**Section 3.3**

1. (Problem 20) Let $R$ be a commutative ring.

   (a)

   (b) Prove that if $R$ is finite, then every prime ideal of $R$ is maximal.

   **Solution:** Let $P$ be a prime ideal of $R$. Then $R/P$ is an integral domain, but $R/P$ is finite because $R$ is finite, so we can invoke the fact that finite integral domains are fields (Section 3.2 Theorem 3) to see that $R/P$ is a field. Thus we conclude $P$ is maximal.

   (c) Is every prime ideal of $\mathbf{Z}$ maximal?

   **Solution:** No, because $\langle 0 \rangle$ is a prime ideal of $\mathbf{Z}$ (for instance, because $\mathbf{Z}$ is an integral domain) but it is not maximal because we have proper inclusions $\langle 0 \rangle \subset \langle 2 \rangle \subset \mathbf{Z}$.

**Section 3.4**

2. (Problem 33) Prove the Third Isomorphism Theorem: If $A \subseteq B \subseteq R$, where $A$ and $B$ are ideals of $R$, then $B/A = \{b + A \mid b \in B\}$ is an ideal of $R/A$ and $(R/A)/(B/A) \cong R/B$.

**Solution:** Consider the projection homomorphism $\varphi : R \to R/B$, i.e. $\varphi(r) = r + B$. We have $B = \ker \varphi$, and in particular $A \subseteq \ker \varphi$, so the universal property of quotients implies that there is an induced homomorphism $\overline{\varphi} : R/A \to R/B$ satisfying $\varphi = \overline{\varphi} \circ \pi$ (where $\pi : R \to R/A$ is the projection $\pi(r) = r + A$), explicitly given by $\overline{\varphi}(r + A) = r + B$. Notice $\overline{\varphi}$ is clearly surjective, and it is simple to check the kernel is exactly $B/A$ (in particular, $B/A$ is an ideal of $R/A$); now the first isomorphism theorem implies $(R/A)/(B/A) \cong R/B$.

3. (Problem 44(a)) Let $A_1, A_2, \ldots, A_n$ be ideals of $R$ and write $A = \bigcap_{i=1}^n A_i$. Prove that $R/A$ is isomorphic to a subring of $R/A_1 \times \cdots \times R/A_n$.

**Solution:** Define $\varphi : R \to R/A_1 \times \cdots \times R/A_n$ by $\varphi(r) = (r+A_1, \ldots, r+A_n)$. It is straightfoward to check this is a ring homomorphism, for instance for additivity we have if $r, r' \in R$

$$\begin{aligned}\varphi(rr') &= (rr' + A_1, \ldots, rr' + A_n) \\ &= ((r + A_1)(r' + A_1), \ldots, (r + A_n)(r' + A_n)) \\ &= (r + A_1, \ldots, r + A_n)\cdot(r' + A_1, \ldots, r' + A_n) \\ &= \varphi(r)\varphi(r').\end{aligned}$$

Furthermore, we calculate the kernel as follows:

$$\begin{aligned}\ker \varphi &= \{r \in R \mid (r + A_1, \ldots, r + A_n) = (0 + A_1, \ldots, 0 + A_n)\} \\ &= \{r \in R \mid r + A_i = 0 + A_i \text{ for } i = 1, \ldots, n\} \\ &= \{r \in R \mid r \in A_i \text{ for } i = 1, \ldots, n\} \\ &= \bigcap_{i=1}^n A_i \\ &= A.\end{aligned}$$

**Section 4.1**

4. (Problem 24)

   (a) Show that $x^p - x$ annihilates $\mathbf{Z}_p$.
   (c) If $p \neq 2$ is prime, show $x^p - x$ annihilates $\mathbf{Z}_{2p}$.

**Solution:**

(a) If $a \in \mathbf{Z}$, write $\bar{a}$ for its corresponding element of $\mathbf{Z}_p$. Recall if $a$ is an integer then Fermat's little theorem tells us that $a^p \equiv a \pmod p$; thus $\bar{a}^p = \overline{a^p} = \bar{a}$ for all $\bar{a} \in \mathbf{Z}_p$. Subtracting we see $\bar{a}^p - \bar{a} = 0$ for any $\bar{a} \in \mathbf{Z}_p$, and this shows $x^p - x$ annihilates $\mathbf{Z}_p$.

(c) Recall because 2 and $p$ are coprime, there exists an isomorphism $\varphi : \mathbf{Z}_{2p} \to \mathbf{Z}_2 \times \mathbf{Z}_p$. Now using the fact that $\varphi$ is an isomorphism we have for $z \in \mathbf{Z}_{2p}$

$$z^p - z = 0 \iff \varphi(z^p - z) = 0 \iff \varphi(z)^p - \varphi(z) = 0,$$

so to show $x^p - x$ annihilates $\mathbf{Z}_{2p}$ is the same as showing that $x^p - x$ annihilates $\mathbf{Z}_2 \times \mathbf{Z}_p$. But if $(a, b) \in \mathbf{Z}_2 \times \mathbf{Z}_p$ then $a^p - a = 0$ (the only possibilities are $a = 0$ and $a = 1$, so $a^p = a$ regardless), and we have $b^p - b = 0$ by part (a), so we have

$$(a, b)^p - (a, b) = (a^p, b^p) - (a, b) = (a^p - a, b^p - b) = (0, 0),$$

which shows $x^p - x$ annihilates $(a, b)$. Since $(a, b)$ was an arbitrary element of $\mathbf{Z}_2 \times \mathbf{Z}_p$ this proves $x^p - x$ annihilates $\mathbf{Z}_2 \times \mathbf{Z}_p$ and we are done.

5. (Problem 26) Show that $\sqrt[n]{m}$ is not rational unless $m = k^n$ for some integer $k$ (where $n$ and $m$ are integers and $n$ is positive).

**Solution:** Suppose $q = \sqrt[n]{m}$ is rational; then $q$ is a root of the polynomial $x^n - m$. If we write $q = a/b$ where $a$ and $b$ are coprime integers, then we can use the Rational Root Theorem to deduce that $a$ divides the constant term of $x^n - m$ and $b$ divides the leading coefficient. But the leading coefficient of $x^n - m$ is 1, so $b \mid 1$, or in other words $b = \pm 1$, and thus $q = \pm a$, which is an integer, so taking $k = q \in \mathbf{Z}$ we have $m = k^n$ as desired.