Adam Jump
Rings and Fields
Chapter 16 Homework

2. In $\mathbb{Z}_3[x]$, show that the distinct polynomials x^4+x and x^2+x determine the same function from $\mathbb{Z}_3$ to $\mathbb{Z}_3$.

x	x^4+x	x^2+x
0	$[x^4+x](0)=0+0=0$	$[x^2+x](0)=0+0=0$
1	$[x^4+x](1)=1^4+1=2$	$[x^2+x](1)=1^2+1=2$
2	$[x^4+x](2)=2^4+2=18 \mod 3=0$	$[x^2+x](2)=2^2+2=6 \mod 3=0$

3. Show that x^2+3x+2 has four zeros in $\mathbb{Z}_6$.

$$\begin{array}{l}
[x^2+3x+2]\,(0)=2 \mod 6=2\\
[x^2+3x+2]\,(1)=6 \mod 6=0\\
[x^2+3x+2]\,(2)=12 \mod 6=0\\
[x^2+3x+2]\,(3)=20 \mod 6=2\\
[x^2+3x+2]\,(4)=30 \mod 6=0\\
[x^2+3x+2]\,(5)=42 \mod 6=0
\end{array}$$

7. Find two distinct cubic polynomials over $\mathbb{Z}_2$ that determine the same function from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.

x	x^3+x	x^3+x^2
0	$0+0=0$	$0+0=0$
1	$1^3+1=2 \mod 2=0$	$1^3+1^2=2 \mod 2=0$

9. 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 $g(x)$.

$$\begin{array}{rrrrrr}
 & & & 4x^2 & +3x & +6\\ \hline
3x^2+2x+1) & +5x^4 & +3x^3 & & & +1\\
 & +5x^4 & +x^3 & +4x^2 & & \\ \hline
 & & +2x^3 & +3x^2 & & +1\\
 & & +2x^3 & +6x^2 & +3x & \\ \hline
 & & & +4x^2 & +4x & +1\\
 & & & +4x^2 & +5x & +6\\ \hline
 & & & & +6x & +2
\end{array}$$

which implies that the quotient of $f(x)/g(x)$ is $4x^2+3x+6$ and the remainder is $6x+2$.
I also learned about the polynom package, although it won't reduce polynomials over finite fields.

$$\begin{array}{l}
\big(\;5x^4 + 3x^3 \qquad\qquad + 1\big) : \big(3x^2+2x+1\big) = \frac{5}{3}x^2 - \frac{1}{9}x - \frac{13}{27} + \dfrac{\frac{29}{27}x+\frac{40}{27}}{3x^2+2x+1}\\
\underline{-5x^4 - \frac{10}{3}x^3 - \frac{5}{3}x^2}\\
\quad -\frac{1}{3}x^3 - \frac{5}{3}x^2\\
\quad \underline{\frac{1}{3}x^3 + \frac{2}{9}x^2 + \frac{1}{9}x}\\
\qquad -\frac{13}{9}x^2 + \frac{1}{9}x + 1\\
\qquad \underline{\frac{13}{9}x^2 + \frac{26}{27}x + \frac{13}{27}}\\
\qquad\qquad \frac{29}{27}x + \frac{40}{27}
\end{array}$$

12. If the rings R and S are isomorphic, show that $R[x]$ and $S[x]$ are isomorphic.

Let ϕ be an isomorphism from R to S, and σ be a homomorphism from $R[x]$ to $S[x]$. We know that $\ker\phi=\{0\}$, and we want to show that $\ker\sigma=\{0\}$. First of all, we should note that all coefficients of $a\in R$ of $R[x]$ are equivalent to $\phi(a)\in S[x]$. We then define σ as the polynomial extension of ϕ, where a polynomial $f(x)=a_nx^n+\cdots+a_0$ in $R[x]$ is mapped by σ to $\sigma(f(x))=\phi(a_n)x^n+\cdots+\phi(a_0)$. Because ϕ is an isomorphism, we know that ϕ^{-1} exists. Now we consider $\phi^{-1}(\phi(a_n))x^n + \cdots + \phi^{-1}(\phi(a_0)) = \sigma^{-1}(\sigma(f(x)))$, which shows that σ^{-1} exists. As a result of ϕ being onto and $\ker\phi = 0$, these attributes are immediately inherited by σ. **Note:** I'm pretty sure I need to show this, and can't immediately assume it.

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

$2x+1$ is its own inverse in $\mathbb{Z}_4[x]$, observe that $(2x+1)^2 = 4x^2+4x+1 \mod 4 = 1$.

20. Prove that the ideal $\langle x\rangle$ in $\mathbb{Q}[x]$ is maximal.

By Theorem 14.4, we know that $\mathbb{Q}[x]/\langle x\rangle$ is a field if and only if $\langle x\rangle$ is maximal. We can see that $\mathbb{Q}[x]/\langle x\rangle = \mathbb{Q}$, and $\mathbb{Q}$ is a field. This immediately implies that $\langle x\rangle$ is maximal.

24. Let $\mathbb{F}$ be an infinite field and let $f(x), g(x) \in \mathbb{F}[x]$. If $f(a) = g(a)$ for infinitely many elements a of $\mathbb{F}$, show that $f(x) = g(x)$.

By the Remainder Theorem, we know that $f(x)/(x-a) = f(a)$, or $f(x) = f(a)(x-a)$. However, because $f(a) = g(a)$, we can assert that $f(x) = g(a)(x-a)$. Likewise, we know that $g(x) = g(a)(x-a)$ by the remainder theorem, which implies that $f(x) = g(x)$.

38. (Wilson's Theorem) For every integer $n > 1$, prove that $(n-1)! \mod n = n-1$ if and only if n is prime.

We can note that our operation is occurring in $\mathbb{Z}_p$, which has characteristic p.

46. Prove that $\mathbb{Q}[x]/\langle x^2-2\rangle$ is ring-isomorphic to $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Let γ be a mapping from $\mathbb{Q}[x]/\langle x^2-2\rangle$ to $\mathbb{Q}[\sqrt{2}]$