Takehome Assignment 3

Due Friday, May 13 **at 11:59 pm**

1. Let's start with some group theory! For this first question, let G be a finite group of order n. We'd like to understand the size of the center of G, say $|Z(G)| = z$.

   (a) Show that it is not possible for z to fall in the range $\frac{n}{4} < z < n$.

   Proof. By Lagrange's theorem, we know that $z|n$, so that $\frac{n}{z} \in \{1, 2, 3, 4, ...\}$. We first show that $\frac{n}{z} \neq 2, 3$ (in fact, it cannot equal any prime number p). Suppose otherwise that $\frac{n}{z}$ is a prime p. Recall (from HW6 Problem 3(a)), that $Z(G) \trianglelefteq G$, so that $G/Z(G)$ is a group of order $\frac{n}{z} = p$. By TH1 Problem 4(a), $G/Z(G) \cong Z_p$ is cyclic, so that by HW6 Problem 3(b) we see that G is abelian. But then $G = Z(G)$ and so $n = z$ and $\frac{n}{z} = 1 \neq p$, which is a contradiction.

   A consequence of the previous paragraph is that if $\frac{n}{z} \neq 1$ then $\frac{n}{z} \geq 4$ (since it must be a positive integer and cannot be 2 or 3). Rearranging this says that if $n \neq z$ then $z \leq \frac{z}{4}$, which is precisely what we were hoping to show! □

   (b) Show that these bounds are optimal. That is, give examples of a group where $z = n$, and one where $z = \frac{n}{4}$.

   Proof. Any abelian group (for example Z_2) satisfies $z = n$.

   Next consider D_8, whose center was computed in to be $\{1, r^2\}$ in HW6 Problem 2. In this case $n = 8$ and $z = 2$ which is indeed $\frac{n}{4}$.

   A second example is Z_8, whose center was computed to be $\{\pm 1\}$ in HW6 Problem 5(g). Again in this case $n = 8$ and $z = 2$. □

Now let's think about some special ideals in commutative unital rings. We remind the reader of the following definition.

Definition 1. *Let R be a commutative unital ring. An ideal $\mathfrak{p} \subseteq R$ is called a prime ideal if $\mathfrak{p} \neq R$ and for any $a, b \in R$, if $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.*

2. Let R be a commutative ring with $1 \neq 0$. Recall that in ideal $\mathfrak{m} \subseteq R$ is maximal if and only if $R/\mathfrak{m}$ is a field. We will see there is a similar characterization of primality.

   (a) Prove that an ideal $\mathfrak{p} \subseteq R$ is prime if and only if the quotient ring $R/\mathfrak{p}$ is an integral domain.

   Proof. Suppose that $R/\mathfrak{p}$ is an integral domain. If $R = \mathfrak{p}$ then $R/\mathfrak{p} = \{0\}$ is the zero ring, which is not an integral domain (which requires $1 \neq 0$), so $\mathfrak{p} \subsetneq R$. Now fix $a, b \in R$ with product $ab \in \mathfrak{p}$. We must show that one of a or b are in $\mathfrak{p}$. Reducing modulo $\mathfrak{p}$ we see that $(a + \mathfrak{p})(b + \mathfrak{p}) = (ab + \mathfrak{p}) = 0$. Since $R/\mathfrak{p}$ has no zero divisors, we know either $a + \mathfrak{p}$ or $b + \mathfrak{p}$ must by zero. But if $a + \mathfrak{p} = 0$ then $a \in \mathfrak{p}$ and similarly if $b + \mathfrak{p} = 0$ then $b \in \mathfrak{p}$. This shows that $\mathfrak{p}$ is prime.

