December 4, 2023

Polynomials

Table of Contents

Let R be a commutative ring.

---

1. General definitions and properties of polynomial rings

1.1. *Polynomials* over R are formal sums of the form $f = \sum_{i=0}^{n} a_i x^i = a_n x^n + \cdots + a_1 x + a_0$ with $n \geq 0$ and $a_i \in R$ for all i; the terms with $a_i = 0$ can be added to or dropped from this sum. The summands $a_i x^i$ are called *monomials*. The elements a_i of R are called *the coefficients* of f. The coefficient a_0 is also called *the constant term* of f. A nonzero polynomial f can always be written in the form $f = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \neq 0$, and then a_n is called *the senior coefficient* of f.

1.2. For polynomials $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ over R, their sum $f + g$ and their product fg are defined by $f+g = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$ and $fg = \sum_{k=0}^{n+m} \bigl(\sum_{i=0}^{k} a_i b_{k-i}\bigr) x^k$ (where we assume $a_i = 0$ for $i > n$ and $b_j = 0$ for $j > m$). Under these operations, the set of polynomials over R is a ring, denoted by $R[x]$.

1.3. R is a subring of $R[x]$; its elements are called *constant polynomials*, or just *constants*.

1.4. The ring $R[x_1, \ldots, x_k]$ of polynomials in k variables is defined similarly, as the ring of formal sums of distinct monomials $a x_1^{m_1} \cdots x_k^{m_k}$, with $a \in R$ and integer $m_1, \ldots, m_k \geq 0$. It is easy to see that $R[x_1, x_2] \cong (R[x_1])[x_2]$ and by induction, $R[x_1, \ldots, x_k] = (R[x_1, \ldots, x_{k-1}])[x_k]$ for any k.

1.5. If S is a commutative ring, $\varphi\colon R \longrightarrow S$ is a ring homomorphism, and $\alpha_1, \ldots, \alpha_k \in S$, then φ extends to a homomorphism $R[x_1, \ldots, x_k] \longrightarrow S$ with $\varphi(x_i) = \alpha_i$ for all i.

1.6. For $f = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \neq 0$, n is called *the degree* of f and is denoted by $\deg f$. (The degree of the zero polynomial is assumed to be 0, or, sometimes, $-\infty$.)

Polynomials of degree 0, that is, elements of R, are called *constants*. Polynomials of degree 1 are called *linear*. Polynomials of degrees $2, 3, 4, 5$ are called, respectively, *quadratic, cubic, quartic* and *quintic*.

1.7. For any two polynomials $f, g \in R[x]$, $\deg(f + g) \leq \max(\deg f, \deg g)$ and $\deg(fg) \leq \deg f + \deg g$. If R is an integral domain and $f, g \neq 0$, then $\deg(fg) = \deg f + \deg g$.

1.8. If R is unital, a nonzero polynomial is said to be *monic* if its senior coefficient is 1.

1.9. If S is a subring of R, then $S[x]$ is a subring of $R[x]$.

1.10. Any homomorphism $\varphi\colon R \longrightarrow S$ of (commutative) rings induces a homomorphism $\tilde{\varphi}\colon R[x] \longrightarrow S[x]$ by $\tilde{\varphi}\bigl(a_n x^n + \cdots + a_1 x + a_0\bigr) = \varphi(a_n) x^n + \cdots + \varphi(a_1) x + \varphi(a_0)$. If φ is injective then $\tilde{\varphi}$ is injective; if φ is surjective then $\tilde{\varphi}$ is surjective.

1.11. If I is an ideal in R, then $R[x]/I(x) \cong (R/I)[x]$.

1.12. A polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ is a zero divisor iff there is a nonzero $b \in R$ such that $a_i b = 0$ for all $i = 0, \ldots, n$ (and so, $fb = 0$). f is nilpotent iff the coefficients $a_0, \ldots, a_n$ are all nilpotent. And, assuming that R is unital, f is a unit iff a_0 is a unit and $a_1, \ldots, a_n$ are all nilpotent.

1.13. If R is an integral domain, then $R[x]$ is an integral domain. In this case, the only units in $R[x]$ are those from R.

