Univariate polynomials

Marc Moreno Maza

CS 9652, February 3, 2020
Plan

Polynomials in algebra

Univariate polynomials over arbitrary commutative rings

Univariate polynomials over direct products of rings

Resultants of Univariate Polynomials

Univariate polynomial data-type
Plan

Polynomials in algebra

Univariate polynomials over arbitrary commutative rings

Univariate polynomials over direct products of rings

Resultants of Univariate Polynomials

Univariate polynomial data-type
Monoid Rings (1/6)

Notation
From now on, we consider a semi-group \( M \) whose operation is denoted multiplicatively and a ring \( A \) which may not be commutative and which may not have an identity element.

- Let \( a = (a_m)_{m \in M} \) be a sequence of elements of \( A \) indexed by \( M \), that is a map from \( M \) to \( A \).
- For every \( m \in M \) the element \( a_m \) of the sequence \( a \) is called the coefficient at \( m \) of \( a \). The support of \( a \) is the subset of \( M \) defined by
  \[
  \text{supp}(a) = \{ m \in M \mid a_m \neq 0 \} \tag{1}
  \]
The elements of \( \text{supp}(a) \) are called the monomials of \( a \).
- The sequence \( a \) is a linear combination of elements from \( M \) with coefficients from \( A \) if its support is finite.
- The set of the linear combinations of elements from \( M \) with coefficients from \( A \) is denoted by \( A[M] \) and called the monoid ring of \( M \) over \( A \).
- An element of \( A[M] \) which has only one monomial is called a term. In the case where \( M \) is a group, then \( A[M] \) is said to be a group ring.
Monoid Rings (2/6)

- Let $a, b$ be in $A[M]$.
- The *sum* of $a$ and $b$ is the map $s$ from $M$ to $A$ defined for every $m \in M$ by
  \[ s_m = a_m + b_m \]
  and denoted by $a + b$.
- The *product* of $a$ and $b$ is the map $p$ from $M$ to $A$ defined for every $m \in M$ by
  \[
  p_m = \sum_{(m', m'') \in M \times M} a_{m'} b_{m''} \quad \text{for} \quad m' m'' = m
  \]
  and denoted by $ab$. 
Proposition

For $a, b$ in $A[M]$ the sum $a + b$ and the product $ab$ belong to $A[M]$.

Proposition

The set $A[M]$ endowed with the addition

$$(a, b) \mapsto a + b$$

and the multiplication

$$(a, b) \mapsto ab$$

is a ring.
Proposition

- Assume that $\mathbb{M}$ is a monoid with identity element $1_{\mathbb{M}}$ and that $\mathbb{A}$ is a ring with (multiplicative) identity element $1_{\mathbb{A}}$.
- Let $1$ be the element of $\mathbb{A}[\mathbb{M}]$ with support $\{1_{\mathbb{M}}\}$ and with coefficient $1_{\mathbb{A}}$ at $1_{\mathbb{M}}$.
- Then, the ring $\mathbb{A}[\mathbb{M}]$ has $1$ as (multiplicative) identity element.
Definition
Assume again that $\mathbb{M}$ is a monoid with identity element $1_{\mathbb{M}}$ and that $\mathbb{A}$ is a ring with identity element $1_{\mathbb{A}}$. Then, we define a map from $\mathbb{A}$ to $\mathbb{A}[\mathbb{M}]$ by

$$a \mapsto a1_{\mathbb{M}}$$

where $a1_{\mathbb{M}}$ is the element of $\mathbb{A}[\mathbb{M}]$ whose support is $\{1_{\mathbb{M}}\}$ and whose coefficient at $1_{\mathbb{M}}$ is $a$. This map allows us to view $\mathbb{A}$ as a subset of $\mathbb{A}[\mathbb{M}]$.

Proposition
With the hypothesis of the above definition, let us assume that $\mathbb{A}$ is a commutative ring. Then, for every $a \in \mathbb{A}$ and every $b \in \mathbb{A}[\mathbb{M}]$ we have

$$(a1_{\mathbb{M}})b = b(a1_{\mathbb{M}}).$$
Remark

It follows from Proposition 4 that every element of $A$ commutes with every element of $A[M]$. However, commutativity of the multiplication in $A[M]$ requires also commutativity for $M$.

Proposition

Assume that $M$ is an abelian monoid and that $A$ is a commutative ring. Then, the ring $A[M]$ is commutative too.
The free abelian monoid

- Let $X$ be a set. The *free monoid generated by $X$* is the set denoted by $X^*$ of all words (or finite sequences) over $X$ endowed with the concatenation as multiplication and with the empty word $\varepsilon$ as identity element.

- For later user, we define $X^+ = X^* \setminus \{\varepsilon\}$.

- We consider in $X^*$ the following equivalence relation: two words $w, w'$ over $X$ are equivalent if for every $x \in X$ the number of occurrences of $x$ is the same in both $w$ and $w'$.

- The set of the residue classes of this relation is an abelian monoid (for the multiplication induced by that of $X^*$) called the *free abelian monoid generated by $X$*. Let us denote it by $\mathbb{X}$. 
Multivariate polynomials (1/4)

- Let $m$ be any element of $\mathbb{X}$. For any $x \in X$, the number of occurrences of $x$ in a representative of $m$ is called the degree of $m$ w.r.t. $x$ and is denoted by $\deg(m, x)$.

- The total degree of $m$ is the sum of the numbers $\deg(m, x)$ where $x$ runs over the elements of $X$ occurring in $m$.

- The ring $A[\mathbb{X}]$ is also denoted by $A[X]$ and its elements are called multivariate polynomials in $X$ with coefficients in $A$. If $X$ is a finite set $\{x_1, \ldots, x_p\}$ then

- $A[\mathbb{X}]$ is also denoted by $A[x_1, \ldots, x_p]$. Let $p \in A[\mathbb{X}]$ be non-zero.

- For any $x \in X$, the maximum value of $\deg(m, x)$ for $m \in \text{supp}(p)$ is the degree of $p$ w.r.t. $x$ and is denoted by $\deg(p, x)$.

- The maximum total degree of a monomial of $p$ is called the total degree of $p$. 
Univariate polynomials

- Assume from now on that $X$ is a singleton $\{x\}$.
- Observe that the free monoid generated by $X$ is clearly identical to the free abelian monoid generated by $X$.
- Moreover, every element of $\mathbb{A}[x]$ is called a univariate polynomial in $x$ with coefficients in $\mathbb{A}$.
- In addition, the total degree of a non-zero element $p$ of $\mathbb{A}[x]$ is simply called its degree and is denoted by $\deg(p)$. 
Multivariate polynomials (2/4)

Because the monoid ring $A[M]$ is a generalization of the polynomial ring $A[x]$, it is natural and convenient to use the following notation. An element $a = (a_m)_{m \in M}$ of $A[M]$ can be written

$$a = \sum_{m \in M} a_m$$
Without any additional assumption on $\mathbb{M}$, computing in $\mathbb{A}[\mathbb{M}]$ is not easy. First, one would like to have a *canonical way* to represent the elements of $\mathbb{A}[\mathbb{M}]$. That would make the comparison or the addition of two elements from $\mathbb{A}[\mathbb{M}]$ simpler. Second, computing the product of two elements $a$ and $b$ of $\mathbb{A}[\mathbb{M}]$ implies to compute all the couples $(m', m'') \in \mathbb{M} \times \mathbb{M}$ such that $m'm''$ is equal to a given $m \in \mathbb{M}$. If $\mathbb{M}$ is a group, then the equation $m'm'' = m$ is simpler since we must have $m'' = m'^{-1}m$.

**Definition**
A total order $\leq$ on an abelian monoid $\mathbb{M}$ is a *term order* if the following two conditions hold

(i) for every $m \in \mathbb{M}$ we have $1_{\mathbb{M}} \leq m$

(ii) for every $m, m', m'' \in \mathbb{M}$ we have $m \leq m' \Rightarrow mm'' \leq m'm''$
Assume that $\mathbb{M}$ is an abelian monoid endowed with a term order $\leq$ and let $a \in \mathbb{A}[\mathbb{M}]$ be a non-zero element.

