Homework 7 (Due March 19, 2025)

Jack Hyatt
MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Let $\phi : R \to S$ be a ring homomorphism.

   (a) Let J be an ideal of R. Assume that ϕ is surjective. Prove that $\phi(J) := \{\phi(x) : x \in J\}$ is an ideal of S.

   Proof. Let $\phi(x), \phi(y) \in \phi(J)$. Then since ϕ is a homomorphism, $\phi(x) - \phi(y) = \phi(x - y) \in \phi(J)$. So $(\phi(J), +)$ is a subgroup of $(S, +)$.
   Let $\phi(x) \in \phi(J), s \in S$. Then since ϕ is surjective, $\exists y \in R$ s.t. $\phi(y) = s$. So $s\phi(x) = \phi(y)\phi(x) = \phi(yx) \in \phi(J)$.
   So $\phi(J)$ is an ideal of S. ∎

   (b) Give a counterexample to show that the conclusion from part a. does not hold if the assumption that ϕ is surjective is removed.

   Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be defined by $\phi(x) = x$. We have $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\phi(2\mathbb{Z}) = 2\mathbb{Z}$ is not an ideal of $\mathbb{Q}$ since $2 \in 2\mathbb{Z}$ and $\frac{1}{2} \cdot 2 \notin 2\mathbb{Z}$.

   (c) Let K be an ideal of S. Prove that $\phi^{-1}(K) := \{x \in R : \phi(x) \in K\}$ is an ideal of R.

   Proof. Let $x, y \in \phi^{-1}(K)$. Then $\phi(x), \phi(y) \in K$, meaning $\phi(x - y) \in K$. So, $x - y \in \phi^{-1}(K)$. So $(\phi^{-1}(K), +)$ is a subgroup of $(R, +)$.
   Let $x \in \phi^{-1}(K), r \in R$. Then since ϕ is a homomorphism and K is an ideal, $\phi(rx) = \phi(r)\phi(x) \in K$ because $\phi(r) \in S$ and $\phi(x) \in K$. So $rx \in \phi^{-1}(K)$.
   So $\phi^{-1}(K)$ is an ideal of R. ∎

2. Let R be a ring and I an ideal of R. Let $\pi : R \to R/I$ be the canonical projection, $\pi(x) = \overline{x}$. Prove that

   (a) If J is an ideal of R such that $I \subseteq J$, then $\pi^{-1}(\pi(J)) = J$.

Proof.

$$\pi^{-1}(\pi(J)) = \{x \in R : \overline{x} \in \pi(J)\}$$

Since $\pi(J) = \{\overline{x} : x \in J\}$, we can rewrite this as:

$$\pi^{-1}(\pi(J)) = \{x \in R : x + I = y + I \text{ for some } y \in J\}$$

This means $x - y \in I$, so we can express $x = y + i$ for some $i \in I$. Since $y \in I$ and $i \in I$, and $I \subseteq J$, it follows that $x \in J$. Thus, $\pi^{-1}(\pi(J)) \subseteq J$.

Let $x \in J$. Then $\pi(x) = \overline{x} \in \pi(J)$. By definition of preimage, we have that $x \in \pi^{-1}(\pi(J))$. So $J \subseteq \pi^{-1}(\pi(J))$.

So $\pi^{-1}(\pi(J)) = J$. ■

(b) If K is an ideal of R/I, then $\pi(\pi^{-1}(K)) = K$.

