Math 402 Homework 5

Alexandre Lipson

February 19, 2025

Problem 1. Find all irreducible polynomials of the given degree in the given field.

a) Degree 2 in $\mathbb{Z}_2[x]$.

b) Degree 3 in $\mathbb{Z}_2[x]$.

c) Degree 2 in $\mathbb{Z}_3[x]$.

Proof of a. As given in lecture, we have x^2+x+1 as the only such irreducible polynomial. $x \cdot x = x^2$, $x(x+1) = x^2+x$, and $(x+1)^2 = x^2+1$, which covers all $2^2 = 4$ possible polynomials of degree 2 in $\mathbb{Z}_2[x]$. □

Proof of b. We will consider the product of all combinations of irreducible linear factors x and $x+1$.

$$\begin{aligned} x \cdot x \cdot x = &\quad x^3, \\ (x)(x)(x+1) = &\quad x^3+x^2, \\ (x)(x+1)(x+1) = &\quad x^3+x, \\ (x+1)(x+1)(x+1) = &\quad x^3+x^2+x+1. \end{aligned}$$

We have x^3+1, x^3+x+1, x^3+x^2+x, and x^3+x^2+1 left over; these must be the irreducibles as we have covered all $2^3 = 8$ possible degree 3 polynomials in $\mathbb{Z}_2[x]$. □

Proof of c . We have $2 \cdot 3^2 = 18$ possible polynomials of degree 2 in $\mathbb{Z}_3[x]$. We will first consider the polynomials with leading coefficient of 1.

$$\begin{aligned} x \cdot x = &\quad x^2 \\ (x)(x+1) = &\quad x^2+x \\ (x)(x+2) = &\quad x^2+2x \\ (x+1)(x+1) = &\quad x^2+2x+1 \\ (x+1)(x+2) = &\quad x^2+2 \\ (x+2)(x+2) = &\quad x^2+x+1 \end{aligned}$$

Now, we are left with three remaining irreducible polynomials with leading coefficient of 1. These are x^2+x+2, x^2+1, and x^2+2x+2.

Since 2 is a unit in $\mathbb{Z}_3$, we also have that the associate polynomials with leading coefficient 2 are irreducibles. So, we also have $2x^2+2x+1$, $2x^2+2$, and $2x^2+x+1$.

Thus, we have found 6 irreducibles and 12 reducibles for a total of 18 possible polynomials. □

Problem 2. Determine if the give polynomial is reducible.

a) $x^2 - 3$ in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$.

b) $x^2 + x - 2$ in $\mathbb{Z}_3[x]$ and in $\mathbb{Z}_7[x]$.

Proof of a. The polynomial of degree 2 has no rational roots, so it is irreducible over $\mathbb{Q}[x]$. In $\mathbb{R}[x]$, it factors as $(x + \sqrt{3})(x - \sqrt{3})$. □

Proof of b. $x^2 + x - 2 = x^2 + x + 1 = (x + 2)(x + 2)$ in $\mathbb{Z}_3[x]$, so the polynomial is reducible over $\mathbb{Z}_3[x]$.

$x^2 + x - 2 = x^2 + x + 5$ in $\mathbb{Z}_7[x]$ factors as $(x + 2)(x + 6)$ in $\mathbb{Z}_7[x]$, so it is a reducible polynomial. □

Problem 3. a) Prove $x^2 + 2$ is irreducible in $\mathbb{Z}_5[x]$.

b) Factor $x^4 - 4$ as a product of irreducibles in $\mathbb{Z}_5[x]$.

Proof of a. Suppose $x^2 + 2$ was reducible in $\mathbb{Z}_5[x]$. Then, it must have integer roots. But,

$$\begin{aligned} 0^2 + 2 = &\quad 2 \neq 0 \\ 1^2 + 2 = &\quad 3 \neq 0 \\ 2^2 + 2 = &\quad 6 = 1 \neq 0 \\ 3^2 + 2 = &\quad 11 = 1 \neq 0 \\ 4^2 + 2 = &\quad 18 = 3 \neq 0. \end{aligned}$$

Since $x^2 + 2$ has no integer roots, then it must be irreducible. □

Proof of b. We can factor by the difference of squares,

$$x^4 - 4 = (x^2 + 2)(x^2 - 2).$$

By part a, $x^2 + 2$ is irreducible. So, we wish to show that $x^2 - 2 = x^2 + 3$ is irreducible.

