Abstract Algebra by Pinter, Chapter 25

Amir Taaki

Abstract

Chapter 24 on Factoring Polynomials

Contents

1 A. Examples of Factoring into Irreducible Factors

1.1 Q1

$\mathbb{Q}: x^4 - 4 = (x^2 - 2)(x^2 + 2)$

$\mathbb{R}: x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$

$\mathbb{C}: x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{2}i)(x + \sqrt{2}i)$

1.2 Q2

Factor $x^6 - 16$

$\mathbb{Q}: (x^3 - 4)(x^3 + 4)$

$\mathbb{R}: (x^3 - (\sqrt[3]{4})^3)(x^3 + (\sqrt[3]{4})^3) = (x - \sqrt[3]{4})(x^2 + \sqrt[3]{4}x + (\sqrt[3]{4})^2)(x + \sqrt[3]{4})(x^2 - \sqrt[3]{4}x + (\sqrt[3]{4})^2)$

(using the sum and differences of cubes formulas: $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$ and $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$.)

Using the quadratic formula to find the roots, for $\mathbb{C}$ and setting $b = \sqrt[3]{4}$ we get:

$$(x^6 - 16) = (x - b)(x^2 + bx + b^2)(x + b)(x^2 - bx + b^2)$$
$$a = 1, b = \sqrt[3]{4}, c = b^2 = (\sqrt[3]{4})^2$$

$$\begin{aligned} x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \\ &= \frac{-b \pm \sqrt{b^2 - 4b^2}}{2} \\ &= \frac{-b \pm b\sqrt{-3}}{2} \\ &= \frac{-b - b\sqrt{3}i}{2}, \frac{-b + b\sqrt{3}i}{2} \end{aligned}$$

And so therefore the roots for $(x^2 + bx + b^2)$ are:

$$\begin{aligned} (x^2 + bx + b^2) &= (x - [\frac{-b - b\sqrt{3}i}{2}])(x - [\frac{-b + b\sqrt{3}i}{2}]) \\ (x^2 + \sqrt[3]{4}x + (\sqrt[3]{4})^2) &= (x - [\frac{-\sqrt[3]{4} - \sqrt[3]{4}\sqrt{3}i}{2}])(x - [\frac{-\sqrt[3]{4} + \sqrt[3]{4}\sqrt{3}i}{2}]) \\ &= \left(x + \frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)\left(x + \frac{\sqrt[3]{4}}{2} + \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right) \end{aligned}$$

Likewise

$$(x^2 - \sqrt[3]{4}x + (\sqrt[3]{4})^2) = \left(x - \frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)\left(x - \frac{\sqrt[3]{4}}{2} + \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)$$

Thus

$$(x^6 - 16) = (x - \sqrt[3]{4})\left(x + \frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)\left(x + \frac{\sqrt[3]{4}}{2} + \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)(x + \sqrt[3]{4})\left(x - \frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)\left(x - \frac{\sqrt[3]{4}}{2} + \frac{\sqrt[3]{4}}{2}\sqrt{3}i\right)$$

1.3 Q3

Note $f(x) = 0$ implies it has roots and so is reducible.

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

1.4 Q4

$$x^2 + 2 = (x + a)(x + b)$$

Find x given $x^2 + 2 = 0$. The only squares in $\mathbb{Z}_5$ are 1 and 4. Neither is valid for x so $x^2 + 2$ is irreducible in $\mathbb{Z}_5$.

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

1.5 Q5

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

Roots are $2 + 3 = 0$ and $4 + 1 = 0$. Factoring we get $2(x + 3)(x + 1)^2$ (actually I just used a Berklecamp calculator).

1.6 Q6

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

2 B. Short Questions Relating to Irreducible Polynomials

2.1 Q1

Polynomials of degree 1 in a field are irreducible. There are no zero divisors. Multiplying constant terms produces another constant term. Multiplying factors with degrees m and n respectively will produce a new factor with degree $m + n$, and since there are no zero divisors the product of two non-zero coefficients can never be zero.

2.2 Q2

If $a(x)$ and $b(x)$ have different degrees they cannot be associates since there are no zero divisors in a field and so no constant term can cancel factors in a polynomial.