Proof. Consider the preimage under π:

$$\pi^{-1}(K) = \{x \in R : \overline{x} \in K\}.$$

Applying π to this set, we obtain:

$$\pi(\pi^{-1}(K)) = \{\pi(x) : x \in R, \overline{x} \in K\}.$$

Since $\pi(x) = \overline{x}$, this simplifies to:

$$\pi(\pi^{-1}(K)) = \{\overline{x} : \overline{x} \in K\}.$$

Since K consists of equivalence classes $\overline{x}$, we immediately conclude:

$$\pi(\pi^{-1}(K)) = K.$$

■

3. (a) Let R be a commutative ring and I an ideal of R. Let J be an ideal of R that contains I, and consider $\pi(J) = J/I$ as an ideal of R/I (as per the correspondence theorem). Prove that

$$\frac{R}{J} \cong \frac{\left(\frac{R}{I}\right)}{\left(\frac{J}{I}\right)}$$

Proof. By the correspondence theorem, the set $\pi(J) = J/I$ is an ideal of R/I. Consider the canonical projection $\pi : R \to R/I$ given by $\pi(x) = \overline{x} = x + I$. This induces a natural projection

$$\overline{\pi} : R/I \to (R/I)/(J/I)$$

given by $\overline{\pi}(\overline{x}) = \overline{x} + J/I$.

Define the map $\varphi : R \to (R/I)/(J/I)$ by

$$\varphi(x) = \overline{x} + J/I.$$

Since φ is the composition of two quotient maps, it is a ring homomorphism. The kernel of φ consists of elements $x \in R$ such that

$$\overline{x} + J/I = J/I,$$

which means $\overline{x} \in J/I$, or equivalently, $x \in J$. Thus, $\ker \varphi = J$.
By the F.H.T, we conclude that

$$\frac{R}{J} \cong \frac{\left(\frac{R}{I}\right)}{\left(\frac{J}{I}\right)},$$

as required.

■

(b) With notation as in part a., prove that J is a prime ideal of R if and only if $\frac{J}{I}$ is a prime ideal of $\frac{R}{I}$.

Proof. Suppose J is a prime ideal of R. To show that J/I is prime in R/I, assume that $\overline{ab} \in J/I$ for some $\overline{a}, \overline{b} \in R/I$. This means that $ab \in J$. Since J is prime, we must have either $a \in J$ or $b \in J$, implying $\overline{a} \in J/I$ or $\overline{b} \in J/I$. Thus, J/I is prime in R/I.

Conversely, suppose J/I is prime in R/I. Assume that $ab \in J$ for some $a, b \in R$. Then $\overline{ab} \in J/I$. Since J/I is prime, we must have $\overline{a} \in J/I$ or $\overline{b} \in J/I$, which means $a \in J$ or $b \in J$. Hence, J is prime in R.

So, J is prime in R if and only if J/I is prime in R/I.

■

4. Let $R = \mathbb{Z}[X]$ and let P be a prime ideal such that $(X) \subseteq P \subseteq (X, 5)$. Use the result from 3b. to prove that P must be equal to (X) or $(X, 5)$ (that is, there are no other prime ideals in between).

Proof. First, we want to quickly prove that isomorphisms preserve prime ideals. Let $\phi : R \to S$ be an isomorphism between rings R and S, and let P be a prime ideal of R. We want to check that $\phi(P)$ is a prime ideal (we already get that it is an ideal from problem 1).

Let $\phi(a)\phi(b) \in \phi(P)$. We then have $\phi(ab) \in \phi(P)$, giving $ab \in P$. And since P is prime, we have $a \in P$ or $b \in P$, which finally implies $\phi(a) \in \phi(P)$ or $\phi(b) \in \phi(P)$.

So isomorphisms preserve prime ideals.

From 3b, we know that P being a prime ideal of $\mathbb{Z}[X]$ with $(X) \subseteq P$ implies that $P/(X)$ is a prime ideal of $\mathbb{Z}[X]/(X)$. We also have that $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ with $\phi(\overline{a}) = a$ as the isomorphism.

Then we have $\phi(P/(X))$ is a prime ideal of $\mathbb{Z}$.

The only prime ideals in $\mathbb{Z}$ are (0) and (p) for prime numbers p. This means $P/(X)$ must either be $\overline{0}$ or $\overline{p}$.

Case 1: $P/(X) = \overline{0}$, corresponding to $P = (X)$.