By the table above, $x^2 + 2$ was never congruent to 4 mod 5, so $x^2 + 2 + 1 = x^2 + 3 = x^2 - 2$ in $\mathbb{Z}_5[x]$ has no rational roots.

Thus, $x^4 - 4 = (x^2 + 2)(x^2 + 3)$ is a product of irreducible polynomials. □

Problem 4. Find remained when $f(x)$ is divided by $g(x)$.

i) $f(x) = x^{10} + x^8$, $g(x) = x - 1$ in $\mathbb{Q}[x]$.

ii) $f(x) = 2x^5 - 3x^4 + x^3 + 2x + 3$, $g(x) = x - 3$ in $\mathbb{Z}_5[x]$.

Proof of a. We will perform polynomial long division, noting that the middle coefficients are the result of a repeated production and cancellation of the term $2x^k$ for $1 \leq k \leq 7$.

$$\begin{array}{r l}
 & x^9 + x^8 + 2x^7 + \cdots + 2x + 2 \\ \cline{2-2}
x - 1 \big) & x^{10} \qquad + x^8 \\
 & \underline{-x^{10} + x^9} \\
 & \qquad x^9 + x^8 \\
 & \qquad \underline{-x^9 + x^8} \\
 & \qquad\qquad 2x^8 \\
 & \qquad\quad \underline{-2x^8 + 2x^7} \\
 & \qquad\qquad\qquad \ddots \\
 & \qquad\qquad\qquad\quad 2x^2 \\
 & \qquad\qquad\qquad\quad \underline{-2x^2 + 2x} \\
 & \qquad\qquad\qquad\qquad\quad 2x \\
 & \qquad\qquad\qquad\qquad\quad \underline{-2x + 2} \\
 & \qquad\qquad\qquad\qquad\qquad\quad 2
\end{array}$$

So, the remainder of $f(x)$ divided by $g(x)$ is 2. □

Proof of b.

$$\begin{array}{r l}
 & \qquad 2x^4 + 3x^3 \qquad + 2 \\ \cline{2-2}
x - 3 \big) & 2x^5 - 3x^4 + \ x^3 + 2x + 3 \\
 & \underline{-2x^5 + 6x^4} \\
 & \qquad 3x^4 + \ x^3 \\
 & \qquad \underline{-3x^4 + 9x^3} \\
 & \qquad\qquad\qquad 2x + 3 \\
 & \qquad\qquad\qquad \underline{-2x + 6} \\
 & \qquad\qquad\qquad\qquad 4
\end{array}$$

Thus, the remainder of $f(x)$ divided by $g(x)$ is 4. □

Problem 5. Determine if the given polynomial is irreducible.

a) $x^2 - 7$ in $\mathbb{R}[x]$.
The difference of squares gives that $\pm\sqrt{7}$ is a root. Therefore the polynomial is reducible in $\mathbb{R}[x]$.

b) $x^2 - 7$ in $\mathbb{Q}[x]$.
$\sqrt{7} \notin \mathbb{Q}$, so the polynomial does not have rational roots, and is therefore irreducible.

c) $x^2 + 7$ in $\mathbb{C}[x]$.
By the difference of squares, $\pm\sqrt{7i}$ is a root in $\mathbb{C}$; therefore the polynomial is reducible in $\mathbb{C}[x]$.

d) $2x^3 + x^2 + x + 2$ in $\mathbb{Z}_5[x]$.
Note that $2x^3 + x^2 + x + 2 = 2(x^3 + 3x^2 + 3x + x)$ in $\mathbb{Z}_5[x]$. This polynomial is $2(x+1)^3$ by the binomial expansion. Since the polynomial factors as $2(x+1)^3$, it is reducible.

e) $x^3 - 9$ in $\mathbb{Z}_{11}[x]$.
Note that $4^3 - 9 = 64 - 9 = 55 = 0$ in $\mathbb{Z}_{11}$. So, $x = 4$ is a rational root. Since the polynomial has a rational root, it is reducible.

f) $x^4 + x^2 + 1$ in $\mathbb{Z}_3[x]$.
We have a rational root at $x = 1$ as $1^4 + 1^2 + 1 = 3 = 0$ in $\mathbb{Z}_3$. Since the polynomial has a rational root, then it is reducible.

