MATH 521A: Abstract Algebra
Exam 3 Solutions

1. Factor $f(x) = x^4 + 3x^3 - x^2 + 3x + 1$ into irreducibles in $\mathbb{Z}_5[x]$.

   We first look for any linear factors, by computing $f(0) = 1, f(1) = 2, f(2) = 3, f(3) = 3, f(-1) = 0$. Hence $(x + 1)$ is a (possibly multiple) factor of $f(x)$. We now calculate $f(x) = (x+1)(x^3+2x^2+2x+1)$. It turns out that -1 is a root of x^3+2x^2+2x+1, so we divide again to get $f(x) = (x + 1)^2(x^2 + x + 1)$. Now -1 is not a root of $x^2 + x + 1$; hence $x^2 + x + 1$ has no roots. Since it is of degree 2, it is irreducible and we are done.

2. Prove that $f(x) = x^3 + 9x^2 + 8x + 96301$ is irreducible in $\mathbb{Q}[x]$.

   Eisenstein's criterion is not appealing, as 96301 is hard to factor (it equals $23 \cdot 53 \cdot 79$, so to use Eisenstein we would need to test 16 values).

   By Gauss' Lemma, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if it is irreducible in $\mathbb{Z}[x]$. By homework 8 problem 6, $f(x)$ is irreducible in $\mathbb{Z}[x]$ if it is irreducible in $\mathbb{Z}_3[x]$. Working in $\mathbb{Z}_3$, we have $f(x) = x^3 + 2x + 1$. We check $f(0) = 1, f(1) = 1, f(-1) = 1$. Hence $f(x)$ has no linear factors over $\mathbb{Z}_3$, but since it is of degree 3 it is irreducible.

3. Let R be an integral domain. Prove that all linear polynomials in $R[x]$ are irreducible, if and only if R is a field.

   Let $f(x) = ax + b$, for $a, b \in R$. If $f(x) = g(x)h(x)$, then (since R is an integral domain), one of g, h must be of degree 0. If R is a field, this is a unit, so $f(x)$ is irreducible. On the other hand, if R is not a field, there is some $c \in R$ that is not zero and not a unit. We take $f(x) = cx + c = c(x + 1)$, a factorization into two nonunits. Hence $f(x)$ is reducible.

4. Set $f(x) = x^4 + 3x^3 - x^2 + x - 1, g(x) = 2x^5 + 3x^4 + 3x^2 + 2x - 1$, both in $\mathbb{Z}_5[x]$. Use the extended Euclidean algorithm to find $\gcd(f, g)$ and to find polynomials $a(x), b(x)$ such that $\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.

   $$\begin{aligned} 2x^5 + 3x^4 + 3x^2 + 2x - 1 &= (2x + 2)(x^4 + 3x^3 - x^2 + x - 1) + (x^3 + 3x^2 + 2x + 1) \\ x^4 + 3x^3 - x^2 + x - 1 &= (x)(x^3 + 3x^2 + 2x + 1) + (2x^2 - 1) \\ x^3 + 3x^2 + 2x + 1 &= (3x - 1)(2x^2 - 1) + 0 \end{aligned}$$

   Hence $\gcd(f, g)$ is the monic multiple of $2x^2 - 1$, which is $3(2x^2 - 1) = x^2 + 2$. We now back-substitute, as $2x^2-1 = (x^4+3x^3-x^2+x-1)-x(x^3+3x^2+2x+1) = (x^4+3x^3-x^2+x-1)-x(2x^5+3x^4+3x^2+2x-1-(2x+2)(x^4+3x^3-x^2+x-1)) = (x^4+3x^3-x^2+x-1)(1+x(2x+2))+(2x^5+3x^4+3x^2+2x-1)(-x)$. We multiply both sides by the unit 3, to get $x^2+2 = (x^4+3x^3-x^2+x-1)3(1+x(2x+2))+(2x^5+3x^4+3x^2+2x-1)3(-x)$. Hence $a(x) = x^2 + x + 3, b(x) = 2x$.

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

   We factor $f(x)$ into irreducibles as $f(x) = (x - 1)x^{n-1}$. Because $F[x]$ has unique factorization, every divisor of $f(x)$ must be of the form $u(x - 1)^i x^j$, where u is a unit (i.e. any nonzero element of F), i satisfies $0 \leq i \leq 1$, and j satisfies $0 \leq j \leq n - 1$.

6. Let $f(x), g(x), h(x) \in F[x]$. Suppose that $f(x)|g(x)h(x)$ and $\gcd(f(x), g(x)) = 1$. Prove that $f(x)|h(x)$.

We use the extended Euclidean algorithm to find $a(x), b(x) \in F[x]$ such that $1 = \gcd(f, g) = a(x)f(x)+b(x)g(x)$. Multiply both sides by $h(x)$ to get $h(x) = a(x)f(x)h(x)+b(x)g(x)h(x)$. Because $f(x)|g(x)h(x)$, there is some $c(x) \in F[x]$ such that $g(x)h(x) = f(x)c(x)$. Substituting, we get $h(x) = a(x)f(x)h(x) + b(x)f(x)c(x) = f(x)[a(x)h(x) + b(x)c(x)]$. Hence $f(x)|h(x)$.

7. Let p be an odd prime. Prove there is at least one $a \in \mathbb{Z}_p$ such that $x^2 - a$ is irreducible in $\mathbb{Z}_p[x]$.

Consider the function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f : x \mapsto x^2$. Note that $f(1) = f(-1) = 1$, so it is not injective ($1 \neq -1$ in $\mathbb{Z}_p$ for odd p). Since its domain is the same as its codomain, and is finite, f is also not surjective. Hence there is some $a \in \mathbb{Z}_p$ not in the range of f. Take that for our a. Now, $x^2 - a$ will have no roots, since if b were a root then $f(b) = b^2 = a$ (which is impossible). Since $x^2 - a$ is quadratic polynomial with no roots, it is irreducible.

8. We call a polynomial in $F[x]$ *cinom* if its constant coefficient is 1. Suppose that $f(x)$ is a nonconstant, cinom, polynomial in $F[x]$. Prove that we may write $f(x)$ as the product of irreducible cinom polynomials.

By Theorem 4.14, we may write $f(x) = f_1(x) \cdots f_k(x)$, the product of irreducible polynomials. The proof proceeds via induction on k. If $k = 1$ then $f(x)$ is itself irreducible and cinom, so it is the product of one irreducible cinom polynomial. Otherwise we write $f(x) = f_1(x)g(x)$, where $g(x) = f_2(x) \cdots f_k(x)$. Suppose that $f_1(x)$ has constant coefficient a, while $g(x)$ has constant coefficient b. Since $f(x)$ is cinom, we know that $ab = 1$. Hence we can write $f(x) = (bf_1(x))(ag(x))$. Now, $bf_1(x)$ has constant coefficient $ba = 1$, while $ag(x)$ has constant coefficient $ab = 1$. So both factors are cinom. Since $f_1(x)$ was irreducible, so is $bf_1(x)$. Since $ag(x)$ is cinom, nonconstant, and of degree smaller than $f(x)$, we may apply the inductive hypothesis to write $ag(x)$ as the product of irreducible cinom polynomials.