From the text (pages 98 – 106): 9, 14, 18

1. Recall that if R is a ring, then R^* denotes the group of units of R. Also, if n is a natural number, then the Euler phi function is defined as

$$\varphi(n) = |\mathbb{Z}_n^*| = |\{m : 1 \leq m < n \text{ with } \gcd(n, m) = 1\}|.$$

   (a) If R and S are rings, show that $(R \times S)^* \cong R^* \times S^*$.

   (b) Verify that φ is a multiplicative function. That is, show that $\varphi(nm) = \varphi(n)\varphi(m)$ if n and m are relatively prime. (*Hint:* Part (a) may be useful.)

   (c) If p is a prime, show that $\varphi(p^k) = p^k - p^{k-1}$.

   (d) Prove the following formula for $\varphi(n)$:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right),$$

   where $p_1, \ldots, p_k$ are the distinct prime divisors of n.

2. Let $\varphi : R \to S$ be a homomorphism of commutative rings. Recall that if $A \subseteq S$, then $\varphi^{-1}(A) = \{r \in R : \varphi(r) \in A\}$

   (a) Prove that if P is a prime ideal of S, then $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case where R is a subring of S and φ is the inclusion homomorphism to conclude that if P is a prime ideal of S, then $P \cap R$ is a prime ideal of R.

   (b) Prove that if M is a maximal ideal of S and φ is surjective, then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

3. Assume that R is commutative and let $f(X) \in R[X]$ be a monic polynomial of degree $n \geq 1$. Let $S = R[X]/\langle f(X)\rangle$ be the quotient ring. Thus, a typical element of S is a coset $p(X) + \langle f(X)\rangle$, which we will denote more succinctly by the bar notation $\overline{p(X)}$.

   (a) Show that every element of S is of the form $\overline{p(X)}$ for some polynomial $p(X) \in R[X]$ of degree less than n. That is,

$$R[X]/\langle f(X)\rangle = \left\{\overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}} : a_0, a_1, \ldots, a_{n-1} \in R\right\}.$$

   (b) Prove that if $p(X)$ and $q(X)$ are distinct polynomials in $R[X]$ which are both of degree less than n, then $\overline{p(X)} \neq \overline{q(X)}$. Thus, the representation of elements of $R[X]/\langle f(X)\rangle$ given in part (a) is unique.

   (c) If $f(X) = a(X)b(X)$ where $a(X)$ and $b(X)$ have degree less than n, prove that $\overline{a(X)}$ is a zero divisor in $R[X]\langle f(X)\rangle$.

4. Let $f(X) = X^2 + X + 1 \in \mathbb{Z}_2[X]$, and use the bar notation introduced in the previous exercise to denote passage to the quotient ring $S = \mathbb{Z}_2[X]/\langle f(X)\rangle$.

(a) Show that S has 4 elements: $\overline{0}$, $\overline{1}$, $\overline{X}$, and $\overline{X+1}$.

(b) Write out the addition table for S and deduce that the additive group of S is isomorphic to the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Write out the multiplication table for S and prove that S^* is isomorphic to the cyclic group of order 3. Deduce that S is a field.

5. Let $f(X) = X^3 - 2X + 1 \in \mathbb{Z}[X]$, and use bar notation to denote passage to the quotient ring $S = \mathbb{Z}[X]/\langle f(X)\rangle$. Let $p(X) = 2x^7 - 7X^5 + 4X^3 - 9X + 1$ and let $q(X) = (X-1)^4$.

(a) Express each of the following elements of S in the form $\overline{g(X)}$ for some polynomial $g(X)$ of degree ≤ 2: $\overline{p(X)}$, $\overline{q(X)}$, $\overline{p(X)+q(X)}$, $\overline{p(X)q(X)}$.

(b) Prove that S is not an integral domain.

(c) Prove that $\overline{X}$ is a unit in S.