10 *Irreducible Polynomials*

Although the irreducibility depends on the coefficients, irreducible polynomials are much like positive prime integers. In some ways, they are even simpler.

10.0 Factoring polynomials

When are polynomial rings unique factorization domains? To answer this question, we need an auxiliary invariant.

Definition 10.0.0. Let R be a unique factorization domain and consider a polynomial $f := a_m\,x^m + a_{m-1}\,x^{m-1} + \cdots + a_1\,x + a_0$ in $R[x]$. The *content* of the polynomial f is defined to be

$$\operatorname{cont}(f) := \gcd(a_m, a_{m-1}, \dots, a_0)\,.$$

The polynomial f is *primitive* if $\operatorname{cont}(f) = 1$.

To define the content, we need to know that greatest common divisors exist. The greatest common divisor, if it exists, is unique only up to multiplication by a unit. Hence, the content of a polynomial is an equivalence class.

Lemma 10.0.1 (Gauss)**.** *Let R be a unique factorization domain. For any two polynomials f and g in $R[x]$, we have*

$$\operatorname{cont}(f\,g) = \operatorname{cont}(f)\,\operatorname{cont}(g)\,.$$

In particular, when f and g are primitive, the product $f\,g$ also is.

Proof. We write $f = \operatorname{cont}(f)\,\widehat{f}$ and $g = \operatorname{cont}(g)\,\widehat{g}$ where $\widehat{f}$ and $\widehat{g}$ are primitive polynomials in $R[x]$. As $f\,g = \operatorname{cont}(f)\,\operatorname{cont}(g)\,\widehat{f}\,\widehat{g}$, it suffices to verify that the product $\widehat{f}\,\widehat{g}$ is a primitive polynomial. Let $\widehat{f} = a_0 + a_1\,x + \cdots + a_m\,x^m$ and $\widehat{g} = b_0 + b_1\,x + \cdots + b_n\,x^n$ for some $a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n$ in R. Suppose that the coefficients of $\widehat{f}\,\widehat{g}$ have a common divisor d which is not a unit. If the element p in R were an irreducible divisor of d, then p must divide all the coefficients of $\widehat{f}\,\widehat{g}$. Since $\widehat{f}$ and $\widehat{g}$ are primitive, p does not divide all the coefficients of $\widehat{f}$ or $\widehat{g}$. Let a_j be the first coefficient of $\widehat{f}$ not divisible by p and let b_k be the first coefficient of $\widehat{g}$ not divisible by p. Consider the coefficient of x^{j+k} in $\widehat{f}\,\widehat{g}$; it has the form

$$a_j\,b_k + (a_{j+1}\,b_{k-1} + a_{j+2}\,b_{k-2} + \cdots) + (a_{j-1}\,b_{k+1} + a_{j-2}\,b_{k+2} + \cdots)\,.$$

By hypothesis, p divides this sum. Moreover, all the terms in the first parenthesis are divisible by p (because p divides b_i for all $i < j$) and all terms in the second parenthesis are divisible by p (because p divides a_i for all $i < k$). It follows that p divides $a_j\,b_k$. Since $\langle p \rangle$ is prime ideal, the element p divides either a_j or b_k contrary to our choice of a_j and b_k. This contradiction shows that no irreducible element divides all the coefficients of $\widehat{f}\,\widehat{g}$ and, therefore, the product $\widehat{f}\,\widehat{g}$ is primitive. □

Replacing the coefficient domain by its fields of fraction does not alter irreduciblity.

