Takehome Assigment 4 Solutions

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.

   Proof. Let $r \in R^\times$, and call its multiplicative inverse r^{-1}. Then

   $$\varphi(r)\varphi(r^{-1}) = \varphi(rr^{-1}) = \varphi(1_R) = 1_S,$$

   $$\varphi(r^{-1})\varphi(r) = \varphi(r^{-1}r) = \varphi(1_R) = 1_S,$$

   where we use that φ is unital in the last step. Therefore $\varphi(r)$ has an inverse, as desired. Counterexamples where φ is not unital include the 0 map, which takes every element of R to 0 (which is not a unit if S is not the 0 ring), or multiplication by 2 on $\mathbb{Z}$ which takes the unit 1 to 2. □

   (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.

   Proof. By part (a) we know that the image of $\varphi^\times$ lands in $S^\times$, so the function is well defined. Furthermore, since φ is a ring homomorphism, $\varphi^\times(rs) = \varphi^\times(r)\varphi^\times(s)$. Furthermore, the restriction of an injective map is plainly injective. □

   (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.

   Proof. Consider the surjective unital homomorphism $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$. The restriction to units is $\{-1, 1\} \to \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ which cannot possibly be 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.

   Proof. As $\ker \varphi$ is contained in the Jacobson radical of R, it is contained in each maximal ideal of R. Therefore, by the fourth isomorphism theorem, the image in S of any maximal ideal of R, is a proper (and even maximal) ideal of S. This implies that if $r \in R$ is not a unit, then $\varphi(r)$ is contained in a proper ideal of S and is therefore not a unit either. It follows that if $s \in S^\times$, any element mapping to s must be a unit. Such elements must exist since φ was surjective to begin with. □

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).

Proof. We perform Euclidean divison of $f(x)$ by $(x - a)$ to write

$$f(x) = q(x)(x - a) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg(x - a) = 1$. If $r(x) = 0$ we win, otherwise $r(x)$ is degree 0, i.e., $r(x) = c \in F$ is a constant function. So $f(x) = q(x)(x - a) + c$. Evaluating at $x = a$ gives $f(a) = q(a)(a - a) + c$. Since $f(a) = 0$ this proves $c = 0$ as desired. □

(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 $f(x)$.

Proof. We proceed by induction on r. The base case is part (a). For the general case, suppose $(x - a_1)(x - a_2) \cdots (x - a_{r-1})$ divides $f(x)$. In particular, there is some $g(x)$ such that $f(x) = (x - a_1) \cdots (x - a_{r-1})g(x)$. Evaluating at a_r gives

$$0 = (a_r - a_1) \cdots (a_r - a_{r-1})g(a_r).$$

Since $F[x]$ is an integral domain, and all the a_i are distinct, we may conclude that $g(a_r) = 0$. Therefore by part (a), $(x - a_r)$ divides $g(x)$, so that $g(x) = (x - a_r)h(x)$. Substituting we get $f(x) = (x - a_1) \cdots (x - a_{r-1})(x - a_r)h(x)$ giving the result. □

(c) Deduce from part (b) that if the degree of $f(x)$ is n, then $f(x)$ has at most n-roots.

Proof. Suppose $f(x)$ has r roots $a_1, \cdots, a_r$. Then by part (b) we see that $f(x) = (x - a_1) \cdots (x - a_r)h(x)$ so that:

$$n = \deg f(x) = \deg(x - a_1) + \cdots + \deg(x - a_r) + \deg h(x) = r + \deg h(x) \geq r.$$

□

(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.

Proof. Since $F[x]$ is a PID, and $f(x) \neq 0$, we know that $f(x)$ is irreducible if and only if $(f(x))$ is maximal, if and only if $F[x]/(f(x))$ is a field. Therefore it suffices to prove that $f(x)$ is irreducible if and only if it has no roots if F. If it has a root in F, it is reducible by part (a). Conversely, if $f(x)$ is reducible, $f(x) = h(x)g(x)$ for $h(x), g(x)$ nonunits. In particular, $\deg h(x) + \deg g(x) = 2$ or 3, and since they are nonunits, neither can be constant functions, so they both have degree at least one. In particular, one of them must have degree equal to 1, say $h(x) = ax + b$. Then $x = -b/a$ is a root of $h(x)$, thus of $f(x)$.

