Abstract Algebra by Pinter, Chapter 26

Amir Taaki

Abstract

Chapter 26 on Substitution in Polynomials

Contents

1 A. Finding Roots of Polynomials over Finite Fields 2
1.1 Q1 . . . 2
1.1.1 $f(x) = x^3 + x^2 + x + 1$ . . . 2
1.1.2 $f(x) = 3x^4 + x^2 + 1$ . . . 2
1.1.3 $f(x) = x^5 + 1$ . . . 3
1.1.4 $f(x) = x^4 + 1$ . . . 3
1.1.5 $f(x) = x^4 + 4$ . . . 3
1.2 Q2 . . . 3
1.2.1 $a(x) = x^{100} - 1$ . . . 3
1.2.2 $a(x) = 3x^{98} + x^{19} + 3$ . . . 3
1.2.3 $a(x) = 2x^{74} - x^{55} + 2x + 6$ . . . 3
1.3 Q3 . . . 3
1.4 Q4 . . . 3

2 B. Finding Roots of Polynomials over $\mathbb{Q}$ 3
2.1 Q1 . . . 3
2.1.1 $9x^3 + 18x^2 - 4x - 8$ . . . 3
2.1.2 $4x^3 - 3x^2 - 8x + 6$ . . . 4
2.1.3 $2x^4 + 3x^3 - 8x - 12$ . . . 4
2.1.4 $6x^4 - 7x^3 + 8x^2 - 7x + 2$ . . . 4
2.2 Q2 . . . 4
2.2.1 $9x^3 + 18x^2 - 4x - 8$ . . . 4
2.2.2 $4x^3 - 3x^2 - 8x + 6$ . . . 4
2.2.3 $2x^4 + 3x^3 - 8x - 12$ . . . 4
2.2.4 $6x^4 - 7x^3 + 8x^2 - 7x + 2$ . . . 5
2.3 Q3 . . . 5
2.4 Q4 . . . 5
2.4.1 $18x^3 + 27x^2 - 8x - 12$ . . . 5
2.4.2 $2x^3 - x^2 - 2x + 1$ . . . 6
2.4.3 $3x^3 + x^2 - 3x - 1$ . . . 6
2.5 Q5 . . . 6

3 C. Short Questions Relating to Roots 6
3.1 Q1 . . . 6
3.2 Q2 . . . 6
3.3 Q3 . . . 6
3.4 Q4 . . . 6
3.5 Q5 . . . 6
3.6 Q6 . . . 7
3.7 Q7 . . . 7
3.8 Q8 . . . 7

4 D. Irreducible Polynomials in $\mathbb{Q}[x]$ by Eisenstein's Criterion (and Variations on the Theme) 7
4.1 Q1 . . . 7
4.2 Q2 . . . 8
4.2.1 a . . . 8

4.2.2 b . . . 8
4.3 Q3 . . . 8
4.4 Q4 . . . 8
4.5 Q5 . . . 8

5 E. Irreducibility of Polynomials of Degree ≤ 4 9
5.1 Q1 . . . 9
5.2 Q2 . . . 9
5.3 Q3 . . . 9
5.3.1 $x^4 - 5x^2 + 1$ . . . 9
5.3.2 $3x^4 - x^2 - 2$ . . . 9
5.3.3 $x^4 + x^3 + 3x + 1$ . . . 9
5.4 Q4 . . . 9
5.4.1 $2x^3 + x^2 + 4x + 1$ . . . 9
5.4.2 $x^4 + 2$ . . . 10
5.4.3 $x^4 + 4x^2 + 2$ . . . 10
5.4.4 $x^4 + 1$ . . . 10

6 F. Mapping onto $\mathbb{Z}_n$ to Determine Irreducibility over $\mathbb{Q}$ 10
6.1 Q1 . . . 10
6.2 Q2 . . . 10
6.3 Q3 . . . 10

7 F. Roots and Factors in $A[x]$ When A Is an Integral Domain 10
7.1 Q1 . . . 10
7.2 Q2 . . . 11
7.3 Q3 . . . 11
7.4 Q4 . . . 11

8 H. Polynomial Interpolation 11
8.1 Q1 . . . 11
8.2 Q2 . . . 11
8.3 Q3 . . . 11
8.4 Q4 . . . 11
8.5 Q5 . . . 12

9 I. Polynomial Functions over a Finite Field 12
9.1 Q1 . . . 12
9.2 Q2 . . . 12
9.3 Q3 . . . 13
9.4 Q4 . . . 13
9.5 Q5 . . . 13
9.6 Q6 . . . 13
9.7 Q7 . . . 13

1 A. Finding Roots of Polynomials over Finite Fields

1.1 Q1

1.1.1 $f(x) = x^3 + x^2 + x + 1$

$f(4) = 0 \implies (x+1)$ is a factor.