1.14. If P is a prime ideal in R, then $P[x]$ is a prime ideal in $R[x]$.

1.15. If R is unital, for any nonconstant monic polynomial $g \in R[x]$ and any $f \in R[x]$ there exist $h, r \in R[x]$ with $\deg r < \deg g$ such that $f = gh + r$.

1.15.1. We also have:

Theorem. *If R is a Noetherian ring, then the polynomial ring $R[x]$ is also Noetherian.*

Proof. Let I be an ideal in $R[x]$. For each i, let J_i be the set of senior coefficients of elements of I of degree $\le i$; then J_i are ideals in R with $J_1 \subseteq J_2 \subseteq \ldots$. (Indeed, if $f = ax^n + \cdots$ and $g = bx^m + \cdots$, with $a, b \neq 0$ and $m \le n$, are elements of I of degree $\le i$, then $cf = cax^n + \cdots \in I$ for all $c \in R$ and $f + x^{n-m} g = (a+b)x^n + \cdots \in I$, so $ca, a+b \in J_i$.) Since R is Noetherian, there is d such that $J_i = J_d$ for all $i \ge d$. For every $i = 1, \ldots, d$ let $\{a_{i,1}, \ldots, a_{i,k_i}\}$ be a set of generators of J_i and let $f_{i,1}, \ldots, f_{i,k_i} \in I$ be such that for every $j = 1, \ldots, k_i$, $a_{i,j}$ is the senior coefficient of $f_{i,j}$. We claim that the set $A = \{f_{i,j},\ i = 1, \ldots, d,\ j = 1, \ldots, k_i\}$ generates I, $I = (A)$. Indeed, let $f \in I$, $\deg f = n$, and let a be the senior coefficient of f. Then $a \in J_i$ where $i = n$ if $n < d$ and $i = d$ if $n \ge d$. Thus there are $c_1, \ldots, c_{k_i} \in R$ such that $a = \sum_{j=1}^{k_i} c_j a_{i,j}$. Now, the polynomial $f - \sum_{j=1}^{k_i} c_j x^{n - \deg f_{i,j}} f_{i,j}$ has degree $< n$ and belongs to I, so by induction on n, it is contained in (A). Hence, $f \in (A)$ as well. ■

---

2. Roots of polynomials

2.1. For $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ and $c \in R$, *the value* of f at c is $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in R$. If $x \in Z(R)$, the mapping $R[x] \longrightarrow R$, $f \mapsto f(c)$, is a ring homomorphism, called *the evaluation homomorphism* at c.

2.2. For $f \in R[x]$, an element $c \in R$ is said to be *a root* of f if $f(c) = 0$.

2.3. If R is commutative and has no zero divisors, then for polynomials $f, g \in R[x]$, $c \in R$ is a root of fg iff c is a root of f or a root of g.

2.4. For a unital ring R, $c \in R$ is a root of a polynomial $f \in R[x]$ iff $(x - c) \mid f$ in $R[x]$ (that is, $f = (x-c)g$ for some $g \in R[x]$).

2.5. If R is an integral domain and $c_1, \ldots, c_k \in R$ are roots of a polynomial $f \in R[x]$, then $f = (x - c_1) \cdots (x - c_k)g$ for some $g \in R[x]$.

2.6. As a corollary we obtain that if R is an integral domain and a nonzero $f \in R[x]$ has degree n, then f has $\le n$ roots in R.

2.7. Notice that the statement 2.6 fails if R has zero divisors, or is noncommutative: the polynomial $x^2 - 1$ has roots $1, 3, 5, 7$ in $\mathbb{Z}_8[x]$, and the polynomial $x^2 + 1$ has roots $\pm i, \pm j, \pm k$ in the ring of integer quaternions.

2.8. Let R be unital, and let $c \in R$ be a root of $f \in R[x]$; then $f(x) = (x-c)^m g(x)$ for some $m \ge 1$ and $g \in R[x]$ with $g(c) \neq 0$. The integer m is called *the multiplicity*, or *the order* of the root c. If $m = 1$, c is said to be *a simple root* of f, and *a multiple root* if $m \ge 2$.

