
Polynomials

SOLUTIONS TO THE REVIEW PROBLEMS

1. Use the Euclidean algorithm to find $\gcd(x^8 - 1, x^6 - 1)$ in $\mathbf{Q}[x]$ and write it as a linear combination of $x^8 - 1$ and $x^6 - 1$.

Solution: Let $x^8 - 1 = f(x)$ and $x^6 - 1 = g(x)$. We have $f(x) = x^2g(x) + (x^2 - 1)$, and $g(x) = (x^4 + x^2 + 1)(x^2 - 1)$, so this shows that $\gcd(x^8 - 1, x^6 - 1) = x^2 - 1$, and $x^2 - 1 = f(x) - x^2g(x)$.

2. Over the field of rational numbers, use the Euclidean algorithm to show that $2x^3 - 2x^2 - 3x + 1$ and $2x^2 - x - 2$ are relatively prime.

Solution: Let $2x^3 - 2x^2 - 3x + 1 = f(x)$ and $2x^2 - x - 2 = g(x)$. We first obtain $f(x) = (x - \frac{1}{2})g(x) - \frac{3}{2}x$. At the next step we can use x rather than $\frac{3}{2}x$, and then $g(x) = (2x - 1)g(x) - 2$. The constant remainder at the second step implies that $\gcd(f(x), g(x)) = 1$.

3. Over the field of rational numbers, find the greatest common divisor of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$, and express it as a linear combination of the given polynomials.

Solution: Let $x^4 + x^3 + 2x^2 + x + 1 = f(x)$ and $x^3 - 1 = g(x)$. We first obtain $f(x) = (x + 1)g(x) + 2(x^2 + x + 1)$, and then the next step yields

$g(x) = (x-1)(x^2+x+1)$, so $\gcd(f(x), g(x)) = x^2+x+1$, and $(x^2+x+1) = \frac{1}{2}f(x) - \frac{1}{2}(x+1)g(x)$.

4. Over the field of rational numbers, find the greatest common divisor of $2x^4 - x^3 + x^2 + 3x + 1$ and $2x^3 - 3x^2 + 2x + 2$ and express it as a linear combination of the given polynomials.

Solution: To simplify the computations, let $2x^4 - x^3 + x^2 + 3x + 1 = f(x)$ and $2x^3 - 3x^2 + 2x + 2 = g(x)$. Using the Euclidean algorithm, we first obtain $f(x) = (x+1)g(x) + (2x^2 - x - 1)$, and then $g(x) = (x-1)(2x^2 - x - 1) + (2x+1)$. At the next step we obtain $2x^2 - x - 1 = (x-1)(2x+1)$, so $2x+1$ is the greatest common divisor (we must then divide by 2 to make it monic).

Beginning with the last equation and back-solving, we get

$$\begin{aligned} 2x+1 &= g(x) - (x-1)(2x^2 - x - 1) \\ &= g(x) - (x-1)(f(x) - (x+1)g(x)) \\ &= g(x) + (x^2-1)g(x) - (x-1)f(x) \\ &= x^2g(x) - (x-1)f(x) \end{aligned}$$

This gives the final answer, $x + \frac{1}{2} = \frac{1}{2}x^2g(x) + (-\frac{1}{2})(x-1)f(x)$.

5. Are the following polynomials irreducible over \mathbf{Q} ?

(a) $3x^5 + 18x^2 + 24x + 6$

Solution: Dividing by 3 we obtain $x^5 + 6x^2 + 8x + 2$, and this satisfies Eisenstein's criterion for $p = 2$.

(b) $7x^3 + 12x^2 + 3x + 45$

Solution: Reducing the coefficients modulo 2 gives the polynomial $x^3 + x + 1$, which is irreducible in $\mathbf{Z}_2[x]$. This implies that the polynomial is irreducible over \mathbf{Q} .

(c) $2x^{10} + 25x^3 + 10x^2 - 30$

Solution: Eisenstein's criterion is satisfied for $p = 5$.