$f(x)/(x+1) = x^2 + 1$, and $x^2 + 1 = (x+3)(x-3)$ because $(2)^2 + 1 = 0$, so $f(x) = (x+1)(x+3)(x-3)$.

1.1.2 $f(x) = 3x^4 + x^2 + 1$

$f(1) = 0 \implies (x+4)$ is a factor.

$f(4) = 0 \implies (x+1)$ is a factor.

$(x+4)(x+1) = x^2 + 4$. And $f(x)/(x^2+4) = 3x^2 + 4$

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

1.1.3 $f(x) = x^5 + 1$

$(x+1)$ is a factor.

$$\begin{aligned}(x+1)^5 &= x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1\\ &= x^5 + 1\end{aligned}$$

1.1.4 $f(x) = x^4 + 1$

No roots

1.1.5 $f(x) = x^4 + 4$

$f(1), f(2), f(3), f(4) = 0$

$x^4 + 4 = (x+1)(x+2)(x+3)(x+4)$. That is all values of $\mathbb{Z}_5[x]$ where $a \neq 0$.

1.2 Q2

1.2.1 $a(x) = x^{100} - 1$

$\phi(7) = 6$ and so $x^{100} \equiv (x^6)^{16}x^4 \equiv x^4 \pmod 7$ because $x^6 = 1$. This is true for all $a \in \mathbb{Z}_7$ so any root in $x^{100} - 1$ must also be in $x^4 - 1$.

$f(1), f(6) = 0$ so these are the roots.

1.2.2 $a(x) = 3x^{98} + x^{19} + 3$

$\forall a \in \mathbb{Z}_7[x], 3x^{98} + x^{19} + 3 = 3x^2 + x + 3$. The only root is 1.

1.2.3 $a(x) = 2x^{74} - x^{55} + 2x + 6$

$a(x) = 2x^2 + x + 6$. Roots are 4 and 6.

1.3 Q3

$$3x^3 - 5 + 2x - x^2$$

$$5 + 6x^5 - 2x^3$$

$$3x - x + 3x - x = 4x$$

1.4 Q4

Power act like an additive group modulo $\phi(p) = p - 1$, so any $x^{\phi(p)q+r}$ where $r < \phi(p)$ can be reduced to x^r.

2 B. Finding Roots of Polynomials over $\mathbb{Q}$

2.1 Q1

2.1.1 $9x^3 + 18x^2 - 4x - 8$

$a_0 = -8$ and $a_n = 9$.

$$s = \pm 1, \pm 8, \pm 2, \pm 4$$

$$t = \pm 1, \pm 9, \pm 3$$

Possible roots are $\pm 1, \pm 2, \pm 4, \pm 8, \pm 1/9, \pm 1/3, \pm 8/9, \pm 8/3, \pm 2/9, \pm 2/3, \pm 4/9, \pm 4/3$. Substituting in we find roots for 2, $\pm 2/3$.

$$9x^3 + 18x^2 - 4x - 8 = 9(x - 2/3)(x + 2/3)(x + 2)$$

2.1.2 $4x^3 - 3x^2 - 8x + 6$

$a_0 = 6$ and $a_n = 4$.

$$s = \pm 1, \pm 6, \pm 2, \pm 3$$
$$t = \pm 1, \pm 4, \pm 2$$

Possible roots are $\pm 1, \pm 6, \pm 2, \pm 3, \pm 3/2, \pm 1/2, \pm 3/4$. Substituting in we find a root for $3/4$. Dividing $a(x)$ by $(x - 3/4)$ in sage, we get $4x^2 - 8$ as the remaining term.

$$4x^3 - 3x^2 - 8x + 6 = 4(x - 3/4)(x^2 - 2)$$

2.1.3 $2x^4 + 3x^3 - 8x - 12$

$a_0 = -12$ and $a_n = 2$

$$s = \pm 1, \pm 12, \pm 3, \pm 2, \pm 4, \pm 6$$
$$t = \pm 1, \pm 2$$

Possible roots: $\pm 1, \pm 12, \pm 3, \pm 2, \pm 4, \pm 6, \pm 3/2$. Root is $-3/2$. Dividing by $(x + 3/2)$, we get $(2x^3 - 8)$ as the remaining term.