- The maximum (w.r.t. the total order of $\mathbb{M}$) element of $\text{supp}(a)$ is called the *leading monomial of $a$* and is denoted by $\text{lm}(a)$.
- The coefficient of $a$ at $\text{lm}(a)$ is called the *leading coefficient of $a$* and is denoted by $\text{lc}(a)$.
- The term of $\mathbb{A}[\mathbb{M}]$ whose leading monomial is $\text{lm}(a)$ and whose leading coefficient is $\text{lc}(a)$ is called the *leading term of $a$* and is denoted by $\text{lt}(a)$.
- The element $a - \text{lt}(a)$ is called the *reductum of $a$*.
- Finally, the leading coefficient, the leading term and the reductum of 0 are defined to be 0.

It is sometimes convenient to set $\text{lm}(0) = 0$ as well.
Example (1/4)

- This example is taken from *Automata Theory* and assume that the reader is familiar with the notion of a finite automaton.
- Let us consider an alphabet $\Sigma$, a finite automaton (not necessarily deterministic) $A$ recognizing a language $\mathcal{L}$ over $\Sigma$ and a positive integer $n$.
- We are interested in computing the words of $\mathcal{L}$ with length $n$. 
Example (2/4)

- Let $Q = \{1, \ldots, q\}$ be the set of states of $A$ and let $\Sigma^*$ be the set of words over $\Sigma$.
- Recall that $\Sigma^*$ is a monoid whose identity element is the empty word.
- Let $A$ be the ring $\mathbb{Z}[\Sigma^*]$ of linear combinations of words from $\Sigma^*$ with coefficients from the ring of integer numbers $\mathbb{Z}$.
- Let $\delta : (Q, \Sigma \cup \{\varepsilon\}) \rightarrow 2^Q$ be the transition function of $A$. To every couple $(i, j) \in Q \times Q$ of states we associate the element $T_{i,j}$ of $\mathbb{Z}[\Sigma^*]$ defined by

\[
T_{i,j} = \sum_{\substack{x \in \Sigma \cup \{\varepsilon\} \\ j \in \delta(i,x)}} x.
\]

- In broad words, the element $T_{i,j}$ is the sum of the $x \in \Sigma \cup \{\varepsilon\}$ such that one transits from state $i$ to state $j$ by reading $x$. 
Example (3/4)

- Let $T$ be the square matrix of order $q$ with coefficients in $\mathbb{Z}[\Sigma^*]$ such that $T_{i,j}$ is the element of $T$ at the intersection of row $i$ and column $j$.
- Let $S$ be the horizontal vector of length $q$ with coefficients in $\mathbb{Z}$ such that $S_i = 1$ if $i$ is an initial state and $S_i = 0$ otherwise.
- Let $F$ be the vertical vector of length $q$ with coefficients in $\mathbb{Z}$ such that $F_i = 1$ if $i$ is a final state and $F_i = 0$ otherwise.
- Then we define the following element of $\mathbb{Z}[\Sigma^*]$

$$p_n(A) = ST^nF.$$

- Let us compute this quantity for $n = 2$, $\Sigma = \{a, b\}$, $Q = \{1, 2\}$, the initial state 1, the final state 2 and the following transition function

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>$\varepsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1, 2</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>$\emptyset$</td>
</tr>
</tbody>
</table>
Example (4/4)

Then, the matrix $T$ is

$$
T = \begin{pmatrix}
   a + b & b \\
   0 & a + b
\end{pmatrix}
$$

and its square is

$$
T^2 = \begin{pmatrix}
   (a + b)(a + b) & (a + b)b + b(a + b) \\
   0 & (a + b)(a + b)
\end{pmatrix}
$$

$$
= \begin{pmatrix}
   a^2 + ab + ba + b^2 & ab + ba + 2b^2 \\
   0 & a^2 + ab + ba + b^2
\end{pmatrix}
$$

Then we have

$$
p_2(A) = ST^2F
$$

$$
= \begin{pmatrix}
   1 & 0
\end{pmatrix} \begin{pmatrix}
   0 \\
   1
\end{pmatrix}
$$

$$
= ab + ba + 2b^2
$$

Observe that $ab$, $ba$ and $b^2$ are the three words of length 2 that the automaton $A$ recognizes. The coefficient 2 of $b^2$ comes from the fact that there are two ways to recognize this word.
Plan

Polynomials in algebra

Univariate polynomials over arbitrary commutative rings

Univariate polynomials over direct products of rings

Resultants of Univariate Polynomials

Univariate polynomial data-type
Throughout this section, we consider a commutative ring $\mathbb{A}$ with identity element, a symbol $x$ and the ring $\mathbb{A}[x]$ of the univariate polynomials in $x$ with coefficients in $\mathbb{A}$. We start our study of $\mathbb{A}[x]$ by characterizing its nilpotents, zero-divisors and units.

**Lemma**

Let $u$ be a unit of $\mathbb{A}$. Assume that $\mathbb{A}$ possesses nilpotents and let $a$ be one of them. Then $u + a$ is a unit of $\mathbb{A}$.

**Proof.**

Let $m > 0$ be such that $a^m = 0$. We have:

$$(u + a)\left(\frac{1}{u} - \frac{a}{u^2} + \frac{a^2}{u^3} + \cdots + (-1)^{m-1}\frac{a^{m-1}}{u^m}\right) = 1$$

Note that the above fractions make sense since $u$ is a unit of $\mathbb{A}$. The calculation shows that $u + a$ is a unit of $\mathbb{A}$. $\blacksquare$
Proposition

Let \( f = \sum_0^n a_i x^i \in A[x] \) be a non-zero polynomial. The polynomial \( f \) is a unit of \( A[x] \) if and only if \( a_0 \) is a unit of \( A \) and all other coefficients of \( f \) are nilpotents of \( A \).

Proof.

This is clear if \( n \) is null. Assume \( n > 0 \). First, assume there is a \( g \in A[x] \) such that \( f g = 1 \). Define \( g = \sum_0^m b_j x^j \). We may assume \( m \geq n \) (otherwise consider that some \( b_j \) are zero). Hence, we may have \( b_m = 0, b_{m-1} = 0, \ldots \). We obtain:

\[
\begin{align*}
    a_n b_m &= 0 \\
    a_n b_{m-1} + a_{n-1} b_m &= 0 \\
    a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m &= 0 \\
    &\vdots \\
    a_0 b_n + \cdots + a_n b_0 &= 0
\end{align*}
\]

Multiplying the second equation by \( a_n \) we get from both equations that \( a_n^2 b_{m-1} = 0 \) holds. Next, by multiplying the third equation by \( a_n^2 \) we get \( a_n^3 b_{m-2} = 0 \). Then, by induction we obtain \( a_n^{m+1} b_0 = 0 \). However we have \( a_0 b_0 = 1 \). Therefore we get \( a_n^{m+1} = 0 \). Hence \( a_n \) is a nilpotent. It follows from Lemma 2 that \( f - a_n x^n = \sum_0^{n-1} a_i x^i \) is a unit. By induction on \( n \) it follows that the \( a_i \) for \( 1 \leq i \leq n \) are nilpotents of \( A \). This shows that the condition is necessary. It is also sufficient (use Lemma 2 again). \( \square \)
Proposition

Let \( f = \sum_{0}^{n} a_{i} x^{i} \in \mathbb{A}[x] \) be a non-zero polynomial. The polynomial \( f \) is a nilpotent of \( \mathbb{A}[x] \) if and only if all coefficients of \( f \) are nilpotents of \( \mathbb{A} \).

Proof.

If \( f \) is nilpotent then \( 1 + xf \) is a unit by virtue of Lemma 2. Then, the conclusion follows from Proposition 6. The converse is shown by raising \( f \) to a sufficiently large power.  \( \square \)
Proposition
Let \( f = \sum_{0}^{n} a_{i}x^{i} \in A[x] \) be a non-zero polynomial. The polynomial \( f \) is a zero-divisor of \( A[x] \) if and only if there exists an element \( a \in A \) such that \( af = 0 \) holds.