Lemma 10.0.2. *Let R be a unique factorization domain and let K be its field of fractions.*

- *For any nonzero polynomial f in the ring $K[x]$, we have $f = c\,\widehat{f}$ where $c \in K$ and $\widehat{f}$ is a primitive polynomial in $R[x]$. Moreover, this factorization is unique up to multiplication by in unit of R.*
- *Let f be a polynomial in $R[x]$ having positive degree. When f is irreducible in $R[x]$, the polynomial f is also irreducible in $K[x]$.*

Proof. Finding a common denominator d for the coefficients of the polynomial f, we obtain $f = \left(\frac{1}{d}\right)\widetilde{f}$ where $\widetilde{f}$ is a polynomial in $R[x]$. Setting $c := \frac{1}{d}\operatorname{cont}(\widetilde{f})$, it follows that $f = c\,\widehat{f}$ where $\widehat{f}$ is a primitive polynomial in $R[x]$. Suppose that $f = \left(\frac{a}{b}\right) g$ for some the fraction $\frac{a}{b}$ in K and some primitive polynomial g in $R[x]$. It follows that $a\,d\,g = b\operatorname{cont}(f)\,\widehat{f}$. Taking the content of both sides yields $u\,a\,d = b\operatorname{cont}(f)$ for some unit u in R. We deduce that $u\,g = \widehat{f}$.

Since $\operatorname{cont}(f)$ divides f, the polynomial f is primitive in $R[x]$. Suppose that f is reducible in $K[x]$. It follows that $f = g_1\,g_2$ for some polynomials g_1 and g_2 in $K[x]$ having positive degree. The first part implies that, for any index j, we have $g_j = c_j\,h_j$ for some $c_j \in K$ and some primitive polynomial h_j in $R[x]$. Hence, $f = c_1\,c_2\,h_1\,h_2$ and the product $h_1\,h_2$ is primitive by Lemma 10.0.1. The first part implies f and $h_1\,h_2$ differ up to multiplication by a unit of R, which contradicts the irreducibility of f in $R[x]$. □

Theorem 10.0.3. *For any unique factorization domain R, the polynomial ring $R[x]$ is also a unique factorization domain.*

Proof. Let K be the field of fractions for the domain R. Consider a nonzero polynomial f in the ring $R[x]$. As $K[x]$ is a principal ideal domain, Corollary 9.1.5 shows that it a unique factorization domain. Hence, we can write $f = p_1\,p_2\,\cdots\,p_r$ where each p_j is an irreducible polynomial in $K[x]$. Lemma 10.0.2 implies that, for all $1 \leqslant i \leqslant r$, we have $p_j = c_j\,q_j$ for some $c_j \in K$ and some primitive polynomial q_j in $R[x]$. Thus, we deduce that $f = c\,q_1\,q_2\,\cdots\,q_r$ where $c = \prod_j c_j \in K$. Write $c = \frac{a}{b}$ for some elements a and b in R. Taking contents, we obtain $\operatorname{cont}(b\,f) = \operatorname{cont}(a\,q_1\,q_2\,\cdots\,q_r) = a$ by Lemma 10.0.1. We deduce that $b\operatorname{cont}(f) = a$, so b divides a and $\operatorname{cont}(f) = c$ lies in R. Since each q_j is irreducible in $K[x]$, it is irreducible in $R[x]$. The ring R is a unique factorization domain, so we have $c = u\,d_1\,d_2\,\cdots\,d_s$ where each d_i is irreducible in R and u in R is a unit. It follows that $f = u\,d_1\,d_2\,\cdots\,d_s\,q_1\,q_2\,\cdots\,q_r$ is a factorization of f into a product of irreducible elements in $R[x]$.

It remains to check uniqueness. Suppose that we have a second factorization: $f = u'\,d_1'\,d_2'\,\cdots\,d_t'\,q_1'\,q_2'\,\cdots\,q_k'$ where each q_j' is primitive polynomial in $R[x]$ and d_j' is irreducible element in R. Since this is also a factorization in $K[x]$, it is unique, so $r = k$ and $q_j' = q_j$ (up to units and reordering). If primitive polynomials differ by a unit in $K[x]$, then they also differ by a unit in $R[x]$. Furthermore, we have $\operatorname{cont}(f) = u' \, d_1' \, d_2' \, \cdots \, d_t' = u \, d_1 \, d_2 \, \cdots \, d_s$ so $s = t$ and $d_j' = d_j$ (up to units and reordering). □

Example 10.0.4. The ring $\mathbb{Z}[x]$ is a unique factorization domain, but not a principal ideal domain.

