Universidad Nacional Del Sur

TESIS DE DOCTOR EN MATEMÁTICA

Resolución de sistemas de ecuaciones polinomiales sobre álgebras de Post k-cíclicas

Blanca Fernanda López Martinolich

BAHÍA BLANCA ARGENTINA

2011

PREFACIO

Esta Tesis es presentada como parte de los requisitos para optar al grado académico de Doctor en Matemática de la Universidad Nacional del Sur y no ha sido presentada previamente para la obtención de otro título en esta universidad u otra. La misma contiene los resultados obtenidos en investigaciones llevadas a cabo en el ámbito de los departamentos de Matemática de la Universidad Nacional del Comahue y de la Universidad Nacional del Sur durante el período comprendido entre el 24 de febrero del 2009 y el 8 de julio del 2011, bajo la dirección del Dr. José Patricio Díaz Varela, Profesor Titular del Dpto. de Matemática de la Universidad Nacional del Sur.

A mi esposo Pablo
y a mis hijos Alejandra y Sebastián

Agradecimientos

Quisiera expresar mi agradecimiento al Dr. José Patricio Díaz Varela, director de esta tesis, cuya colaboración y paciente atención hicieron posible la culminación de este trabajo.

Al Dr. Manuel Abad, a la Lic. Nelli Meske de Jenkins y al Dra. Isabel Bermejo Díaz, por su asistencia en mi formación académica.

A la Mg. María del Carmen Vannicola, compañera de estudio, con quien probamos en forma conjunta la equivalencia entre las variedades.

Al Dr. Walter Reartes, cuyas explicaciones fueron de gran utilidad para la programación de los algoritmos en Maple.

Asimismo quiero agradecer el apoyo institucional que me brindaron los departamentos de Matemática de la Universidad Nacional del Comahue y de la Universidad Nacional del Sur.

8 de julio de 2011
Departamento de Matemática
Universidad Nacional del Comahue

RESUMEN

En el trabajo *An equivalence between Varieties of ciclic Post Algebras and Varieties generated by a finite field* [1] demostramos una equivalencia entre la variedad $\mathcal{V}(\mathcal{L}_{p,k})$ generada por el álgebra de Post $k-$cíclica simple de orden p, $L_{p,k}$ y la variedad $\mathcal{V}(\mathcal{F}(p^k))$ generada por el cuerpo con p^k elementos $\langle F(p^k); +, \cdot, F(p)\rangle$. La existencia de una interpretación entre ambas variedades nos ha permitido estudiar la resolución de sistemas de ecuaciones polinomiales sobre un álgebra $L_{p,k}$, utilizando técnicas usuales del Álgebra Conmutativa en un problema propio de la Lógica Algebraica.

En *Resolution of Algebraic Systems of Equations in the Variety of Cyclic Post Algebras* [13] mostramos un camino para resolver un sistema de ecuaciones algebraicas sobre una álgebra de Post cíclica de orden p, con p primo, utilizando la interpretación anterior, bases de Gröbner y algoritmos programados en Maple.

En esta tesis describimos un método contructivo que permite obtener a partir de un cuerpo $\langle F(p^k); +, \cdot, F(p)\rangle$, un álgebra de Post $k-$cíclica de orden p, con p primo positivo y $k \geq 1$. Las operaciones del álgebra de Post cíclica se expresan como términos en el lenguaje del cuerpo, y recíprocamente, las operaciones del cuerpo como términos en el lenguaje del álgebra de Post k-cíclica. Los algoritmos programados en Maple muestran cómo calcular estas operaciones de manera efectiva. De esto se deduce una interpretación Φ_1 entre la variedad $\mathcal{V}(\mathcal{L}_{p,k})$ y la variedad $\mathcal{V}(\mathcal{F}(p^k))$, y una interpretación Φ_2 de $\mathcal{V}(\mathcal{F}(p^k))$ en $\mathcal{V}(\mathcal{L}_{p,k})$ tal que $\Phi_2\Phi_1(B) = B$ para toda álgebra $B \in \mathcal{V}(\mathcal{L}_{p,k})$ y $\Phi_1\Phi_2(R) = R$ para todo $R \in \mathcal{V}(\mathcal{F}(p^k))$. Esta equivalencia permite analizar la existencia y búsqueda de soluciones de un sistema de ecuaciones polinomiales en $L_{p,k}[X_1, \ldots, X_n]$. Mostramos en este trabajo dos caminos diferentes para la resolución de estos sistemas.

El primer camino consiste en aplicar la interpretación Φ_1 para obtener la expresión de una ecuación algebraica postiana en el lenguaje de $F(p^k)[X_1, \ldots, X_n]$ y así poder expresar todas las ecuaciones del sistema en $F(p^k)[X_1, \ldots, X_n]$. De esta forma es posible buscar una base de Gröbner del ideal generado por los polinomios del sistema, analizar la existencia de soluciones y organizar su búsqueda. Aplicando luego la interpretación Φ_2 obtenemos un sistema equivalente al original en el lenguaje postiano de $L_{p,k}[X_1, \ldots, X_n]$. Completamos esta idea presentando varios ejemplos que explican detalladamente el método propuesto junto con los algoritmos que muestran a un mismo polinomio en ambos anillos.

El segundo camino consiste en definir el concepto de base de Gröbner de un ideal I en $L_{p,k}[X_1, \ldots, X_n]$ utilizando nuevamente las interpretaciones Φ_1 y Φ_2. Explicamos este proceso en general y en el caso particular de $p = 2$ y $k = 1$, damos un algoritmo de división y un teorema para calcular el S-polinomio de dos polinomios en dos variables. Enunciamos las dificultades que se presentan al buscar directamente una base de Gröbner de un ideal I en $L_{p,k}[X_1, \ldots, X_n]$ cuando $p \geq 3$, destacando que a pesar de las mismas, resulta interesante poder dividir en un anillo de polinomios sobre una estructura algebraica ordenada.

ABSTRACT

In the work *An equivalence between Varieties of ciclic Post Algebras and Varieties generated by a finite field* [1] we proved an equivalence between the variety $\mathcal{V}(\mathcal{L}_{p,k})$ generated by the simple k-cyclic Post algebra of order p, $L_{p,k}$, and the variety $\mathcal{V}(\mathcal{F}(p^k))$ generated by the finite field with p^k elements $\langle F(p^k); +, \cdot, F(p)\rangle$. The existence of an interpretation between both varieties has let us study the resolution of algebraic systems of equations over an algebra $L_{p,k}$, using usual techniques of Commutative Algebra in a problem of Algebraic Logic.

In *Resolution of Algebraic Systems of Equations in the Variety of Cyclic Post Algebras* [13] we show a way to solve an algebraic system of equations over a cyclic Post algebra of order p, with p prime, using the above interpretation, Gröbner bases and algorithms programmed in Maple.

In this thesis, we describe a constructive method which lets obtain from a field $\langle F(p^k); +, \cdot, F(p)\rangle$, a k-cyclic Post algebra of order p, with p prime and $k \geq 1$. The Post cyclic algebra operations are expressed as terms in the language of the field, and conversely, the field operations as terms in the language of cyclic Post algebras. The algorithms programmed in Maple show how to calculate these operations effectively. From this, we deduce an interpretation Φ_1 between the variety $\mathcal{V}(\mathcal{L}_{p,k})$ and the variety $\mathcal{V}(\mathcal{F}(p^k))$ and an interpretation Φ_2 of $\mathcal{V}(\mathcal{F}(p^k))$ into $\mathcal{V}(\mathcal{L}_{p,k})$ such that $\Phi_2\Phi_1(B) = B$ for every $B \in \mathcal{V}(\mathcal{L}_{p,k})$ and $\Phi_1\Phi_2(R) = R$ for every $R \in \mathcal{V}(\mathcal{F}(p^k))$. This equivalence lets us analyze the existence and search for solutions of an algebraic system of equations in $L_{p,k}[X_1, \ldots, X_n]$. In this work we show two differents ways for the resolution of these systems.

The first way consists in applying the interpretation Φ_1 in order to obtain the expression of a postian algebraic equation in the language of $F(p^k)[X_1, \ldots, X_n]$ and so we could show all the equations of the system in $F(p^k)[X_1, \ldots, X_n]$. In this way, it is possible to find a Gröbner base of the ideal generated by the polynomials of the system, analyze the existence of solutions and organize its search. We complete this idea giving some examples which explain in detail the proposed method with the algorithms which show the same polynomial in both rings.

The second way consists in defining the concept of Gröbner base of an ideal in $L_{p,k}[X_1, \ldots, X_n]$ using again the interpretations Φ_1 and Φ_2. We explain this process in general and in the particular case of $p = 2$ and $k = 1$, we give a division algorithm and a theorem to calculate the S-polynomial of two polynomials in two variables. We enunciate the difficulties which are presented while finding directly a Gróbner base of an ideal I in $L_{p,k}[X_1, \ldots, X_n]$ when $p \geq 3$, emphasizing that, despite them, it is interesting the fact that we could divide in a ring of polynomials over an ordered algebraic structure.

Índice general

Introducción

El objetivo de esta tesis es mostrar cómo puede abordarse el estudio de un sistema de ecuaciones polinomiales sobre un álgebra de Post k-cíclica de orden p, siendo p un entero primo positivo. La investigación aquí desarrollada tiene su origen en los trabajos de G. Moisil [31], [32], H. Cendra [10], M. Serfati [38] y S. Rudeanu [37], y en la teoría de bases de Gröbner, herramienta de gran utilidad para trabajar con sistemas de ecuaciones algebraicas [3], [7], [12].

En el primer capítulo comenzamos introduciendo algunas definiciones y resultados de álgebra universal necesarios para el desarrollo de esta tesis. Damos la definición de la variedad de las álgebras de Post de orden r k-cíclicas y mostramos que las álgebras simples, que coinciden con las álgebras subdirectamente irreducibles, son las álgebras de Post d-cíclicas de orden r, $L_{r,d}$, siendo d un divisor de k.

En el capítulo dos exponemos resultados conocidos de cuerpos finitos y extensiones de Galois que pueden verse en [18], [27], [36]. Comenzamos introduciendo extensiones arbitrarias, caracterizamos las extensiones finitas y construímos el cuerpo de raíces de un polinomio no constante f en el anillo $K[X]$, donde K es un cuerpo cualquiera. También mostramos que dos clausuras algebraicas de K son K-isomorfas y caracterizamos las extensiones de Galois, que juegan un rol fundamental en la demostración del teorema de la base normal. Dedicamos especial atención al estudio de los cuerpos finitos, mostrando que tienen p^n elementos, con p primo y la unicidad a menos de isomorfismo. Vemos que toda extensión de un cuerpo finito es una extensión de Galois y que el grupo de Galois de un cuerpo con p^n elementos es cíclico de orden n. Para finalizar damos la demostración del teorema de la base normal para el caso infinito y finito. La demostración de este último caso no se encuentra en la literatura habitual.

Extendemos en el capítulo tres los resultados de H. Cendra para cuerpos con p^n elementos describiendo la equivalencia demostrada en *An equivalence between Varieties of ciclic Post Algebras and Varieties generate by a finite field* [1]. Para esto introducimos los polinomios de Lagrange sobre el cuerpo $F(p^k)$ y los polinomios de Lagrange sobre el álgebra $L_{p,k}$ mostrando que ambos son términos discriminadores. Utilizando el método de interpolación de Lagrange de Moisil [31], damos una representación de una función $f : (F(p^k))^m \longrightarrow F(p^k)$ como un polinomio con coeficientes en el cuerpo $F(p^k)$ y expresamos toda función de $(L_{p,k})^m$ en $L_{p,k}$ como un polinomio con coeficientes en el álgebra. La equivalencia entre las variedades $\mathcal{V}(L_{p,k})$ y $\mathcal{V}(F(p^k))$ demostrada en este capítulo es uno de los resultados más importantes de esta tesis que aplicaremos en los capítulos 5 y 6. Para finalizar damos ejemplos que explican el proceso constructivo, incluyendo las operaciones cuyos programas se detallan en el apéndice.

En el capítulo cuatro estudiamos las bases de Gröbner en el anillo $K[X_1, \ldots, X_n]$, siendo K un cuerpo arbitrario. Definimos distintos órdenes monomiales, damos el lema de Dickson y el algoritmo de división en el anillo mencionado. Mostramos el teorema de la base de Hilbert y explicamos el proceso de obtención de las bases

de Gröbner, presentando una primera versión del algoritmo de Buchberger, para calcularlas de manera algorítmica. Damos la demostración del teorema de los ceros de Hilbert en sus versiones fuerte y débil y mostramos estos teoremas cuando K es un cuerpo finito. Para finalizar analizamos el caso en que la variedad de un ideal I es finita.

El capítulo cinco está dedicado a la resolución de sistemas de ecuaciones algebraicas sobre las álgebras de Post k-cíclicas. Comenzamos dando una condición necesaria y suficiente para que una ecuación postiana en n variables tenga solución [38]. Aplicamos la interpretación Φ_1 dada en el capítulo tres y con la ayuda de algoritmos programados en Maple, obtenemos las ecuaciones de los polinomios postianos en el anillo $F(p^k)[X_1, \ldots, X_n]$. Buscamos una base de Gröbner del ideal formado por los polinomios del sistema y las soluciones del mismo. Por último aplicando la interpretación Φ_2 damos un sistema equivalente al original en $L_{p,k}[X_1, \ldots, X_n]$. Para ilustrar este procedimiento mostramos varios ejemplos.

Para finalizar, en el capítulo seis imitamos el método descripto en el capítulo cuatro para construir una base de Gröbner en el anillo $L_{p,k}[X_1, \ldots, X_n]$. Mostramos ejemplos para $p = 2$ y $p = 3$, damos un algoritmo de división para $p = 2$ y $k = 1$ y un teorema para calcular S-polinomios en $L_2[X, Y]$. Analizamos las dificultadas que existen para encontrar una base en el caso general y expresamos las conclusiones obtenidas en el desarrollo de esta tesis.

En el apéndice incluímos los algoritmos programados en Maple que han sido necesarios para la mayoría de los ejemplos dados. Mostramos cómo calcular las operaciones de un álgebra de Post k-cíclica de orden 3 para $k = 1$ y $k = 2$ como términos en el lenguaje de los cuerpos $F(3)$ y $F(3^2)$, y recíprocamente, como obtener las operaciones de estos cuerpos como términos en el lenguaje de las álgebras L_3 y $L_{3,2}$. También presentamos algoritmos que muestran la expresión en $F(3)[X, Y]$ y $F(3^2)[X, Y]$ de polinomios dados en $L_3[X, Y]$ y $L_{3,2}[X, Y]$ y recíprocamente.

En esta tesis hemos logrado **vincular** algunos conceptos de las estructuras algebraicas tradicionales como los cuerpos finitos, con otros de las estructuras algebraicas ordenadas como las álgebras de Post cíclicas. La interpretación descripta en el capítulo 3 nos ha permitido expresar las operaciones de un álgebra de Post cíclica como términos en el lenguaje del cuerpo, y recíprocamente, las operaciones del cuerpo como términos en el lenguaje del álgebra de Post cíclica, resolver sistemas de ecuaciones sobre estas álgebras, poder dividir en un anillo de polinomios sobre una estructura algebraica ordenada y definir las bases de Gröbner de un ideal en un anillo de ecuaciones polinomiales postianas. Este puente establecido entre las estructuras mencionadas deja abierto un camino para resolver otro tipo de problemas sobre las álgebras de Post cíclicas.

Capítulo 1

La variedad de las álgebras de Post de orden r, k-cíclicas

Introducimos en la primera sección de este capítulo algunos conceptos conocidos de álgebra universal necesarios para el desarrollo de los capítulos siguientes.

En la segunda sección damos la definición de álgebra de Post de orden r dada por G. Epstein en 1960 y la dada por T. Traczyk en 1963, presentando diferentes propiedades que permiten demostrar la equivalencia de ambas definiciones. También mostramos que las álgebras de Post de orden r forman una variedad aritmética.

En la última sección de este capítulo definimos las álgebras de Post de orden r k-cíclicas y mostramos que son isomorfas a un producto subdirecto de álgebras simples.

1.1. Elementos de álgebra universal

En esta sección comenzamos introduciendo la definición de álgebra y algunos ejemplos de álgebras particulares. Damos la definición de homomorfismo y los teoremas de isomorfismos que se aplican a todo tipo de estructuras algebraicas, como así también las nociones de subálgebra, congruencia, producto directo y subdirecto, término, identidad y álgebra libre. Para finalizar mostramos cómo puede clasificarse una variedad a partir de las propiedades de sus miembros y caracterizamos las álgebras primales.

Más información sobre estos temas puede consultarse en [9], [30].

Dado un conjunto no vacío A y un entero positivo o nulo n definimos:
$A^0 = \emptyset$, y si $n > 0$,
$A^n = \{(a_1, \ldots, a_n) : a_i \in A\}$

Definición 1.1.1 *Una* **operación n-aria** *sobre A es una función $f : A^n \longrightarrow A$. Decimos que n es la* **aridad** *de f. Una operación* **0-aria** *se llama constante y es un elemento de A.*

Definición 1.1.2 *Un* **álgebra universal** *o simplemente un* **álgebra de tipo de similaridad** $\mathcal{F}$*, es un par* $(A, \mathcal{F})$ *donde* A *es un conjunto no vacío y* $\mathcal{F}$ *es una familia* $\{f_1, \ldots, f_{\mathcal{O}(\mathcal{F})}\}$ *tal que* f_i *es una operación* n_i*-aria sobre* A*, para cada* i*, con* $1 \leq i \leq \mathcal{O}(\mathcal{F})$*.*

Por simplicidad notaremos a un álgebra con A.

Es importante observar que $\mathcal{O}(\mathcal{F})$ no es necesariamante finito y puede ser vacío.

Ejemplos 1.1.1 *Veamos algunos ejemplos de álgebras.*

1. *Un* **grupo** *es un álgebra* $\langle G; *, ^{-1}, 1\rangle$ *de tipo* $(2, 1, 0)$ *que verifica los siguientes axiomas para* $x, y, z \in G$ *:*

   $(G1)$ $x * (y * z) = (x * y) * z$,

   $(G2)$ $x * 1 = 1 * x = x$,

   $(G3)$ $x * x^{-1} = x^{-1} * x = 1$.

   Un grupo G *es* **abeliano** *si satisface*

   $(G4)$ $x * y = y * x$.

   Es claro que esta no es la definición usual de grupo. Habitualmente se usa una operación binaria y axiomas que contienen cuantificadores.

2. *Un* **anillo** *es un álgebra* $\langle R; +, \cdot, -, 0\rangle$ *de tipo* $(2, 2, 1, 0)$ *que verifica las siguientes condiciones, cualquiera sean* $x, y, z \in R$*:*

   $(R1)$ $\langle R; +, -, 0\rangle$ *es un grupo abeliano,*

   $(R2)$ $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

   $(R3)$ $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $\qquad (y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

   Un **anillo conmutativo con unidad** *es un álgebra* $\langle R; +, \cdot, -, 0, 1\rangle$ *de tipo* $(2, 2, 1, 0, 0)$ *tal que* $\langle R; +, \cdot, -, 0\rangle$ *es un anillo y verifica las siguientes identidades, para todo* $x, y \in R$*:*

   $(R4)$ $x \cdot y = y \cdot x$,

   $(R5)$ $x \cdot 1 = x$.

3. *Un* **cuerpo** *es un álgebra* $\langle K; +, \cdot, -, 0, 1\rangle$ *de tipo* $(2, 2, 1, 0, 0)$ *tal que* $\langle K; +, \cdot, -, 0, 1\rangle$ *es un anillo conmutativo con unidad y "*$\cdot$*" verifica: cualquiera sea* $x \in K \setminus \{0\}$*, existe* $x^{-1} \in K$ *tal que* $x \cdot x^{-1} = 1$*.*

4. *Un* $K-$**espacio vectorial** *es un álgebra* $\langle M; +, -, \{f_k\}_{k\in K}, 0\rangle$ *de tipo* $(2, 1, \{1\}_{k\in K}, 0)$ *tal que* $\langle M; +, -, 0\rangle$ *es un grupo abeliano y las operaciones unarias* f_k *verifican:*

$(M1)$ $f_k(x+y) = f_k(x) + f_k(y)$, *cualquiera sea* $k \in K$,

$(M2)$ $f_{k+t}(x) = f_k(x) + f_t(x)$, *cualquiera sea* $k, t \in K$,

$(M3)$ $f_k(f_t(x)) = f_{kt}(x)$, *cualquiera sea* $k, t \in K$,

$(M4)$ $f_1(x) = x$.

5. *Un* **retículo distributivo** *es un álgebra* $\langle L; \wedge, \vee \rangle$ *de tipo* $(2,2)$ *tal que satisface las siguientes identidades para todos los elementos de* L*:*

$(L1)$ $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $\quad x \vee (y \vee z) = (x \vee y) \vee z$,

$(L2)$ $x \wedge y = y \wedge x$, $\quad x \vee y = y \vee x$,

$(L3)$ $x = x \wedge x$, $\quad x = x \vee x$,

$(L4)$ $x = x \wedge (x \vee y)$, $\quad x = x \vee (x \wedge y)$.

(D) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $\quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

6. *Un* **retículo distributivo acotado** *es un álgebra* $\langle L; \wedge, \vee, \mathbf{0}, \mathbf{1} \rangle$ *de tipo* $(2,2,0,0)$ *tal que* $\langle L; \wedge, \vee \rangle$ *es un retículo distributivo que satisface*

$x \wedge \mathbf{0} = \mathbf{0}$ *y*

$x \vee \mathbf{1} = \mathbf{1}$,

para todo $x \in L$.

7. *Un* **álgebra de Boole** *es un álgebra* $\langle B; \wedge, \vee, ', \mathbf{0}, \mathbf{1} \rangle$ *de tipo* $(2,2,1,0,0)$ *tal que* $\langle B; \wedge, \vee, 0, 1 \rangle$ *es un retículo distributivo acotado y* $'$ *satisface las siguientes identidades*

$a \vee a' = 1$;

$(a')' = a$;

$(a \vee b)' = a' \wedge b'$,

para todo a, $b \in B$.

8. *Un* **retículo modular** *es un retículo* $\langle L; \wedge, \vee \rangle$ *de tipo* $(2,2)$ *tal que* $\langle L; \wedge, \vee \rangle$ *es un retículo que satisface la ley modular*

(M) *Si* $x \leq y$ *entonces* $x \vee (y \wedge z) = y \wedge (x \vee z)$*paratodox, y,* $z \in L$.

El concepto de homomorfismo en teoría de grupos, anillos o retículos es un caso particular del de homomorfismo entre álgebras. La definición es la siguiente:

Definición 1.1.3 *Sean* A *y* B *dos álgebras del mismo tipo* $\mathcal{F}$*. Una aplicación* $\alpha : A \longrightarrow B$ *se dice un* **homomorfismo** *de* A *en* B *si:*

$$\alpha(f^A(a_1, \ldots, a_n)) = f^B(\alpha(a_1), \ldots, \alpha(a_n))$$

para cada operación n-aria en $\mathcal{F}$ y cada n-upla $(a_1, \ldots, a_n)$ de A^n.

Si la aplicación α es sobreyectiva decimos que B es una **imagen homomórfica** *de A y que α es un* **epimorfismo**. *Si α es inyectiva y sobreyectiva decimos que α es un* **isomorfismo.**

Si $A = B$, α recibe el nombre de **endomorfismo** *y de* **automorfismo** *si la aplicación α es biyectiva.*

Si A y B son dos álgebras del mismo tipo de similaridad, decimos que A y B son **similares**.

Definición 1.1.4 *Dada un álgebra A de tipo $\mathcal{F}$ y S un subconjunto no vacío de A, decimos que $(S, \mathcal{F})$ es una* **subálgebra** *de $(A, \mathcal{F})$ si S es cerrado para todas las operaciones de $\mathcal{F}$, i.e. si dada $f \in \mathcal{F}$ una operación n-aria, para todo $(x_1, \ldots, x_n) \in S^n$ resulta $f(x_1, \ldots, x_n) \in S$.*

Las subálgebras de A son similares a A. Además si f es una operación 0-aria, i.e. si f es una constante $a \in A$ entonces la restricción de f a una subálgebra S también toma el valor a. En consecuencia todas las constantes pertenecen a la subálgebra S.

Resulta de las definiciones anteriores que si $\alpha : A \longrightarrow B$ es un homomorfismo entonces $\alpha(A)$ es una subálgebra de B.

En lo que sigue estudiaremos el reticulado de congruencias de un álgebra A.

Definición 1.1.5 *Sea $(A, \mathcal{F})$ un álgebra. Una* **congruencia** *sobre A es una relación de equivalencia θ sobre A, que satisface la siguiente propiedad de compatibilidad:*

si f es una operación n-aria y a_i, b_i son elementos de A tal que $a_i \theta b_i$ se verifica para $1 \leq i \leq n$, entonces

$$f^A(a_1, \ldots, a_n) \theta f^A(b_1, \ldots, b_n).$$

De esta manera podemos introducir una estructura algebraica en el conjunto cociente A/θ en la forma conocida.

Definición 1.1.6 *El conjunto de todas las congruencias sobre un álgebra A se nota $Con(A)$. Si θ es una congruencia sobre A entonces el* **álgebra cociente** *de A por θ notada A/θ es el álgebra que satisface:*

$$f^{A/\theta}(|a_1|, \ldots, |a_n|) = |f^A(a_1, \ldots, a_n)|,$$

donde $a_1, \ldots, a_n \in A$, $|a_i|$ es la clase del elemento a_i determinada por θ y f es una operación n-aria en $\mathcal{F}$.

Las álgebras cocientes de A son del mismo tipo de similaridad que A.

Ejemplos 1.1.2 *Veamos los siguientes ejemplos de congruencias:*

1. *En un grupo G existe la siguiente conexión entre las congruencias de G y los subgrupos normales de G:*

   Si $\theta \in Con(G)$ entonces $|1|_\theta \lhd G$ y $(a,b) \in \theta$ si y sólo si $a * b^{-1} \in |1|_\theta$.

   Si $N \lhd G$ entonces $\theta = \{(a,b)/a * b^{-1} \in N\}$ es una congruencia sobre G tal que $|1|_\theta = N$.

   Luego existe una biyección entre $Con(G)$ y los subgrupos normales de G que preserva el orden tal que $\theta \longrightarrow |1|_\theta$.

2. *Dado un anillo R se tiene la siguiente relación:*

   Si $\theta \in Con(R)$ entonces $|0|_\theta$ es un ideal bilátero y $(a,b) \in \theta$ si y sólo si $a - b \in |0|_\theta$.

   Si I es un ideal bilátero de R entonces $\theta = \{(a,b)\}/a-b \in I\}$ es una congruencia sobre R tal que $|0|_\theta = I$.

   Luego la aplicación $\theta \longrightarrow |0|_\theta$ es una biyección que preserva el orden entre $Con(R)$ y el conjunto de ideales biláteros de R.

   Las congruencias anteriores pueden inducir a pensar que cualquier congruencia sobre un álgebra puede quedar determinada por una de sus clases, pero esto no es válido en general.

3. *Consideremos una cadena L pensada como retículo.*

   Si θ es una partición de L en subconjuntos convexos, (i.e. $a\theta b$ y $a \leq c \leq b \Rightarrow a\theta c$) es una congruencia.

   En este caso ninguna clase de equivalencia determina la congruencia.

El reticulado $Con(A)$ verifica el siguiente teorema:

Teorema 1.1.1 *$(Con(A), \subseteq)$ es un subreticulado completo de $(Eq(A), \subseteq)$.*

Definición 1.1.7 *Se dice que un álgebra A posee la* **propiedad de distributividad de congruencias** *si $Con(A)$ es un retículo distributivo, y que posee la propiedad de* **congruencias modulares** *si $Con(A)$ es* **modular.**
Si $\theta_1, \theta_2 \in Con(A)$ y $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ decimos que θ_1 y θ_2 **permutan**.
Decimos que A satisface la propiedad de **congruencias permutables** *si todo par de congruencias sobre A permuta.*

Una clase $\mathcal{K}$ de álgebras satisface la **propiedad de distributividad de congruencias** si y sólo si cada álgebra de $\mathcal{K}$ posee dicha propiedad. Análogamente decimos que una clase $\mathcal{K}$ posee las propiedades de **congruencias modulares** o **congruencias permutables**.

Una clase $\mathcal{K}$ de álgebras se dice **aritmética** si $\mathcal{K}$ tiene la propiedad de distributividad de congruencias y congruencias permutables.

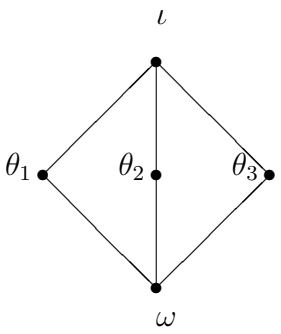
Teorema 1.1.2 *Sea A un álgebra y $\theta_1, \theta_2 \in Con(A)$. Las siguientes condiciones son equivalentes:*
a) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$,
b) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$,
c) $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$

Teorema 1.1.3 (Birkhoff) *Si A satisface la propiedad de* **congruencias permutables** *entonces satisface la propiedad de* **congruencias modulares**.

Definición 1.1.8 *Dada un álgebra A y $a_1, \ldots, a_n \in A$ notamos por $\Theta(a_1, \ldots, a_n)$ la* **congruencia generada** *por $\{(a_i, a_j) : 1 \leq i, j \leq n\}$, i.e. la menor congruencia tal que $a_1, \ldots, a_n$ están en la misma clase.*
La congruencia $\Theta(a_1, a_2)$ se llama **congruencia principal**. *Si $X \subseteq A$, $\Theta(X)$ es la congruencia generada por $X \times X$.*

Ejemplos 1.1.3 *Veamos algunos ejemplos de $Con(A)$ para un álgebra A dada.*

1. *Sea $G = Z_2 \times Z_2$. Las congruencias de G son:*
   ω: para cada $(a, b) \in Z_2 \times Z_2$ entonces $|(a, b)| = \{(a, b)\}$.
   Si θ_1 está determinada por el subgrupo normal $N = \{(0, 0); (1, 0)\}$ resulta $|(0, 0)| = N, \quad |(0, 1)| = \{(0, 1), (1, 1)\}$.
   Si θ_2 está determinada por el subgrupo normal $N = \{(0, 0); (0, 1)\}$ resulta $|(0, 0)| = N, \quad |(0, 1)| = \{(1, 0), (1, 1)\}$.
   Si θ_3 está determinada por el subgrupo normal $N = \{(0, 0); (1, 1)\}$ resulta $|(0, 0)| = N, \quad |(0, 1)| = \{(0, 1), (1, 0)\}$.
   ι: tenemos una sóla clase $|(0, 0)| = \{(0, 0); (1, 0); (0, 1); (1, 1)\}$.
   El retículo de las congruencias $Con(G)$ es:



$Con(G)$ no es distributivo

2. *Todo grupo y todo anillo verifica la propiedad de* **congruencias permutables**.

3. *Todo retículo verifica la propiedad de* **distributividad de congruencias**.

4. *Si L es la cadena con 5 elementos, $Con(L)$ no verifica la propiedad de* **congruencias permutables**.

Los teoremas de homomorfismo para retículos, grupos, anillos o módulos son casos particulares de los teoremas de homomorfismo de un álgebra en general.

Definición 1.1.9 *Sea $\alpha : A \longrightarrow B$ un homomorfismo. Llamamos* **kernel de** *α y notamos $Ker(\alpha)$ al conjunto*

$$Ker(\alpha) = \{(a, b) \in A^2 : \alpha(a) = \alpha(b)\}$$

El kernel de un homomorfismo $\alpha : A \longrightarrow B$ es una congruencia sobre A.

Dada un álgebra A y una congruencia θ sobre A, la **aplicación canónica** $\nu_\theta : A \longrightarrow A/\theta$ con $\nu_\theta(a) = |a|$ es un homomorfismo sobreyectivo.

Teorema 1.1.4 (Primer teorema de isomorfismo) *Sea $\alpha : A \longrightarrow B$ un homomorfismo sobreyectivo. Entonces existe un isomorfismo $\beta : A/Ker(\alpha) \longrightarrow B$ tal que $\alpha = \beta \circ \nu$ donde ν es el homomorfismo canónico de A en $A/Ker(\alpha)$.*

Del teorema resulta que un álgebra es una imagen homomórfica de un álgebra A si y sólo si es isomorfa a un álgebra cociente de A. Esto nos dice que el problema de encontrar **imágenes homomórficas** se reduce al de buscar **congruencias** sobre A.

Antes de dar el segundo teorema de isomorfismo veamos la definición y el lema siguientes:

Definición 1.1.10 *Sea A un álgebra y $\phi, \theta \in Con(A)$ con $\theta \subseteq \phi$. Definimos*

$$\phi/\theta = \{\ (|a|_\theta, |b|_\theta) \in (A/\theta)^2 : (a, b) \in \phi\}$$

Lema 1.1.1 *Si $\phi, \theta \in Con(A)$ y $\theta \subseteq \phi$ entonces ϕ/θ es una congruencia sobre A/θ.*

Teorema 1.1.5 (Segundo teorema de isomorfismo). *Si $\phi, \theta \in Con(A)$ y $\theta \subseteq \phi$ entonces la aplicación*

$$\alpha : (A/\theta)/(\phi/\theta) \longrightarrow A/\phi$$

definida por

$$\alpha(|a|_{\phi/\theta}) = |a|_\phi$$

es un isomorfismo de $(A/\theta)/(\phi/\theta)$ en A/ϕ.

Sea $B \subseteq A$ y θ una congruencia sobre A. Consideremos la subálgebra de A, B^θ generada por el conjunto $\{a \in A : B \cap |a|_\theta \neq \emptyset\}$ y $\theta|_B = \theta \cap B^2$ la restricción de θ a B. Entonces se verifican el lema y teorema siguientes:

Lema 1.1.2 *Si B es una subálgebra de A y $\theta \in Con(A)$ entonces $\theta|_B$ es una congruencia sobre B.*

Teorema 1.1.6 (Tercer teorema de isomorfismo). *Si B es una subálgebra de A y $\theta \in Con(A)$ entonces $B/\theta|_B \cong B^\theta/\theta|_{B^\theta}$.*

Una forma de crear nuevas álgebras es tomar el producto directo de ellas. La definición es la siguiente:

Definición 1.1.11 *Sean $(A, \mathcal{F})$ y $(B, \mathcal{F})$ dos álgebras similares. Definimos el* **producto directo de A y B** *notado por $(A \times B, \mathcal{F})$ como el conjunto de pares $A \times B$ donde cada operación n-aria f de $\mathcal{F}$ se define sobre el producto de la siguiente manera:*

$$f : (A \times B)^n \longrightarrow A \times B \text{ donde}$$

$$f((a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)) = (f(a_1, \ldots, a_n), f(b_1, \ldots, b_n))$$

para $a_i \in A, b_i \in B$ y $1 \leq i \leq n$.

Observemos que en general A_1 y A_2 no pueden sumergirse en $A_1 \times A_2$ excepto en casos especiales como los grupos, donde siempre existen álgebras triviales. Sin embargo A_1 y A_2 son imágenes homomórficas de $A_1 \times A_2$ como puede verse a partir de la definición y teorema siguientes.

Definición 1.1.12 *La aplicación*

$$\pi_i : A_1 \times A_2 \longrightarrow A_i, \ i \in \{1, 2\} \ definida \ por$$

$$\pi_i(a_1, a_2) = a_i$$

se llama **aplicación proyección sobre la i-ésima coordenada.**

Teorema 1.1.7 *Para cada $i = 1, 2$, la aplicación $\pi_i : A_1 \times A_2 \longrightarrow A_i$ es sobreyectiva. Además en $Con(A_1 \times A_2)$ se tiene:*

$$Ker(\pi_1) \cap Ker(\pi_2) = \omega,$$

$$Ker(\pi_1) \circ Ker(\pi_2) = Ker(\pi_2) \circ Ker(\pi_1) \ y$$

$$Ker(\pi_1) \vee Ker(\pi_2) = \iota.$$

donde $\omega = \{(a, a) : a \in A_1 \times A_2\}$ y $\iota = \{(a, b) : a, b \in A_1 \times A_2\} = (A_1 \times A_2)^2$

El teorema anterior motiva la siguiente definición:

Definición 1.1.13 *Decimos que una congruencia θ sobre A es una* **congruencia factor** *si existe una congruencia θ^* sobre A tal que*

$$\theta \wedge \theta^* = \omega,$$

$$\theta \text{ permuta con } \theta^* \text{ y}$$

$$\theta \vee \theta^* = \iota.$$

El par (θ, θ^*) se llama **par de congruencias factor** *sobre A.*

Teorema 1.1.8 *Si θ y θ^* son un par de congruencias factor sobre A, entonces la aplicación*

$$\alpha : A \longrightarrow A/\theta \times A/\theta^*$$

definida por

$$\alpha(a) = (|a|_\theta, |a|_{\theta^*})$$

es un isomorfismo.

Definición 1.1.14 *Un álgebra A se dice* **directamente indescomponible** *si A no es isomorfa al producto directo de dos álgebras no triviales.*

Ejemplos 1.1.4 *Z_p con p, primo es un álgebra directamente indescomponible.*
Las cadenas con r elementos L_r es directamente indescomponible.

Corolario 1.1.1 *Un álgebra A es directamente indescomponible si y sólo si las únicas congruencias factores son ω y ι.*

La generalización del producto directo de álgebras la da la siguiente definición:

Definición 1.1.15 *Sea $\{A_i\}_{i\in I}$ una familia de álgebras de tipo $\mathcal{F}$. El* **producto directo** *$A = \Pi_{i\in I} A_i$ es el álgebra que verifica lo siguiente:*
si $f \in \mathcal{F}$ y $a_1, \ldots, a_n \in \Pi_{i\in I} A_i$, entonces

$$f^A(a_1, \ldots, a_n)(i) = f^{A_i}(a_1(i), \ldots, a_n(i)) \text{ para } i \in I.$$

En forma análoga al producto directo de dos álgebras se tienen los homomorfismos epiyectivos

$$\pi_j : \Pi_{i\in I} A_i \longrightarrow A_j \; definido \; para \; cada \; j \in J \; por$$

$$\pi_j(a) = a(j).$$

Si $I = \{1, 2, \ldots, n\}$ escribimos $A_1 \times \ldots \times A_n$.