Proof.
First, assume there is a \( g \in A[x] \) such that \( fg = 0 \). Among the possible polynomials \( g \) such that \( fg = 0 \) let us choose one with minimal degree. Define \( g = \sum_{0}^{m} b_{j}x^{j} \) with \( b_{m} \neq 0 \). Let \( r \in \mathbb{N} \) be such that \( 0 \leq r \leq n \). We have

\[
(\sum_{r}^{n} a_{i}x^{i})g = -(\sum_{0}^{r-1} a_{i}x^{i})g.
\]

The polynomial in each hand side of the above equation has degree strictly less than \( r + m \). Define \( h = (\sum_{r}^{n} a_{i}x^{i-r})g \) and assume \( h \neq 0 \). Observe that degree of \( h \) is strictly less than that of \( g \). However we have

\[
(\sum_{r}^{n} a_{i}x^{i-r})g f = 0
\]

which implies \( hf = 0 \). This contradiction with the choice for \( g \) shows that \( h \) must be zero. Therefore we have

\[
(\sum_{r}^{n} a_{i}x^{i-r})g = 0.
\]

For the case where \( r = n \) holds this leads to \( an g = 0 \). Similarly for \( r = n - 1, \ldots, r = 0 \), we obtain

\[
a_{n-1}g = a_{n-2}g = \cdots = a_{0}g = 0
\]

This shows that the condition is necessary. It is clear that the condition is also sufficient.
Example

Let us consider for $A$ the ring $\mathbb{Z}/8\mathbb{Z}$. Is the polynomial $p = 3 + 2x$ a unit of $A[x]$? Yes, this follows from Proposition 6 since its leading coefficients 3 is a unit and its other coefficient 2 is a nilpotent element. How do we compute its inverse? We can directly apply Lemma 2 with $u = 3$ and $a = 2x$. This leads to

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

Let $f, g$ be two polynomials in $\mathbb{A}[x]$ such that $g$ is a non-constant polynomial whose leading coefficient is a unit. Then, there exists a unique couple $(q, r)$ of polynomials in $\mathbb{A}[x]$ such that

$$f = qg + r \quad \text{and} \quad (r = 0 \, \text{or} \, \deg(r) < \deg(g)) \quad (3)$$

and we write

$$\begin{array}{c|cc}
 f & g \\
 r & q \\
\end{array}$$

The polynomials $q$ and $r$ are called the quotient and the remainder in the division with remainder (or simply division) of $f$ by $g$. Moreover, the couple $(q, r)$ is computed by the following algorithm.
### Division with remainder

**Input:** univariate polynomials \( f = \sum_{0}^{n} a_{i}x^{i} \) and \( g = \sum_{0}^{m} b_{i}x^{i} \) in \( \mathbb{A}[x] \) with respective degrees \( n \) and \( m \) such that \( b_{m} \) is a unit.

**Output:** the quotient \( q \) and the remainder \( r \) of \( f \) w.r.t. \( g \).

\[
\begin{align*}
n < m & \Rightarrow \textbf{return } (0, f) \\
r & := f \\
\text{for } i = n - m, n - m - 1, \ldots, 0 & \textbf{ repeat} \\
\text{if } \deg r = m + i & \textbf{ then} \\
q_{i} & := \text{lcm}(r) / b_{m} \\
r & := r - q_{i}x^{i}g \\
\text{else } q_{i} & := 0 \\
q & := \sum_{0}^{n-m} q_{i}x^{i} \\
\text{return } (q, r)
\end{align*}
\]

**Exercise**
Assuming that each element of \( \mathbb{A} \) can fit a machine word, what is the minimum space requirement for implementing the above algorithm in the case of DUP? SUP?
Proof.
We leave to the reader as an exercise to prove that Algorithm ?? computes a couple \((q, r)\) of polynomials in \(\mathbb{A}[x]\) satisfying Relation (3). So, let us assume now that we have two couples \((q, r)\) and \((q', r')\) satisfying

\[
\begin{array}{c|c}
  f & g \\
  r & q \\
\end{array}
\quad \text{and} \quad
\begin{array}{c|c}
  f & g \\
  r' & q' \\
\end{array}
\]

Then, we have

\[(q - q')g = r' - r.\]

Observe that if \(q \neq q'\) then the degree of \((q - q')g\) is at least that of \(g\). Indeed, the leading coefficient of \(g\) is a unit. Hence the product \(\text{lc}(q - q')\text{lc}(g)\) cannot be null. On the other hand, the degree of \(r' - r\) is strictly less than than of \(g\). Therefore, we must have \(q = q'\), and thus \(r = r'\). Finally, there exists a unique couple \((q, r)\) satisfying Relation (3). \qed
Proposition

Let $f, g$ be as in Proposition 9. Then, we have

\[ f \in \langle g \rangle \iff (\exists q \in A[x]) \begin{array}{c} \vdots \\ 0 \end{array} \frac{f}{g} q \]

Proof.

Left to the reader as Exercise.
Example

Assume that in $\mathbb{Z}/6\mathbb{Z}[x]$ we would like to divide $f = x^2 + 3x + 2$ by $g = 3x^2 + 4x + 1$. Since the leading coefficient of $g$ is not a unit, we cannot apply directly Algorithm ?? . However, since $\mathbb{Z}/6\mathbb{Z}$ is a direct product of fields, we can apply the D5 Principle. The element $e = 3$ is an idempotent since we have $e^2 = 3 \times 3 = 3 = e$. We define $f = 1 - e = 4$ in $\mathbb{Z}/6\mathbb{Z}$. Since $\langle 4 \rangle = \{0, 2, 4\} = \langle 2 \rangle$ in $\mathbb{Z}/6\mathbb{Z}$ we have

$$
\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/6\mathbb{Z})/\langle e \rangle \times (\mathbb{Z}/6\mathbb{Z})/\langle f \rangle \\
\cong (\mathbb{Z}/6\mathbb{Z})/\langle 3 \rangle \times (\mathbb{Z}/6\mathbb{Z})/\langle 2 \rangle \\
\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}
$$

In $\mathbb{Z}/2\mathbb{Z}[x]$ the polynomials $f$ and $g$ become respectively $\overline{f}^2 = x^2 + x$ and $\overline{g}^2 = x^2 + 1$. Since $\mathbb{Z}/2\mathbb{Z}[x]$ is an Euclidean domain the division is well defined and we obtain

$$
\begin{array}{c|cc}
  x^2 + x & x^2 + 1 \\
  x + 1 & 1
\end{array}
$$

In $\mathbb{Z}/3\mathbb{Z}[x]$ the polynomials $f$ and $g$ become respectively $\overline{f}^3 = x^2 + 2$ and $\overline{g}^3 = x + 1$ and we have

$$
\begin{array}{c|cc}
  x^2 + 2 & x + 1 \\
  0 & x + 2
\end{array}
$$

Note that there are several couples $(q, r)$ of polynomials such that $\begin{array}{c|cc}
f & g \\
r & q
\end{array}$ holds in $\mathbb{Z}/6\mathbb{Z}[x]$:

$$
\begin{array}{c|cc}
x^2 + 3x + 2 & 3x^2 + 4x + 1 \\
5x + 5 & 4x + 3
\end{array} \text{ and } \begin{array}{c|cc}
x^2 + 3x + 2 & 3x^2 + 4x + 1 \\
3x + 3 & 4x + 5
\end{array}
$$

where here we make an abusive use of this notation, since $\text{lcm}(g)$ is not a unit.
Definition
Let \( f = \sum_{0}^{n} a_{i} x^{i} \in A[x] \) be a non-zero polynomial. An element \( \alpha \in A \) is called a root of \( f \) if we have \( \sum_{0}^{n} a_{i} \alpha^{i} = 0 \).

Proposition
Let \( f \in A[x] \) be a non-constant polynomial. An element \( \alpha \in A \) is a root of \( f \) if and only if there exists a polynomial \( q \in A[x] \) such that
\[
f = q(x - \alpha) \quad \text{and} \quad \deg(q) < \deg(f).
\]

Proof.
The condition is clearly sufficient. Let us prove that it is necessary. From Proposition 9 we know that there exits a unique couple \((q, r)\) of polynomials of \( A[x] \) such that
\[
f = q(x - \alpha) + r \quad \text{and} \quad (r = 0 \quad \text{or} \quad \deg(r) < 1).
\]
Since \( f(\alpha) = 0 \) we have \( r = r(\alpha) = 0 \). In addition, since \( \text{lc}(x - \alpha) \) is a unit we also have \( \deg(f) = \deg(q) + \deg(x - \alpha) \) and thus \( \deg(q) < \deg(f) \). This completes the proof. \( \square \)
Proposition

The ring $A$ is an integral domain if and only if for every non-constant polynomial $f \in A[x]$ the number of roots of $f$ is at most the degree of $f$.

