SOLUTION KEY
Produced by: Kyle Dahlin

Problems:
Chap 16: 13, 15, 35, 44
Chap 17: 8, 10, 12, 14, 15, 23, 34

Problem 16.13. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

Solution:
$f(x) = g(x) \times (4x^2 + 3x + 6) + (6x + 2)$. The quotient is $4x^2 + 3x + 6$ and the remainder is $6x + 2$. Alternative equivalent representations may be obtained if "negative" numbers are used. ■

Problem 16.15. Show that the polynomial $2x + 1$ in $\mathbb{Z}_4[x]$ has a multiplicative inverse in $\mathbb{Z}_4[x]$.

Solution:
$2x + 1$ is its own multiplicative inverse: $(2x + 1)^2 = 4x^2 + 4x + 1 = 1 \in \mathbb{Z}_4[x]$. ■

Problem 16.35. For every prime p, show that

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots [x - (p - 1)]$$

in $\mathbb{Z}_p[x]$.

Solution:
The $p - 1$ elements, 1 through $p - 1$, are distinct and are each roots of $f(x) = x^{p-1} - 1$ by Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \bmod p$$

By the Factor Theorem, $(x - a)$ divides $f(x)$ for each such a. Further, since $f(x)$ has at most $p - 1$ zeros, it must be that

$$f(x) = (x - 1)(x - 2) \cdots [x - (p - 1)].$$

■

Problem 16.44. Let R be a commutative ring with unity. If I is a prime ideal of R, prove that $I[x]$ is a prime ideal of $R[x]$.

Solution:
We will show that $R[x]/I[x]$ is an integral domain and then apply Theorem 14.3 to show that then $I[x]$ is a prime ideal.

First, by Theorem 14.3, R/I is an integral domain and by Theorem 16.1, $(R/I)[x]$ is an integral domain. Let ϕ be the natural homomorphism from R to R/I and denote $\bar{a} = \phi(a)$, the image of a under ϕ.

Now define $\psi : R[x] \to (R/I)[x]$ by:

$$\psi(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} \cdots + \bar{a}_1 x + \bar{a}_0.$$

This is a homomorphism. Clearly $\psi(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = 0$ if and only if $a_n, a_{n-1}, \ldots, a_1, a_0 \in I$.

Thus $\ker \psi = I[x]$ and by the First Homomorphism Theorem, $(R/I)[x] \cong R[x]/I[x]$. Hence $R[x]/I[x]$ is an integral domain and, again by Theorem 14.3, $I[x]$ is a prime ideal. ■

Problem 17.8. Suppose that $f(x) \in \mathbb{Z}_p[x]$ and $f(x)$ is irreducible over $\mathbb{Z}_p$, where p is a prime. If $\deg f(x) = n$, prove that $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with p^n elements.

Solution:
$\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field by Corollary 1 to Theorem 17.5. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$. Let $\psi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]/\langle f(x)\rangle$ be the natural homomorphism.

Let c be such that $-ca_n = 1$. Then in $\mathbb{Z}_p[x]/\langle f(x)\rangle$,

$$\begin{aligned}\phi(x^n) &= ca_{n-1}x^{n-1} + \cdots + ca_1 x + ca_0\\ \phi(x^{n+1}) &= ca_{n-1}x^n + \cdots + ca_1 x^2 + ca_0 x\\ &= ca_{n-1}(ca_{n-1}x^{n-1} + \cdots ca_1 x + ca_0) + \cdots + ca_1 x^2 + ca_0 x.\end{aligned}$$

Hence $\deg \phi(x^n) = n-1$ and $\deg \phi(x^{n+1}) = n-1$ and, in general, for any $h(x) \in \mathbb{Z}_p[x]$, $\deg \phi(h(x)) \leq n-1$.

Suppose there exists $h(x) \in \mathbb{Z}_p[x]$ with $\deg h(x) < n-1$ and $\psi(h(x)) = 0$. Then $h(x) \in \langle f(x)\rangle$ and there exists $g(x) \in \mathbb{Z}_p[x]$ such that $g(x)h(x) = f(x)$. But this is impossible since $f(x)$ is irreducible over $\mathbb{Z}_p$.

Thus the elements of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ have the form:

$$b_{n-1}x^{n-1} + \cdots + b_0$$

for $b_i \in \mathbb{Z}_p$. Counting the possible combinations of entries, there are in total p^n elements of $\mathbb{Z}_p[x]/\langle f(x)\rangle$. ■

Problem 17.10. Construct a field of order 27.