Conversely, suppose $\mathfrak{p}$ is prime, we must show that $R/\mathfrak{p}$ is an integral domain. The fact that it is commutative follows because R is, and $1+\mathfrak{p}$ serves as a multiplicative unit so it is unital. Furthermore, $1+\mathfrak{p} \neq 0$ because otherwise $1 \in \mathfrak{p}$ so that $\mathfrak{p} = R$ by HW13 Problem 6(c), and prime ideals must be proper. Therefore we have shown that $R/\mathfrak{p}$ is a commutative ring with $1 \neq 0$. It remains to show there are no nontrivial zero divisors. Fix two elements $(a+\mathfrak{p}), (b+\mathfrak{p}) \in R/\mathfrak{p}$ whose product is 0. This means that $ab+\mathfrak{p} = 0+\mathfrak{p} \in R/\mathfrak{p}$, or equivalently that $ab \in \mathfrak{p}$. By primality, this means that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which means that either $a+\mathfrak{p} = 0$ or $b+\mathfrak{p} = 0$, as desired. □

(b) Prove that a maximal ideal $\mathfrak{m} \subseteq R$ is prime.

Proof. Observe that $R/\mathfrak{m}$ is a field, which by definition is a commutative ring with $1 \neq 0$ such that every nonzero element is a unit. By HW12 Problem 2(b) units cannot be zero divisors, so $R/\mathfrak{m}$ has no nontrivial zero divisors, and is therefore an integral domain. Thus by part (a) $\mathfrak{m}$ is prime. □

(c) What are all the prime ideals of $\mathbb{Z}$?

Proof. We first observe that the ideals of $\mathbb{Z}$ are precisely the ideals (m) for $m \in \mathbb{Z}$. Indeed, an ideal must in particular be an additive subgroup. Subgroups of cyclic groups are cyclic, so we know that all the additive subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. But these are precisely the multiples of m, which is exactly the ideal (m) generated by m.

We claim that the prime ideals of $\mathbb{Z}$ are (0) and (p) for $p \in \mathbb{Z}$ prime. Indeed, $\mathbb{Z}/(0) \cong \mathbb{Z}$ is an integral domain, so (0) is prime by part (a), and $\mathbb{Z}/(p) \cong \mathbb{F}_p$ is a field, so that (p) is prime by part (b).

To conclude we consider $m \in \mathbb{Z}$ nonzero and not prime. We must show (m) is not prime. If $m = \pm 1$ then $(m) = \mathbb{Z}$ (by HW13 problem 6(a)) so that (m) is not prime. Else we can factor $m = ab$ for $1 < |a|, |b| < |m|$. Then $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ are nonzero, but $\overline{a}\overline{b} = \overline{m} = 0 \in \mathbb{Z}/m\mathbb{Z}$, so that $\mathbb{Z}/m\mathbb{Z}$ has zero divisors and is therefore not a domain. □

(d) Prove that the ideal $(x) \subseteq \mathbb{Z}[x]$ is prime but not maximal.

Proof. We know that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ which is an integral domain (so that (x) is prime), but not a field (so that (x) is not maximal). □

3. Let $\varphi : R \to S$ be a homomorphism between commutative unital rings with $\varphi(1_R) = 1_S$.

(a) Let $\mathfrak{q} \subseteq S$ be a prime ideal. Show that $\varphi^{-1}(\mathfrak{q})$ is a prime ideal of R.

Proof. We present two proofs. The first is direct. We first must show $\varphi^{-1}(\mathfrak{q})$ is a proper ideal. But $1_R \notin \varphi^{-1}(\mathfrak{q})$ because $\varphi(1_R) = 1_S \notin \mathfrak{q}$ since $\mathfrak{q}$ is proper and therefore cannot contain 1_S (say by HW 13 Problem 6(c)). Now let $x, y \in R$ with $xy \in \varphi^{-1}(\mathfrak{q})$. Then $\varphi(xy) = \varphi(x)\varphi(y) \in \mathfrak{q}$, so that $\varphi(x) \in \mathfrak{q}$ or else $\varphi(y) \in \mathfrak{q}$ (by the primality of $\mathfrak{q}$). This in turn implies that either x or y are in $\varphi^{-1}(\mathfrak{q})$, which implies primality of $\varphi^{-1}(\mathfrak{q})$.