2.9. If R is an integral domain and a nonzero $f \in R[x]$ has degree n, then f has $\le n$ zeroes in R *counting with multiplicities*: if $c_1, \ldots, c_k$ are roots of f of multiplicites $m_1, \ldots, m_k$, then $m_1 + \cdots + m_k \le n$.

2.10. For a polynomial $f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in R[x]$, *the derivative* of f is the polynomial $f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$.

For any $f, g \in R[x]$ we have $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$.

2.11. Let R be unital.

Lemma. *A root c of a polynomial $f \in R[x]$ is a multiple root iff it is a root of f' as well, $f'(c) = 0$.*

---

3. Polynomials over fields

Let F be a field.

3.1. The ring $F[x]$ is a Euclidean domain, with deg as a Euclidean norm. $F[x]$ is therefore a PID and a UFD.

3.2. If $q \in F[x]$ is an irreducible (=prime) polynomial, then $F[x]/(q)$ is a field. The additive group of $F[x]/(q)$ is isomorphic to F^n where $n = \deg q$.

For $r \geq 2$, the quotient ring $F[x]/(q^r)$ is not an integral domain, but has no zero divisors other than nilpotent elements; it is a local ring whose only maximal ideal is its nilradical.

3.3. Let $f \in F[x]$, and let $f = q_1^{r_1} \cdots q_k^{r_k}$ be the (unique) factorization of f where $q_1, \ldots, q_k$ are irreducible elements of $F[x]$. Then $(f) = (q_1^{r_1}) \cdots (q_k^{r_k})$, and the $(q_i^{r_i})$ are comaximal, so by the Chinese remainder theorem,

$$F[x]/(f) \cong \big(F[x]/(q_1^{r_1})\big) \times \cdots \times \big(F[x]/(q_k^{r_k})\big).$$

3.4. Determining irreducible elements in the ring $F[x]$ is an important task.

In $\mathbb{C}[x]$, since $\mathbb{C}$ is an *algebraically closed* field, the only irreducible polynomials are linear: $x + c$, $c \in \mathbb{C}$.

In $\mathbb{R}[x]$ the only irreducible polynomials are linear $x + c$, $c \in \mathbb{R}$, and quadratic $x^2 + ax + b$, $a, b \in \mathbb{R}$, with $a^2 - 4b < 0$.

In $\mathbb{Q}[x]$ there are irreducible polynomials of all degrees. (We will see that the polynomials $x^n - 2$ are irreducible for all n.)

---

4. Polynomials over UFDs and Gauss's lemma

In this section, let R be a UFD and F be the field of fractions of R.

4.1. For a nonzero polynomial $f \in R[x]$, *the content* $c(f)$ of f is the gcd of the coefficients of f. (The content is defined up to multiplication by units in R.)

4.2. A polynomial $f \in R[x]$ is said to be *primitive* if $c(f) = 1$.

Monic polynomials are primitive.

Note that a polynomial f is primitive iff $f \notin (p)[x]$ for all prime $p \in R$.

4.3. Every nonzero polynomial $f \in R[x]$ is uniquely representable in the form $f = c(f)\tilde{f}$ where $\tilde{f} \in R[x]$ is primitive.

4.4. Every nonzero polynomial $f \in F[x]$ is uniquely representable in the form $f = c\tilde{f}$ where $\tilde{f} \in R[x]$ is primitive (in $R[x]$) and $c \in F$. We call c *the content* of f, $c(f)$.

4.5. The following lemma is crucial for what follows:

Lemma. *If $f, g \in R[x]$ are primitive, then fg is also primitive.*

Proof. For any prime $p \in R$, $(p)[x]$ is a prime ideal in $R[x]$ by 1.14; so, if $f, g \notin (p)[x]$, then $fg \notin (p)[x]$. ∎

4.6. As a corollary we get that for any $f, g \in R[x]$, $c(fg) = c(f)c(g)$.

4.7. For any integral domain R, if a nonzero polynomial $f \in R[x]$ is reducible in $R[x]$, $f = gh$, with both $g, h \notin R$, then f is also reducible in $F[x]$, because $g, h \in F[x]$ and are not units there. *Gauss's lemma* claims that over UFDs, the converse is also true:

