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 $(R \times S)^* \cong R^* \times S^*$.

▶ **Solution.** Since $(r, s)(t, v) = (rt, sv) = (1, 1)$ if and only if $rt = 1$ and $sv = 1$, it follows that $(r, s) \in (R \times S)^*$ if and only if $r \in R^*$ and $s \in S^*$. Thus, the identity map $I : R \times S \to R \times S$ takes $(R \times S)^*$ bijectively to $R^* \times S^*$, and the identity map is multiplicative, so it is a group isomorphism. ◀

(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.)

▶ **Solution.** According to the Chinese Remainder Theorem (see Corollary 2.25, Page 66), if m and n are relatively prime, there is an isomorphism of *rings*:

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Then using part (a) and the definition of φ given above:

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |(\mathbb{Z}_m \times \mathbb{Z}_n)^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*|\,|\mathbb{Z}_n^*| = \varphi(m)\varphi(n).$$

◀

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

▶ **Solution.** To compute $\varphi(p^k)$, it is necessary to find the number of integers between 1 and p^k that are not divisible by p (since $\gcd(p^k, m) = 1$ if and only if $p \nmid m$), that is, if and only if m is not a multiple of p. But the multiples of p less than or equal to p^k are the integers pr where $1 \leq r \leq p^{k-1}$, a total of p^{k-1} integers. Hence there are $p^k - p^{k-1}$ integers between 1 and p^k that are *not* multiples of p. Hence $\varphi(p^k) = p^k - p^{k-1}$. ◀

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

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

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

▶ **Solution.** Write n in its prime factorization

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where each exponent $r_i \geq 1$. Then using parts (b) and (c) gives

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) \\
&= \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}) \\
&= (p_1^{r_1} - p_1^{r_1-1})(p_2^{r_2} - p_2^{r_2-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}) \\
&= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) p_2^{r_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{r_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

◀

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.

   ▶ **Solution.** First observe that if $I \subseteq S$ is any ideal, then $\varphi^{-1}(I)$ is an ideal of R. To see this, note that if a and b are in $\varphi^{-1}(I)$ and $r \in R$, then $\varphi(a) \in I$ and $\varphi(b) \in I$, while $\varphi(r) \in S$. Since φ is a ring homomorphism and I is an ideal of S, it follows that $\varphi(a-b) = \varphi(a) - \varphi(b) \in I$, and $\varphi(ra) = \varphi(r)\varphi(a) \in I$. Hence $a - b$ and ra are in $\varphi^{-1}(I)$. Now suppose that $ab \in \varphi^{-1}(P)$. This means that $\varphi(ab) \in P$. But $\varphi(ab) = \varphi(a)\varphi(b)$. Since P is prime, it follows that $\varphi(a)$ or $\varphi(b)$ is in P, which means that a or b is in $\varphi^{-1}(P)$. Hence $\varphi^{-1}(P)$ is prime once we have observed that $\varphi^{-1}(P) \neq R$. But $\varphi(1_R) = 1_S \notin P$ (since P is a prime ideal of S) so that $1_R \notin \varphi^{-1}(P)$.
   If R is a subring of S, then let φ be the inclusion map $\varphi(r) = r$. Then $\varphi^{-1}(P) = P \cap R$ in this situation, so $P \cap R$ is a prime idea of R whenever P is a prime ideal of S. ◀

   (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.

   ▶ **Solution.** Let $\pi : S \to S/M$ be the canonical projection map onto the quotient ring, and let $\psi = \pi \circ \varphi$ so that $\psi : R \to S/M$ by means of the formula $\psi(r) = \varphi(r) + M$. Thus, $\operatorname{Ker}(\psi) = \{r \in R : \varphi(r) \in M\} = \varphi^{-1}(M)$. Since φ is surjective it follows that ψ is surjective (if $s + M \in S/M$ and $\varphi(r) = s$ then $\psi(r) = s + M$). Thus,

$$R/\varphi^{-1}(M) = R/\operatorname{Ker}(\psi) \cong \operatorname{Im}(\psi) = S/M,$$

and since M is a maximal ideal of S, S/M is a field. Hence, $R/\varphi^{-1}(M)$ is a field and $\varphi^{-1}(M)$ is a maximal ideal of R.

For an example where the result fails if φ is not surjective, let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion homomorphism $\varphi(n) = n$. Then $M = \{0\}$ is a maximal ideal of the field $\mathbb{Q}$, but $\varphi^{-1}(M) = \{0\}$ is not a maximal ideal of $\mathbb{Z}$. ◀

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,

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

   ▶ **Solution.** Let $g(X) \in R[X]$ be arbitrary. By the division algorithm, we can write $g(X) = f(X)q(X) + p(X)$ where $p(X)$ is 0 or $\deg p(X) < n$. Applying the bar notation is a ring homomorphism (it is just the projection map $h(X) \mapsto h(X) + \langle f(X)\rangle$). Thus

$$\overline{g(X)} = \overline{f(X)q(X)} + \overline{p(X)} = \overline{p(X)}.$$

   Since $\deg p(X) \leq n - 1$, $\overline{p(X)}$ has the requested form. ◀

   (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.