Here's another proof I consider cuter. Consider the composition $R \to S \to S/\mathfrak{q}$. The kernel of this map is plainly $\varphi^{-1}(\mathfrak{q})$, so that by the first isomorphism theorem we obtain an injective unital ring homomorphisms $R/\varphi^{-1}(\mathfrak{q}) \hookrightarrow S/\mathfrak{q}$. Since $\mathfrak{q}$ is prime, $S/\mathfrak{q}$ is an integral domain. Therefore $R/\varphi^{-1}(\mathfrak{q})$ is isomorphic to a subring of an integral domain, so it cannot have any zero divisors (else $S/\mathfrak{q}$ would), must be commutative, and must have $1 \neq 0$. This in turn implies $\varphi^{-1}(\mathfrak{q})$ is prime. □

(b) Suppose φ is surjective, and $\mathfrak{m} \subseteq S$ is a maximal ideal. Show that $\varphi^{-1}(\mathfrak{m})$ is a maximal ideal of R.

Proof. Consider the composition $R \to S \to S/\mathfrak{m}$. The composition is surjective, and the kernel is $\varphi^{-1}(\mathfrak{m})$. Therefore by the first isomorphism theorem, $R/\varphi^{-1}(\mathfrak{m}) \cong S/\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $S/\mathfrak{m}$ is a field, and therefore so is $R/\varphi^{-1}(\mathfrak{m})$, so that $\varphi^{-1}(\mathfrak{m})$ is maximal in R.

Here's another proof using the fourth isomorphism theorem. Since $S \cong R/\ker\varphi$, there is an inclusion preserving bijection between ideals of S and those of R containing $\ker\varphi$. In particular, an ideal I with $\varphi^{-1}(\mathfrak{m}) \subseteq I \subsetneq R$ corresponds to an ideal $\mathfrak{m} \subseteq \overline{I} \subsetneq S$. The maximality of $\mathfrak{m}$ shows that $\overline{I} = \mathfrak{m}$, so that $I = \varphi^{-1}(\mathfrak{m})$. □

(c) Give a counterexample to part (b) if φ is not surjective.

Proof. Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Then the 0 ideal is maximal in $\mathbb{Q}$ (by HW13 Problem 6(d)), but its preimage in $\mathbb{Z}$ is also the zero ideal, which is not maximal, since for any $n \geq 2$ we have $0 \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}$. □

4. In this exercise we calculate the intersection of all the maximal ideals in a commutative unital ring R. Given a ring R, we define the *Jacobson radical* of R to be the ideal:

$$\mathfrak{J}(R) = \bigcap_{\mathfrak{m} \subseteq R \text{ maximal}} \mathfrak{m}.$$

(a) Show that $\mathfrak{N}(R) \subseteq \mathfrak{J}(R)$.

Proof. We first record the following inductive characterization of primality.

Lemma 2. *Let $\mathfrak{p}$ be prime, and $a_1, \cdots, a_t \in R$ such that the product $a_1 a_2 \cdots a_t \in \mathfrak{p}$. Then at least one of the $a_i \in \mathfrak{p}$.*

Proof. We proceed by induction. The base case for $t = 1$ is trivial. For the general case, notice that if:

$$a_1 a_2 \cdots a_t = (a_1)(a_2 \cdots a_t) \in \mathfrak{p},$$

then either $a_1 \in \mathfrak{p}$ (in which case we win), or $a_2 \cdots a_t \in \mathfrak{p}$, in which case $a_i \in \mathfrak{p}$ for some $i = 2, \cdots, t$ by the inductive hypothesis. □

With this in hand we let $\mathfrak{m} \subseteq R$ be a maximal ideal, and fix $x \in \mathfrak{N}(R)$. We'd ike to show that $x \in \mathfrak{m}$. By nilpotence $x^n = 0 \in \mathfrak{m}$ (using that $\mathfrak{m}$ is an additive subgroup). Since $\mathfrak{m}$ is prime (by 2(b)), then Lemma 2 implies that $x \in \mathfrak{m}$. Since $\mathfrak{m}$ was an arbitrary maximal ideal, we see that $x \in \mathfrak{J}(R)$. □

(b) Show that an element $r \in R$ is a unit if and only if it is not contained in any maximal ideal.

