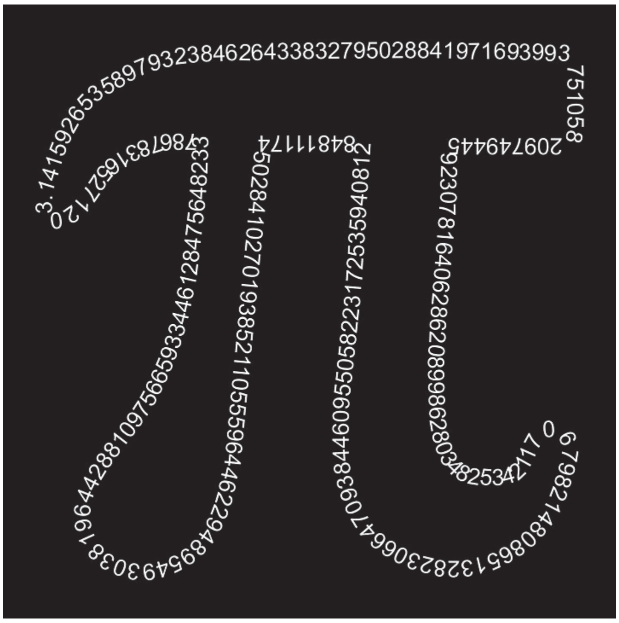
eman ta zabal zazu

Universidad del País Vasco   Euskal Herriko Unibertsitatea

OCW OpenCourseWare

MATHS BASIC COURSE FOR UNDERGRADUATES



Leire Legarreta, Iker Malaina and Luis Martínez

Faculty of Science and Technology

Department of Mathematics

University of the Basque Country

6th SUBJECT: POLYNOMIALS

The ring of polynomials. Divisibility. Polynomial greatest common divisor-Euclidean algorithm. Factorization. Irreducibility criteria. Partial fraction decomposition.

1 The ring of polynomials

Definition. *Let K be a field. (Generally, K will be the field $\mathbb{Q}$ of the rational numbers, the field $\mathbb{R}$ of the real numbers or the field $\mathbb{C}$ of the complex numbers.) A polynomial with coefficients in K is represented by the following expression,*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where the scalars $a_0, a_1, \ldots, a_n$ are elements of K, called the coefficients of the polynomial. On the other hand, the letter x is the indeterminate of the polynomial. Any two polynomials with the same coefficients are said to be equal, and the polynomial with all the coefficients equal to zero is said to be the null polynomial. A polynomial is said to be constant if for any $i \geq 1$, $a_i = 0$. In addition to this, the set formed by all the possible polynomials with coefficients in K is denoted by $K[x]$.

Definition. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ be a polynomial. The biggest index i such that $a_i \neq 0$ is called the degree of the polynomial, and it is denoted by $dg(f(x))$. By agreement, the null polynomial does not have degree and the non-zero constant polynomials are of degree zero. In addition to this, if the leading coefficient a_n of a polynomial equals 1, the polynomial is said to be a monic polynomial.*

Definition. *Let $f(x), g(x) \in K[x]$ be two polynomials expressed as $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots + b_mx^m$. Assume without any loss of generality that $m \geq n$ and that $a_n \neq 0, b_m \neq 0$. Let us define the following two operations in the set $K[x]$:*

(i) *Addition of polynomials:*

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+ \cdots + b_mx^m$$

(ii) *Product of polynomials:*

$$f(x).g(x) = a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots+(a_nb_m)x^{n+m} = \sum_{j=0}^{n+m}(\sum_{k=0}^{j} a_kb_{j-k})x^j.$$

Therefore, dg$(f(x)+g(x)) \leq$ *max*$\{$*dg*$(f(x)),$ *dg*$(g(x))\}$*, and dg*$(f(x)g(x)) =$ *dg*$(f(x))+$ *dg*$(g(x))$.