Notation

Let $I$ be an ideal of $A$. We denote by $I[X]$ the ideal generated by $I$ in $A[x]$. 
Proposition

Let $\mathcal{I}$ be an ideal of $A$ and let $f = \sum_{0}^{n} a_{i}x^{i} \in A[x]$ be a polynomial. Then, we have

$$f \in \mathcal{I}[x] \iff (\forall i \in \{0, \ldots, n\}) \ a_{i} \in \mathcal{I}.$$
Proposition
Let \( \mathcal{I} \) be an ideal of \( \mathbb{A} \) and let \( h \) be an element of \( \mathbb{A} \). Then, the following properties hold:

(i) The rings \( \mathbb{A}[X]/(\mathcal{I}[X]) \) and \( (\mathbb{A}/\mathcal{I})[X] \) are isomorphic.
(ii) The ideal \( \mathcal{I} \) is prime if and only if the ideal \( \mathcal{I}[X] \) is prime.
(iii) We have: \( \sqrt{\mathcal{I}[X]} = \sqrt{\mathcal{I}}[X] \).
(iv) The ideal \( \mathcal{I} \) is primary if and only if the ideal \( \mathcal{I}[X] \) is primary.
(v) We have: \( (\mathcal{I} : h^\infty)[X] = (\mathcal{I}[X]) : h^\infty \).

Theorem
If \( \mathbb{A} \) is an integral domain, then \( \mathbb{A}[x] \) is an integral domain.

Theorem (Hilbert Basis Theorem)
If \( \mathbb{A} \) is a Noetherian ring, then \( \mathbb{A}[x] \) is a Noetherian ring.

Theorem
If \( \mathbb{A} \) is a UFD, the \( \mathbb{A} \) is a UFD.
Plan

Polynomials in algebra

Univariate polynomials over arbitrary commutative rings

Univariate polynomials over direct products of rings

Resultants of Univariate Polynomials

Univariate polynomial data-type
Throughout this section, we consider a commutative ring $\mathbb{A}$ with identity element, a symbol $y$ and the ring $\mathbb{A}[y]$ of the univariate polynomials in $y$ with coefficients in $\mathbb{A}$.

**Definition**

Let $f_1, f_2, g$ be univariate polynomials in $\mathbb{A}[y]$. We say that $g$ is a gcd of $f_1$ and $f_2$ if $f_1$ and $f_2$ generate the same ideal in $\mathbb{F}(\mathbb{A})[y]$ as $g$ does.
Remark
Observe that if $A$ is a field, then Definition 9 coincides with the usual definition. Consider now the general case. Let $f_1, f_2, g$ be univariate polynomials in $A[y]$ such that $g$ is a gcd of $f_1, f_2$. This means that $f_1, f_2$ belongs to the ideal generated by $g$ in $Fr(A)[y]$ and that $g$ belongs to the ideal generated by $f_1, f_2$ in $Fr(A)[y]$. In other words

$$(\exists h_1, h_2, u_1, u_2 \in Fr(A)[y]) \left\{ \begin{array}{l} f_1 = h_1g \\ f_2 = h_2g \\ g = u_1f_1 + u_2f_2 \end{array} \right.$$  \hspace{1cm} (4)

Observe that a polynomial in $Fr(A)[y]$ can be viewed as an element of $(\text{Reg}(A))^{-1}(A[y])$, that is a fraction whose numerator is a polynomial in $A[y]$ and whose denominator is an element of $\text{Reg}(A)$. Hence, Relation (4) can be written

$$(\exists d_1, d_2, d_g \in \text{Reg}(A)) \left( \exists h_1, h_2, u_1, u_2 \in A[y] \right) \left\{ \begin{array}{l} d_1f_1 = h_1g \\ d_2f_2 = h_2g \\ d_gg = u_1f_1 + u_2f_2 \end{array} \right.$$  \hspace{1cm} (5)

Therefore we have proved the following proposition.

Proposition

The polynomial $g \in A[y]$ is a gcd of the polynomials $f_1, f_2 \in A[y]$ if and only there exist $d, d_1, d_2 \in \text{Reg}(A)$ such that we have

$$d_1f_1 \in \langle g \rangle, \ d_2f_2 \in \langle g \rangle, \ \text{and} \ d_gg \in \langle f_1, f_2 \rangle.$$
Proposition

Let $f_1, f_2, g, g' \in A[y]$ be such that $g, g'$ are both quasi-monic and gcds of $f_1, f_2$. Then, there exist regular elements $s, s' \in A$ such that $sg = s'g'$. In particular, we have $\deg(g) = \deg(g')$.

Proof.

Indeed, the hypothesis implies that the ideals $\langle g \rangle$ and $\langle g' \rangle$ of $\text{Fr}(A)[y]$ are equal. Hence we have $g \in \langle g' \rangle$ and $g' \in \langle g \rangle$. Thus, there exist $r, r' \in \text{Reg}(A)$ and $h, h' \in A[y]$ such that

$$rg = h'g' \quad \text{and} \quad r'g' = hg$$

leading to $r'rg = h'r'g' = h'hg$. Since $g$ and $g'$ are quasi-monic and since $r$ and $r'$ are regular elements, the leading coefficients of $h$ and $h'$ must be regular. With Relation (6) this shows that $h'$ and $h$ must have degree zero. Therefore, we have found $s = rr' \in \text{Reg}(A)$ and $s' = hh' \in \text{Reg}(A)$ such that $sg = s'g'$ holds. Consequently, the polynomials $g$ and $g'$ have the same degree. \qed
Proposition

Let \( A_1, \ldots, A_n \) be rings and let \( A \) be their direct product. Then, the polynomial ring \( A[y] \) is isomorphic with the direct product of the polynomial rings \( A_1[y], \ldots, A_n[y] \).

Proof.

The map

\[
\begin{pmatrix}
 a_{m,1} \\
 \vdots \\
 a_{m,n}
\end{pmatrix}
y^m + \cdots +
\begin{pmatrix}
 a_{1,1} \\
 \vdots \\
 a_{1,n}
\end{pmatrix}
y +
\begin{pmatrix}
 a_{0,1} \\
 \vdots \\
 a_{0,n}
\end{pmatrix}
\rightarrow
\begin{pmatrix}
 a_{m,1}y^m + \cdots + a_{1,1}y + a_{0,1} \\
 \vdots \\
 a_{m,n}y^m + \cdots + a_{1,n}y + a_{0,n}
\end{pmatrix}
\]

shows clearly the isomorphism.
Proposition

Let $A_1, \ldots, A_n$ be rings and let $A$ be their direct product. Let $f_1, f_2, g$ be in $A[x]$ and let $d$ be a positive integer. For any $i = 1, \ldots, n$ let $f_{1,i}, f_{2,i}, g_i$ be the projections on $A_i[X]$ of $f_1, f_2, g$ respectively. If for any $i = 1, \ldots, n$, the polynomial $g_i$ is a gcd of the polynomials $f_{1,i}$ and $f_{2,i}$, then $g$ is a gcd of $f_1$ and $f_2$. In addition, if every polynomial $g_i$ is quasi-monic gcd of $f_{1,i}$ and $f_{2,i}$ with degree $d$, then $g$ is quasi-monic gcd of $p$ and $q$ with degree $d$.

Proof.

