Math 8201 Graduate abstract algebra- Fall 2010, Vic Reiner
Midterm exam 1- Due Friday October 15, in class

Instructions: This is an open book, open library, open notes, take-home exam, but you are *not* to collaborate. The instructor is the only human source you are allowed to consult. Each of the 6 problems is worth approximately the same number of points.

1. Let H, K be subgroups of a group G.
(a) Show that the following conditions are equivalent:
(i) HK is a subgroup of G.
(ii) KH is a subgroup of G.
(iii) $HK = \langle H, K \rangle$, the subgroup of G generated by $H \cup K$.
(iv) $HK = KH$.

(b) Suppose that H_1, H_2 are both *normal* subgroups of G, and that $\gcd(|H_1|, |H_2|) = 1$. Show that $h_1 h_2 = h_2 h_1$ for all $h_1 \in H_1$ and $h_2 \in H_2$.

2. Prove or disprove the existence of the following group isomorphisms:
(i) $S_4 \cong D_{24}$
(ii) $D_{12} \cong \mathbb{Z}/2\mathbb{Z} \times D_6$
(iii) $D_{16} \cong \mathbb{Z}/2\mathbb{Z} \times D_8$

3. (a) Let G be a group, and $H \leq G$ a subgroup with finite index $n = [G : H]$. Show that H contains a subgroup N with $N \lhd G$ and index $[G : N]$ dividing $n!$.
(Hint: let G act on G/H by left-translation, that is, $g \cdot aH := gaH$)

(b) Given two subgroups H_1, H_2 of G, both of finite index in G, show that $H_1 \cap H_2$ is also of finite index in G.

4. Let P be a group of order p^n for a prime number p and $n \geq 2$. Show that for any element x in P, the map $\mathrm{ad}_x : P \to P$ defined by $\mathrm{ad}_x(y) = xyx^{-1}y^{-1}$ has the following property: $\mathrm{ad}_x^{n-1}(y) = e$ for every y in P.

Here ad_x^{n-1} means the composition of the map ad_x repeatedly $n-1$ times, so for example, $\mathrm{ad}_x^2(y) = \mathrm{ad}_x(\mathrm{ad}_x(y))$.

5. Let p be the smallest prime number dividing the order $|G|$ of a finite group G, and let $H \lhd G$ with $|H| = p$. Show that $H \leq Z(G)$, the center of G.

(Hint: Let G act on H via conjugation, that is, $g \cdot h := ghg^{-1}$. Note also that every g in G fixes the identity element e in H under this action.)

6. Consider the integers $\mathbb{Z}/n\mathbb{Z}$ modulo n as a ring with usual $\times$ and $+$ operations, and make the Cartesian product $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$ into a ring with componentwise $\times$ and $+$ operations.

(a) For $n := n_1 \cdots n_t$, show that the map

$$\begin{array}{rcl} f : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z} \\ \bar{r} & \longmapsto & (\bar{r}, \ldots, \bar{r}) \end{array}$$

is both well-defined, and a *ring homomorphism*, that is, $f(ab) = f(a)f(b)$ and $f(a+b) = f(a)+f(b)$ for all a, b in $\mathbb{Z}/n\mathbb{Z}$. Here $\bar{r}$ on the left means "r mod n", but in the i^{th} component on the right it means "r mod n_i".

(b) Show that if, in addition, if one has $\gcd(n_i, n_j) = 1$ for $i \neq j$ then the above map f is injective, and hence bijective (so a ring *isomorphism*).

(c) Use this to show that if n has prime factorization $n = p_1^{e_1} \cdots p_t^{e_t}$ with p_i primes and $e_i \geq 1$, then the Euler phi function defined by

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^{\times}|$$

has the formula

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_t^{e_t}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_t^{e_t} - p_t^{e_t-1})$$

(d) Recall that Fermat's Little Theorem says any integer x satisfies $x^p \equiv x \mod p$ when p is prime. Prove the following generalization: If n is *squarefree* in the sense that $n = p_1 \cdots p_t$ for distinct primes p_i, then every integer x satisfies $x^{\varphi(n)+1} \equiv x \mod n$.

(e) Show that the result in part (d) is false whenever n is *not* squarefree, that is, for each nonsquarefree n, show how to exhibit some integer x for which $x^{\varphi(n)+1} \not\equiv x \mod n$.