Assume $a(x)$ and $b(x)$ have the same degree. Then their leading terms are both x^n. If there is some constant term $c > 1$ such that $a(x) = c \cdot b(x)$ then the leading term of $c \cdot b(x)$ will be cx^n which is not the leading term in $a(x)$. Hence there is a contradiction and both polynomials are *not* associates.

2.3 Q3

$a(x)$ and $b(x)$ are distinct so $a(x) \neq b(x)$, and since $a(x)$ and $b(x)$ cannot be factored, then they share no factors and are relatively prime.

2.4 Q4

An associate of $a(x)$ is $b(x) = ka(x)$, and since $a(x)$ is irreducible, so is $b(x)$, hence all associates of $a(x)$ are irreducible if $a(x)$ is irreducible.

2.5 Q5

In a field, no constants multiplied can equal 0, so there is no $ka(x) = 0$.

2.6 Q6

$$|\mathbb{Z}_p| = \phi(p) = p - 1$$

There are $p-1$ possible values for k and hence $p-1$ associates of non-zero $a(x)$.

2.7 Q7

Polynomial factors for x^2+1 are lower degree since it's reducible in $\mathbb{Z}_p$.

$a(x) = x^2 + 1 = kp_1(x)p_2(x)$ where $p_1(x)$ and $p_2(x)$ are monic irreducible polynomials.

$$x^2 + 1 = k(x+a)(x+b) \text{ in } \mathbb{Z}_p[x]$$
$$a + b \equiv 0 \pmod{p}$$
$$ab \equiv 1 \pmod{p}$$

Since $a, b \in \mathbb{Z}_p$, then $p = a + b$ (otherwise $a = ka_1, b = kb_1$ and $p = a_1 + b_1$)

3 C. Number of Irreducible Quadratics over a Finite Field

3.1 Q1

By theorem 4, each factorization is unique so $(x+a_1)(x+b_1) \neq (x+a_2)(x+b_2)$ for all $a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$.

$(x+a)^2$, there are 5 possible values and $\binom{5}{2} = 10$, so there are 10 combinations for $(x+a)(x+b)$ (disregarding order since $\mathbb{Z}_5$ is commutative). There are 15 reducible monic quadratics in $\mathbb{Z}_5[x]$.

3.2 Q2

There are 15 reducible monics, and 0 is not an associate, 1 is unity, leaving $ka(x)$ different associates where $k \in \{2, 3, 4\}$ and $|k| = 5 - 2 = 3$.

Therefore the total number of reducible quadratics is $4 \times 15 = 60$.

The total number of quadradics in $\mathbb{Z}_5[x]$ is $5^3 = 125$ from all the possible combos of $ax^2 + bx + c$.

So there are $125 - 60$ irreducible quadratics.

3.3 Q3

$$n^3 - (n-1)\left[\binom{n}{2} + n\right]$$

3.4 Q4

$$n^4 - (n-1)\left[\binom{n}{3} + n\right]$$

4 D. Ideals in Domains of Polynomials

4.1 Q1

$$J = \langle b(x) \rangle = \langle a(x) \rangle$$

So it follows $\deg a(x) = \deg b(x)$ yet they are both in J and so multiples of each other. So $a(x)$ and $b(x)$ are associates.

4.2 Q2

$a(x) = b(x)m(x) : b(x) \in F[x]$ and $J = \langle m(x) \rangle \implies a(x) \in J$

$a(x) \in J$ and $J = \langle m(x) \rangle \implies a(x) = b(x)m(x)$ for some $b(x) \in F[x]$

4.3 Q3

$$a(x)b(x) = kp_1(x)\cdots p_r(x)$$

$J = \langle m(x)\rangle$ where $m(x)$ is irreducible. Since J is an ideal $a(x)b(x) \in J \implies a(x)b(x) = c(x)m(x)$ for some $c(x) \in F[x]$. But $m(x)$ is irreducible so $m(x) = p_i(x)$ where i is one of the factors from 1 to r.

Likewise if J is a prime ideal then $a(x)b(x) \in J \implies a(x) \in J$ or $b(x) \in J$. Say $a(x) \in J$, then $a(x) = kp_1(x)\cdots p_r(x) \implies p_i(x) \in J$ for some $i \in \{1,\dots,r\} \implies J = \langle m(x)\rangle$ where $m(x)$ is irreducible.