Theorem. *Let* $(K, +, .)$ *be a field. Then,* $(K[x], +, .)$ *is a commutative ring with identity. Besides,* $\mathbb{U}(K[x]) = \{$*non-zero constant polynomials*$\}$ *and* $(\mathbb{U}(K[x]), .)$ *has a group structure.*

2 Divisibility

Theorem. Division algorithm. *Let* $f(x), g(x) \in K[x]$ *be two polynomials such that dg*$(g(x)) = m > 0$ *and dg*$(f(x)) \geq$ *dg*$(g(x))$*. Then, there exist two unique polynomials* $q(x), r(x) \in K[x]$*, such that* $f(x) = g(x)q(x) + r(x)$*, with dg*$(r(x)) <$ *dg*$(g(x))$ *or* $r(x) = 0$.

Proof. *Let us define the following* P *set:* $P = \{f(x) - g(x)k(x) : k(x) \in K[x]\}$*. Since the set* P *is not empty, let us define* $r(x)$ *an element of* P *whose degree is the minimum in the set* P*. In particular,* $r(x) = f(x) - g(x)q(x)$*, for some polynomial* $q(x) \in K[x]$*. Thus,* $f(x) = g(x)q(x) + r(x)$*, being* $q(x), r(x) \in K[x]$*. Now, let us prove that dg*$(r(x)) <$ *dg*$(g(x))$ *or that* $r(x) = 0$*. First, assume that* $r(x) \neq 0$ *and denote dg*$(r(x)) = n \geq 0$*. We will prove that* $n < m$*. If not,* $n \geq m$ *or* $n - m \geq 0$*. Let us express* $r(x) = b_0 + b_1x + \cdots + b_nx^n$ *and* $g(x) = a_0 + a_1x + \cdots + a_mx^m$*.*
We define now the following polynomial of degree less than n*:*

$$h(x) = f(x) - g(x)q(x) - \frac{b_n}{a_m}x^{n-m}g(x) = r(x) - \frac{b_n}{a_m}x^{n-m}(a_0 + a_1x + \cdots + a_mx^m)$$

$$= b_0 + \cdots + b_nx^n - \frac{b_n}{a_m}x^{n-m}(a_0 + a_1x + \cdots + a_{m-1}x^{m-1}) - \frac{b_n}{a_m}x^{n-m}a_mx^m.$$

Besides, $h(x) = f(x) - g(x)(q(x) - \frac{b_n}{a_m}x^{n-m}) \in P$*, and this contradicts the fact that dg*$(r(x)) = n$ *is the minimum degree among the elements of* P*. In consequence,* $n < m$*. On the other hand, if we suppose that there exist two couples of polynomials* $(q_1(x), r_1(x))$ *and* $(q_2(x), r_2(x))$ *such that* $f(x) = g(x)q_1(x) + r_1(x),$ *dg*$(r_1(x)) <$ *dg*$(g(x))$ *or* $r_1(x) = 0$*, and* $f(x) = g(x)q_2(x) + r_2(x),$ *dg*$(r_2(x)) <$ *dg*$(g(x))$ *or* $r_2(x) = 0$*, then* $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$*. Considering now the degrees in both sides of the expression, it follows that dg*$(g(x)) +$ *dg*$(q_1(x) - q_2(x)) =$ *dg*$(r_2(x) - r_1(x)) \leq$ *max*$(r_2(x), r_1(x)) < m$*. Besides, if the polynomial of the of the left side is non-zero, then its degree is* $\geq m+0 = m$*. Consequently,* $q_1(x)-q_2(x) = 0$ *and* $r_1(x)-r_2(x) = 0$*, in other words,* $q_1(x) = q_2(x)$ *and* $r_1(x) = r_2(x)$*.*

Definition. *Let* $f(x), g(x) \in K[x]$ *be two polynomials. We say that the polynomial* $f(x)$ *divides the polynomial* $g(x)$ *or that the polynomial* $f(x)$ *is a divisor of the polynomial*

$g(x)$, if there exists some polynomial $q(x) \in K[x]$ such that $g(x) = f(x)q(x)$. The previous mentioned concept is denoted by $f(x)|g(x)$ or $f|g$.