$$2x^4 + 3x^3 - 8x - 12 = 2(x + 3/2)(x^3 - 4)$$

2.1.4 $6x^4 - 7x^3 + 8x^2 - 7x + 2$

$a_0 = 2$ and $a_n = 6$

$$s = \pm 1, \pm 2$$
$$t = \pm 1, \pm 6, \pm 2, \pm 3$$

Possible roots: $\pm 1, \pm 2, \pm 1/6, \pm 1/2, \pm 1/3, \pm 2/3$. Roots: $1/2, 2/3$. Dividing by $(x-1/2)(x-2/3)$, we get $6(x^2+1)$ as the remaining term.

$$6x^4 - 7x^3 + 8x^2 - 7x + 2 = 6(x - 1/2)(x - 2/3)(x^2 + 1)$$

2.2 Q2

2.2.1 $9x^3 + 18x^2 - 4x - 8$

$$9x^3 + 18x^2 - 4x - 8 = 9(x - 2/3)(x + 2/3)(x + 2)$$

2.2.1.1 $\mathbb{R}[x]$ Unchanged from above.

2.2.1.2 $\mathbb{C}[x]$ Unchanged from above. Every factor is of degree 1.

2.2.2 $4x^3 - 3x^2 - 8x + 6$

$$4x^3 - 3x^2 - 8x + 6 = 4(x - 3/4)(x^2 - 2)$$

2.2.2.1 $\mathbb{R}[x]$

$$(x^2 - 2) = (x - \sqrt{2})(x + \sqrt{2})$$
$$4x^3 - 3x^2 - 8x + 6 = 4(x - 3/4)(x - \sqrt{2})(x + \sqrt{2})$$

2.2.2.2 $\mathbb{C}[x]$ Unchanged from above

2.2.3 $2x^4 + 3x^3 - 8x - 12$

$$2x^4 + 3x^3 - 8x - 12 = 2(x + 3/2)(x^3 - 4)$$

2.2.3.1 $\mathbb{R}[x]$

$$(x^3 - 4) = (x - \sqrt[3]{4})(x^2 + \sqrt[3]{4}x + (\sqrt[3]{4})^2)$$
$$2x^4 + 3x^3 - 8x - 12 = 2(x + 3/2)(x - \sqrt[3]{4})(x^2 + \sqrt[3]{4}x + (\sqrt[3]{4})^2)$$

2.2.3.2 $\mathbb{C}[x]$ Let $A = \sqrt[3]{4}$

$$x^2 + Ax + A^2 = 0$$

$$(x + A/2)^2 - (A/2)^2 + A^2 = (x + A/2)^2 + (A/2)^2 = 0$$

$$\implies x = \sqrt{-(A/2)^2} - A/2 = \pm iA/2 - A/2$$

$$\begin{aligned}\implies x^2 + Ax + A^2 &= (x - (\pm iA/2 - A/2)) \\ &= (x + A/2 + iA/2)(x + A/2 - iA/2)\end{aligned}$$

$$2x^4 + 3x^3 - 8x - 12 = 2(x + 3/2)(x - A)(x + A/2 + iA/2)(x + A/2 - iA/2)$$

2.2.4 $6x^4 - 7x^3 + 8x^2 - 7x + 2$

$$6x^4 - 7x^3 + 8x^2 - 7x + 2 = 6(x - 1/2)(x - 2/3)(x^2 + 1)$$

2.2.4.1 $\mathbb{R}[x]$ Same as above.

2.2.4.2 $\mathbb{C}[x]$

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

$$6x^4 - 7x^3 + 8x^2 - 7x + 2 = 6(x - 1/2)(x - 2/3)(x - i)(x + i)$$

2.3 Q3

$$18x^3 + 27x^2 - 8x - 12$$

$$2x^3 - x^2 - 2x + 1$$

$$3x^3 + x^2 - 3x - 1$$

2.4 Q4

2.4.1 $18x^3 + 27x^2 - 8x - 12$

$$a_0 = -12, a_n = 18$$

Factors of $a_0 : \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

Factors of $a_n : \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

```
a = lambda x: 18*x**3 + 27*x**2 - 8*x - 12

for s in [1, 2, 3, 4, 6, 12]:
    for t in [1, 2, 3, 6, 9, 18]:
        st = s/t
        if abs(a(st)) < 0.001:
            print("+", s, t)
        if abs(a(-st)) < 0.001:
            print("-", s, t)
```