   ▶ **Solution.** $\overline{p(X)} = \overline{q(X)}$ if and only if $f(X)$ divides $p(X) - q(X)$. Since $\deg f(X) = n$ and $\deg(p(X) - q(X)) < n$ unless $p(X) - q(X) = 0$, the only way that $f(X)$ can divide $p(X) - q(X)$ is if $p(X) - q(X) = 0$. That is, $\overline{p(X)} = \overline{q(X)}$ if and only if $p(X) = q(X)$. ◀

   (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 $R[X]/\langle f(X)\rangle$.

   ▶ **Solution.** It is only necessary to observe that $\overline{0} = \overline{f(X)} = \overline{a(X)b(X)}$ and by the previous part $\overline{a(X)} \neq \overline{0}$ and $\overline{b(X)} \neq \overline{0}$. ◀

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 $\overline{X+1}$.

   ▶ **Solution.** Since $\mathbb{Z}_2$ has two elements, namely, 0 and 1, there are 4 polynomials of degree < 2: 0, 1, X, and $X + 1$. By part (a) of the previous exercise, S has the 4 elements that are the bars of these 4 polynomials. ◀

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

► **Solution.**

$+$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\overline{0}$	$\overline{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\overline{1}$	$\overline{0}$

This group of order 4 has every element of order 2 (look at all the elements $\overline{0}$ on the diagonal). Thus, it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. ◄

(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.

► **Solution.**

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

$S^* = \left\{\overline{1}, \overline{X}, \overline{X+1}\right\}$ is a cyclic group of order 3 generated by $\overline{X}$ since $\overline{X}^2 = \overline{X+1}$ and $\overline{X}^3 = \overline{1}$. Since S^* is a group, 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: $\overline{p(X)}$, $\overline{q(X)}$, $\overline{p(X)+q(X)}$, $\overline{p(X)q(X)}$.

► **Solution.** Applying the division algorithm:

$$\begin{aligned} p(X) &= (X^3 - 2X + 1)(2X^4 - 3X^2 - 2X - 2) + (-X^2 - 11X + 3) \\ &= f(X)h_1(X) + (-X^2 - 11X + 3), \text{ and} \\ q(X) &= X^4 - 4X^3 + 6X^2 - 4X + 1 \\ &= (X^3 - 2X + 1)(X - 4) + (8X^2 - 13X + 5) \\ &= f(X)h_2(X) + (8X^2 - 13X + 5). \end{aligned}$$

Thus, $\overline{p(X)} = \overline{-X^2 - 11X + 3}$ and $\overline{q(X)} = \overline{8X^2 - 13X + 5}$. Since the bar operation is a ring homomorphism, it follows that

$$\overline{p(X) + q(X)} = \overline{7X^2 - 24X + 8},$$

while

$$\begin{aligned}\overline{p(X)q(X)} &= \overline{(-X^2-11X+3)(8X^2-13X+5)}\\ &= \overline{-8X^4-75X^3+162X^2-94X+15}\\ &= \overline{-8X^4}-\overline{75X^3}+\overline{162X^2-94X+15}\\ &= \overline{-8(2X^2-X)}-\overline{75(2X-1)}+\overline{162X^2-94X+15}\\ &= \overline{146X^2-236X+90}.\end{aligned}$$

Note that we have used the reductions $\overline{X}^3 = \overline{2X-1}$ and $\overline{X^4} = \overline{2X^2-X}$ which follow from the fact that $\overline{X^3-2X+1} = \overline{0}$ in S. ◀

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

▶ **Solution.** Since $f(X) = X^3-2X+1 = (X^2+X-1)(X-1)$ we conclude that

$$\overline{0} = \overline{f(X)} = \overline{(X^2+X-1)(X-1)}$$

and since $\overline{X^2+X_1}$ and $\overline{X-1}$ are both nonzero in S, we conclude that both of these elements are zero divisors, so that S is not an integral domain. ◀

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

▶ **Solution.** Note that $\overline{X(2-X^2)} = \overline{1}$ since $X(2-X^2)-1 = -f(X)$. Thus $\overline{X}$ is a unit with inverse $\overline{2-X^2}$. ◀

Text Exercises:

9. ▶ **Solution.** Ideals of $\mathbb{Z}_{60}$: Since $\mathbb{Z}_{60} = \mathbb{Z}/\langle 60\rangle$, the ideals of $\mathbb{Z}_{60}$ are all ideals of the form $I + \langle 60\rangle = \langle n\rangle$ where $I = \langle n\rangle$ is an ideal of $\mathbb{Z}$ containing $\langle 60\rangle$. Thus, the ideals of $\mathbb{Z}_{60}$ are the ideals $\langle n\rangle$ where n is a divisor of 60. Thus, $n = 1$, 2, 4, 3, 5, 6, 10, 12, 15, 20, 30, or 60. The prime ideals and the maximal ideals are those ideals in the above list where n is prime, i.e., $n = 2$, 3, or 5.