Definition. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ be a polynomial and $\alpha \in K$. The value of $f(x)$ in α is reached replacing the indeterminate x of the polynomial $f(x)$ by α. Such obtained element of K is denoted by $f(\alpha)$. In particular, if $f(\alpha) = 0$, then α is said to be a zero or a root of the polynomial $f(x)$.*

Theorem. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ be a polynomial and $\alpha \in K$. Then, α is a zero or a root of the polynomial $f(x)$ if and only if the binomial $(x - \alpha)$ divides the polynomial $f(x)$. Anyway, the division between $f(x)$ and $(x - \alpha)$ has as remainder the value $f(\alpha)$.*

Proof. $\Longrightarrow$) *Assume that α is a root of the polynomial $f(x)$. Thus, $dg(f(x)) \geq 1$. Since $dg(x-\alpha) = 1$, from the division algorithm applied to $f(x)$ and to $(x-\alpha)$, it follows that $f(x) = (x-\alpha)q(x)+r(x)$, for some $q(x), r(x) \in K[x]$, such that $dg(r(x)) < dg(x-\alpha)$ or $r(x) = 0$. Assume that $f(x) = (x-\alpha)q(x)+a_0$. Since $f(\alpha) = (\alpha-\alpha)q(\alpha)+a_0 = 0$, it follows that $a_0 = 0$ or $r(x) = 0$.*

$\Longleftarrow$) *Assume that $(x-\alpha) \mid f(x)$. Then, $f(x) = (x-\alpha)q(x)$, for some $q(x) \in K[x]$, and consequently $f(\alpha) = (\alpha-\alpha)q(\alpha) = 0$, in other words, α is a root of the polynomial $f(x)$.*

Theorem. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ be a polynomial with $dg(f(x)) = n$. Then, the polynomial $f(x)$ has at most n roots in the field K.*

Proof. *We prove this result by induction on n. If $dg(f(x)) = 0$, then the polynomial $f(x)$ does not have zeros (or roots). If $dg(f(x)) = 1$, then $f(x) = ax + b$ and $x = -\frac{b}{a}$ is the unique root of $f(x)$. Assume now that $dg(f(x)) = n > 1$, and suppose that the statement of the theorem holds for polynomials of degree less than n. Assume also that the polynomial $f(x)$ has at least a root $a \in K$. On the contrary, the statement of the theorem holds trivially. Consider the division between $f(x)$ and $(x - a)$. Applying the division algorithm, we have $f(x) = (x - a)q(x) + r(x)$ for some $q(x), r(x) \in K[x]$, such that $dg(r(x)) = 0 < dg(x - a)$ or $r(x) = 0$. Since a is a root of the polynomial $f(x)$, using the previous theorem, we get $x-a \mid f(x)$, and consequently $r(x) = 0$. Thus, $f(x) = (x - a)q(x)$ for some $q(x) \in K[x]$, such that $dg(q(x)) = n - 1$. Therefore, applying the induction hypothesis to the polynomial $q(x)$, it follows that $q(x)$ has at most $n - 1$ roots in the field K. Moreover, since the roots of $f(x)$ in K are a and the roots coming from the polynomial $q(x)$, it follows that $f(x)$ has at most $1 + (n-1) = n$ roots in K.*

Example. *The polynomial $f(x) = x^3 - 1 = (x - 1)(x^2 + x + 1)$ has an unique root in $\mathbb{R}$.*

3 Polynomial greatest common divisor. Euclidean algorithm

Definition. *Let $f(x), g(x) \in K[x] - \{0\}$ be two polynomials. The polynomial greatest common divisor of those polynomials is defined as the polynomial $d(x)$ satisfying the following properties:*

(i) $d(x)|f(x)$ *and* $d(x)|g(x)$

(ii) *if there exists $l(x) \in K[x]$ such that $l(x)|f(x)$ and $l(x)|g(x)$, then $l(x)|d(x)$*

(iii) *$d(x)$ is taken a monic polynomial.*

In that case, it is denoted by $d(x) = gcd(f(x), g(x))$ or $d(x) = gcd(f, g) = (f, g)$.