4.4 Q4

$p(x)$ is irreducible.

$$J = \langle p(x)\rangle$$

Let there be an ideal K such that $J \subset K$, and let $a(x) \in K$ such that $a(x) \notin J$.

Thus $a(x)$ is not a multiple of $p(x)$ and they share no common factors.

$$\begin{aligned} 1 &= r(x)a(x) + s(x)p(x) \\ \implies r(x)a(x) &= 1 - s(x)p(x) \\ \implies r(a)a(x) &\in J + 1 \end{aligned}$$

So $a(x)$ is invertible and so $a(x) \in K \implies K = A$.

4.5 Q5

Coefficient sum of $x-1$ is $1+(-1) = 0$ so $x-1 \in S$. $x-1$ is irreducible so it is a maximal ideal and $S = \langle x-1\rangle$.

4.6 Q6

$$g(a(x)) = g(a_0 + \cdots + a_n x^n) = a_0 + \cdots + a_n$$
$$k(x) \in K = \ker g \implies g(k(x)) = 0$$

From previous question $k = \langle x-1\rangle$.

$$g : F[x] \underset{\langle x-1\rangle}{\twoheadrightarrow} F$$

$$F[x]/\langle x-1\rangle \cong F$$

4.7 Q7

$$a(x,y) = x \in J, b(x,y) = y \in J$$

But there is no polynomial in $F[x,y]$ such that $a(x,y) = r(x,y)b(x,y)$ and vice versa. Therefore J cannot be principal and $F[x,y]$ can have non-principal ideals.

5 E. Proof of the Unique Factorization Theorem

5.1 Q1

Euclid's lemma for polynomials: let $p(x)$ be irreducible. If $p(x) \mid a(x)b(x)$ then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

If $p(x) \mid a(x)$ we are done. So lets assume $p(x) \nmid a(x)$. What integers are common divisors?

$p(x)$ is irreducible, so the only divisors are ± 1 and $\pm p(x)$. But $p(x) \nmid a(x)$, so $\pm p(x)$ is not a common divisor of $p(x)$ and $a(x)$. So therefore that leaves ± 1 as their common divisors. So by theorem 2

$$1 = k(x)p(x) + l(x)a(x)$$

$$b(x) = k(x)p(x)b(x) + l(x)a(x)b(x)$$

But $p(x) \mid a(x)b(x)$ so there is an $h(x)$ such that $a(x)b(x) = p(x)h(x)$. Therefore

$$k(x)p(x)b(x) + l(x)p(x)h(x) = b(x)$$

that is $p(x)[k(x)b(x) + l(x)h(x)] = b(x)$ or $p(x) \mid b(x)$.

5.2 Q2

Grouping terms, we see that $p \mid a_1(x)$ or $p(x) \mid (a_2(x) \cdots a_n(x))$, and if $p(x) \nmid a_1(x)$, then $p(x) \mid a_2(x)$ or $p(x) \mid (a_3(x) \cdots a_n(x))$ and so on.

For corollary 2, $p(x) \mid q_i(x)$ for one of the factors. Since the factors $q_1(x) \cdots q_r(x)$ are irreducible, so if $p(x) \mid q_i(x)$ for some integer, that means $p(x) = q_i(x)$.

5.3 Q3

Cancelling terms from both sides of

$$a(x) = kp_1(x) \cdots p_r(x) = lq_1(x) \cdots q_s(x)$$

Since for all $i \in \{1, \dots, r\}, p_i(x) \mid (lq_1(x) \cdots q_s(x))$ then $p_i(x) = q_j(x)$ for some j in $\{1, \dots, s\}$. Cancelling terms we eventually end up with $k = l$.