For a counterexample, we need only mutliply together 2 irreducible quadratics. Say $(x^2 + 1)(x^2 - 2) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$. We gave a factorization so it certainly isn't irreducible, but the complex roots are $\pm i, \pm\sqrt{2} \notin \mathbb{Q}$, so it has no roots in $\mathbb{Q}$. □

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.

   Proof. By HW2 Problem 8(c), we need only provide more that $n_k + 1$ elements z such that $z^{n_k} = 1$. Certainly $(1, 1, \cdots, 1, x)$ is such an element for any $x \in Z_{n_k}$, so this gives n_k many, we need only one more. Let g be a generator for Z_{n_1}. Notice that $n_1 = tn_k$ for some t, so that $|g^t| = n_k \neq 1$. In particular $g^t \neq 1$ and $(g^t, 1, \cdots, 1)$ has order n_k and isn't equal to any if the elements already listed, giving the extra element desired. □

   (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 $F[x]$?)

   Proof. By the *Fundamental Theorem of Finite Abelian Groups* (TH2 Theorem 1), we may express $G \cong Z_{n_1} \times \cdots \times Z_{n_k}$ with $n_k | n_{k-1} | \cdots | n_1$, and G is cyclic if and only if $k = 1$. If $k > 1$, then by part (a), G has more that n_k elements z with $z^{n_k} = 1$. But $G \subseteq F$, so that this gives more than n_k solutions to the polynomial $x^{n_k} - 1 \in F[x]$. This contradicts 2(c), so we must have $k = 1$ and therefore G is cyclic.

   An immediate consequence is that $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ is cyclic (since it is automatically finite). Since we know it has $p-1$ elements, it must be isomorphic to Z_{p-1}. □

   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.

   Proof. Let $P_1, \cdots, P_n$ be the Sylow subgroups of G. By TH2 Problem 1(e) we have that $G \cong P_1 \times \cdots \times P_n$. Suppose all the P_i are cyclic. Since they all have coprime orders, then applying HW4 Problem 5(c) inductively says 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).

   Proof. The kernel of π is the ideal generated by p, which by HW12 Problem 3(c) is the unique maximal ideal $\mathbb{Z}/p^n\mathbb{Z}$. In particular, $\ker \pi = \mathfrak{J}(\mathbb{Z}/p^n\mathbb{Z})$, so that applying 1(d) we may conclude that $\pi^\times$ is surjective. By HW12 Problem 1(d), we know that $|\mathbb{Z}/p^n\mathbb{Z}| = p^{n-1}(p-1)$. Since $\pi^\times$ is a surjection onto a group of order $p-1$, Lagrange's theorem says that $|\ker \pi| = \frac{p^{n-1}(p-1)}{p-1} = p^{n-1}$ as desired. □

(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.

Proof. Let P_q be a Sylow q-subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Then by Lagrange's theorem, $P_q \cap \ker\pi = \{1\}$, so that $\pi^\times$ restricted to P_q is injective. In particular, P_q is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Since subgroups of cyclic groups are cyclic, P_q must be 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.

- $(1+p)^{p^k} \equiv 1 \mod p^{k+1}$
- $(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$

Proof. The first identity certainly follows from the second, but because the proof of the second is a slightly more complicated application of the same ideas in the proof of the first, we include both for expository purposes. We begin with the first identity, proceeding by induction on k. If $k = 0$ there is nothing to prove. For the general case, we may assume by induction that $(1+p)^{p^{k-1}} = 1 + np^k$ for some $n \in \mathbb{Z}$. Raising to the p power gives:

$$(1+p)^{p^k} = (1+np^k)^p = 1 + \binom{p}{1} np^k + \binom{p}{2} n^2 p^{2k} + \cdots + n^p p^{pk} \equiv 1 \mod p^{k+1}.$$

In the last step we used that $\binom{p}{1} = p$, and that the remaining terms clearly have larger powers of p, so that everything except the first term is zero modulo p^{k+1}.