6. Factor $x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ over \mathbf{Q} .

Solution: The possible rational roots of $f(x) = x^5 - 10x^4 + 24x^3 + 9x^2 - 33x - 12$ are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. We have $f(1) = 21$, so for any root we must have $(r-1)|21$, so this eliminates all but $\pm 2, 4, -6$ as possibilities. Then $f(2) = 32$, $f(-2) = -294$, and finally we obtain the factorization $f(x) = (x-4)(x^4 - 6x^3 + 9x + 3)$. The second factor is irreducible over \mathbf{Q} since it satisfies Eisenstein's criterion for $p = 3$.

7. Factor $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2$ over \mathbf{Q} .

Solution: The possible rational roots are $\pm 1, \pm 2$, and since 2 is a root we have the factorization $x^5 - 2x^4 - 2x^3 + 12x^2 - 15x - 2 = (x-2)(x^4 - 2x^2 + 8x + 1)$.

The only possible rational roots of the second factor are 1 and -1 , and these do not work. (It is important to note that since the degree of the polynomial is greater than 3, the fact that it has not roots in \mathbf{Q} does not mean that it is irreducible over \mathbf{Q} .) Since the polynomial has no linear factors, the only possible factorization has the form $x^4 - 2x^2 + 8x + 1 = (x^2 + ax + b)(x^2 + cx + d)$. This leads to the equations $a + c = 0$, $ac + b + d = -2$, $ad + bc = 8$, and $bd = 1$. We have either $b = d = 1$, in which case $a + c = 8$, or $b = d = -1$, in which case $a + c = -8$. Either case contradicts $a + c = 0$, so $x^4 - 2x^2 + 8x + 1$ is irreducible over \mathbf{Q} .

As an alternate solution, we could reduce $x^4 - 2x^2 + 8x + 1$ modulo 3 to get $p(x) = x^4 + x^2 + 2x + 1$. This polynomial has no roots in \mathbf{Z}_3 , so the only possible factors are of degree 2. The monic irreducible polynomials of degree 2 over \mathbf{Z}_3 are $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$. Since the constant term of $p(x)$ is 1, the only possible factorizations are $p(x) = (x^2 + x + 2)^2$, $p(x) = (x^2 + 2x + 2)^2$, or $p(x) = (x^2 + x + 2)(x^2 + 2x + 2)$. In the first the coefficient of x is 1; the second has a nonzero cubic term; in the third the coefficient of x is 0. Thus $p(x)$ is irreducible over \mathbf{Z}_3 , and hence over \mathbf{Q} .

8. (a) Show that $x^2 + 1$ is irreducible over \mathbf{Z}_3 .

Solution: To show that $p(x) = x^2 + 1$ is irreducible over \mathbf{Z}_3 , we only need to check that it has no roots in \mathbf{Z}_3 , and this follows from the computations $p(0) = 1$, $p(1) = 2$, and $p(-1) = 2$.

- (b) List the elements of the field $F = \mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$.

Solution: The congruence classes are in one-to-one correspondence with the linear polynomials, so we have the nine elements $[0]$, $[1]$, $[2]$, $[x]$, $[x + 1]$, $[x + 2]$, $[2x]$, $[2x + 1]$, $[2x + 2]$.

- (c) In the multiplicative group of nonzero elements of F , show that $[x + 1]$ is a generator, but $[x]$ is not.

Solution: The multiplicative group of F has 8 elements, and since $[x]^2 = [-1]$, it follows that $[x]$ has order 4 and is not a generator. On the other hand, $[x + 1]^2 = [x^2 + 2x + 1] = [-1 + 2x + 1] = [2x] = [-x]$, and so $[x + 1]^4 = [-x]^2 = [-1]$, which shows that $[x + 1]$ does not have order 2 or 4. The only remaining possibility (by Lagrange's theorem) is that $[x + 1]$ has order 8, and so it is a generator for the multiplicative group of F .

