Math 110A HW 5

Sava Spasojevic

July 29, 2018

1) Use the Rational Root Test to write $x^5 + 4x^4 + x^3 - x^2$ as a product of irreducible polynomials in $\mathbb{Q}[x]$.

Factoring yields $x^2(x^3 + 4x^2 + x - 1)$. For the polynomial in parenthesis, $r = \pm 1$ and $s = \pm 1$. Thus, the only possible roots are ± 1. Neither are roots however, so the final product is $x^2(x^3 + 4x^2 + x - 1)$.

2) Show that $\sqrt{p}$ is irrational for every positive prime integer p.

Proof. Suppose that p is a positive prime integer. Consider the function $f(x) = x^2 - p$. By The Rational Root Test, the possible roots in $\mathbb{Q}$ of $f(x)$ are of the form $\frac{r}{s}$ where r is one of $\pm 1, \pm p$ and s is ± 1. This reduces the search for roots of $f(x)$ to $\pm 1, \pm p$. Plugging in yields

$$f(\pm p) = (\pm p)^2 - p = p^2 - p \neq 0$$
$$f(\pm 1) = (\pm 1)^2 - p = 1 - p \neq 0$$

This is the case since $p \neq \pm 1, 0$. Thus, there are no rational roots of $f(x)$. But we know that $f(\sqrt{p}) = (\sqrt{p})^2 - p = p - p = 0$ This shows that $\sqrt{p}$ is a root. But, since there are no rational roots, $\sqrt{p} \notin \mathbb{Q}$. Thus, $\sqrt{p}$ is irrational. $\square$

3) Show that $f(x) = 9x^4 + 4x^3 - 3x + 7$ is irreducible in $\mathbb{Q}[x]$ by finding a prime p such that $f(x)$ is irreducible in $\mathbb{Z}_p[x]$.

Proof. Consider $p = 2$. Then $f(x)$ becomes

$$\bar{f}(x) = x^4 - x + 1 \tag{1}$$

By the Rational Root Test, the only possible roots are ± 1. But,

$$\bar{f}(1) = 1^4 - 1 + 1 = 1 \neq 0$$
$$\bar{f}(-1) = (-1)^4 - 1 + 1 = 1 \neq 0$$

Thus, this polynomial has no first degree factors. The only quadratic factors in $\mathbb{Z}_2[x]$ are x^2, x^2+x, and x^2+x+1. However, if these were factors, then (1) would have linear factors, a contradiction. Finally, if $\bar{f}(x)$ has a factor of degree 3 then the other factor would have degree 1, another contradiction. Therefore, $\bar{f}(x)$ is irreducible in $\mathbb{Z}_2[x]$, hence by Theorem 4.25 $f(x)$ is irreducible in $\mathbb{Q}[x]$. $\square$

4) Prove that for p prime,

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

Proof. Consider $(x-1)f(x) = x^p - 1$. Then,

$$f(x) = \frac{x^p - 1}{x - 1}$$
$$\text{and } f(x+1) = \frac{(x+1)^p - 1}{x}$$

Expanding $(x+1)^p$ by the Binomial theorem gives,

$$f(x+1) = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + \binom{p}{p-1}x}{x}$$

$$f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1}$$

Note that $p \nmid 1$ and $p \mid \binom{p}{p-1}$ since $\binom{p}{p-1} = p$. But $p^2 \nmid p = \binom{p}{p-1}$, so by Eisenstein's Criterion, $f(x+1)$ is irreducible. Since $f(x+1)$ is irreducible $f(x)$ too must be irreducible. □

5) Prove that $f(x) \equiv g(x) \mod p(x)$ if and only if $f(x)$ and $g(x)$ leave the same remainder when divided by $p(x)$.

Proof. Suppose that $f(x) \equiv g(x) \mod p(x)$. Then

$$f(x) - g(x) = p(x)q(x) \text{ for some } q(x) \in F[x]$$

$f(x) = p(x)q_1(x) + r_1(x)$ and $g(x) = p(x)q_2(x) + r_2(x)$. Subtracting gives,

$$f(x) - g(x) = p(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x))$$

But, $p(x) \mid f(x) - g(x)$ so $r_1(x) - r_2(x) = 0$ or $r_1(x) = r_2(x)$, meaning that $f(x)$ and $g(x)$ have the same remainder.

Assume that $f(x)$ and $g(x)$ leave the same remainder when divided by $p(x)$. This means $[f(x)] = [g(x)]$. Since $f(x) \equiv f(x) \mod p(x)$, $f(x) \in [f(x)]$. So, $f(x) \in [g(x)]$ by assumption. This means $f(x) \equiv g(x) \mod p(x)$. □

6) Let $f(x), g(x), p(x) \in \mathbb{Q}[x]$. Determine whether $f(x) \equiv g(x) \mod p(x)$ where $f(x) = x^5 - 2x^4 + 4x^3 - 3x + 1; g(x) = 3x^4 + 2x^3 - 5x^2 + 2; p(x) = x^2 + 1$.

$f(x) - g(x) = x^5 - 5x^4 + 2x^3 + 5x^2 - 3x - 2 = (x^2+1)q(x)$ for some $q(x) \in F[x]$.

$$x^5 - 5x^4 + 2x^3 + 5x^2 - 3x - 2 = (x^3 - 5x^2 + x + 10)(x^2+1) - 4x - 8$$

There is a nonzero remainder, hence $f(x) \not\equiv g(x) \mod p(x)$.