Theorem. *There always exists the greatest common divisor $d(x)$ of any two non-zero polynomials $f(x), g(x) \in K[x]$, and in the case, there exists another $d'(x)$ satisfying the same conditions as $d(x)$, they must be equal. Moreover, there exist $\alpha(x), \beta(x) \in K[x]$ such that $gcd(f(x), g(x)) = d(x) = \alpha(x)f(x) + \beta(x)g(x)$. This is called Bezòut's identity.*

Proof. *Let us define the following P set: $P = \{\alpha(x)f(x) + \beta(x)g(x) \mid \alpha(x), \beta(x) \in K[x]\}$. Note that considering $\alpha(x) = 0$ and $\beta(x) = 1$, $0f(x)+1g(x) = g(x) \in P$; that considering $\alpha(x) = 1$ and $\beta(x) = 0$, $1f(x) + 0g(x) = f(x) \in P$, and that considering $\alpha(x) = 0$ and $\beta(x) = 0$, $0f(x) + 0g(x) = 0 \in P$.*
Since there exist non-zero polynomials in the set P, let us choose one of minimum degree in P. Call it $d_0(x)$ (without any loss of generality we can suppose that $d_0(x)$ is a monic polynomial). Thus, for that polynomial $d_0(x)$ there exist $\alpha_0(x), \beta_0(x) \in K[x]$, such that

$$d_0(x) = \alpha_0(x)f(x) + \beta_0(x)g(x).$$

We claim that $d_0(x) = gcd(f(x), g(x)) = (f, g)$.

(i) First, we prove that $d_0(x) \mid f(x)$. (Latter, in an analogous way, $d_0(x) \mid g(x)$ can be proved). Applying the division algorithm to the polynomials $f(x)$ and $d_0(x)$, it follows that there exist $q(x), r(x) \in K[x]$, such that

$$f(x) = d_0(x)q(x) + r(x), dg(r(x)) < dg(d_0(x)) \text{ or } r(x) = 0.$$

If we suppose that $r(x) \neq 0$ then,

$$r(x) = f(x) - (\alpha_0(x)f(x) + \beta_0(x)g(x))q(x) = f(x) - \alpha_0(x)f(x)q(x) - \beta_0(x)g(x)q(x)$$

$$= f(x)(1 - \alpha_0(x)q(x)) + g(x)(-\beta_0(x)q(x)) \in P,$$

and this is a contradiction with the definition of $d_0(x)$, being $dg(r(x)) < dg(d_0(x))$ and $r(x) \in P$. Thus, $r(x) = 0$ and consequently $d_0(x) \mid f(x)$.

(ii) If we suppose that there exists $l(x) \in K[x]$ such that $l(x)|f(x)$ and $l(x)|g(x)$, we should prove that $l(x)|d_0(x)$. In fact, since $l(x)|f(x)$, then $l(x)|\alpha_0(x)f(x)$, and since $l(x)|g(x)$, then $l(x)|\beta_0(x)g(x)$. Thus, $l(x) \mid \alpha_0(x)f(x) + \beta_0(x)g(x) = d_0(x)$, as required.