Para álgebras finitas tenemos el siguiente teorema:

Teorema 1.1.9 *Toda álgebra finita es isomorfa al producto directo de álgebras directamente indescomponibles.*

Definición 1.1.16 *Dadas las aplicaciones:*
a) $\alpha_i : A \longrightarrow A_i, i \in I$ *definimos la* **aplicación natural**

$$\alpha : A \longrightarrow \Pi_{i\in I} A_i \text{ dada por } (\alpha a)(i) = \alpha_i(a), \quad y$$

b) $\alpha_i : A_i \longrightarrow B_i, i \in I$ *definimos la* **aplicación natural**

$$\alpha : \Pi_{i\in I} A_i \longrightarrow \Pi_{i\in I} B_i \; definida \text{ por } (\alpha a)(i) = \alpha_i(a(i)).$$

Si las aplicaciones α_i *son homomorfismos entonces la aplicación* α *es un homomorfismo.*

Lema 1.1.3 *Dada una familia de aplicaciones* $\alpha_i : A \longrightarrow A_i$ *las siguientes condiciones son equivalentes:*
a) α *es inyectiva*
b) $\bigcap_{i\in I} Ker(\alpha_i) = \omega$.

Teorema 1.1.10 *Dada la familia de homomorfismos* $\alpha_i : A \longrightarrow A_i, i \in I$ *el homomorfismo* $\alpha : A \longrightarrow \Pi_{i\in I} A_i$ *es una inmersión si y sólo si* $\bigcap_{i\in I} Ker(\alpha_i) = \omega$.

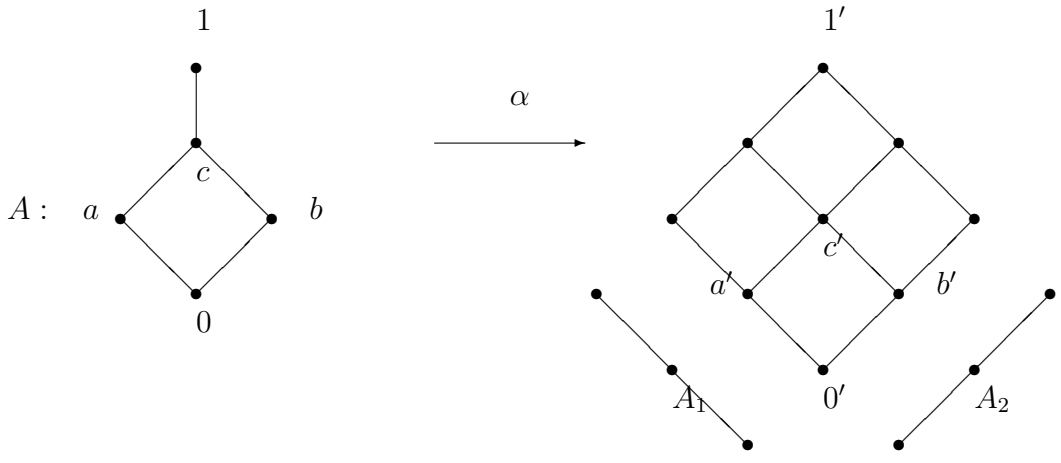
En general un álgebra infinita no es isomorfa al producto directo de álgebras directamente indescomponibles. Esto llevó a Birkhoff a estudiar las álgebras subdirectamente irreducibles en el campo del álgebra universal.

Definición 1.1.17 *Un álgebra* A *se dice* **producto subdirecto** *de una familia* $\{A_i\}_{i\in I}$ *de álgebras similares no triviales si existe una inmersión* $\alpha : A \longrightarrow \Pi_{i\in I} A_i$ *de tal manera que para cada* $i \in I, p_i \circ \alpha$ *es sobre.*

Definición 1.1.18 *Un álgebra* A *se dice* **subdirectamente irreducible** *si:*
i) A *tiene más de un elemento,*
ii) si A *es producto subdirecto de* $\{A_i\}_{i\in I}$ *con inmersión* α*, entonces* $p_i \circ \alpha$ *es un isomorfismo para algún* $i \in I$.

Veamos el siguiente ejemplo.

Ejemplo 1.1.1 *Si* A *es el reticulado distributivo*



A es isomorfa a una subálgebra de $A_1 \times A_2$. Las aplicaciones $p_1 \circ \alpha$ y $p_2 \circ \alpha$ son sobreyectivas.

Proposición 1.1.1 *Sea $\alpha : A \longrightarrow \Pi_{i\in I} A_i$ una aplicación. Entonces α es un homomorfismo si y sólo si $p_i \circ \alpha$ es un homomorfismo para todo i. Además $Ker(\alpha) = \bigcap_{i\in I} Ker(p_i \circ \alpha)$.*

Corolario 1.1.2 *La aplicación $\alpha : A \longrightarrow \Pi_{i\in I} A_i$ es un homomorfismo inyectivo si y sólo si $p_i \circ \alpha$ es un homomorfismo y $\bigcap_{i\in I} Ker(p_i \circ \alpha) = \omega$.*

Si A es producto subdirecto de $\{A_i\}_{i\in I}$ con inmersión α, entonces
$A_i \cong A/Ker(p_i \circ \alpha)$.

El teorema que sigue nos da una caracterización muy útil de las álgebras subdirectamente irreducibles.

Teorema 1.1.11 *Un álgebra A es subdirectamente irreducible si y sólo si existe una congruencia θ_0 tal que $\theta_0 \neq \omega$ y $\theta_0 \leq \theta$ para todo $\theta \in Con(A)$.*

Si A es subdirectamente irreducible el retículo $\mathbf{Con}(A)$ tiene el siguiente aspecto,

Ejemplos 1.1.5 *Veamos algunos ejemplos de álgebras subdirectamente irreducibles.*
1) Un grupo abeliano finito G es **subdirectamente irreducible** *si y sólo si es cíclico y $|G| = p^n$ para algún primo p, $n \in N$.*
2) Todo grupo simple es subdirectamente irreducible
3) En los reticulados distributivos la cadena de dos elementos es subdirectamente irreducible (simple) pero la de tres elementos no lo es.

Teorema 1.1.12 *Toda álgebra subdirectamente irreducible es directamente indescomponible.*

Teorema 1.1.13 (Birkhoff) *Toda álgebra A es isomorfa a un producto subdirecto de álgebras subdirectamente irreducibles (que son imágenes homomórficas de A).*

Corolario 1.1.3 *Toda álgebra finita es isomorfa a un producto subdirecto de un número finito de álgebras subdirectamente irreducibles finitas.*

La definición que sigue extiende el concepto de grupo o anillo simple al de un álgebra arbitraria.

Definición 1.1.19 *Un álgebra A se dice simple si $Con(A) = \{\omega, i\}$.*

Vamos a introducir los siguientes operadores entre clases de álgebras. Sea $\mathcal{K}$ una clase de álgebras similares. Indicaremos

$A \in \mathbf{S}(\mathcal{K})$ si y sólo si A es isomorfa a una subálgebra de algún miembro de $\mathcal{K}$.

$A \in \mathbf{S}_{fin}(\mathcal{K})$ si y sólo si A es isomorfa a una subálgebra finita de algún miembro de $\mathcal{K}$.

$A \in \mathbf{H}(\mathcal{K})$ si y sólo si A es isomorfa a una imagen homomórfica de algún álgebra de $\mathcal{K}$.

$A \in \mathbf{P}(\mathcal{K})$ si y sólo si A es isomorfa a un producto directo de una familia no vacía de álgebras de $\mathcal{K}$.

$A \in \mathbf{I}(\mathcal{K})$ si y sólo si A es isomorfa a un álgebra de $\mathcal{K}$.

Si $\mathcal{K} = \{A\}$, escribiremos $\mathbf{S}(A)$, $\mathbf{S}_{fin}(A)$, $\mathbf{H}(A)$ y $\mathbf{P}(A)$.

Si $\mathbf{O}_1$ y $\mathbf{O}_2$ son dos operadores entre clases de álgebras, notaremos $\mathbf{O}_1\mathbf{O}_2$ a la composición entre estos dos operadores. Diremos que una clase $\mathcal{K}$ de álgebras es **cerrada bajo un operador O** si $\mathbf{O}(\mathcal{K}) \subseteq \mathcal{K}$.

Lema 1.1.4 *Las siguientes desigualdades son válidas:*

$$\mathbf{SH} \leq \mathbf{HS}, \mathbf{PS} \leq \mathbf{SP} \text{ y } \mathbf{PH} \leq \mathbf{HP}.$$

Además los operadores $\mathbf{H}$, $\mathbf{S}$ *e* $\mathbf{IP}$ *son idempotentes.*

En Álgebra Universal interesa estudiar las clases de álgebras del mismo tipo de similaridad que son cerradas bajo uno o más operadores.

Definición 1.1.20 *Una clase $\mathcal{V}$ de álgebras similares forman una* **variedad** *si es cerrada bajo imágenes homomórficas, subálgebras y productos directos, es decir, si $\mathcal{V}$ es una clase de álgebras similares, entonces*

$$\mathcal{V} \text{ es una variedad si y sólo si } \mathbf{H}(\mathcal{V}) = \mathbf{S}(\mathcal{V}) = \mathbf{P}(\mathcal{V}) = \mathcal{V}.$$

Si $\mathcal{V}$ está formada por una sóla álgebra con un sólo elemento, entonces llamaremos a $\mathcal{V}$, **variedad trivial**. Si $\mathcal{V}$ y $\mathcal{V}'$ son variedades tales que todo miembro de $\mathcal{V}'$ pertenece a $\mathcal{V}$, entonces diremos que $\mathcal{V}'$ es una **subvariedad** de $\mathcal{V}$.

Como la intersección de variedades es una variedad, podemos decir que para toda clase $\mathcal{K}$ de álgebras similares existe la menor variedad que contiene a $\mathcal{K}$ y la notaremos con $\mathcal{V}(\mathcal{K})$. Diremos que $\mathcal{V}(\mathcal{K})$ es la **variedad generada por** $\mathcal{K}$.

Uno de los primeros resultados importantes en el estudio general de variedades se debe a A. Tarski quien determinó la variedad generada por una clase de álgebras similares.

Teorema 1.1.14 (A. Tarski) *Sea $\mathcal{K}$ una clase de álgebras similares. La menor variedad que contiene a $\mathcal{K}$, es decir, $\mathcal{V}(\mathcal{K})$ es* $\mathbf{HSP}(\mathcal{K})$.

A continuación presentamos la definición de álgebra libre.

Definición 1.1.21 *Decimos que un álgebra F es* **libre** *con respecto a una clase $\mathcal{K}$ de álgebras, si existe un conjunto $X \subseteq F$ tal que:*
1) X genera F,
2) para toda álgebra A de $\mathcal{K}$ y para toda aplicación $g : X \longrightarrow A$ existe un homomorfismo $f : F \longrightarrow A$ tal que $f(x) = g(x)$ para todo $x \in X$.
El conjunto X se llama **conjunto de generadores libres** *de F.*

Ejemplo 1.1.2 *Una base X de un espacio vectorial $\mathbf{V}$ sobre un cuerpo K es un conjunto de generadores libres de $\mathbf{V}$.*

Observemos que en la definición de álgebra libre no se pide que $F \in \mathcal{K}$, solamente que F tenga la misma similaridad que las álgebras de $\mathcal{K}$.

Veremos que siempre existe un álgebra libre con respecto a una clase $\mathcal{K}$ y cuándo ésta pertenece a $\mathcal{K}$.

Lema 1.1.5 *La aplicación f de la definición es única.*

El teorema que sigue nos dice que dado un cardinal λ, existe a menos de isomorfismo, a lo sumo un álgebra libre en una clase $\mathcal{K}$ sobre un conjunto de generadores libres de cardinal λ.

Teorema 1.1.15 *Sean F y F' dos álgebras libres en una clase $\mathcal{K}$ con conjuntos de generadores X e Y respectivamente. Si $|X| = |Y|$ entonces $F \cong F'$.*

Veamos cómo se construye el álgebra libre de una clase $\mathcal{K}$ de álgebras.

Definición 1.1.22 *Dado un conjunto X de objetos llamados* **variables** *y $\mathcal{F}$ un tipo de similaridad, el conjunto $T(X)$ de* **términos** *de tipo $\mathcal{F}$ sobre X es el menor conjunto que verifica:*
$X \cup \mathcal{F}_0 \subseteq T(X)$.
Si $t_1, t_2, \ldots, t_k \in T(X)$ y f es una operación $r-$aria entonces $f(t_1, t_2, \ldots, t_k) \in T(X)$.

Es importante observar que si bien X puede ser infinito, cada término depende sólo de un número finito de variables.
Si $t \in T(X)$ escribimos $t(x_1, \ldots, x_n)$ para indicar que algunas de las variables $x_1, x_2, \ldots, x_n$ aparecen en t.

Ejemplos 1.1.6 *Son ejemplos de términos:*
1) Si $X = \{x, y, z\}$ y "$*$" es una operación entonces $x, y, z,\ x * y,\ y * z,\ (x * y) * z$ son términos sobre X.
2) El anillo de polinomios $R[X]$ consiste en los términos de tipo $\mathcal{F} = \{+, \cdot, -, r\}$ donde $r \in R$ es una función 0-aria.

Dado un término t de tipo $\mathcal{F}$ sobre algún conjunto X y dada un álgebra A de tipo $\mathcal{F}$, definimos una aplicación $t^A : A^n \longrightarrow A$ como sigue:
1) Si t es una variable x_i entonces

$$t^A(a_1, \ldots, a_n) = a_i$$

2) Si t es de la forma $f(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n))$ donde f es una operación $k-$aria entonces

$$t^A(a_1, \ldots, a_n) = (f(t_1, \ldots, t_k))^A(a_1, \ldots, a_n) = f(t_1^A(a_1, \ldots, a_n), \ldots, t_k^A(a_1, \ldots, a_n)).$$

El conjunto $T(X)$ puede transformarse de manera natural en un álgebra.

Definición 1.1.23 *Dados $\mathcal{F}$ y X, el conjunto $T(X)$ tiene una estructura algebraica del mismo tipo de similaridad $\mathcal{F}$:*
Si f es una función k-aria y $t_1, t_2, \ldots, t_k$ son términos definimos:

$$f^{T(X)}(t_1, t_2, \ldots, t_k) = f(t_1, \ldots, t_k).$$

Ejemplo 1.1.3 *Si $t_1(x, y) = x \wedge (y \vee x)$, $t_2(x, y) = x \vee y$ y $f = \wedge$, entonces $f^{T(X)}(t_1, t_2) = [x \wedge (y \vee x)] \wedge (x \vee y)$.*

Se observa claramente que $T(X)$ está generado por X.

Teorema 1.1.16 *$T(X)$ es libre para cualquier clase de álgebras $\mathcal{K}$ de tipo $\mathcal{F}$.*

Definición 1.1.24 *Sea $\mathcal{K}$ una clase de álgebras de tipo $\mathcal{F}$. Dado un conjunto X de variables, definimos la congruencia*

$$\theta_{\mathcal{K}}(X) = \cap\{\phi/\phi \text{ es una congruencia sobre } T(X) : T(X)/\phi \in \mathbf{IS}(\mathcal{K})\}.$$

Notamos $F_{\mathcal{K}}(\bar{X}) = T(X)/\theta_{\mathcal{K}}(X)$, $\bar{X} = X/\theta_{\mathcal{K}}(X)$. Si $x \in X$, escribimos $\bar{x} = x/\theta_{\mathcal{K}}(X)$ y $\nu : T(X) \longrightarrow F_{\mathcal{K}}(\bar{X})$ el homomorfismo natural.

Teorema 1.1.17 (Birkhoff) *$F_{\mathcal{K}}(\bar{X})$ es libre con respecto a la clase $\mathcal{K}$, y tiene como conjunto de generadores libres a $\bar{X}$.*

En general $F_{\mathcal{K}}(\bar{X})$ no es isomorfa a un miembro de $\mathcal{K}$ pero puede sumergirse en un producto de miembros de $\mathcal{K}$.

Teorema 1.1.18 (Birkhoff) *Supongamos que $T(X)$ existe, i.e. $X \neq \emptyset$ o $\mathcal{F} \neq \emptyset$. Entonces $F_{\mathcal{K}}(\bar{X}) \in \mathbf{ISP}(\mathcal{K})$. Luego si $\mathcal{K}$ es cerrada bajo $\mathbf{I}, \mathbf{S}$ y $\mathbf{P}$, en particular, si $\mathcal{K}$ es una variedad, $F_{\mathcal{K}}(\bar{X}) \in \mathcal{K}$.*

Si $\mathcal{K}$ es una variedad, siempre existe un álgebra libre para cualquier cardinal positivo y pertenece a $\mathcal{K}$.

Decimos que una **identidad** del tipo $p(x_1, x_2, \ldots, x_n) = q(x_1, x_2, \ldots, x_n)$ se satisface en un álgebra dada A si para cualquier elección de elementos $a_1, a_2, \ldots, a_n \in A$ se tiene $p(a_1, a_2, \ldots, a_n) = q(a_1, a_2, \ldots, a_n)$.

Si $\mathcal{K}$ es una clase de álgebras que satisface un conjunto Σ de ecuaciones, como las identidades se preservan bajo imágenes homomórficas, subálgebras y productos directos, la variedad $\mathcal{V}(\mathcal{K})$ satisface Σ.

Uno de los resultados más importantes de G. Birkhoff dice que una clase de álgebras definida por identidades es exactamente aquella clase de álgebras que es cerrada bajo los operadores $\mathbf{H}, \mathbf{S}$ y $\mathbf{P}$. Es por eso que muchas veces se denomina **clase ecuacional** a una variedad.

Una **base ecuacional** para una variedad $\mathcal{V}$ es una colección Σ de identidades tal que $\mathcal{V}$ es la clase de álgebras que satisfacen todas las identidades de Σ. Observemos que la clase de álgebras formadas por los retículos distributivos acotados, las álgebras de Boole, los grupos abelianos, los anillos conmutativos con unidad y los $K-$espacios vectoriales tiene una base ecuacional.

En lo que sigue daremos una caracterización de las álgebras primales.

Definición 1.1.25 *Sea A un álgebra y $f : A^n \longrightarrow A$ una operación $n-$aria definida sobre A. Se dice que f es* **representable por un término** *si existe un término t en el lenguaje del álgebra A tal que para todo $a_1, a_2, \ldots, a_n \in A$ se tiene:*

$$f(a_1, a_2, \ldots, a_n) = t(a_1, a_2, \ldots, a_n).$$

Definición 1.1.26 *Sea A un álgebra finita. A es un álgebra* **primal** *si toda operación $n-$aria definida sobre A, para todo $n \geq 1$ puede ser representada por un término.*

Definición 1.1.27 *Sea A un conjunto. La función $s : A^4 \longrightarrow A$ definida por*

$$s(a, b, c, d) = \begin{cases} c & si\ a = b \\ d & si\ a \neq b \end{cases}$$

se denomina una **función switching** *de A. Si un término $s(x, y, u, v)$ representa una función switching sobre un álgebra A entonces a s se lo llama* **término switching**.

Definición 1.1.28 *La* **función discriminador** *sobre un conjunto A es una función $t : A^3 \longrightarrow A$ definida por:*

$$t(a, b, c) = \begin{cases} c & si\ a = b \\ a & si\ a \neq b \end{cases}.$$

Un término $t(x, y, z)$ que representa una función discriminador sobre un álgebra A se denomina **término discriminador** *en A.*

Proposición 1.1.2

1. *Un álgebra A tiene un término discriminador si y sólo si A tiene un término switching.*
2. *Un álgebra A con un término discriminador es simple.*

Definición 1.1.29 *Si $\mathcal{K}$ es una clase de álgebras con un término discriminador $t(x, y, z)$ común entonces $\mathcal{V}(\mathcal{K})$ se llama* **variedad con discriminador**.

Por ejemplo si A es un álgebra primal entonces $\mathcal{V}(A)$ es una variedad con discriminador.

Los siguientes resultados *caracterizan* las álgebras primales y resultan importantes para las próximas secciones [9].

Teorema 1.1.19 *Si existe un término discriminador $t(x, y, z)$ para toda álgebra de $\mathcal{K}$, entonces $\mathcal{V}(\mathcal{K})$ es una variedad aritmética.*

Teorema 1.1.20 *Las siguientes condiciones son equivalentes:*

1. *A es un álgebra primal.*
2. *$\mathcal{V}(A)$ es aritmética y A es simple, sin subálgebras propias y con un único automorfismo, que es la aplicación identidad.*

1.2. Álgebras de Post de orden r

En esta sección comenzamos dando la definición de álgebra de Post de orden r dada por T.Traczyck y la dada por G. Epstein que es equivalente a la anterior. También presentamos la noción de álgebra de Moisil r-valuada con centro introducida por Cignoli y demostramos que es equivalente a la de álgebra de Post de orden r, lo que nos permite afirmar que estas álgebras forman una variedad. Al final de esta sección mostramos que la variedad de las álgebras de Post de orden r es una variedad aritmética.

Notamos con $\mathcal{D}_{0,1}$ a la clase de los retículos distributivos con primer y último elemento y con $B(L)$ al conjunto de todos los elementos booleanos de un retículo L. Al complemento booleano de $b \in B(L)$, lo notamos con b'.

Definición 1.2.1 (T. Traczyk) *Sea $r \in \mathbb{N}$, $r \geq 2$. Un* **álgebra de Post de orden** r *es un álgebra $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1}, \{e_i\}_{i=1}^{r-2} \rangle$ de tipo $(2, 2, 0, 0, \{0\}_{i=1}^{r-2})$, tal que $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1} \rangle$ es un retículo distributivo con $\mathbf{0}$ y $\mathbf{1}$, que verifica:*

$(T1)$ $\mathbf{0} = e_0 \leq e_1 \leq e_2 \leq \ldots \leq e_{r-2} \leq e_{r-1} = \mathbf{1}$ *y*

$(T2)$ *cualquiera sea $x \in A$, puede expresarse de una única manera como:*

$$x = (b_1 \wedge e_1) \vee (b_2 \wedge e_2) \vee \ldots \vee (b_{r-1} \wedge e_{r-1}),$$

donde $b_i \in B(L)$, $1 \leq i \leq n-1$ y $b_1 \geq b_2 \geq \ldots \geq b_{r-1}$.

El conjunto de elementos e_i, $1 \leq i \leq n-1$ se denomina **cadena ascendente de constantes** y la representación del elemento x dada en $(T2)$ se llama **representación monótona de** x.

G. Epstein da en [15], la siguiente definición:

Definición 1.2.2 (G. Epstein) *Un álgebra de Post de orden r, $r \geq 2$, es un álgebra $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1}, \sim, \{C_i\}_{i=0}^{r-1}, \{e_i\}_{i=1}^{r-2} \rangle$, tal que $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1} \rangle$ es un retículo distributivo con $\mathbf{0}$ y $\mathbf{1}$, $\sim$ y C_i son operaciones unarias, y las e_i operaciones 0-arias que satisfacen:*
(P1) $\sim\sim x = x$,
(P2) $\sim (x \wedge y) = \sim x \vee \sim y$, $\sim (x \vee y) = \sim x \wedge \sim y$,
(P3) $C_i(x) \wedge C_j(x) = 0$ *para* $i \neq j$, *y* $\bigvee_{i=0}^{r-1} C_i(x) = \mathbf{1}$,
(P4) $\mathbf{0} = e_0 \leq e_1 \leq \ldots \leq e_{r-1} = \mathbf{1}$,
(P5) *si* $x \wedge e_1 = 0$ *entonces* $x = 0$,
(P6) *si* $x \vee e_{i-1} = e_i$ *entonces* $x = e_i$,
(P7) *para cada* $x \in A$, $x = \bigvee_{i=0}^{r-1} C_i(x) \wedge e_i$.

Las propiedades y teoremas que damos a continuación son válidas para un álgebra de Post L de orden r:

Proposición 1.2.1 *Sea L un álgebra de Post de orden r:*

1. *Si $x \in L$ y $x \wedge e_i = \mathbf{0}$ para algún i, $1 \leq i \leq r-1$ entonces $x = \mathbf{0}$.*
2. *Dado $x \in L$, si existen $i, j \in \{0, \ldots, r-1\}$ tales que $i < j$ y $x \vee e_i = e_j$ entonces $x = e_j$.*
3. *Dado $b \in B(L)$, si existen $i, j \in \{0, \ldots, r-1\}$ tales que $i < j$ y $b \wedge e_i = b \wedge e_j$ entonces $b = \mathbf{0}$.*

Teorema 1.2.1 *Se L un álgebra de Post de orden r y $x \in L$. Entonces $x \in B(L)$ si y sólo si existe $y \in L$ tal que $x = C_i(y)$ para algún i.*

Demostración: Supongamos que existe $y \in L$ tal que $x = C_i(y)$ para algún i. Por la condición $(P3)$ resulta que $x' = \bigvee_{j=0, i \neq j}^{r-1} C_j(y)$. Luego $x \in B(L)$.
Recíprocamente, supongamos que $x \in B(L)$. Por $(P7)$ se tiene $x \leq e_{r-2} \vee C_{r-1}(x)$ y por lo tanto $e_{r-2} \vee C_{r-1}(x) \vee x' = \mathbf{1} = e_{r-1}$. Además por la proposición anterior $x' \vee C_{r-1}(x) = \mathbf{1}$, de donde resulta $x \leq C_{r-1}(x)$.
Como por $(P7)$, $C_{r-1}(x) \leq x$, entonces $x = C_{r-1}(x)$. □

El teorema que sigue nos muestra que los $C_i(x)$ son únicos, en el siguiente sentido: para cada $x \in A$ existe una única sucesión de elementos $C_0(x), C_1(x), \ldots, C_{r-1}(x)$ que satisfacen (P3) y (P7).

Teorema 1.2.2 *Sea L un álgebra de Post de orden r. La sucesión de elementos $C_0(x), C_1(x), \ldots, C_{r-1}(x)$ que satisfacen $(P3)$ y $(P7)$ es única para cada $x \in L$.*

Demostración: Supongamos que dado $x \in L$, existe otra suceción
$\tilde{C}_0(x),\ \tilde{C}_1(x),\ \ldots,\ \tilde{C}_{r-1}(x)$ que verifica $(P3)$ y $(P7)$. Luego se tiene que
$\bigvee_{k=0}^{r-1}(C_k(x) \wedge e_k) = \bigvee_{k=0}^{r-1}(\tilde{C}_k(x) \wedge e_k)$.
Si $i \neq j$,

$$C_i(x) \wedge \tilde{C}_j(x) \wedge (\bigvee_{k=0}^{r-1}(C_k(x) \wedge e_k)) = C_i(x) \wedge \tilde{C}_j(x) \wedge (\bigvee_{k=0}^{r-1}(\tilde{C}_k(x) \wedge e_k)).$$

Por $(P3)$ resulta $C_i(x) \wedge \tilde{C}_j(x) \wedge e_i = C_i(x) \wedge \tilde{C}_j(x) \wedge e_j$, y como $C_i(x) \wedge \tilde{C}_j(x) \in B(L)$, por el teorema anterior $C_i(x) \wedge \tilde{C}_j(x) = \mathbf{0}$.
Luego, de esta última condición resulta que para cada j,

$$\tilde{C}_j(x) = \tilde{C}_j(x) \wedge \bigvee_{k=0}^{r-1} C_k(x) = \tilde{C}_j(x) \wedge C_j(x).$$

De manera análoga se demuestra que $C_j(x) = C_j(x) \wedge \tilde{C}_j(x)$, de donde resulta

$$C_j(x) = \tilde{C}_j(x).$$

□

Los teoremas que siguen serán útiles en los algoritmos programados en Maple que se dan en el Apéndice de esta tesis.

Teorema 1.2.3 *Para cada* $i,\ 1 \leq i \leq r-1$ *se tiene*

$$\begin{aligned} C_{r-1}(C_i(x)) &= C_i(x), \\ C_j(C_i(x)) &= \mathbf{0} \quad \textit{para}\ \ 0 < j < r-1 \quad \textit{y} \\ C_0(C_i(x)) &= \bigvee_{k=1,k\neq i}^{r-1} C_k(x) = (C_i(x))'. \end{aligned}$$

Demostración: Para cada i, los r elementos del conjunto

$$\{ \bigvee_{k=1,k\neq i}^{r-1} C_k(x),\ \underbrace{\mathbf{0},\ \mathbf{0},\ \ldots,\ \mathbf{0}}_{r-2},\ C_i(x)\}$$

son disjuntos dos a dos y el supremo de todos los elementos del conjunto anterior es $\mathbf{1}$, por lo que se cumple $(P3)$.
Además

$$C_i(x) = \big((\bigvee_{k=1,k\neq i}^{r-1} C_k(x)) \wedge e_0\big) \vee (\mathbf{0} \wedge e_1) \vee \ldots \vee (\mathbf{0} \wedge e_{r-2}) \vee (C_i(x) \wedge e_{r-1}),$$

y por la unicidad de la descomposición de los elementos de L se verifica que

$$\begin{aligned} C_0(C_i(x)) &= \bigvee_{k=0,k\neq i}^{r-1} C_k(x) = (C_i(x))', \\ C_j(C_i(x)) &= \mathbf{0} \quad \text{para}\ \ 0 < j < r-1 \quad \text{y} \\ C_{r-1}(C_i(x)) &= C_i(x). \end{aligned}$$

□

Observemos que si $b \in B(L)$, para todo $i,\ 1 < i < r-1$ resulta que
$C_0(b) = b', C_{r-1}(b) = b$ y $C_i(b) = \mathbf{0}$.

Teorema 1.2.4 *Si* $i \neq j$ *entonces* $C_i(e_j) = \mathbf{0}$ *y* $C_i(e_i) = \mathbf{1}$*. Además los elementos* e_i*, para* $i = 1, 2, \ldots, n-1$ *son únicos y todos distintos entre sí.*

Demostración: Del teorema 1.2.1 resulta inmediatamente que si $i \neq j$, $C_i(e_j) = \mathbf{0}$ y $C_i(e_i) = \mathbf{1}$. Además para $i \neq j$ y $e_i = e_j$ resulta $C_i(e_j) = C_i(e_i) = \mathbf{1}$ lo que contradice $(P3)$, luego los e_i son distintos dos a dos.
Supongamos que existe otra sucesión de elementos

$$\mathbf{0} = \tilde{e}_0,\ \tilde{e}_1,\ \ldots,\ \tilde{e}_{r-2},\ \tilde{e}_{r-1} = \mathbf{1}$$

que verifican $(P3)$ y $(P7)$. Entonces para cada $x \in L$ resulta:

$$x = \bigvee_{k=0}^{r-1} (C_k(x) \wedge \tilde{e}_k).$$

Tomando $x = e_i$, para todo $i,\ 1 \leq i \leq r-2$ se tiene $e_i = \tilde{e}_i$, y por lo tanto los elementos e_i son únicos. □

Teorema 1.2.5 *Si $b_i \in B(L)$ y $x = \bigvee_{i=1}^{r-1}(b_i \wedge e_i)$ entonces*

$$x = \bigvee_{i=1}^{r-1} ((\bigvee_{j=i}^{r-1} b_j) \wedge e_i),$$

$$C_0(x) = \bigwedge_{j=1}^{r-1} b'_j, \qquad C_{r-1}(x) = b_{r-1} \quad y$$

$$C_i(x) = b_i \wedge \big(\bigwedge_{j=i+1}^{r-1} b'_j \big), \quad \textit{para todo } i,\ 1 \leq i \leq r-2.$$

Demostración: Si $x = \bigvee_{j=1}^{r-1}(b_j \wedge e_j)$ entonces

$$x = \bigvee_{j=1}^{r-1} (b_j \wedge (\bigvee_{i=1}^{j} e_i) = \bigvee_{i=1}^{r-1} ((\bigvee_{j=i}^{r-1} b_j) \wedge e_i).$$

Para todo $k = 1, 2, \ldots, r-2$, se verifica que:

$$\bigvee_{i=k}^{r-2} (b_i \wedge (\bigwedge_{j=i+1}^{r-1} b'_j)) \vee b_{r-1} = \bigvee_{i=k}^{r-1} b_i \ .$$

A los efectos de simplificar la notación, escribiendo

$$a_{r-1} = b_{r-1} \quad \text{y} \quad a_i = b_i \wedge (\bigwedge_{j=i+1}^{r-1} b'_j), \quad \text{para todo } i = 1, 2, \ldots, r-2, \text{ se tiene que}$$

$$x = \bigvee_{i=1}^{r-1} ((\bigvee_{j=i}^{r-1} b_j) \wedge e_i) = \bigvee_{i=1}^{r-1} ((\bigvee_{j=i}^{r-1} a_j) \wedge e_i) = \bigvee_{j=1}^{r-1} ((\bigvee_{i=1}^{j} e_i) \wedge a_j) = \bigvee_{j=1}^{r-1} (e_j \wedge a_j).$$

De esta manera los elementos $\bigwedge_{i=1}^{r-1} b_i'$, a_1, $\ldots$, a_{r-1} son distintos dos a dos y el supremo de todos es $\mathbf{1}$. Por el teorema 1.2.1 resulta

$$C_0(x) = \bigwedge_{i=1}^{r-1} b_i' \quad \text{y} \quad C_i(x) = a_i \quad \text{para todo } i = 1, 2, \ldots, r-2.$$

□

Definiendo $D_i(x) = \bigwedge_{j=i}^{r-1} C_j(x)$ para todo $i = 1, 2, \ldots, r-2$, resulta que $D_i(x) \in B(L)$ y $D_i(x) \geq D_j(x)$ para todo $x \in L$ y para i, j tales que $1 \leq i \leq j \leq r-1$. Luego por $(P7)$ y el teorema anterior,

$$x = \bigvee_{i=1}^{r-1} (D_i(x) \wedge e_i).$$

Los elementos $D_i(x)$ son únicos y verifican el siguiente:

Teorema 1.2.6 *Dados $x, y \in L$, para cada i, $1 \leq i \leq r-1$ se verifica:*

(a) $D_i(x \vee y) = D_i(x) \vee D_i(y)$.

(b) $x \leq y$ *si y sólo si* $D_i(x) \leq D_i(y)$.

Demostración:

(a) Como $D_i(x) \geq D_j(x)$ y $D_i(y) \geq D_j(y)$ para todo i, j tal que $1 \leq i \leq j \leq r-1$, resulta

$$D_i(x) \vee D_i(y) \geq D_j(x) \geq D_j(y).$$

Además como

$$x \vee y = \bigvee_{i=1}^{r-1} (D_i(x) \wedge e_i) \vee \bigvee_{i=1}^{r-1} (D_i(y) \wedge e_i) = \bigvee_{i=1}^{r-1} ((D_i(x) \vee D_i(y)) \wedge e_i),$$

entonces $D_i(x \vee y) = D_i(x) \vee D_i(y)$ por la unicidad de la representación de $x \vee y$.

(b) Si $x \leq y$ entonces $x \vee y = y$ y $D_i(x) \vee D_i(y) = D_i(x \vee y) = D_i(y)$, es decir, $D_i(x) \leq D_i(y)$.

Recíprocamente, supongamos que $D_i(x) \leq D_i(y)$ para todo i, $1 \leq i \leq r-1$, luego

$$x = \bigvee_{i=1}^{r-1} (D_i(x) \wedge e_i) \leq \bigvee_{i=1}^{r-1} (D_i(y) \wedge e_i) = y.$$

□

A partir de la definición de los D_i y del teorema anterior se obtiene el siguiente:

Teorema 1.2.7 *El retículo L es dualmente isomorfo a si mismo mismo bajo la aplicación $\beta : L \longrightarrow L$ dada por:*

$$\beta(x) = \bigvee_{i=1}^{r-1}((D_{r-i}(x))' \wedge e_i).$$

Además si L^* es el retículo dual de L y C_i^*, e_i^* son operadores unarios y elementos de L^* que verifican $(P3) - (P7)$ en L^*, y D_i^* es el operador definido en 1.2.3 sobre L^* entonces se verifican:

1. $e_i^* = e_{r-i-1}$,
2. $C_i^*(x) = (C_{r-i-1}(x))' \quad y$
3. $D_i^*(x) = D_{r-i}(x)$.

Demostración: Dados i, j tales que $1 \leq i \leq j \leq r-1$ vimos que $(D_{r-i}(x))' \geq (D_{r-j}(x))'$ y como $\beta(x) = \bigvee_{i=1}^{r-1}((D_{r-i}(x))' \wedge e_i)$ se tiene

$$D_i(\beta(x)) = (D_{r-i}(x))'.$$

Luego

$$\beta(\beta(x)) = \bigvee_{i=1}^{r-1}((D_{r-i}(\beta(x)))' \wedge e_i) = \bigvee_{i=1}^{r-1}(D_i(x) \wedge e_i) = x.$$

Por el teorema 1.2.6 y la igualdad anterior resulta que, $x \leq y$ si y sólo si $D_{r-i}(x) \leq D_{r-i}(y)$ lo que es equivalente a $D_i(\beta(y)) \leq D_i(\beta(x))$ y en consecuencia $\beta(y) \leq \beta(x)$. Luego el retículo dual L^* es isomorfo a L y L^* es un retículo distributivo que verifica las condiciones $(P3)$ a $(P7)$.
Como $(D_{r-i}(x))' = \bigvee_{j=o}^{r-i-1} C_j(x)$ y

$$\beta(x) = \bigvee_{i=1}^{r-1}(\bigvee_{j=0}^{r-i-1} C_j(x) \wedge e_i) = \bigvee_{j=0}^{r-2}(C_j(x) \wedge \bigvee_{i=0}^{r-j-1} e_i) = \bigvee_{j=0}^{r-2}(C_j(x) \wedge e_{r-j-1}),$$

tomando $i = r - j - 1$ obtenemos

$$\beta(x) = \bigvee_{i=1}^{r-1}(C_{r-i-1}(x) \wedge e_i) \quad (1)$$

y por el Teorema 1.2.4 resulta $e_i^* = \beta(e_i) = e_{r-i-1}$.