Left to the reader as an exercise.
Proposition
Let $\mathbb{A}$ be a direct product of fields. Every pair of polynomials in $\mathbb{A}[y]$ admits a gcd in the sense of Definition 9

Proof.
Assume $\mathbb{A}$ is isomorphic with a direct product of fields $K_1 \times \cdots \times K_n$. Let $f_1, f_2 \in \mathbb{A}[y]$. For all $i = 1, \ldots, n$, the projections of the polynomials $f_1, f_2$ over $K_i$ have a gcd in the sense of Definition 9. Indeed, the polynomial ring $K_i[y]$ is a PID and the total quotient ring of $K_i$ is $K_i$ itself. Therefore, it follows from Proposition 18, that $f_1, f_2$ have a gcd in $\mathbb{A}[y]$. \hfill $\square$
Definition
We say that the univariate polynomial \( f \in \mathbb{A}[y] \) is *square-free* if the ideal generated by \( f \) in \( \mathbb{A}[y] \) is radical.

Definition
We say that two polynomials \( f_1, f_2 \in \mathbb{A}[y] \) are *relatively prime* if the ideal they generate in \( \mathbb{A}[y] \) is the unit ideal. That is, \( \langle f_1, f_2 \rangle_{\mathbb{A}[y]} = \langle 1 \rangle \).

Proposition
Let \( p_1, \ldots, p_n \in \mathbb{A}[y] \) be square-free polynomials such that they are pairwise relatively prime. Then, their product \( f = p_1 \cdots p_n \) is square-free.

Proof.
Left to the reader as an exercise. \( \square \)
Fundamental results

**Theorem**

Let $A$ be a direct product of fields. Let $m \in A[y]$ be non-constant, monic and square-free. Then, the residue class ring $A[y]/\langle m \rangle$ is a direct product of fields.

**Proposition**

Let $A$ be a direct product of fields. Then, the total ring of fractions $\text{Fr}(A[y])$ is a direct products of fields.
Consider $A = \mathbb{Q}[x]/(x^2 + x - 2)$. The polynomial $m = x^2 + x - 2 = (x - 1)(x + 2)$ is square-free. It follows from Theorem 12 that $A$ is a direct product of fields. Consider the polynomials $f_1, f_2 \in A[y]$ below

$$f_1 = (2x + 1) y^2 + (5x + 10) y + 6x + 12 \quad \text{and} \quad f_2 = 3 y^2 + (4x + 8) y + 4x + 5.$$ 

We aim to compute a gcd of $f_1$ and $f_2$. In practice, it is sufficient to return a component-wise gcd.

Computing over $A$ as if it was a field, we start the Euclidean Algorithm with $f_1$ and $f_2$. Since the leading coefficient of $f_2$ is a unit, we can divide $f_1$ w.r.t. $f_2$. In $\mathbb{Q}[x][y]$ we obtain

$$\begin{array}{c|c}
 f_1 & f_2 \\
 1/3(-8x^2 - 5x + 22)y - 8x^2 + 4x + 31 & 1/3(2x + 1)
\end{array}$$

and in $A[y]$ we obtain

$$\begin{array}{c|c}
 f_1 & f_2 \\
 (x + 2)y + 4x + 5 & 1/3(2x + 1)
\end{array}$$

We define $f_3 = (3x + 6)y + 12x + 15$. The next step would be to divide $f_2$ w.r.t. $f_3$. This requires to figure out if $a = 3x + 6$ is a unit or not, and if yes, to compute its inverse.
To do so, we compute the gcd $g$ of $a$ and $m = x^2 + x - 2$ together with their Bézout coefficients. We obtain:

$$g = x + 2 = \frac{1}{3}a + 0m.$$  

Since $g$ has positive degree, the element $a$ is a zero-divisor. An element $b$ such that $ab = 0$ and $b \neq 0$ is clearly $b = \frac{m}{g} = x - 1$. Since $a$ and $b$ are relatively prime we have

$$\mathbb{A} \cong \mathbb{A}/\langle a \rangle \times \mathbb{A}/\langle b \rangle$$

and thus

$$\mathbb{A}[y] \cong (\mathbb{A}/\langle a \rangle)[y] \times (\mathbb{A}/\langle b \rangle)[y].$$

Therefore, we can split the computations into two cases: $a = 0$ or $b = 0$. 
The polynomial $f_3$ becomes $-9$. This shows that $f_1$ and $f_2$ are relatively prime modulo $\langle x + 2 \rangle$.

The polynomial $f_3$ becomes $9(y + 3)$. So we need to divide $f_2 \equiv 3y^2 + 12y + 9 \mod x - 1$ w.r.t. $f_3$. We obtain

\[
\begin{array}{c|c}
3y^2 + 12y + 9 & 9(y + 3) \\
0 & \frac{1}{3}(y + 1)
\end{array}
\]

which halts the Euclidean Algorithm modulo $\langle x - 1 \rangle$ and shows that a gcd of $f_1$ and $f_2$ modulo $\langle x - 1 \rangle$ is $y + 3$.

Therefore, the D5 solution is

\[
g = \begin{cases} 
1 & \text{if } x + 2 = 0 \\
(y + 3) & \text{if } x - 1 = 0
\end{cases}
\] (7)

whereas the solution based on the idempotents would be a single output, like Relation (??) in Example ??.
Consider $\mathbb{A} = \mathbb{Q}[x]/\langle m \rangle$ where $m = x^2 + 3x + 2 = (x + 1)(x + 2)$ is square-free. Thus, $\mathbb{A}$ is a direct product of fields. Consider the polynomials $f_1, f_2 \in \mathbb{A}[y]$ below

$$f_1 = (x + 1)y^2 + y + 2x + 4 \quad \text{and} \quad f_2 = (2x + 3)y^2 + (2x + 3)y - 2x - 4.$$ 

A gcd of $f_1$ and $f_2$ computed by the D5 solution is

$$g = \begin{cases} 
  y & \text{if } x + 2 = 0, \\
  y + 2 & \text{if } x + 1 = 0.
\end{cases}$$
Consider again $\mathbb{A} = \mathbb{Q}[x]/\langle m \rangle$ where $m = x^2 + 3x + 2 = (x + 1)(x + 2)$. Consider the polynomials $f_1, f_2 \in \mathbb{A}[y]$ below

$$f_1 = (x + 2)y^2 + (2x + 3)y - 2 \quad \text{and} \quad f_2 = (x + 1)y^2 + (4x + 5)y + 4x + 6.$$ 

A gcd of $f_1$ and $f_2$ computed by the D5 solution is

$$g = \begin{cases} 
    y + 2 & \text{if } x + 2 = 0, \\
    y + 2 & \text{if } x + 1 = 0.
\end{cases}$$
Plan

- Polynomials in algebra
- Univariate polynomials over arbitrary commutative rings
- Univariate polynomials over direct products of rings
- Resultants of Univariate Polynomials
- Univariate polynomial data-type
Throughout this section, we consider a commutative ring $\mathbb{A}$ with identity element and a field $\mathbb{K}$.

**Proposition**

Let $f, g \in \mathbb{K}[x]$ be two polynomials of positive degree. The following conditions are equivalent.

1. The polynomials $f, g$ have a common factor of positive degree.
2. There exists at least one couple $(u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]$ such that

   $$uf + vg = 0, \ (u, v) \neq (0, 0), \ \text{deg}(u) < \text{deg}(g) \ \text{and} \ \text{deg}(v) < \text{deg}(f). \ (8)$$

**Proof.**

First assume that there exists $d \in \mathbb{K}[x]$ with positive degree and dividing $f$ and $g$. Let $f_1, g_1 \in \mathbb{K}[x]$ be such that $f = f_1d$ and $g = g_1d$. Then $(u, v) := (g_1, -f_1)$ satisfies Relation (8).

