Takehome Assigment 4

Due Friday, May 14

In this assignment unless otherwise indicated, **all rings are unital rings** (although they will not necessarily be commutative), and **all homomorphisms are unital homomorphisms**.

1. Let's begin by exploring unit groups. Recall that if R is a (unital) ring, then $R^\times$ is the set of units, endowed with a group structure given by multiplication in R (cf. HW10 Problem 2).
   (a) Let $\varphi : R \to S$ be a (unital) homomorphism of rings. Show that if $r \in R^\times$ then $\varphi(r) \in S^\times$. Give a counterexample where φ is not unital.
   (b) Show that the restriction of φ to $R^\times$ is a group homomorphism $\varphi^\times : R^\times \to S^\times$, which is injective if φ is.
   (c) The analogous statement does not hold for φ surjective. Give an example of a surjective (unital) homomorphism $\varphi : R \to S$, but such that the induced map on unit groups $\varphi^\times : R^\times \to S^\times$ is not surjective.
   (d) Let $\varphi : R \to S$ be a surjective (unital) homomorphism of *commutative* rings, and suppose that $\ker \varphi \subseteq \mathfrak{J}(R)$ (where $\mathfrak{J}$ is the *Jacobson radical* from TH3 Problem 4). Prove that the induced map $\varphi^\times : R^\times \to S^\times$ is surjective.

2. In elementary calculus one often uses the fact that a polynomial of degree n over the real numbers has at most n roots. This turns out to be true over any field! For this problem we fix a field F.
   (a) Let $f(x) \in F[x]$, and suppose that $f(a) = 0$ for some $a \in F$. Show that $(x - a)$ divides $f(x)$. (Hint: recall that $F[x]$ is Euclidean domain).
   (b) Let $f(x) \in F[x]$, and suppose $f(a_1) = f(a_2) = \cdots = f(a_r) = 0$, for $a_i \in F$ all distinct. Prove by induction that $(x - a_1)(x - a_2)\cdots(x - a_r)$ divides $f(x)$.
   (c) Deduce from part (b) that if the degree of $f(x)$ is n, then $f(x)$ has at most n-roots.
   (d) As a corollary, let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ has no roots in F. Give an example to show this is not true for polynomials of degree 4.

3. We used many times this semester, (for example when classifying groups like in HW9) that if p is prime, the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$, and more generally that if p is an odd prime then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. But if you've been paying close attention you should notice that we haven't actually proved that fact yet! So let's come full circle and deduce this fact as a consequence of Problems 1 and 2.
   (a) Consider a finite abelian group $G = Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$ in invariant factor form (so that $n_k | n_{k-1} | \cdots | n_2 | n_1$). Prove that if $k \neq 1$ then there are more than n_k elements in G whose order divides n_k.
   (b) Let F be a field, and let $G \leq F^\times$ be a finite subgroup of the unit group of F. Prove that G is cyclic. Deduce that $(\mathbb{Z}/p\mathbb{Z})^\times \cong Z_{p-1}$. (*Hint:* Can you express the condition in (a) in terms of solutions to a polynomial in $F[x]$?)

   Let's now deduce the analogous result of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for an odd prime p.

   (c) Let G be a finite abelian group and suppose all it's Sylow subgroups are cyclic. Show that G is cyclic.

(d) Show that the surjection of rings $\pi : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induces a surjection of groups $\pi^\times : (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ whose kernel has order p^{n-1}. (Hint: use 1(d) and Lagrange's theorem).

(e) Deduce from part (d) that for all primes $p \neq q$, the Sylow q-subgroups of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ are cyclic.

It remains to show that the Sylow p-subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. We will need the following technical result.

(f) Let p be an odd prime. Prove the following identities by induction on k.
- $(1+p)^{p^k} \equiv 1 \mod p^{k+1}$
- $(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$

(g) Deduce from part (f) that the Sylow p-subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. (*Hint:* Prove $(1+p)$ is a generator!). Conclude that that $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong Z_{p^{n-1}(p-1)}$.

By TH2 we know abstractly that for any n, $(\mathbb{Z}/n\mathbb{Z})^\times$ can be expressed as a product of cyclic groups. In the case that n is odd we can now compute exactly which ones!

(h) Fix an odd integer n with prime factorization $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$. Express $(\mathbb{Z}/n\mathbb{Z})^\times$ as a product of cyclic groups in terms of the prime factorization. (*Note:* Putting this into invariant factor form depends on the factorizations of the $p_i - 1$, which can vary wildly as the primes do, so don't worry about doing that).

Congratulations!! We've covered a ton of material and done a ton of problems this semester. **Good work!**