Por el Teorema 1.2.2 $C_i(\beta(x)) = C_{r-i-1}(x)$.
Además, si $b \in B(L)$, $C_i(\beta(b)) = C_{r-i-1}(b) = \mathbf{0}$, para todo i, $1 \leq i \leq r-2$ y $C_{r-1}(\beta(b)) = C_0(b) = b'$. Entonces $\beta(b) = b'$. Por el isomorfismo β tenemos que $\beta(C_i(x)) = C_i^*(\beta(x))$, de donde

$$C_i^*(x) = C_i^*(\beta(\beta(x))) = \beta(C_i(\beta(x))) = (C_i(\beta(x)))' = (C_{r-i-1}(x))'$$

y

$$D_i^*(x) = D_i^*(\beta(\beta(x))) = \beta(D_i(\beta(x))) = (D_i(\beta(x)))' = D_{r-i}(x).$$

Por otra parte como $\beta(x \vee y) = \beta(x) \wedge \beta(y)$ y $\beta(x \wedge y) = \beta(x) \vee \beta(y)$ entonces

$$\begin{aligned} x &= \beta(\beta(x)) = \beta(\textstyle\bigvee_{i=1}^{r-1}(C_{r-i-1}(x) \wedge e_i)) = \\ &= \textstyle\bigwedge_{i=1}^{r-1}(\beta(C_{r-i-1}(x)) \vee \beta(e_i)) = \bigwedge_{i=1}^{r-1}((C_{r-i-1}(x))' \vee e_{r-i-1}). \end{aligned}$$

Luego podemos obtener una fórmula dual a la dada en $(P7)$,

$$x = \bigwedge_{i=0}^{r-2}((C_i(x))' \vee e_i),$$

donde $((C_0(x))' \leq ((C_1(x))' \leq \ldots \leq ((C_{r-2}(x))'$. □

Teorema 1.2.8 *Para cada $i = 1, 2, \ldots, r-1$ y para cada $x \in L$, $y \in L$ se verifica que $D_i(x \wedge y) = D_i(x) \wedge D_i(y)$.*

Demostración: Por a) del teorema 1.2.6, para cada $i = 1, 2, \ldots, r-1$ resulta $D_{r-i}(\beta(x) \vee \beta(y))) = D_{r-i}(\beta(x)) \vee D_{r-i}(\beta(y)))$. Luego $D_{r-i}(\beta(x \wedge y)) = D_{r-i}(\beta(x) \vee D_{r-i}(\beta(y)))$ y por el teorema 1.2.7 se tiene que $D_i(x \wedge y) = D_i(x) \wedge D_i(y)$. □

Teorema 1.2.9 *Las siguientes identidades se verifican para cada $i = 1, 2, \ldots r-1$.*

$$(a) \quad C_i(x \vee y) = (C_i(x) \wedge \bigvee_{j=0}^{i} C_j(y)) \vee (C_i(y) \wedge \bigvee_{j=0}^{i} C_j(x)).$$

$$(b) \quad C_i(x \wedge y) = (C_i(x) \wedge \bigvee_{j=i}^{r-1} C_j(y)) \vee (C_i(y) \wedge \bigvee_{j=i}^{r-1} C_j(x)).$$

Demostración: De los teoremas anteriores resulta

(a) $C_i(x \vee y) = D_i(x \vee y) \wedge (D_{i+1}(x \vee y))' = (D_i(x) \vee D_i(y)) \wedge (D_{i+1}(x))' \wedge (D_{i+1}(y))' =$

$$= (C_i(x) \wedge (D_{i+1}(y))') \vee (C_i(y) \wedge (D_{i+1}(x))') = (C_i(x) \wedge \bigvee_{j=0}^{i} C_j(y)) \vee (C_i(y) \wedge \bigvee_{j=0}^{i} C_j(x)).$$

Análogamente,

(b) $C_i(x \wedge y) = D_i(x \wedge y) \wedge (D_{i+1}(x \wedge y))' = D_i(x) \wedge D_i(y) \wedge ((D_{i+1}(x))' \vee (D_{i+1}(y))') =$

$$= (C_i(x) \wedge D_i(y)) \vee (C_i(y) \wedge D_i(x)) = (C_i(x) \wedge \bigvee_{j=i}^{r-1} C_j(y)) \vee (C_i(y) \wedge \bigvee_{j=i}^{r-1} C_j(x)).$$

□

R. Cignoli introduce en [11] la variedad de las álgebras de Moisil r-valuadas con centro. Demostraremos más adelante que un álgebra L es un álgebra de Post de orden r si y sólo si L es un álgebra de Moisil r-valuada con centro.

Definición 1.2.3 *Un* **álgebra de De Morgan** *es un álgebra* $\langle A; \wedge, \vee, \sim, \mathbf{0}, \mathbf{1}, \rangle$ *de tipo* $(2, 2, 1, 0, 0,)$ *tal que* $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1} \rangle$ *es un retículo distributivo y se verifican los siguientes axiomas:*

$(M1)$ $\sim\sim x = x$,

$(M2)$ $\sim (x \vee y) = \sim x \wedge \sim y$.

Se deducen de la definición las siguientes propiedades:

$(M3)$ $x \leq y$ si y sólo si $\sim y \leq \sim x$.

$(M4)$ $\sim (x \wedge y) = \sim x \vee \sim y$.

$(M5)$ $\sim \mathbf{1} = \mathbf{0}$.

Definición 1.2.4 (R. Cignoli [11]) *Sea* $r \geq 2$. *Un* **álgebra de Moisil** $r-$**valuada con centro** *es un álgebra* $\langle A; \wedge, \vee, \sim, \{\varphi_i\}_{i=1}^{r-1}, \mathbf{0}, \mathbf{1}, \{c_i\}_{i=1}^{r-2} \rangle$ *de tipo* $(2, 2, 1, \{1\}_{i=1}^{r-1}, 0, 0, \{0\}_{i=1}^{r-2})$ *que verifica:*

$(C1)$ $\langle A; \wedge, \vee, \sim, \mathbf{0}, \mathbf{1} \rangle$ *es un álgebra de De Morgan,*

$(C2)$ $\varphi_i(x \wedge y) = \varphi_i(x) \wedge \varphi_i(y)$,

$(C3)$ $\varphi_i x \vee \sim \varphi_i x = \mathbf{1}$,

$(C4)$ $\varphi_i \varphi_j x = \varphi_j x$,

$(C5)$ $\varphi_i(\sim x) = \sim \varphi_{r-i} x$,

$(C6)$ $\varphi_1 x \leq \varphi_2 x \leq \ldots \leq \varphi_{r-2} x \leq \varphi_{r-1} x$,

$(C7)$ *Si* $\varphi_i x = \varphi_i y$ *para todo* i, $1 \leq i \leq r-1$, *entonces* $x = y$,

$(C8)$

$$\varphi_i c_j = \begin{cases} \mathbf{0} & si\ i + j < r \\ \mathbf{1} & si\ i + j \geq r \end{cases}.$$

La condición $(C7)$ recibe el nombre de **Principio de Determinación de Moisil**. En las álgebras de Moisil $r-$valuadas con centro se verifican las siguientes propiedades.

Proposición 1.2.2 *Dada un álgebra de Moisil $r-$valuada con centro $\langle A;\wedge,\vee,\sim,\{\varphi_i\}_{i=1}^{r-1},\mathbf{0},\mathbf{1},\{c_i\}_{i=1}^{r-2}\rangle$, se verifican:*

$(C9)$ $\varphi_i(x\wedge y)=\varphi_i(x)\wedge\varphi_i(y)$,

$(C10)$ $\varphi_i x\wedge\sim\varphi_i x=\mathbf{0}$,

$(C11)$ $x\leq y$ *si y sólo si* $\varphi_i x\leq\varphi_i y$, *para todo* $i,\ 1\leq i\leq r-1$,

$(C12)$ $x\leq\varphi_{r-1}x$,

$(C13)$ $\varphi_1 x\leq x$,

$(C14)$ $\varphi_i\mathbf{0}=\mathbf{0},\ \varphi_i\mathbf{1}=\mathbf{1}$, *para todo* $i,\ 1\leq i\leq r-1$,

$(C15)$ $\sim x\vee\varphi_{r-1}x=\mathbf{1}$,

$(C16)$ $x\wedge\sim\varphi_i x\wedge\varphi_{i+1}y\leq y,\ 1\leq i\leq r-2\quad y$

$(C17)$ *si* $1\leq k\leq r-2$ *entonces*

$$\bigvee_{i=1}^{k}((\sim\varphi_i y\vee y)\wedge(\varphi_{i+1}y\vee y))=\varphi_{k+1}y\vee y.$$

Las demostraciones de las proposiciones $(C12)$ y $(C16)$ se utilizarán en el Teorema 1.2.10. El resto de las propiedades pueden probarse fácilmente.

Demostración: Para demostrar que $x\leq\varphi_{r-1}x$, veamos que $\varphi_i(x\vee\varphi_{r-1}x)=\varphi_i(\varphi_{r-1}x)$ para $i,\ 1\leq i\leq r-1$. Dado $i\in\{1,2,\ldots,r-1\}$ se tiene que,

$$\varphi_i(x\vee\varphi_{r-1}x)=\varphi_i x\vee\varphi_i(\varphi_{r-1}x)=\varphi_i x\vee\varphi_{r-1}x=\varphi_{r-1}x=\varphi_i(\varphi_{r-1}x)$$

y por la condición $(C7)$ resulta $x\leq\varphi_{r-1}x$.
Para probar $(C16)$ consideremos la igualdad $z=x\wedge\sim\varphi_i x\wedge\varphi_{i+1}y$. Si j es tal que $1\leq j\leq i$ entonces $\varphi_j z\leq\varphi_j y$. En efecto:

$$\varphi_j z=\varphi_j x\wedge\varphi_j(\varphi_{r-i}\sim x)\wedge\varphi_j\varphi_{i+1}y\leq\varphi_j x\wedge\varphi_{r-i}\sim x=\varphi_j x\wedge\sim\varphi_i x\leq$$
$$\leq\varphi_i x\wedge\sim\varphi_i x=\mathbf{0}\leq\varphi_j y.$$

Si j es tal que $i+1\leq j\leq r-1$ entonces $\varphi_j z\leq\varphi_j\varphi_{i+1}y=\varphi_{i+1}y\leq\varphi_j y$.
Luego $\varphi_j z\leq\varphi_j y$, cualquiera sea $j,\ 1\leq j\leq r-1$ y por $(C7)$ resulta $z\leq y$. □

El teorema que sigue nos dice que las álgebras de Moisil $r-$valuadas con centro forman una variedad.

Teorema 1.2.10 *Un sistema* $\langle A;\wedge,\vee,\sim,\{\varphi_i\}_{i=1}^{r-1},\mathbf{0},\mathbf{1},\{c_i\}_{i=1}^{r-2}\rangle$ *es un álgebra de Moisil* $r-$*valuada con centro si y sólo si* $\langle A;\wedge,\vee,\sim,\mathbf{0},\mathbf{1}\rangle$ *es un álgebra de De Morgan, los* $\{\varphi_i\}_{i=1}^{r-1}$ *son operaciones unarias y los* $\{c_i\}_{i=1}^{r-2}$ *operaciones* $0-$*arias que verifican las propiedades* $(C2)-(C6),\ (C8),\ (C12)$ *y* $(C16)$.

Demostración: Sea $\langle A; \wedge, \vee, \sim, \mathbf{0}, \mathbf{1}\rangle$ un álgebra de De Morgan y $\{\varphi_i\}_{i=1}^{r-1}$ y $\{c_i\}_{i=1}^{r-2}$ operaciones que verifican las condiciones del teorema. Veamos que $\langle A; \wedge, \vee, \sim, \{\varphi_i\}_{i=1}^{r-1}, \mathbf{0}, \mathbf{1}, \{c_i\}_{i=1}^{r-2}\rangle$ es un álgebra de Moisil $r-$valuada con centro. Sólo debemos probar $(C7)$.
Sean $x, y \in A$ tales que $\varphi_i x = \varphi_i y$, para todo $i,\ 1 \leq i \leq r-1$. Reemplazando en $(C16)$ $\varphi_i x$ por $\varphi_i y$, para todo $i,\ 1 \leq i \leq r-3$ y $\varphi_{r-1} y$ por $\varphi_{r-1} x$ para $i = r-2$, obtenemos las siguientes igualdades:

(1) $y = (x \vee y) \wedge (\sim \varphi_i y \vee y) \wedge (\varphi_{i+1} y \vee y)$ para todo $i,\ 1 \leq i \leq r-3$ y

(2) $y = (x \vee y) \wedge (\sim \varphi_{r-2} y \vee y) \wedge (\varphi_{r-1} x \vee y)$.

De $(C12)$ y la identidad $\varphi_{r-2} x = \varphi_{r-2} y$, en (2) resulta:

$$(3) \quad y = (x \vee y) \wedge (\sim \varphi_{r-2} y \vee y).$$

De (1) y esta última igualdad obtenemos:

$$y = (x \vee y) \wedge (\bigvee_{i=1}^{r-3} ((\sim \varphi_i y \vee y) \wedge (\varphi_{i+1} y \vee y)) \vee (\sim \varphi_{r-2} y \vee y)).$$

Como $(C17)$ verifica las condiciones enunciadas tenemos que $y = x \vee y$, i.e. $x \leq y$. Razonando de manera análoga, obtenemos que $x \geq y$ y de aquí que $x = y$. □

El teorema anterior da una **caracterización ecuacional** de las álgebras de Mosil $r-$valuadas con centro ya que las álgebras de De Morgan están definidas por igualdades, así como también los axiomas $(C2) - (C5)$ y $(C8)$. Por otra parte los axiomas $(C5), (C12)$ y $(C16)$ pueden escribirse de la siguiente manera:

$(C5)$ $\varphi_i x \vee \varphi_{i+1} x = \varphi_{i+1} x$, para todo $i,\ 1 \leq i \leq r-2$.

$(C12)$ $x \vee \varphi_{r-1} x = \varphi_{r-1} x$.

$(C16)$ $(x \wedge \sim \varphi_i x \wedge \varphi_{i+1} y) \vee y = y$, para todo $i,\ 1 \leq i \leq r-2$.

De esta forma hemos probado que las álgebras de Moisil $r-$valuadas con centro forman una **variedad**.

A continuación veremos que las álgebras de Post de orden r son álgebras de Moisil $r-$valuadas con centro y recíprocamente.

Dada un álgebra de Post L de orden r, sabemos que cada elemento $x \in L$ puede representarse de una única manera en la siguiente forma:

$$x = (b_1 \wedge e_1) \vee (b_2 \wedge e_2) \vee \ldots \vee (b_{r-1} \wedge e_{r-1}),$$

donde $b_i \in B(L),\ 1 \leq i \leq r-1$ y $b_1 \geq b_2 \geq \ldots \geq b_{r-1}$

Vimos en el Teorema 1.2.7 que

$$\beta(x) = \bigvee_{i=1}^{r-1} (e_i \wedge (D_i(x))')$$

verifica $(M1)$ y $(M2)$. Definiendo $\sim x = \beta(x)$ se tiene que toda álgebra de Post de orden r es un álgebra de De Morgan.

Si definimos

$$\varphi_i x = D_{r-i}(x), \text{ para todo } i,\ 1 \leq i \leq r-1$$

se verifican $(C2) - (C7)$ y se cumple que:

$$\varphi_i e_j = D_{r-i}(e_j) = \begin{cases} \mathbf{0} & \text{si } i+j < r \\ \mathbf{1} & \text{si } i+j \geq r \end{cases} .$$

Dada un álgebra de Moisil A $r-$valuada con centro, tomando $e_i = c_i$, para $1 \leq i \leq r-2$, $e_0 = \mathbf{0}$ y $e_{r-1} = \mathbf{1}$, obtenemos a partir de de $(C8)$ y $(C11)$, $e_0 \leq e_1 \leq \ldots \leq e_{r-1}$.

Utilizando la condición $(C7)$ podemos escribir cualquier elemento x de A de una única manera, como sigue:

$$x = (\varphi_{r-1}x \wedge c_1) \vee (\varphi_{r-2}x \wedge c_2) \vee \ldots \vee (\varphi_2 x \wedge c_{r-2}) \vee (\varphi_1 x \wedge c_{r-1}).$$

Por último definiendo $b_i = \varphi_{r-i}(x)$, obtenemos:

$$x = (b_1 \wedge e_1) \vee (b_2 \wedge e_2) \vee \ldots \vee (b_{r-2} \wedge e_{r-2}) \vee (b_{r-1} \wedge e_{r-1}).$$

Los axiomas $(C3)$ y $(C10)$ nos aseguran que $b_i = \varphi_i(x) \in B(A)$, cualquiera sea $i,\ 1 \leq i \leq r-1$ y por $(C6)$, $b_1 \geq b_2 \geq \ldots \geq b_{r-1}$.

Hemos demostrado el siguiente teorema que nos asegura que las álgebras de Post de orden r forman una variedad.

Teorema 1.2.11 *L es un álgebra de Post de orden r si y sólo si L es un álgebra de Moisil $r-$valuada con centro.*

Ejemplos 1.2.1 *Veamos los siguientes ejemplos:*

1. *Toda álgebra de Boole es un álgebra de Post $2-$valuada.*

2. *La cadena con r elementos L_r es un álgebra de Post $r-$valuada donde $\mathbf{0}$ y $\mathbf{1}$ son el primer y último elemento de la cadena respectivamente, y e_i es el $(i+1)-$ésimo elemento.*

   También podemos ver a L_r como el conjunto de las fracciones $j/(r-1)$ con $j = 1, 2, \ldots, r-1$ donde

$$\sim (j/(r-1)) = 1 - j/(r-1) \quad y \quad C_i(j/(r-1)) = \begin{cases} \mathbf{0} & si\ i = j \\ \mathbf{1} & si\ i \neq j \end{cases}$$

3. *Sean* $\mathcal{B} = \langle B; \wedge, \vee, ', \mathbf{0}, \mathbf{1}, \rangle$ *un álgebra de Boole y* L_{r-1} *la cadena con* $r-1$ *elementos.*

   Consideremos el conjunto de todas las funciones crecientes de L_{r-1} *en* B

   $$B^{[\mathbf{r-1}]} = \{f : \mathbf{r-1} \longrightarrow B/ \ si\ i \leq j\ entonces\ f(i) \leq f(j)\ \}$$

   y el álgebra

   $$\mathcal{B}^{[\mathbf{r-1}]} = \langle B^{[\mathbf{r-1}]}; \wedge, \vee, \sim, \{\varphi_i\}_{i=1}^{r-1}, \mathbf{0}, \mathbf{1}, \{e_i\}_{i=1}^{r-2} \rangle,$$

   con las operaciones del retículo distributivo $\langle B^{[\mathbf{r-1}]}; \wedge, \vee, \mathbf{0}, \mathbf{1} \rangle$ *definidas coordenada a coordenada. Las demás operaciones se definen de la manera siguiente:*

   $(\sim f)(j) = (f(r-j))'$,

   $\varphi_i(f)(j) = f(i)$ *para todo* $i = 1, 2, \ldots, r-1$ *y todo* $j \in L_{r-1}$,

   y las constantes son las funciones

   $$e_i(j) = \begin{cases} \mathbf{0} & si\ i + j < r \\ \mathbf{1} & si\ i + j \geq r \end{cases} .$$

   Estas operaciones definen sobre $\mathcal{B}^{[\mathbf{r-1}]}$ *una estructura de álgebra de Post de orden* r*, tal que*

   $$\mathcal{B} \cong B(\mathcal{B}^{[\mathbf{r-1}]}) = \{f \in B^{[\mathbf{r-1}]} \ : f\ es\ constante\}.$$

Este ejemplo nos muestra que toda álgebra de Post L *de orden* r*, puede representarse como el conjunto de funciones crecientes de una cadena con* $r-1$ *elementos en el álgebra de Boole* $B(L)$ *mediante la aplicación*

$$F_L : L \longrightarrow (B(L))^{[\mathbf{r-1}]}\ tal\ que\ F_L(x)(i) = \varphi_i(x).$$

La aplicación F_L recientemente definida verifica el teorema siguiente:

Teorema 1.2.12 *F_L es un isomorfismo de álgebras de Post.*

A continuación mostraremos que las álgebras de Post de orden r son productos subdirectos de copias de L_r. Luego, veremos que el álgebra L_r es un álgebra primal y mostraremos un término discriminador sobre la cadena L_r.

Si θ es una **congruencia** sobre un álgebra de Post $r-$valuada L entonces θ es una congruencia de retículos distributivos que satisface la siguiente condición:

si $(x, y) \in \theta$ entonces $(\varphi_i(x), \varphi_i(y)) \in \theta$ y $(\sim x, \sim y) \in \theta$ para todo $x, y \in L$ y todo i tal que $1 \leq i \leq r-1$.

Proposición 1.2.3 *Sea θ una congruencia sobre un álgebra de Post $r-$valuada L. Si $(\varphi_i(x), \varphi_i(y)) \in \theta$ para todo $i,\ 1 \leq i \leq r-1$, entonces $(x, y) \in \theta$.*

Demostración: Como θ es una congruencia, resulta que $e_i \theta e_i$, cualquiera sea $i \in \{1, \ldots, r-1\}$. Además $\varphi_i(x) \theta \varphi_i(y)$ para todo $i = 1, 2, \ldots r-1$, entonces

$$\varphi_{r-i}(x) \wedge e_i \theta \varphi_{r-i}(y) \wedge e_i.$$

Luego

$$x = \bigvee_{i=1}^{r-1} (\varphi_{r-i}(x) \wedge e_i) \theta \bigvee_{i=1}^{r-1} (\varphi_{r-i}(y) \wedge e_i) = y,$$

de donde resulta $x \theta y$. □

Teorema 1.2.13 *Dada un álgebra de Post $r-$valuada L, los retículos $Con(L)$ y $Con(B(L))$ son isomorfos.*

Demostración: Veamos que la aplicación: $f : Con(L) \longrightarrow Con(B(L))$ definida por $f(\theta) = \theta \cap (B(L))^2$ es un isomorfismo de retículos. Probemos primero que f es un isomorfismo de orden, i.e. que si $\theta_1 \cap (B(L))^2 \subseteq \theta_2 \cap (B(L))^2$ entonces $\theta_1 \subseteq \theta_2$, ya que la implicación $\theta_1 \subseteq \theta_2 \Rightarrow \theta_1 \cap (B(L))^2 \subseteq \theta_2 \cap (B(L))^2$ se verifica trivialmente.
Supongamos que $\theta_1 \cap (B(L))^2 \subseteq \theta_2 \cap (B(L))^2$ para $\theta_1, \theta_2 \in Con(L)$. Si $x \theta_1 y$ con $x, y \in L$, entonces por la representación monótona de $x \in L$ resulta que $x \theta_2 y$.
Dada $\theta \in Con(B(L))$ definimos $\theta_0 \subseteq L^2$ como sigue:

$$x \theta_0 y \text{ si y sólo si } \varphi_i(x) \theta \varphi_i(y) \text{ para todo } i,\ 1 \leq i \leq r-1.$$

Veamos que $\theta_0 \in Con(L)$. Sean $x, y \in L$ tal que $x \theta_0 y$. Como $(\varphi_j(\varphi_i(x)), \varphi_j(\varphi_i(y))) = (\varphi_i(x), \varphi_i(y)) \in \theta$, para todo i, j tal que $1 \leq i, j \leq r-1$ entonces $(\varphi_i(x), \varphi_i(y)) \in \theta_0$, cualquiera sea $i = 1, 2, \ldots, r-1$.
Además $(\varphi_i(\sim x), \varphi_i(\sim y)) = (\sim \varphi_{r-i}(x), \sim \varphi_{r-i}(y)) \in \theta$, para todo $i,\ 1 \leq i \leq r-1$, de donde resulta $(\sim x, \sim y) \in \theta_0$. Luego $\theta_0 \in Con(L)$ y $\theta_0 \cap Con(B(L)) = \theta$. □

Teorema 1.2.14 *Sea L un álgebra de Post $r-$valuada. Entoces L es subdirectamente irreducible si y sólo si $L \cong L_r$. Más aún L_r es simple.*

Demostración: Por el teorema anterior L es subdirectamente irreducible si y sólo si $B(L) \cong \mathbf{L_2}$, luego del Teorema 1.2.12 resulta

$$L \cong B(L)^{[\mathbf{r-1}]} \cong L_2^{[\mathbf{r-1}]} \cong L_r$$

□

El teorema siguiente **caracteriza** las álgebras de Post $r-$valuadas y su demostración puede encontrarse en [8].

Teorema 1.2.15 *Las siguientes condiciones son equivalentes en un álgebra de Post $r-$valuada L,*

1. *L es producto directo de copias de L_r.*
2. *L es completa y atómica.*
3. *$B(L)$ es completa y atómica.*

Corolario 1.2.1 *Si L es un álgebra de Post $r-$valuada tal que $B(L) \cong L_2^m$ entonces $L \cong L_r^m$.*

Del corolario anterior resulta que si L es un álgebra de Post de orden r finita y m es el número de átomos del álgebra de Boole formada por los elementos complementados de L, entonces L tiene r^m elementos.

A continuación veremos que las álgebras de Post de orden r forman una variedad con discriminador. Para ello es suficiente probar que el álgebra de Post L_r es un álgebra primal.

La cadena L_r no tiene subálgebras propias y el único automorfismo es la aplicación identidad.

Dados $a, b \in L_r$ se tiene que

$$\bigwedge_{1\leq k\leq r} (a^{(k)} \vee b^{(k)}) = \mathbf{0} \quad \text{si y sólo si } a = b$$

y

$$\Big(\bigwedge_{1\leq j\leq r-1} a^{(j)}\Big)' = \begin{cases} \mathbf{0} & \text{si y sólo si } a = \mathbf{0} \\ \mathbf{1} & \text{si y sólo si } a \neq \mathbf{0}. \end{cases}$$

Llamando

$$g(a,b) = \Big[\bigwedge_{1\leq j\leq r-1} \Big(\bigwedge_{1\leq k\leq r} (a^{(k)} \vee b^{(k)})\Big)^{(j)}\Big]'$$

resulta que

$$g(a,b) = \begin{cases} \mathbf{0} & \text{si y sólo si } a = b \\ \mathbf{1} & \text{si y sólo si } a \neq b. \end{cases}$$

Definiendo

$$t(x,y,z) = [g(x,y) \wedge x] \vee [g(g(x,y),\mathbf{1}) \wedge z],$$

obtenemos un término discriminador t, ya que

$t(a,a,c) = g(\mathbf{0},\mathbf{1}) \wedge c = c.$

Si $a \neq b$ entonces $t(a,b,c) = [\mathbf{1} \wedge a] \vee [g(\mathbf{1},\mathbf{1}) \wedge c] = a.$

Como existe un término discriminador para toda álgebra L_r, entonces por el Teorema 1.1.19, $\mathcal{V}(L_r)$ es una variedad aritmética. Como además L_r es simple, sin subálgebras propias y con un único automorfismo, entonces por el Teorema 1.1.20, L_r es un álgebra primal.

1.3. Álgebras de Post de orden r, k-cíclicas

Vimos en la sección anterior que la variedad de las álgebras de Post de orden r es una variedad con discriminador que está generada por la cadena de r elementos.

Definición 1.3.1 *Un* **álgebra de Post $k-$cíclica de orden** r, ($r \geq 2$, $k \geq 1$, r, k *fijos*) *es un par* $\langle A; T\rangle$, *donde* A *es un álgebra de Post de orden* r *y* T *es un automorfismo del álgebra* A *tal que* $T^k(x) = x$ *para cada* $x \in A$.

Como la clase de las álgebras de Post de orden r es definible ecuacionalmente, la clase de las álgebras de Post $k-$cíclicas de orden r también lo es y en consecuencia forma una variedad.

El conjunto $(L_r)^k$ de las sucesiones $x = (x_1, x_2, \ldots, x_k)$, con $x_i \in L_r$, con las operaciones definidas componente a componente, también es un álgebra de Post de orden r.

Definiendo $T(x_1, x_2, \ldots, x_k) = (x_k, x_1, x_2, \ldots, x_{k-1})$ obtenemos un automorfismo de $(L_r)^k$ tal que $T^k(x) = x$ para cada $x \in (L_r)^k$.

Luego $\langle (L_r)^k; T\rangle$ es un álgebra de Post $k-$cíclica de orden r, que notamos $L_{r,k}$.

En lo que sigue describimos las congruencias de la variedad $\mathcal{V}(L_{r,k})$ y el álgebra cociente de un álgebra de Post k- cíclica.

Definición 1.3.2 *Dada un álgebra de Post de orden* r, $k-$*cíclica* L, *llamamos* $T-$**filtro** *de* L *a un subconjunto* $N \subseteq L$ *que verifica:*

$(N1)$ N *es un filtro de* L,

$(N2)$ *si* $x \in N$ *entonces* $\varphi_1(x) \in N$ *y*

$(N3)$ *si* $x \in N$ *entonces* $T(x) \in N$.

Decimos que N *es un* $T-$*filtro* **propio** *si* $N \neq L$.

Definición 1.3.3 *Sean* L *un álgebra de Post de orden* r, $k-$*cíclica y* N *un* $T-$*filtro de* L. *Para todo* $a, b \in L$ *decimos que* a *y* b *son* **congruentes módulo** N *y se nota* $a \equiv b(N)$ *si y sólo si existe* $u \in N$ *tal que* $a \wedge u = b \wedge u$.

La relación "$\equiv$" es una congruencia en L.

Si $L' = L/N$ es el álgebra cociente algebrizada en el sentido canónico, entonces L' es un álgebra de Post $k-$cíclica de orden r.

Notaremos con $\overline{x}$ a la clase de equivalencia de x módulo N. La aplicación

$h : L \longrightarrow L/N$ definida por $h(x) = \overline{x}$ es un epimorfismo que llamamos **epimorfismo canónico**.

Si U es un filtro maximal de $B(L)$ entonces los conjuntos

$$U_i = \{x \in L \ : \ \varphi_i x \in U\}$$

para $1 \leq i \leq r-1$ son filtros primos de L y verifican las siguientes propiedades:

- $U = U_i \cap B(L)$ para todo $i = 1, 2, \ldots, r-1$ y
- $U_1 \subset U_2 \subset \ldots \subset U_{r-1}$.

Además si P es un filtro primo de L y $P^* = P \cap B(L)$ entonces P^* es un filtro maximal de $B(L)$ y $P_1^* \subseteq P \subseteq P_{r-1}^*$.

Proposición 1.3.1 *Si $1 \leq i \leq r-1$ entonces $P \subseteq P_i^*$ o $P_{i+1}^* \subseteq P$.*

Demostración: Supongamos que $P \nsubseteq P_i^*$ y que $P_{i+1}^* \nsubseteq P$. Entonces existen $x, y \in L$ tales que

$$x \in P, \quad x \notin P_i^*, \quad y \in P_{i+1}^* \ \text{ e } \ y \notin P.$$

Si $x \notin P_i^*$ resulta $\varphi_i(x) \notin P^*$. Luego $\sim \varphi_i(x) \in P^*$ ya que P^* es un ultrafiltro de $B(L)$. Además como $P^* \subseteq P$ resulta que $\sim \varphi_i(x) \in P$.
Si $y \in P_{i+1}^*$ entonces $\varphi_{i+1}(y) \in P^*$ y como $P^* \subseteq P$ se tiene que $\varphi_{i+1}(y) \in P$.
Luego como $x \sim \varphi_i(x), \ \varphi_{i+1}(y) \in P$ entonces

$$x \wedge \sim \varphi_i(x) \wedge \varphi_{i+1}(y) \in P.$$

Como P es un filtro y $x \wedge \sim \varphi_i(x) \wedge \varphi_{i+1}(y) \leq y$ entonces $y \in P$ lo que contradice la suposición del comienzo. □

Teorema 1.3.1 *Si P es un filtro primo de L entonces existe un único ultrafiltro P^* de $B(L)$ y un índice i, $1 \leq i \leq r-1$ tal que $P = P_i^*$.*

Demostración: Sea $P^* = P \cap B(L)$. Como P^* es un filtro primo de $B(L)$ y $P_1^* \subseteq P \subseteq P_{r-1}^*$ entonces $\{i \ : \ P_i^* \subseteq P\}$ es un conjunto finito no vacío. Sea $i_0 = max\{i \ : \ P_i^* \subseteq P\}$. Si $i_0 = r-1$ entonces $P = P_{r-1}^*$.
Si $i_0 \leq r-2$ entonces $P_{i_0}^* \subseteq P$ y $P_{i_0+1}^* \nsubseteq P$ y por el lema anterior $P \subseteq P_{i_0+1}^*$, de donde resulta $P = P_{i_0+1}^*$.
Como $P^* = P_i^* \cap B(L)$ para todo i, $1 \leq i \leq r-1$ entonces P^* es único. □

Veamos a continuación una caracterización de los $T-$filtros maximales.

Teorema 1.3.2 *Si P es un filtro primo minimal de L entonces $T(P), T^2(P), \ldots, T^{k-1}(P)$ son filtros primos minimales de L.*

Teorema 1.3.3 *Si N es un $T-$filtro y P un filtro primo minimal de L tal que $N \subseteq P$ entonces $N \subseteq T(P)$.*

Teorema 1.3.4 *Si P es un filtro primo minimal entonces*

$$N = P \cap T(P) \cap T^2(P) \cap \ldots \cap T^{k-1}(P)$$

es un $T-$filtro maximal. Recíprocamente, si N es un $T-$filtro maximal entonces existe un filtro primo minimal P tal que

$$N = P \cap T(P) \cap T^2(P) \cap \ldots \cap T^{k-1}(P).$$

Demostración: Sea P es un filtro primo minimal de L. Si P es de período d entonces d es el menor entero positivo tal que $T^d(P) = P$ y d es un divisor de k. Además $N = P \cap T(P) \cap T^2(P) \cap \ldots \cap T^{k-1}(P)$ es un $T-$filtro maximal de período d.
Recíprocamente, si $N = P \cap T(P) \cap T^2(P) \cap \ldots \cap T^{k-1}(P)$ es un $T-$filtro maximal de período d, los $(n-1)d$ filtros primos

$$\begin{array}{ccccccc}
P = P_1^* & \subset & P_2^* & \subset & \ldots & \subset & P_{r-1}^* \\
T(P)_1^* & \subset & T(P)_2^* & \subset & \ldots & \subset & T(P)_{r-1}^* \\
\vdots & & \vdots & & \ldots & & \vdots \\
T^{d-1}(P)_1^* & \subset & T^{d-1}(P)_2^* & \subset & \ldots & \subset & T^{d-1}(P)_{r-1}^*
\end{array}$$

son disjuntos dos a dos y los únicos filtros primos que contienen a N.
Si notamos $P_0^* = \phi$ y $P_n^* = L$ entonces los conjuntos

$$\eta(j_1, j_2, \ldots, j_d) = (P_{j_1}^* - P_{j_1-1}^*) \cap (T(P)_{j_2}^* - T(P)_{j_2-1}^*) \cap \ldots \cap (T^{d-1}(P)_{j_d}^* - T^{d-1}(P)_{j_d-1}^*)$$

con $1 \leq j_i \leq r$, son clases módulo N y las operaciones inducidas por L/N están dadas por:

$$\begin{array}{l}
\eta(j_1, j_2, \ldots, j_d) \wedge \eta(i_1, i_2, \ldots, i_d) = \\
= \eta(max(j_1, i_1), max(j_2, i_2), \ldots, max(j_d, i_d)) - \eta(j_1, j_2, \ldots, j_d) = \\
= \eta(r - j_1 + 1, r - j_2 + 1, \ldots, r - j_d + 1).
\end{array}$$

Para $1 \leq i \leq r-1$, $\varphi_i \eta(j_1, j_2, \ldots, j_d) = \eta(t_1, t_2, \ldots, t_d)$ donde

$$t_h = \begin{cases} 1 & \text{si } i \geq j_h \\ r & \text{si } i < j_h \end{cases},$$

y $T(\eta(j_1, j_2, \ldots, j_{d-1}, j_d)) = \eta(j_d, j_1, j_2, \ldots, j_{d-1})$.

La aplicación $f : L/N \longrightarrow L_{r,d}$ definida por

$$f(\eta(j_1, j_2, \ldots, j_d)) = (\frac{r - j_1}{r-1},\ \frac{r - j_2}{r-1},\ \ldots,\ \frac{r - j_d}{r-1})$$

es un isomorfismo.
Luego el álgebra cociente L/N es isomorfa al álgebra $L_{r,d}$ donde d es un divisor de k y las álgebras simples son las álgebras $L_{r,d}$ con d es un divisor de k. □

Hemos demostrado el siguiente teorema:

Teorema 1.3.5 *Toda álgebra de Post $k-$cíclica de orden r es isomorfa a un producto subdirecto de álgebras simples.*

Si d es un divisor de k, el conjunto

$$D = \{x \in L_{r,k} \ :\ T^d(x) = x\},$$

es una subálgebra $d-$periódica del álgebra $L_{r,k}$ isomorfa al álgebra $L_{r,d}$ y los elementos de D tienen la forma:

$$x = (\underbrace{x_1, x_2, \ldots, x_d}_{1},\ \underbrace{x_1, x_2, \ldots, x_d}_{2},\ \ldots,\ \underbrace{x_1, x_2, \ldots, x_d}_{q})$$

donde $q = \dfrac{k}{d}$.

Además las únicas subálgebras de $L_{r,k}$, a menos de isomofismo, son las álgebras $L_{r,d}$ con d un divisor de k.