(iii) We have chosen $d_0(x)$ as a monic polynomial.
Suppose now that there exists another $d'(x) \in K[x]$ satisfying the same properties as $d_0(x)$ (the greatest common divisor of the polynomials $f(x)$ and $g(x)$). Then, since the polynomial $d_0(x)$ satisfies the property (i), it follows that $d_0(x) \mid f(x)$ and that $d_0(x) \mid g(x)$. Moreover, since the polynomial $d'(x)$ satisfies the property (ii), we have $d_0(x) \mid d'(x)$. In an analogous way, since the polynomial $d'(x)$ satisfies the property (i), it follows that $d'(x) \mid f(x)$ and $d'(x) \mid g(x)$. Besides, since the polynomial $d_0(x)$ satisfies the property (ii), we have $d'(x) \mid d_0(x)$. Thus, $d'(x) = d_0(x)c_1(x)$ and $d_0(x) = d'(x)c_2(x)$, for some $c_1(x), c_2(x) \in K[x]$. In consequence, $d'(x) = d'(x)c_2(x)c_1(x)$, being $c_1(x) = k_0 \in K$ and $c_2(x) = 1/k_0 \in K$, for some $k_0 \in K$. Finally, since $d'(x)$ and $d_0(x)$ are both monic polynomials, it follows necessarily that $k_0 = 1 = 1/k_0$, in other words, that $d'(x) = d_0(x)$.

Properties. (i) *If $f(x)$ is monic and $f(x)|g(x)$, then gcd$(f(x), g(x)) = f(x)$.*

(ii) *If $f(x) = g(x)q(x) + r(x)$, being dg$(r(x)) <$ dg$(g(x))$, then gcd$(f(x), g(x)) =$ gcd$(g(x), r(x))$.*

Proof. *Proof of item (ii). Denote by $d(x) =$ gcd$(f(x), g(x))$. We claim that $d(x) =$ gcd$(g(x), r(x))$. Since $d(x) \mid g(x)$, then $d(x) \mid g(x)q(x)$, and since also $d(x) \mid f(x)$, it follows that $d(x) \mid (f(x) - g(x)q(x)) = r(x)$. In particular, $d(x) \mid g(x)$ and $d(x) \mid r(x)$. Assume now that there exists $l(x) \in K[x]$ such that $l(x) \mid g(x)$ and $l(x) \mid r(x)$. Thus, $l(x) \mid g(x)q(x)$ and $l(x) \mid (g(x)q(x) + r(x))$, in other words, $l(x) \mid f(x)$. On the other hand, since $l(x) \mid f(x)$, $l(x) \mid g(x)$, using the second item held by $d(x) =$ gcd$(f(x), g(x))$, it holds that $l(x) \mid d(x)$. Finally, since $d(x)$ is a monic polynomial, we have $d(x) =$ gcd$(g(x), r(x))$.*

Theorem. Euclidean algorithm. *Let $f(x), g(x) \in K[x] - \{0\}$ be two polynomials such that dg$(f(x)) \geq$ dg$(g(x)) = m > 0$, and let $c_1(x), c_2(x), \ldots, c_n(x), c_{n+1}(x) \in K[x]$ and $r_1(x), r_2(x), \ldots, r_n(x) \in K[x] - \{0\}$ be a family of polynomials satisfying the following properties:*

$$f(x) = c_1(x)g(x) + r_1(x), dg(r_1(x)) < dg(g(x))$$

$$g(x) = c_2(x)r_1(x) + r_2(x), dg(r_2(x)) < dg(r_1(x))$$

$$r_1(x) = c_3(x)r_2(x) + r_3(x), dg(r_3(x)) < dg(r_2(x))$$

$$\vdots$$

$$\vdots$$

$$r_{n-2}(x) = c_n(x)r_{n-1}(x) + r_n(x), dg(r_n(x)) < dg(r_{n-1}(x))$$

$$r_{n-1}(x) = c_{n+1}(x)r_n(x) + r_{n+1}(x) = c_{n+1}(x)r_n(x) + 0 = c_{n+1}(x)r_n(x).$$

Then, applying once and again, the previously proved (ii) property, we have gcd$(f(x), g(x)) = (f(x), g(x)) = (g(x), r_1(x)) = (r_1(x), r_2(x)) = (r_2(x), r_3(x)) = \cdots = (r_{n-1}(x), r_n(x)) = (r_n(x), 0) = r_n(x)$ *(strictly speaking, proportional to* $r_n(x)$*).*

Example. *gcd*$(x^5-1, x^3+x-2) = (x^3+x-2, 2x^2+x-3) = (2x^2+x-3, \frac{11x}{4}-\frac{11}{4}) = \frac{11x}{4} - \frac{11}{4} \cong x - 1$

