MATH 320 S26, Exam 3 Solutions

1. Let R be an integral domain, and let $f(x) \in R[x]$. Prove that $f(x)$ is a unit in $R[x]$, if and only if, $f(x) = a_0$, where a_0 is some unit of R.

There are two directions to prove. Suppose first that $f(x)$ is a unit, i.e there is some $g(x) \in R[x]$ with $f(x)g(x) = 1_R (= 1_{R[x]})$. By the degree sum theorem, $\deg(f(x)) + \deg(g(x)) = \deg(1_R) = 0$. Hence $\deg(f(x)) = \deg(g(x)) = 0$, so in fact $f(x) = a_0, g(x) = b_0$, for some $a_0, b_0 \in R$ satisfying $a_0 b_0 = 1_R$. Hence a_0 is a unit of R.

Second, suppose $f(x) = a_0$, where a_0 is a unit of R. Let $a_0^{-1} \in R$ satisfy $a_0 a_0^{-1} = 1_R$. Taking $g(x) = a_0^{-1} \in R[x]$, we see that $f(x)g(x) = 1_R$, so $f(x)$ is a unit in $R[x]$.

2. Let $f(x), g(x) \in \mathbb{Q}[x]$, where $f(x) \neq 0$. Prove that $\gcd(f(x), g(x)) = \gcd(f(x), g(x) + xf(x))$.

SOLUTION 1: Set $u(x) = \gcd(f(x), g(x))$ and $v(x) = \gcd(f(x), g(x) + xf(x))$. Now there are $a(x), b(x)$ with $f(x) = u(x)a(x), g(x) = u(x)b(x)$. Hence, $g(x) + xf(x) = u(x)b(x) + xu(x)a(x) = u(x)(b(x) + xa(x))$, so $u(x)$ is a common divisor of $f(x)$ and $g(x) + xf(x)$. By exercise 3.6, we have $u(x)|v(x)$.

Now, take $c(x), d(x)$ with $f(x) = v(x)c(x), g(x) + xf(x) = v(x)d(x)$. Hence, $g(x) = (g(x) + xf(x)) - xf(x) = v(x)d(x) - xv(x)c(x) = v(x)(d(x) - xc(x))$, so $v(x)$ is a common divisor of $f(x)$ and $g(x)$. By exercise 3.6 again, we have $v(x)|u(x)$.

By exercise 3.12, $u(x)$ and $v(x)$ are associates. Since they are both monic, $u(x) = v(x)$.
[optional full explanation: $u(x) = w(x)v(x)$ for some unit $w(x)$. By exercise 3.3, $w(x) = a_0$, a unit in $\mathbb{Q}$. Looking at the leading coefficients of $u(x)$ and $v(x)$ we have $1 = u_n = a_0 v_n = a_0 1 = a_0$, so $a_0 = 1$.]

SOLUTION 2: We will prove the lemma below, that the common divisors of $\{f(x), g(x)\}$ are exactly the common divisors of $\{f(x), g(x) + xf(x)\}$. Since these are the same set, the monic element of greatest degree (i.e., the gcd) of both is the same.

Lemma: The common divisors of $\{f(x), g(x)\}$ are exactly the common divisors of $\{f(x), g(x) + xf(x)\}$.
Proof: $\subseteq$: Let $d(x)$ be a common divisor of $f(x), g(x)$. Then there are $f'(x), g'(x)$ with $f(x) = f'(x)d(x)$ and $g(x) = g'(x)d(x)$. Now $g(x)+xf(x) = g'(x)d(x)+xf'(x)d(x) = (g'(x)+xf'(x))d(x)$, so $d(x)$ divides $g(x)+xf(x)$. Since it also divides $f(x)$, it is a common divisor of $f(x), g(x)+xf(x)$.
$\supseteq$: Let $d'(x)$ be a common divisor of $f(x), g(x) + xf(x)$. Then there are $f'(x), h(x)$ with $f(x) = f'(x)d'(x)$ and $g(x) + xf(x) = h(x)d'(x)$. Now $g(x) = g(x) + xf(x) - xf(x) = h(x)d'(x) - xf'(x)d'(x) = (h(x) - xf'(x))d'(x)$, so $d'(x)$ divides $g(x)$. Since it also divides $f(x)$, it is a common divisor of $f(x), g(x)$.

NOT A SOLUTION: This problem is a special case of exercise 3.8, which cannot be used to prove itself.

3. Working in $\mathbb{Q}[x]$, set $f(x) = x^3 - 2x^2 + x - 2$ and $g(x) = 2x^4 + x^3 + 3x^2 + x + 1$. Use the $\mathbb{F}[x]$ Euclidean algorithm to find $\gcd(f(x), g(x))$ and also to find $u(x), v(x) \in \mathbb{Q}[x]$ satisfying $u(x)f(x) + v(x)g(x) = \gcd(f(x), g(x))$.

Step 1: Using long division, we find $g(x) = (2x + 5)f(x) + (11x^2 + 11)$.
Step 2: Using long division, we find $f(x) = (\frac{1}{11}x - \frac{2}{11})(11x^2 + 11) + 0$.
Hence the desired $\gcd(f(x), g(x)) = x^2 + 1$, the monic version of $11x^2 + 11$.
Step 3: We rearrange step 1 to find $11x^2 + 11 = g(x) - (2x + 5)f(x)$.
Step 4: We divide by 11 to get $x^2 + 1 = \frac{1}{11}g(x) + (\frac{-2}{11}x + \frac{-5}{11})f(x)$.
Hence the desired $u(x) = \frac{-2}{11}x + \frac{-5}{11}$, $v(x) = \frac{1}{11}$.