Output:

```
+ 2 3
- 2 3
- 3 2
+ 4 6
- 4 6
+ 6 9
- 6 9
+ 12 18
- 12 18
```

Roots: $\pm 2/3, -3/2$

$(x - 2/3)(x + 2/3)(x + 3/2)$

2.4.2 $2x^3 - x^2 - 2x + 1$

$$a_0 = 1, a_n = 2$$

Factors of $a_0 : \pm 1$

Factors of $a_n : \pm 1, \pm 2$

Roots: $\pm 1, 1/2$

$$\frac{1}{2}(x+1)(x-1)(x-1/2)$$

2.4.3 $3x^3 + x^2 - 3x - 1$

$$a_0 = -1, a_n = 3$$

Factors of $a_0 : \pm 1$

Factors of $a_n : \pm 1, \pm 3$

Roots: $\pm 1, -1/3$

$$\sqrt{3}(x+1)(x-1)(x+1/3)$$

2.5 Q5

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

So there are no rational roots.

3 C. Short Questions Relating to Roots

3.1 Q1

Let $a(x) = p(x) - p(c)$, then $a(c) = 0 \implies (x - c) \mid [p(x) - p(x)]$ and so $p(x) - p(c) = q(x)(x - c)$ or $p(x) = q(x)(x - c) + p(c)$. $\deg p(c) = 0$ and $\deg(x - c) = 1$.

3.2 Q2

$$\begin{aligned} p(x) - p(c) &= a_1(x - c) + \cdots + a_n(x^n - c^n) \\ &= q(x)(x - c) + r(x) \end{aligned}$$

$$\deg r(x) < \deg(x - c) \implies r(x) = r \geq 0$$

$$p(c) - p(c) = 0 = q(x)(c - c) + r = 0 + r = r$$

Thus $r = 0$ and $(x - c) \mid (p(x) - p(c))$.

3.3 Q3

$a(x)$ and $b(x)$ are associates if $a(x) \mid b(x)$ and $b(x) \mid a(x) \iff$ they are constant multiples of each other. So $a(x) = db(x)$, and $b(c) = 0 \implies a(x) = db(c) = d \cdot 0 = 0$.

3.4 Q4

$a(x) = (x - c)^m$ and $b(x) = (x - c)^n$ both have the same roots but differ by non-constant factors and so are not associates.

3.5 Q5

$a(x)$ has n roots $c_1, \ldots, c_n \in F$

$$\implies a(x) = q(x)[(x - c_1) \cdots (x - c_n)]$$

but $\deg[(x - c_1) \cdots (x - c_n)] = n = \deg a(x)$ and $a(x)$ is monic, and so is $(x - c_1) \ldots (x - c_n) = x^n + \cdots + (-c_1) \cdots (-c_n) \implies q(x) = 1$ and so

$$a(x) = (x - c_1) \cdots (x - c_n)$$

3.6 Q6

$$a(c) = b(c) \implies a(c) - b(c) = 0$$

Let $\deg[a(x) - b(x)] = m < n$, then $a(x) - b(x)$ can be factored in at most m ways $(x - c_1) \cdots (x - c_m)$ but there exists a c such that $c \neq c_i$ for all m values, yet

$$a(c) - b(c) = 0 = k(c - c_1) \cdots (c - c_m)$$

by the fact F is a field, then $F[x]$ is an integral domain and has no zero divisors. This means $k = 0$ since all the other terms are nonzero.

$$a(x) - b(x) = 0$$
$$a(x) = b(x)$$

3.7 Q7

In $\mathbb{Z}_5, 2 \nmid 1$ and $2^2 \nmid 2$, so by Eisenstein's irreducibility criterion, any polynomial of the form

$$2 + \cdots + x^n$$

is irreducible. There are an infinite number of these polynomials.

3.8 Q8

$$x(x-1) = 0$$
$$\mathbb{Z}_{10} : 0, 1, 5, 6$$
$$\mathbb{Z}_{11} : 0, 1$$

there are no divisors of zero in $\mathbb{Z}_1 1$.