Teorema 1.3.6 *El retículo de las subálgebras de $L_{r,k}$ es isomorfo al retículo de los divisores de k.*

Demostración: Considerando la función que aplica a cada divisor d de k en el álgebra $L_{r,d}$, vemos que si d_1 y d_2 son divisores de k entonces $d_1 \wedge d_2$ es el máximo común divisor entre d_1 y d_2. Luego

$$L_{r,d_1} \cap L_{r,d_2} = L_{r,d_1 \wedge d_2}.$$

□

Capítulo 2

Extensiones de Galois

En este capítulo comenzamos presentando algunos resultados conocidos acerca de cuerpos finitos y extensiones de Galois [24],[21] y [36]. Estas extensiones, la unicidad de los cuerpos finitos, a menos de isomorfismo y el teorema de la base normal que demostramos en la última sección jugarán un importante papel en la equivalencia entre las variedades de álgebras de Post cíclicas y las variedades generadas por cuerpos finitos. Esta equivalencia, uno de los resultados más importantes de esta tesis, se demostrará en el próximo capítulo.

2.1. Extensiones de cuerpos. Clausura algebraica.

En esta sección comenzamos introduciendo las extensiones de cuerpos y caracterizamos las extensiones finitas. Definimos la clausura algebraica de una extensión E de un cuerpo K, construimos el cuerpo de raíces de un polinomio no constante $f \in K[X]$ y probamos que dos clausuras algebraicas de K son K-isomorfas.

Comencemos recordando algunas definiciones y teoremas básicos. Las definiciones de anillo y cuerpo fueron dadas en el primer capítulo.

Definición 2.1.1 *Decimos que un anillo R es un* **dominio de integridad**, *si R es un anillo conmutativo sin divisores de cero.*

Definición 2.1.2 *Sea R un anillo. Un conjunto no vacío $I \subset R$ se llama* **ideal** *de R si verifica:*
(I1) $0 \in I$
(I2) Para todo, $a, b \in I$, $a + b \in I$;
(I3) Para todo $a \in I$, $b \in R$, $a \cdot r \in I$.

Dado $r \in R$ definimos

$$r + I = \{r + a : a \in I\}$$
$$r \cdot I = \{r \cdot a : a \in I\}.$$

Esto nos permite dar la siguiente definición:

Definición 2.1.3 *Sea $r \in R$ e I un ideal de R. El* **anillo cociente** *R/I se define como el conjunto*

$$R/J = \{r + J : r \in R\},$$

con las operaciones siguientes:

$$(r_1 + J) + (r_2 + J) = (r_1 + r_2) + J,$$

$$(r_1 + J) \cdot (r_2 + J) = (r_1 \cdot r_2) + J.$$

El neutro de la suma es $0 + J$ y la unidad $1 + J$.

Definición 2.1.4 *Un ideal $I \subset R$ se dice un ideal* **primo** *si I es propio y verifica*

$$a \cdot b \in I \Rightarrow a \in I \text{ o } b \in I$$

Definición 2.1.5 *Un ideal $I \subset R$ se dice un ideal* **maximal** *si dado cualquier ideal $J \subseteq I$ verifica que*

$$\text{si } I \subseteq J \text{ entonces } J = I \text{ o } J = R.$$

Teorema 2.1.1 *Sea I un ideal de R. Entonces el anillo cociente R/I es un cuerpo si y sólo si I es un ideal maximal de R.*

En lo que sigue estudiaremos las extensiones de un cuerpo K.

Definición 2.1.6 *Decimos que un cuerpo E es una* **extensión** *de un cuerpo K si K es un subcuerpo de E. Notamos $K \subset E$.*

Si E es una extension de un cuerpo K entonces E puede considerarse como un espacio vectorial sobre K. Luego podemos definir el *grado* de una extensión E de K.

Definición 2.1.7 *Decimos que una extensión E de un cuerpo K es* **finita de grado** *n si el $K-$espacio vectorial E tiene dimensión n y notamos $[E : K] = n$. Si la extensión E del cuerpo K no es finita decimos que es* **infinita**.

Son ejemplos de extensiones de cuerpos, $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{C}$. La extensión $[\mathbb{C} : \mathbb{R}]$ es finita de grado 2 y el resto de las extensiones mencionadas son infinitas.

Otro ejemplo es la cadena de extensiones $\mathbb{Q}(X) \subset \mathbb{R}(X) \subset \mathbb{C}(X)$, donde $\mathbb{Q}(X)$, $\mathbb{R}(X)$ y $\mathbb{C}(X)$ son los cuerpos de cocientes de los anillos de polinomios $\mathbb{Q}[X], \mathbb{R}[X]$ y $\mathbb{C}[X]$ respectivamente. Estas extensiones son todas infinitas, a excepción de la extensión $\mathbb{R}(X) \subset \mathbb{C}(X)$ que es de grado 2.

A partir de una extensión E de un cuerpo K, es posible encontrar extensiones intermedias F del cuerpo K tal que $K \subset F \subset E$. Si tomamos un subconjunto no vacío A y el subanillo $K[A]$ de E generado por K y A, y construimos el cuerpo cociente de $K[A]$, $K(A)$, obtenemos una extensión intermedia $K \subset K(A) \subset E$.

Si $A = \{a_1, a_2, \ldots, a_n\}$ es un conjunto finito, notamos al subanillo $K[A]$ por $K[a_1, a_2, \ldots, a_n]$ y al subcuerpo $K(A)$ por $K(a_1, a_2, \ldots, a_n)$.

La demostración del teorema que enunciamos a continuación puede encontrarse en [21].

Teorema 2.1.2 *Si E es una extensión de un cuerpo K y $A \neq \emptyset$ es un subconjunto de E entonces:*

a) $K[A] = \{f(a_1, a_2, \ldots, a_n) : n \in \mathbb{N}, f \in K[X_1, X_2, \ldots, X_n], a_1, \ldots, a_n \in A\}$.
En particular, si A es un subanillo de E (que contiene la unidad de E), $K[A]$ está formado por todas las sumas finitas $\sum_{i=1}^{n} k_i a_i,\ k_i \in K,\ a_i \in A$.

b) $K(A) = \{\frac{u}{v} : u, v \in K[A], v \neq 0\}$.

Ejemplos 2.1.1 *Son ejemplos de extensiones:*

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{R}, \quad \mathbb{R}(i) \subset \mathbb{C}$.
Es fácil ver que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y que $R[i] = \mathbb{C}$.

2. *Si E es una extensión de un cuerpo K y $u, v \in E$ entonces puede probarse fácilmente que $K(u, v) = K(u)(v) = K(v)(u)$. En general, dados A y B subconjuntos de E se tiene que $K(A \cup B) = K(A)(B) = K(B)(A)$.*

Definición 2.1.8 *Una extensión $K(a)$ de K que se obtiene adjuntando un sólo elemento $a \notin K$ se dice una extensión* **simple** *de K.*

El teorema que sigue permite caracterizar un extensión finita de un cuerpo.

Teorema 2.1.3 *Sean K un cuerpo, F una extensión de K y E una extensión de F. Entonces*

$$[E : K] = [E : F][F : K]$$

Mas aún si $\{x_i\}_{i \in I}$ es una base de F sobre K y $\{y_j\}_{j \in J}$ es una base de E sobre F, entonces $\{x_i y_j\}_{(i,j) \in I \times J}$ es una base de E sobre K.

Demostración: Sea $z \in E$ y $\{y_j\}_{j \in J}$ una base de E sobre F. Entonces existen elementos $a_j \in F$, no todos nulos tales que

$$z = \sum_{j \in J} a_j y_j,$$

y para cada $j \in J$, elementos $b_{ij} \in K$, no todos nulos tales que

$$a_j = \sum_{i \in I} b_{ij} x_i.$$

Luego

$$z = \sum_{j\in J}\sum_{i\in I} b_{ij}x_i y_j$$

y la familia $\{x_i y_j\}$ es una familia de generadores de E sobre K.
Veamos que $\{x_i y_j\}$ es un conjunto linealmente independiente sobre K.
Sea $\{c_{ij}\}_{(i,j)\in I\times J}$ una familia de elementos de K que verifican,

$$\sum_{j\in J}\sum_{i\in I} c_{ij}x_i y_j = 0.$$

Como los elementos y_j son linealmente independientes sobre F, resulta $\sum_{i\in I} c_{ij}x_i = 0$ para cada $j \in J$. De esta última expresión y como $\{x_i\}_{i\in I}$ es una base de F sobre K, se tiene que $c_{ij} = 0$ para todo $i \in I, j \in J$. □

Corolario 2.1.1 *Una extensión E de K es finita si y sólo si E es una extensión finita sobre F y F es finita sobre K.*

Dada una extensión E de K, los elementos de E que son raíces de polinomios con coeficientes en K permitirán **caracterizar** las extensiones finitas.

Definición 2.1.9 *Sea E una extensión de un cuerpo K. Un elemento $\alpha \in E$ se dice* **algebraico** *sobre K si α es raíz de un polinomio no nulo $p(X) \in K[X]$.*
Decimos que α es **trascendente** *sobre K, si α no es algebraico sobre K. Una extensión E de K se llama una* **extensión algebraica** *sobre K si todo elemento de E es algebraico sobre K. En caso contrario decimos que E es una* **extensión trascendente** *sobre K.*

Ejemplos 2.1.2 *Son ejemplos de extensiones:*

1. *La unidad imaginaria $i \in \mathbb{C}$ es un elemento algebraico sobre $\mathbb{Q}$ y sobre $\mathbb{R}$. Los números complejos que son algebraicos sobre $\mathbb{Q}$ se llaman* **números algebraicos**.

2. *Un elemento $\alpha \in K$ es algebraico sobre K.*

3. *Si ε es una raíz $n-$ésima de la unidad entonces ε es algebraico sobre cualquier cuerpo numérico K, ya que el polinomio $p(X) = X^n - 1 \in K[X]$.*

4. *Los números irracionales e y π son trascendentes sobre $\mathbb{Q}$. La demostración de la trascendencia de e se debe a Hermite y la de π a Lindemann.*

5. *los números irracionales de la forma α^β, con α algebraico y β algebraico irracional son trascendentes sobre $\mathbb{Q}$. Luego $\mathbb{R}$ es una extensión trascendente de $\mathbb{Q}$.*

6. *$\mathbb{C}$ es una extensión algebraica de $\mathbb{R}$ pues $a + bi \in \mathbb{C}$ es raíz del polinomio $f(X) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$.*

Dado un cuerpo K y un polinomio no constante $f \in K[X]$, buscamos una extensión E de K, tal que el polinomio f tenga todas sus raíces en E.

Sea E una extensión de K y $\alpha \in E$. La aplicación

$$\psi : K[X] \longrightarrow E,$$

$$\psi(p) = p(\alpha),\ p(X) \in K[X],$$

es un homomorfismo de anillos.

La imagen de ψ es $K[\alpha]$ y $Ker(\psi) = \{p \in K[X]/p(\alpha) = 0\}$. Luego por el primer teorema de isomorfismo resulta

$$K[X]/Ker(\psi) \cong K[\alpha].$$

Si $Ker(\psi) = \{0\}$, entonces α es trascendente sobre K y $K[X] \cong K[\alpha]$.

Si $Ker(\psi) \neq \{0\}$, α es algebraico sobre K y $Ker(\psi) = (p_0)$, con $p_0 \neq 0$, pues $K[X]$ es un dominio a ideales principales. Supongamos sin pérdida de generalidad, que p_0 es un polinomio mónico. Entonces $K[X]/(p_0) \cong K[\alpha]$.

Como $K[\alpha]$ es un dominio de integridad, entonces (p_0) es un ideal primo, p_0 es irreducible en $K[X]$ y por lo tanto $K[X]/(p_0)$ es un cuerpo, es decir, $K[\alpha] = K(\alpha)$.

El teorema que sigue nos permite encontrar el grado de una extensión arbitraria de un cuerpo K y la existencia de una extensión de K donde un polinomio $f \in K[X]$ no constante tiene una raíz.

Teorema 2.1.4 *Sean E una extensión del cuerpo K y $\alpha \in E$ un elemento algebraico sobre K, entonces:*

a) Existe un único polinomio mónico e irreducible $p \in K[X]$ tal que $p(\alpha) = 0$.

b) Dado $f \in K[X], f(\alpha) = 0$ si y sólo si p divide a f.

c) $K[\alpha] = K(\alpha)$.

d) Si $gr(p) = n$ entonces $[K(\alpha) : K] = n$ y $\{1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$ es una base de $K(\alpha)$ sobre K.

Demostración: Los incisos a), b) y c) se deducen del razonamiento anterior.
Para demostrar d) veamos que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ son linealmente independientes sobre K.
Si $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un conjunto linealmente dependiente sobre K, existen elementos $a_i \in K$ no todos nulos, con $0 \leq i \leq n-1$, , tales que α es raíz del

polinomio $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{n-1}X^{n-1}$ y $f \neq 0$. Esto contradice b) pues $gr(f) < gr(p)$.
Probemos a continuación que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un conjunto de generadores de $K[\alpha]$.
Dado $f(X) \in K[X]$, al dividir f por p, por el algoritmo de división obtenemos polinomios $q(X)$ y $r(X)$ en $K[X]$ tales que

$$f(X) = q(X)p(X) + r(X) \quad y \quad gr(r) < n$$

Entonces $f(\alpha) = r(\alpha)$ y de aquí resulta que el conjunto

$$\{1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$$

genera el $K-$espacio vectorial $K[\alpha]$. □

Definición 2.1.10 *Llamamos al polinomio irreducible mónico $p \in K[X]$ del teorema anterior,* **polinomio minimal** *de α sobre K. Si $gr(p) = n$ decimos que α es algebraico sobre K de* **grado** *n.*

Ejemplos 2.1.3 *Sea K un cuerpo.*

1. *Un elemento α es algebraico sobre K de grado uno si y sólo si $\alpha \in K$.*
2. *$\sqrt{2}$ es algebrico sobre $\mathbb{Q}$, su polinomio minimal es $X^2 - 2$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y una base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{2}\}$. Luego $\mathbb{Q}(\sqrt{2})$ es una extensión algebraica de $\mathbb{Q}$.*
3. *$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. El elemento $\sqrt[4]{2}$ es algebraico sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(\sqrt{2})$. El polinomio minimal sobre Q es $f(X) = X^4 - 2$, pero este polinomio no es irreducible sobre $\mathbb{Q}(\sqrt{2})[X]$, pues $f(X) = X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$. El polinomio minimal sobre $\mathbb{Q}(\sqrt{2})$ es $X^2 - \sqrt{2}$.*
4. *Si ε_i son las raíces $n-$ésimas de la unidad de orden n, $n \in \mathbb{N}$, el polinomio ciclotómico $f_n(X) = \Pi_{i=0}^{n-1}(X - \varepsilon_i)$ es un polinomio con coeficientes enteros irreducible sobre $\mathbb{Q}$. Luego $f_n(X)$ es el polinomio minimal de cualquier raíz primitiva de la unidad ε de orden n y $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \phi(n)$, siendo $\phi(n)$ el indicador de Euler. Al cuerpo $\mathbb{Q}(\varepsilon)$ se lo denomina el* **cuerpo ciclotómico de orden** *n.*

A continuación veremos que toda extensión finita de un cuerpo es algebraica.

Teorema 2.1.5 *Sea E una extensión finita de un cuerpo K. Entonces $K \subset E$ es una extensión algebraica. Más aún, si $[E : K] = n$ entonces todo elemento de E es raíz de un polinomio con coeficientes en K de grado menor o igual que n.*

Demostración: Dado $\alpha \in E$, como $[E : K] = n$, entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ es un conjunto linealmente dependiente sobre K. Luego existen elementos $a_i \in K$, con $0 \leq i \leq n$, no todos nulos tales que α es raíz del polinomio

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{n-1}X^{n-1} + a_nX^n \quad \text{con} \quad gr(f) \leq n.$$

Luego α es algebraico sobre K. □

Del teorema se deduce lo siguiente:
1) $K \subset K(\alpha) \subset E$ y el grado de α sobre K divide a n.
2) La recíproca del teorema no se verifica ya que existen extensiones algebraicas que no son finitas.
3) α es algebraico sobre K si y sólo si $K(\alpha)$ es una extensión finita de K.

Una extensión importante es la que da la definición que sigue:

Definición 2.1.11 *Sea E una extensión de un cuerpo K. Decimos que E es una extensión* **finitamente generada** *de K si existe un número finito de elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tales que $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Toda extensión finita E de K es finitamente generada. Si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base del $K-$espacio vectorial E entonces $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Sin embargo la recíproca de esta proposición es falsa pues $K(X)$ es una extensión finitamente generada de K pero no es una extensión finita de K.

Teorema 2.1.6 *Sea $K \subset E$. El cuerpo E es una extensión finita de K si y sólo si E es finitamente generado sobre K por elementos algebraicos.*

Demostración: Si E es una extensión finita de K entonces E es una extensión algebraica de K finitamente generada. Luego existen $\alpha_i \in K$ algebraicos, con $1 \leq i \leq n$, tales que $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
Recíprocamente, sea $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, con $\alpha_1, \alpha_2, \ldots, \alpha_n$ algebraicos sobre K. La demostración la haremos haciendo inducción sobre el número de elementos que generan a E.
Si E está generado por un único elemento algebraico α entonces $[K(\alpha) : K]$ es igual al grado del polinomio minimal de α sobre K. Luego $[K(\alpha) : K]$ es finito y en consecuencia E es una extensión finita sobre K.
Sea $n > 1$ y supongamos que $[K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : K]$ es finito. Como α_n es algebraico sobre K entonces también lo es sobre $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. Luego
$K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n)$ es una extensión finita de $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$.
Como

$$K \subset K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \subset K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n) = E$$

resulta

$$[E : K] = [E : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})][K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : K]$$

y de aquí que $[E : K]$ es finito. $\square$

La relación "... es una extensión algebraica de ..." es transitiva como prueba el siguiente teorema:

Teorema 2.1.7 *Sea $K \subset F \subset E$. El cuerpo E es una extensión algebraica sobre K si y sólo si E es una extensión algebraica sobre F y F es una extensión algebraica sobre K.*

Teorema 2.1.8 *Sea E una extensión de K.*

a) Si $\alpha, \beta \in E$ son elementos algebraicos sobre K entonces $\alpha \pm \beta$, $\alpha \cdot \beta$ y α^{-1}, con $\alpha \neq 0$, son algebraicos sobre K.

b) El conjunto L de todos los elementos de E que son algebraicos sobre K es un subcuerpo de E.

Definición 2.1.12 *La extensión L de K dada en el teorema anterior se llama* **clausura algebraica** *de K en E.*

De la definición de L se deduce que L es la mayor de las extensiones algebraicas de K contenidas en E.

A continuación veremos cómo podemos construir el cuerpo de raíces de un polinomio no constante $f \in K[X]$. Esto nos permitirá encontrar una clausura algebraica del cuerpo K.

Dado un cuerpo K y un polinomio no constante $f(X) \in K[X]$, puede suceder que ninguna raíz de $f(X)$ esté en K, o bien que tenga algunas de sus raíces en él. Buscamos alguna extensión E de K en la que f tenga todas sus raíces. Veremos que existe una extensión algebraica E de K, donde f puede factorizarse en producto de polinomios de primer grado por una constante no nula, y que esta extensión es única a menos de $K-$isomorfismos.

Dados dos cuerpos K y E, todo homomorfismo de anillos

$$\varphi : K \longrightarrow E$$

es inyectivo o nulo. Luego si φ es un homomorfismo de anillos no nulo entonces es un monomorfismo y $K \cong \varphi(K) \subset E$. Luego $\varphi(K)$ es un subcuerpo de E y E es una extensión de $\varphi(K)$. Construimos una extensión F de K y un isomorfismo $\overline{\varphi} : F \longrightarrow E$ que extiende a φ. Luego $\overline{\varphi}\restriction_K = \varphi$. El diagrama es el siguiente:

$$\begin{array}{ccc} K & \subset & F \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\overline{\varphi}} \\ \varphi(K) & \subset & E\ . \end{array}$$

Sea S un conjunto disjunto de K coordinable con $E - \varphi(K)$ y $F = K \cup S$. El homomorfismo φ puede extenderse a una biyección $\overline{\varphi} : F \longrightarrow E$.
Definiendo en F las siguientes operaciones de suma y producto:

$$x + y = \overline{\varphi}^{-1}(\overline{\varphi}(x) + \overline{\varphi}(y))$$

$$x \cdot y = \overline{\varphi}^{-1}(\overline{\varphi}(x) \cdot \overline{\varphi}(y)),$$

resulta que $(F, +, \cdot)$ es un cuerpo y estas operaciones restringidas a K coinciden con las de K. Luego K es un subcuerpo de F y $\overline{\varphi}$ es un isomorfismo.

Es importante observar que si $\varphi(K) \neq E$, la construcción de F no es única.
Identificando a K con $\varphi(K)$, E puede verse como una extensión de K.

Dadas E y F dos extensiones de un cuerpo K, nuestro objetivo es estudiar aquellos homomorfismos $\varphi : E \longrightarrow F$ que dejan fijos los elementos de K, ya que esto nos permitirá afirmar que si α y β son dos raíces de un polinomio irreducible en $K[X]$ entonces $K(\alpha)$ es isomorfo a $K(\beta)$.

Comencemos dando la definición de $K-$homomorfismo.

Definición 2.1.13 *Dadas E y F dos extensiones de un cuerpo K, un homomorfismo no nulo $\varphi : E \to F$ se dice un $K-$***homomorfismo** *si $\varphi\restriction_K = id_K$, es decir si $\varphi(a) = a$ para todo $a \in K$.*

Veamos a continuación que un $K-$homomorfismo aplica raíces de un polinomio no constante $f \in K[X]$ en raíces de f, de donde resultará que todo $K-$endomorfismo es un automofismo.

Teorema 2.1.9 *Sean E y F extensiones de un cuerpo K y $\varphi : E \longrightarrow F$ un $K-$homomorfismo. Entonces*

a) φ es un homomorfismo de $K-$espacios vectoriales.

b) Si $\alpha \in E$ es una raíz de un polinomio $f(X) \in K[X]$ entonces $\varphi(\alpha) \in F$ también es raíz de $f(X)$.

Demostración: El homomorfismo φ deja fijo los elementos de K y de aquí resulta inmediatamente que φ es un homomorfismo de $K-$espacios vectoriales.

Sea α una raíz del polinomio $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in K[X]$. Entonces

$$\begin{aligned} f(\varphi(\alpha)) &= a_0 + a_1\varphi(\alpha) + a_2(\varphi(\alpha))^2 + \ldots + a_n(\varphi(\alpha))^n = \\ &= \varphi(a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n) = \varphi(f(\alpha)) = 0. \end{aligned}$$

Luego el $K-$homomorfismo φ aplica raíces de f es raíces de f. □

Teorema 2.1.10 *Si $K \subset E$ es una extensión algebraica entonces todo $K-$homomorfismo $\varphi : E \longrightarrow E$ es un automorfismo.*

Demostración: Por ser φ un $K-$homomorfismo es un homomorfismo no nulo y en consecuencia un monomorfismo. Veamos que φ es sobreyectiva.
Dada $\alpha \in E$, sabemos que existe un polinomio $f(X) \in K[X]$ tal que α es raíz de f por ser E una extensión algebraica de K. Sea $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ con $\alpha_1 = \alpha$ el conjunto de todas las raíces de f que son elementos de E. Por el teorema anterior, φ aplica raíces de f en raíces de f y como φ es un endomorfismo inyectivo y S es finito, $\varphi(S) = S$. Luego existe un índice i con $1 \leq i \leq k$ tal que $\varphi(\alpha_i) = \alpha$ y por lo tanto φ es sobreyectiva. □

Si la aplicación $\varphi : E \longrightarrow E$ es un endomorfismo no nulo, los elementos que quedan fijos por φ, forman un subcuerpo K de E. Por el teorema anterior sabemos que si E es una extensión algebraica sobre K, φ es un automorfismo.

Dados dos cuerpos K y K', un isomorfismo $\varphi : K \longrightarrow K'$ puede extenderse a un isomorfismo $\tilde{\varphi} : K[X] \longrightarrow K'[X]$ de la siguiente manera:

$$\tilde{\varphi}(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi(a_i) X^i.$$

Luego, un polinomio $f(X) \in K[X]$ es irreducible sobre K si y sólo si $\tilde{\varphi}(f(X)) \in K'[X]$ es irreducible sobre K'.

En lo que sigue probaremos que el cuerpo de raíces de un polinomio no constante es único a menos de $K-$isomorfismo.

Teorema 2.1.11 *Sean K y K' dos cuerpos, $\varphi : K \longrightarrow K'$ un isomorfismo, y $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ y $\tilde{f}(X) = \sum_{i=0}^{n} \varphi(a_i) X^i \in K'[X]$ polinomios irreducibles sobre K y K' respectivamente. Si α es una raíz de f en alguna extensión de K y β es una raíz de $\tilde{f}$ en alguna extensión de K', entonces existe un único isomorfismo $\overline{\varphi} : K(\alpha) \longrightarrow K'(\beta)$ tal que $\overline{\varphi}(\alpha) = \beta$ y $\overline{\varphi}\restriction_K = \varphi$.*
Más aún, si α es una raíz de f en alguna extensión de K y E' es una extensión de K', φ puede extenderse a un homomorfismo $\overline{\varphi} : K(\alpha) \longrightarrow E'$ si y sólo si $\tilde{f}$ tiene una raíz en E'. Además existen tantas extensiones de φ como raíces distintas tiene $\tilde{f}$ en E'.

Demostración: Supongamos que $gr(f) = gr(f') = n$, y que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ y $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ son bases de los $K-$espacios vectoriales $K(\alpha)$ y $K'(\beta)$ respectivamente.
Sea $\overline{\varphi} : K(\alpha) \longrightarrow K'(\beta)$ definida por:

$$\overline{\varphi}(x) = \varphi(b_0) + \varphi(b_1)\beta + \varphi(b_2)\beta^2 + \ldots + \varphi(b_{n-1})\beta^{n-1},$$

cualquiera sea $x \in K(\alpha)$, $x = b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1}$, $b_i \in K$, $1 \leq i \leq n-1$. Es fácil ver que $\overline{\varphi}$ es un isomorfismo tal que $\overline{\varphi}\restriction_K = \varphi$ y $\overline{\varphi}(\alpha) = \beta$.

Como $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base del $K-$espacio vectorial $K(\alpha)$ y $\overline{\varphi}(\alpha) = \beta$ entonces $x \in K(\alpha)$ se escribe de una única manera como combinación lineal de los elementos de la base, de donde resulta la unicidad de $\overline{\varphi}$.
Recíprocamente, si α es una raíz de f en alguna extensión de K y E' es una extensión de K' tal que existe un homorfismo $\overline{\varphi} : K(\alpha) \longrightarrow E'$ que extiende a φ, entonces

$$\tilde{f}(\overline{\varphi}(\alpha)) = \sum_{i=0}^{n} \varphi(a_i)\overline{\varphi}(\alpha)^i = \sum_{i=0}^{n} \overline{\varphi}(a_i)\overline{\varphi}(\alpha^i) = \overline{\varphi}(\sum_{i=0}^{n} a_i\alpha^i) = \overline{\varphi}(0) = 0.$$

Luego $\overline{\varphi}(\alpha)$ es raíz de $\tilde{f}$. □

Corolario 2.1.2 *Sean E y F dos extensiones de K y $\alpha \in E$, $\beta \in F$ dos elementos algebraicos sobre K. Entonces α y β tienen el mismo polinomio minimal sobre K si y sólo si existe un $K-$isomorfismo de $K(\alpha)$ en $K(\beta)$ que aplica α en β.*

Demostración: Considerando en el teorema anterior $K = K'$ y $\varphi = id_K$, sabemos que existe un $K-$isomorfismo de $K(\alpha)$ sobre $K(\beta)$ que aplica α en β.
Recíprocamente, consideremos un $K-$isomorfismo $\psi : K(\alpha) \longrightarrow K(\beta)$ tal que $\psi(\alpha) = \beta$. Si $f = \sum_{i=0}^{n} a_i X^i$ y $f' = \sum_{i=0}^{m} b_i X^i$ son los polinomios minimales de α y β respectivamente, entonces

$$f(\beta) = f(\psi(\alpha)) = \sum_{i=0}^{n} a_i(\psi(\alpha))^i = \psi(\sum_{i=0}^{n} a_i(\alpha)^i) = \psi(0) = 0.$$

Luego f'/f. Como f y f' son polinomios irreducibles mónicos resulta $f = f'$. □

Corolario 2.1.3 *Si E es una extensión de K, $f(X) \in K[X]$ un polinomio irreducible y $\alpha, \beta \in E$ son dos raíces de f, entonces los cuerpos $K(\alpha)$ y $K(\beta)$ son $K-$isomorfos.*

Ejemplos 2.1.4 *Veamos los siguientes ejemplos de extensiones isomorfas.*

1. *Los polinomios $f(X) = X^2 - 2$ y $f'(X) = X^2 - 4X + 2$ son irreducibles en $\mathbb{Q}[X]$ y las extensiones $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(2 + \sqrt{2})$ son isomorfas.*

2. *Sean $f(X) = X^2 + X + 1$ y $g(X) = X^2 + 1$ dos polinomios irreducibles en $\mathbb{Z}_3[X]$. Si δ y ε son raíces de f y g respectivamente, resulta que*

   $$f(X) = (X - \delta)(X - (2 + 2\delta)) \quad y \quad g(X) = (X - \varepsilon)(X - 2\varepsilon).$$

   Luego $\mathbb{Z}_3(\delta)$ es isomorfo a $\mathbb{Z}_3(2 + 2\delta)$.

   Como f y g son los polinomios minimales de δ y ε respectivamente entonces no existe un $K-$isomofismo de $\mathbb{Z}_3(\delta)$ sobre $\mathbb{Z}_3(\varepsilon)$ que aplique δ en ε. Sin embargo, los cuerpos $\mathbb{Z}_3(\delta)$ y $\mathbb{Z}_3(\varepsilon)$ son isomorfos, pues si consideramos $\varphi : \mathbb{Z}_3(\delta) \longrightarrow \mathbb{Z}_3(\varepsilon)$ tal que $\varphi(\delta) = 1 + \varepsilon$ queda definido un isomorfismo de cuerpos.

Observemos que el teorema 2.1.11 no es verdadero si f no es un polinomio irreducible. Si consideramos el polinomio $f(X) = (X^2-2)(X^2-3)$, los elementos $\pm\sqrt{2}$ y $\pm\sqrt{3}$ son raíces de f. Sin embargo los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ no son isomorfos, ya que en el cuerpo $\mathbb{Q}(\sqrt{3})$ no existe ningún elemento que elevado a cuadrado sea dos y en el cuerpo $\mathbb{Q}(\sqrt{2})$ si existe dicho elemento.

Dado un polinomio $f(X) \in K[X]$, con K cuerpo, veremos a continuación cómo construir una extensión de K que contenga una raíz de f. Reiterando este procedimmiento, obtendremos una extensión del cuerpo que contenga todas las raíces del polinomio, y de esta forma podremos demostrar la existencia de un cuerpo algebraicamente cerrado que contiene a K como subcuerpo.

Teorema 2.1.12 *Si K es un cuerpo y $f(X) \in K[X]$ un polinomio no constante, entonces existe una extensión E de K donde f tiene una raíz.*

Demostración: Supongamos sin pérdida de generalidad que f es irreducible. Luego $K[X]/(f)$ es un cuerpo. Sea $\varphi : K[X] \longrightarrow K[X]/(f)$ el homomorfismo canónico y K' el conjunto de las clases de equivalencia que contienen los polinomios constantes. Entonces el homomorfismo φ restringido a K es un isomorfismo de K en K'. Luego el cuerpo $K[X]/(f) = E$ es una extensión del cuerpo K' y como $K \cong K'$, identificando los elementos de K con los de K' podemos considerar que E contiene a K .
Veamos que $\alpha = \varphi(X)$ es raíz de f.
Si

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

entonces

$$f(\alpha) = f(\varphi(X)) = \varphi(a_0 + a_1X + a_2X^2 + \ldots + a_nX^n) = \varphi(f) = 0.$$

Observemos que $E = K(\alpha)$ y que f es el polinomio minimal de α, a menos del producto por una constante. □

Corolario 2.1.4 *Si K es un cuerpo y $f(X) \in K[X]$ es un polinomio no constante, existe una extensión E de K tal que:*

$$f(X) = c(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n), c \in K - \{0\}, \alpha_i \in E$$

con $1 \leq i \leq n$.

Demostración: Hacemos la demostración por inducción sobre el grado del polinomio f. Si $gr(f) = 1$ el teorema se verifica trivialmente.
Supongamos que $gr(f) > 1$ y que la propiedad se verifica para todo polinomio de grado $n-1$. Por el Teorema 2.1.12 existe una extensión E_1 de K donde f tiene una raíz α_1, i.e. $f(X) = (X-\alpha_1)f_1(X)$ con $f_1(X) \in E_1[X]$.

Como el grado de f_1 es $n-1$, existe una extensión E de E_1 tal que f_1 tiene todas sus raíces en E, y de aquí resulta que f tiene todas sus raíces en E. Luego

$$f(X) = c(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n), \quad c \in K, \quad c \neq 0, \quad \alpha_i \in E, \quad 1 \leq i \leq n.$$

□

Los resultados anteriores nos conducen a la siguiente definición:

Definición 2.1.14 *Sea K un cuerpo y $f(X) \in K[X]$ un polinomio no constante. Una extensión L de K se dice un* **cuerpo de raíces** *de f sobre K si verifica:*

1. *f puede escribirse como productos de polinomios de primer grado en $L[X]$,*

   $$f(X) = c(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n), \quad c \in K,\ c \neq 0,\ \alpha_i \in E,\ 1 \leq i \leq n.$$

2. *$L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.*

La segunda condición dada en la definición anterior es equivalente a la siguiente:

Si $K \subset L' \subset L$ y f se descompone en productos de polinomios de primer grado en $L'[X]$ entonces $L = L'$.

Ejemplos 2.1.5 *Veamos los siguientes ejemplos:*

1. *Sea $f(X) = (X+1)(X^2-3)(X^2-X+\frac{3}{4}) \in \mathbb{Q}[x]$. Las raíces de f en $\mathbb{C}$ son:* $-1,\ \pm\sqrt{3}$ *y* $\frac{1 \pm \sqrt{2}i}{2}$. *El cuerpo de raíces del polinomio f es*

   $$E = \mathbb{Q}(\sqrt{3},\ \frac{1 \pm \sqrt{2}i}{2}) = \mathbb{Q}(\sqrt{3},\ \sqrt{2}, i) \text{ y } [E : \mathbb{Q}] = 4.$$

2. *Dado el polinomio*

   $$f(X) = X^2 + X + 1 \in \mathbb{Z}_2[X],$$

   como f es irreducible, usando el Teorema 2.1.12 construimos una extensión $\mathbb{Z}_2(\varepsilon)$ de $\mathbb{Z}_2$, donde ε es una raíz de f.

   $\varphi : \mathbb{Z}_2[X] \longrightarrow \mathbb{Z}_2[X]/(f)$ *tal que* $\varphi(X) = \varepsilon$ *y* $E = \mathbb{Z}_2[X]/(f) = \mathbb{Z}_2(\varepsilon)$.

   La raíz ε tiene a f como polinomio minimal sobre $\mathbb{Z}_2$, luego $[\mathbb{Z}_2(\varepsilon) : \mathbb{Z}_2] = 2$, $\varepsilon^2 + \varepsilon + 1 = 0$, y $\{1, \varepsilon\}$ es una base de $\mathbb{Z}_2(\varepsilon)$ sobre $\mathbb{Z}_2$ y $\mathbb{Z}_2(\varepsilon) = \{0, 1, \varepsilon, 1+\varepsilon\}$.

El Corolario 2.1.4 asegura la existencia del cuerpo de raíces de un polinomio no constante $f \in K[X]$, pero éste no es único como se muestra en el ejemplo que sigue.

Si $f(X) = X^2 - 2 \in \mathbb{Q}[X]$, la extensión de $\mathbb{Q}$, $E = \mathbb{Q}[X]/(X^2-2)$ es un cuerpo de raíces de f. Otro cuerpo de raíces de f es la extensión $\mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$.

El teorema siguiente nos dice cuando el cuerpo de raíces de un polinomio no constante es único.

Teorema 2.1.13 *Dado* $\varphi : K \longrightarrow K'$ *un isomorfismo de cuerpos,* $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ *un polinomio no constante y* $\varphi(f) = \tilde{f}(X) = \sum_{i=0}^{n} \varphi(a_i) X^i \in K'[X]$. *Sea* L *un cuerpo de raíces de* f *sobre* K *y* L' *un cuerpo de raíces de* $\tilde{f}$ *sobre* K', *entonces el isomorfismo* φ *puede extenderse a un isomorfismo de* L *sobre* L'. *La extensión puede hacerse de más de una manera aplicando cada raíz de* f *en* L *en una raíz de* $\tilde{f}$ *en* L'.

Demostración: La demostración la hacemos por inducción sobre el grado de f.
Si $gr(f) = 1$, L coincide con K y por lo tanto $L' = K'$ y el teorema se satisface.