9. (a) Express $x^4 + x$ as a product of polynomials irreducible over \mathbf{Z}_5 .

Solution: In general, we have $x^4 + x = x(x^3 + 1) = x(x + 1)(x^2 - x + 1)$. The factor $p(x) = x^2 - x + 1$ is irreducible over \mathbf{Z}_5 since it can be checked that it has no roots in \mathbf{Z}_5 . (We get $p(0) = 1$, $p(1) = 1$, $p(-1) = 3$, $p(2) = 3$, $p(-2) = 2$.)

- (b) Show that $x^3 + 2x^2 + 3$ is irreducible over \mathbf{Z}_5 .

Solution: If $p(x) = x^3 + 2x^2 + 3$, then $p(0) = 3$, $p(1) = 1$, $p(-1) = -1$, $p(2) = 4$, and $p(-2) = 3$, so $p(x)$ is irreducible over \mathbf{Z}_5 .

10. Express $2x^3 + x^2 + 2x + 2$ as a product of polynomials irreducible over \mathbf{Z}_5 .

Solution: We first factor out 2, using $(2)(-2) = -4 \equiv 1 \pmod{5}$. This reduces the question to factoring $p(x) = x^3 - 2x^2 + x + 1$. (We could also multiply each term by 3.) Checking for roots shows that $p(0) = 1$, $p(1) = 1$, $p(-1) = -3$, $p(2) = 3$, and $p(-2) \equiv -2$, so $p(x)$ itself is irreducible over \mathbf{Z}_5 .

11. Construct an example of a field with $343 = 7^3$ elements.

Solution: We only need to find a cubic polynomial over \mathbf{Z}_7 that has no roots. The simplest case would be to look for a polynomial of the form $x^3 + a$. The cube of any element of \mathbf{Z}_7 gives either 1 or -1 , so $x^3 = 2$ has no root over \mathbf{Z}_7 , and thus $p(x) = x^3 - 2$ is an irreducible cubic over \mathbf{Z}_7 . Using the modulus $p(x)$, the elements of $\mathbf{Z}_7[x]/\langle p(x) \rangle$ correspond to polynomials of degree 2 or less, giving the required 7^3 elements. With this modulus, the identities necessary to determine multiplication are $[x^3] = [5]$ and $[x^4] = [5x]$.

12. In $\mathbf{Z}_2[x]/\langle x^3 + x + 1 \rangle$, find the multiplicative inverse of $[x + 1]$.

Solution: We first give a solution using the Euclidean algorithm. For $p(x) = x^3 + x + 1$ and $f(x) = x + 1$, the first step of the Euclidean algorithm gives $p(x) = (x^2 + x)f(x) + 1$. Thus $p(x) - (x^2 + x)f(x) = 1$, and so reducing modulo $p(x)$ gives $[-x^2 - x][f(x)] = [1]$, and thus $[x + 1]^{-1} = [-x^2 - x] = [x^2 + x]$.

We next give an alternate solution, which uses the identity $[x^3] = [x + 1]$ to solve a system of equations. We need to solve $[1] = [x + 1][ax^2 + bx + c]$ or

$$\begin{aligned} [1] &= [ax^3 + bx^2 + cx + ax^2 + bx + c] \\ &= [ax^3 + (a + b)x^2 + (b + c)x + c] \\ &= [a(x + 1) + (a + b)x^2 + (b + c)x + c] \\ &= [(a + b)x^2 + (a + b + c)x + (a + c)], \end{aligned}$$

so we need $a + b \equiv 0 \pmod{2}$, $a + b + c \equiv 0 \pmod{2}$, and $a + c \equiv 1 \pmod{2}$. This gives $c \equiv 0 \pmod{2}$, and therefore $a \equiv 1 \pmod{2}$, and then $b \equiv 1 \pmod{2}$. Again, we see that $[x + 1]^{-1} = [x^2 + x]$.