4 Factorization

Definition. *Let* $f(x) \in K[x] - \{0\}$ *be a polynomial. We say that the polynomial* $f(x)$ *is irreducible over the field* K*, if there do not exist a couple of polynomials* $g(x), h(x) \in K[x]$ *such that* $f(x) = g(x)h(x)$ *and* $1 \leq dg(g(x)), dg(h(x)) < dg(f(x))$*. In a contrary case, the polynomial* $f(x)$ *is said to be reducible over the field* K*.*

Properties. (i) *Any polynomial of degree* 1 *with coefficients in a field* K *is reducible over the field* K*.*

(ii) *If* $f(x) \in K[x]$ *is an irreducible polynomial of degree* $dg(f(x)) \geq 2$*, then* $f(x)$ *does not have roots in the field* K*.*

(iii) *The fact of not having roots in the field* K *does not imply necessarily that the polynomial is irreducible over the field* K*. For instance, the polynomial* $f(x) = (x^2+1)^2 = (x^2+1)(x^2+1)$ *does not have roots in* $\mathbb{R}$*, but the polynomial* $f(x)$ *is reducible over the field* $\mathbb{R}$*. The converse of the previous item (ii) holds necessarily only if* $dg(f(x)) = 2$ *or* 3*. (We leave its proof to the reader.)*

Theorem. *Let* $f(x) \in K[x]$ *be a non-constant polynomial. Then, there exist* $f_1(x), \ldots, f_t(x) \in K[x]$ *irreducible polynomials over* K*, such that* $f(x) = f_1(x) \ldots f_t(x)$*. In addition to this, if there exists another decomposition for the polynomial* $f(x)$*, in other words, if* $f(x) = g_1(x) \ldots g_s(x)$*, for some irreducible polynomials over* K*,* $g_1(x), \ldots, g_s(x) \in K[x]$*, then* $s = t$*, and except the order or proportional constants, for any value* i*, we have* $f_i(x) = g_i(x)$ *for any* $i \in \{1, \ldots, s\}$*.*

Definition. *Let* $f(x) \in K[x]$ *be a non-constant polynomial. If* $f(x)$ *factorizes as the product of polynomials of degree* 1*, then* $f(x)$ *is said to be completely decomposed in the ring* $K[x]$*.*

Definition. *Let $f(x) \in K[x]$ be a polynomial and $\alpha \in K$ a root of $f(x)$. Assume that there exists some $m \in \mathbb{N}$, such that $(x-\alpha)^m | f(x)$, but that the polynomial $(x-\alpha)^{m+1}$ does not divide the polynomial $f(x)$. Then, α is said to be a root of $f(x)$ of multiplicity m. Moreover, if $m = 1$, then the root α is called a simple root, and if $m > 1$, the root α is a multiple root.*

Definition. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ be a polynomial. The derivative polynomial of the polynomial $f(x)$ corresponds to the following expression: $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. Analogously, the derivative polynomials of greater orders can be defined.*

Theorem. *Let $f(x) \in K[x]$ be a polynomial and $\alpha \in K$ a root of $f(x)$. Then, in the ring $K[x]$ the multiplicity of the root α in $f(x)$ is m if and only if $f(\alpha) = f'(\alpha) = \ldots = f^{(m-1)'}(\alpha) = 0$ and $f^{(m)'}(\alpha) \neq 0$.*

Proof. *We leave the proof of it to the reader.*

5 Irreducibility criteria

Proposition. *In this result, we analyze some criteria to determine whether a polynomial $f(x)$ is irreducible or not.*

(i) *Let $f(x) \in K[x]$ be a polynomial of $dg(f(x)) = 2$ or 3. Then, $f(x)$ is irreducible over the field K if and only if $f(x)$ does not have roots in K. (We have previously proved this result.) For instance, the polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$.*