Assume now that Relation (8) holds for a couple $(u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]$. We may assume $u \neq 0$. In addition, we assume that $f$ and $g$ does not have a common factor of positive degree. This implies that $f$ and $g$ are relatively prime. Hence, there exist $a, b \in \mathbb{K}[x]$ such that $af + bg = 1$. Therefore, we obtain

$$u = (af + bg)u = afu + bgu = -agv + bgu = (bu - va)g.$$ 

Since $u \neq 0$, we deduce $\text{deg}(u) \geq \text{deg}(g)$. A contradiction.
**Definition**

Let \( f, g \in \mathbb{A}[x] \) be two non-zero polynomials of respective degrees \( m \) and \( n \) such that \( n + m > 0 \). We define

\[
f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \quad \text{and} \quad g = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0
\]

Then, the *Sylvester matrix* of \( f \) and \( g \) is the square matrix of order \( n + m \) with coefficients in \( \mathbb{A} \), denoted by \( \text{sylv}(f, g) \) and defined by

\[
\begin{pmatrix}
  a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\
  a_{m-1} & a_m & \ddots & \vdots & b_{n-1} & b_n & \ddots & \vdots \\
  a_{m-2} & a_{m-1} & \ddots & 0 & b_{n-2} & b_{n-1} & \ddots & 0 \\
  \vdots & \ddots & a_m & \ddots & \vdots & \ddots & b_n & \vdots \\
  \vdots & \ddots & a_{m-1} & \ddots & \vdots & \ddots & b_{n-1} & \vdots \\
  a_0 & & & & b_0 \\
  0 & a_0 & & & 0 & b_0 & & \\
  \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots \\
  0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0
\end{pmatrix}
\]

Its determinant is denoted by \( \text{res}(f, g) \) and called the *resultant* of \( f \) and \( g \).
Remark
Note that if \( n = 0 \) then we have \( \text{res}(f, g) = b_0^m \) and if \( m = 0 \) then we have \( \text{res}(f, g) = a_0^n \). Note also that we have \( \text{res}(f, g) = (-1)^{nm}\text{res}(g, f) \). It is convenient to extend the definition of \( \text{res}(f, g) \) as follows: If both \( f = 0 \) and \( g = 0 \) hold, or \( fg = 0 \) and \( f + g \) is not constant, then \( \text{res}(f, g) = 0 \); if \( fg = 0 \) and \( f + g \) is a non-zero constant, then \( \text{res}(f, g) = 1 \).
Proposition

Let \( f, g \in \mathbb{K}[x] \) be two polynomials of positive degrees. Then, the following conditions are equivalent.

1. The polynomials \( f, g \) have a common factor of positive degree.
2. \( \text{res}(f, g) = 0 \).

Proof.

Let us use the notations of Definition 13. Observe that we can turn the problem given by Relation (8) into a linear system. Indeed, let

\[
\begin{align*}
    u &= c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \quad \text{and} \quad v = d_{m-1}x^{m-1} + \cdots + d_1x + d_0
\end{align*}
\]

Then, the equation \( uf + vg = 0 \) becomes the linear system below

\[
\begin{align*}
    a_mc_{n-1} + b_nd_{m-1} &= 0 \\
    a_{m-1}c_{n-1} + a_mc_{n-2} + b_{n-1}d_{m-1} + b_n d_{m-2} &= 0 \\
    \vdots
    \end{align*}
\]

with \( \text{sylv}(f, g) \) as matrix and with \( w = ^t(c_{n-1}, \ldots, c_1, c_0, d_{m-1}, \ldots, d_1, d_0) \) as unknown vector. Since this linear system is homogeneous, it admits the trivial determinant solution \( ^t(0, \ldots, 0) \). This solution is its unique one if and only its determinant \( \text{res}(f, g) \) is not null. Hence, there exists at least one couple \( (u, v) \in \mathbb{K}[x] \times \mathbb{K}[x] \) satisfying Relation (8) if and only \( \text{res}(f, g) = 0 \).

Therefore, by virtue of Proposition 22, the polynomials \( f, g \) have a common factor of positive degree if and only \( \text{res}(f, g) = 0 \). This completes the proof.
Proposition

Assume that $\mathbb{A}$ is a UFD. Let $f, g \in \mathbb{A}[x]$ be two polynomials of positive degrees. Then, the polynomials $f, g$ have a common factor of positive degree if and only if $\text{res}(f, g) = 0$ holds.

Proof.

Let $\mathbb{K}$ be the field of fractions of $\mathbb{A}$. Assume that $f, g$ have a common factor of positive degree. Regarding $f, g$ as polynomials in $\mathbb{K}[x]$ we deduce $\text{res}(f, g) = 0$ by virtue of Proposition 23. Conversely, assume that $\text{res}(f, g) = 0$ holds. Then, the polynomials $f, g$ regarded in $\mathbb{K}[x]$ have a common factor of positive degree. Thus, they have also a common factor of positive degree, as polynomials in $\mathbb{A}[x]$. \qed
Proposition
Let \( f, g \in \mathbb{K}[x] \) be two polynomials of positive degrees and relatively prime. Then, there exists a unique couple \((u, v) \in \mathbb{K}[x] \times \mathbb{K}[x]\) such that
\[
uf + vg = 1, \quad (u, v) \neq (0, 0), \quad \deg(u) < \deg(g) \quad \text{and} \quad \deg(v) < \deg(f).
\] (10)

Proof.
By running the Extended Euclidean Algorithm, one can compute \(s, t \in \mathbb{K}[x]\) such that \(sf + tg = 1\). Indeed, the gcd of \(f\) and \(g\) in \(\mathbb{K}[x]\) is 1. Let \(q_s\) and \(r_s\) be the quotient and the remainder of \(s\) w.r.t. \(g\). Then, we define
\[
u = f q_s + t.
\]
We obtain
\[
uf + vg = fr_s + (fq_s + t)g = f(q_s g + r_s) + tg = 1
\]
In addition, we have \(\deg(u) < \deg(g)\). Since we have \(\deg(uf) = \deg(vg)\) we deduce \(\deg(v) < \deg(f)\). Therefore, the couple \((u, v)\) can be viewed as a solution of the linear system obtained from Relation (9) by replacing the last 0 (in the right-hand sides of the equalities) by 1. The determinant of this new linear system is again \(\text{res}(f, g)\). By Proposition 24 we have \(\text{res}(f, g) \neq 0\). Therefore, the couple \((u, v)\) is the unique solution of this system and the proposition is proved.
Proposition

Assume that $A$ is an integral domain. Let $f, g \in A[x]$ be two polynomials of positive degrees $m$ and $n$. Define

$$f = \sum_{k=0}^{m} a_k x^k \quad \text{and} \quad g = \sum_{k=0}^{n} b_k x^k.$$ 

Then, there exists $u, v \in A[x]$ such that we have $uf + vg = \text{res}(f, g)$. Moreover, the coefficients of $u$ and $v$ are polynomial expressions in the coefficients of $f$ and $g$. More precisely, we have

$$u, v \in \mathbb{Z}[a_m, \ldots, a_0, b_n, \ldots, b_0].$$

Proof.

Let $K$ be the field of fractions of $A$. Assume first that $f$ and $g$ have a common factor $d \in K[x]$ of positive degree. By Proposition 23, we have $\text{res}(f, g) = 0$. It is easy to see, using the Euclidean Algorithm, that the coefficients of $d$ are fractions of polynomials in $\mathbb{Z}[a_m, \ldots, a_0, b_n, \ldots, b_0]$. Let $f_1, g_1 \in K[x]$ be such that $f = f_1 d$ et $g = g_1 d$. The coefficients of the polynomials $f_1, g_1$ are fractions of polynomials in $\mathbb{Z}[a_m, \ldots, a_0, b_n, \ldots, b_0]$ too. Moreover, we have $g_1 f - f_1 g = 0$. Cleaning up the denominators in this latter equality shows the existence of $u, v \in \mathbb{Z}[a_m, \ldots, a_0, b_n, \ldots, b_0]$ such that $uf + vg = 0 = \text{res}(f, g)$.

Assume from now on that $f$ and $g$ have no common factors of positive degree. Then, by Proposition 25 there exists a unique couple of polynomials $u, v \in K[x]$ such that $uf + vg = 1$, $\deg(u) < \deg(g)$ and $\deg(v) < \deg(f)$ hold. The vector

$$w = \begin{pmatrix} c_{n-1}, \ldots, c_1, c_0, d_{m-1}, \ldots, d_1, d_0 \end{pmatrix}$$

of the coefficients of $u$ followed by those of $v$ can be viewed as the solution of a linear system which matrix is $\text{sylv}(f, g)$ and which right-hand side is a vector which coordinates are equal to 1. Therefore, Cramer formulas show that each of the coefficients of $w$ is a fraction with numerator in $\mathbb{Z}[a_m, \ldots, a_0, b_n, \ldots, b_0]$ and which denominator is $\text{res}(f, g)$. This completes the proof of the proposition.
Proposition

The algorithm below terminates and is correct.