Gauss's lemma. *If R is a UFD and $f \in R[x]$ is reducible in $F[x]$, then f is reducible in $R[x]$: if $f = gh$ with $g, h \in F[x]$, then there is $b \in F$ such that $bg, b^{-1}h \in R[x]$.*

Proof. Write $g = a\tilde{g}$ and $h = b\tilde{h}$ where $\tilde{g}, \tilde{h} \in R[x]$ are primitive and $a, b \in F$. Then $\tilde{g}\tilde{h}$ is primitive and $f = (ab)(\tilde{g}\tilde{h})$, so $ab = c(f) \in R$. Hence, both $c(f)\tilde{g} = bg \in R[x]$ and $\tilde{h} = b^{-1}h \in R[x]$. ∎

Corollary of the proof. $f = c(f)\tilde{g}\tilde{h}$.

4.8. As a "counterexample", consider the polynomial $f = x^2 + 1$ over the ring $R = \mathbb{Z}[2i]$. The field of fractions of R is $\mathbb{Q}[i]$, and f is reducible over this field: $f = (x - i)(x + i)$; however, f is irreducible over R. (This proves that R is not a UFD.)

4.9. As a corollary we see that if $f \in R[x]$ is primitive, then f is irreducible in $R[x]$ iff f is irreducible in $F[x]$.

4.10. If $f \in R[x]$ is monic (so primitive), $f = gh$ where $g, h \in F[x]$, and one of g, h is monic (and so the other is monic too), then, in fact, $g, h \in R[x]$. Indeed, $f = \tilde{g}\tilde{h}$ where $\tilde{g}, \tilde{h} \in R[x]$, $\tilde{g} = ag$, $\tilde{h} = bh$ for some $a, b \in F$; but since $\tilde{g}\tilde{h} = f$, they must be monic, so $\tilde{g} = g$ and $\tilde{h} = h$. (All this is up to multiplicaion by units in R, of course.)

In particular, if a monic polynomial $f \in R[x]$ has a root $\alpha \in F$, then $f(x) = (x-\alpha)g(x)$, so $x-\alpha \in R[x]$, so $\alpha \in R$.

4.11. We obtain that if R is a UFD, the irreducible elements in $R[x]$ are

(i) the primitive polynomials that are irreducible in $F[x]$; and

(ii) the prime (=irreducible) elements of R.

4.12. Theorem. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Let $f \in R[x]$, $f \neq 0$. $f \in F[x]$ and $F[x]$ is a UFD; factorize $f = \widehat{p}_1 \cdots \widehat{p}_k$ into a product of irreducibles in $F[x]$. For for each i, write $\widehat{p}_i = c_i p_i$ where $p_i \in R[x]$ is primitive and $c_i \in F$; then all p_i are nonconstant and irreducible in $R[x]$. Then $f = cp_1 \cdots p_k$, where $c = c(f)$. Factorize $c = d_1 \cdots d_l$ into a product of irreducibles in R. Then $d_1 \cdots d_l p_1 \cdots p_k$ is a factorization of f into a product of irreducibles in $R[x]$.

Let $f = b_1 \cdots b_r q_1 \cdots q_s$ be another such factorization, where $b_1, \ldots, b_r$ are irreducible elements of R and $q_1, \ldots, q_s \in R[x]$ are nonconstant primitive irreducible polynomials. Then $b_1 \cdots b_r = c(f)$, so $d_1 \cdots d_k$ and $b_1 \cdots b_r$ are two factorizations of $c(f) \in R$ and must coincide (up to permutation and association). And $q_1 \cdots q_s$ is a factorization of $c(f)^{-1} f$ in $F[x]$, so, after a renumeration, q_j coincide with $\widehat{p}_j$ and so with p_j, $j = 1, \ldots, k$, up to multiplying by a constant. But since p_j and q_j are primitive, we have $p_j = q_j$. ■

4.13. If R is a UFD, then the ring $R[x_1, \ldots, x_n]$ is a UFD for every $n \in \mathbb{N}$. In particular, the rings $F[x_1, \ldots, x_n]$ where F is a field and $\mathbb{Z}[x_1, \ldots, x_n]$ are UFDs.