(ii) *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ be a polynomial with coefficients in $\mathbb{Z}$ of $dg(f(x)) \geq 2$. Then, in case, there exists a root of this polynomial $f(x)$ in $\mathbb{Q}$, it must be of the type $\frac{r}{s}$, such that $r \mid a_0, s \mid a_n$, $r, s \in \mathbb{Z}$ and $gcd(r, s) = 1$. (We leave the proof of it to the reader.)*

Thus, if the polynomial $f(x) = 2x^3 - x^2 + 8x + 1 \in \mathbb{Z}[x]$ had a rational root, it will be $1, -1, 1/2$ or $-1/2$. However, $f(1) \neq 0$, $f(-1) \neq 0, f(1/2) \neq 0$ and $f(-1/2) \neq 0$. In consequence, the polynomial $f(x)$ does not have rational roots.

(iii) **Gauss Lemma**

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with coefficients in $\mathbb{Z}$. Then, in the ring $\mathbb{Q}[x]$ the polynomial $f(x)$ can be decomposed as the product of two polynomials $g(x)$ and $h(x) \in \mathbb{Q}[x]$, such that $1 \leq dg(g(x)), dg(h(x)) < dg(f(x))$ if and only if in the ring $\mathbb{Z}[x]$, the polynomial $f(x)$ can be also decomposed as the product of two polynomials with coefficients in $\mathbb{Z}$ of the same previous degrees, respectively.

For instance, the polynomial $f(x) = x^4 - 2x^2 + 8x + 1 \in \mathbb{Z}[x]$ *does not have rational roots. On the other hand, if this polynomial* $f(x)$ *admitted a decomposition as a product of two polynomials of degree* 2 *with coefficients in* $\mathbb{Z}$*, then* $f(x)$ *will be expressed as* $f(x) = (x^2 + ax + b)(x^2 + cx + d)$*, satisfying the following conditions:*

$$bd = 1, bc + da = 8, d + b + ac = -2 \textit{ and } a + c = 0.$$

However, the previous system is incompatible, and consequently we conclude that $f(x)$ *is irreducible over the field* $\mathbb{Q}$*.*

(iv) **Eisenstein's extended criterion.** *Let* $p \in \mathbb{N}$ *be a prime number and* $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ *be a polynomial. Assume that,*

(a) $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$*, for* $1 \leq r \leq n$*,*

(b) $p^2 \nmid a_0$*,*

(c) $p \nmid a_r$*.*

Then, the polynomial $f(x)$ *has an irreducible factor of degree* r *or greater than* r *in the ring* $\mathbb{Z}[x]$*. In the particular case* $r = n$*, then* $f(x)$ *is also irreducible over the field* $\mathbb{Q}$*.*

For instance, let us consider the polynomial $f(x) = x^6 - 25x^5 + 3x^2 + 12 \in \mathbb{Z}[x]$ *and the prime* $p = 3$*. We have,*

(a) $3 \mid 12, 3 \mid 0, 3 \mid 3, 3 \mid 0, 3 \mid 0$,

(b) $9 \nmid 12$

(c) $3 \nmid -25$.

Then, the polynomial $f(x)$ *admits in* $\mathbb{Z}[x]$ *an irreducible factor of degree* 5 *or* 6*. In the former case, if* $f(x)$ *admits an irreducible factor of degree* 5*, then* $f(x)$ *would have also a rational root (and this does not happen; it can be proved easily). Thus,* $f(x)$ *admits an irreducible factor of degree* 6 *in* $\mathbb{Z}[x]$*, and this means that* $f(x)$ *is irreducible over the field* $\mathbb{Q}$*.*

6 Partial fraction decomposition

In this section we will describe an operation that consists in expressing a rational fraction as a sum of a polynomial (possibly zero) and one or several fractions with a simpler denominator.

