Math 581 Problem Set 2 Solutions

1. Determine if the following polynomials are irreducible over $\mathbb{Q}$. If they are, prove it. If not, write them as a product of irreducible polynomials.
(a) $f(x) = 5x^{11} - 6x^4 + 12x^3 + 36x - 6$

This is irreducible by Eisenstein's criterion with $p = 3$.

(b) $f(x) = 2x^4 + 7x^3 + 5x^2 + 7x + 3$

The Rational Root Theorem gives the factorization

$$f(x) = (x+3)(2x+1)(x^2+1).$$

(c) $f(x) = 9x^4 + 4x^3 - 3x + 7$

Consider this polynomial reduced modulo 2. One then only needs to show that $x^4 + x + 1$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$. There are no roots as one can check by substituting $\overline{0}$ and $\overline{1}$ into the equation. To see it does not factor as quadratics, use the method of undetermined coefficients. Since the coefficients must all be $\overline{0}$ or $\overline{1}$, it is particularly easy to check. Thus $f(x)$ is irreducible. ■

2. Let F be a field and $f(x) \in F[x]$. If $c \in F$ and $f(x+c)$ is irreducible in $F[x]$, prove that $f(x)$ is irreducible in $F[x]$.

Proof: Suppose that $f(x)$ is reducible, i.e., there exist nonconstant $g(x), h(x) \in F[x]$ so that $f(x) = g(x)h(x)$. In particular, then we have $f(x+c) = g(x+c)h(x+c)$. Note that $g(x+c)$ and $h(x+c)$ have the same degree at $g(x)$ and $h(x)$; in particular, they are nonconstant polynomials. ■

3. Let p be a prime. Prove that $\sqrt[n]{p} \notin \mathbb{Q}$ for all integers $n \geq 2$. (It may help to look at the polynomial $f(x) = x^n - p$.)

Proof: Note that $f(x) = x^n - p$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion applied with the prime p. If $\sqrt[n]{p} \in \mathbb{Q}$, then we must have that $f(x)$ has a root in $\mathbb{Q}$, so is reducible, a contradiction. ■

4. Show that there are infinitely many integers n such that $f(x) = x^9 + 12x^5 - 21x + n$ is irreducible in $\mathbb{Q}[x]$.

Proof: Set $n = 3 \cdot 2^k$ for $k \in \mathbb{N}$. With this value of n we have that $f(x)$ is irreducible for infinitely many values of n by Eisenstein's criterion with $p = 3$. ■

5. Prove that $f(x) \in (\mathbb{Z}/2\mathbb{Z})[x]$ has $x + \overline{1}$ as a factor if and only if it has an even number of nonzero coefficients.

Proof: Suppose $x + \overline{1}$ is a factor of $f(x) = a_n x^n + \cdots + a_1 x + a_0$. This means that $f(\overline{1}) = \overline{0}$, i.e., $a_n + \cdots + a_1 + a_0 = \overline{0}$. These are all $\overline{0}$'s and $\overline{1}$'s since we are in $\mathbb{Z}/2\mathbb{Z}$, so we see this is $\overline{0}$ if and only if it is a multiple of 2, i.e., if and only if there are an even number of nonzero terms. ■

6. Prove that for any prime p, $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof: Recall that one has the identity

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

We prove that $f(x+1)$ is irreducible and then apply Problem 2 to conclude that $f(x)$ is irreducible. Note that

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + px^{p-1} + \cdots + px}{x} \\ &= x^{p-1} + px^{p-2} + \cdots + p. \end{aligned}$$

Using that the binomial coefficients occurring above are all divisible by p, we have that $f(x+1)$ is irreducible by Eisenstein's criterion applied with p. ■.

7. In this problem you will show that the polynomial $f(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ but is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p.
(a) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: It is easy to see there are no rational roots by the Rational Root Theorem. To see it does not factor as two quadratic terms we use the method of undetermined coefficients. Suppose there are $a, b, c, d \in \mathbb{Z}$ so that $x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$. This leads to the equations

$$\begin{aligned} a + c &= 0 \\ d + b + ac &= -10 \\ ad + bc &= 0 \\ bd &= 1. \end{aligned}$$

This leads to the equations $bd = 1$, $d + b - a^2 = -10$, and $a(d - b) = 0$ since $a = -c$. Thus we have either $a = 0$ or $b = d$. Since $bd = 1$ we must have $b = d = 1$ or $b = d = -1$. If $a = 0$ then $d+b = -10$, which is a contradiction. If $a \neq 0$, then we have two possibilities. If $b = d = 1$ then $a^2 = 8$, which is a contradiction. Similarly, if $b = d = -1$ we get a contradiction. Thus it must be that $f(x)$ is irreducible in $\mathbb{Q}[x]$. ■

(b) Prove that $f(x)$ is reducible in $(\mathbb{Z}/p\mathbb{Z})\,[x]$ for every prime p. It may be helpful to use the method of undetermined coefficients along with the following lemma, which you may use without proof:
Lemma: If neither 2 nor 3 is a square modulo p, then 6 is a square modulo p.

Proof: We need to determine how we can factor this polynomial modulo p for each prime p. First we suppose that 2 is a square modulo p, i.e., there is an α so that $\alpha^2 = \overline{2}$. Then our polynomial factors as

$$x^4 - \overline{10}x^2 + \overline{1} = (x^2 + \overline{2}\alpha x - \overline{1})(x^2 - \overline{2}\alpha x - \overline{1}).$$

Now if 3 is a square modulo p, i.e., there is a β so that $\beta^2 = \overline{3}$, then we can factor the polynomial as

$$x^4 - \overline{10}x^2 + \overline{1} = (x^2 + \overline{2}\beta x + \overline{1})(x^2 - \overline{2}\beta x + \overline{1}).$$

If neither 2 nor 3 is a square modulo p, then the lemma shows that 6 must be a square modulo p, say $\gamma^2 = \overline{6}$. In this case the polynomial factors as

$$x^4 - \overline{10}x^2 + \overline{1} = (x^2 - (\overline{5} + \overline{2}\gamma))(x^2 - (\overline{5} - \overline{2}\gamma)).$$

Thus we see that $f(x)$ is reducible modulo every prime p. ■