---

5. Criteria of irreducibility of polynomials

In this section, let R be an integral domain and F be the field of fractions of R.

5.1. If a polynomial $f \in F[x]$ of degree ≥ 2 has a root α in F, then it is reducible, since is divisible by $x - \alpha$. If $\deg f = 2$ or 3, then f is reducible iff it has a root.

5.2. Examples. The polynomials $x^2 + x + 1$, $x^3 + x^2 + 1$ and $x^3 + x + 1$ are irreducible in $\mathbb{F}_2[x]$, since they have no roots in $\mathbb{F}_2$. The polynomial $f = x^4 + x^2 + 1$ is reducible in $\mathbb{F}_2[x]$, $f = (x^2 + x + 1)^2$, though it has no roots in $\mathbb{F}_2$. Same polynomial is reducible in $\mathbb{R}[x]$ and has no roots in $\mathbb{R}$ as well.

5.3. If R is a UFD, $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ and f has a root $\alpha \in F$, $\alpha = b/c$ in the lowest terms, then $b \mid a_0$ and $c \mid a_n$. (Indeed, we have $a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n$.) In particular, if f is monic, then c is a unit and $\alpha = c^{-1} b \in R$, with $\alpha \mid a_0$.

5.4. Examples. (i) The polynomial $f = x^4 - 2x^3 - x^2 - 2x + 1 \in \mathbb{Z}[x]$ has no roots in $\mathbb{Z}$ (and in $\mathbb{Q}$): all its roots must be integer and divide 1, but $f(-1), f(1) \neq 0$.

(ii) If a polynomial $x^n - a$ with $a \in \mathbb{Z}$ has a root $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$, and $a = \alpha^n$.

5.5. If $f \in R[x]$ is reducible, $f = gh$, then for every $c \in R$, $f(c) = g(c)h(c)$, that is, $g(c), h(c) \mid f(c)$. This fact can be used to factorize f: if we conjecture that f is divisible by a polynomial g of degree k, we can choose $k+1$ elements $c_0, \dots, c_k$ of R, construct all the polynomials $g \in F[x]$ of degree k such that $g(c_i) \mid f(c_i)$ for all i, and check whether some of them are in $R[x]$ and divide f. To construct a polynomial g of degree $\le k$ satisfying $f(c_i) = b_i$, $i = 0, \dots, k$, for given $c_0, \dots, c_k, b_0, \dots, b_k \in R$, one can utilize *Lagrange's interpolation formula*

$$g = b_0 \tfrac{(x-x_1)(x-x_2)\cdots(x-x_k)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)} + b_1 \tfrac{(x-x_0)(x-x_2)\cdots(x-x_k)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_k)} + \cdots + b_k \tfrac{(x-x_0)(x-x_1)\cdots(x-x_{k-1})}{(x_k-x_0)(x_k-x_1)\cdots(x_k-x_{k-1})}.$$

Example. Let $f = x^4 - 2x^3 - x^2 - 2x + 1 \in \mathbb{Z}[x]$. f has no roots in $\mathbb{Z}$ by 5.4(i); so if f is reducible, then $f = gh$ where both g and h are quadratic and irreducible. Put $g = a_2x^2 + a_1x + a_0$ and $h = b_2x^2 + b_1x + b_0$, with $a_i, b_i \in \mathbb{Z}$; then $a_2b_2 = 1$, so we may assume that $a_2 = b_2 = 1$, and $a_0b_0 = 1$, so $a_0 = b_0 = \pm 1$. Next, $f(1) = -3$, so $g(1) = \pm 1, \pm 3$ and $h(1) = -3/g(1)$. We therefore have only the following options for the pair g, h: $\{x^2-x+1, x^2-5x+1\}$, $\{x^2-3x+1, x^2+x+1\}$, $\{x^2+x-1, x^2-3x-1\}$, and $\{x^2-x-1, x^2+3x-1\}$. And we find that, indeed, the second pair works and $f = (x^2 - 3x + 1)(x^2 + x + 1)$.