Corollary 10.0.5. *For any nonnegative integer n and any unique factorization domain R, the polynomial ring $R[x_1, x_2, \dots, x_n]$ is also a unique factorization domain.*

Proof. We proceed by induction on n. When $n = 0$, the assertion is trivial. Since Theorem 10.0.3 establishes the induction step, the claim follows. □

Exercises

Problem 10.0.6. Euclid proves that there are infinitely many prime integers in the following way: if $p_1, p_2, \dots, p_k$ are positive prime integers, then any prime factor of $1 + p_1 \, p_2 \cdots p_k$ must be different from p_j for any $1 \leqslant j \leqslant k$.

(i) Adapt this argument to show that the set of prime integers of the form $4\,n - 1$ is infinite.

(ii) Adapt this argument to show that, for any field $\mathbb{K}$, there are infinitely many monic irreducible polynomials in $\mathbb{K}[x]$.

Problem 10.0.7. Let R be a principal ideal domain and let K be its field of fractions.

(i) Suppose $R = \mathbb{Z}$. Write $r = \frac{7}{24} \in \mathbb{Q}$ in the form $r = \frac{b}{3} + \frac{a}{8}$ for some integers a and b.

(ii) Let $g := p\,q \in R$ where p and q are coprime. Prove that every fraction $f/g \in K$ can written in the form

$$\frac{f}{g} = \frac{u}{q} + \frac{v}{p}$$

for some elements u and v in R.

(iii) Let $g := p_1^{e_1} \, p_2^{e_2} \cdots p_m^{e_m} \in R$ be the factorization of g into irreducible elements p_j, for all $1 \leqslant j \leqslant m$, such that the relation $p_j = u \, p_k$ for some unit $u \in R$ implies that $j = k$. Prove that every fraction $f/g \in K$ can be written in the form

$$\frac{f}{g} = \sum_{j=1}^{k} \frac{h_j}{p_j^{e_j}}$$

for some elements $h_1, h_2, \dots, h_m$ in R.

10.1 Irreducibility Criteria

Can we identify irreducible polynomials? In some situations, this can be relatively easy.

Problem 10.1.0. Is $f(x) = x^3 + 6x^2 + 7$ in $\mathbb{Z}[x]$ irreducible?

Solution. Yes. Otherwise f would have linear factor and its root would divide 7. However, we have $f(1) = 14$, $f(-1) = 12$, $f(7) > 0$, and $f(-7) = (-1)(49) + 7 < 0$. □

Proposition 10.1.1. *Let $f = a_m\, x^m + \cdots + a_1\, x + a_0$ be a polynomial in the ring $R[x]$ and let $\langle p \rangle$ be a prime ideal in R that does not contain a_m. When the image of f in $\big(R/\langle p\rangle\big)[x]$ is irreducible, the polynomial f is irreducible in $R[x]$.*

Proof. The canonical surjection $\pi\colon R \to R \,/\, \langle p \rangle$ induces a ring homomorphism $\varphi\colon R[x] \to R/\langle p\rangle\,[x]\big(R/\langle p\rangle\big)[x]$. When $f = g\, h$ in the ring R, we obtain $\varphi(f) = \varphi(g)\, \varphi(h)$. The assumption that the element p does not divide a_m implies that $\deg\big(\varphi(g)\big) = \deg(g)$ and $\deg\big(\varphi(h)\big) = \deg(h)$. Therefore, reducibility of the polynomial f in $R[x]$ implies the reducibility of the image $\varphi(f)$ in $\big(R/\langle p\rangle\big)[x]$. □

Problem 10.1.2. Is $x^4 + 15x^3 + 7$ in $\mathbb{Q}[x]$ irreducible?

