Solution Outlines for Chapter 17

 # 2: Suppose that D is an integral domain and F is a field containing D. If $f(x) \in D[x]$ and $f(x)$ is irreducible over F but reducible over D, what can you say about the factorization of $f(x)$ over D?

Suppose that $f(x)$ is reducible over D. Then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in D[x]$. Now, all elements of D are in F, so $f(x) = g(x)h(x)$ in $F[x]$. But since $f(x)$ is irreducible, $g(x)$ or $h(x)$ is a unit in F. So $f(x) = ag(x)$ for some $g(x)$ and some $a \in D$ that is not a unit in D but is a unit in F.

 # 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 $\mathbb{Z}_p[x]/ < f(x) >$ is a field with p^n elements.

Since $f(x)$ is irreducible, $< f(x) >$ is maximal and $\mathbb{Z}_p[x]/ < f(x) >$ is a field. Now since the degree of $f(x)$ is n, every element in $\mathbb{Z}_p[x]/ < f(x) >$ can be written as $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 + < f(x) >$. [Not sure why the previous statement is true? Recall that for any polynomial $g(x)$ in $\mathbb{Z}_p[x]$, $g(x) = f(x)q(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $f(x)$ or $r(x) = 0$. So $g(x)+ < f(x) >= f(x)q(x) + r(x)+ < f(x) >= r(x)+ < f(x) >$.] Since each a_i is in $\mathbb{Z}_p$, there are p options for each coefficient in the coset representative. So there are $p \times p \times \cdots \times p = p^n$ possible standard representatives. Moreover, it is clear that each is unique.

 # 9: Construct a field of order 25.

Since $25 = 5^2$, start with $\mathbb{Z}_5[x]$. Now, we must find a degree 2 polynomial, $p(x)$, that is irreducible over $\mathbb{Z}_5$. Then $\mathbb{Z}_5[x]/ < p(x) >$ is a field of order 5*5 = 25. Now, lets start with $p(x) = x^2 + x + a$. Then $p(0) = a$, $p(1) = a + 2$, $p(2) = a + 1$, $p(3) = 2 + a$, and $p(4) = a$. So $a \neq 0, 3, 4$. Choose $a = 1$. Then $p(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_5$ and works to give us the field we want.

 # 12: Determine which of the polynomials below is (are) irreducible over $\mathbb{Q}$.

a. $x^5 + 9x^4 + 12x^2 + 6$: Irreducible. Use Eisenstein's with $p = 3$.

b. $x^4 + x + 1$: Irreducible. In $\mathbb{Z}_2[x]$ this polynomial is $f(x) = x^4 + x + 1$ (notice the degree is preserved). Now $f(0) = 1$ and $f(1) = 1$ so $f(x)$ is irreducible over $\mathbb{Z}_2$ and thus over $\mathbb{Q}$. Alternately, the rational roots theorem tells us ± 1 are the only possible rational roots and neither works.

c. $x^4 + 3x^2 + 3$: Irreducible. Use Eisenstein's with $p = 3$.

d. $x^5 + 5x^2 + 1$: Irreducible. In $\mathbb{Z}_2[x]$ this polynomial is $f(x) = x^5 + x^2 + 1$ (notice the degree is preserved). Now $f(0) = 1$ and $f(1) = 1$ so $f(x)$ is irreducible over $\mathbb{Z}_2$ and thus over $\mathbb{Q}$. Alternately, the rational roots theorem tells us ± 1 are the only possible rational roots and neither works.

e. $(\frac{5}{2})x^5 + (\frac{9}{2})x^4 + 15x^3 + (\frac{3}{7})x^2 + 6x + \frac{3}{14}$: Irreducible. Call the polynomial $f(x)$. Then $14f(x) = 35x^5 + 63x^4 + 105x^3 + 6x^2 + 84x + 3$. Now $14f(x)$ is irreducible by Eisenstein's with $p = 3$. Hence $f(x)$ is irreducible.

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

Since the degree of $f(x)$ is 3, any factor must correspond to a 0. So $f(0) = 3$, $f(1) = 0$, $f(2) = 0$, $f(3) = 5$, $f(4) = 0$, $f(5) = 5$, $f(6) = 5$. So $f(x) = (x-1)(x-2)(x-4) = (x+6)(x+5)(x+3)$. (Notice that each root occurs with multiplicity 1 because of the degree.)

 # 19: Show that for every prime p there exists a field of order p^2.

Let's think about $\mathbb{Z}_p[x]$. By exercise 18/17 (these are fundamentally the same problem), there is a degree 2 polynomial that is irreducible over $\mathbb{Z}_p$, say $f(x)$. Thus $\mathbb{Z}_p[x]/ < f(x) >$ is a field of order p^2 or less (see exercise 9 if you don't understand why this is the order). Now $ax + b + < f(x) > = cx + d + < f(x) >$ implies that $(a-c)x + (b-d)$ is divisible by $f(x)$. This means that $a = c$ and $b = d$. Thus the order is precisely p^2.

 # 20: Prove that, for every positive integer n, there are infinitely many polynomials of degree n in $\mathbb{Z}[x]$ that are irreducible over $\mathbb{Q}$.