5.6. Let $f \in R[x]$, and let I be a proper ideal in R. If f is reducible in $R[x]$, $f = gh$ with nonconstant $g, h \in R[x]$, then $\overline{f} = \overline{g}\overline{h}$ in $(R/I)[x]$ (where $\overline{p}$ denotes the image of $p \in R[x]$ in $(R/I)[x]$). If f is monic, then both g and h are monic; therefore $\overline{g}, \overline{h}$ are nonconstant, and $\overline{f}$ is reducible in $(R/I)[x]$. Hence, if a monic polynomial $f \in R[x]$ is irreducible in $(R/I)[x]$, then f is irreducible in $R[x]$.

5.7. Example. The polynomial $x^5 + 10x^4 - 3x^3 + 2x^2 - 6x + 3 \in \mathbb{Z}[x]$ modulo 2 equals $\overline{f} = x^5 + x^3 + 1$. $\overline{f}$ has no roots in $\mathbb{F}_2$; hence it is reducible only if it can be written as $\overline{g}\overline{h}$ where $\overline{g}$ and $\overline{h}$ are irreducible in $\mathbb{F}_2[x]$ with $\deg \overline{g} = 3$ and $\deg \overline{h} = 2$. The only such polynomials are $\overline{h} = x^2 + x + 1$ and $\overline{g} = x^3 + x^2 + 1$ or $x^3 + x + 1$; but $(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1 \ne \overline{f}$ and $(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1 \ne \overline{f}$, thus $\overline{f}$ is irreducible, and so is f.

5.8. *The Eisenstein's criterion* of irreducibility looks artificial but turns out to be very useful:

The Eisenstein criterion. *Let $f = a_nx^n + \cdots + a_1x + a_0 \in R[x]$, and assume that there is a prime ideal P in R such that $a_n \notin P$, $a_0, \dots, a_{n-1} \in P$, and $a_0 \notin P^2$. Then f is irreducible in $R[x]$.*

Proof. Assume that f is reducible, $f = gh$ in $R[x]$ with $g = b_kx^k + \cdots + b_1x + b_0$ and $h = c_lx^l + \cdots + c_1x + c_0$. Modulo P, f takes form $\overline{f} = a_nx^n$; since $\overline{f} = \overline{g}\overline{h}$ in R/P, both $\overline{g}$ and $\overline{h}$ must have form bx^k and cx^l. This means that $b_{k-1}, \dots, b_0, c_{l-1}, \dots, c_0 \in P$. But then $a_0 = b_0c_0 \in P^2$, contradiction. ∎

5.9. Examples. (i) The polynomials $3x^4 - 4x^3 + 6x^2 + 12x - 10$ and $2x^5 + 3x^3 + 9x^2 - 6$ are irreducible in $\mathbb{Z}[x]$. (Put $P = (2)$ and $P = (3)$ respectively.)

(ii) If for $a \in \mathbb{Z}$ there is a prime p such that $p \mid a$ and $p^2 \nmid a$, then the polynomial $x^n - a$ is irreducible in $\mathbb{Z}[x]$ for all $n \in \mathbb{N}$. (Put $P = (p)$.)

(iii) Let $p \in \mathbb{N}$ be a prime. *The p-th cyclotomic polynomial* is $\Phi_p = x^{p-1} + \cdots + x + 1 = \frac{x^p-1}{x-1}$. The polynomial $f(x) = \Phi_p(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p$ is irreducible by Eisenstein's criterion with $P = (p)$; hence, Φ_p is irreducible too.

(iv) For all n, the polynomial $y^n - x$ is irreducible in $R[x, y] = (R[x])[y]$. (Put $P = (x)$.)

(v) The polynomial $xz^4 + 3z^4 + xyz^3 - 2x^2z^3 + 6z^3 + 11y^5z^2 + 2xy^2z - 12x^5z - 8z + x^4 - 6xy^7 + 2$ is irreducible in $R[x, y, z] = (R[x, y])[z]$. (Put $P = (x, y, 2)$.)

---

6. Symmetric polynomials

In this section, R is any ring, and $n \in \mathbb{N}$.

6.1. The symmetric group S_n acts on the polynomial ring $R[x_1, \dots, x_n]$ by permutations of the variables $x_1, \dots, x_n$; the polynomials invariant under this action are said to be *symmetric*.