Solution. The image of this polynomial in $\mathbb{F}_5[x]$ is $x^4 + 2$. Since $x^4 \equiv 0, 1 \pmod{5}$, we see that $x^4 + 2$ has no root in $\mathbb{F}_5$. Suppose that $x^4 + 2 = (x^2 + a\,x + b)(x^2 + c\,x + d)$. It follows that $a + c = 0$, $ac + b + d = 0$, $ad + bc = 0$, and $bd = 2$. Since $c = -a$, we have $0 = ad + bc = a(d - b)$, so $a = 0$ or $d = b$.

- Suppose that $a = 0$. We have $c = 0$. The equations $b + d = 0$ and $bd = 2$ imply that $d = -b$, $-b^2 = 2$, and $b^2 = 3$. However, $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, and $4^2 = 1$. Hence, there is no element $b \in \mathbb{F}_5$ such that $b^2 = 3$.
- Suppose that $b = d$. We have $b^2 = 2$. This is again impossible because the only perfect squares in $\mathbb{F}_5$ are 0, 1, and 4.

We see that the polynomial $x^4 + 2$ is irreducible in $\mathbb{F}_5[x]$. Thus, Proposition 10.1.1 shows that $x^4 + 15\,x^3 + 7$ is irreducible in $\mathbb{Z}[x]$ and Lemma 10.0.1 shows that it is irreducible in $\mathbb{Q}[x]$. □

Theorem 10.1.3 (Eisenstein Criterion). *Let R a commutative domain and let $f := a_0 + a_1\, x + \cdots + a_m\, x^m$ be a primitive polynomial in $R[x]$ of positive degree n. When there exists a prime ideal P in R such that*

- *$a_m \notin P$,*
- *$a_0, a_1, \dots, a_{m-1} \in P$, and*
- *$a_0 \notin P^2$,*

the polynomial f is irreducible in $R[x]$.

Theodor Schönemann first published a version of this criterion in 1846. Gotthold Eisenstein published a somewhat different version in the same journal in 1850.

Proof. Suppose that $f = g\, h$ for some polynomials g and h in $R[x]$ having positive degree. Set $g := b_0 + b_1\, x + \cdots + b_j\, x^j$ and $h := c_0 + c_1\, x + \cdots + c_k\, x^k$ where $\deg(g) = j$ and $\deg(h) = k$. It follows that $a_0 = b_0\, c_0$ belongs to the ideal P. Since P is a prime ideal, we have $b_0 \in P$ or $c_0 \in P$. Having both b_0 and c_0 belong to P would imply that $a_0 \in P^2$ contradicting our hypotheses. Without loss of generality, we may assume that $b_0 \in P$ and $c_0 \notin P$. If every coefficient of g were in P, then every coefficient of f would also be in P again contradicting our hypothesis. Let b_i be the first coefficient of g such that $b_i \notin P$. Since

$$a_i = b_i\, c_0 + b_{i-1}\, c_1 + \cdots + b_0\, c_i\,,$$

we obtain the equation $b_i\, c_0 \;=\; a_i - b_{i-1}\, c_1 - \cdots - b_0\, c_i$. Every element on the right side of this equation lies in P. However, this implies that $b_i\, c_0 \in P$. Because P is a prime ideal, we deduce that either $b_i \in P$ or $c_0 \in P$ which is a contradiction. □

We record the following special case.

Corollary 10.1.4. *Let R be a unique factorization domain with fraction field K and consider $f := a_0 + a_1\, x + \cdots + a_m\, x^m$ in the ring $R[x]$. When there exists an irreducible element $p \in R$ such that*

- *p does not divide a_m,*
- *p divides a_i for all $0 \leqslant i \leqslant m-1$, and*
- *p^2 does not divide a_0,*

the polynomial f is irreducible in $K[x]$.

Proof. Theorem 10.1.3 shows that the polynomial f is irreducible in $R[x]$ and Lemma 10.0.1 shows that f is irreducible in $K[x]$. □

Problem 10.1.5. Is $x^5 - 6\,x^4 + 3 \in \mathbb{Q}[x]$ irreducible?

