Additive Decomposition of Polynomials over Unique Factorization Domains

Manar Benoumhani
Supervisor: Dr.Leila Benferhat

Department of Mathematics
University of sciences and technology Houari Boumediene

October 21, 2019

Outline

1. Preliminaries.
2. The Diamond Product over $\mathbb{F}_q$.
3. Additive Decompositon Over UFD's.

- $\mathbb{F}_q$: The finite field of order q where $q = p^s$, p is prime.
- $R[x]$: The ring of polynomials with coefficients in R.

Definition

Let a, b and c be elements of an integral domain R.

1. a and b are associates, $a = ub$, where u is a unit of R.
2. If a is not zero, a is called an irreducible if it is not a unit and, whenever $a = bc$, then b or c is a unit.
3. If a is not zero, a is called a prime if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Definition (UFD)

An integral domain R is a unique factorization domain if

1. Every nonzero element of R that is not a unit can be written as a product of irreducibles of R; and
2. The factorization into irreducibles is unique up to associates and the order in which the factors appear.

Definition (UFD)

An integral domain R is a unique factorization domain if

1. Every nonzero element of R that is not a unit can be written as a product of irreducibles of R; and
2. The factorization into irreducibles is unique up to associates and the order in which the factors appear.

Theorem

- *Let F be a field. Then, $F[x]$ is a UFD.*
- *If R is a UFD, then $R[x]$ is a UFD.*

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ be two polynomials over a commutative ring R with identity. The Sylvester matrix of f and g is the following $(n+m) \times (n+m)$ matrix:

$$Sylv = \begin{pmatrix} a_m & \cdots & a_0 & & \\ & \ddots & \cdots & \ddots & \\ & & a_m & \cdots & a_0 \\ b_n & \cdots & b_0 & & \\ & \ddots & \cdots & \ddots & \\ & & b_n & \cdots & b_0 \end{pmatrix}$$

Definition (Resultant)

The resultant of two polynomials f and g is defined by:

$$Res_x(f,g) = \det(Sylv)$$

Theorem

Let $f(x) = a_n \prod_{i=1}^{n}(x-\alpha_i)$ *and* $g(x) = b_m \prod_{j=1}^{m}(x-\beta_j)$ *be two polynomials of an integral domain* R *with indeterminates* $\alpha_1, \ldots, \alpha_n$ *and* $\beta_1, \ldots, \beta_m$*. Then*

$$Res_x(f,g) = (-1)^{nm} b_m^n \prod_{i=1}^{m} f(\beta_i). \tag{1}$$

$$Res_x(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i). \tag{2}$$

$$Res_x(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \tag{3}$$

Theorem (Rüdiger G.K. Loos 1973)

Let $f(x) = a_n \prod_{i=1}^{n}(x-\alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m}(x-\beta_j)$ be two polynomials of positive degree over an integral domain R with roots $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ respectively. Then the polynomial

$$r(x) = (-1)^{nm} g\, a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\gamma_{ij})$$

has nm roots, not necessarily distinct, suct that:

1. $r(x) = Res_y(f(x-y), g(y)), \gamma_{ij} = \alpha_i + \beta_j$, $g = 1$.
2. $r(x) = Res_y(f(x+y), g(y)), \gamma_{ij} = \alpha_i - \beta_j$, $g = 1$.
3. $r(x) = Res_y(y^m f(x/y), g(y)), \gamma_{ij} = \alpha_i \beta_j$, $g = 1$.
4. $B_0^{-m} r(x) = Res_y(f(xy), g(y)), \gamma_{ij} = \alpha_i/\beta_j$, $g = (-1)^{nm} g(0)^n / b_m^n$, $g(0) \neq 0$.

Proof.

The proof is based on (1)in all cases. □

Proof.

The proof is based on (1)in all cases. $\square$

Corollary

Except for [4], the polynomial $r(x)$ is monic if f and g are.