Problem 6. Let $a \in F$ be a nonzero root of

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n \in F[x].$$

Prove that a^{-1} is a root of

$$g(x) = c_n + c_{n-1} x + \cdots + c_1 x^{n-1} + c_0 x^n.$$

Proof. Plug in a^{-1} to $g(x)$,

$$g(a^{-1}) = c_n + c_{n-1} a^{-1} + \cdots + c_1 a^{-(n-1)} + c_0 a^{-n}.$$

Since a is a root of f, then $f(a) = 0$. Multiplying by a^n, we have,

$$a^n g(a^{-1}) = a^n c_n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 = f(a) = 0.$$

Since $a \neq 0$, then $g(a^{-1}) = 0$. So, a^{-1} is a root of g. □

Problem 7. $a \in F$ is a multiple root of $f(x) \in F[x]$ iff $(x-a)^k$ is a factor of f for $k \geq 2$.

a) Prove that $a \in \mathbb{R}$ is a multiple root of $f(x) \in \mathbb{R}[x]$ iff it is a root of both f and f', the derivative of f.

b) Prove for $f(x) \in \mathbb{R}[x]$, if f is relatively prime to f', then f has no multiple roots in $\mathbb{R}$.

Proof of a. ($\Longrightarrow$) Let $f(x) = (x-a)^k g(x)$ for some $k \geq 2$.

Then, $f'(x) = (x-a)^{k-1}(kg(x) + (x-a)g'(x))$.

Thus, a is a root of both f and f'.

($\Longleftarrow$) As above, let $f'(x) = (x-a)(2g(x) + (x-a)g'(x))$.

Then, $f(x) = (x-a)^2 g(x)$.

So, a is a multiple root of f. □

Problem 8. Let $\mathbb{Q}[\sqrt{2}]$ be the set of reals of the form

$$r_0 + r_1\sqrt{2} + r_2(\sqrt{2})^2 + \cdots + r_n(\sqrt{2})^n,$$

with $n \geq 0$ and $r_i \in \mathbb{Q}$.

a) Prove $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

b) Prove $\theta : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ defined by $\theta(f(x)) \mapsto f(\sqrt{2})$ is epimorphic, but not monomorphic.

Proof of a. Firstly, we have that $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$.

Note that we have the additive identity zero in $\mathbb{Q}[\sqrt{2}]$.

Then, addition in $\mathbb{Q}[\sqrt{2}]$ is closed because we add corresponding coefficients for each power of $\sqrt{2}$ and addition is closed under $\mathbb{Q}$.

Similarly, for multiplication, we have that all the new coefficients of a product come from adding and multiplying the coefficients in the factors. Since multiplication is closed under $\mathbb{Q}$, then it is also closed under $\mathbb{Q}[\sqrt{2}]$.

Since $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ and $\mathbb{Q}[\sqrt{2}]$ is closed under the operations of addition and multiplication, then $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$. □

Proof of b. We see that the image of f on $\sqrt{2}$, $f(\sqrt{2})$ is a subset of the image of f on all $x \in \mathbb{R}$, so the map θ with $f(x) \mapsto f(\sqrt{2})$ is surjective.

Note that, $\forall x \in \mathbb{R}$, $x \neq \sqrt{2}$ is not mapped under θ, so @q is not injective, and therefore cannot be bijective.

Now, we will show that θ is a homomorphism. $\forall f, g \in \mathbb{Q}[x]$, we have for addition

$$f(\sqrt{2}) + g(\sqrt{2}) = (f(x) + g(x))(\sqrt{2}) = \theta(f(x) + g(x)) = \theta(f(x)) + \theta(g(x)) = f(\sqrt{2}) + g(\sqrt{2}),$$

and for multiplication,

$$f(\sqrt{2})g(\sqrt{2}) = (f(x)g(x))(\sqrt{2}) = \theta(f(x)g(x)) = \theta(f(x))\theta(g(x)) = f(\sqrt{2})g(\sqrt{2}).$$

Therefore θ is a ring homomorphism.

Since θ is a homomorphism and a surjection, then θ is an epimorphism. □

Problem 9. Consider $f(x) = x^4 - 6x^2 + 1$.

a) Write f as a product of irreducible polynomials in $\mathbb{Q}[x]$.

b) Write f as a product of irreducible polynomials in $\mathbb{R}[x]$.

c) Explain why parts a and b do not contradict the Unique Factorization Theorem in $F[x]$.