Solution. Yes, apply Corollary 10.1.4 with $p = 3$. □

Corollary 10.1.6. *For any positive prime integer p, the polynomial*

$$f := x^{p-1} + x^{p-2} + \cdots + x + 1$$

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

Proof. Since $(x-1)\,f(x) = x^p - 1$, the ring isomorphism given by $x \mapsto y + 1$ yields

$$y f(y+1) = (y+1)^p - 1 = y^p + \tbinom{p}{1}\, y^{p-1} + \tbinom{p}{2}\, y^{p-2} + \cdots + \tbinom{p}{p-1}\, y\,.$$

We have $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$. When $i < p$, the prime integer p is not a factor of $i!$, so $i!$ divides the product $(p-1)(p-2)\cdots(p-i+1)$ which implies that $\binom{p}{i}$ is divisible by p. Dividing the expansion of $y\, f(y+1)$ by y shows that $f(y+1)$ satisfies the hypothesis of Corollary 10.1.4. Therefore, the polynomial

$$y^{p-1} + \tbinom{p}{1}\, y^{p-2} + \tbinom{p}{2}\, y^{p-3} + \cdots + \tbinom{p}{p-1}$$

is irreducible. We conclude that f is irreducible. □

Exercises

Problem 10.1.7. Let $f := a_3\, x^3 + a_2\, x^2 + a_1\, x + a_0$ be a polynomial in $\mathbb{Z}[x]$ having degree 3. Assume that a_0, $a_1 + a_2$, and a_3 are all odd. Prove that f is irreducible in $\mathbb{Q}[x]$.

Problem 10.1.8. Prove that the polynomial

$$g := x^5 + 6\,x^4 - 12\,x^3 + 9\,x^2 - 3\,x + k$$

in $\mathbb{Q}[x]$ is irreducible for infinitely many integers k.

Problem 10.1.9. Prove that $h := x^5 + x^4 + x - 1$ is irreducible in $\mathbb{Q}[x]$ using the Eisenstein criterion.

10.2 Counting Irreducibles

How do we count irreducible elements? The *sieve of Eratosthenes* is a method of determining the primes less than a given number n. List the integers from 2 to n. The smallest entry 2 is prime. Cross out the multiples of 2 from our list. The smallest remaining entry 3 is prime because it is not divisible by any smaller prime. Cross out the multiples of 3. Repeat. Using this method, Table 10.1 list the positive prime integers less than 100.

The Greek polymath, Eratosthenes of Cyrene (276BCE–194BCE), is famous for his work on prime numbers and for measuring the diameter of the earth.

	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	

Table 10.1: The 25 positive prime integers less than 100

The asymptotic distribution of the primes among the positive integers has a famous description.

Definition 10.2.0. The *prime-counting function* $\pi \colon \mathbb{R} \to \mathbb{N}$ counts the number of positive prime integers less than or equal to some real number; $\pi(x) := |\{p \in \mathbb{N} \mid p \text{ is a positive prime integer and } p \leqslant x\}|$.

The *logarithmic integral function* $\operatorname{li} \colon (1, \infty) \to \mathbb{R}$ is defined by

$$\operatorname{li}(x) := \int_0^x \frac{dy}{\ln(y)} \,.$$

Prime Number Theorem 10.2.1. *We have* $\lim\limits_{x \to \infty} \dfrac{\pi(x)}{\operatorname{li}(x)} = 1$. ■

Assuming the Riemann hypothesis, one has

$$|\pi(x) - \operatorname{li}(x)| < \frac{\sqrt{x}\,\ln(x)}{8\pi} \,.$$

For any positive prime integer p, sieve methods also allows one to identify the irreducible polynomials in $\mathbb{F}_p[x]$. List all polynomials by degree and then cross out products. Table 10.2 lists the irreducible polynomials of degree at most 4 in $\mathbb{F}_2[x]$.

