MATH 521A: Abstract Algebra
Exam 3 Solutions

1. Set $f(x) = 3x^3 + 5x^2 + 6x$, $g(x) = 3x^4 + 5x^3 + x^2 + 3x + 2$, both in $\mathbb{Z}_7[x]$. Use the extended Euclidean algorithm to find $\gcd(f, g)$ and to find polynomials $s(x), t(x)$ such that $\gcd(f, g) = f(x)s(x) + g(x)t(x)$.

We perform the division algorithm repeatedly to get:

$$3x^4 + 5x^3 + x^2 + 3x + 2 = (x)(3x^3 + 5x^2 + 6x) + (2x^2 + 3x + 2)$$
$$3x^3 + 5x^2 + 6x = (5x + 2)(2x^2 + 3x + 2) + (4x + 3)$$
$$2x^2 + 3x + 2 = (4x + 3)(4x + 3) + 0$$

Hence $\gcd(f, g)$ is the monic multiple of $4x + 3$, namely $2(4x + 3) = x + 6$. We now back-substitute twice, simplify, and double both sides, to get:

$$\begin{aligned}
4x + 3 &= (3x^3 + 5x^2 + 6x) + (2x + 5)(2x^2 + 3x + 2)\\
4x + 3 &= (3x^3 + 5x^2 + 6x) + (2x + 5)\big((3x^4 + 5x^3 + x^2 + 3x + 2) + (-x)(3x^3 + 5x^2 + 6x)\big)\\
4x + 3 &= \big(1 + (2x + 5)(-x)\big)(3x^3 + 5x^2 + 6x) + (2x + 5)(3x^4 + 5x^3 + x^2 + 3x + 2)\\
4x + 3 &= (5x^2 + 2x + 1)(3x^3 + 5x^2 + 6x) + (2x + 5)(3x^4 + 5x^3 + x^2 + 3x + 2)\\
x + 6 &= (3x^2 + 4x + 2)(3x^3 + 5x^2 + 6x) + (4x + 3)(3x^4 + 5x^3 + x^2 + 3x + 2)
\end{aligned}$$

Hence we want $s(x) = 3x^2 + 4x + 2$ and $t(x) = 4x + 3$.

2. Factor $f(x) = x^4 + x^3 + 6x^2 - 14x + 16 \in \mathbb{Q}[x]$ into irreducibles.

We calculate $f(x+1) = x^4 + 5x^3 + 15x^2 + 5x + 10$. Note that $p = 5$ divides each coefficient except the leading one, and $p^2 = 25$ does not divide the constant. Hence by Eisenstein's criterion $f(x+1)$ is irreducible. By the translation trick, $f(x)$ is irreducible.

3. Let F be a field. We define the "derivative" operator $D : F[x] \to F[x]$ via

$$D(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 1a_1.$$

This operator satisfies, for all $f, g \in F[x]$ and for all $c \in F$:
(a) $D(f + g) = D(f) + D(g)$; (b) $D(cf) = cD(f)$; (c) $D(fg) = fD(g) + D(f)g$
Suppose $f, g \in F[x]$ and $f^2|g$. Prove that $f|D(g)$.

Because $f^2|g$ there is some polynomial $h \in F[x]$ such that $g(x) = f(x)f(x)h(x)$. We apply property (c) twice to get $D(g) = D(f(fh)) = fD(fh) + D(f)fh = f\big(fD(h) + D(f)h\big) + D(f)fh = f\big(fD(h) + D(f)h + D(f)h\big) = f\big(fD(h) + 2D(f)h\big)$. Since $fD(h) + 2D(f)h \in F[x]$, we have $f|D(g)$, as desired.

4. Set $f(x) = x + 2x^2, g(x) = x + 4x^2$, both in $\mathbb{Z}_8[x]$. Prove that $f|g$ and $g|f$.

All solutions involve at least some trial and error.
Direct Solution: $(x + 2x^2)(1 + 2x + 4x^2) = x + 4x^2$ and $(x + 4x^2)(1 + 6x) = x + 2x^2$.
Alternate Solution: $(x + 2x^2)(1 + 2x + 4x^2) = x + 4x^2$. But $1 + 2x + 4x^2$ is a unit, since $(1 + 2x + 4x^2)(1 + 6x) = 1$, so in fact f, g are associates.

5. Set $f(x) = x^n + x^{n-1} \in F[x]$. Carefully determine all divisors of $f(x)$.

Polynomial f splits into n linear factors, namely $x^{n-1}(x+1)$. Because $F[x]$ has unique factorization, any factor must be an associate of a product of some subset of those n linear factors. Hence, the factors are precisely $ax^i(x + 1)^j$, where a is any nonzero element of F, i satisfies $0 \le i \le n - 1$, and j satisfies $0 \le j \le 1$.

6. For ring R, $a \in R$, and $n \in \mathbb{N}$, we say a has *additive order* n if $\underbrace{a + a + \cdots + a}_{n} = 0_R$, and for $m < n$ we have $\underbrace{a + a + \cdots + a}_{m} \ne 0_R$. We write this $ord_R(a) = n$. Suppose every element of R has an order (not necessarily the same one). Prove that every element of $R[x]$ has an order.

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$, an arbitrary element of $R[x]$. Set $t = \prod_{i=0}^{n} ord_R(a_i)$. We calculate $\underbrace{f + f + \cdots f}_{t} = (\underbrace{a_n + \cdots + a_n}_{t})x^n + \cdots + (\underbrace{a_1 + \cdots + a_1}_{t})x + (\underbrace{a_0 + \cdots + a_0}_{t}) = 0$, since t is a multiple of the orders of each coefficient. Hence f has some order, and that order is at most t. [If we choose t as the lcm of the orders of the coefficients, instead of their product, then we get the order of f exactly (instead of a bound).]