Part I

Additive decomposition for polynomials over $\mathbb{F}_q$

The diamond product

- Let Ω be the algebraic closure of $\mathbb{F}_q$ and $\emptyset \neq G \subset \Omega$ such that $\forall \alpha \in G, \sigma(\alpha) \in G$ where σ is the Frobenius automorphism of Ω.

The diamond product

- Let Ω be the algebraic closure of $\mathbb{F}_q$ and $\emptyset \neq G \subset \Omega$ such that $\forall \alpha \in G, \sigma(\alpha) \in G$ where σ is the Frobenius automorphism of Ω.
- There is defined a binary operation $\diamond$ on G such that:$\forall \alpha, \beta \in G : \sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta)$.

The diamond product

- Let Ω be the algebraic closure of $\mathbb{F}_q$ and $\emptyset \neq G \subset \Omega$ such that $\forall \alpha \in G, \sigma(\alpha) \in G$ where σ is the Frobenius automorphism of Ω.
- There is defined a binary operation $\diamond$ on G such that:$\forall \alpha, \beta \in G : \sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta)$.
- $M_G[q, x]$ denote the set of all monic polynomials f in $\mathbb{F}_q$ such that:

  1. The degree of $f \geq 1$.
  2. All the roots of f lie in G.

The diamond product

- Let $f, g \in M_G[q, x]$ such that $f = \prod\limits_{\alpha}(x - \alpha)$ and $g = \prod\limits_{\beta}(x - \beta)$, then:

- Let $f, g \in M_G[q, x]$ such that $f = \prod_{\alpha}(x - \alpha)$ and $g = \prod_{\beta}(x - \beta)$, then:

Definition

The diamond product of f and g is defined as:

$$f \diamond g = \prod_{\alpha}\prod_{\beta}(x - \alpha \diamond \beta) \tag{4}$$

The diamond product

- Let $f, g \in M_G[q, x]$ such that $f = \prod_{\alpha}(x - \alpha)$ and $g = \prod_{\beta}(x - \beta)$, then:

Definition

The diamond product of f and g is defined as:

$$f \diamond g = \prod_{\alpha}\prod_{\beta}(x - \alpha \diamond \beta) \tag{4}$$

- Clearly, if $\deg(f) = n$ and $\deg(g) = m$ then $\deg(f \diamond g) = nm$.

The diamond product

Example

1. Let $G = \Omega$ and $\alpha \diamond \beta = \alpha + \beta$. We'll have

$$f \diamond g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)) \tag{5}$$

$$= \prod_{\alpha} g(x - \alpha) = \prod_{\beta} f(x - \beta), \tag{6}$$

$$= f * g. \tag{7}$$

2. If $G = \Omega/\{0\}$ and $\alpha \diamond \beta = \alpha\beta$, then:

$$f \diamond g = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta), \tag{8}$$

$$= \prod_{\alpha} \alpha^m g(x/\alpha) = \prod_{\beta} \beta^n f(x/\beta), \tag{9}$$

$$= f \circ g. \tag{10}$$

Example

Let $f = x^2 + x + 1$ and $g = x^3 + x + 1$ be two polynomials in $\mathbb{F}_2[x]$.
In $\Omega[x]$, we have

$$f = (x-\alpha)(x-\alpha^2), g = (x-\beta)(x-\beta^2)(x-\beta^4)$$

where α and β are the roots of f and g respectively.
Applying **(6)** and **(8)**, it follows that:

$$\begin{aligned} f * g &= g(x-\alpha)g(x-\alpha^2), \\ &= x^6 + x^5 + x^3 + x^2 + 1. \\ f \circ g &= \alpha^3 g(x/\alpha)\alpha^6 g(x/\alpha^2) = (x^3 + \alpha^2 x + \alpha^3)(x^3 + \alpha^4 x + \alpha^6), \\ &= x^6 + x^4 + x^2 + x + 1. \end{aligned}$$

$f * f = x^2(x+1)^2$ and $f \circ f = (x+1)^2(x^2 + x + 1)$.