Proof. Let r be a unit. If r is contained in some maximal ideal $\mathfrak{m}$, that ideal must be all of R by HW13 Problem 5(c). But maximal ideals are proper, so this cannot be. Therefore units aren't contained in maximal ideals. Conversely, suppose r is not contained in any maximal ideal. If (r) were a proper ideal, it would have to be contained in some maximal ideal, so this says that (r) isn't proper, that is, $(r) = R$. By HW13 Problem 5(a) we may conclude that r is a unit. □

(c) Suppose $\mathfrak{m}$ is a maximal ideal and $r \in R \setminus \mathfrak{m}$. Compute the ideal $(\mathfrak{m}, r)$ generated by $\mathfrak{m}$ and r.

Proof. Notice that $\mathfrak{m} \subseteq (\mathfrak{m}, r) \subseteq R$. Since $r \in (\mathfrak{m}, r) \setminus \mathfrak{m}$, we see that $\mathfrak{m} \neq (\mathfrak{m}, r)$. By the maximality of $\mathfrak{m}$, we conclude that $(\mathfrak{m}, r) = R$. □

(d) Prove that $r \in \mathfrak{J}(R)$ if and only if $1 - ry \in R^\times$ for every $y \in R$. (Parts (b) and (c) might help!)

Proof. Suppose $r \in \mathfrak{J}(R)$, then so is ry. If $1 - ry$ is not a unit, then $1 - ry \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, but so is ry (since it is in every maximal ideal), so that $1 - ry + ry = 1 \in \mathfrak{m}$, implying that $\mathfrak{m} = R$, contradicting that it is a maximal ideal. Therefore $1 - ry$ must be a unit.

Conversely, if $r \notin \mathfrak{J}(R)$ then $r \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. But then $(r, \mathfrak{m}) = R$, Therefore, there is some $y \in Y$ and $m \in \mathfrak{m}$ so that $ry + m = 1$. In particular, $1 - ry \in \mathfrak{m}$ and therefore is not a unit. □

5. Let's finish by exploring unit groups. For parts (a)-(c) we do not assume that R is commutative. 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.

(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). □

(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, $\varphi^\times(rs) = \varphi^\times(r)\varphi^\times(s)$. Finally, the restriction of an injective map is always 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 $\ker \varphi \subseteq \mathfrak{J}(R)$. Prove that the induced map $\varphi^\times : R^\times \to S^\times$ is surjective.

Proof. The crucial observation is that if $\varphi(r) \in S^\times$, then $r \in R^\times$. Assume this holds and fix $s \in S^\times$. Since φ is surjective, there is some r mapping to s, and by the previous sentence it must be a unit. To complete the proof, we must verify the first sentence of this paragraph. We will give two proofs.

First proof: notice that since $\ker \varphi$ 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.

Second proof: Suppose $\varphi(r)$ is a unit, and fix r' mapping to $\varphi(r)^{-1}$. Then $\varphi(1 - rr') = 1 - \varphi(r)\varphi(r)^{-1} = 0$, so that $1 - rr' \in \ker \varphi \subseteq \mathfrak{J}(R)$. Therefore applying 4(d) we know $rr' = 1 - (1 - rr) \in R^\times$. Therefore $r^{-1} = r'(rr')^{-1}$ and so r has has an inverse and is therefore a unit! □

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