   The nilpotent elements of $\mathbb{Z}_{60}$ are the elements of the ideal $\langle 30\rangle$, since an integer a satisfies $a^m \equiv 0 \pmod{60}$ if and only if $60|a^m$ for some $m \in \mathbb{N}$ if and only if a is divisible by each of the prime divisors of 60, that is 2, 3, and 5. Hence, $a^m = 0 \in \mathbb{Z}_{60} \iff 30|a$. ◀

14. Verify that $\mathbb{Z}[i]/\langle 3+i\rangle \cong \mathbb{Z}_{10}$.

▶ **Solution.** Define a ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 3+i\rangle$ by the formula

$$\varphi(n) = n + \langle 3+i\rangle.$$

The required isomorphism is derived from the first isomorphism theorem if we can show that φ is surjective and that $\mathrm{Ker}(\varphi) = \langle 10\rangle$.

φ is surjective: To see this, we need to show that every coset $(k+mi)+\langle 3+i\rangle$ in the quotient ring $\mathbb{Z}[i]/\langle 3+i\rangle$ contains an ordinary integer n. But in $\mathbb{Z}[i]/\langle 3+i\rangle$, the element $3+i$ is set to 0, so that, in this quotient ring, $3=-i$. This suggests that there is an equality of cosets

$$(k+mi)+\langle 3+i\rangle = (k-3m)+\langle 3+i\rangle,$$

which we can check formally to be true by observing that

$$(k+mi)-(k-3m) = m(3+i) \in \langle 3+i\rangle.$$

Thus, $\varphi(k-3m) = (k-3m)+\langle 3+i\rangle = (k+mi)+\langle 3+i\rangle$, so φ is surjective.

$\operatorname{Ker}(\varphi) = \langle 10\rangle$: Suppose $\varphi(n) = 0 = 0+\langle 3+i\rangle$. Thus, we are assuming that $n \in \langle 3+i\rangle$, which means that $n = (r+si)(3+i) = (3r-s)+(3s+r)i$. Since $n \in \mathbb{Z}$ this means that the imaginary part $3s+r=0$ so $r=-3s$, which means $n = 3r-s = -10s$ so $10|n$, and $\operatorname{Ker}(\varphi) \subseteq \langle 10\rangle$. Since $10 = (3+i)(3-i)$, we have that $10 \in \operatorname{Ker}(\varphi)$. Hence, $\operatorname{Ker}(\varphi) = \langle 10\rangle$.

Now by the isomorphism theorem: $\mathbb{Z}_{10} = \mathbb{Z}/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) = \mathbb{Z}[i]/\langle 3+i\rangle$. ◀

18. (a) Given the complex number $z = 1+i$, let $\phi : \mathbb{R}[X] \to \mathbb{C}$ be the substitution homomorphism determined by z. Compute $\operatorname{Ker}(\phi)$.

▶ **Solution.** If $f(X) \in \mathbb{R}[X]$, then $\phi(f(X)) = f(z) = f(1+i)$. If $f(X) \in \operatorname{Ker}(\phi)$ then $f(1+i) = 0$. For any $w \in \mathbb{C}$, since complex conjugation is a ring homomorphism, it follows that $\overline{f(w)} = f(\overline{w})$. Thus, $f(1-i) = 0$ whenever $f(X) \in \mathbb{R}[X]$ and $f(1+i) = 0$. Thus, by the remainder theorem (Corollary 4.5, Page 75), if $f(X) \in \operatorname{Ker}(\phi)$, then $(X-(1+i))$ and $(X-(1-i))$ both divide $f(X)$ in $\mathbb{C}[X]$, so that $X^2-2X+2 = (X-(1+i))(X-(1-i))$ divides $f(X)$ in $\mathbb{C}[X]$. This suggests that $\operatorname{Ker}(\phi) = \langle X^2-2X+2\rangle$. To see it formally, note that $X^2-2X+2 = (X-(1+i))(X-(1-i))$, so certainly $X^2-2X+2 \in \operatorname{Ker}(\phi)$. Now let $f(X) \in \mathbb{R}[X]$ be any polynomial in $\operatorname{Ker}(\phi)$. Now divide $f(X)$ by X^2-2X+2 in $\mathbb{R}[X]$ to get

$$f(X) = (X^2-2X+2)q(X) + aX + b.$$

Since $f(X) \in \operatorname{Ker}(\phi)$, it follows that

$$0 = f(1+i) = a(1+i)+b = (a+b)+ai.$$

Since a and b are real, it follows that $a=b=0$, so (X^2-2X+2) divides $f(X)$. Hence, we conclude that $\operatorname{Ker}(\phi) = \langle X^2-2X+2\rangle$, as required. ◀

(b) The substitution homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$ given by $\phi(f(X)) = f(1+i)$ (from part (a)) is a surjective homomorphism with $\operatorname{Ker}(\phi) = \langle X^2-2X+2\rangle$. Thus, ϕ induces a isomorphism $\overline{\phi} : \mathbb{R}[X]/\langle X^2-2X+2\rangle \to \mathbb{C}$. This is given explicitly by $\phi(aX+b+\langle X^2-2X+2\rangle) = a(1+i)+b$.