Input: \( f, g \in \mathbb{K}[x] \) with \( f \neq 0, g \neq 0 \) and \( \deg(f) + \deg(g) > 0 \)

Output: \( \text{res}(f, g) \)

\[
\begin{align*}
m &:= \deg(f) \\
n &:= \deg(g) \\
\text{if } m < n \text{ then return } (-1)^{nm} \text{res}(g, f) \\
\text{else} \\
&\quad b_n := \text{lcm}(g) \\
&\quad \text{if } n = 0 \text{ then return } b_n^m \\
&\quad \text{else} \\
&\quad \quad h := f \text{ rem } g \\
&\quad \quad \text{if } h = 0 \text{ then return } h \\
&\quad \quad \text{else} \\
&\quad \quad \quad p := \deg(h) \\
&\quad \quad \text{return } (-1)^{nm} b_n^{m-p} \text{res}(g, h)
\end{align*}
\]
Proof.
The cases where $m < n$ or $n = 0$ follow immediately from Remark 2. So, we focus on the case where $0 < n \leq m$. Consider the matrix shown in Definition 13. Observe that for $1 \leq i \leq n$, column $i$ represents $x^{n-i}f$ and for $1 \leq j \leq m$, column $n+j$ represents $x^{m-j}g$. Observe that column $n$ (which represents $f$) can be replaced by any combination of this column and the last $m$ columns without changing the value of $\text{res}(f, g)$. For this combination, we can chose that leading to $h$. Similarly, for $1 \leq i < n$, we can replace column $i$ by $x^{n-i}h$. Now let us exchange the first $n$ columns with the $m$ last ones: this means that for $1 \leq i \leq n$ column $i$ moves to $i+n$ and that for $1 \leq j \leq m$ column $n+j$ moves to $j$. This has the effect of multiplying $\text{res}(f, g)$ by $(-1)^{nm}$. Moreover, the resulting matrix $M$ looks like

$$
\begin{pmatrix}
B & 0 \\
C & R
\end{pmatrix}
$$

where $B$ is a diagonal matrix of order $m-p$ where every diagonal element is $b_n$, $R$ is $\text{sylv}(g, h)$ and $C$ is a matrix of order $n+p$. Finally, observe that the determinant of $M$ is $b_n^{m-p}$ times the determinant of $R$. This completes the proof. \qed
Remark
It is not difficult to see that the previous algorithm can be transformed such that it computes the gcd of $f, g \in K[x]$ in case $\text{res}(f, g)$ is null. This leads to the next algorithm. In addition, this latter algorithm can be generalized to $\mathbb{A}[x]$ where $\mathbb{A}$ is a direct product of fields.
**Input:** $f, g \in \mathbb{K}[x]$ with $f \neq 0$, $g \neq 0$ and $\deg(f) + \deg(g) > 0$.

**Output:** if $\text{res}(f, g) = 0$ then $\gcd(f, g)$ else $\text{res}(f, g)$.

$m := \deg(f)$

$n := \deg(g)$

if $m < n$ then
  $r := (-1)^{nm}$
  $(f, g, m, n) := (g, f, n, m)$

else
  $r := 1$

repeat
  $b_n := \text{lcm}(g)$
  if $n = 0$ then return $r b_n^m$
  $h := f \text{ rem } g$
  if $h = 0$ then return $(1/b_n)g$
  $p := \deg(h)$
  $r := r (-1)^{nm} b_n^{m-p}$
  $(f, g, m, n) := (g, h, n, p)$
Remark
The above algorithm has been obtained from the previous one by avoiding
the recursive calls and by returning the monic gcd of the input polynomials
\( f, g \), when this gcd has a positive degree. This iterative computation raises
an interesting formula for the resultant. Let \( g_1 = g, \ldots, g_r \) be the successive
values of the variable \( g \) in the algorithm and set \( g_0 = f \). Hence we have

\[ g_r \in \mathbb{K} \text{ or } \deg(g_r) > 0 \text{ and } g_{r-1} \text{ rem } g_r = 0. \]

We define \( c_i = \text{lc}(g_i) \) and \( d_i = \deg(g_i) \) for \( 1 \leq i \leq r \). Then we have

\[ \text{res}(f, g) = c_1^{d_0-d_2} c_2^{d_1-d_3} \ldots c_{r-1}^{d_{r-2}-d_r} c_r^{d_{r-1}} \quad (11) \]

Observe that the sum of the powers in Relation (11) is \( d_0 + d_1 \).

Remark
In the next algorithm, we assume that for every polynomial \( f \in \mathbb{A}[x] \) where
\( \mathbb{A} \) is a direct product of fields the call \( \text{regularLc}(f, \mathbb{A}) \) returns a list
\( [[f_1, \mathbb{A}_1], \ldots, [f_s, \mathbb{A}_s]] \) such that the direct product \( \mathbb{A}_1 \times \cdots \times \mathbb{A}_s \) is
isomorphic with \( \mathbb{A} \) and such that \( f_i \) is the projection of \( f \) over \( \mathbb{A}_i \) and
either \( f_i = 0 \) or \( \text{lc}(f_i) \) is regular (that is, invertible since we are over a
product of fields). Observe also that this latter algorithm produces a list of
couples, returning these couples one after the other via the output
statement.
Input: A direct product of fields, \( f, g \in A[x] \) with \( f \neq 0, g \neq 0, \)
\( \deg(f) + \deg(g) > 0, \) and such that \( \text{lcm}(f), \text{lcm}(g) \) are units.

Output: \( [[l_1, A_1], \ldots, [l_s, A_s]] \) s. t. \( A_1 \times \cdots \times A_s \simeq A \) and when applied to the
projections of \( f \) and \( g \) over \( A_i \) the previous algorithm returns \( l_i. \)

\[
m := \deg(f) \\
n := \deg(g) \\
\text{if } m < n \text{ then} \\
\quad r := (-1)^{nm} \\
\quad (f, g, m, n) := (g, f, n, m) \\
\text{else} \\
\quad r := 1 \\
Tasks := [[[f, g, m, n], r, A]] \\
\text{while } Tasks \neq [] \text{ repeat} \\
\quad task := \text{first } Tasks \\
\quad Tasks := \text{rest } Tasks \\
\quad [[[f, g, m, n], r, A]] := task \\
\quad b_n := \text{lcm}(g) \\
\quad \text{if } n = 0 \text{ then output } [r b_n^m, A] \\
\quad h := f \text{ rem } g \\
\quad \text{for } [h_i, A_i] \in \text{regularLc}(h, A) \text{ repeat} \\
\quad \quad \text{if } h_i = 0 \text{ then output } [(1/b_n)g, A_i] \\
\quad \quad p := \deg(h_i) \\
\quad \quad r := r (-1)^{nm} b_n^{m-p} \\
\quad Tasks := \text{cons}([[g, h_i, n, p], r, A_i], Tasks)
Proposition
Assume that $\mathbb{A}$ is a UFD. Let $\mathbb{B}$ be another UFD of which $\mathbb{A}$ is a sub-ring. Let $f, g \in \mathbb{A}[x]$ be two polynomials of positive degree. Then, the polynomials $f, g$ have a common factor in $\mathbb{A}[x]$ if and only they have a common factor in $\mathbb{B}[x]$.

Proof.
If $f, g$ have a common factor in $\mathbb{A}[x]$, then they clearly have a common factor in $\mathbb{B}[x]$. Conversely, if they have a common factor in $\mathbb{B}[x]$, then their resultant must be zero (Proposition 24) and, thus, they have a common factor in $\mathbb{A}[x]$ (Proposition 24 again).

Remark
Proposition 28 implies that if $f, g \in \mathbb{A}[x]$ have no common factors in $\mathbb{A}[x]$, they will not have common factors in any UFD extending $\mathbb{A}$. This is not a contradiction with the fact that a polynomial may be irreducible in $\mathbb{A}[x]$ but not over a UFD extending $\mathbb{A}$. 