4 D. Irreducible Polynomials in $\mathbb{Q}[x]$ by Eisenstein's Criterion (and Variations on the Theme)

4.1 Q1

$$2 \mid (-8x^3 + 6x^2 - 4x)$$
$$2 \nmid 3x^4$$
$$2^2 \nmid 6$$

So $3x^4 - 8x^3 + 6x^2 - 4x + 6$ is irreducible over $\mathbb{Q}$.

$$a(x) = \frac{1}{6}(4x^5 + 3x^4 - 12x^2 + 3)$$
$$3 \mid (3x^4 - 12x^2 + 3)$$
$$3 \nmid 4x^5$$
$$3^2 \nmid 3$$

So $a(x)$ is irreducible over $\mathbb{Q}$.

$$a(x) = \frac{1}{15}(3x^4 - 5x^3 - 10x + 15)$$
$$5 \mid (-5x^3 - 10x + 15)$$
$$5 \nmid 3x^4$$
$$5^2 \nmid 15$$

So $a(x)$ is irreducible over $\mathbb{Q}$.

$$a(x) = \frac{1}{6}(3x^4 + 8x^3 - 4x^2 + 6)$$
$$2 \mid (8x^3 - 4x^2 + 6)$$
$$2 \nmid 3x^4$$
$$2^2 \nmid 6$$

So $a(x)$ is irreducible over $\mathbb{Q}$.

4.2 Q2

4.2.1 a

```
sage: (x + 1)^4 + 4*(x + 1) + 1
x^4 + 4*x^3 + 6*x^2 + 8*x + 6
```

$$(x+1)^4 + 4(x+1) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$$

$$p = 2$$
$$p \mid (4x^3 + 6x^2 + 8x + 6)$$
$$p \nmid x^4$$
$$p^2 \nmid 6$$

4.2.2 b

```
sage: x = PolynomialRing(RationalField(), 'x').gen()
sage: a = lambda x: x^4 + 2*x^2 - 1
sage: a(x + 1)
x^4 + 4*x^3 + 8*x^2 + 8*x + 2
```

$p = 2$

```
sage: a = lambda x: x^3 + 3*x + 1
sage: a(x + 1)
x^3 + 3*x^2 + 6*x + 5
sage: a(x + 2)
x^3 + 6*x^2 + 15*x + 15
```

$p = 3$

```
sage: a = lambda x: x^4 + 1
sage: a(x + 1)
x^4 + 4*x^3 + 6*x^2 + 4*x + 2
```

$p = 2$

```
sage: a = lambda x: x^4 - 10*x**2 + 1
sage: a(x + 1)
x^4 + 4*x^3 - 4*x^2 - 16*x - 8
```

$p = 4$

4.3 Q3

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

All the coefficients except a_n are divisible by p, and p^2 does not divide p which is the constant term.

4.4 Q4

$a(x)$ is irreducible $\implies$ $h(a(x))$ is irreducible.

p divides every coefficient except a_0 and p^2 does not divide a_n, then $a(x)$ is irreducible.

4.5 Q5

$$2 \mid (6x^4 + 4x^3 - 6x^2 - 8x), 2 \nmid 5, 2^2 \nmid 6x^4$$
$$3 \mid (6x^4 - 3x^2 + 9x), 3nmid - 8, 3^2 \nmid 6x^4$$
$$5 \mid (10x^3 + 5x^2 - 15x), 5 \nmid 12, 5^2 \nmid 10x^3$$

5 E. Irreducibility of Polynomials of Degree ≤ 4

5.1 Q1

Any quadratic $ax^2 + bx + c$ is only reducible to degree 1 factors of the form $(x - c_1)(x - c_2)$. Likewise a cubic is reducible to either a quadratic and linear factor or 3 linear factors.

Since reducible polynomials of degree 2 and 3 both contain linear factors of the form $(x - c)$ then they both have roots when $x = c$.

Thus an irreducible polynomial of degree 2 or 3 has no roots, and if a polynomial of degree 2 or 3 has no roots, then it is irreducible.

5.2 Q2

There are no roots for $x^3 + 4x = x(x^2 + 4) = 3$.

Using completing the square method $x^2 - \frac{2}{3}x - \frac{4}{3} = 0$ or $x^2 - \frac{2}{3}x = \frac{4}{3} = (x - \frac{2}{6})^2 - \frac{4}{36}$. Further solving for x we get $x = \sqrt{\frac{1}{9} + \frac{4}{3}} + \frac{2}{6} = \sqrt{\frac{13}{9}} + \frac{2}{6}$. There is no rational root of 13 so the equation has no roots.

$x(2x^2 + 2x + 3) = -1 \implies x = \pm 1$ (NOTE: remember we are testing the equations in $\mathbb{Z}$ for a solution). Therefore equation has no solution.

$x^3 = -1/2$ has no rational roots.

Solving for x, we get $x = \sqrt{-\frac{3}{2} + \frac{5}{4}} = \sqrt{-\frac{1}{4}}$ which has no rational roots.