Solution:
Consider $\mathbb{Z}_3[x]/\langle x^3 + 2x + 2\rangle$. Since $x^3 + 2x + 2$ has no roots over $\mathbb{Z}_3$, it is irreducible (by Theorem 17.1). Hence by **Problem 17.8**, this is a field with $3^3 = 27$ elements. ■

Problem 17.12. Determine which of the polynomials below is (are) irreducible over $\mathbb{Q}$.

a. $x^5 + 9x^4 + 12x^2 + 6$

b. $x^4 + x + 1$

c. $x^4 + 3x^2 + 3$

d. $x^5 + 5x^2 + 1$

e. $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$

Solution:

a. $x^5 + 9x^4 + 12x^2 + 6$
This polynomial is irreducible. Apply Eisenstein's Criterion with $p = 3$.

b. $x^4 + x + 1$
Apply the Mod 2 Irreducibility Test to obtain $\bar{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. This has no linear factors since it has no roots in $\mathbb{Z}_2$. Thus $\bar{f}$ must be a product of degree 2 elements of $\mathbb{Z}_2[x]$. There is a unique irreducible degree 2 element of $\mathbb{Z}_2[x]$, $x^2 + x + 1$, with $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Hence $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2[x]$, and by Theorem 17.3, the original polynomial is irreducible over $\mathbb{Q}$.

c. $x^4 + 3x^2 + 3$
This polynomial is irreducible. Apply Eisenstein's Criterion with $p = 3$

d. $x^5 + 5x^2 + 1$
Apply the Mod 2 Irreducibility Test to obtain $\bar{f}(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$. Then $\bar{f}(0) = 1$ and $\bar{f}(1) = 1$, so $\bar{f}$ has no linear factors. Thus $\bar{f}$ is either irreducible or is a product of a degree 2 and a degree 3 polynomial. The irreducible degree 2 polynomial in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$. Dividing $\bar{f}(x)$ by $x^2 + x + 1$ yields

$$\bar{f}(x) = (x^2 + x + 1)(x^3 + x^2) + 1.$$

So $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2[x]$, and by Theorem 17.3, the original polynomial is irreducible over $\mathbb{Q}$.

e. $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$
Consider $f(x) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3$, which is the original polynomial multiplied by 14. Apply Eisenstein's Criterion to $f(x)$ with $p = 3$. Then $f(x)$ is irreducible over $\mathbb{Q}$ and hence $(1/14)f(x)$ is irreducible over $\mathbb{Q}$.

■

Problem 17.14. Show that $x^2 + x + 4$ is irreducible over $\mathbb{Z}_{11}$.

Solution:
Completing the square gives $f(x) = (x + 6)^2 + 1$. Since $f(x)$ has degree 2 and $\mathbb{Z}_{11}$ is a field, $f(x)$ is reducible if and only if it has linear factors (i.e. roots). If a is a root of $f(x)$, then $(a + 6)^2 \equiv -1 \bmod 11$. However, there is no $b \in \mathbb{Z}_{11}$ such that $b^2 \equiv -1 \bmod 11$ since then $(b^2)^5 \equiv -1 \bmod 11$ but, by Fermat's Little Theorem, $b^{11-1} \equiv 1 \bmod 11$. Hence $f(x)$ is irreducible.

Alternatively, one can check that $f(a) \neq 0$ for all $a \in \mathbb{Z}_{11}$. This method would be very inefficient when working with a field with more elements. Then by Theorem 17.1, $f(x)$ is irreducible.

a	$f(a)$
0	4
1	6
2	10
3	5
4	2
5	1
6	2
7	5
8	10
9	6
10	4

■

Problem 17.15. let $f(x) = x^3 + 6 \in \mathbb{Z}_7[x]$. Write $f(x)$ as a product of irreducible polynomials over $\mathbb{Z}_7$.

Solution:
Since $f(1) = 0 \in \mathbb{Z}_7$, $x + 6$ is a factor of f. Using polynomial long division, we obtain, $f(x) = (x + 6)(x^2 + x + 1)$. Since $x^2 + x + 1$ is degree 2, it is irreducible if it has no zeros in $\mathbb{Z}_7$. It can be shown that 2 and 4 are roots of x^2+x+1 and thus, $f(x) = (x+6)(x+5)(x+3)$. Equivalently, $f(x) = (x - 1)(x - 2)(x - 4)$. ■

Problem 17.23. Find all monic irreducible polynomials of degree 2 over $\mathbb{Z}_3$.

Solution:
By Theorem 17.1, we need only find the monic degree 2 polynomials over $\mathbb{Z}_3$ (of which there are 9 total) which have no roots over $\mathbb{Z}_3$. These are precisely:
$x^2 + 1$,
$x^2 + x + 2$, and
$x^2 + 2x + 2$. ■

Problem 17.34. Let F be a field and let $f(x)$ be a polynomial in $F[x]$ that is reducible over F. Prove that $\langle f(x)\rangle$ is not a prime ideal in $F[x]$.

Solution:
Suppose that $\langle f(x)\rangle$ is a prime ideal in $F[x]$ and $f(x) = g(x)h(x)$ for some non-units $g(x)$, $h(x) \in F[x]$. By Theorem 14.3, $F[x]/\langle f(x)\rangle$ is an integral domain. Let $\pi : F(x) \to F(x)/\langle f(x)\rangle$ be the natural homomorphism. Then

$$\pi(g(x))\pi(h(x)) = \pi(g(x)h(x)) = \pi(f(x)) = 0.$$

Without loss of generality, suppose that $\pi(g(x)) = 0$. Then $g(x) = q(x)f(x)$ for some $q(x) \in F[x]$ and $\deg g(x) \geq \deg f(x)$. But since $f(x) = g(x)h(x)$, this implies that $\deg h(x) = 0$, thus $h(x)$ is a unit, a contradiction. Hence $\langle f(x)\rangle$ cannot be a prime ideal in $F[x]$. ■