\qed
Proposition

Let $A$ and $B$ be two commutative rings with identity element and let $\phi$ be a ring homomorphism from $A$ to $B$. Let $f, g \in A[x]$ be such that $\phi(1c(f)) \neq 0$. Define again

$$f = \sum_{k=0}^{k=m} a_k x^k \quad \text{and} \quad g = \sum_{k=0}^{k=n} b_k x^k.$$ 

Let $i$ be the smallest index such that $\phi(b_{n-i}) \neq 0$. Then, we have

$$\phi(\text{res}(f, g)) = \phi(a_m^i) \text{res}(\phi(f), \phi(g)).$$

(12)

In particular, if 0 is the only nilpotent element of both $A$ and $B$, we have $\phi(\text{res}(f, g)) = 0$ if and only if $\text{res}(\phi(f), \phi(g)) = 0$ holds.

Proof.

Let $S = \text{sylv}(f, g)$. The image of the matrix $S$ by $\phi$ has the following shape:

$$\begin{pmatrix}
A & 0 \\
C & R
\end{pmatrix}$$

where

$$A = \begin{pmatrix}
\phi(a_m) & 0 & \ldots & 0 \\
\phi(a_{m-1}) & \phi(a_m) & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
\phi(a_{m-i+1}) & \phi(a_{m-i+2}) & \ddots & \phi(a_m)
\end{pmatrix} \quad \text{and} \quad R = \text{sylv}(\phi(f), \phi(g)).$$

Therefore, we have:

$$\phi(\text{res}(f, g)) = \det(A) \det(R) = \phi(a_m^i) \text{res}(\phi(f), \phi(g)).$$
Proposition

Let $f, g \in \mathbb{K}[x]$ be polynomials of positive degrees $m$ and $n$ respectively. Let $\mathbb{L}$ be a field extending $\mathbb{K}$ such that $f$ and $g$ factorizes in $\mathbb{L}[x]$ into polynomials of degree 1 as follows:

$$f = a_m \prod_{i=1}^{m} (x - \alpha_i) \quad \text{and} \quad g = b_n \prod_{j=1}^{n} (x - \beta_j)$$

Then, we have the following formulas

1. $\text{res}(f, g) = a_m \prod_{i=1}^{m} g(\alpha_i)$,
2. $\text{res}(f, g) = (-1)^{nm} b_n \prod_{j=1}^{n} f(\beta_j)$,
3. $\text{res}(f, g) = a_m b_n \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$.

Proof.

Let us denote by $R_2(f, g)$, $R_3(f, g)$, $R_4(f, g)$ the respective right-hand sides of the above formulas. It is clear that $R_2(f, g) = R_4(f, g)$ and $R_3(f, g) = R_4(f, g)$ hold. In order to prove that $R_2(f, g)$, $R_3(f, g)$, $R_4(f, g)$ equal $\text{res}(f, g)$ we proceed by induction on $\min(n, m)$. If $f$ and $g$ are exchanged, then both $\text{res}(f, g)$ and $R_4(f, g)$ are multiplied by $(-1)^{nm}$ such that we can assume $n \leq m$. In addition, if $n = 0$ holds then both $\text{res}(f, g)$ and $R_3(f, g)$ are equal to $(-1)^{nm} b_n^m$ such that we can assume $0 \leq n$. Then, let $q$ and $h$ be the quotient and the remainder of $f$ by $g$. If $0 \leq n \leq m$ and $h = 0$ hold, then $f$ and $g$ have a common factor, and thus $\text{res}(f, g)$ and $R_4(f, g)$ are null. So, let assume that $0 < n \leq m$ and that $h \neq 0$ hold. We have $f = q g + h$ Then, we have

$$R_3(f, g) = (-1)^{nm} b_n^m \prod_{j=1}^{n} f(\beta_j)$$

$$= (-1)^{nm} b_n^m \prod_{j=1}^{n} (q g + h)(\beta_j)$$

$$= (-1)^{nm} b_n^m \prod_{j=1}^{n} b_n^{\prod_{j=1}^{n} h(\beta_j)}$$

$$= (-1)^{n(m-p)} b_n^{m-p} (-1)^{np} b_n^{\prod_{j=1}^{n} h(\beta_j)}$$

$$= (-1)^{n(m-p)} b_n^{m-p} R_3(h, g)$$

$$= (-1)^{nm} b_n^{m-p} R_3(g, h)$$

In the course of the proof of an algorithm above we established

$$\text{res}(f, g) = (-1)^{nm} b_n^{m-p} \text{res}(f, h).$$

This completes the proof.
Remark
Proposition 30 is remarkable. Indeed, the resultant of \( f, g \in K[x] \) is an element of \( K \) whereas the right-hand sides of the three formulas belong a priori to \( L \). The existence of such a field \( L \) where \( f \) and \( g \) factorizes in \( L[x] \) into polynomials of degree 1 will be established in Section ??.

Proposition

Let \( f, g_1, g_2 \in K[x] \) be polynomials of positive degrees. Then we have

\[
\text{res}(f, g_1g_2) = \text{res}(f, g_1) \text{res}(f, g_2).
\]

Proof.

Let \( L \) be a field extending \( K \) such that \( f \) factorizes over \( L \) into polynomials of degree 1 as \( f = \prod_{i=1}^{m}(x - \alpha_i) \). (The existence of such a field will be established in Section ??.) Define \( n_1 = \deg(g_1) \) and \( n_2 = \deg(g_2) \). From Proposition 30 we have

\[
\begin{align*}
\text{res}(f, g_1g_2) &= a_m^{n_1 + n_2} \prod_{i=1}^{m}(g_1g_2)(\alpha_i) \\
&= a_m^{n_1} \prod_{i=1}^{m}g_1(\alpha_i) a_m^{n_2} \prod_{i=1}^{m}g_2(\alpha_i) \\
&= \text{res}(f, g_1) \text{res}(f, g_2).
\end{align*}
\]
Plan

Polynomials in algebra

Univariate polynomials over arbitrary commutative rings

Univariate polynomials over direct products of rings

Resultants of Univariate Polynomials

Univariate polynomial data-type
Univariate polynomial data-type

Let $A$ be a ring. The univariate polynomial of $A[x]$ can be implemented using different data-types in a computer program:

- dense univariate polynomial (DUP)
- sparse univariate polynomial (SUP)
- Straight-line program (SLP)
- ...
Dense univariate polynomial (DUP)

The polynomial

\[ p(x) = a_n x^n + \cdots + a_1 x + a_0 \]  \tag{13}

is coded by a record consisting of

- a single integer \( s \),
- a single integer \( d \leq s + 1 \),
- an array of size \( s \) such that \( a_0 + \cdots + a_n x^n \) is represented by \([a_0, \ldots, a_n, \ldots]\) and \( d = n \).

- This representation is said \textit{dense} because all \( a_i \) are coded, even those which are null.
- This representation is said \textit{canonical} (when \( d = s + 1 \) holds) because two different polynomials have different such representations.
- Hence operations like \textsc{degree}, \textsc{leading coefficient}, \textsc{reductum} are in \( \mathcal{O}(1) \).
- Addition and equality-test are in \( \mathcal{O}(n) \) and multiplication is in \( \mathcal{O}(n^2) \).
- This representation is especially good when the ring of coefficients is a small prime field, i.e. \( \mathbb{Z}/p\mathbb{Z} \) with \( p \) prime and in the range \([2, 2^N - 1]\), for a fixed \( N \).
Sparse univariate polynomial (SUP)

The polynomial

\[ p(x) = a_n x^n + \cdots + a_1 x + a_0 \]  

(14)

is coded by the list \( L \) of records \([a_i, i]\) where \( a_i \) is a nonzero coefficient and such that \( L \) is sorted decreasingly w.r.t. \( i \).

- This representation is said *sparse*, since only the nonzero \( a_i \) are coded.
- This representation is also canonical.
- Hence operations like \textsc{degree}, \textsc{leading coefficient}, \textsc{reductum} are in \( \mathcal{O}(1) \).
- Moreover the operation \textsc{reductum} does not require coefficient duplication (on the contrary of the previous representation).
- Addition and equality-test are in \( \mathcal{O}(n) \) and multiplication is in \( \mathcal{O}(n^2) \).
- This representation is especially good when the ring of coefficients is itself a ring of sparse polynomials.