Sea $gr(f) > 1$ y supongamos que la propiedad se verifica para todos los polonomios de grado $n - 1$.
Sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ y $\beta_1, \beta_2, \ldots, \beta_n$ las raíces de f y $\tilde{f}$ en L y L' respectivamente, es decir $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ y $L' = K'(\beta_1, \beta_2, \ldots, \beta_n)$.
Sea f_1 un factor irreducible de f y α una raíz de f_1 en L. Sea $\tilde{f}_1$ el factor irreducible de $\tilde{f}$ y β la raíz de $\tilde{f}_1$ en L'. Entonces φ puede extenderse a un isomorfisomo $\overline{\varphi} : K(\alpha_1) \longrightarrow K'(\beta_1)$ tal que $\overline{\varphi}(\alpha_1) = \beta_1$. Además,

$$f = (X - \alpha_1) g_1, \text{ con } g_1 \in K(\alpha_1)[X] \text{ y } gr(g_1) = n - 1$$

$$\tilde{f} = (X - \beta_1) \tilde{g}_1, \text{ con } \tilde{g}_1 \in K(\beta_1)[X], \text{ y } gr(\tilde{g}_1) = n - 1$$

siendo $\tilde{g}_1$ la imagen de g_1 por el isomorfismo $\overline{\varphi}$.
A su vez el isomorfismo $\overline{\varphi} : K(\alpha_1) \longrightarrow K'(\beta_1)$ puede extenderse al isomorfismo

$$\tilde{\overline{\varphi}} : K(\alpha_1)[X] \longrightarrow K'(\beta_1)[X].$$

Como $\alpha_2, \ldots, \alpha_n$ y $\beta_2, \ldots, \beta_n$ son las raíces de g_1 y $\tilde{g}_1$ sobre $K(\alpha_1)$ y $K'(\beta_1)$ resulta $K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = L$ y $K'(\beta_1)(\beta_2, \ldots, \beta_n) = L'$. Por hipótesis de inducción podemos extender el isomorfismo $\overline{\varphi}$ a un isomorfismo

$$\overline{\overline{\varphi}} : K(\alpha_1)(\alpha_2, \ldots, \alpha_n) \longrightarrow K'(\beta_1)(\beta_2, \ldots, \beta_n),$$

que aplica cada raíz α_i en β_j con $2 \leq i \leq n$ y $2 \leq j \leq n$.

La situación es la siguiente:

$$\begin{array}{ccc}
K & \xrightarrow{\varphi} & K' \\
i \downarrow & & \downarrow i \\
K(\alpha_1) & \xrightarrow{\overline{\varphi}} & K'(\beta_1) \\
i \downarrow & & \downarrow i \\
K(\alpha_1)(\alpha_2, \ldots, \alpha_n) & \xrightarrow{\overline{\overline{\varphi}}} & K'(\beta_1)(\beta_2, \ldots, \beta_n),
\end{array}$$

donde $\overline{\overline{\varphi}} : L \longrightarrow L'$ es el isomorfismo buscado. □

A continuación probaremos que dado un cuerpo K, existe una extensión algebraica E de K, tal que cada polinomio no constante de $E[X]$ tiene todas sus raíces en E. Además esta extensión es única a menos de $K-$isomorfismos.

Comenzamos dando las siguientes definiciones:

Definición 2.1.15 *Decimos que un cuerpo K es* **algebraicamente cerrado** *si todo polinomio no constante de $K[X]$ tiene una raíz en K.*

De la definición resulta que si K es algebraicamente cerrado, los polinomios irreducibles de $K[X]$ son los de grado uno.

Definición 2.1.16 *Dado un cuerpo K, una extensión E de K se dice una* **clausura algebraica** *de K si E es una extensión algebraica de K y E es algebraicamente cerrado.*

Si $K \subset F \subset E$ y E es una clausura algebraica de K entonces E es una clausura algebraica de F.

Sin embargo la recíproca de esta afirmación no es válida. Sabemos que $\mathbb{C}$ es algebraicamente cerrado y algebraico sobre $\mathbb{R}$. Luego $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$, pero no lo es de $\mathbb{Q}$ ya que $\mathbb{C}$ es una extensión trascendente de $\mathbb{Q}$.

Teorema 2.1.14 *Si K es un cuerpo entonces existe un cuerpo algebraicamente cerra- do que contiene a K como subcuerpo.*

Demostración: Comencemos construyendo una extensión E_1 de K en donde todo polinomio no constante de $K[X]$ tiene una raíz en E_1.
A cada polinomio no constante $f \in K[X]$ le asociamos una indeterminada X_f. Sea S el conjunto de todas estas indeterminadas y $K[S]$ el anillo de polinomios con coeficientes en K en infinitas indeterminadas,

$$K[S] = \bigcup_{n\in\mathbb{N}} K[X_{f_1}, X_{f_2}, \ldots, X_{f_n}]$$

Sea I el ideal de $K[S]$ generado por los polinomios $f(X_f)$. Veamos que I es un ideal propio de $K[S]$. Si $1 \in I$ entonces existen $g_i \in K[S]$, con $1 \leq i \leq n$ tal que:

$$g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \ldots + g_n f_n(X_{f_n}) = 1$$

Como en cada polinomio g_i figuran en total un número finito de indeterminadas, $X_1, X_2, \ldots, X_m$ $(m \geq n)$, la ecuación anterior puede escribirse

$$\sum_{i=1}^{n} g_i(X_{f_1}, X_{f_2}, \ldots, X_{f_m}) f_i(X_{f_i}) = 1$$

Por el Teorema 2.1.12 podemos encontrar una extensión F de K tal que cada polinomio f_i tenga una raíz α_i, para $1 \leq i \leq n$. Considerando $\alpha_i = 0$ con $n < i \leq m$ y reemplazamos las indeterminadas X_{f_i} por $\alpha_i,\ 1 \leq i \leq m$, en la última ecuación obtenemos $0 = 1$. Luego $1 \notin I$.
Como I es un ideal propio existe un ideal $M \subset K[S]$ maximal entre los que contienen a I. Luego $K[S]/M$ es un cuerpo. El epimorfismo canónico $\psi : K[S] \longrightarrow K[S]/M$ restringido a K es un monomorfismo. Identificando K con su imagen y tomando $E_1 = K[S]/M$ como una extensión de K, cada polinomio no constante $f \in K[X]$ tiene una raíz en E_1 pues,

$$f(\psi(X_f)) = \psi(f(X_f)) = 0,$$

ya que $f(X_f) \in M$. Luego $\psi(X_f) \in E_1$ es raíz de f.
Reiterando este procedimiento podemos formar una cadena de cuerpos

$$K \subset E_1 \subset E_2 \subset \ldots \subset E_n \subset \ldots$$

tal que todo polinomio no constante de $E_i[X]$ tiene una raíz en E_{i+1}.
Veamos que $E = \bigcup_{i \geq 1} E_i$ es un cuerpo algebraicamente cerrado.
Si $x, y \in E$, existe un índice n tal que $x, y \in E_n$. Luego $x + y$, $x \cdot y \in E_n$ y como las operaciones no dependen del índice resulta que E es un cuerpo.
Además por la construcción de $E[X]$, cualquier polinomio no constante de $E[X]$ tiene todos sus coeficientes en algún E_n y una raíz en E_{n+1}. Luego dicha raíz está en E y por lo tanto E es algebraicamente cerrado. □

Corolario 2.1.5 *Todo cuerpo K posee una clausura algebraica.*

Demostración: Sea E una extensión de K algebraicamente cerrada y $\overline{K}$ la clausura algebraica de K en E. Luego $K \subset \overline{K} \subset E$. Vimos que $\overline{K}$ es algebraica sobre K y además es un cuerpo algebraicamente cerrado ya que todo polinomio no constante $f \in \overline{K}[X]$ tiene una raíz α en E. Como α es algebraico sobre $\overline{K}$, entonces $\overline{K}(\alpha)$ es algebraico sobre $\overline{K}$ y como $\overline{K}$ es algebraico sobre K, resulta α algebraico sobre K. Luego $\alpha \in \overline{K}$. □

A continuación veremos que dos clausuras algebraicas de un cuerpo K son $K-$isomorfas.

Teorema 2.1.15 *Sea $\psi : K \longrightarrow L$ la inmersión de un cuerpo K en un cuerpo L algebraicamente cerrado y $K(\alpha)$ una extensión algebraica de K. Entonces ψ puede extenderse a una aplicación $\overline{\psi} : K(\alpha) \longrightarrow L$ y el número de estas aplicaciones coincide con el número de raíces distintas que tiene el polinomio minimal de α en un cuerpo de raíces arbitrario del mismo.*

Demostración: Por el Teorema 2.1.11 sabemos que existen tantas extensiones

$\overline{\psi} : K(\alpha) \longrightarrow L$ como raíces distintas tiene el polinomio $\tilde{f} \in \psi(K)[X]$, siendo $f \in K[X]$ el polinomio minimal de α sobre K.
Como L es algebraicamente cerrado, contiene todas las raíces de $\tilde{f}$, y en consecuencia contiene al cuerpo de raíces de $\tilde{f}$, que es isomorfo al de f. □

Teorema 2.1.16 *Sea E una extensión algebraica de K y ψ una inmersión de K en un cuerpo algebraicamente cerrado L. Entonces ψ puede extenderse a una inmersión $\overline{\psi} : E \longrightarrow L$. Si E es algebraicamente cerrado y L es algebraico sobre $\psi(K)$ entonces $\overline{\psi}$ es un isomorfismo de E en L.*

Demostración: Consideremos los pares (F, σ), con $K \subset F \subset E$ y $\sigma : F \longrightarrow L$ un homomorfismo que extiende a ψ, i.e. $\sigma\restriction_K = \psi$.
El conjunto S de todos los pares de la forma (F, σ) es no vacío pues $(K, \psi) \in S$.
Definimos en S la siguiente relación:

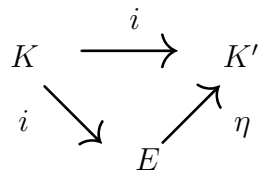
$$(F_1, \sigma_1) \leq (F_2, \sigma_2) \text{ si y sólo si } F_1 \subset F_2 \text{ y } \sigma_2\restriction_{F_1} = \sigma_1.$$

Es fácil ver que " $\leq$ " es una relación de orden definida sobre S.
$(S, \leq)$ es inductivo superiormente. En efecto, si $\{(F_i, \sigma_i)\}_{i \in I}$ es una cadena de S, tomando $F = \bigcup_{i \in I} F_i$ y $\sigma : F \longrightarrow L$ definida por $\sigma(x) = \sigma_i(x)$, para $x \in F_i$, resulta que F es un subcuerpo de E que contiene a K. La aplicación σ está bien definida y es un homomorfismo que extiende a ψ. Por el Lema de Zorn existe un elemento maximal en S, $(H, \overline{\psi})$.
Veamos que $H = E$. Si $H \neq E$ existe $\alpha \in E$ tal que $\alpha \notin H$. Como E es una extensión algebraica sobre K, α es algebrico sobre K y por lo tanto lo es sobre H. Luego por el teorema anterior, $\overline{\psi} : H \longrightarrow L$ puede extenderse a un homomorfismo $\overline{\overline{\psi}} : H(\alpha) \longrightarrow L$. De aquí resulta que $(H(\alpha), \overline{\overline{\psi}}) \in S$, lo que contradice la maximalidad de $(H, \overline{\psi})$. Luego $H = E$ y $\overline{\psi} : E \longrightarrow L$ es la extensión buscada.
Si E es algebraicamente cerrado, como $E \simeq \overline{\psi}(E)$ entonces $\overline{\psi}(E)$ es algebraicamente cerrado. Si L es algebraico sobre $\psi(K)$ entonces L es algebraico sobre $\overline{\psi}(E)$ pues $\psi(K) \subset \overline{\psi}(E) \subset L$. Luego $L = \overline{\psi}(E)$. □

Corolario 2.1.6 *Dos clausuras algebraicas de un cuerpo K son $K-$isomorfas.*

Toda extensión algebraica E de un cuerpo K está contenida en una clausura algebraica de K. Si E es una extensión algebraica de K y $\overline{E}$ es una clausura algebraica de E resulta que $\overline{E}$ es una extensión algebraica de K. Como $\overline{E}$ es algebraicamente cerrrado resulta $\overline{K} = \overline{E}$.
Recíprocamente, si $\overline{K}$ es una clausura algebraica de K, todo subcuerpo intermedio $K \subset E \subset \overline{K}$ es una extensión algebraica de K y por lo tanto $\overline{K} = \overline{E}$.

Si $\overline{K}$ es la clausura algebraica de un cuerpo K, toda extensión algebraica E de K puede sumergirse en $\overline{K}$ por un $K-$homomorfismo. El teorema anterior muestra que la aplicación inclusión $i : K \longrightarrow \overline{K}$ puede extenderse a un $K-$homomorfismo η de la siguiente manera:



Luego $E \cong \eta(E)$ y $K \subset \eta(E) \subset \overline{K}$.

Corolario 2.1.7 *Si $K \subset E \subset \overline{K}$ y $\eta : E \longrightarrow \overline{K}$ es un $K-$homomorfismo entonces existe un $K-$automorfismo $\overline{\eta} : \overline{K} \longrightarrow \overline{K}$ que extiende a η.*

2.2. Extensiones de Galois.

En esta sección comenzamos definiendo las extensiones separables y normales. Luego damos una caracterización de las mismas para el caso finito. Las extensiones normales y separables, llamadas extensiones de Galois tendrán un rol fundamental en la demostración del teorema de la base normal que daremos en la última sección de este capítulo.

Definición 2.2.1 *Dada una clausura algebraica $\overline{K}$ de un cuerpo K y una extensión E de K tal que $K \subset E \subset \overline{K}$, al cardinal del conjunto de todos los $K-$homomorfismos de E en $\overline{K}$ lo llamamos* **grado de separabilidad de** E **sobre** K *y lo notamos* $[E : K]_s$.

Por el Teorema 2.1.15 sabemos que si α es un elemento algebraico sobre K entonces $K \subset K(\alpha) \subset \overline{K}$ y el número de $K-$homomorfismos de $K(\alpha)$ en $\overline{K}$ es igual al número de raíces distintas del polinomio minimal f de α sobre K.

Teorema 2.2.1 *Si E es una extensión de K tal que $K \subset E \subset \overline{K}$ entonces:*

a) Si $K \subset E \subset F \subset \overline{K}$ entonces:

$$[F : K]_s = [F : E]_s [E : K]_s.$$

Sea $\{\mu_i\}_{i \in I}$ el conjunto de los $K-$homomorfismos de E en $\overline{K}$ y $\{\tau_j\}_{j \in J}$ el de los $E-$homomorfismos de F en $\overline{K}$. Para cada índice $i \in I$, $\overline{\mu_i}$ es un $K-$automorfismo de $\overline{K}$ que extiende a μ_i.

Definiendo $\omega_{ij} : F \longrightarrow \overline{K}$ como la composición $\overline{\mu_i} \circ \tau_j$ resulta que $\{\omega_{ij}\}_{(i,j) \in I \times J}$ es el conjunto de todos los $K-$homomorfismos de F en $\overline{K}$.

b) Si E es una extensión finita de K entonces $[E : K]_s \leq [E : K]$.

Demostración:

a) Para cada par $(i,j) \in I \times J$, las aplicaciones ω_{ij} son $K-$homomorfismos de F en $\overline{K}$ todos distintos. En efecto, si tenemos dos pares $(i,j),(t,r) \in I \times J$ tales que $\omega_{ij} = \omega_{tr}$ entonces para todo $b \in E$,

$$\mu_i(b) = \overline{\mu_i}(b) = \overline{\mu_i}(\tau_j(b)) = \overline{\mu_i}\tau_j(b) = \overline{\mu_t}\tau_r(b) = \overline{\mu_t}(\tau_r(b)) = \overline{\mu_t}(b) = \mu_t(b)$$

Luego $\mu_i = \mu_t$ y $\tau_j = \tau_r$, de donde resulta $i = t$ y $j = r$.

Veamos que si ω es un $K-$homomorfismo de F en $\overline{K}$, ω es alguna de las aplicaciones ω_{ij} definidas anteriormente. Como la aplicación $\omega\restriction_E : E \longrightarrow \overline{K}$ es un $K-$homomorfismo, existe $i \in I$ tal que $\omega\restriction_E = \mu_i$.

Consideremos el $E-$homomorfismo $\overline{\mu_i}^{-1}\omega : F \longrightarrow \overline{K}$. Entonces $\overline{\mu_i}^{-1}\omega = \tau_j$ para algún $j \in J$ de donde resulta $\omega = \overline{\mu_i}\tau_j = \omega_{ij}$.

Como $[F : K]_s = \#(I \times J)$ entonces $[F : E]_s = \#(J)$ y $[E : K]_s = \#(I)$. Luego

$$[F : K]_s = [F : E]_s[E : K]_s.$$

b) Sea E una extensión finita de K. Por el Teorema 2.1.6 sabemos que E es finitamente generada sobre K por elementos algebraicos $\alpha_1, \alpha_2, \ldots, \alpha_n$ y en consecuencia E puede obtenerse a partir de K por una sucesión finita de extensiones simples como se indica a continuación:

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n) = E$$

Sean $F_0 = K$ y $F_{i+1} = F_i(\alpha_{i+1})$ para $0 \leq i \leq n-1$. Por el Teorema 2.1.15, el número de extensiones posibles de un monomorfismo $F_i \longrightarrow \overline{K}$ a un homomorfismo de $F_i(\alpha_{i+1})$ en $\overline{K}$, es menor o igual que el grado del polinomio minimal de α_{i+1} sobre F_i, que coincide con $[F_{i+1} : F_i]$. Luego $[F_i(\alpha_{i+1}) : F_i]_s \leq [F_i(\alpha_{i+1}) : F_i]$. Como esta desigualdad se verifica para cada par de cuerpos consecutivos de la cadena dada, por la multiplicidad del grado de las extensiones y por el grado de separabilidad de las mismas resulta

$$[E : K]_s \leq [E : K].$$

□

Definición 2.2.2 *Un elemento α algebraico sobre un cuerpo K se dice* **separable sobre** *K si $[K(\alpha) : K]_s = [K(\alpha) : K]$. Si $K \subset E \subset \overline{K}$, la extensión E se dice* **separable sobre** *K si todos los elementos de E son separables sobre K. Una extensión que no es separable se dice* **inseparable**.
Decimos que un polinomio irreducible $f \in K[X]$ es **separable** *si no tiene raíces múltiples. Un polinomio no constante en $K[X]$ se dice* **separable** *si todos sus factores irreducibles lo son.*

De la definición resulta que un elemento algebraico sobre K es separable si y sólo si su polinomio minimal lo es.

El teorema que sigue da una **condición necesaria y suficiente** para asegurar la separabilidad de una extensión finita.

Teorema 2.2.2 *Dados K, E y F cuerpos se verifica que:*

a) Si $K \subset E \subset F$ y $\alpha \in F$ es un elemento separable sobre K entonces α es separable sobre E.

b) Sea E una extensión finita de K. Entonces E es separable sobre K si y sólo si $[E : K]_s = [E : K]$.

c) Dada $\{\alpha_i\}_{i\in I}$ una familia de elementos de $\overline{K}$. Los elementos α_i con $i \in I$ son separables sobre K si y sólo si $K(\{\alpha_i\}_{i\in I})$ es una extensión separable de K.

d) Si E es una extensión de K, el conjunto L de todos los elementos de E que son separables sobre K es una extensión separable de K.

Demostración:

a) Sea $\alpha \in F$ un elemento separable sobre K. Entonces su polinomio minimal f sobre K no tiene raíces múltiples. Además el polinomio minimal g de α sobre E divide a f y por lo tanto las raíces de g son simples.

b) Sea $K \subset E$ una extensión finita y separable. Luego $E = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, con α_i separable para $1 \leq i \leq m$. Dadas las extensiones

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \alpha_2, \ldots, \alpha_m) = E,$$

por a) α_i es separable sobre $K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, para $2 \leq i \leq m$ y α_1 es separable sobre K. Luego

$$[K(\alpha_1, \alpha_2, \ldots, \alpha_i) : K(\alpha_1, \alpha_2, \ldots, \alpha_i)]_s = [K(\alpha_1, \alpha_2, \ldots, \alpha_i) : K(\alpha_1, \alpha_2, \ldots, \alpha_i)]$$

con $2 \leq i \leq m$ y $[K(\alpha_1) : K]_s = [K(\alpha_1) : K]$.

Por la multiplicidad del grado de las extensiones finitas y por el grado de separabilidad resulta

$$[E : K]_s = [E : K].$$

Recíprocamente, sea $K \subset E$ una extensión finita y $[E : K]_s = [E : K]$. Si $\alpha \in E$ entonces $K \subset K(\alpha) \subset E$ es una cadena finita y por el teorema 2.2.1, $[E : K(\alpha)]_s \leq [E : K(\alpha)]$ y $[K(\alpha) : K]_s \leq [K(\alpha) : K]$. Luego

$$[E : K]_s = [E : K(\alpha)]_s[K(\alpha) : K]_s \leq [E : K(\alpha)][K(\alpha) : K] = [E : K]$$

de donde resulta

$$[E : K(\alpha)]_s = [E : K(\alpha)] \text{ y } [K(\alpha) : K]_s = [K(\alpha) : K],$$

y de aquí que α es separable sobre K.

c) Es fácil ver que si $K(\{\alpha_i\}_{i\in I})$ es una extensión separable de K entonces cada α_i es separable sobre K.

Supongamos que para cada $i \in I$, α_i es separable sobre K y probemos que $K(\{\alpha_i\}_{i\in I})$ es una extensión separable de K.

Sea $\alpha \in K(\{\alpha_i\}_{i\in I})$. Entonces α pertenece a una subextensión de $K(\{\alpha_i\}_{i\in I})$ finitamente generada, por lo que es suficiente probar que esa extensión es separable sobre K. Sea $\alpha \in K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}) \subset K(\{\alpha_i\}_{i\in I})$ y la cadena de extensiones

$$K \subset K(\alpha_{i_1}) \subset K(\alpha_{i_1}, \alpha_{i_2}) \subset \ldots \subset K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}). \quad (1)$$

De a) resulta que cada α_{i_j} es separable sobre $K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{j-1}})$. Entonces en cada eslabón de la cadena (1) el grado de la extensión y el grado de separabilidad de la misma coinciden.

Por la multiplicidad de estos grados resulta:

$$[K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}) : K]_s = [K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}) : K]$$

y por b), $K(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t})$ separable sobre K.

d) Sea $K \subset E$ y L el conjunto de todos los elementos de E que son separables sobre K. Por el inciso c), $K(L)$ es una extensión separable de K y

$K \subset K(L) \subset E$. Luego $K(L) = L$.

□

Veremos en el teorema que sigue que la relación "... es una extensión separable de ..." es transitiva.

Teorema 2.2.3 *Sea $K \subset E \subset F$. F es separable sobre K si y sólo si F es separable sobre E y E es separable sobre K.*

Demostración: Si F es separable sobre K entonces E es separable sobre K y por el inciso a) del teorema anterior F es separable sobre E.
Recíprocamente, sea $\alpha \in F$, F separable sobre E y E separable sobre K. Como α es separable sobre E, si $f(X) = c_0 + c_1X + c_2X^2 + \ldots + X^n \in E[X]$ es el polinomio minimal de α sobre E, f es separable y α es separable sobre $K(c_0, c_1, \ldots, c_{n-1})$.
Como para cada i, $c_i \in E$, c_i es separable sobre K. Luego en la cadena

$$K \subset K(c_0, c_1, \ldots, c_{n-1}) \subset K(c_0, c_1, \ldots, c_{n-1}, \alpha)$$

cada extensión es finita y separable sobre la anterior. Para cada par de extensiones consecutivas resulta que el grado de separabilidad coincide con el grado de la extensión y de aquí que

$$[K(c_0, c_1, \ldots, c_{n-1}, \alpha) : K]_s = [K(c_0, c_1, \ldots, c_{n-1}, \alpha) : K].$$

Luego $K(c_0, c_1, \ldots, c_{n-1}, \alpha)$ es separable sobre K y α también lo es. $\square$

Si $E = K(\alpha)$, todo $K-$homomorfismo $\psi : K(\alpha) \longrightarrow \overline{K}$ queda definido por la imagen de α, y se verifica que $\psi(K(\alpha)) = K(\psi(\alpha))$. Luego α y $\psi(\alpha)$ son raíces del mismo polinomio irreducible mónico de $K[X]$.

De manera análoga si $E = K(\alpha_1, \ldots, \alpha_n)$, todo homomorfismo $\psi : E \longrightarrow \overline{K}$ está unívocamente determinado por las imágenes de los α_i. Para $1 \leq i \leq n$, α_i y $\psi(\alpha_i)$ son raíces del mismo polinomio irreducible mónico con coeficientes en K.

Si la extensión $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ contiene todas las raíces de los polinomios minimales $f_i \in K[X]$, para $1 \leq i \leq n$, entonces dado un $K-$homomorfismo $\psi : E \longrightarrow \overline{K}$ los elementos $\psi(\alpha_1), \psi(\alpha_2), \ldots, \psi(\alpha_n) \in E$ y en consecuencia ψ es un automorfismo de E.

Esta observación nos induce a dar las siguiente definición:

Definición 2.2.3 *Sea $K \subset E \subset \overline{K}$. Decimos que E es una* **extensión normal** *de K si todo K-automorfismo $\psi : E \longrightarrow \overline{K}$ es un automorfismo de E.*

El teorema que sigue **caracteriza** a las extensiones normales.

Teorema 2.2.4 *Sea $K \subset E \subset \overline{K}$.*

a) E es una extensión normal de K si y sólo si todo polinomio irreducible de $K[X]$ que tiene una raíz en E tiene todas sus raíces en E.

b) E es una extensión normal y finita de K si y sólo si E es el cuerpo de raíces de un polinomio en $K[X]$.

Demostración:

a) Sea E una extensión normal de K, $f \in K[X]$ un polinomio irreducible mónico y $\alpha \in E$ una raíz de f. Supongamos que $\beta \in \overline{K}$ es otra raíz de f, entonces existe un $K-$homomorfismo $\psi : K(\alpha) \longrightarrow \overline{K}$ que aplica α en β. Consideremos la aplicación $\overline{\psi} : K(\alpha) \longrightarrow \overline{K}$ que extiende a ψ. Como E es una extensión normal, $\overline{\psi}$ es un automorfismo de E y resulta $\overline{\psi}(\alpha) = \psi(\alpha) = \beta \in E$. Luego f tiene todas sus raíces en E.

   Veamos que todo polinomio irreducible de $K[X]$ que tiene una raíz en E, tiene todas sus raíces en E. Sea $\psi : E \longrightarrow \overline{K}$ un $K-$homomorfismo. Probemos que $\psi(E) \subset E$. Sea $\alpha \in E$ y $f \in K[X]$ su polinomio minimal. Como $\psi(\alpha)$ es otra raíz de f entonces la hipótesis nos asegura que $\psi(\alpha) \in E$.

b) Sea E una extensión finita y normal de K. Luego $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con α_i algebraico sobre K para todo i, $1 \leq i \leq n$. Sea f_i el polinomio minimal sobre K de cada α_i. Como E es normal y α_i es una raíz de f_i, entonces E

contiene todas las raíces de cada f_i. Luego E contiene todas las raíces del polinomio $f = \prod_{i=1}^{n} f_i$ y E es el cuerpo de raíces de f.

Recíprocamente, sea E el cuerpo de raíces de un polinomio $f(X) \in K[X]$ y $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de f. Entonces $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Como cada α_i es algebraico sobre K, E es una extensión finita de K.

Veamos que E es normal. Sea $\psi : K(\alpha_1, \alpha_2, \ldots, \alpha_n) \longrightarrow \overline{K}$ un $K-$homomorfismo. Como ψ aplica raíces de f en raíces de f, ψ queda determinado por los elementos

$$\psi(\alpha_1),\ \psi(\alpha_2),\ \ldots,\ \psi(\alpha_n) \in E.$$

Luego ψ es un endomorfismo de E y E es normal sobre K.

□

La siguiente proposición es válida para extensiones normales.

Teorema 2.2.5 *Sean $K \subset E \subset F$. Si F es una extensión normal de K entonces F es una extensión normal de E.*

Demostración: Todo $E-$homomorfismo de una clausura algebraica $\overline{K}$ de un cuerpo K, es en particular un $K-$homomorfismo. □

2.3. Cuerpos finitos

En esta sección comenzamos demostrando que los cuerpos finitos tienen p^n elementos, con p primo. Probamos la unicidad de los mismos a menos de isomorfismo y mostramos que todo cuerpo finito es perfecto. También vemos que toda extensión finita de un cuerpo finito F es una extensión de Galois y al final de la sección demostramos que el grupo de Galois de un cuerpo F con p^n elementos es cíclico de orden n.

En el estudio de los cuerpos finitos un primer teorema a destacar es el siguiente:

Teorema 2.3.1 *Si A es un dominio de integridad finito entonces A es un cuerpo.*

El teorema anterior nos permite demostrar el siguiente:

Teorema 2.3.2 *El anillo $\mathbb{Z}_n$ de los enteros módulo n es un cuerpo si y sólo si n es un número primo.*

Teorema 2.3.3 *Sea F un cuerpo y U un subgrupo finito del grupo multiplicativo $F^* = F - \{0\}$. Entonces U es cíclico.*

Corolario 2.3.1 *El grupo multiplicativo de un cuerpo finito es cíclico.*

A continuación damos la definición de cuerpo primo y probamos que el cuerpo primo de un cuerpo F es isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p$, con p primo.

Definición 2.3.1 *Llamamos* **cuerpo primo** *de un cuerpo F a la intersección de todos los subcuerpos de F.*

Teorema 2.3.4 *Sea F un cuerpo y F' su cuerpo primo. Entonces F' es isomorfo a $\mathbb{Q}$ o F' es isomorfo a $\mathbb{Z}_p$, para algún primo p.*

Demostración: Sea $\psi : \mathbb{Z} \longrightarrow F$ la aplicación definida por $\psi(z) = z \cdot 1$, donde 1 es la unidad de F. Es claro que ψ es un homomorfismo de anillos. Si $I = Ker(\psi)$ entonces como $\mathbb{Z}/I$ es isomorfo a un subanillo de F resulta que $\mathbb{Z}/I$ es un dominio de integridad. Luego I es un ideal primo de $\mathbb{Z}$ y por lo tanto $I = (0)$ ó $I = (p)$, con p primo.
Si $I = (0)$, $\psi(\mathbb{Z})$ está contenido en F y en consecuencia el cuerpo primo de F es isomorfo a $\mathbb{Q}$.
Si $I = (p)$, con p primo, por el primer teorema de isomorfismo de anillos resulta $Im(\psi) = \mathbb{Z}/(p)$ que es isomorfo a $\mathbb{Z}_p$. Luego $Im(\psi)$ es el cuerpo primo de F. □

El teorema anterior nos conduce a la definición siguiente:

Definición 2.3.2 *Decimos que un cuerpo F es de* **característica 0** *si su cuerpo primo es isomorfo a $\mathbb{Q}$. El cuerpo F es de* **característica** *p con p primo, si su cuerpo primo es isomorfo a $\mathbb{Z}_p$.*

Corolario 2.3.2 *Si F es un cuerpo finito de característica p, con p primo, entonces F tiene p^n elementos con $n \in \mathbb{N},\ n \geq 1$.*

Demostración: Como el cuerpo F es finito, en la aplicación ψ del teorema anterior resulta $Ker(\psi) = (p)$, p primo. En efecto si $Ker(\psi) = (0)$ entonces el cuerpo F tendría un subcuerpo con infinitos elementos. Contradicción. Luego F tiene como cuerpo primo a $\mathbb{Z}_p$ y tiene característica p.
El único isomorfismo que existe entre el cuerpo primo de F y $\mathbb{Z}_p$ es el que aplica 1_F en $1_{\mathbb{Z}_p}$. Este isomorfismo identifica el cuerpo primo de F con $\mathbb{Z}_p$ y puede verse a F como una extensión finita de $\mathbb{Z}_p$.
Si $[F : \mathbb{Z}_p] = n$ entonces el $\mathbb{Z}_p-$espacio vectorial F tiene una base con n elementos. Luego si $x \in F$, x puede escribirse de la siguiente manera:

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \text{ donde } \alpha_i \in \mathbb{Z}_p,\ 1 \leq i \leq n$$

donde $\{v_1, v_2, \ldots, v_n\}$ es una base del $\mathbb{Z}_p$-espacio vectorial F. De aquí resulta que el cardinal del cuerpo F depende de los escalares $\alpha_i,\ 1 \leq i \leq n$ y como cada uno de ellos puede tomar p valores distintos resulta que F tiene p^n elementos. □

La recíproca de la proposición anterior es falsa pues $\mathbb{Z}_p(X)$ es un cuerpo infinito de característica p.

Corolario 2.3.3 *Sea F un cuerpo finito con p^n elementos. Entonces todo elemento de F es raíz del polinomio $f(X) = X^{p^n} - X = 0$.*

Corolario 2.3.4 *Si F es un cuerpo con p^n elementos entonces F es el cuerpo de raíces del polinomio $f(X) = X^{p^n} - X$ sobre su cuerpo primo.*

Por lo demostrado anteriormente se tiene el siguiente

Teorema 2.3.5 *Dos cuerpos finitos con el mismo número de elementos son isomorfos.*

A continuación veremos cómo construir a partir de un primo p y $n \in \mathbb{N}$ un cuerpo con p^n elementos.

Teorema 2.3.6 *Sea p un número primo y n un entero tal que $n \geq 1$. Entonces existe un cuerpo F con p^n elementos.*

Demostración: El polinomio $f(X) = X^{p^n} - X \in \mathbb{Z}_p[X]$ no tiene raíces múltiples ya que $f'(X) = -1$ y $(f, f') = 1$. Luego $f(X)$ tiene p^n raíces distintas en una clausura algebraica $\overline{\mathbb{Z}_p}$. Veamos que estas p^n raíces forman un subcuerpo de $\overline{\mathbb{Z}_p}$.
Sean $\alpha, \beta \in \overline{\mathbb{Z}_p}$ raíces de $f(X)$. Entonces como $\overline{\mathbb{Z}_p}$ tiene característica p resulta
$(\alpha \pm \beta)^{p^n} - (\alpha \pm \beta) = \alpha^{p^n} \pm \beta^{p^n} - \alpha \mp \beta = 0$, y $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$.
Luego $(\alpha\beta)^{p^n} - \alpha\beta = 0$.
Si $\alpha \neq 0$ entonces $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$.
Hemos probado que las raíces del polinomio $f(X) = X^{p^n} - X \in \mathbb{Z}_p[X]$ forman un cuerpo con p^n elementos, que notaremos con $F(p^n)$. □

A partir de los resultados anteriores hemos demostrado el siguiente

Teorema 2.3.7 *Dado un primo p y una clausura algebraica $\overline{\mathbb{Z}_p}$, para cada $n \in \mathbb{N}$, existe un único un subcuerpo de $\overline{\mathbb{Z}_p}$ con p^n elementos. Este subcuerpo es el cuerpo de raíces $F(p^n)$ del polinomio $f(X) = X^{p^n} - X$ sobre $\mathbb{Z}_p$.*

Corolario 2.3.5 *Toda extensión finita de un cuerpo finito es normal.*

Demostración: Toda extensión finita de un cuerpo finito es un cuerpo finito $F(p^m)$. Luego es el cuerpo de raíces del polinomio $X^{p^m} - X \in \mathbb{Z}_p[X]$. Por el Teorema 2.2.4 resulta que esta extensión es normal. □

Corolario 2.3.6 *Sea $F(p^n)$ un cuerpo finito y $\overline{F(p^n)}$ una clausura algebraica. Para cada número natural m existe en $\overline{F(p^n)}$ una única extensión de $F(p^n)$ de grado m, que es el cuerpo $F(p^{nm})$.*

Demostración: Es suficiente probar el corolario para el caso en que $F(p^n)$ sea un subcuerpo de una clausura algebrica $\overline{\mathbb{Z}_p}$.
El cuerpo de raíces de $f(X) = X^{p^{nm}} - X$ sobre $\mathbb{Z}_p$ es $F(p^{nm})$. Veamos que $F(p^n) \subset F(p^{nm})$. Demostremos haciendo inducción sobre t que, si $\alpha \in F(p^n)$ entonces $\alpha \in F(p^{nt})$.
Si $t = 1$ la proposición se verifica trivialmente.
Supongamos que la proposición es válida para $t \in \mathbb{N}$ con $t > 1$ y probemos que $\alpha \in F(p^{n(t+1)})$. Dado $\alpha \in F(p^n)$,

$$\alpha^{p^{n(t+1)}} = \alpha^{p^{nt} \cdot p^n} = (\alpha^{p^n})^{p^{nt}} = \alpha^{p^{nt}} = \alpha,$$

y en particular $\alpha^{p^{nm}} = \alpha$.
Como $\mathbb{Z}_p \subset F(p^n) \subset F(p^{nm})$ resulta que

$$[F(p^{nm}) : \mathbb{Z}_p] = [F(p^{nm}) : F(p^n)][F(p^n) : \mathbb{Z}_p],$$

$$[F(p^{nm}) : \mathbb{Z}_p] = nm \quad \text{y} \quad [F(p^n) : \mathbb{Z}_p] = n.$$

Luego $[F(p^{nm}) : F(p^n)] = m$. □

A continuación veremos que toda extensión finita de un cuerpo finito es separable.

Definición 2.3.3 *Decimos que un cuerpo K es* **perfecto** *si todo polinomio no constante de $K[X]$ es separable.*

Todo cuerpo algebraicamente cerrado es perfecto. En general si $car(K) = 0$, un polinomio irreducible $f \in K[X]$ tiene a su derivado f' no nulo. Luego f no tiene raíces múltiples y en consecuencia es un polinomio separable.

Definición 2.3.4 *Sea K un cuerpo de característica $p \neq 0$, la aplicación $\sigma : K \longrightarrow K$ definida por $\sigma(x) = x^p$, es un homomorfismo de anillos llamado* **homomorfismo de Frobenius**.
La imagen de σ es un subcuerpo de K que indicaremos con K^p.

Teorema 2.3.8 *Las siguientes proposiciones son equivalentes:*

a) K es un cuerpo perfecto.

b) La característica de K es cero, o es un número primo p y $K^p = K$.

c) Toda extensión algebraica de K es separable.

Demostración: Probemos la equivalencia de *a*) y *b*). Si K es un cuerpo perfecto entonces $car(K) = 0$ ó $car(K) = p$ con p primo y $K^p = K$.
En efecto, supongamos que la característica de K es distinta de cero y consideremos $\alpha \in K$ y $\beta \in \overline{K}$ una raíz del polinomio $f(X) = X^p - \alpha \in K[X]$, esto es, $\beta^p = \alpha$.