We continue with the second, again by induction on k. If $k = 0$ there is nothing to prove. If $k = 1$ this is:

$$(1+p)^p = 1 + \binom{p}{1} p + \binom{p}{2} p^2 + \binom{p}{3} p^3 + \cdots + p^p.$$

Since p is odd, p divides $\binom{p}{2} = p\frac{p-1}{2}$ so that all terms after the first two are zero modulo p^3, giving the result. (This where we use that p is an odd prime, notice that the formula isn't true if $p = 2$).

For the general case, we may assume by induction that $(1+p)^{p^{k-1}} = 1 + p^k + np^{k+1} = 1 + p^k(1+np)$ for some $n \in \mathbb{Z}$. Raising to the p power gives:

$$(1+p)^{p^k} = (1+p^k(1+np))^p = 1 + \binom{p}{1} p^k(1+np) + \binom{p}{2}(p^{2k})(1+np)^2 + \cdots + p^{pk}(1+np)^p$$

From the third term onward there is a p^{jk} term for $j \geq 2$, so that these terms become zero modulo p^{k+2} (here we use that $k \geq 2$ so that $jk \geq 2k \geq k+2$). On the other hand, since $\binom{p}{1} = p$, we have:

$$(1+p)^{p^k} \equiv 1 + \binom{p}{1} p^k(1+np) = 1 + p^{k+1} + np^{k+2} \equiv 1 + p^{k+1} \mod p^{k+2},$$

as desired.

□

(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 $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong Z_{p^{n-1}(p-1)}$.

Proof. We claim that $(1+p)$ is an element of order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Since p^{n-1} is a maximal p-divisor of $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^{n-1}(p-1)$, this would imply that $1+p$ generates the Sylow p-subgroup, so that it must be cyclic.

Notice that the first identity from part (f) says that $(1+p)^{p^{n-1}} \equiv 1 \mod p^n$. This shows first off that $1+p$ is a unit, so it is indeed an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, and second that its order as an element of the unit group divides p^{n-1}. We will show this is the exact order of $1+p$. Indeed, the second identity from part (f) says that $(1+p)^{p^{n-2}} \neq 1 \mod p^n$, so that the order of $(1+p)$ is strictly larger than p^{n-2}. The only number larger than p^{n-2} which divides p^{n-1} is p^{n-1} itself, so we have that $|(1+p)| = p^{n-1}$ as desired.

From this we easily conclude that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. Indeed, by part (c) it suffices to show that every Sylow subgroup is cyclic. But we just saw that it's Sylow p-subgroup is cyclic, and in part (e) we showed that the same holds for each Sylow q-subgroup for every prime $q \neq p$. $\square$

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).

Proof. Since n is odd, each p_i is odd. We now proceed with a direct computation in 3 steps. The first equality is Sun Tzu's theorem. The second equality is HW12 Problem 1(a) (applied inductively), and the third step is part (g) above.

$$\begin{aligned}
(\mathbb{Z}/n\mathbb{Z})^\times &\cong (\mathbb{Z}/p_1^{\alpha_1} \times \cdots \times \mathbb{Z}/p_t^{\alpha_t})^\times \\
&\cong (\mathbb{Z}/p_1^{\alpha_1})^\times \times \cdots \times (\mathbb{Z}/p_t^{\alpha_t})^\times \\
&\cong Z_{p_1^{\alpha_1-1}(p_1-1)} \times \cdots \times Z_{p_t^{\alpha_t-1}(p_t-1)}
\end{aligned}$$

$\square$

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