Fix n. Consider the infinite class of polynomials of order $x^n + p$ where p is a prime. Then, by Eisenstein's, $x^n + p$ is irreducible over $\mathbb{Q}$.

 # 21: Show that the field given in Example 11 in this chapter is isomorphic to the field given in Example 9 in Chapter 13.

The example 11 field is: $\mathbb{Z}_3[x]/ < x^2+1 >$. The example 9 field is: $\mathbb{Z}_3[i]$. Define $\phi : \mathbb{Z}_3[x]/ < x^2+1 > \to \mathbb{Z}_3[i]$ by $\phi(f(x) + < x^2+1 >) = f(i)$. Then $\phi(f(x) + < x^2+1 > + g(x) + < x^2+1 >) = \phi(f(x) + g(x) + < x^2+1 >) = f(i) + g(i) = \phi(f(x) + < x^2+1 >) + \phi(g(x) + < x^2+1 >)$ and $\phi((f(x) + < x^2+1 >)(g(x) + < x^2+1 >)) = \phi(f(x)g(x) + < x^2+1 >) = f(i)g(i) = \phi(f(x) + < x^2+1 >)\phi(g(x) + < x^2+1 >)$. Thus ϕ is a homomorphism. Now, $ker\phi = \{f(x) + < x^2+1 > | f(i) = 0\} = \{ax+b + < x^2+1 > | ai+b = 0 \text{ where } a, b \in \mathbb{Z}_3\} = < x^2+1 >$ so ϕ is 1-1. Now let $a + bi \in \mathbb{Z}_3[i]$. Then $a + bx + < x^2+1 >$ maps to $a + bi$ so ϕ is onto. Thus, these fields are isomorphic.

 # 23: Find all monic irreducible polynomials of degree 2 over $\mathbb{Z}_3$.

So this means that the polynomial must look like $x^2 + ax + b$ where $b \neq 0$. Suppose $b = 1$. Then $x^2 + ax + 1 = f(x)$. Then $f(0) = 1$, $f(1) = a + 2$, and $f(2) = 2 + 2a$. So $a \neq 1, 2$. Thus $x^2 + 1$ is irreducible. Now suppose $b = 2$. Then $f(x) = x^2 + ax + 2$. So $f(0) = 2$, $f(1) = a$, and $f(2) = 2a$. Thus $a \neq 0$ So $x^2 + x + 2$ and $x^2 + 2x + 2$ are irreducible. Final answer: $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$.

 # 24: Given that π is not the zero of a nonzero polynomial with rational coefficients, prove that π^2 cannot be written in the form $a\pi + b$, where a and b are rational.

Suppose that π^2 can be written as $a\pi + b$. Then set $g(x) = x^2 - ax - b$. So $g(\pi) = \pi^2 - a\pi - b = a\pi + b - a\pi - b = 0$ so π is a zero of a nonzero polynomial with rational coefficients, which is a contradiction.

 # 26: Find all zeros of $f(x) = 3x^2 + x + 4$ over $\mathbb{Z}_7$ by substitution. Find all zeros of $f(x)$ by using the quadratic formula. Do your answers agree? Should they? Find all zeros of $g(x) = 2x^2 + x + 3$ over $\mathbb{Z}_5$ by substitution. Try the quadratic formula on $g(x)$. Do your answers agree? State necessary and sufficient conditions for the quadratic formula to yield the zeros of a quadratic from $\mathbb{Z}_p[x]$, where p is a prime greater than 2.

Using substitution we see $f(4) = 0 = f(5)$ so the roots are 4 and 5 Using the quadratic formula, we have $(-1 \pm \sqrt{-47})(6)^{-1} = (6 \pm \sqrt{2})(6) = (6 \pm 3)(6) = 4, 5$.

Now for $g(x)$, we see by substitution that there are no zeros in $\mathbb{Z}_5$. Using the quadratic formula, we have $(-1 \pm \sqrt{2})(2^{-1})$ but no number in $\mathbb{Z}_5$ squares to 5, so there are no solutions.

Since every number has a multiplicative inverse in $\mathbb{Z}_p$, the only problem occurs when $b^2 - 4ac$ is not a square. Thus there are zeros in $\mathbb{Z}_p$ when $b^2 - 4ac = d^2$ for some $d \in \mathbb{Z}_p$.

 # 31: Let F be a field and let $p(x)$ be irreducible over F. If E is a field that contains F and there is an element a in E such that $p(a) = 0$, show that the mapping $\phi : F[x] \to E$ given by $f(x) \to f(a)$ is a ring homomorphism with kernel $< p(x) >$.

Let ϕ, F, $p(x)$, E and a be defined as above. Then $\phi(f(x) + g(x)) = f(a) + g(a) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = f(a)g(a) = \phi(f(x))\phi(g(x))$. Clearly $p(x)$ is in the kernel of ϕ. Moreover, since $p(x)$ is irreducible, $< p(x) >$ is a maximal ideal. So that means that the kernel of ϕ is precisely $< p(x) >$.