5.3 Q3

5.3.1 $x^4 - 5x^2 + 1$

$a + c = 0, ac + b + d = -5, bd = 1$. So $b = d = \pm 1$. And $ac = -7$ or $ac = -3$, but $a = -c$, so $c^2 = 7$ or $c^2 = 3$ which is has no rational roots.

5.3.2 $3x^4 - x^2 - 2$

$a + c = 0, ac + b + d = -1, bc + ad = 0, bd = -2$. Then $a = -c \implies bc - cd = c(b - d) = 0$. Either $c = 0$ or $b - d = 0$. If $c = 0$ then $a = 0 implies ac + b + d = b + d = -1 \implies b = -1 - d \implies bd = (-1 - d)d = -2 \implies d^2 + d + 2 = 0 \implies d = \sqrt{-2 - 1/4} - 1/2$ which has no solutions. If $b - d = 0$ then $b = d \implies bd = b^2 = -2$ which has no rational solution.

5.3.3 $x^4 + x^3 + 3x + 1$

$a + c = 1, ac + b + d = 0, bc + ad = 3, bd = 1$.

$$a = 1 - c$$
$$bc + ad = bc + (1 - c)d = 3$$

$bd = 1 \implies b = d = \pm 1$ so $bc + (1 - c)d$ is either $c + (1 - c) = 3$ or $-c - (1 - c) = 3$. In the first case $c + (1 - c) = 1 \neq 3$. In the second case $-c - (1 - c) = -1 \neq 3$. So the equation is inconsistent and has no solutions.

5.4 Q4

5.4.1 $2x^3 + x^2 + 4x + 1$

```
>>> a = lambda x: (2*x**3 + x**2 + 4*x + 1) % 5
>>> for i in range(5):
...     print(i, a(i), a(i) == 0)
...
0 1 False
1 3 False
2 4 False
3 1 False
4 1 False
```

5.4.2 $x^4 + 2$

$a + c = 0, ac + b + d = 0, bc + ad = 0, bd = 2 \implies a = -c, c(b - d) = 0$. Either $c = 0$, then $a = 0$ and $b + d = 0 \implies b = -d$ and $d^2 = -2$ which has no solutions, or $b - d = 0 \implies b = d$ and $b^2 = 2$ which has no integer solutions.

5.4.3 $x^4 + 4x^2 + 2$

$a + c = 0, ac + b + d = 4, bc + ad = 0, bd = 2 \implies a = -c$.

Either $b = 2, d = 1$ or $b = 1, d = 2$.

$b = 2 \implies bc + ad = 2c - c = c = 0 \implies a = 0 \implies ac + b + d = 0 + 2 + 1 = 3 \neq 0$

$b = 1 \implies bc + ad = c - 2c = -c = 0$ which leads to the same conclusion as when $b = 2$. Thus equation has no solution and cannot be reduced.

5.4.4 $x^4 + 1$

$a + c = 0, ac + b + d = 0, bc + ad = 0, bd = 1$

$\implies b = d = \pm 1$ and $a = -c$. Then $ac + b + d = -c^2 + 2b = 0$ or $c^2 = 2$ or -2, both of which do not have solutions.

6 F. Mapping onto $\mathbb{Z}_n$ to Determine Irreducibility over $\mathbb{Q}$

6.1 Q1

If $a(x)$ is reducible, this is the same as saying there exists $b(x), c(x)$ such that $a(x) = b(x)c(x)$. Since $\bar{h}(a(x))$ is homomorphic, then $\bar{h}(a(x)) = \bar{h}(b(x))\bar{h}(c(x))$. However the polynomial $a(x)$ must be monic and hence so are its factors, otherwise $a(x)$ could be reducible to factors with coefficients that divide n and so disappear from the homomorphism with the result not meaningfully factored (the degree of the result is less than the original preimage factorisation in $\mathbb{Z}[x]$).

6.2 Q2

$\bar{h}(x^4 + 10x^3 + 7) = x^4 + 7$ cannot be reduced because 7 has no factors in $\mathbb{Z}_5$. Therefore $a(x)$ is irreducible in $\mathbb{Q}[x]$.

6.3 Q3

$h : \mathbb{Z} \to \mathbb{Z}_5, \bar{h}(x^4 - 10x + 1) = x^4 + 1$ which is irreducible.

$h : \mathbb{Z} \to \mathbb{Z}_7, \bar{h}(x^4 + 7x^3 + 14x^2 + 3) = x^4 + 3$ which is irreducible.

