Selected Solutions to HW 7:

5.9(d): Let $I = (x^5 + x^2 + 1)$, where the coefficients belong to F_2. Given $I+f(x) \in F_2[x]/I$, write $f(x) = q(x)(x^5+x^2+1)+a+b+cx+dx^2+ex^3+dx^4$. Then $I+f(x) = I+a+bx+cx^2+dx^3+ex^4$. We must show that a, b, c, d, e are unique. Suppose $I+a+bx+cx^2+dx^3+ex^4 = I+A+Bx+Cx^2+Dx^3+Ex^4$. Then

$$(a - A) + (b - B)x + (c - C)x^2 - (d - D)x^3 - (e - E)x^4 \in I,$$

which implies

$$(a - A) + (b - B)x + (c - C)x^2 - (d - D)x^3 - (e - E)x^4 = g(x)(x^5 + x^2 + 1)$$

for some $g(x) \in F_2[x]$. Since the left-hand-side of this equation has degree ≤ 4, the right-hand side of this equation also has degree ≤ 4. This can only be the case if $g(x) = 0$, which implies $(a - A) + (b - B)x + (c - C)x^2 - (d - D)x^3 - (e - E)x^4 = 0$, which by definition of $F_2[x]$ implies $a - A = b - B = c - C = d - D = e - E = 0$. Therefore $a = A, b = B, c = C, d = D, e = E$.

5.10: Note that $\mathbb{Z}_n$ is a field if and only if n is prime. Proof: if n is prime and $a \not\equiv 0 \bmod n$ then $\gcd(a, n) = 1$, therefore $ja + kn = 1$ has a solution in integers j and k, hence $ja \equiv 1 \bmod n$, hence a is invertible. Moreover, if n is not prime then $n = rs$ where $1 < r < n$ and $1 < s < n$, hence r is not invertible in $\mathbb{Z}_n$, for if it is then the equation $jr \equiv 1 \bmod n$ has an integer solution for j, which implies an integer solution to $jr+kn = 1$, which implies $jrs + kns = s$, which implies $jn + kns = s$, which implies $n|s$, which is impossible because $1 < s < n$.

So there is no field F_4 that you can use to construct this example. However, F_2 is a perfectly good field. Since $x^4 + x + 1$ has no linear and quadratic factors in $F_2[x]$, it is irreducible in $F_2[x]$. Hence $F_2[x]/(x^4 + x + 1)$ is a field with 16 elements.

5.13: $x^4 + 1 = x^4 - 4 = (x^2 + 2)(x^2 - 2)$ in $F_5[x]$.

5.17: Set $f_n(x) = 1 + x + \cdots + x^{n-1}$. Then $f_n(x) = \frac{x^n-1}{x-1}$. If $n = ab$ where $a > 1$ and $b > 1$ then we have

$$f_n(x) = \frac{x^{ab} - 1}{x^a - 1} = \frac{x^{ab} - 1}{x^a - 1}\frac{x^a - 1}{x - 1} = f_b(x^a)f_a(x),$$

hence $f_n(x)$ is not irreducible.