6 F. A Method for Computing the gcd

6.1 Q1

$$\begin{aligned} d(x) &= \gcd(a(x), b(x)) \\ a(x) &= d(x)a_1(x) \\ b(x) &= d(x)b_1(x) \end{aligned}$$

$$\begin{aligned} a(x) &= b(x)q_1(x) + r_1(x) \\ d(x)a_1(x) &= d(x)b_1(x)q_1(x) + r_1(x) \\ r_1(x) &= d(x)(a_1(x) - b_1(x)q_1(x)) \\ &\implies d(x) \mid r_1(x) \end{aligned}$$

6.2 Q2

Using a long division calculator.

$$\begin{aligned} x^4 + x^3 + 2x^2 + x - 1 &= (x^3 + 1)(x + 1) + (2x^2 - 2) \\ x^3 + 1 &= (2x^2 - 2)(\frac{x}{2}) + (x + 1) \\ 2x^2 - 2 &= (x + 1)(2x - 2) + 0 \end{aligned}$$

$\implies$ gcd is $x + 1$

6.3 Q3

$$\begin{aligned} x^24 - 1 &= (x^15 - 1)x^9 + (x^9 - 1) \\ x^15 - 1 &= (x^9 - 1)x^6 + (x^6 - 1) \\ x^9 - 1 &= (x^6 - 1)x^3 + (x^3 - 1) \\ x^6 - 1 &= (x^3 - 1)x^3 + (x^3 - 1) \\ x^3 - 1 &= (x^3 - 1)1 + 0 \end{aligned}$$

gcd is $x^3 - 1$

6.4 Q4

$$\begin{aligned} x^4 + x^3 + 2x^2 + 2x &= (x^3 + x^2 + x + 1)x + (x^2 + x) \\ x^3 + x^2 + x + 1 &= (x^2 + x)x + (x + 1) \\ x^2 + x &= (x + 1)x + 0 \end{aligned}$$

gcd is $x + 1$

7 F. A Transformation of $F[x]$

7.1 Q1

$$\begin{aligned}
h[a(x)b(x)] &= h(a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_nx^{2n}) \\
&= a_0b_0x^{2n} + (a_0b_1 + a_1b_0)x^{2n-1} + \cdots + a_nb_n \\
h[a(x)]h[b(x)] &= h(a_0 + a_1x + \cdots + a_nx^n)h(b_0 + b_1x + \cdots + b_nx^n) \\
&= (a_0x^n + a_1x^{n-1} + \cdots + a_n)(b_0x^n + b_1x^{n-1} + \cdots + b_n) \\
&= a_0b_0x^{2n} + (a_0b_1 + b_0a_1)x^{2n-1} + \cdots + a_nb_n
\end{aligned}$$

7.2 Q2

Injective: $\forall a(x), b(x) \in F[x], h[a(x)] = h[b(x)] \implies a(x) = b(x)$. This is trivially visible.

Surjective: $\forall b(x) \in F[x], \exists a(x) \in F[x] : h[a(x)] = b(x)$. The value of $a(x)$ is simply $b(x)$.

Indeed $h(h(a_0 + a_1x + \cdots + a_nx^n)) = h(a_n + a_{n-1}x + \cdots + a_0x^n) = a_0 + a_1x + \cdots + a_nx^n$. This means that $h \cdot h = \epsilon$.

7.3 Q3

Let $a(x) = a_0 + a_1x + \cdots + a_nx^n$ be irreducible but $b(x) = a_n + a_{n-1}x + \cdots + a_0x^n$ be reducible so that $b(x) = c(x)d(x)$. But then $a(x) = h[b(x)] = h[c(x)d(x)] = h[c(x)]h[d(x)]$ meaning $a(x)$ is in fact reducible.

7.4 Q4

$$\begin{aligned}
h(a_0 + a_1x + \cdots + a_nx^n) &= a_n + a_{n-1}x + \cdots + a_0x^n \\
&= h[(b_0 + \cdots + b_mx^m)(c_0 + \cdots + c_qx^q)] \\
&= h(b_0 + \cdots + b_mx^m)h(c_0 + \cdots + c_qx^q) \\
a_n + a_{n-1}x + \cdots + a_0x^n &= (b_m + \cdots + b_0x^m)(c_q + \cdots + c_0x^q)
\end{aligned}$$

7.5 Q5

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

$$\begin{aligned}
\bar{a}(x) = h[a(x)] &= h[b(x)]h(x - c) \\
&= h[b(x)](1 - cx)
\end{aligned}$$

$$\begin{aligned}
\bar{a}(1/c) &= h[b(1/c)][1 - c(1/c)] \\
&= 0
\end{aligned}$$