Theorem

The diamond product is a binary operation on $M_G[q,x]$.

- The units of $M_G[q,x]$ are the polynomials $x - c$ where c is a unit in G.
- f and g are associates ($f \sim g$) iff $f = (x-c) \diamond g$ for some unit $x - c$.

- A polynomial h in $M_G[q,x]$ which is not a unit is said to be **decomposable** with respect to $\diamond$ iff there are polynomials f and g such that $h = f \diamond g$, otherwise, h is **idecomposable**.

The diamond product

Theorem

Suppose that $(G, \diamond)$ is a group and let f and g be polynomials in $M_G[q,x]$ with $\deg(f) = n$ and $\deg(g) = m$. Then, the diamond product $f \diamond g$ is irreducible iff both f and g are irreducible and (n,m)=1.

Proof.

- Brawley, J. V., and Carlitz, L. (1987). Irreducibles and the composed product for polynomials over a finite field. Discrete Mathematics, 65(2), 115-139.

$\square$

The diamond product

Theorem

Suppose that $(G, \diamond)$ *is a group and let* f *and* g *be polynomials in* $M_G[q, x]$ *with* $\deg(f) = n$ *and* $\deg(g) = m$. *Then, the diamond product* $f \diamond g$ *is irreducible iff both* f *and* g *are irreducible and (n,m)=1.*

Proof.

- Brawley, J. V., and Carlitz, L. (1987). Irreducibles and the composed product for polynomials over a finite field. Discrete Mathematics, 65(2), 115-139.
- Munemasa, Akihiro, and Hiroko Nakamura. "A note on the Brawley-Carlitz theorem on irreducibility of composed products of polynomials over finite fields." International Workshop on the Arithmetic of Finite Fields. Springer, Cham, 2016.

$\square$

Theorem

Let G denote the additive group of Ω and let f be an irreducible polynomial in $M_G[q,x]$ of degree n. If f is additivley decomposable in $M_G[q,x]$ as

$$f = f_1 * f_2 * \cdots * f_t = g_1 * g_2 * \cdots * g_t,$$

where $\deg f_i = \deg g_i = n_i$, $i = 1, 2, \ldots, t$, *then:*

1. *The n_i's are pairwise relatively prime, where $n = n_1 \ldots\ n_t$.*
2. *The f_i's and g_i's are irreducible, and*
3. *f_i and g_i are associates for each other.*

Part II

Additive decomposition over UFD

Let $h \in \mathbb{F}_q[x]$, a monic polynomial that is decomposable as $f * g$. Let $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_m$ be the roots of f and g. Clearly we have:

$$(-1)^n f(x-t) = \prod_{i=1}^{n}(t-(x-\alpha_i))$$

Hence,

$$f * g = \prod_{i=1}^{n}\prod_{j=1}^{m}(x-(\alpha_i+\beta_j)). \tag{11}$$

$$= Res_t((-1)^n f(x-t), g(t)). \tag{12}$$

Using 12, we can define composed additon for polyomials over a commutative ring.

Additive decomposition over Commutative Rings

Let R be a commutative ring and let $f, g \in R[x]$. Then,

$$f * g = Res_t((-1)^n f(x-t), g(t)) = a^m b^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)) \tag{13}$$

where α_i and β_j are the roots of f and g respectively.

Proposition

Let R be an integral domain and K its field of fractions. Let $h, f, g \in R[x]$ such that $h = ch_1$, $f = af_1$ and $g = bg_1$ where $c, a, b \in R$ and $h_1, f_1, g_1 \in K[x]$ are monic polynomials. Then $h = f * g$ iff $h_1 = f_1 * g_1$ over K and $c = a^{\deg(g)} b^{\deg(f)}$.

Some Indecomposable Polynomials

Theorem

Let R be an integral domain. If $h \in R[x]$ has leading coefficient p, where p is prime, then h is additively indecomposable.