Como el polinomio minimal de β sobre K divide a $f(X) = X^p - \alpha = (X - \beta)^p$, entonces es de la forma $(X - \beta)^q$, pero como K es perfecto resulta que $q = 1$, pues en caso contrario el polinomio minimal tendría raíces múltiples. Luego el polinomio minimal de β sobre K es $X - \beta$ y $\beta \in K$. Luego $K^p = K$.
Recíprocamente, si K es un cuerpo de característica cero entonces es perfecto. Sea K un cuerpo de característica p, p primo tal que $K^p = K$ y supongamos que K no es perfecto. Luego existe un polinomio $g \in K[X]$ irreducible, mónico y no separable. Entonces $g' = 0$ y g es de la forma

$$g(X) = h(X^p) = a_0 + a_1X^p + a_2X^{2p} + \ldots + a_nX^{np}, \quad n \geq 1, \ y \ a_n \neq 0$$

Como $K^p = K$, para cada a_i existe $b_i \in K$, tal que $a_i = b_i^p$, con $1 \leq i \leq n$. Luego

$$g(X) = (b_0 + b_1X + b_2X^2 + \ldots + b_nX^n)^p,$$

y por lo tanto g no es irreducible. Contradicción. En consecuencia K es perfecto.
Veamos ahora que K es un cuerpo perfecto si y sólo si toda extensión algebraica de K es separable.
Sea K un cuerpo perfecto, E es una extensión algebraica de K y $\alpha \in E$. Como α es algebraico sobre K y su polinomio minimal es separable sobre K entonces α es separable sobre K.
Supongamos que toda extensión algebraica de K es separable. Si f es un polinomio irreducible de $K[X]$ que tiene una raíz α, entonces la extensión $K(\alpha)$ de K es algebraica y separable. Luego el polinomio minimal de α es separable sobre K y todo polinomio irreducible de $K[X]$ es separable sobre K, de donde resulta que K es perfecto. □

Corolario 2.3.7 *Sea $F(p^n)$ un cuerpo con p^n elementos. Entonces la aplicación $\sigma : F(p^n) \longrightarrow F(p^n)$ definida por $\sigma(x) = x^p$ es un automorfismo de cuerpos.*

Demostración: La aplicación σ es un monomorfismo ya que de la igualdad $x^p = y^p$ resulta que $x^{p^n} = y^{p^n}$, y como los elementos de $F(p^n)$ son las raíces del polinomio $f(X) = X^{p^n} - X$, se sigue que $x = y$. Además σ está definida sobre conjuntos finitos y por lo tanto es sobreyectiva. □

De los resultados anteriores se deduce que toda extensión finita de un cuerpo finito es una extensión de Galois.

En lo que sigue estudiaremos el grupo de automorfismos de un cuerpo finito $F(p^n)$.

Definición 2.3.5 *Sea K un subcuerpo de F. El grupo de todos los $K-$automorfismos de F se llama* **grupo de Galois** *de F sobre K y se nota $G(F/K)$.*

Teorema 2.3.9 *El grupo de automorfismos de $F(p^n)$, $Aut(F(p^n))$, es un grupo cíclico de orden n con generador σ.*

Demostración: Como $\sigma^n(x) = x^{p^n} = x$, cualquiera sea $x \in F(p^n)$, entonces $\sigma^n = id$.
Sea t el orden del automorfismo σ. Entonces $t \leq n$ y dado $x \in F(p^n)$ resulta $\sigma^t(x) = x^{p^t} = x$. Como el polinomio $f(X) = X^{p^t} - X$ tiene a lo sumo p^t raíces, resulta $p^t \geq p^n$ y de aquí que $t = n$.
Veamos que σ es un generador del grupo $Aut(F(p^n))$. Si $\phi \in Aut(F(p^n)$ entonces ϕ deja fijo los elementos de su cuerpo primo $\mathbb{Z}_p$, es decir, ϕ es un $\mathbb{Z}_p-$automorfismo. Además el número de $\mathbb{Z}_p-$automorfismo de $F(p^n)$ es n, ya que $F(p^n)$ es una extensión finita, normal y separable de $\mathbb{Z}_p$. Luego $Aut(F(p^n)) = (\sigma)$. □

Teorema 2.3.10 *Sean $n, m \in \mathbb{N}$, $\overline{\mathbb{Z}_p}$ una clausura dada y $F(p^n)$, $F(p^m)$ subcuerpos de $\overline{\mathbb{Z}_p}$. Entonces $F(p^n) \subset F(p^m)$ si y sólo si n divide a m. Si $F(p^n) \subset F(p^m)$, $F(p^m)$ es una extensión normal y separable de $F(p^n)$ de grado $\frac{m}{n}$ y el grupo de $F(p^n)-$automorfismos de $F(p^m)$ es cíclico, generado por σ^n, siendo σ el automorfismo de Frobenius de $F(p^m)$.*

Demostración: Si $F(p^n) \subset F(p^m)$ entonces

$$[F(p^m) : \mathbb{Z}_p] = [F(p^m) : F(p^n)][F(p^n) : \mathbb{Z}_p].$$

Como $[F(p^m) : \mathbb{Z}_p] = m$ y $[F(p^n) : \mathbb{Z}_p] = n$ resulta que n divide a m.
Recíprocamente, supongamos que n divide a m. Por el Corolario 2.3.6, $F(p^n)$ tiene una única extensión de grado $\frac{m}{n}$ en $\overline{\mathbb{Z}_p}$ que es el cuerpo $F(p^m)$. Luego $F(p^n) \subset F(p^m)$.
Sea $F(p^n) \subset F(p^m)$. El cuerpo $F(p^m)$ es una extensión de Galois de $\mathbb{Z}_p$. Por el Teorema 2.2.5 y como las extensiones separables verifican la propiedad transitiva, resulta que $F(p^m)$ es una extensión de Galois de $F(p^n)$. □

Teorema 2.3.11 *Sea F una extensión de K y H un subgrupo del grupo $G(F/K)$. Entonces el conjunto*

$$F^H = \{x \in F : \sigma(x) = x,\ \sigma \in H\}$$

es un cuerpo.

Definición 2.3.6 *Dada una extensión F de K y H un subgrupo del grupo $G(F/K)$, el cuerpo*

$$F^H = \{x \in F : \sigma(x) = x, \sigma \in H\}$$

se llama **cuerpo fijo** *de H.*

Definición 2.3.7 *Sea F una extensión de un cuerpo K tal que el cuerpo fijo del grupo de Galois $Aut_K(F)$ es K. Entonces F se llama* **cuerpo de Galois** *o* **extensión de Galois** *de K.*

2.4. Teorema de la base normal

En esta sección comenzaremos estudiando la descomposición de un endomorfismo para luego dar una demostración del Teorema de la base normal. Primero daremos la demostración para el caso infinito y luego la del caso finito, que no se encuentra en la literatura usual.

Dado un cuerpo K y un espacio vectorial F de dimensión finita n sobre K, consideremos un homomorfismo $f \in End_K(F)$.

Si t es un elemento trascendente sobre K definimos la representación del anillo de polinomios $K[t]$ en F como sigue:

La aplicación

$$\psi : K[t] \longrightarrow K[f] \subseteq End_K(F)$$

definida por

$$\psi(p(t)) = p(f)$$

tal que para cada $v \in F$,

$$p(t)(v) = p(f)(v),$$

es un homomorfismo de anillos.

El espacio vectorial $K[f]$ tiene dimensión finita sobre K pues $K[f] \subseteq End_K(F) \cong M_n(K)$.

Como $K[t]$ es un dominio principal, $Ker(\psi)$ es un ideal principal de $K[t]$ y $Ker(\psi) \neq \{0\}$ pues la dimensión de $K[f]$ sobre K es finita. Luego $Ker(\psi) = (q_f)$ donde $gr(q_f) > 0$ y q_f es mónico.

Definición 2.4.1 *El polinomio q_f recién definido se llama* **polinomio minimal de f sobre K.**

Si existe un elemento $w \in F$ tal que $F = K[t]w = K[f]w$ entonces F está generado sobre K por los elementos

$$w,\ f(w),\ f^2(w),\ f^3(w),\ \ldots\ .$$

Al $K[t]$-módulo $F = (w)$ lo llamamos **módulo principal**.

Proposición 2.4.1 *Sea q_f el polinomio minimal de f sobre K.*

Si el polinomio $q_f(t)$ es de la forma $q_f(t) = t^d + a_{d-1}t^{d-1} + \ldots + a_0$ entonces el conjunto

$$\{w, f(w), f^2(w), \ldots, f^{d-1}(w)\}$$

es una base de F sobre K.

Demostración: El conjunto $\{w, f(w), f^2(w), \ldots, f^{d-1}(w)\}$ es linealmente independiente. En efecto, sea

$$k_0 w + k_1 f(w) + k_2 f^2(w) + \ldots + k_{d-1} f^{d-1}(w) = 0 \quad (1)$$

con $k_i \in K,\ 0 \leq i \leq d-1$ y el polinomio $g(t) = k_0 + k_1 t + k_2 t^2 + \ldots + k_{d-1} t^{d-1} \in K[t]$. Como F es un $K[t]$-módulo principal, $g(t) \in Ker(\psi)$ si y sólo si $g(f)(w) = 0$. Luego por (1) resulta que $g(t) \in Ker(\psi) = (q_f)$ y que $g(t) = s(t)q_f(t)$. Como $gr(g) < gr(q_f)$ entonces $g(t) = 0$, y por lo tanto $k_i = 0$ cualquiera sea $i,\ 0 \leq i \leq d-1$. Veamos a continuación que $\{w, f(w), f^2(w), \ldots, f^{d-1}(w)\}$ genera a F.
Como $F = K[f]w$, si $v \in F$ existe $p(f) \in K[f]$ tal que $v = p(f)w$. Dividiendo a p por q_f resulta $p(t) = m(t)q_f(t) + r(t)$, con $gr(r) < gr(q_f)$. Luego aplicando ψ obtenemos $p(f) = r(f)$, i.e. $p(f) = k_0 + k_1 f + k_2 f^2 + \ldots + k_l f^l$ con $l \leq d-1$ y $v = k_0 w + k_1 f(w) + k_2 f^2(w) + \ldots + k_l f^l(w)$. □

La matriz de f en la base $\{w, f(w), f^2(w), \ldots, f^{d-1}(w)\}$ tiene la siguiente forma:

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & -a_{d-2} \\ 0 & 0 & 0 & \ldots & 1 & -a_{d-1} \end{bmatrix}$$

Si $F = (w)$ entonces $F \cong K[t]/(q_f)$ ya que la aplicación $\mu : K[t] \longrightarrow F$ definida por $\mu(p(t)) = p(f)(w)$ es sobreyectiva y $Ker(\mu) = (q_f)$.

El polinomio q_f está unívocamente determinado por f y no depende de w. Este polinomio se llama **polinomio invariante de F con respecto a f.**

La demostración del teorema que sigue puede encontrarse en [24].

Teorema 2.4.1 *Sea F un espacio vectorial no nulo de dimensión finita sobre K, y $f \in End_K(F)$. Entonces F puede descomponerse en suma directa*

$$F = F_1 \oplus \ldots \oplus F_r$$

donde cada F_i es un $K[f]$-submódulo principal, con polinomio invariante no nulo q_i tal que q_i divide a q_j, si $i \leq j$. Los polinomios $q_1, q_2, \ldots, q_r$ están unívocamente determinados por F y f, y el polinomio q_r es el polinomio minimal de f.

Corolario 2.4.1 *Sea F un espacio vectorial no nulo de dimensión finita sobre K y $f \in End_K(F)$. Entonces F es un $K[f]$-módulo principal si y sólo si tiene un único factor invariante.*

A continuación daremos la demostración del Teorema de la base normal. Este teorema nos permitirá construir una base del $F(p^n)$ espacio vectorial $\mathbb{Z}_{p^n}$.

Definición 2.4.2 *Sea C un cuerpo algebraicamente cerrado, K, E y F subcuerpos de C tales que $K \subset E \cap F$. Decimos que E es* **linealmente disjunto** *de F sobre K si todo conjunto finito de elementos de E que es linealmente independiente sobre K, también lo es sobre F.*

Ejemplos 2.4.1 *Dados K y E cuerpos,*

1. *Si $K \subset E$ entonces E y K son linealmente disjuntos sobre K.*
2. *En la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\pi)$, el cuerpo $\mathbb{Q}(\pi)$ es linealmente disjunto de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.*
3. *Dada la extensión $\mathbb{Q} \subset \mathbb{Q}(e) \cap \mathbb{Q}(X_1, X_2, \ldots, X_n)$, el cuerpo $\mathbb{Q}(X_1, X_2, \ldots, X_n)$ es linealmente disjunto de $\mathbb{Q}(e)$ sobre $\mathbb{Q}$.*

La definición de linealmente disjunto sobre un cuerpo no es simétrica. Sin embargo la propiedad de ser linealmente disjunta para E y F si lo es.

Teorema 2.4.2 *Sea C un cuerpo algebraicamente cerrado y K, E y F subcuerpos de C tales que $K \subset E \cap F$. Entonces E es linealmente disjunto de F sobre K si y sólo si F es linealmente disjunto de E sobre K.*

Demostración: Es suficiente probar que si E es linealmente disjunto de F sobre K entonces F es linealmente disjunto de E sobre K.
Supongamos que existe un conjunto $X \subseteq F$ que es linealmente independiente sobre K pero no lo es sobre E. Entonces para algunos $u_i \in X$ y $r_i \in E$ no todos nulos resulta $r_1u_1 + r_2u_2 + \ldots + r_nu_n = 0$.
Tomemos un subconjunto de $\{r_1, r_2, \ldots, r_n\}$ linealmente independiente maximal sobre K, por ejemplo $\{r_1, r_2, \ldots, r_t\}$, reordenando los índices si fuese necesario. Entonces para cada $j > t$ resulta

$$r_j = \sum_{i=1}^{t} a_{ij} r_i \quad \text{con } a_{ij} \in K,$$

y

$$0 = \sum_{j=1}^{n} r_j u_j = \sum_{j=1}^{t} r_j u_j + \sum_{j=t+1}^{n} (\sum_{i=1}^{t} a_{ij} r_i) u_j = \sum_{k=1}^{t} (u_k + \sum_{j=t+1}^{n} a_{kj} u_j) r_k.$$

Como E y F son linealmente disjuntos sobre K entonces $\{r_1, r_2, \ldots, r_t\}$ es linealmente independiente sobre F y por lo tanto

$$u_k + \sum_{j=t+1}^{n} a_{kj} u_j = 0 \text{ cualquiera sea } k \leq t,$$

lo que contradice la independencia lineal de X sobre K. Luego X es linealmente independiente sobre E. □

Los teoremas que siguen nos indican cuando una extensión es linealmente disjunta de otra sobre un cuerpo K.

Teorema 2.4.3 *Sea C un cuerpo algebraicamente cerrado, con subcuerpos K, E y F tales que $K \subset E \cap F$. Sea R un subanillo de E tal que $K(R) = E$ y $K \subset R$. Si todo subconjunto de R que es linealmente independiente sobre K también lo es sobre F entonces E y F son linealmente disjuntos sobre K.*

Demostración: Sea $X = \{u_1, u_2, \ldots, u_n\}$ un subconjunto finito de E linealmente independiente sobre K y probemos que X es linealmente independiente sobre F. Como para cada $i,\ 1 \leq i \leq n$, $u_i \in E = K(R)$, resulta $u_i = c_i d_i^{-1}$ donde
$c_i = f_i(r_1, r_2, \ldots, r_{t_i})$,
$0 \neq d_i = g_i(r_1, r_2, \ldots, r_{t_i})$, para $r_j \in R,\ 1 \leq j \leq t_i$ y
$f_i, g_i \in K[X_1, X_2, \ldots, X_{t_i}]$.
Sea $d = d_1 d_2 \ldots d_n$ y para cada $i,\ 1 \leq i \leq n$ sea v_i un elemento de R definido por:

$$v_i = c_i d_1 \ldots d_{i-1} d_{i+1} \ldots d_n.$$

Entonces $u_i = v_i d^{-1}$ y el conjunto $X' = \{v_1, v_2, \ldots, v_n\} \subseteq R$ es linealmente independiente sobre un subcuerpo de C si y sólo si X lo es. Como por hipótesis X es linalmente independiente sobre K,entonces X' es linealmente independiente sobre K. Luego X' es linealmente independiente sobre F y de aquí resulta que X es linealmente independiente sobre F. □

Teorema 2.4.4 *Dado un cuerpo algebraicamente cerrado C, y K, E y F subcuerpos de C tales que $K \subset E \cap F$, consideremos un subanillo R de E, tal que E es su cuerpo de cocientes y R es un espacio vectorial sobre K. Si $\{u_i\}$ es una base de R sobre K entonces para probar que E y F son linealmente disjuntos sobre K es suficiente mostrar que el conjunto $\{u_i\}$ es linealmente independiente sobre F.*

Demostración: Supongamos que la base $\{u_i\}$ es linealmente independiente sobre F y tomemos $r_1, r_2, \ldots, r_m$ elementos de R linealmente independientes sobre K. Como estos elementos están en un subespacio vectorial S de dimensión finita generado por algunos de los elementos del conjunto $\{u_i\}$, supongamos sin pérdida de generalidad que son $u_1, u_2, \ldots, u_n$. Entonces el conjunto $\{r_1, r_2, \ldots, r_m\}$ puede extenderse a una base $\mathcal{B}$ de S sobre K y el espacio vectorial generado por $u_1, u_2, \ldots, u_n$ sobre F tiene dimensión n, ya que estos vectores son linealmente independientes sobre F por hipótesis y además coincide con el espacio generado por $\mathcal{B}$. Luego $r_1, r_2, \ldots, r_m$ son linealmente independientes sobre F. Aplicando el Teorema 2.4.3, resulta que E y F son linealmente disjuntos sobre K. □

La demostración del Teorema de la base normal en el caso infinito, se basa en el siguiente teorema de independencia lineal de automorfismos, [24].

Teorema 2.4.5 *Sea K un cuerpo infinito y $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ un grupo de automorfismos de un cuerpo K y $p \in K[x_1, \ldots, x_n]$, entonces*

$$p(\sigma_1(v), \sigma_2(v), \ldots, \sigma_n(v)) = 0$$

para todo $v \in K$ si y sólo si $p = 0$.

Demostraremos primero el teorema de la base normal para un cuerpo K infinito. Para probar el teorema para el caso finito se necesita la demostración anterior y algunos resultados de la teoría de representación de grupos.

Teorema 2.4.6 (Teorema de la base normal) *Sea F una extensión de Galois de un cuerpo K finita de grado n y $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ el grupo de Galois de F. Entonces existe un elemento $w \in F$ tal que $\{\sigma_1(w), \sigma_2(w), \ldots, \sigma_n(w)\}$ es un base del $K-$espacio vectorial F.*

Demostración: Sea K un cuerpo infinito, F una extensión de Galois de K y $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ el grupo de Galois. Para cada $\sigma_i \in G$ construimos la matriz $A = (a_{ij})$ de la siguiente manera

$$a_{ij} = x_k \text{ si } \sigma_i^{-1}\sigma_j = \sigma_k, \text{ para } 1 \leq i, j, k \leq n.$$

Consideremos la función $p(x_1, \ldots, x_n) = det(a_{ij})$. Es claro que p no es idénticamente nulo pues $p(1, 0, \ldots, 0) = det(I) = 1$.
Por el Teorema 2.4.5 existe $w \in F$ tal que $p(\sigma_1(w), \ldots, \sigma_n(w)) \neq 0$, y de aquí resulta que $det(\sigma_i^{-1}\sigma_j(w)) \neq 0$. Probemos que a partir de esta última condición se tiene que

$$\{\sigma_1(w),\ \sigma_2(w),\ \ldots,\ \sigma_n(w)\}$$

es una base del K espacio vectorial F. Es suficiente probar que $\{\sigma_1(w), \sigma_2(w), \ldots, \sigma_n(w)\}$ es linealmente independiente pues $[F : K] = n$. Sea

$$\lambda_1\sigma_1(w) + \lambda_2\sigma_2(w) + \ldots + \lambda_n\sigma_n(w) = 0, \quad \lambda_i \in K, \quad 1 \leq i \leq n.$$

Aplicando σ_i^{-1}, tenemos

$$\lambda_1\sigma_i^{-1}\sigma_1(w) + \lambda_2\sigma_i^{-1}\sigma_2(w) + \ldots + \lambda_n\sigma_i^{-1}\sigma_n(w) = 0.$$

Como $det(\sigma_i^{-1}\sigma_j(w)) \neq 0$ entonces $\lambda_i = 0$ para todo $1 \leq i \leq n$.

A continuación daremos la demostración para el caso finito.
Sea K un cuerpo finito y F una extensión finita de K. Sabemos que F es una extensión de Galois sobre K con grupo de Galois $G = (\sigma)$, siendo $\sigma \in End_K(F)$ el automorfismo de Frobenius. Sea t un elemento trascendente sobre K. Vimos al comienzo de esta sección que la aplicación

$$\psi : K[t] \longrightarrow K[\sigma] \subseteq End_K(F)$$

$$p(t) \longrightarrow p(\sigma)$$

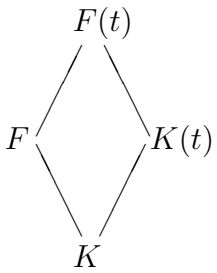
tal que para cada $v \in F,\ p(t)(v) = p(\sigma)(v)$, es un homomorfismo de anillos.
Veamos primero que demostrar el teorema de la base normal en el caso finito es equivalente a probar que F es un $K[t]$-módulo principal.
Supongamos que F es un $K[t]$-módulo principal. Luego existe $w \in F$ tal que $F = K[t]w$ y dado $v \in F,\ v = p(t)w$. Aplicando ψ resulta $v = p(\sigma)w$, i.e.,

$$v = k_0 + k_1\sigma(w) + \ldots + k_r\sigma^r(w) \quad \text{con } r \leq n-1.$$

Luego $\{w, \sigma(w), \ldots, \sigma^{n-1}(w)\}$ es un conjunto de generadores de F sobre K y como $[F : K] = n$ entonces $\{w, \sigma(w), \ldots, \sigma^{n-1}(w)\}$ es una base de F sobre K.
Recíprocamente supongamos que existe $w \in F$ tal que $\{w, \sigma(w), \ldots, \sigma^{n-1}(w)\}$ es una base de F sobre K. Luego existen $k_0, k_1, \ldots, k_{n-1} \in K$ tal si $v \in F$ entonces

$$v = k_0 + k_1\sigma(w) + \ldots + k_{n-1}\sigma^{n-1}(w).$$

Tomando $p(t) = k_0 + k_1t + \ldots + k_{n-1}t^{n-1}$ resulta por la acción de ψ que $v = p(t)w$, i.e., F es un $K[t]-$ módulo principal generado por w.
Por el Corolario 2.4.1 para probar que el $K[t]-$módulo F es principal, debemos ver que tiene un único factor invariante. Consideremos el siguiente diagrama de extensiones



Veamos que la extensión F es linealmente disjunta de $K(t)$ sobre K. Como $K(t)$ es el cuerpo cociente de $K[t]$ y $K[t]$ es un espacio vectorial sobre K, la base $\{1, t, t^2, \ldots\}$ es linealmente independiente sobre F por ser t trascendente. Luego por el Teorema 2.4.4 resulta que F y $K(t)$ son linealmente disjuntos sobre K.
La aplicación

$$\tau : G(F(t)/K(t)) \longrightarrow G(F/K)$$

definida por $\tau(\mu) = \mu/K$ es un isomorfismo de grupos.
A partir del automorfismo de Frobenius σ definimos $\overline{\sigma} \in G(F(t)/K(t))$ de la siguiente manera:

$$\overline{\sigma}\left(\frac{a_0 + a_1x + \ldots + a_sx^s}{b_0 + b_1x + \ldots + b_lx^l}\right) = \frac{\sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_s)x^s}{\sigma(b_0) + \sigma(b_1)x + \ldots + \sigma(b_l)x^l}$$

El automorfismo $\overline{\sigma}$ extiende a σ y es un generador de $G(F(t)/K(t))$. Además $F(t)$ es una extensión de $K(t)$ de grado n.
Veamos que si $\{v_1, \ldots, v_n\}$ es una base de F sobre K entonces es una base de $F(t)$ sobre $K(t)$. El conjunto $\{v_1, \ldots, v_n\} \subseteq F$ es linealmente independiente sobre K y como $F \subset F(t)$ entonces $\{v_1, \ldots, v_n\}$ es linealmente independiente sobre $K(t)$ ya que F y $K(t)$ son linealmente disjuntos sobre K. Además como $[F(t) : K(t)] = n$ resulta que $\{v_1, \ldots, v_n\}$ es una base de $F(t)$ sobre $K(t)$.
Las matrices de σ y $\overline{\sigma}$ en la base $\{v_1, \ldots, v_n\}$ coinciden. Luego los factores invariantes de σ y $\overline{\sigma}$ son los mismos. Como $F(t)$ es infinito y el teorema de la base normal lo hemos demostrado al comienzo de esta demostración, $\overline{\sigma}$ tiene un único factor invariante. Luego σ tiene un único factor invariante y queda demostrado el teorema de la base normal para el caso finito. $\square$

Capítulo 3

Equivalencia entre variedades de álgebras de Post cíclicas de orden p y variedades generadas por cuerpos finitos

H. Cendra presenta en *Cyclic Boolean algebras and Galois fields* $F(2^k)$ [10] un método contructivo para definir un álgebra de Boole $k-$cíclica simple $\langle A; T\rangle$ sobre un cuerpo finito con 2^k elementos y muestra el camino recíproco.
En este capítulo extendemos el resultado de H. Cendra para cuerpos finitos con p^k elementos y álgebras de Post de orden p, $k-$cíclicas, siendo p un primo positivo y $k \geq 1$.

Damos un método constructivo que transforma un cuerpo $\langle F(p^k); +, \cdot, F(p)\rangle$ en un álgebra de Post de orden p, $k-$cíclica con p primo y $k \geq 1$, y expresamos las operaciones del álgebra de Post como términos en el lenguaje de los cuerpos. Recíprocamente, también obtenemos las operaciones del cuerpo como términos en el lenguaje de las álgebras de Post $k-$cíclicas de orden p.

Si $\mathcal{V}(L_{p,k})$ es la variedad generada por las álgebras de Post de orden p, $k-$cíclicas y $\mathcal{V}(F(p^k))$ es la variedad generada por los cuerpos con p^k elementos $\langle F(p^k); +, \cdot, F(p)\rangle$, probamos que existe una interpretación Φ_1 de $\mathcal{V}(L_{p,k})$ en $\mathcal{V}(F(p^k))$ y una interpretación Φ_2 de $\mathcal{V}(F(p^k))$ en $\mathcal{V}(L_{p,k})$ tal que $\Phi_2\Phi_1(A) = A$, cualquiera sea el álgebra $A \in \mathcal{V}(L_{p,k})$ y $\Phi_1\Phi_2(R) = R$, para todo $R \in \mathcal{V}(F(p^k))$. De esta manera obtenemos una equivalencia entre las variedades $\mathcal{V}(L_{p,k})$ y $\mathcal{V}(F(p^k))$. Estos resultados han sido publicados en [1].

En la primera sección introducimos los polinomios de Lagrange sobre el cuerpo $F(p^k)$ y los polinomios de Lagrange sobre el álgebra $L_{p,k}$ y mostramos que ambos son términos discriminadores. El método de interpolación de Lagrange descripto por Moisil en [31] nos permite dar una representación de una función $f : (F(p^k))^m \longrightarrow F(p^k)$ como un polinomio con coeficientes en el cuerpo $F(p^k)$ y a partir de un procedimento similar podemos expresar toda función de $(L_{p,k})^m$ en $L_{p,k}$ como un

polinomio con coeficientes en el álgebra.

En la segunda sección presentamos uno de los resultados más importantes de esta tesis. Demostramos la equivalencia entre las variedades $\mathcal{V}(L_{p,k})$ y $\mathcal{V}(F(p^k))$, resultado que aplicaremos en los capítulos 5 y 6.

Para finalizar, en la última sección damos dos ejemplos que muestran claramente el proceso constructivo descripto en la primera, incluyendo las operaciones cuyos programas se detallan en el apéndice.

3.1. Polinomios de Lagrange en $F(p^k)$ y en $L_{p,k}$

En el capítulo anterior demostramos que dado un primo p y un número natural k, existe un único cuerpo F con p^k elementos, a menos de isomorfismo, que llamamos $F(p^k)$.

A los efectos de utilizar la notación de álgebra universal dada en el primer capítulo, notaremos al cuerpo $F(p^k)$ por $\langle F(p^k); +, \cdot, F(p)\rangle$, teniendo en cuenta que el cuerpo primo $F(p)$ es el conjunto de constantes del álgebra.

A partir de un conjunto con p^k elementos y una estructura de cuerpo finito $F = F(p^k)$ definida sobre él, construimos el anillo de funciones $\langle F^{F^m}; +, \cdot\rangle$ que consiste en las aplicaciones

$$f : F^m \longrightarrow F$$

con las operaciones de suma y producto definidas de la siguiente manera:

$(f + g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) + g(x_1, x_2, \ldots, x_m)$,

$(f \cdot g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) \cdot g(x_1, x_2, \ldots, x_m)$.

Al anillo de polinomios en m indeterminadas sobre el cuerpo F, lo notamos $\langle F[x_1, x_2, \ldots, x_m]; +, \cdot\rangle$.

Lema 3.1.1 *Toda función $f \in F^{F^m}$ puede representarse de una única manera como un polinomio $\sum_i \lambda_i \cdot M_i$ con $\lambda_i \in F(p^k)$, $M_i = x_1^{r_{i_1}} \cdot x_2^{r_{i_2}} \cdot \ldots \cdot x_m^{r_{i_m}}$ y $0 \leq r_{i_j} < p^k$.*

Demostración: Todo polinomio define una función de manera natural [24]. Luego la aplicación

$$\psi : F[x_1, x_2, \ldots, x_m] \longrightarrow F^{F^m}$$

restringida al conjunto de polinomios de la forma $p(x_1, x_2, \ldots, x_m) = \sum_i \lambda_i \cdot M_i$, con $\lambda_i \in F(p^k)$, $M_i = x_1^{r_{i_1}} \cdot x_2^{r_{i_2}} \cdot \ldots \cdot x_m^{r_{i_m}}$ y $0 \leq r_{i_j} < p^k$, es inyectiva.

Como los monomios $M_i = x_1^{r_{i_1}} \cdot x_2^{r_{i_2}} \cdot \ldots \cdot x_m^{r_{i_m}}$ con $0 \leq r_{i_j} < p^k$ son p^{km}, existen $(p^k)^{p^{km}}$ polinomios de la forma $\sum_i^{p^{km}} \lambda_i \cdot M_i$, y este número coincide con el cardinal del anillo F^{F^m}. □

El **método de interpolación de Lagrange** dado por Moisil en [31], permite dar una representación de una función $f \in F^{F^m}$, siendo $F = F(p^k)$, $F(p^k) = \{0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p^k-1}\}$, a partir de los polinomios de Lagrange siguientes:

$$L_0(x) = (p-1)x^{p^k-1} + 1 \quad \text{y}$$

$$L_{\varepsilon^i}(x) = L_0(x + (p-1)\varepsilon^i).$$

De la identidad $x^{p^k} + (p-1)x = 0$, resulta:

$$L_0(x) = \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{si } x \neq 0 \end{cases} \quad \text{y} \quad L_{\varepsilon^i}(x) = \begin{cases} 1 & \text{si } x = \varepsilon^i \\ 0 & \text{si } x \neq \varepsilon^i \end{cases} .$$

Luego, para $f \in F^{F^m}$,

$$f(x_1, x_2, \ldots, x_m) = \sum_{(\alpha_1,\ldots,\alpha_m)\in F(p^k)^m} f(\alpha_1, \alpha_2, \ldots, \alpha_m) \cdot L_{\alpha_1}(x_1) \cdot \ldots \cdot L_{\alpha_m}(x_m). \quad \text{(I)}$$

Es importante destacar que los polinomios $L_0(x)$ y $L_{\varepsilon^i}(x)$ son términos switching ya que $L_0(x) = s(0, x, 1, 0)$ y $L_{\varepsilon^i}(x) = s(\varepsilon^i, x, 1, 0)$.

A continuación describimos cómo representar una función definida sobre un álgebra de Post $k-$cíclica de orden p, como un polinomio de Post con coeficientes en el álgebra. Para realizar este procedimiento utilizaremos la definición de G. Epstein [15] dada en la segunda sección del capítulo 1.

Definimos sobre el álgebra de Post simple $k-$cíclica de orden p, $L_{p,k} = \langle (L_p)^k; T \rangle$, las operaciones binarias Δ y $\odot$ de la siguiente manera:

$$C_i(x \Delta y) = \bigvee_{s+t\equiv i(mod\ p)} (C_s(x) \wedge C_t(y)),$$

$$C_i(x \odot y) = \bigvee_{s\cdot t\equiv -i(mod\ p)} (C_s(x) \wedge C_t(y)).$$

De la la definición 1.2.2 resulta:

$$x \Delta y = \bigvee_{i=0}^{p-1} (C_i(x \Delta y) \wedge e_i) \quad \text{y} \quad x \odot y = \bigvee_{i=0}^{p-1} (C_i(x \odot y) \wedge e_i).$$

A los efectos de simplificar la notación escribiremos $px = \underbrace{x \Delta x \Delta \ldots \Delta x}_{p\ veces}$ y $x^p = \underbrace{x \odot x \odot \ldots \odot x}_{p\ veces}$.

Proposición 3.1.1 $\langle (L_p)^k; \Delta, \odot \rangle$ *es un anillo conmutativo con unidad* $\mathbf{1} = e_{p-1}$.

Demostración: Es suficiente probar que $\langle L_p; \Delta, \odot \rangle$ es un anillo conmutativo con unidad $\mathbf{1}$.
Si $x \in L_p$ entonces $x = e_i$, para algún i con $0 \leq i \leq p-1$ y

$$C_j(x) = C_j(e_i) = \begin{cases} \mathbf{0} & \text{si } i \neq j \\ \mathbf{1} & \text{si } i = j \end{cases}.$$

Veamos que

$$e_i \Delta e_j = e_k \text{ si y sólo si } i + j \equiv k (mod\ p) \quad \text{y}$$
$$e_i \odot e_j = e_k \text{ si y sólo si } i \cdot j \equiv -k (mod\ p).$$

Si $k = t$ resulta $i + j \equiv t (mod\ p)$ e $i \cdot j \equiv -t (mod\ p)$. Luego

$$C_t(e_k) = \mathbf{1} = C_i(e_i) \wedge C_j(e_j) = \bigvee_{r+l \equiv t (mod\ p)} (C_r(e_i) \wedge C_l(e_j)) = C_t(e_i \Delta e_j),$$

$$C_t(e_k) = \mathbf{1} = C_i(e_i) \wedge C_j(e_j) = \bigvee_{r \cdot l \equiv -t (mod\ p)} (C_r(e_i) \wedge C_l(e_j)) = C_t(e_i \odot e_j).$$

Si $k \neq t$ tenemos que $i + j \not\equiv t (mod\ p)$ e $i \cdot j \not\equiv -t (mod\ p)$. Luego dados r, l tales que $0 \leq r, l \leq p-1$, para $r + l \equiv t (mod\ p)$ ó $r \cdot l \equiv -t (mod\ p)$ resulta

$$C_t(e_k) = \mathbf{0} = C_r(e_i) \wedge C_l(e_j) = \bigvee_{r+l \equiv t (mod\ p)} (C_r(e_i) \wedge C_l(e_j)) = C_t(e_i \Delta e_j),$$

$$C_t(e_k) = \mathbf{0} = C_r(e_i) \wedge C_l(e_j) = \bigvee_{r \cdot l \equiv -t (mod\ p)} (C_r(e_i) \wedge C_l(e_j)) = C_t(e_i \odot e_j).$$

Es fácil ver que las operaciones Δ y $\odot$ son asociativas y conmutativas. Probemos que la operación $\odot$ distribuye respecto de Δ.
Como

$$e_i \odot e_j = e_l \text{ si y sólo si } i \cdot j \equiv -l (mod\ p),$$
$$e_i \odot e_k = e_t \text{ si y sólo si } i \cdot k \equiv -t (mod\ p) \quad \text{y}$$
$$e_l \Delta e_t = e_r \text{ si y sólo si } l + t \equiv r (mod\ p),$$

entonces $i \cdot (j+k) \equiv i \cdot j + i \cdot k \equiv -(l+t) \equiv -r (mod\ p)$ y $e_i \odot (e_j \Delta e_k) = e_r$. Luego

$$e_i \odot (e_j \Delta e_k) = (e_i \odot e_j) \Delta (e_i \odot e_k).$$

Para finalizar veamos que $e_0 = \mathbf{0}$ es el elemento neutro de la operación Δ y que $e_{p-1} = \mathbf{1}$ es el neutro de $\odot$.
Como la igualdad $e_i \Delta e_0 = e_j$ es equivalente a $i + 0 \equiv j (mod\ p)$, si $0 \leq i, j \leq p-1$, entonces si $i = j$, $e_i \Delta e_0 = e_i$, cualquiera sea i, $0 \leq i \leq p-1$.

