a power of p_i. I'll look for a **short, coherent** argument.)

(e) Of course if G is cyclic, then $exp(G) = |G|$. Use what you've proven above to show that $|G| = exp(G)$ implies G is cyclic. (So we now know that if G is finite, Abelian, then G is cyclic if and only if $|G| = exp(G)$.)

(f) We proved in class that (***) if F is a field and $g(x) \in F[x]$ with $\deg(g(x) = n \in \mathbb{N}$, then $g(x)$ has no more than n roots in F. Use (***) and (e) to prove that $\mathbb{Z}_p^x$ is cyclic.

(g) More generally, suppose F is a field, and K is a finite subfield of F. Let $K^* = K - \{0\}$, the units of K, a finite subgroup. Using (***) and (e), prove that K^* is cyclic.

3. Number 4, page 293 (Don't turn in–Scott and Christen will present.)
4. Number 4. page 301. (Don't turn in—YoYo and Jacob will present.)
5. Number 4, page 306, (a), (b), (c) only.