Case 2: $P/(X) = \overline{p}$, meaning $P = (X, p)$. Since $P \subseteq (X, 5)$, that forces p to be 5. So $P = (X, 5)$. ∎

5. Prove that

   (a) $\frac{\mathbb{Z}[x]}{(2,x^2+5)} \cong \frac{\mathbb{Z}_2[x]}{(x^2+5)}$

   Proof. Let us first note that $(2) \subseteq (2, x^2+5)$. Then right away, problem 3a gives that

$$\frac{\mathbb{Z}[x]}{(2, x^2+5)} \cong \frac{\left(\frac{\mathbb{Z}[X]}{(2)}\right)}{\left(\frac{(2,x^2+5)}{(2)}\right)}.$$

   It is clear that $\frac{\mathbb{Z}[X]}{(2)} \cong \mathbb{Z}_2[X]$ and $\frac{(2,x^2+5)}{(2)} \cong (x^2+5)$. So we easily get that

$$\frac{\mathbb{Z}[x]}{(2, x^2+5)} \cong \frac{\mathbb{Z}_2[x]}{(x^2+5)}$$

   ∎

   (b) $(2, x^2+5)$ is not a prime ideal of $\mathbb{Z}[x]$.

   Proof. To show that $(2, x^2+5)$ is not prime, we must find $f(x), g(x) \in \mathbb{Z}[x]$ such that

$$f(x)g(x) \in (2, x^2+5)$$

   but neither $f(x)$ nor $g(x)$ belongs to $(2, x^2+5)$.
   Consider $f(x) = x+1$ and $g(x) = x-1$. Then,

$$f(x)g(x) = (x+1)(x-1) = x^2 - 1.$$

   We rewrite this as

$$x^2 - 1 = x^2 + 5 - 3 \cdot 2 \in (2, x^2+5),$$

   However $f(x) = x + 1 \notin (2, x^2+5)$ and $g(x) = x - 1 \notin (2, x^2+5)$. This is easy to see since their linear combination $a \cdot 2 + b \cdot (x^2+5)$ both require b to be 0, which immediately fails since they are not strictly a multiple of 2. ∎

6. (a) Let R, S be rings and let $(r, s) \in R \times S$. Prove that $(r, s) \in (R \times S)^* \iff r \in R^*$ and $s \in S^*$.

Proof. An element $(r, s) \in R \times S$ is a unit if and only if there exists an element $(r', s') \in R \times S$ such that

$$(r, s)(r', s') = (1, 1).$$

Expanding the product in the direct product ring,

$$(rr', ss') = (1, 1).$$

This implies that $rr' = 1$ in R and $ss' = 1$ in S, which means that $r \in R^*$ and $s \in S^*$.

Conversely, if $r \in R^*$ and $s \in S^*$, then there exist elements $r' \in R$ and $s' \in S$ such that $rr' = 1$ and $ss' = 1$. Then, (r', s') is an inverse of (r, s), proving that $(r, s) \in (R \times S)^*$. ∎

(b) Use the result from part a. and the Chinese Remainder Theorem to find and prove a formula for the number of units in $\mathbb{Z}_N$, in terms of the prime factorization of n.

Proof. The units in $\mathbb{Z}_{p^k}$ are elements that are coprime to p^k. The total number of elements in $\mathbb{Z}_{p^k}$ is p^k, and the number of elements that are divisible by p is p^{k-1} since they are of the form mp for $m = 0, 1, 2, \dots, p^{k-1} - 1$.

Let N have the prime factorization

$$N = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}.$$

Since we know $\mathbb{Z}_N \cong \frac{\mathbb{Z}}{(N)}$, the Chinese Remainder Theorem gives us an isomorphism:

$$\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

By part (a), the number of units in $\mathbb{Z}_N$, is the product of the number of units in each factor, giving

$$o(\mathbb{Z}_n^*) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_m^{k_m} - p_m^{k_m-1}).$$

∎