~~0~~	~~1~~	x	$x+1$
~~x^2~~	~~x^2+1~~	~~x^2+x~~	x^2+x+1
~~x^3~~	~~x^3+1~~	~~x^3+x~~	x^3+x+1
~~x^3+x^2~~	x^3+x^2+1	~~x^3+x^2+x~~	~~x^3+x^2+x+1~~
~~x^4~~	~~x^4+1~~	~~x^4+x~~	x^4+x+1
~~x^4+x^2~~	~~x^4+x^2+1~~	~~x^4+x^2+x~~	~~x^4+x^2+x+1~~
~~x^4+x^3~~	x^4+x^3+1	~~x^4+x^3+x~~	~~x^4+x^3+x+1~~
~~$x^4+x^3+x^2$~~	~~$x^4+x^3+x^2+1$~~	~~$x^4+x^3+x^2+x$~~	$x^4+x^3+x^2+x+1$

Table 10.2: Irreducible polynomials in $\mathbb{F}_2[x]$ having small degree

Problem 10.2.2. Is $x^4 - 6x^3 + 12x^2 - 3x + 9$ in $\mathbb{Z}[x]$ irreducible?

Solution. This polynomial is irreducible because its image in $\mathbb{F}_2[x]$ is the irreducible polynomial $x^4 + x + 1$. □

Remark 10.2.3. Since $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, Proposition 9.0.11 implies that the quotient ring $K := \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ is a field. When α denotes the image of x in K, the set $\{1, \alpha\}$ forms a basis of K over $\mathbb{F}_2$. The field K has four elements: $\{0, 1, \alpha, 1 + \alpha\}$.

An analogue of the prime number theorem counts irreducible polynomials over a finite field.

Theorem 10.2.4. *Let p be a positive prime integer. For some positive integer e, set $q := p^e$. Setting N_d to be the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d, we have*

$$\sum_{d|n} d\, N_d = q^n\,.$$

One can even prove an analogue of the Riemann hypothesis, namely that

$$N_d = \frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right).$$

Sketch of Proof. Consider the formal power series $\sum_g t^{\deg(g)}$ having integer coefficients where the summation is over all monic polynomials g in the ring $\mathbb{F}_q[x]$. The total number of monic polynomials g in $\mathbb{F}_q[x]$ of degree n is q^n, so we have

$$\sum_g t^{\deg(f)} = \sum_{n=0}^{\infty} q^n\, t^n = \frac{1}{1 - q\,t}\,.$$

The polynomial ring $\mathbb{F}_q[x]$ is a unique factorization domain. As a consequence, we obtain

$$\sum_g t^{\deg(g)} = \prod_f (1 - t^{\deg(f)})^{-1} = \prod_{d=1}^{\infty} (1 - t^d)^{-N_d}$$

where the middle product runs over the monic irreducible polynomials in f in $\mathbb{F}_q[x]$. It follows that

$$\frac{1}{1 - q\,t} = \prod_{d=1}^{\infty} (1 - t^d)^{-N_d}\,,$$

Taking logarithms gives

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{q^n\, t^n}{n} &= -\log(1 - q\,t) = -\sum_{d=1}^{\infty} N_d \log(1 - t^d) \\ &= \sum_{d=1}^{\infty} \sum_{c=1}^{\infty} d\, N_d \frac{t^{dc}}{dc} = \sum_{n=1}^{\infty} \frac{t^n}{n} \left(\sum_{dc=n} d\, N_d \right). \end{aligned}$$ □

Theorem 10.2.5. *Let p be a positive prime integer. For some positive integer e, set $q := p^e$. The irreducible factors of $x^q - x$ are precisely the monic irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divides d.* ■

Example 10.2.6. In $\mathbb{F}_2[x]$, we have

$$\begin{aligned} x^8 - x &= x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \\ x^{16} - x &= x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)\,. \end{aligned}$$

Similarly, in $\mathbb{F}_3[x]$, we have

$$x^9 - x = x(x + 1)(x - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1)\,.$$