Además $e_i \odot e_{p-1} = e_j$ si y sólo si $i \cdot (p-1) \equiv -j(mod\ p)$ y esto es equivalente a que $i \equiv j(mod\ p)$. Razonando de manera análoga resulta que $e_i \odot e_{p-1} = e_i$, cualquiera sea i, con $0 \leq i \leq p-1$.
Como $e_0 = \mathbf{0}$ es el neutro para la operación Δ entonces el opuesto de cualquier constante e_i es e_j con $j \equiv -i(mod\ p)$. □

Proposición 3.1.2 *En* $L_{p,k} = \langle (L_p)^k; \Delta, \odot \rangle$ *se verifican las siguientes identidades:* $px = \mathbf{0}$, $x^p = x$, $\sim x = \mathbf{1}\Delta(p-1)x$ *y sobre la cadena de constantes*

$$x^{p-1} = \begin{cases} \mathbf{0} & si\ x = \mathbf{0} \\ e_{p-1} = \mathbf{1} & si\ x \neq \mathbf{0} \end{cases}.$$

Demostración: La demostración la hacemos sobre el álgebra L_p. De la proposición anterior resulta

$$\underbrace{i + i + \ldots + i}_{p\ veces} \equiv pi \equiv 0(mod\ p),$$

luego

$$pe_i = \underbrace{e_i \Delta e_i \Delta \ldots \Delta e_i}_{p\ veces} = e_0 = \mathbf{0}.$$

Además como

$$p - 1 + \underbrace{i + i + \ldots + i}_{p-1\ veces} \equiv p - 1 + pi - i \equiv p - i - 1(mod\ p)$$

resulta $\mathbf{1}\Delta(p-1)e_i = e_{p-1}\Delta(p-1)e_i = e_{p-i-1} = \sim e_i$.
Si $i \neq 0$ tenemos que

$$\underbrace{i \cdot i \cdot \ldots \cdot i}_{p-1\ veces} \equiv i^{p-1} \equiv p - 1(mod\ p),$$

y por lo tanto $e_i^{p-1} = e_{p-1} = \mathbf{1}$. □

En el conjunto $\mathcal{F}_m((L_p)^k)$ de todas las funciones $f : [(L_p)^k]^m \longrightarrow (L_p)^k$ podemos definir una estructura de anillo a partir de las operaciones definidas sobre $(L_p)^k$ de la siguiente manera:

$$\begin{aligned} (f\Delta g)(x_1, x_2, \ldots, x_m) &= f(x_1, x_2, \ldots, x_m)\Delta g(x_1, x_2, \ldots, x_m), \\ (f \odot g)(x_1, x_2, \ldots, x_m) &= f(x_1, x_2, \ldots, x_m) \odot g(x_1, x_2, \ldots, x_m). \end{aligned}$$

Llamamos $\langle (L_p)^k[x_1, x_2, \ldots, x_m]; \Delta, \odot \rangle$ al anillo de polinomios en m indeterminadas con coeficientes en el álgebra $(L_p)^k$, formado por todas las clases de equivalencia de expresiones del tipo

$$\Delta\mu_i \odot N_i(x_1, x_2, \ldots, x_m),$$

donde $\mu_i \in (L_p)^k$ y $N_i = \mathbf{1}$ (el monomio asociado al conjunto vacío), o N_i se obtiene del conjunto

$$\{x_1, T(x_1), \ldots, T^{k-1}(x_1), x_2, T(x_2), \ldots, T^{k-1}(x_2), \ldots, x_m, T(x_m), \ldots, T^{k-1}(x_m)\}$$

aplicando la operación $\odot$.

A continuación definimos los siguientes polinomios de Lagrange $\mathcal{L}_a(x) \in (L_p)^k[x]$.

$$\begin{aligned} \mathcal{L}_0(x) &= \sim x^{p-1} \odot \sim T(x^{p-1}) \odot \ldots \odot \sim T^{k-1}(x^{p-1}). \\ \mathcal{L}_a(x) &= \mathcal{L}_0(x\Delta(p-1)a). \end{aligned}$$

Estos polinomios verifican

$$\mathcal{L}_0(x) = \begin{cases} \mathbf{1} & \text{si } x = \mathbf{0} \\ \mathbf{0} & \text{si } x \neq \mathbf{0} \end{cases} \quad \text{y} \quad \mathcal{L}_a(x) = \begin{cases} \mathbf{1} & \text{si } x = a \\ \mathbf{0} & \text{si } x \neq a \end{cases}.$$

Como $x^{p-1} \in B((L_p)^k)$ entonces las operaciones de $\sim$, T y $\odot$ coinciden con las dadas por H. Cendra en [10] en la variedad de las álgebras de Boole cíclicas.

Los polinomios $\mathcal{L}_0(x)$ y $\mathcal{L}_a(x)$ son términos switching ya que $\mathcal{L}_0(x) = s(\mathbf{0}, x, \mathbf{1}, \mathbf{0})$ y $\mathcal{L}_a(x) = s(a, x, \mathbf{1}, \mathbf{0})$.

De esta manera obtenemos la siguiente fórmula de interpolación:

$$f(x_1, x_2, \ldots, x_m) = \Delta_{(\alpha_1,\ldots,\alpha_m)\in((L_p)^k)^m} f(\alpha_1, \ldots, \alpha_m) \odot \mathcal{L}_{\alpha_1}(x_1) \odot \ldots \odot \mathcal{L}_{\alpha_m}(x_m) \text{ (II)}$$

y el teorema que sigue:

Teorema 3.1.1 *Toda función $f \in \mathcal{F}_m((L_p)^k)$ puede representarse de una única manera como $\Delta\mu_i \odot N_i(x_1, x_2, \ldots, x_m)$, donde $\mu_i \in (L_p)^k$ y $N_i = \mathbf{1}$ ó es el producto (con $\odot$ como producto) de elementos del conjunto*

$$\{x_1, T(x_1), \ldots, T^{k-1}(x_1), x_2, T(x_2), \ldots, T^{k-1}(x_2), \ldots, x_m, T(x_m), \ldots, T^{k-1}(x_m)\}.$$

Demostración: Por la proposición 3.1.2 resulta que el número de polinomios reducidos de la forma $\Delta\mu_i \odot N_i(x_1, x_2, \ldots, x_m)$, con $\mu_i \in (L_p)^k$ es $(p^k)^{p^{km}}$ y éste coincide con el número de funciones $f : [(L_p)^k]^m \longrightarrow (L_p)^k$.
A cada polinomio $p(x_1, x_2, \ldots, x_m)$ le asignamos la función definida de manera natural, mediante la aplicación

$$\tau : (L_p)^k[x_1, x_2, \ldots, x_m] \longrightarrow \mathcal{F}_m((L_p)^k).$$

Por la fórmula de interpolación resulta que τ es sobreyectiva y por lo visto anteriormente es la única representación que admite la función f en términos de los polinomios reducidos. □

3.2. Interpretaciones

A continuación describimos un **método constructivo** que permite expresar las operaciones de las álgebras de Post de orden p, $k-$cíclicas, con p primo y $k \geq 1$, como términos en el lenguaje de los cuerpos $\langle F(p^k); +, \cdot, F(p)\rangle$ y recíprocamente.

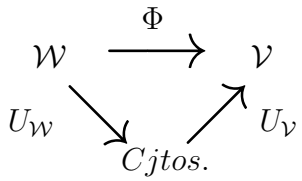
Demostramos en el teorema 3.2.2 que existe una equivalencia entre la variedad $\mathcal{V}(L_{p,k})$ y la variedad $\mathcal{V}(F(p^k))$.

Definición 3.2.1 *Decimos que una variedad $\mathcal{V}$ es* **interpretable** *[26], [30] en una variedad $\mathcal{W}$ (no necesariamente del mismo tipo de similaridad), si para cada $\mathcal{V}-$operación $F_t(x_1, \ldots, x_n)$ existe un $\mathcal{W}-$término $f_t(x_1, \ldots, x_n)$ tal que si $\langle A; G_t\rangle$ es un álgebra en $\mathcal{W}$, entonces $\langle A; f_t\rangle$ pertenece a $\mathcal{V}$.*

Las constantes de $\mathcal{V}$ deben ser interpretadas como constantes en el lenguaje de $\mathcal{W}$.

Una variedad $\mathcal{V}$ es interpretable en $\mathcal{W}$ cuando toda álgebra de $\mathcal{W}$ puede transformarse en un álgebra de $\mathcal{V}$, i.e. toda álgebra de $\mathcal{W}$ pueden convertirse en un álgebra de $\mathcal{V}$, expresando las $\mathcal{V}-$operaciones como una composición formal de las $\mathcal{W}-$operaciones.

Además si $\mathcal{V}$ es interpretable en $\mathcal{W}$ existe un funtor $\Phi : \mathcal{W} \longrightarrow \mathcal{V}$ que conmuta con los funtores olvido $U_{\mathcal{W}}$ y $U_{\mathcal{V}}$, que asignan a cada álgebra de $\mathcal{V}$ o $\mathcal{W}$ su universo. En consecuencia el siguiente diagrama es conmutativo:



Si $\langle A; G_t\rangle$ es un álgebra y para cada $\mathcal{V}-$operación $F_t(x_1, \ldots, x_n)$ existe un término $f_t(x_1, \ldots, x_n)$ en el lenguaje de $\langle A; G_t\rangle$ tal que $\langle A; f_t\rangle \in \mathcal{V}$, entonces el término $f_t(x_1, \ldots, x_n)$ define una interpretación de $\mathcal{V}$ en $\mathcal{V}(\langle A; G_t\rangle)$, la variedad generada por $\langle A; G_t\rangle$.

La evaluación de un término en un álgebra B de $\mathcal{V}(\langle A; G_t\rangle)$, está determinada por su evaluación en A y por el hecho de que ambas álgebras, $\langle A; G_t\rangle$ y $\langle B; G_t\rangle$ satisfacen las mismas ecuaciones. De esta manera tenemos una aplicación
$\Phi : \mathcal{V}(\langle A; G_t\rangle) \longrightarrow \mathcal{V}$ y decimos que $\Phi(\langle A; G_t\rangle)$ es una interpretación de $\mathcal{V}$ en $\mathcal{V}(\langle A; G_t\rangle)$.

Definición 3.2.2 *Decimos que dos variedades $\mathcal{V}$ y $\mathcal{W}$ son* **equivalentes** *[30] si existe un par de interpretaciones Φ_1 de $\mathcal{V}$ en $\mathcal{W}$ y Φ_2 de $\mathcal{W}$ en $\mathcal{V}$ tales que $\Phi_2\Phi_1 = Id_{\mathcal{V}}$ y $\Phi_1\Phi_2 = Id_{\mathcal{W}}$. En particular, dos álgebras A y B se dicen* **equivalentes** *si y sólo si existen dos interpretaciones $\Phi : \mathcal{V}(A) \longrightarrow \mathcal{V}(B)$ y $\Psi : \mathcal{V}(B) \longrightarrow \mathcal{V}(A)$ tal que $\Phi\Psi_2(B) = B$ y $\Psi\Phi(A) = A$.*

Las álgebras A y B son álgebras equivalentes si y sólo si toda operación en el lenguaje de A puede escribirse como un término en el lenguaje de B y recíprocamente.

Teorema 3.2.1 *[30] Sean $\mathcal{V}$ y $\mathcal{W}$ variedades. Decimos que $\mathcal{V}$ es equivalente a $\mathcal{W}$ si y sólo si existen álgebras A y B equivalentes tales que $\mathcal{V} = \mathcal{V}(A)$ y $\mathcal{W} = \mathcal{W}(B)$.*

Ahora veremos cómo obtener la estructura de álgebra de Post $k-$cíclica de orden p, con p primo, $\langle (L_p)^k; T\rangle$ a partir del cuerpo $F(p^k)$ y recíprocamente.

Sea p un número primo, $F(p) = \{0, 1, 2, \ldots, p-1\}$ el cuerpo primo de $F(p^k)$ y σ el automorfismo de Frobenius. Por el teorema de la base normal, existe $w \in F(p^k)$ tal que $\{w, \sigma(w), \ldots, \sigma^{k-1}(w)\}$ es una base del $F(p)-$espacio vectorial $F(p^k)$.

Luego dado $x \in F(p^k)$, éste puede representarse de una única manera como

$$x = \sum_{i=0}^{k-1} \lambda_i(x)\sigma^i(w), \quad \lambda_i(x) \in F(p), \quad 0 \leq i \leq k-1.$$

Así podemos asociarle a x una única k-upla $(\lambda_0(x), \lambda_1(x), \ldots, \lambda_{k-1}(x))$. En particular el elemento neutro del cuerpo $F(p^k)$, 0, se identifica con la k-upla $(0, 0, \ldots, 0)$.

Como $\sigma((\lambda_0(x), \lambda_1(x), \ldots, \lambda_{k-2}(x), \lambda_{k-1}(x))) = (\lambda_{k-1}(x), \lambda_0(x), \ldots, \lambda_{k-2}(x))$, el automorfismo de Frobenius σ permuta cíclicamente las coordenadas $\lambda_i(x)$. De aquí resulta que los únicos elementos de $F(p^k)$ que quedan fijos por la acción de σ son:

$$(0, 0, \ldots, 0),\ (1, 1, \ldots, 1),\ \ldots,\ (p-1,\ p-1,\ \ldots,\ p-1).$$

Por ser $F(p)$ el cuerpo fijo de $F(p^k)$, $\sigma(x) = x$, cualquiera sea $x \in F(p)$. Luego,

$$(\lambda_0(x),\ \lambda_1(x),\ \ldots,\ \lambda_{k-2}(x),\ \lambda_{k-1}(x)) = (\lambda_{k-1}(x),\ \lambda_0(x),\ \lambda_1(x),\ \ldots,\ \lambda_{k-2}(x)),$$

de donde resulta que

$$\lambda_0(x) = \lambda_1(x) = \ldots = \lambda_{k-1}(x).$$

De esta manera concluimos que si $x \in F(p)$ entonces $x = (\lambda(x), \lambda(x), \ldots, \lambda(x))$ con $\lambda(x) \in F(p)$.

El teorema que sigue es uno de los resultados más importantes de esta tesis y su aplicación es fundamental en los próximos capítulos. La demostración nos da un **método constructivo** para expresar las operaciones de un cuerpo $F(p^k)$ como términos en el lenguaje de las álgebras de Post $k-$cíclicas de orden p y recíprocamente.

Teorema 3.2.2 *Dado un cuerpo finito $F(p^k)$ con p^k elementos, p primo, $k \in N$, se puede definir una única estructura de álgebra de Post de orden p, k-periódica sobre $F(p^k)$, isomorfa a*

$$L_{p,k} = \langle (L_p)^k; \wedge, \vee, \sim, \{C_i\}_{i=0}^{p-1}, \mathbf{0}, \mathbf{1}, \{e_i\}_{i=1}^{p-2}, T\rangle$$

tal que:

1. *Las constantes e_i de $(L_p)^k$ coinciden con los elementos del cuerpo primo $F(p)$.*

2. *Los operadores $\wedge$ y $\vee$ son polinomios in $F(p)[x_1, x_2]$ de la forma*

$$\sum_{i=1}^{p^{2k}} \lambda_i \cdot x_1^{r_{i_1}} \cdot x_2^{r_{i_2}}, \quad \lambda_i \in F(p), \quad 1 \leq i \leq p^{2k},$$

y las operaciones $\sim$, C_i y T están determinadas por polinomios in $F(p)[x]$ de la forma

$$\sum_{i=1}^{p^k} \lambda_i \cdot x_i^{r_i}, \quad \lambda_i \in F(p).$$

Además estas operaciones están unívocamente determinadas bajo las condiciones $r_{i_j} < p^k$ y $r_i < p^k$.

3. *Las operaciones $+$ y $\cdot$ están unívocamente determinadas por los polinomios pertenecientes a $L_p[x_1, x_2]$ de la forma:*

$$\Delta\mu_i \odot N_i(x_1, x_2, \ldots, x_m),$$

donde $\mu_i \in \{e_0, e_1, \ldots, e_{p-1}\}$ y $N_i = \mathbf{1}$ ó es el producto (con $\odot$ como producto) de elementos del conjunto

$$\{x_1, T(x_1), \ldots, T^{k-1}(x_1), x_2, T(x_2), \ldots, T^{k-1}(x_2), \ldots, x_m, T(x_m), \ldots, T^{k-1}(x_m)\}.$$

Demostración: Fijamos sobre el cuerpo $F(p) = \{0, 1, \ldots, p-1\}$ el siguiente orden total:

$$0 < p-1 < p-2 < \ldots < 2 < 1.$$

Definiendo

$$e_0 = 0, \ e_i = p - i, \quad 1 \leq i \leq p-1,$$
$$\sim e_i = e_{p-i-1}, 1 \leq i \leq p-1 \ \ y$$
$$C_i(e_j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases},$$

el cuerpo primo $F(p)$ es un álgebra de Post L_p de orden p.
Sea $A = (L_p)^k$, la cadena L_p y el cuerpo $F(p)$ forman el mismo conjunto, al igual que el álgebra de Post de orden p, A y el cuerpo $F(p^k)$. De esta manera queda determinada sobre $F(p^k)$ una estructura de álgebra de Post de orden p, donde $A = \langle F(p^k); \wedge, \vee, \sim, \{C_i\}_{i=0}^{p-1}, \mathbf{0}, \mathbf{1}, \{e_i\}_{i=1}^{p-2} \rangle$, las operaciones $\wedge, \vee, \sim, \{C_i\}_{i=0}^{p-1}$ se definen coordenada a coordenada a partir de las operaciones del álgebra de Post definida sobre $F(p)$ y las constantes de A son las k-uplas

$$\mathbf{0} = e_0 = (0, 0, \ldots, 0), \quad \mathbf{1} = e_{p-1} = (1, 1, \ldots, 1)$$

y para i, con $1 \leq i \leq p-2$,

$$e_i = (p-i, p-i, \ldots, p-i).$$

El primer elemento de A, $\mathbf{0} = e_0$, es el 0 del cuerpo $F(p^k)$.
La aplicación $T : A \longrightarrow A$ definida por

$$T(x) = \sigma(x) = x^p,$$

es un automorfismo del álgebra de Post A. En efecto,

$$\begin{aligned} T(x \wedge y) &= T((\lambda_0(x), \lambda_1(x), \ldots, \lambda_{k-1}(x)) \wedge (\lambda_0(y), \lambda_1(y), \ldots, \lambda_{k-1}(y))) = \\ &= T((\lambda_0(x) \wedge \lambda_0(y), \lambda_1(x) \wedge \lambda_1(y), \ldots, \lambda_{k-1}(x) \wedge \lambda_{k-1}(y))) = \\ &= (\lambda_{k-1}(x) \wedge \lambda_{k-1}(y), \lambda_0(x) \wedge \lambda_o(y), \ldots, \lambda_{k-2}(x) \wedge \lambda_{k-2}(y)) = \\ &= (\lambda_{k-1}(x), \lambda_0(x), \ldots, \lambda_{k-2}(x)) \wedge (\lambda_{k-1}(y), \lambda_0(y), \ldots, \lambda_{k-2}(y)) = \\ &= T(x) \wedge T(y). \end{aligned}$$

Puede probarse de manera análoga que T respeta las operaciones $\vee, \sim, \{C_i\}_{i=0}^{p-1}$, y como T es una aplicación biyectiva resulta que T es un automorfismo de álgebras de Post.
Como $T^k(x) = x$ entonces $\langle A; T \rangle$ es un álgebra de Post $k-$cíclica de orden p simple.
Veamos ahora que las operaciones $\wedge, \vee, \{C_i\}_{i=0}^{p-1}$ y T son polinomios en $F(p)[x_1, x_2, \ldots, x_m]$.
Vimos en la sección anterior, que cada función $f : F(p^k)^m \to F(p^k)$ tiene una única expresión de la forma

$$f(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{p^{km}} \eta_i M_i, \quad \eta_i \in F(p^k),$$

donde $M_i = M_i(x_1, x_2, \ldots, x_m) = x_1^{r_{i_1}} \cdot x_2^{r_{i_2}} \cdot \ldots \cdot x_m^{r_{i_m}}$ con $0 \leq r_{i_j} < p^k$ e
$i = 1, 2, \ldots, p^{km}$.
Si $x \in F(p^k)$ entonces $\sigma^k(x) = x^{p^k} = x$. Luego para cada $i \in \{1, 2, \ldots, p^{km}\}$ existe $j \in \{1, 2, \ldots, p^{km}\}$ tal que

$$\sigma(M_i(x_1, x_2, \ldots, x_m)) = M_i(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)) = M_j(x_1, x_2, \ldots, x_m).$$

La aplicación σ es un automorfismo de álgebras de Post y un automorfismo de cuerpos, de donde resulta que $f(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)) = \sigma(f(x_1, x_2, \ldots, x_m))$, i.e.,

$$\sum_{i=1}^{p^{km}} \eta_i M_i(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)) = \sum_{i=1}^{p^{km}} \eta_i^p M_i(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)).$$

Luego $\eta_i^p = \eta_i$ y en consecuencia $\eta_i \in \{0, 1, \ldots, p-1\}$, para $i = 1, 2, \ldots, p^{km}$.
Las operaciones $\wedge,\ \vee,\ \sim,\ \{C_i\}_{i=0}^{p-1}$ y T son funciones de $F(p^k)^m$ en $F(p^k)$ para algún m y como el operador T respeta estas operaciones, cada una de las funciones $\wedge, \vee$ tiene una única representación de la forma

$$\sum_{i=1}^{p^{2k}} \lambda_i \cdot x_1^{r_{i_1}} \cdot x_2^{r_{i_2}}, \quad \lambda_i \in F(p), \quad 1 \leq i \leq p^{2k}.$$

Las operaciones $\sim,\ \{C_i\}_{i=0}^{p-1}$ y T son polinomios in $F(p)[x]$ de la forma

$$\sum_{i=1}^{p^k} \lambda_i \cdot x_i^{r_i}, \quad \lambda_i \in F(p), \quad 1 \leq i \leq p^k$$

que están unívocamente determinadas por las condiciones $r_i < p^k$ y $r_{i_j} < p^k$.
Por otro lado sabemos que toda función $f : A^m \longrightarrow A$ puede expresarse de una única manera como

$$f(x_1, x_2, \ldots, x_m) = \Delta_{(\alpha_1,\ldots,\alpha_m)\in A^m} f(\alpha_1, \ldots, \alpha_m) \odot \mathcal{L}_{\alpha_1}(x_1) \odot \ldots \odot \mathcal{L}_{\alpha_m}(x_m),$$

donde los $\mathcal{L}_{\alpha_1}(x_i)$ son los polinomios de Lagrange del álgebra de Post A.
Como los elementos de A y $F(p^k)$ coinciden, las funciones $f_1, f_2 : A^2 \longrightarrow A$ definidas por $f_1(x_1, x_2) = x_1 + x_2$ y $f_2(x_1, x_2) = x_1 \cdot x_2$ tienen una representación única de la forma

$$f_1(x_1, x_2) = \Delta_{(\alpha_1,\alpha_2)\in A^2} f_1(\alpha_1, \alpha_2) \odot \mathcal{L}_{\alpha_1}(x_1) \odot \mathcal{L}_{\alpha_2}(x_2)$$

y

$$f_2(x_1, x_2) = \Delta_{(\alpha_1,\alpha_2)\in A^2} f_2(\alpha_1, \alpha_2) \odot \mathcal{L}_{\alpha_1}(x_1) \odot \mathcal{L}_{\alpha_2}(x_2).$$

Luego las operaciones del cuerpo $F(p^k)$ pueden ser expresadas como términos en el lenguaje del álgebra $\langle A; T \rangle$. □

Los corolarios que damos a continuación son una consecuencia de la demostración del teorema anterior y prueban que las variedades $\mathcal{V}(L_{p,k})$ y $\mathcal{V}(F(p^k))$ son **equivalentes**.

Corolario 3.2.1 *Existe un interpretación Φ_1 de $\mathcal{V}(L_{p,k})$ en $\mathcal{V}(F(p^k))$ y una interpretación Φ_2 de $\mathcal{V}(F(p^k))$ en $\mathcal{V}(L_{p,k})$ tal que $\Phi_1\Phi_2(B) = B$, cualquiera sea $B \in \mathcal{V}(L_{p,k})$ y $\Phi_2\Phi_1(R) = R$ para todo $R \in \mathcal{V}(F(p^k))$.*

Corolario 3.2.2 *Toda función $f : [L_{p,k}]^m \longrightarrow L_{p,k}$ que conmute con T puede representarse con un término en el lenguaje de $\mathcal{V}(L_{p,k})$. Análogamente toda función $f : [F(p^k)]^m \longrightarrow F(p^k)$ que conmute con σ puede ser representada con un polinomio con coeficientes en $F(p)$.*

3.3. Ejemplos

En los siguientes ejemplos mostraremos el proceso constructivo enunciado en el teorema 3.2.2.

Ejemplo 3.3.1 *Consideremos el cuerpo* $F(3) \cong \mathbb{Z}_3 = \{0, 1, 2\}$ *y sobre él el orden total* $0 < 2 < 1$.

Las operaciones C_0, C_1 *y* C_2 *definidas en la tabla, dan sobre* $F(3)$ *una estructura de álgebra de Post,* L_3.

x	$C_0(x)$	$C_1(x)$	$C_2(x)$
0	*1*	*0*	*0*
2	*0*	*1*	*0*
1	*0*	*0*	*1*

Las constantes del álgebra son

$$e_0 = 0, \quad e_1 = 2 \quad y \quad e_2 = 1$$

y los polinomios de Lagrange en $F(3)$ *están dados por las siguientes expresiones:*

$$L_0(x) = 2x^2 + 1, \quad L_1(x) = 2x^2 + 2x \quad y \quad L_2(x) = 2x^2 + x.$$

Utilizando la fórmula (I) podemos expresar las operaciones $\wedge, \vee, \sim, C_0, C_1$ *y* C_2 *en el lenguaje de los cuerpos. Las constantes son* $\mathbf{0} = 0$, $\mathbf{1} = 2$ *y el resto de las operaciones vienen dadas por*

$x \wedge y = x^2y^2 + 2x^2y + 2xy^2 + 2xy,$

$x \vee y = 2x^2y^2 + x^2y + xy^2 + xy + x + y,$

$\sim x = 2x + 1,$

$C_0(x) = 2x^2 + 1, \quad C_1(x) = 2x^2 + x, \quad C_2(x) = 2x^2 + 2x \quad y$

$T(x) = x.$

Los programas que permiten calcular los polinomios de Lagrange, el ínfimo y el supremo en el lenguaje de $F(3)$ **han sido incluídos en la primera sección del apéndice que se encuentra al final de esta tesis.**

Recíprocamente, los polinomios de Lagrange para el álgebra de Post L_3 *son:*

$$\mathcal{L}_0(x) = 2 \odot x^2\Delta 1, \quad \mathcal{L}_1(x) = 2 \odot x^2\Delta 2 \odot x \quad y \quad \mathcal{L}_2(x) = 2 \odot x^2\Delta x.$$

Utilizando la fórmula (II) las operaciones $+$ *y* $\cdot$ *del cuerpo pueden expresarse como sigue*

$$x + y = x\Delta y \qquad y \qquad x \cdot y = x \odot y.$$

Como las operaciones Δ *y* $\odot$ *están definidas en términos de* $\wedge, \vee, C_0, C_1$ *y* C_2*, obtenemos*

$$x\Delta y = \{[(C_0(x) \wedge C_1(y)) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_2(y))] \wedge e_1\} \vee$$

$$\vee (C_0(x) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_0(y)),$$

$$x \odot y = \{[(C_1(x) \wedge C_2(y)) \vee (C_2(x) \wedge C_1(y))] \wedge e_1\} \vee \ (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y)).$$

En la primera sección del apéndice también se incluyen los programas de los polinomios de Lagrange, la suma y el producto en el lenguaje del álgebra de Post k**-cíclica** $L(3)$**.**

Ejemplo 3.3.2 *Consideremos ahora el cuerpo* $F(3^2)$ *con* 3^2 *elementos,*

$$F(3^2) = F(3)[x]/(1 + x^2) = \{0,\ 1 + x,\ 2x,\ 1 + 2x,\ 2,\ 2 + 2x,\ x,\ 2 + x,\ 1\}.$$

Sabemos que $\varepsilon = 1 + x$ *es un generador del grupo multiplicativo* $F(3^2) \setminus \{0\}$*, entonces*

$$F(3^2) = \{0,\ \varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,\ \varepsilon^5,\ \varepsilon^6,\ \varepsilon^7,\ \varepsilon^8\}.$$

Sea σ *el automorfismo de Frobenius de* $F(3^2)$*,* $\sigma(x) = x^3$*.*

Por el Teorema de la base normal existe $\omega \in F(3^2)$ *tal que* $\{\omega, \sigma(\omega)\}$ *es una base del* $F(3)-$*espacio vectorial* $F(3^2)$*. Luego todo elemento* $x \in F(3^2)$ *puede expresarse de una única manera de la forma* $x = \lambda_0(x)\omega + \lambda_1(x)\sigma(\omega)$*, con* $\lambda_0(x),\ \lambda_1(x) \in F(3)$*.*

Tomamos un elemento ω *de* $F(3^2)$ *que verifique*

$$\begin{vmatrix} \omega & \sigma(\omega) \\ \sigma(\omega) & \omega \end{vmatrix} \neq 0.$$

Si $\omega = \varepsilon$ *entonces* $\{\varepsilon, \sigma(\varepsilon)\}$ *es una base de* $F(3^2)$ *como* $F(3)-$*espacio vectorial y tenemos la identificación siguiente:*

$x \in F(p^2)$	$(\lambda_0(x),\ \lambda_1(x))$
0	$(0,0)$
ε	$(1,0)$
ε^2	$(1,2)$
ε^3	$(0,1)$
$2 = \varepsilon^4$	$(1,1)$
ε^5	$(2,0)$
ε^6	$(2,1)$
ε^7	$(0,2)$
$1 = \varepsilon^8$	$(2,2)$

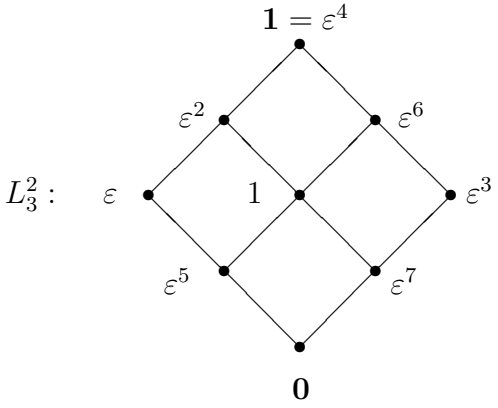
Vimos en el ejemplo anterior que asignando a $F(3)$ *el orden total* $0 < 2 < 1$, *obtenemos el álgebra de Post* L_3.

Ahora consideremos sobre $F(3^2)$ *la estructura de álgebra de Post* A, *donde* $A = L_3^2$, *las operaciones* $\wedge, \vee, C_0, C_1$ *y* C_2 *están definidas componente a componente y las constantes de* A *son:*

$$\mathbf{0} = e_0 = (0,0), \quad e_1 = (2,2) = 1 \quad y \quad \mathbf{1} = e_2 = (1,1) = 2.$$

Las constantes son los elementos del cuerpo primo $F(3)$.

Además, como $\sigma\restriction F(3) = id$, *definiendo* $T = \sigma$ *obtenemos la siguiente álgebra de Post de orden* 3, $2-$*cíclica* $\langle A; T\rangle$ *asociada al cuerpo* $F(3^2)$.



$x \in F(3^2)$	$\sim x$	$C_0(x)$	$C_1(x)$	$C_2(x)$	$T(x)$
$0 = (0,0)$	$\varepsilon^4 = (1,1)$	$\varepsilon^4 = (1,1)$	$0 = (0,0)$	$0 = (0,0)$	$0 = (0,0)$
$\varepsilon = (1,0)$	$\varepsilon^3 = (0,1)$	$\varepsilon^3 = (0,1)$	$0 = (0,0)$	$\varepsilon = (1,0)$	$\varepsilon^3 = (0,1)$
$\varepsilon^2 = (1,2)$	$\varepsilon^7 = (0,2)$	$0 = (0,0)$	$\varepsilon = (1,0)$	$\varepsilon = (1,0)$	$\varepsilon^6 = (2,1)$
$\varepsilon^3 = (0,1)$	$\varepsilon = (1,0)$	$\varepsilon = (1,0)$	$0 = (0,0)$	$\varepsilon^3 = (0,1)$	$\varepsilon = (1,0)$
$\varepsilon^4 = (1,1)$	$0 = (0,0)$	$0 = (0,0)$	$0 = (0,0)$	$\varepsilon^4 = (1,1)$	$\varepsilon^4 = (1,1)$
$\varepsilon^5 = (2,0)$	$\varepsilon^6 = (2,1)$	$\varepsilon^3 = (0,1)$	$\varepsilon = (1,0)$	$0 = (0,0)$	$\varepsilon^7 = (0,2)$
$\varepsilon^6 = (2,1)$	$\varepsilon^5 = (2,0)$	$0 = (0,0)$	$\varepsilon = (1,0)$	$\varepsilon^3 = (0,1)$	$\varepsilon^2 = (1,2)$
$\varepsilon^7 = (0,2)$	$\varepsilon^2 = (1,2)$	$\varepsilon = (1,0)$	$\varepsilon^3 = (0,1)$	$0 = (0,0)$	$\varepsilon^5 = (2,0)$
$\varepsilon^8 = (2,2)$	$\varepsilon^8 = (2,2)$	$0 = (0,0)$	$\varepsilon^4 = (1,1)$	$0 = (0,0)$	$\varepsilon^8 = (2,2)$

Los polinomios de Lagrange definidos en $F(3^2)$ *son:*

$L_0(x) = \varepsilon^4 x^8 + 1,$

$L_\varepsilon(x) = \varepsilon^4 x^8 + \varepsilon^5 x^7 + \varepsilon^6 x^6 + \varepsilon^7 x^5 + x^4 + \varepsilon x^3 + \varepsilon^2 x^2 + \varepsilon^3 x,$

$L_{\varepsilon^2}(x) = \varepsilon^4 x^8 + \varepsilon^6 x^7 + x^6 + \varepsilon^2 x^5 + \varepsilon^4 x^4 + \varepsilon^6 x^3 + x^2 + \varepsilon^2 x,$

$L_{\varepsilon^3}(x) = \varepsilon^4 x^8 + \varepsilon^7 x^7 + \varepsilon^2 x^6 + \varepsilon^5 x^5 + x^4 + \varepsilon^3 x^3 + \varepsilon^6 x^2 + \varepsilon x,$

$L_{\varepsilon^4}(x) = \varepsilon^4 x^8 + x^7 + \varepsilon^4 x^6 + x^5 + \varepsilon^4 x^4 + x^3 + \varepsilon^4 x^2 + x,$

$L_{\varepsilon^5}(x) = \varepsilon^4 x^8 + \varepsilon x^7 + \varepsilon^6 x^6 + \varepsilon^3 x^5 + x^4 + \varepsilon^5 x^3 + \varepsilon^2 x^2 + \varepsilon^7 x,$

$L_{\varepsilon^6}(x) = \varepsilon^4x^8 + \varepsilon^2x^7 + x^6 + \varepsilon^6x^5 + \varepsilon^4x^4 + \varepsilon^2x^3 + x^2 + \varepsilon^6x,$

$L_{\varepsilon^7}(x) = \varepsilon^4x^8 + \varepsilon^3x^7 + \varepsilon^2x^6 + \varepsilon x^5 + x^4 + \varepsilon^7x^3 + \varepsilon^6x^2 + \varepsilon^5x \quad y$

$L_{\varepsilon^8}(x) = \varepsilon^4x^8 + \varepsilon^4x^7 + \varepsilon^4x^6 + \varepsilon^4x^5 + \varepsilon^4x^4 + \varepsilon^4x^3 + \varepsilon^4x^2 + \varepsilon^4x.$

Como $\varepsilon^4 = 2$, aplicando la fórmula (I), las operaciones de $\wedge, \vee, \sim, C_0, C_1$ y C_2 se expresan en función de las operaciones del cuerpo de la siguiente manera:

$$\begin{aligned} x \wedge y &= x^6[y^6 + \varepsilon^4y^4 + \varepsilon^4y^3 + \varepsilon^4y^2] + x^4[\varepsilon^4y^6 + \varepsilon^4y^4 + y^2 + \varepsilon^4y] + \\ &\quad + x^3[\varepsilon^4y^6 + y^3 + y^2 + \varepsilon^4y] + x^2[\varepsilon^4y^6 + y^4 + y^3 + y^2] + \\ &\quad + x[\varepsilon^4y^4 + \varepsilon^4y^3 + \varepsilon^4y], \end{aligned} \tag{3.1}$$

$$\begin{aligned} x \vee y &= x^6[\varepsilon^4y^6 + y^4 + y^3 + y^2] + x^4[y^6 + y^4 + \varepsilon^4y^2 + y] + \\ &\quad + x^3[y^6 + \varepsilon^4y^3 + \varepsilon^4y^2 + y] + x^2[y^6 + \varepsilon^4y^4 + \varepsilon^4y^3 + \varepsilon^4y^2] + \\ &\quad + x[y^4 + y^3 + y + 1] + y, \end{aligned} \tag{3.2}$$

$\sim x = \varepsilon^4x + \varepsilon^4, \quad C_0(x) = x^6 + x^4 + \varepsilon^4x^2 + \varepsilon^4, \quad C_1(x) = x^6 + x^4 + \varepsilon^4x^2 + x,$

$C_2(x) = x^6 + x^4 + \varepsilon^4x^2 + \varepsilon^4x \quad y \quad T(x) = x^3.$

Las fórmulas de los polinomios de Lagrange en $F(3^2)$, del ínfimo y del supremo están programados en la segunda sección del apéndice de esta tesis.

Veamos como expresar las operaciones del cuerpo $F(3^2)$ en función de las operaciones del álgebra de Post trivalente, 2 cíclica, $L_{3,2}$.