4. Set $R = \mathbb{Z}_{49}$. Find $f(x) \in R[x]$ where $\deg(f(x)) = 2$ and also $f(x)$ is a unit.

Many solutions are possible. For example, $f(x) = [7]x^2 + [1]$, which is a unit since $f(x)([-7]x^2 + [1]) = [-49]x^4 + [7]x^2 + [-7]x^2 + [1] = [0]x^2 + [0]x + [1] = [1]$.

5. Find all monic irreducible polynomials of degree 3, in $\mathbb{Z}_2[x]$. Be sure to justify your answer.

The key is exercise 3.17: if there are no roots, then it will be irreducible. There are exactly 8 such polynomials to check. The table below gives the answer, together with any roots.

x^3	NO: 0	x^3+1	NO: 1	x^3+x	NO: 0, 1	x^3+x+1	YES
x^3+x^2	NO: 0, 1	x^3+x^2+1	YES	x^3+x^2+x	NO: 0	x^3+x^2+x+1	NO: 1

In summary, $x^3 + x + 1$ and $x^3 + x^2 + 1$ are the two irreducible monic polynomials of degree 3 in $\mathbb{Z}_2[x]$.

6. Find a polynomial of degree 5 in $\mathbb{Z}_3[x]$ that induces the zero function on $\mathbb{Z}_3$.

Note that $(-1)^5 = (-1)^3 = -1, (1)^5 = (1)^3 = 1, (0)^5 = (0)^3 = 0$. There are 18 possible answers, the simplest of which is $[1]x^5 + [-1]x$. Whichever polynomial you pick, you need to plug in each of $[-1], [0], [1]$ (or $[0], [1], [2]$) to verify that the result is $[0]$ each time.

7. Let R be a commutative ring with identity. Let $a \in R$ satisfy $a^4 = 0_R$. Prove that $1_R + ax$ is a unit in $R[x]$.

We calculate $(1_R+ax)(1_R-ax+a^2x^2-a^3x^3) = 1_R+ax-ax+a^2x^2-a^2x^2-a^3x^3+a^3x^3-a^4x^4 = 1_R - a^4x^4 = 1_R - 0_Rx^4 = 1_R$. Hence $1_R - ax + a^2x^2 - a^3x^3 = (1_R + ax)^{-1}$, and $1_R + ax$ is a unit in $R[x]$.

8. Set $R = \mathbb{Z}_7[x]$, $f(x) = x^3 + [3]x^2 + [2]x + [6]$, and $g(x) = x^3 - [1]$. Use the Euclidean algorithm to find $\gcd(f(x), g(x))$.

Step 1: Using long division, we find $f(x) = ([1])g(x) + ([3]x^2 + [2]x)$.
Step 2: Using long division, we find $g(x) = (-[2]x - [1])([3]x^2 + [2]x) + ([2]x - [1])$.
Step 3: Using long division, we find $([3]x^2 + [2]x) = (-[2]x)([2]x - [1]) + [0]$.
Hence $\gcd(f(x), g(x))$ is the monic version of $[2]x - [1] = [2]x + [6]$, which is $[1]x + [3]$.

9. Prove the Degree Sum Theorem.

Let R be an integral domain, and let $f(x), g(x) \in R[x]$. There are two cases.
Case 1: Either $f(x) = 0_R$ or $g(x) = 0_R$ (or both). Then $f(x)g(x) = 0_R$, and both $\deg(f(x)g(x))$ and $\deg(f(x)) + \deg(g(x))$ equals $-\infty$.
Case 2: Neither $f(x)$ nor $g(x)$ is 0_R. Then they each have at least one nonzero coefficient, hence a highest-degree nonzero coefficient. Suppose the term with highest-degree nonzero coefficient of $f(x)$ is a_nx^n, while the term with the highest-degree nonzero coefficient of $g(x)$ is b_mx^m. Then $\deg(f(x)) = n$ and $\deg(g(x)) = m$. Also, $f(x)g(x)$ will have a term $a_nb_mx^{n+m}$. Since R is an integral domain, a_nb_m is nonzero, so this is the term of $f(x)g(x)$ with highest-degree nonzero coefficient and thus $\deg(f(x)g(x)) = n + m = \deg(f(x)) + \deg(g(x))$.

10. Prove the Remainder Theorem.

Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, and $a \in \mathbb{F}$. Applying the $\mathbb{F}[x]$ Division Algorithm Theorem to $f(x)$ and $x - a$, we get $q(x), r(x) \in \mathbb{F}[x]$ with $f(x) = (x-a)q(x)+r(x)$ and $\deg(r(x)) < \deg(x-a) = 1$. Hence either $\deg(r(x)) = 0$ or $\deg(r(x)) = -\infty$; in either case, $r(x) = r_0 \in \mathbb{F}$. Now, we evaluate the induced functions $f(x)$ and $(x - a)q(x) + r(x)$ at the value $x = a$, getting $f(a) = (a - a)q(a) + r(a) = 0_R + r(a) = r(a)$. However, we have proved that $r(a) = r_0$, a constant, so in fact $r(x) = f(a)$ (for all x, not just $x = a$).