6.2. Examples. The polynomials $x_1^3 + x_2^3$ and $2x_1^2x_2 + 2x_1x_2^2 + 3x_1x_2$ are symmetric in $\mathbb{Z}[x_1, x_2]$. The polynomial $3x_1^2x_2 + 3x_2^2x_1 + 3x_1^2x_3 + 3x_1x_3^2 + 3x_2^2x_3 + 3x_2x_3^2 - 2x_1x_2x_3 + x_1^5 + x_2^5 + x_3^5$ is symmetric in $\mathbb{Z}[x_1, x_2, x_3]$.

6.3. The symmetric polynomials form a subring of $R[x_1, \dots, x_n]$; let us denote it by $\mathcal{S}_n$.

6.4. *The elementary symmetric polynomials* are

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n = \textstyle\sum_{i=1}^{n} x_i,\\
s_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n = \textstyle\sum_{1\le i<j\le n} x_ix_j,\\
s_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = \textstyle\sum_{1\le i<j<k\le n} x_ix_jx_k,\\
&\ \ \vdots\\
s_n &= x_1x_2\cdots x_n.
\end{aligned}$$

6.5. The main result in "the theory" of symmetric polynomials is the following theorem:

Theorem. *For any n, the elementary symmetric polynomials $s_1, \dots, s_n$ freely generate the ring $\mathcal{S}_n$ of symmetric polynomials in n variables: every $f \in \mathcal{S}_n$ is uniquely representable in the form $f = g\big(s_1, \dots, s_n\big)$ for some $g \in R[y_1, \dots, y_n]$, so that $\mathcal{S}_n \cong R[y_1, \dots, y_n]$.*

6.6. *The multidegree* of a monomial $ax_1^{k_1}\cdots x_n^{k_n}$ is the n-tuple $(k_1, \dots, k_n)$, where $k_i \in \mathbb{Z}_+ = \{0, 1, 2\dots\}$, $i = 1, \dots, n$. On the set $(\mathbb{Z}_+)^n$ of the multidegrees we introduce *the lexicographic order*: we write $(k_1, \dots, k_n) > (l_1, \dots, l_n)$ if there is $1 \le j \le n$ such that $k_i = l_i$ for all $i < j$ and $k_j > l_j$. This order is a well-order, – every nonempty subset of multidegrees has a minimal element, and therefore the complete induction principle is applicable to it: if some statement P is true for a multidegree whenever it is true for all smaller multidegrees, then P is true for all multidegrees.

For a polynomial $f \in R[x_1, \dots, x_n]$, let $\mathrm{LT}(f)$ (the leading term of f) be the monomial of f of maximal multidegree.

6.7. Proof of Theorem 6.5. Let $f \in \mathcal{S}_n$, and let $\mathrm{LT}(f) = ax_1^{k_1}\cdots x_n^{k_n}$, $a \in R$; since f is symmetric, we must have $k_1 \ge k_2 \ge \cdots \ge k_n$. (Otherwise f would have a monomial of larger multidegree.) Put $r_1 = k_1 - k_2$, $r_2 = k_2 - k_3$, …, $r_n = k_n$; then for the symmetric polynomial $h = as_1^{r_1}\cdots s_n^{r_n}$ we have

$$\mathrm{LT}(h) = ax_1^{r_1+\cdots+r_n}x_2^{r_2+\cdots+r_n}\cdots x_n^{r_n} = ax_1^{k_1}\cdots x_n^{k_n} = \mathrm{LT}(f). \tag{6.1}$$

Hence, the multidegree of the symmetric polynomial $f - h$ is smaller than the multidegree of f. By induction on the multidegree, $f - h = \tilde{g}(s_1, \dots, s_n)$ for some $\tilde{g} \in R[y_1, \dots, y_n]$, and if we put $g = ay_1^{r_1}\cdots y_n^{r_n} + \tilde{g}$, then we get $f = g(s_1, \dots, s_n)$.