7) Prove or disprove: If $p(x)$ is irreducible in $F[x]$ and $f(x)g(x) \equiv 0 \mod p(x)$, then $f(x) \equiv 0 \mod p(x)$ or $g(x) \equiv 0 \mod p(x)$.

Proof. $f(x)g(x) \equiv 0 \mod p(x)$ implies that $[f(x)g(x)] = [0]$. Or that $[f(x)] \cdot [g(x)] = [0]$. By Theorem 5.2, either $[f(x)] = [0]$ or $[g(x)] = 0$. This says that $f(x) \equiv 0 \mod p(x)$ or $g(x) \equiv 0 \mod p(x)$. □

8) If $p(x)$ is not irreducible in $F[x]$, prove that there exist $f(x), g(x) \in F[x]$ such that $f(x) \not\equiv 0 \mod p(x)$ and $g(x) \not\equiv 0 \mod p(x)$, but $f(x)g(x) \equiv 0 \mod p(x)$.

Proof. Suppose that $p(x)$ is not irreducible in $F[x]$. Then $p(x)$ can be written as the product of two lower degree polynomials, call them $f(x), g(x) \in F[x]$. Thus, $f(x)g(x) = p(x)$ or $f(x)g(x) - 0 = p(x) \cdot 1_F$. Thus, $f(x)g(x) \equiv 0 \mod p(x)$. But since $f(x)$ and $g(x)$ have lower degree relative to $p(x)$, it is true that $f(x) \not\equiv 0 \mod p(x)$ and $g(x) \not\equiv 0 \mod p(x)$. This makes sense, since if it were not the case $f(x) = p(x)q(x)$ would imply that $\deg f(x) = \deg p(x) + \deg q(x)$ which contradicts the fact that $f(x)$ has lower degree than $p(x)$. The same reasoning applies for $g(x)$. □

9) If $f(x)$ is relatively prime to $p(x)$, prove that there exists a polynomial $g(x) \in F[x]$ such that $f(x)g(x) = 1_F \mod p(x)$.

Proof. Suppose that $f(x)$ is relatively prime to $p(x)$. Then $(f(x), p(x)) = 1_F$. This means $\exists g(x), h(x) \in F[x]$ such that $f(x)g(x) + p(x)h(x) = 1_F$ or that $f(x)g(x) - 1_F = p(x)h(x)$. But, this is the same as saying $f(x)g(x) = 1_F \mod p(x)$. □

10) Show the $\mathbb{R}/(x^2+1)$ is a field by verifying that every nonzero congruence class $[ax+b]$ is a unit.

Proof.

$$\begin{aligned}
[ax+b]\left[\frac{-a}{a^2+b^2}x-\frac{b}{a^2+b^2}\right] &= \left[\frac{-a^2x^2-abx+abx+b^2}{a^2+b^2}\right] \\
&= \left[\frac{-a^2x^2+b^2}{a^2+b^2}\right] \\
&= \left[\frac{a^2+b^2}{a^2+b^2}\right] \\
&= [1]
\end{aligned}$$

Thus, $[ax+b]$ has a multiplicative inverse, so it is a unit. □

11) In each part, explain why $[f(x)]$ is a unit in $F[x]/(p(x))$ and find its inverse.
(a) $[f(x)] = [2x-3] \in \mathbb{Q}/(x^2-1)$
(b) $[f(x)] = [x^2+x+1] \in \mathbb{Z}_3[x]/(x^2+1)$

(a) x^2-1 is irreducible in $\mathbb{Q}$, thus $(2x-3, x^2-1) = 1_F$. This means $2x-3$ is a unit. To find the inverse, we solve for a, b, c, d in

$$\begin{aligned}
(2x-3)(ax+b)+(cx+d)(x^2-1) &= 1 \\
cx^3+(2a+d)x^2+(2b-3a-2c)x-3b-2d &= 1
\end{aligned}$$

After performing calculations (my work is attached to the back), we get $c=0, d=4, b=-3, a=-2$. Thus,

$$(2x-3)(-2x-3)+4(x^2-1)=1$$

So the inverse of $2x-3$ is $-2x-3$.

(b) Clearly $(x^2+x+1, x^2+1) = 1_F$ in $\mathbb{Z}_3[x]$. This means x^2+x+1 is a unit. To find the inverse, we solve for a, b, c, d in

$$\begin{aligned}
(x^2+x+1)(ax+b)+(cx+d)(x^2+1) &= 1 \\
(a+c)x^3+(a+b+d)x^2+(a+b+c)xb+d &= 1
\end{aligned}$$

After performing calculations (my work is attached to the back), we get $c=1, d=1, b=0, a=2$. Thus,

$$(x^2+x+1)(2x)+(x+1)(x^2+1)=1$$

So the inverse of x^2+x+1 is $2x$.

12) Find a fourth degree polynomial in $\mathbb{Z}_2[x]$ whose roots are the four elements of the field $\mathbb{Z}_2[x]/(x^2+x+1)$.

Consider $f(x) = x^2+x+1$

$$\begin{aligned}
f(0) &= 1 \neq 0 \\
f(1) &= 3 = 1 \neq 0 \\
f(x) &= x^2+x+1 = 0 \\
f(x+1) &= (x+1)^2+x+1+1 \\
&= x^2+3x+3 \\
&= x^2+x+1 = 0
\end{aligned}$$

This implies that x and $x+1$ are roots for x^2+x+1. So a fourth degree polynomial with all four elements in $\mathbb{Z}_2[x]$ as roots is $x(x+1)(x^2+x+1)$.