Solutions to Homework 5

1. Recall that an ideal $P \subsetneq R$ is called *prime* if for all $a, b \in R$ with $ab \in P$ we have $a \in P$ or $b \in P$.

a. Suppose that $S \subset R$ is a subring, and let $Q = P \cap S$. Prove that if P is a prime ideal in R then Q is a prime ideal in S.

Solution: First we show that Q is an ideal. For $a, b \in Q = P \cap S$, we have $a + b \in P$ because P is an ideal, and $a + b \in S$ because S is a subring, so $a + b \in Q$. If $s \in S$ and $a \in Q$, then $sa \in P$ because $s \in R$, $a \in P$, and P is an ideal; and $sa \in S$ because S is a subring; so $sa \in Q$. Also, Q is not empty: we have $0 \in P$ and $0 \in S$, so $0 \in P \cap S = Q$.

Next we show that Q is a proper subset of S. If not, then $1 \in Q$, so $1 \in P$, so $P = R$, but we assumed that $P \subsetneq R$.

Finally, suppose that we have $a, b \in S$ with $ab \in Q$. Then $ab \in P$, so $a \in P$ or $b \in P$ because P is a prime ideal. Because $a \in S$ and $b \in S$, we conclude that $a \in Q$ or $b \in Q$.

b. Let $P = \langle 2+i \rangle \subset \mathbb{Z}[i]$, which is a prime ideal because $2+i$ is irreducible. Consider the subring $\mathbb{Z} \subset \mathbb{Z}[i]$ and the intersection $Q = P \cap \mathbb{Z}$. Then Q is a prime ideal of $\mathbb{Z}$, so it's either $\langle 0 \rangle$ or $\langle p \rangle$ for some prime number $p \in \mathbb{Z}$. Which one is it, and if it's the latter, what is p? Give a proof.

Solution: I claim that $Q = \langle 5 \rangle$. We have $5 = (2 + i)(2 - i)$, so $5 \in P$, and $5 \in \mathbb{Z}$, so $5 \in Q$. Thus Q cannot be $\langle 0 \rangle$, but must be $\langle p \rangle$ for some prime number $p \in \mathbb{Z}$. Because $5 \in Q$ we have $p \mid 5$, so $p = 5$.

c. Let $z \in \mathbb{Z}[i]$ be irreducible. Prove that there is a prime number $p \in \mathbb{Z}$ such that z divides p in $\mathbb{Z}[i]$, by considering the ideal $P = \langle z \rangle$ and the intersection $Q = P \cap \mathbb{Z}$. Conclude that either $|z|^2 = p$ or $|z|^2 = p^2$.

Solution: Because z is irreducible, $P = \langle z \rangle$ is a prime ideal of $\mathbb{Z}[i]$, so $Q = P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ by part (a). Thus Q is either $\langle 0 \rangle$ or $\langle p \rangle$ for some prime number $p \in \mathbb{Z}$.

Write $z = a + bi$. Then $z\bar{z} = (a + bi)(a - bi) = a^2 + b^2$ is in P, and it's in $\mathbb{Z}$, so it's in Q. And because $z \neq 0$ we have $a^2 + b^2 \neq 0$, so $Q \neq \langle 0 \rangle$.

Thus $Q = \langle p \rangle$ for some prime number $p \in \mathbb{Z}$. Because $p \in Q$ we have $p \in P$, so $p = zw$ for some $w \in \mathbb{Z}[i]$. Taking norms, we get $p^2 = |z|^2|w|^2$, and in particular $|z|^2$ divides p^2. Because z is not a unit, we have $|z|^2 \neq 1$, so either $|z|^2 = p$ or $|z|^2 = p^2$.

§4.3 #6. Prove that $\mathbb{Z}[i]$ is a principal ideal domain: that is, for every ideal $I \subset \mathbb{Z}[i]$ there is an element $z \in \mathbb{Z}[i]$ such that $I = \langle z \rangle$. Emulate the proof of §4.1 Proposition 1.2, which uses the same ideas as §1.2 Theorem 2.3 and §3.1 Theorem 1.6.

Solution: If $I = \{0\}$ then we're done, because $\{0\} = \langle 0 \rangle$. If not, choose a non-zero $z \in I$ such that $|z|^2$ is as small as possible: that is, for any non-zero $w \in I$ we have $|z|^2 \leq |w|^2$. I claim that $I = \langle z \rangle$. Because $z \in I$ we have $\langle z \rangle \subset I$ by problem 1 of homework 1. To prove the reverse inclusion, let $w \in I$. By the division algorithm, we can write $w = qz + r$ for some $q, r \in \mathbb{Z}[i]$ with $|r|^2 < |z|^2$. If $r \neq 0$ then this contradicts our choice of z, because $r = w - qz$, so $r \in I$ because I is an ideal, but $|r|^2 < |z|^2$. So we must have $r = 0$, so $w = qz$, so $w \in \langle z \rangle$ as desired.

Based on §4.3 #16. Let R be a commutative ring, let $a, b \in R$, let $S = R/\langle a \rangle$, and let $T = S/\langle \bar{b} \rangle$, where $\bar{b} \in S$ is the equivalence class of b modulo $\langle a \rangle$. Prove that $T \cong R/\langle a, b \rangle$.

Solution: Let $\phi\colon R \to S$ be the map $\phi(r) = \bar{r}$, and let $\psi\colon S \to T$ be the map $\psi(s) = \bar{s}$. These are both surjective homomorphisms, so the composition $\psi \circ \phi\colon R \to T$ is also surjective and a homomorphism. Perhaps annoyingly, we will write

$$\psi(\phi(r)) = \psi(\bar{r}) = \bar{\bar{r}},$$

where the lower bar means an equivalence class modulo $\langle a \rangle \subset R$ and the upper one means an equivalence class modulo $\langle \bar{b} \rangle \subset S$.

By the first isomorphism theorem, it is enough to prove that

$$\ker(\psi \circ \phi) = \langle a, b \rangle.$$

In $S = R/\langle a \rangle$ we have $\bar{a} = \bar{0}$, and in $T = S/\langle \bar{b} \rangle$ we have $\bar{\bar{b}} = \bar{\bar{0}}$, so

$$\begin{aligned} \psi(\phi(a)) &= \psi(\bar{a}) = \psi(\bar{0}) = \bar{\bar{0}} \\ \psi(\phi(b)) &= \psi(\bar{b}) = \bar{\bar{b}} = \bar{\bar{0}}. \end{aligned}$$

Thus $a \in \ker(\psi \circ \phi)$ and $b \in \ker(\psi \circ \phi)$, so $\langle a, b \rangle \subset \ker(\psi \circ \phi)$ by problem 1 of homework 1.

For the reverse inclusion, suppose that $r \in \ker(\psi \circ \phi)$, or equivalently, $\bar{\bar{r}} = \bar{\bar{0}}$. Then $\bar{r} = s \cdot \bar{b}$ for some $s \in S$, and we can write $s = \bar{y}$ for some $y \in R$, so $\bar{r} = \bar{y} \cdot \bar{b} = \overline{yb}$. Thus $r - yb = xa$ for some $x \in R$, so $r = xa + yb$, so $r \in \langle a, b \rangle$.

(If you found this confusing, I encourage you again to check out the extra notes from Lecture 14.)