This last one is wrong:

```
sage: x = PolynomialRing(QQ, 'x').gen()
sage: (x^5 + 1).factor()
(x + 1) * (x^4 - x^3 + x^2 - x + 1)
```

7 F. Roots and Factors in $A[x]$ When A Is an Integral Domain

7.1 Q1

$$
\begin{aligned}
(x-c)(x^{k-1} + \cdots + x^{k-2}c + \cdots + c^{k-1}) &= x(x^{k-1}) + x(x^{k-2}c) + x(x^{k-3}c^2) + \cdots + x(c^{k-1}) - c(x^{k-1}) - c(x^{k-2}c) - \cdots - c(xc^{k-2} \\
&= x^k + x^{k-1}c + x^{k-2}c^2 + \cdots + xc^{k-1} - x^{k-1}c - x^{k-2}c^2 - \cdots - xc^{k-1} - c^k \\
&= x^k - c^k
\end{aligned}
$$

$$
a_k(x-c)(x^{k-1} + \cdots + xc^{k-2} + \cdots + c^{k-1}) = a_k(x^k - c^k)
$$

7.2 Q2

Because $a(x)-a(c) = a_1(x-c)+a_2(x^2-c^2)+\cdots+a_n(x^n-c^n)$ and from above we worked out that $a_k(x^k-c^k) = a_k(x-c)(x^{k-1}+x^{k-2}c+\cdots+xc^{k-2}+c^{k-1})$, so then $a(x)-a(c) = a_1(x-c)+a_2(x-c)(x+c)+a_3(x-c)(x^2+xc+c^2)+\cdots+a_n(x-c)(x^{n-1}+x^{n-2}c+\cdots+xc^{n-2}c+c^{k-1})$.

Let $q(x) = a_1+a_2(x+c)+a_3(x^2+xc+c^2)+\cdots+a_n(x^{n-1}+x^{n-2}c+\cdots+xc^{n-2}c+c^{k-1})$, and then $a(x)-a(c) = (x-c)q(x)$.

7.3 Q3

Every field is an integral domain. I think the book is asking when A is an integral domain (and not neccessarily a field).

By above $a(x)-a(c) = (x-c)q(x)$ in integral domains. If c is a root of $a(x)$ then $(x-c)$ is a factor and so $a(c) = 0$, or $a(x) = (x-c)q(x)$. Likewise if $(x-c)$ is a factor of $a(x)$ then $a(x) = (x-c)q(x)$ and $a(c) = 0$.

7.4 Q4

Theorem 2 follows automatically from theorem 1, because integral domains do not have zero divisors.

Theorem 3 also checks out.

8 H. Polynomial Interpolation

8.1 Q1

$q_i(a_i) \neq 0$ because a_i is not a root of $q_i(x)$. All other values of $q_i(a_j) = 0$ because they are roots of $q_i(x)$.

8.2 Q2

For any i, $q_i(x) = c_i$ and

$$p(x) = \cdots + b_i \frac{q_i(x)}{c_i} + \cdots$$

All other terms of $p(x)$ are $q_j(x)$ where $i \neq j$, and $q_j(a_i) = 0$, so $p(a_i) = b_i \frac{q_i(x)}{c_i}$ since all other terms are zero.

Lastly $q_i(x) = c_i$ and $b_i \frac{q_i(x)}{c_i} = b_i \implies p(a_i) = b_i$.

8.3 Q3

Let there be 2 polynomials $p(x)$ and $q(x)$ such that $p(a_i) = b_i = q(q_i)$, then $p(a_i) - q(a_i) = 0$, so $p(x) - q(x)$ has $n+1$ distinct zeros, but $\deg p(x) - q(x) \leq n$. From theorem 3, if $p(x) - q(x)$ has degree n, it has at most n roots. Therefore no such $q(x)$ exists.

8.4 Q4

Let $F = \{a_0, \dots, a_n\}$ and the function $f : F \to F$ be

$$f = \begin{pmatrix} a_0 & & a_n \\ & \cdots & \\ b_0 & & b_n \end{pmatrix}$$

Then $a_i(x) = (x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)$ and $\deg q_i(x) = n-1$.

Since $p(x) = \sum_{i=0}^{n} b_i \frac{q_i(x)}{q_i(a_i)}$, then $\deg p(x) = n-1$.

Lastly all terms $i \neq j$ in $p(a_i)$ are 0,

$$\frac{q_i(x)}{q_i(a_i)} = \frac{q_i(a_i)}{q_i(a_i)} = 1 \implies b_i \frac{q_i(x)}{q_i(a_i)} = b_i$$

So $p(a_i) = b_i$ and $p = f$ from Q2 above since $\deg p(x) = n-1 \implies p(x)$ is unique.