Proof.

We use the previous proposition. $\square$

Some Indecomposable Polynomials

Theorem

Let R be an integral domain. If $h \in R[x]$ has leading coefficient p, where p is prime, then h is additively indecomposable.

Proof.

We use the previous proposition. □

Example

All polynomials $f \in \mathbb{Z}[x]$ are additively indecomposable if their leading coefficient is a prime number.

Theorem

Let R be a unqiue factorization domain and let $h \in R[x]$ with $\deg h > 1$. If h has leading coefficient that is a square-free and not a unit of R, then h is not additively deomposable.

Proof.

Let $c = a^{\deg g} b^{\deg f}$ be the leading coefficient of h where a and b are the leading coefficients of f and g (respectively).
Suppose for the contradiction that h is ADD. Since c is a square-free, $c = up_1 p_2 \ldots p_r$

1. $p_i \mid a$.

$\square$

Some Idecomposable Polynomials

Theorem

Let R be a unqiue factorization domain and let $h \in R[x]$ with $\deg h > 1$. If h has leading coefficient that is a square-free and not a unit of R, then h is not additively deomposable.

Proof.

Let $c = a^{\deg g} b^{\deg f}$ be the leading coefficient of h where a and b are the leading coefficients of f and g (respectively).
Suppose for the contradiction that h is ADD. Since c is a square-free, $c = up_1 p_2 \ldots p_r$

1. $p_i \mid a$.
2. $p_i \mid b$.

$\square$

Some Idecomposable Polynomials

Theorem

Let R be a unqiue factorization domain and let $h \in R[x]$ with $\deg h > 1$. If h has leading coefficient that is a square-free and not a unit of R, then h is not additively deomposable.

Proof.

Let $c = a^{\deg g} b^{\deg f}$ be the leading coefficient of h where a and b are the leading coefficients of f and g (respectively).
Suppose for the contradiction that h is ADD. Since c is a square-free, $c = up_1 p_2 \dots p_r$

1. $p_i \mid a$.
2. $p_i \mid b$.
3. $p_1 p_2 \dots p_k \mid a$ and $p_{k+1} \dots p_r \mid b$.

□

Additively Decomposable Polynomials

Let R and S be two commutative rings and let

$$\sigma : R \longrightarrow S$$

be a unit-preserving homomorphism.

$$\overline{\sigma} : R[x] \longrightarrow S[x]$$
$$a_n x^n + \cdots + a_0 \mapsto \sigma(a_n)x^n + \cdots + \sigma(a_0)$$

Theorem

Let $\sigma : R \longrightarrow S$ be a unit-preserving ring homomorphism from an integral domain R to an integral domain S, and let $h \in R[x]$. If $\deg \overline{\sigma}(h) = \deg h$ and $h = f * g$ over R , then $\overline{\sigma}(h) = \overline{\sigma}(f) * \overline{\sigma}(g)$ over S.

Proof.

We will extend σ to an homomorphism form $R[x, t]$ to $S[x, t]$.

$$\sigma(Res_x(f, g)) = Res_x(\sigma(f), \sigma(g)),$$

$$f * g = Res_t((-1)^{\deg f} f(x-t), g(t)).$$

$\square$

Lemma

Let R be a unique factorization domain and let $h = ax + b \in R[x]$, where a is not a unit in R. Then $h = f_1 * \cdots * f_r$ for some linear polynomials $f_1, \ldots, f_r \in R[x]$ which are additively indecomposable.

Lemma

Let R be a unique factorization domain and let $h = ax + b \in R[x]$, where a is not a unit in R. Then $h = f_1 * \cdots * f_r$ for some linear polynomials $f_1, \ldots, f_r \in R[x]$ which are additively indecomposable.

Theorem

Let R be a unique factorization domain, let $h \in R[x]$ be a nonunit with respect to composed addition. Then $h = f_1 * \cdots * f_r$, for some polynomials $f_1, \ldots, f_r \in R[x]$ which are additively indecomposable.