13. Find the multiplicative inverse of $[x^2 + x + 1]$

(a) in $\mathbf{Q}[x]/\langle x^3 - 2 \rangle$;

Solution: Using the Euclidean algorithm, we have

$$x^3 - 2 = (x^2 + x + 1)(x - 1) + (-1), \text{ and so } [x^2 + x + 1]^{-1} = [x - 1].$$

This can also be done by solving a system of 3 equations in 3 unknowns.

(b) in $\mathbf{Z}_3[x]/\langle x^3 + 2x^2 + x + 1 \rangle$.

Solution: Using the Euclidean algorithm, we have

$$x^3 + 2x^2 + x + 1 = (x + 1)(x^2 + x + 1) + (-x) \text{ and}$$

$x^2 + x + 1 = (-x - 1)(-x) + 1$. Then a substitution gives us

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

Thus $[x^2 + x + 1]^{-1} = [-x^2 - 2x] = [2x^2 + x]$. This can be checked by finding $[x^2 + x + 1][2x^2 + x]$, using the identities $[x^3] = [x^2 - x - 1]$ and $[x^4] = [x - 1]$.

This can also be done by solving a system of equations, or, since the set is finite, by taking successive powers of $[x^2 + x + 1]$. The latter method isn't really practical, since the multiplicative group has order 26, and this element turns out to have order 13.

14. In $\mathbf{Z}_5[x]/\langle x^3 + x + 1 \rangle$, find $[x]^{-1}$ and $[x + 1]^{-1}$, and use your answers to find $[x^2 + x]^{-1}$.

Solution: Using the division algorithm, we obtain $x^3 + x + 1 = x(x^2 + 1) + 1$, and so $[x][x^2 + 1] = [-1]$. Thus $[x]^{-1} = [-x^2 - 1]$.

Next, we have $x^3 + x + 1 = (x + 1)(x^2 - x + 2) - 1$, and so $[x + 1]^{-1} = [x^2 - x + 2]$.

Finally, we have

$$\begin{aligned} [x^2 + x]^{-1} &= [x]^{-1}[x + 1]^{-1} = [-x^2 - 1][x^2 - x + 2] \\ &= [-x^4 + x^3 - 2x^2 - x^2 + x - 2]. \end{aligned}$$

Using the identities $[x^3] = [-x - 1]$ and $[x^4] = [-x^2 - x]$, this reduces to

$$\begin{aligned} [x^2 + x]^{-1} &= [x^2 + x - x - 1 - 3x^2 + x - 2] \\ &= [-2x^2 + x - 3] = [3x^2 + x + 2]. \end{aligned}$$

15. Factor $x^4 + x + 1$ over $\mathbf{Z}_2[x]/\langle x^4 + x + 1 \rangle$.

Solution: There are 4 roots of $x^4 + x + 1$ in the given field, given by the cosets corresponding to x , x^2 , $x + 1$, $x^2 + 1$. This can be shown by using the multiplication table, with the elements in the form 10, 100, 11, and 101, or by computing with polynomials, using the fact that $(a + b)^2 = a^2 + b^2$ since $2ab = 0$. We have $x^4 + x + 1 \equiv 0$,

$$(x^2)^4 + (x^2) + 1 = (x^4)^2 + x^2 + 1 \equiv (x + 1)^2 + x^2 + 1 \equiv x^2 + 1 + x^2 + 1 \equiv 0,$$

$$(x + 1)^4 + (x + 1) + 1 \equiv x^4 + 1 + x \equiv x + 1 + 1 + x \equiv 0, \text{ and}$$

$$(x^2 + 1)^4 + (x^2 + 1) + 1 \equiv (x^4)^2 + 1 + x^2 \equiv (x + 1)^2 + 1 + x^2 \equiv x^2 + 1 + 1 + x^2 \equiv 0.$$

Thus $x^4 + x + 1$ factors as a product of 4 linear terms.