8.5 Q5

$$\forall a_i \in F, t(a_i) - p(a_i) = 0 \implies t(x) - p(x) = (x - a_0) \cdots q(x)$$
$$\deg p(x) = n - 1 < \deg[(x - a_0) \cdots (x - a_n)] = n$$
$$t(x) = (x - a_0) \cdots (x - a_n) q(x) + p(x)$$

9 I. Polynomial Functions over a Finite Field

9.1 Q1

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 3 & 2 & 3 \end{pmatrix}$$

```
sage: x = PolynomialRing(IntegerModRing(5), 'x').gen()
sage: a = lambda x: x^2 -x + 1
sage: p = 0
sage: for i in range(5):
....:     b = a(x)(i)
....:     q = 1
....:     for j in range(5):
....:         if i == j:
....:             continue
....:         q *= (x - j)
....:     q_c = q(i)
....:     p += b*q/q_c
....:
sage: p
x^2 + 4*x + 1
```

So the other functions are determined by $x^2 - x + 1$ which is not surprising since it's degree is less than or equal to 4 which guarantees its uniqueness.

All other polynomials are determined by this one so they have a quotient equal to $(x - a_0) \cdots (x - a_n)$

```
sage: r = 1
sage: for i in range(5):
....:     r *= (x - i)
....:
sage: r
x^5 + 4*x
```

in our case $x^5 + 4x$.

3 examples:

```
sage: p
x^2 + 4*x + 1
sage: r
x^5 + 4*x
sage: f_1 = r*x + p
sage: f_2 = r*x^2 + p
sage: f_3 = r*x^3 + p
sage: (f_1, f_2, f_3)
(x^6 + 4*x + 1, x^7 + 4*x^3 + x^2 + 4*x + 1, x^8 + 4*x^4 + x^2 + 4*x + 1)
sage: for i in range(5):
....:     assert f_1(i) == p(i)
....:     assert f_2(i) == p(i)
....:     assert f_3(i) == p(i)
....:
```

9.2 Q2

$x^p = x$ so $x^p - x \equiv 0 \pmod p$, because $x^{\phi(p)} = x$ and $\phi(p) = p - 1$.

$$\implies x^p - x = x(x-1) \cdots [x - (p-1)]$$

9.3 Q3

$$a(x) = x(x-1)\cdots[x-(p-1)]q(x) + p(x)$$
$$b(x) = x(x-1)\cdots[x-(p-1)]s(x) + p(x)$$

(see 26H5)

But $x(x-1)\cdots[x-(p-1)] = x^p - x$, so

$$a(x) = (x^p - x)q(x) + p(x)$$

$$b(x) = (x^p - x)s(x) + p(x)$$
$$a(x) - b(x) = (x^p - x)[q(x) - s(x)]$$
$$\implies (x^p - x) \mid (a(x) - b(x))$$

9.4 Q4

For every $c \in F, a(c) = b(c)$. There are n values of c, but $\deg a(x) < n$ and $\deg b(x) < n$. From 26H3, there can only be one unique polynomial such that $a(c) = y$. Therefore $a(x) = b(x)$.

9.5 Q5

$a(x), b(x) \in F[x]$, then $a(x) = (x^p - x)q(x) + p(x), b(x) = (x^p - x)s(x) + p(x)$.

9.6 Q6

Let $a(x), b(x) \in F[x]$ be determined by $p_a(x)$ and $p_b(x)$ respectively. Then $h[a(x)] = p_a(x)$ and $h[b(x)] = p_b(x)$.

Then $a(x) = x(x-1)\cdots[x-(p-1)]q_a(x) + p_a(x)$ and b is defined similarly, which for every point in F evaluates to their determinants $p_a(x)$ and $p_b(x)$. Thus $h[a(x)b(x)] = p_a(x)p_b(x) = h[a(x)]h[b(x)]$.

From 26H4, we also see all functions from F to F, are a member of $\mathcal{F}(F)$, and have an equivalency with a polynomial in $F[x]$. Therefore the function $h : F[x] \to \mathcal{F}(F)$ is onto. Every element of the codomain $\mathcal{F}(F)$ has an equivalent value in the domain $F[x]$, such that h is a map from domain to codomain.

9.7 Q7

$$\forall c \in F, p(c) = 0 \implies \forall q \in F[x], pq = 0 \therefore J = p(x), h(J) = 0 \implies F[x]/\langle p(x)\rangle \cong \mathcal{F}(F)$$