Theorem. *Let $f(x), g(x) \in K[x]$ be two polynomials, such that $g(x)$ can be decomposed as the product of two polynomials which are coprimes (i.e. $g(x) = p(x)q(x)$ such that $(p(x), q(x)) = 1$), and with $dg(f(x)) \geq dg(g(x))$. Then, the fraction $f(x)/g(x)$ can be expressed in an unique form as follows,*

$$\frac{f(x)}{g(x)} = h(x) + \frac{u(x)}{q(x)} + \frac{v(x)}{p(x)},$$

$h(x), u(x), v(x) \in K[x], dg(u(x)) < dg(q(x)), dg(v(x)) < dg(p(x))$.

Proof. *First of all, we prove that there exists an expression of this type. Using the division algorithm, we have that there exist two polynomials $h(x), r(x) \in K[x]$, such that $f(x) = h(x)g(x) + r(x)$ and $dg(r(x)) < dg(g(x))$.*
In particular, $\frac{f(x)}{g(x)} = h(x) + \frac{r(x)}{g(x)}$.
Since $gcd(p(x), q(x)) = 1$, by applying Bezòut's identity there exist two polynomials $\rho(x), \phi(x) \in K[x]$ such that $\rho(x)p(x) + \phi(x)q(x) = 1$. Now, multiplying the previous expression by $r(x)$, we get that $r(x)\rho(x)p(x) + r(x)\phi(x)q(x) = r(x)$. Latter, we apply the Euclidean division to $r(x)\rho(x)$ and to $q(x)$.
So, $r(x)\rho(x) = \alpha(x)q(x) + u(x)$, being $dg(u(x)) < dg(q(x))$ and $\alpha(x), u(x) \in K[x]$. Thus, $(\alpha(x)q(x) + u(x))p(x) + r(x)\phi(x)q(x) = u(x)p(x) + (\alpha(x)p(x) + r(x)\phi(x))q(x) = r(x)$, and consequently, calling $v(x) = \alpha(x)p(x) + r(x)\phi(x)$, it follows that $u(x)p(x) + v(x)q(x) = r(x)$. Finally, we will prove that $dg(v(x)) < dg(p(x))$ (note that at this point we are done).
In fact,

$$dg(v(x)q(x)) = dg(r(x) - u(x)p(x)) \leq max(dg(r(x)), dg(u(x)p(x)))$$

$$< dg(q(x)p(x)) = dg(g(x)).$$

Observe that in the previous inequalities we have used, $dg(u(x)) < dg(q(x))$, $g(x) = p(x)q(x)$ and $dg(r(x)) < dg(g(x))$.
Finally, since the constructions made for the mentioned expression are basically unique, the found expression can be considered unique. Otherwise, if there would be another expression, considering the difference between these two expressions, it is enough to prove that the unique expression for the null polynomial is obtained through the polynomials $h(x) = u(x) = v(x) = 0$.

Corollary. *Let $f(x), g(x) \in K[x]$ be two polynomials, such that $g(x) \neq 0$. Let $g(x) = p_1(x)^{e_1} \cdots p_t(x)^{e_t}$ be the decomposition of the polynomial $g(x)$ in terms of irreducible different factors. Then, the rational function $f(x)/g(x)$ can be expressed in an unique form as follows:*

$$\frac{f(x)}{g(x)} = h(x) + \frac{u_{11}(x)}{p_1(x)} + \cdots + \frac{u_{1e_1}(x)}{p_1(x)^{e_1}} + \cdots + \frac{u_{t1}(x)}{p_t(x)} + \cdots + \frac{u_{te_t}(x)}{p_t(x)^{e_t}},$$

$$u_{ij} \in K[x], dg(u_{ij}(x)) < dg(p_i(x)).$$

Proposition. *Let $u(x), p(x) \in K[x]$ be two polynomials, such that $p(x) \neq 0$. Then, the polynomial $u(x)$ can be expressed in an unique form using the polynomial $p(x)$ as basis, as follows:*

$$u(x) = u_0(x) + u_1(x)p(x) + u_2(x)p(x)^2 + \cdots + u_t(x)p(x)^t, dg(u_i(x)) < dg(p(x)).$$

Proof. *The proof is left to the reader.*