Over a finite field, the additive decomposition of an irreducible is unique up to unit. For example,

$$(x^2+x+1)*(x^3+x+1) = (x^2+x+1)*(x^3+x^2+1) = x^6+x^5+x^3+x^2+1$$

where $x^3+x^2+1 = (x+1)*(x^3+x+1)$. However, that is not the case over $\mathbb{Z}$.

$$36x^4 = (2x^2)*(3x^2) = x^2*(6x^2)$$

but there's no polynomial $ax+b \in \mathbb{Z}[x]$ such that $x^2*(ax+b)$ is either $3x^2$ or $6x^2$.

Let $h \in \mathbb{F}_q[x]$, monic and irreducible.

$$\boxed{\text{h=f*g if and only if f and g are irreducible },(\deg f, \deg g) = 1}$$

Let $h = x^4 - 10x + 1 \in \mathbb{Z}[x]$, we have:

$$h = (x^2 - 2) * (x^2 - 3).$$

Let $h \in \mathbb{F}_q[x]$, monic and irreducible.

$$\boxed{\text{h=f*g if and only if f and g are irreducible },(\deg f, \deg g) = 1}$$

Let $h = x^4 - 10x + 1 \in \mathbb{Z}[x]$, we have:

$$h = (x^2 - 2) * (x^2 - 3).$$

Theorem

Let R be an integral domain and let $h \in R[x]$ be an irreducible polynomial over R. If $h = f * g$ over R then both f and g are irreducible.

The content of a polynomial f is defined by $Cont(f) = gcd(a_0, \ldots, a_m)$. When $Cont(f) = 1$, f is said to be primitive.

The content of a polynomial f is defined by $Cont(f) = gcd(a_0, \ldots, a_m)$. When $Cont(f) = 1$, f is said to be primitive.

Theorem

Let R be a unique factorization domain and $h \in R[x]$. Suppose that $h = f * g$ is additively decomposable, where

$$f(x) = \sum_{i=0}^{n} f_i x^i \text{ and } g(x) = \sum_{i=0}^{m} g_i x^i,$$

such that $\deg(f) = n$ and $\deg(g) = m$. Suppose in addition that $gcd(Cont(g), f_n) = 1$ and $gcd(Cont(f), g_m) = 1$. Then, h primitive implies f and g primitive.

The content of a polynomial f is defined by $Cont(f) = gcd(a_0, \ldots, a_m)$. When $Cont(f) = 1$, f is said to be primitive.

Theorem

Let R be a unique factorization domain and $h \in R[x]$. Suppose that $h = f * g$ is additively decomposable, where

$$f(x) = \sum_{i=0}^{n} f_i x^i \text{ and } g(x) = \sum_{i=0}^{m} g_i x^i,$$

such that $\deg(f) = n$ and $\deg(g) = m$. Suppose in addition that $gcd(Cont(g), f_n) = 1$ and $gcd(Cont(f), g_m) = 1$. Then, h primitive implies f and g primitive.

- $2x^3 + 3x^2 - 11x - 6$ and $4x^2 - 13x - 12$ are both primitive in $\mathbb{Z}[x]$ but

$$f * g = 256x^6 - 1728x^5 - 2672x^4 + 26604x^3 - 16610x^2 - 37350x + 31500$$

  is not primitive.

Bibliography

- L. Benferhat, S. M. E. Benoumhani, R. Boumahdi, and J. Larone, *Additive decompositions of polynomials over unique factorization domain*, Journal of Algebra and Its Applications.
- J. V. Brawley and L. Carlitz, *Irreducibles and the composed product for polynomials over a finite field*, Discrete Mathematics, 65 (1987), pp. 115–139.
- J. Gallian, *Contemporary abstract algebra*, Nelson Education, 2012.
- R. Loos, *Computing in algebraic extensions*, in Computer algebra, Springer, 1982, pp. 173–187.

Thank you!