We see that the ring homomorphism $\varphi\colon R[y_1, \dots, y_n] \longrightarrow \mathcal{S}_n$ defined by $\varphi(g) = g(s_1, \dots, s_n)$ is surjective. To prove that φ is injective, given $g \in R[y_1, \dots, y_n]$, find the monomial $ay_1^{r_1}\cdots y_n^{r_n}$ of g for which the n-tuple $\big(r_1 + \cdots + r_n, r_2 + \cdots + r_n, \dots, r_n\big)$ is maximal with respect to the lexicographic order. Then by (6.1), the symmetric polynomial $\varphi(g)$ contains the monomial $ax_1^{k_1}\cdots x_n^{k_n}$, which cannot be canceled by other monomials since they all have a smaller multidegree. Hence, $\varphi(g) \ne 0$, and so $\ker\varphi = 0$. ∎

6.8. If a monic polynomial $h = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ *completely splits* to linear factors, $h = (x - \alpha_1)\cdots(x - \alpha_n)$ with $\alpha_1, \dots, \alpha_n \in R$, so that $\alpha_1, \dots, \alpha_n$ are the roots of h, then we have

$$h = x^n - (\alpha_1 + \cdots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2} - \cdots + (-1)^n\alpha_1\alpha_2\cdots\alpha_n,$$

so that $a_{n-1} = -s_1(\alpha_1, \dots, \alpha_n)$, $a_{n-2} = s_2(\alpha_1, \dots, \alpha_n)$, …, $a_0 = (-1)^n s_n(\alpha_1, \dots, \alpha_n)$. In other words, the coefficients of h are $\pm$ the elementary symmetric polynomials of the roots of h.

6.9. This fact leads to the following corollary of Theorem 6.5:

Theorem. *Any symmetric polynomial of the roots of a polynomial $h \in R[x]$ (assuming that h splits completely) is a polynomial in the coefficients of h.*

To be more precise, for any $n \in \mathbb{N}$, we have a mapping $\eta\colon R^n \longrightarrow R[x]$ defined by $\eta(\alpha_1, \dots, \alpha_n) = (x - \alpha_1)\cdots(x - \alpha_n)$. Assume that $f \in R[x_1, \dots, x_n]$ is a symmetric polynomial. Then there is a polynomial $g \in R[y_1, \dots, y_n]$ such that, as functions on R^n, $f(\alpha_1, \dots, \alpha_n) = g(a_{n-1}, \dots, a_0)$, where $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = \eta(\alpha_1, \dots, \alpha_n)$.

6.10. As an example of application of Theorem 6.9, consider *the discriminant* of polynomial: for a (splitting monic) polynomial $h = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x-\alpha_1)\cdots(x-\alpha_n) \in R[x]$, *the discriminant* $D(h)$ is defined as $\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)^2$. $D(f)$ is a symmetric polynomial in the roots $\alpha_1, \ldots, \alpha_n$ of h, and thus is expressible as a polynomial of the coefficients $a_0, \ldots, a_{n-1}$ of h. And indeed, for $n = 2$, $D(h) = a_1^2 - 4a_0$; for $n = 3$, $D(h) = a_2^2a_1^2 + 18a_2a_1a_0 - 4a_1^3 - 4a_2^3a_0 - 27a_0^2$; etc. Using these formulas, we define discriminant for any polynomial, splitting or not.

6.11. The symmetric polynomials $p_k = x_1^k + \cdots + x_n^k$, $k = 1, 2, \ldots$, are called *the power sums* of $x_1, \ldots, x_n$. *The Newton identities* relate p_k with the elementary symmetric polynomials: put $s_0 = 1$, and $s_i = 0$ for all $i > n$; then for every $k \in \mathbb{N}$,

$$(-1)^k k s_k + \sum_{i=1}^{k} (-1)^{k-i} s_{k-i} p_i = 0.$$

This implies that for every k, $p_k = (-1)^{k-1} k s_k - \sum_{i=0}^{k-1} (-1)^{k-i} s_{k-i} p_i$, which allows us to find the expression for p_k as a polynomial in $s_1, \ldots, s_n$: one has $p_1 = s_1$, $p_2 = s_1^2 - 2s_2$, $p_3 = s_1^3 - 3s_1s_2 + 3s_3$, etc.