Proof of a. f factors as $(x^2 + 2x - 1)(x^2 - 2x - 1)$. These factors themselves are polynomials of degree 2 with irrational roots, so they are irreducible in $\mathbb{Q}$. Thus, we're done. □

Proof of b. f factors further in $\mathbb{R}[x]$; the quadratics in part a factor in $\mathbb{R}[x]$, giving $x = \pm(1 \pm \sqrt{2})$, which can be written as the product of irreducible linear polynomials,

$$f(x) = (x + (1 + \sqrt{2}))(x - (1 + \sqrt{2}))(x + (1 - \sqrt{2}))(x - (1 - \sqrt{2})).$$

□

Proof of c. The Unique Factorization Theorem says that factorizations are unique within a given ring, but $\mathbb{Q}[x]$ and $\mathbb{R}[x]$ are different rings; so, while each ring has its own unique factorization for any given polynomial, these need not be the same between different rings.

What about isomorphic rings? i would suspect that the factor structure is maintained across isomorphic rings. □

Problem 10. Use the Rational Root Theorem to write the polynomials as a product of irreducibles in $\mathbb{Q}[x]$.

i) $f(x) = 3x^5 + 2x^4 - 7x^3 + 2x^2$.

ii) $g(x) = 2x^4 - 5x^3 + 3x^2 + 4x - 6$.

Proof of i. First, we can factor out x^2, so we have $f = x^2(3x^3 + 2x^2 - 7x + 2)$.

Now, we can use the Rational Root Test on the right-hand factor. This gives us a root of the form $q = \frac{r}{s} \in \mathbb{Q}$ where $r|2$ and $s|3$.

So, we could have $r = \pm 1, \pm 2$ and $s = \pm 1, \pm 3$, which gives the possible $q = \pm 1, \pm 2, \pm \frac{1}{3} \pm \frac{2}{3}$.

We will first check $x = 1$, $3(1)^3 + 2(1)^2 - 7(1) + 2 = 0$, so $x - 1$ is a factor of f.

Now that we have a factor, we can use it to divide and simply the remaining unfactored polynomial.

With polynomial long division, we get that $f = x^2(x-1)(3x^2 + 5x - 2)$.

We can apply the Rational Root Test once more on this right-hand factor. Note that we have the same possibilities for the roots as in the previous time when we applied the test as the constant coefficient changed only in sign.

We will pick another root to check, say $x = -2$; [1] then, $3(-2)^2 + 5(-2) - 2 = 0$, so $x + 2$ is a factor of the quadratic.

Polynomial long division then gives us that,

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

□

Proof of ii. By the Rational Root Test, a root $q = \frac{r}{s} \in \mathbb{Q}$ must have that $r|6$ and $s|2$.

So, $r = \pm 1, \pm 2, \pm 3, \pm 6$ and $s = \pm 1, \pm 2$ give $q = \pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{2}, \pm \frac{3}{2}$.

We will try $x = 1$, $2(1)^4 - 5(1)^3 + 3(1)^2 + 4(1) - 6 \neq 0$.

Next, we will try $x = -1$, $2(-1)^4 - 5(-1)^3 + 3(-1)^2 + 4(-1) - 6 = 0$, so 1 is a root of g.

We will divide g by its factor $x + 1$ and apply RRT again.

Polynomial long division gives, $g = (x+1)(2x^3 - 7x^2 + 10x - 6)$, which contain the same leading and constant coefficients as in the first application of RRT.

So, we can try $x = \frac{3}{2}$, $2\left(\frac{3}{2}\right)^3 - 7\left(\frac{3}{2}\right)^2 + 10\left(\frac{3}{2}\right) - 6 = \frac{27}{4} - \frac{63}{4} + \frac{60}{4} - \frac{24}{4} = 0$, so $x = \frac{3}{2}$ is a root of g.

We can reduce the polynomial once more by long division with the factor $x - \frac{3}{2}$, which gives $g(x) = (x+1)\left(x - \frac{3}{2}\right)(2x^2 - 4x + 4)$.

[1] The Rational Root Test is good for getting started on a high-degree polynomial which we could not otherwise factor, but, at this point, with a quadratic, we already have more efficient methods to factor; hence, we knew that $x = -2$ was a good root to check!

We can move a factor of 2 from the right-most term to arrive at,

$$g(x) = (x+1)(2x-3)(x^2-2x+2).$$

Note that $x^2 - 2x + 2$ is irreducible in $\mathbb{Q}[x]$ as it has a negative discriminant and therefore no rational roots.

Thus, the irreducible factors of g are given above. □