Los polinomios de Lagrange están dados por:

$\mathcal{L}_0(x) = x^2 \odot (T(x))^2\Delta e_1 \odot x^2\Delta e_1 \odot (T(x))^2\Delta \mathbf{1},$

$\mathcal{L}_\varepsilon(x) = x^2 \odot (T(x))^2\Delta x \odot (T(x))^2\Delta e_1 \odot x^2\Delta e_1 \odot x,$

$\mathcal{L}_{\varepsilon^2}(x) = x^2 \odot (T(x))^2\Delta e_1 \odot x^2 \odot T(x)\Delta x \odot (T(x))^2\Delta e_1 \odot x \odot T(x),$

$\mathcal{L}_{\varepsilon^3}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta e_1 \odot (T(x))^2\Delta e_1 \odot T(x),$

$\mathcal{L}_{\varepsilon^4}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta x \odot (T(x))^2\Delta x \odot T(x),$

$\mathcal{L}_{\varepsilon^5}(x) = x^2 \odot (T(x))^2\Delta e_1 \odot x \odot (T(x))^2\Delta x \odot (T(x))^2\Delta e_1 \odot x^2\Delta x,$

$\mathcal{L}_{\varepsilon^6}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta e_1 \odot x \odot (T(x))^2\Delta e_1 \odot x \odot T(x),$

$\mathcal{L}_{\varepsilon^7}(x) = x^2 \odot (T(x))^2 \Delta e_1 \odot x^2 \odot T(x) \Delta e_1 \odot (T(x))^2 \Delta T(x) \quad y$

$\mathcal{L}_{\varepsilon^8}(x) = x^2 \odot (T(x))^2 \Delta e_1 \odot x^2 \odot T(x) \Delta e_1 \odot x \odot (T(x))^2 \Delta x \odot T(x).$

De la fórmula (II) obtenemos que:

$$x + y = x \Delta y,$$

$$x \cdot y = T(x) \odot y \Delta x \odot y \Delta x \odot T(y) \Delta e_1 \odot T(x) \odot T(y).$$

De manera análoga al primer ejemplo obtenemos

$x \Delta y = \{[(C_0(x) \wedge C_1(y)) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_2(y))] \wedge e_1\} \vee$
$\vee (C_0(x) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_0(y)), \quad y$

$x \odot y = [\{(C_1(x) \wedge C_2(y))) \vee (C_2(x) \wedge C_1(y))] \wedge e_1\} \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y)).$

En la segunda sección del apéndice pueden encontrarse los programas de los polinomios de Lagrange, de la suma y del producto en el lenguaje del álgebra de Post k-cíclica $L_{3,2}$.

Capítulo 4

Bases de Gröbner

Las bases de Gröbner constituyen una herramienta muy útil para resolver problemas referidos a un ideal I en un anillo de polinomios en n variables $X_1, \ldots, X_n$ con coeficientes en un cuerpo K. El objetivo de este capítulo es introducir estas bases y mostrar su aplicación en la resolución de sistemas de ecuaciones polinomiales sobre un cuerpo K cualquiera y en particular sobre un cuerpo finito $F(p^k)$. Las bases de Gröbner y la interpretación demostrada en el capítulo anterior nos permitirán resolver en los próximos capítulos sistemas de ecuaciones algebraicas sobre las álgebras de Post k-cíclicas.

En la primera sección de este capítulo introducimos los conceptos de variedad algebraica afín e ideal radical de un ideal I de $K[X_1, \ldots, X_n]$ y estudiamos algunas relaciones entre ellos.

A los efectos de generalizar el algoritmo de división conocido para un anillo de polinomios en una sóla variable sobre un cuerpo K y poder dividir en $K[X_1, \ldots, X_n]$ un polinomio g por un conjunto de polinomios $\{f_1, \ldots, f_s\}$, se hace necesario ordenar los monomios de los polinomios. En la segunda sección definimos distintos órdenes monomiales e introducimos el concepto de ideal monomial. Demostramos el lema de Dickson y obtenemos un algoritmo de división en $K[X_1, \ldots, X_n]$. En esta sección también damos el teorema de la base de Hilbert, que demuestra que todo ideal $I \subset K[X_1, \ldots, X_n]$ está finitamente generado e introducimos la definición de base de Gröbner de un ideal I. Estas bases nos permiten resolver el problema de pertenencia a un ideal I en $K[X_1, \ldots, X_n]$. Para finalizar presentamos una primera versión del algoritmo de Buchberger, que calcula de manera efectiva una base de Gröbner de un ideal $I = (f_1, \ldots, f_s)$.

En la tercera sección damos la versión fuerte y la versión débil del teorema de los ceros de Hilbert y en la cuarta mostramos los teoremas anteriores en el caso particular en que K es un cuerpo finito.

Para finalizar en la última sección estudiamos el caso en que la variedad de un ideal I es finita.

Para la redacción de este capítulo hemos utilizado [3], [5], [7], [12], [22] y [28].

4.1. Variedades algebraicas afines. Ideales.

En esta sección comenzamos introduciendo las variedades algebraicas afines pues estas nos conducen al estudio de ideales en el anillo de polinomios $K[X_1, \ldots, X_n]$.

Definición 4.1.1 *Dado un cuerpo K y $f_1, \ldots, f_s$ polinomios en $K[X_1, \ldots, X_n]$, el conjunto*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}$$

se llama **variedad algebraica afín** *definida por $f_1, \ldots, f_s$.*

Las variedades afines se notan con las letras V, W, etc.

Lema 4.1.1 *Si $V, W \subset K^n$ son variedades afines, entonces también lo son $V \cup W$ y $V \cap W$.*

Demostración: Sean $V = \mathbf{V}(f_1, \ldots, f_s)$ y $W = \mathbf{V}(g_1, \ldots, g_t)$. Es claro que $V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots g_t)$ y es en consecuencia una variedad afín. Probemos que $V \cup W = \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$. Si $(a_1, \ldots, a_n) \in V$ (respectivamente $(a_1, \ldots a_n) \in W$) entonces todos los polinomios f_i (respectivamente todos los g_i) se anulan en este punto y por lo tanto también lo hacen todos los productos $f_i g_j$ en $(a_1, \ldots, a_n)$. Luego $V \cup W \subset \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$. Para probar la otra inclusión consideremos $(a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$. Si $(a_1, \ldots, a_n) \in V$ ya queda probado. En caso contrario $f_{i_0}(a_1, \ldots, a_n) \neq 0$ para algún i_0. Como $f_{i_0} g_j$ se anula en $(a_1, \ldots, a_n)$ para todo j, resulta $g_j(a_1, \ldots, a_n) = 0$ para todo j y por lo tanto $(a_1, \ldots, a_n) \in W$. Luego $\mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t) \subset V \cup W$. □

Definición 4.1.2 *Decimos que un ideal I es* **radical** *si verifica la siguiente condición:*

Si $f^m \in I$ para todo $m \geq 1$ entonces $f \in I$.

Definición 4.1.3 *Sea I un ideal de $K[X_1, \ldots, X_n]$. El* **radical** *de I, notado $\sqrt{I}$, es el conjunto*

$$\{f : f^m \in I \text{ para algún } m \geq 1\}.$$

De la definición resulta que $\sqrt{I}$ es un ideal y que $I \subset \sqrt{I}$.

Proposición 4.1.1 *Si I es un ideal primo de $K[X_1, \ldots, X_n]$ entonces I es un ideal radical.*

Proposición 4.1.2 *Sea I un ideal de $K[X_1, \ldots, X_n]$. Entonces $\sqrt{I}$ es la intersección de todos los ideales primos que contienen a I.*

Dados $f_1, \ldots, f_s$ polinomios en $K[X_1, \ldots, X_n]$. El conjunto

$$(f_1, \ldots, f_s) = \{\sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in K[X_1, \ldots, X_n]\}$$

es el ideal de $K[X_1, \ldots, X_n]$ generado por $f_1, \ldots, f_s$. Decimos que un ideal I **está finitamente generado** si existen polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ tales que $I = (f_1, \ldots, f_s)$. En este caso decimos que $f_1, \ldots, f_s$ es una **base** de I.

Veremos a continuación que todo ideal de $K[X_1, \ldots, X_n]$ está finitamente generado, resultado que se conoce como el **Teorema de la base de Hilbert**.

En esta tesis nos interesará estudiar especialmente los anillos de polinomios sobre cuerpos finitos ya que la equivalencia demostrada en el capítulo 3 nos permitirá resolver sistemas de ecuaciones polinomiales sobre un álgebra de Post k-cíclica utilizando herramientas propias del álgebra conmutativa.

Comenzamos estudiando la relación existente entre variedad e ideal.

Proposición 4.1.3 *Si dos conjuntos $\{f_1, \ldots, f_s\}$ y $\{g_1, \ldots, g_t\}$ son bases del mismo ideal en $K[X_1, \ldots, X_n]$, i.e. $(f_1, \ldots, f_s) = (g_1, \ldots, g_t)$, entonces*

$$\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t).$$

Definición 4.1.4 *Sea $V \subset K^n$ una variedad afín. Definimos el* **ideal de V, I(V)** *como el conjunto*
$\mathbf{I(V)} = \{f \in K[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0, (a_1, \ldots, a_n) \in V\}$.

El lema que sigue demuestra que $\mathbf{I(V)}$ es un ideal radical.

Lema 4.1.2 $\mathbf{I(V)}$ *es un ideal radical.*

El ejemplo y el lema siguientes muestran la relación existente entre los ideales $\mathbf{I}(\mathbf{V}(\mathbf{I}))$ e $\mathbf{I}$.

Lema 4.1.3 *Si $f_1, \ldots, f_s \in K[X_1, \ldots X_n]$ entonces $(f_1, \ldots, f_s) \subset \mathbf{I}(\mathbf{V}(f_1, \ldots f_s))$.*

Ejemplo 4.1.1 $\mathbf{I}(\mathbf{V}(X^2, Y^2))$ *no está contenido en (X^2, Y^2) puesto que*

$$\mathbf{I}(\mathbf{V}(X^2, Y^2)) = (X, Y).$$

Proposición 4.1.4 *Sean V y W variedades afines en K^n. Entonces:*
i) $V \subset W$ si y sólo si $\mathbf{I}(V) \supset \mathbf{I}(W)$
ii) $V = W$ si y sólo si $\mathbf{I}(V) = \mathbf{I}(W)$.

En este capítulo nos interesará contestar las siguientes preguntas:

- *Descripción de un ideal:* Dado un ideal $I \subset K[X_1, \ldots, X_n]$, ¿ es posible escribir a I como el ideal $(f_1, \ldots, f_s)$ para algunos $f_1, \ldots, f_s \in K[X_1, \ldots X_n]$?.
- *Pertenencia a un ideal:* Si $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, ¿existe un algoritmo para decidir si un polinomio f en $K[X_1, \ldots, X_n]$ pertenece al ideal $(f_1, \ldots, f_s)$?.
- *Nullstellensatz:* Dados $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, ¿ cuál es la relación exacta entre $(f_1, \ldots, f_s)$ e $\mathbf{IV}(f_1, \ldots, f_s)$?.

Las dos primeras preguntas las contestamos en la próxima sección y la tercera en la sección 4.3.

4.2. Bases de Gröbner

En esta sección comenzamos dando la definición de orden monomial y presentamos distintos órdenes monomiales en $K[X_1, \ldots, X_n]$.

Identificamos en $K[X_1, \ldots, X_n]$ los monomios $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ con las n-uplas $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.

Definición 4.2.1 *Un* **orden monomial** *sobre $K[X_1, \ldots, X_n]$ es una relación $>$ sobre $\mathbb{N}_0^n$, que satisface las siguientes condiciones:*
i) $>$ es un orden total sobre $\mathbb{N}_0^n$.
ii) Si $\alpha > \beta$ y $\gamma \in \mathbb{N}_0^n$, entonces $\alpha + \gamma > \beta + \gamma$.
iii) $>$ es un buen orden sobre $\mathbb{N}_0^n$.

Observemos que en términos de monomios la condición ii) de la definición anterior se traduce en

ii) Si $X^\alpha > X^\beta$ y $\gamma \in \mathbb{N}_0^n$, entonces $X^\alpha X^\gamma > X^\beta X^\gamma$.

El lema que sigue nos da una condición necesaria y suficiente para que el conjunto $(\mathbb{N}_0^n, >)$ esté bien ordenado.

Lema 4.2.1 *Una relación de orden $>$ sobre $\mathbb{N}_0^n$ es un buen orden si y sólo si toda sucesión estrictamente decreciente en $\mathbb{N}_0^n$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

es estacionaria.

Los órdenes que presentamos a continuación son algunos de los más utilizados en Álgebra Computacional.

Definición 4.2.2 (Orden Lexicográfico) *Sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n)$ en $\mathbb{N}_0^n$. Decimos que $\alpha >_{lex} \beta$ si y sólo si existe $i \in \{1, \ldots, n\}$ que verifica $\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}$ y $\alpha_i > \beta_i$. Notaremos $X^\alpha >_{lex} X^\beta$ si $\alpha >_{lex} \beta$.*

Las variables $X_1, \ldots, X_n$ se ordenan de manera usual usando el orden $>_{lex}$.

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 0, 1),$$

i.e. $X_1 >_{lex} X_2 >_{lex} \ldots >_{lex} X_n$.

Proposición 4.2.1 *El orden $>_{lex}$ (o simplemente lex) sobre $\mathbb{N}_0^n$ es un orden monomial.*

Es importante destacar que existen otros órdenes lex, según como se ordenen las variables, por ejemplo

$$X_n > X_{n-1} > \ldots > X_1.$$

Desde el punto de vista computacional existen otros órdenes más eficientes que el *lex* llamados órdenes de grado. Estos comparan primero los órdenes totales y en caso de ser iguales, quiebran la igualdad con algún otro orden. Entre ellos podemos mencionar los siguientes:

Definición 4.2.3 (Orden Lexicográfico Graduado) *Sean α y $\beta \in \mathbb{N}_0^n$. Decimos que $\alpha >_{glex} \beta$ si*

$$\mid \alpha \mid = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = \mid \beta \mid, \ o \ \mid \alpha \mid = \mid \beta \mid \ y \ \alpha >_{lex} \beta.$$

Las variables se ordenan de acuerdo al orden lex, i.e.

$$X_1 >_{glex} X_2 >_{glex} \ldots >_{glex} X_n.$$

El orden *rlex* que definimos a continuación es el más eficiente desde el punto de vista computacional.

Definición 4.2.4 (Orden Lexicográfico Graduado Inverso) *Sean $\alpha, \beta \in \mathbb{N}_0^n$. Decimos que $\alpha >_{rlex} \beta$ si*

$$\mid \alpha \mid = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = \mid \beta \mid,$$

$$o \ \mid \alpha \mid = \mid \beta \mid \ y \ existe \ i \in \{1, \ldots, n\} : \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n \ y \ \alpha_i < \beta_i.$$

Proposición 4.2.2 *Los órdenes glex y rlex son órdenes monomiales.*

Un orden monomial permite ordenar los monomios de un polinomio f en $K[X_1, \ldots, X_n]$. De esta menera, una vez fijado el orden, distinguimos los elementos que se definen a continuación:

Definición 4.2.5 *Sea* $f = \sum_\alpha a_\alpha X^\alpha$ *un polinomio no nulo en* $K[X_1, \ldots, X_n]$ *y sea* $>$ *un orden monomial. Llamamos*
i) **multigrado** *de* f *(relativo a* $>$*)* a

$$multideg(f) = max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\},$$

ii) **coeficiente principal** *de* f *a*

$$LC(f) = a_{multidegf} \in K,$$

iii) **monomio principal** *de* f *a*

$$LM(f) = X^{multideg(f)} \text{ y}$$

iv) **término principal** *de* f *a*

$$LT(f) = LC(f) \cdot LM(f).$$

Ejemplo 4.2.1 *Dado* $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$ *el polinomio queda ordenado según los órdenes*

lex: $f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$ *donde*
$LC(f) = -5, \quad multideg(f) = (3, 0, 0), \quad LT(f) = -5X^3$ *y* $LM(f) = X^3$

glex: $f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2$ *donde*
$LC(f) = 7, \quad multideg(f) = (2, 0, 2), \quad LT(f) = 7X^2Z^2$ *y* $LM(f) = X^2Z^2$

rlex: $f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2$ *donde*
$LC(f) = 4, \quad multideg(f) = (1, 2, 1), \quad LT(f) = 4XY^2Z$, *y* $LM(f) = XY^2Z$

De manera análoga al caso de una sóla variable podemos dar la siguiente proposición.

Proposición 4.2.3 *Sean* f *y* $g \in K[X_1, \ldots, X_n]$ *polinomios no nulos y* $>$ *un orden monomial. Entonces:*
i) $multideg(f.g) = multideg(f) + multideg(g)$.
ii) $LT(f.g) = LT(f).LT(g)$.
iii) Si $f + g \neq 0, multideg(f + g) \leq max\{multideg(f), multideg(g)\}$. *Si* $LT(f) + LT(g) \neq 0$ *entonces* $LT(f + g) = max\{LT(f), LT(g)\}$.

Otro orden monomial útil es el siguiente:

Definición 4.2.6 *Sea* $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$, $>_\sigma$ *un orden monomial (como el lex o el rlex) sobre* $\mathbb{N}_0^n$. *Definimos para* α *y* β *en* $\mathbb{N}_0^n$, $\alpha >_{\mathbf{u},\sigma} \beta$ *si y sólo si*

$$\mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta \text{ o } \mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta \text{ y } \alpha >_\sigma \beta.$$

Llamamos a $>_{\mathbf{u},\sigma}$ *el* **orden pesado** *determinado por* $\mathbf{u}$ *y* $>_\sigma$

Proposición 4.2.4 *El orden $>_{\mathbf{u},\sigma}$ satisface las siguientes propiedades:*
i) $>_{\mathbf{u},\sigma}$ es un orden monomial.
ii) Si $\mathbf{u} = (1, 1, \ldots, 1)$ entonces $>_{\mathbf{u},lex}$ coincide con el orden glex.
iii) Si i es un entero $1 \leq i \leq n$ y $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$, donde u tiene i unos, y $n - i$ ceros, el orden pesado $>_{\mathbf{u},rlex}$ se llama **i-ésimo orden de eliminación** *$>_i$. Este orden $>_i$ satisface la siguiente propiedad:*

$$f \in K[X_{i+1}, \ldots, X_n] \Leftrightarrow LT(f) \in K[X_{i+1}, \ldots, X_n]$$

iv) El orden lexicográfico también verifica la propiedad enunciada en iii) para el i-ésimo orden de eliminación.

El estudio de los ideales monomiales es el camino previo a la definición de base de Gröbner que daremos al final de esta sección. La definición de ideal monomial en $K[X_1, \ldots, X_n]$ es la siguiente:

Definición 4.2.7 *Decimos que un ideal $I \subset K[X_1, \ldots, X_n]$ es un* **ideal monomial** *si existe un subconjunto $A \subset \mathbb{N}_0^n$ (posiblemente infinito) tal que I está formado por todos los polinomios que son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha X^\alpha$, donde $h_\alpha \in K[X_1, \ldots, X_n]$. En este caso escribimos $I = (\{X^\alpha : \alpha \in A\})$.*

Un ejemplo de ideal monomial es $I = (X^4Y^2, X^3Y^4, X^2Y^5) \subset K[X, Y]$. Los monomios que pertenecen a un ideal monomial nos los da el siguiente lema:

Lema 4.2.2 *Sea $I = (\{X^\alpha : \alpha \in A\})$ un ideal monomial. Entonces un monomio $X^\beta \in I$ si y sólo si X^β es divisible por X^α para algún $\alpha \in A$.*

Demostración: $\Rightarrow$) Supongamos que $X^\beta \in I$, entonces $X^\beta = \sum_{i=1}^s h_i X^{\alpha(i)}$, donde $h_i \in K[X_1, \ldots X_n]$ y $\alpha(i) \in A$. Si descomponemos h_i como combinación lineal de sus monomios, vemos que cada término de la derecha de la ecuación es divisible por algún $X^{\alpha(i)}$. Luego X^β debe cumplir la misma propiedad.
$\Leftarrow$) Si X^β es un múltiplo de X^α para algún $\alpha \in A$, entonces $X^\beta \in I$ por definición de ideal. □

Podemos determinar cuando un polinomio f pertenece a un ideal monomial observando sus monomios.

Lema 4.2.3 *Sea I un ideal monomial, y sea $f \in K[X_1, \ldots, X_n]$. Entonces las siguientes condiciones son equivalentes:*
i)$f \in I$.
ii) Todo término de f está en I.
iii) f es una combinación K-lineal de los monomios en I.

El lema que sigue prueba que todos los ideales monomiales de $K[X_1, \ldots, X_n]$ están finitamente generados.

Teorema 4.2.1 (Lema de Dickson) *Sea $I = (\{X^\alpha : \alpha \in A\})$ un ideal monomial de $K[X_1, \ldots, X_n]$. Entonces I puede escribirse en la forma $I = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$, donde $\alpha(1), \ldots, \alpha(s) \in A$. En particular I tiene una base finita.*

Demostración: Demostramos el teorema haciendo inducción sobre el número de variables. Si $n = 1$, entonces I está generado por los monomios X^α, donde $\alpha \in A \subset \mathbb{N}_0$. Sea β el menor elemento de $A \subset \mathbb{N}_0$. Entonces X^β divide a todos los otros generadores, y por lo tanto $I = (X^\beta)$.

Sea $n > 1$ y supongamos que el teorema es cierto para $n - 1$. Notemos las variables como $X_1, \ldots, X_{n-1}, Y$, así los monomios en $K[X_1, \ldots, X_{n-1}, Y]$ pueden escribirse como $X^\alpha Y^m$, donde $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}_0^{n-1}$ y $m \in \mathbb{N}_0$.

Supongamos que $I \subset K[X_1, \ldots X_{n-1}, Y]$ es un ideal monomial. Sea J el ideal en $K[X_1, \ldots, X_{n-1}]$ generado por los monomios X^α para los cuales $X^\alpha Y^m \in I$ para algún $m \geq 0$. Como J es un ideal monomial en $K[X_1, \ldots, X_{n-1}]$, por hipótesis de inducción J está generado por un número finito de X^α, i.e. $J = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$.

Por la construcción de J, para cada $i \in \{1, \ldots, s\}$, resulta que $X^{\alpha(i)} Y^{m_i} \in I$ para algún $m_i \geq 0$. Tomando $m = max\{m_1, \ldots, m_s\}$ resulta que $X^{\alpha(i)} Y^m \in I$. Para cada k, con $0 \leq k \leq m - 1$ sea J_k el ideal de $K[X_1, \ldots, X_{n-1}]$ generado por los monomios X^β tales que $X^\beta Y^k \in I$. Por hipótesis de inducción, J_k tiene un conjunto finito de generadores, es decir $J_k = (\{X^{\alpha_k(1)}, \ldots, X^{\alpha_k(s_k)}\})$.

Probemos que I está generado por los siguientes monomios:

$$
\begin{aligned}
de\ J\ &: X^{\alpha(1)} Y^m, \ldots, X^{\alpha(s)} Y^m, \\
de\ J_0\ &: X^{\alpha_0(1)}, \ldots, X^{\alpha_0(s_0)}, \\
de\ J_1\ &: X^{\alpha_1(1)} Y, \ldots, X^{\alpha_1(s_1)} Y, \\
&\vdots \\
de\ J_{m-1}\ &: X^{\alpha_{m-1}(1)} Y^{m-1}, \ldots, X^{\alpha_{m-1}(s_{m-1})} Y^{m-1}.
\end{aligned}
$$

Probemos primero que todo monomio de I es divisible por algún monomio de la lista. Sea $X^\alpha Y^p \in I$. Si $p \geq m$, entonces $X^\alpha Y^p$ es divisible por algún $X^{\alpha(i)} Y^m$ por la construcción de J. Por otro lado, si $p \leq m - 1$, entonces $X^p Y^p$ es divisible por algún $X^{\alpha_p(j)} Y^p$ por la construcción de J_p. Luego por el lema 4.2.2 resulta que el ideal generado por los monomios de $J, J_0, J_1, \ldots, J_{m-1}$ está contenido en I. Como además I está contenido trivialmente en el ideal generado por $J, J_0, J_1, \ldots, J_{m-1}$ queda probada la primera parte del teorema.

Para finalizar la demostración hace falta probar que el conjunto finito de generadores puede extraerse de un conjunto de generadores del ideal. Si $I = \{X^\alpha : \alpha \in A\} \subset K[X_1, \ldots, X_n]$ entonces por lo demostrado anteriormente, $I = (X^{\beta(1)}, \ldots, X^{\beta(s)})$ para algunos monomios $X^{\beta(i)} \in I$. Luego $X^{\beta(i)}$ es divisible por algún $X^{\alpha(i)}$. De aquí es fácil probar que $I = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$, lo que completa la demostración. $\square$

Corolario 4.2.1 *Sea $>$ una relación sobre $\mathbb{N}_0^n$ que satisface:*
i) $>$ es un orden total sobre $\mathbb{N}_0^n$.
ii) si $\alpha > \beta$ y $\gamma \in \mathbb{N}_0^n$, entonces $\alpha + \gamma > \beta + \gamma$.
Entonces $>$ es un buen orden si y sólo si $\alpha \geq 0$ para todo $\alpha \in \mathbb{N}_0^n$.

A los efectos de poder resolver el problema de pertenencia a un ideal en el anillo $K[X_1, \ldots, X_n]$, necesitamos un algoritmo que extienda el algoritmo de división conocido en $K[X]$. Nuestro objetivo será dividir un polinomio $f \in K[X_1, \ldots, X_n]$ por s polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$.

De manera similar al caso de una sóla variable, necesitamos cancelar el término principal del polinomio f, (con respecto a un orden monomial fijo), multiplicando algún f_i por un monomio apropiado y restándolo luego. Este monomio se convertirá luego en un término del cociente. Para realizar el proceso de una manera ordenada definimos primero una *partición* del conjunto $\mathbb{N}_0^n$.

Dado $>$ un orden monomial sobre $\mathbb{N}_0^n$ y dados $f_1, \ldots, f_s$ polinomios no nulos en $K[X_1, \ldots, X_n]$, definimos la siguiente partición de $\mathbb{N}_0^n$:

$$\Delta_1 = multideg(f_1) + \mathbb{N}_0^n,$$

$$\Delta_2 = (multideg(f_2) + \mathbb{N}_0^n) - \Delta_1,$$

$$\vdots$$

$$\Delta_s = (multideg(f_s) + \mathbb{N}_0^n) - \cup_{j<s}\Delta_j,$$

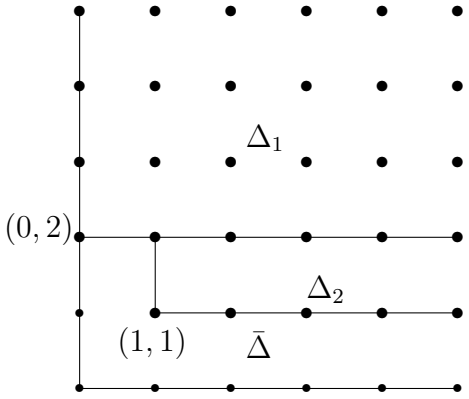
$$\bar{\Delta} = \mathbb{N}_0^n - \cup_{i=1}^{s}\Delta_i.$$

Probaremos que en las condiciones anteriores, dado $f \in K[X_1, \ldots, X_n]$ existen únicos $q_1, \ldots, q_s, r \in K[X]$ tales que:
i) $f = q_1 f_1 + \ldots + q_s f_s + r$,
ii) Si $q_i = \sum c_\alpha X^\alpha$ y $c_\alpha \neq 0$ entonces $\alpha + multideg(f_i) \in \Delta_i$,
iii) Si $r = \sum c_\alpha X^\alpha$ y $c_\alpha \neq 0$ entonces $\alpha \in \bar{\Delta}$.

Para ilustrar de manera clara el proceso, comenzamos dando un ejemplo.

Ejemplo 4.2.2 *Supongamos que queremos dividir el polinomio $f = X^2Y + XY^2 + Y^2$ por $f_1 = Y^2 - 1$ y $f_2 = XY - 1$ donde el orden elegido es el orden lexicográfico con $X > Y$. Entonces se tiene:*

$\Delta_1 = multideg(f_1) + \mathbb{N}_0^2 = (0,2) + \mathbb{N}_0^2$,
$\Delta_2 = multideg(f_2) + \mathbb{N}_0^2 - \Delta_1 = (1,1) + \mathbb{N}_0^2 - \Delta_1$, *y*
$\bar{\Delta} = \mathbb{N}_0^2 - (\Delta_1 \cup \Delta_2)$



Como $f = X^2Y + XY^2 + Y^2$ *entonces* $multideg(f) = (2,1) \in \Delta_2$.
Para eliminar el término principal de f *hacemos*

$$f^{(1)} = f - Xf_2 = XY^2 + Y^2 + X, \quad multideg(f^{(1)}) = (1,2) \in \Delta_1.$$

Para eliminar el término principal de $f^{(1)}$

$$f^{(2)} = f^{(1)} - Xf_1 = Y^2 + 2X, \quad multideg(f^{(2)}) = (1,0) \in \bar{\Delta},$$

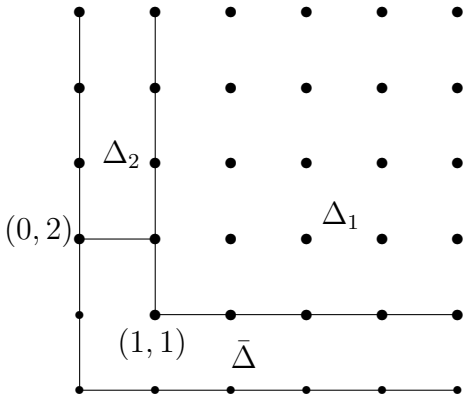
y así sucesivamente obtenemos

$$f^{(3)} = f^{(2)} - 2X = Y^2, \quad multideg(f^{(3)}) = (0,2) \in \Delta_1,$$
$$f^{(4)} = f^{(3)} - f_1 = 1, \quad multideg(f^{(4)}) = (0,0) \in \bar{\Delta},$$
$$f^{(5)} = f^{(4)} - 1 = 0.$$

Despejando resulta

$$f = (X+1)f_1 + Xf_2 + 2X + 1.$$

Es importante observar que si en cambio dividimos $f = X^2Y + XY^2 + Y^2$ *por* f_2 *y* f_1 *obtenemos*
$\Delta_1 = multideg(f_2) + \mathbb{N}_0^2 = (1,1) + \mathbb{N}_0^2$,
$\Delta_2 = multideg(f_1) + \mathbb{N}_0^2 - \Delta_1 = (0,2) + \mathbb{N}_0^2 - \Delta_1$, *y*
$\bar{\Delta} = \mathbb{N}_0^2 - (\Delta_1 \cup \Delta_2)$



Como $multideg(f) = (2,1) \in \Delta_1$ *resulta*

$f^{(1)} = f - Xf_2 = XY^2 + Y^2 + X, \quad multideg(f^{(1)}) = (1,2) \in \Delta_1,$
$f^{(2)} = f^{(1)} - Yf_2 = Y^2 + Y + X, \quad multideg(f^{(2)}) = (0,2) \in \Delta_2,$
$f^{(3)} = f^{(2)} - f_1 = Y + X + 1, \quad multideg(f^{(3)}) = (1,0) \in \bar{\Delta},$
$f^{(4)} = f^{(3)} - X = Y + 1, \quad multideg(f^{(4)}) = (0,1) \in \bar{\Delta},$
$f^{(5)} = f^{(4)} - Y = 1, \quad multideg(f^{(5)}) = (0,0) \in \bar{\Delta},$
$f^{(6)} = f^5 - 1 = 0.$
Así podemos expresar a f *como*
$f = (X + Y)f_2 + f_1 + (X + Y + 1).$

Puede observarse en el ejemplo que los cocientes y el resto que se obtienen al dividir f por f_1 y f_2 no son los mismos que los que se obtienen al dividir f por f_2 y f_1.

La forma general del algoritmo cuya demostración puede verse en [28] es la siguiente:

Teorema 4.2.2 (Algoritmo de División) *Sea* $>$ *un orden monomial sobre el anillo* $K[X_1, \ldots, X_n]$ *y* $F = \{f_1, \ldots, f_s\}$ *una s-upla ordenada de polinomios en* $K[X_1, \ldots, X_n]$. *Entonces para cada* $f \in K[X_1, \ldots, X_n]$, *existen únicos* $q_1, \ldots, q_s$ *y* $r \in K[X_1, \ldots, X_n]$ *tales que:*
i) $f = q_1 f_1 + \ldots + q_s f_s + r$,
ii) Si $q_i = \sum c_\alpha X^\alpha$ *y* $c_\alpha \neq 0$ *entonces* $\alpha + multideg(f_i) \in \Delta_i$,
iii) Si $r = \sum c_\alpha X^\alpha$ *y* $c_\alpha \neq 0$ *entonces* $\alpha \in \bar{\Delta}$.
Además si $q_i \neq 0$, $multideg(q_i) + multideg(f_i) \leq multideg(f)$ *y si* $r \neq 0$, $multideg(r) \leq multideg(f)$.

En el ejemplo 4.2.2 vimos que un cambio en el orden de los polinomios del conjunto por el cual dividimos determina que el resto no esté unívocamente determinado. Sin embargo, el algoritmo de división en $K[X]$ no posee este problema. Para resolver el problema de pertenencia a un ideal, una condición suficiente se obtiene fácilmente como corolario del teorema 4.2.2. Si luego de dividir f por $F = \{f_1, \ldots, f_s\}$ se obtiene $r = 0$, entonces $f \in (f_1, \ldots, f_s)$. Sin embargo el ejemplo que sigue muestra que $r = 0$ no es una condición necesaria para que f pertenezca al ideal $(f_1, \ldots, f_s)$.

Ejemplo 4.2.3 *Sean los polinomios* $f_1 = XY + 1$, $f_2 = Y^2 - 1 \in K[X, Y]$ *y lex el orden elegido. Al dividir* $f = XY^2 - X$ *por* $F = \{f_1, f_2\}$, *el resultado es*

$$XY^2 - X = Y.(XY + 1) + 0.(Y^2 - 1) + (-X - Y).$$

Si el orden de F *es* $F = \{f_2, f_1\}$, *se tiene*

$$XY^2 - X = X.(Y^2 - 1) + 0.(XY + 1) + 0.$$

Nuestro objetivo es buscar un sistema de generadores "adecuado"para el ideal I donde el resto esté unívocamente determinado y la condición $r = 0$ sea *equivalente* a la pertenencia al ideal.

Definición 4.2.8 *Sea $I \subset K[X_1, \ldots, X_n]$ un ideal no nulo y $>$ un orden monomial fijo. El* **ideal principal de I** *es el ideal generado por los términos principales de los polinomios $f \in I - \{0\}$, i.e.*

$$LT(I) = (\{LT(f)/f \in I - \{0\}\}).$$

Proposición 4.2.5 *Sea $I \subset K[X_1, \ldots, X_n]$ un ideal. Entonces*
i) $LT(I)$ es un ideal monomial.
ii) Existen $g_1, \ldots, g_t \in I$ tales que $LT(I) = (LT(g_1), \ldots, LT(g_t))$.

Demostración:
i) El ideal monomial $(X^\alpha : \alpha = mutideg(g), g \in I - \{0\})$ coincide con el ideal monomial $(LT(g) : g \in I - \{0\})$, ya que X^α y $LT(g)$ difieren sólo en una constante no nula. Luego $LT(I)$ es un ideal monomial.
ii) Como $LT(I)$ es un ideal monomial, entonces por el lema de Dickson existen $g_1, \ldots, g_t \in I$ tales que $LT(I) = (LT(g_1), \ldots, LT(g_t))$. □

Ahora estamos en condiciones de demostrar el teorema de la base de Hilbert.

Teorema 4.2.3 (Teorema de la base de Hilbert) *Todo ideal $I \subset K[X_1, \ldots, X_n]$ tiene un conjunto finito de generadores. Luego $I = (g_1, \ldots, g_t)$ para algunos $g_1, \ldots, g_t \in I$.*

Demostración: Si $I = (0)$ el teorema es válido.
Si $I \neq (0)$ entonces eligiendo un orden monomial sobre $K[X_1, \ldots, X_n]$ construimos el conjunto de generadores $g_1, \ldots, g_t$ de I de la siguiente manera. Por la proposición 6.1.1, existen $g_1, \ldots, g_t \in I$ tales que $LT(I) = (LT(g_1), \ldots, LT(g_t))$. Veamos que $I = (g_1, \ldots, g_t)$.

Como cada $g_i \in I$ entonces $(g_1, \ldots, g_t) \subset I$. Recíprocamente, dado $f \in I$, al dividir f por $g_1, \ldots, g_t$, aplicando el algoritmo de la división obtenemos

$$f = a_1 g_1 + \ldots a_t g_t + r$$

donde $r \in \bar{\Delta}$. Probemos que $r = 0$. El polinomio

$$r = f - a_1 g_1 - \ldots - a_t g_t \in I.$$

Si $r \neq 0$, entonces $LT(r) \in LT(I) = (LT(g_1), \ldots, LT(g_t))$, y por el lema 4.2.2 resulta que algún $LT(g_i)$ debe ser divisible por $LT(r)$. Contradicción. Luego $r = 0$ y

$$f \in (g_1, \ldots, g_t),$$

lo que demuestra que $I \subset (g_1, \ldots, g_t)$. □

Definición 4.2.9 *Un anillo A se dice* **noetheriano** *si todo ideal I de A está finitamente generado.*

El teorema de la base de Hilbert nos dice que el anillo $K[X_1, \ldots, X_n]$ es noetheriano. Es importante observar que si A es un anillo conmutativo las siguientes condiciones son equivalentes:
i) A es noetheriano
ii) Toda cadena ascendente de ideales de A (respecto de la inclusión) es estacionaria.

La condición ii) se conoce con el nombre de **condición de cadena ascendente**. Veamos la equivalencia anterior para el caso particular en que A es el anillo de polinomios $K[X_1, \ldots, X_n]$.

Teorema 4.2.4 (Condición de cadena ascendente) *Sea $I_1 \subset I_2 \subset I_3 \subset \ldots$ una cadena ascendente de ideales en $K[X_1, \ldots, X_n]$. Entonces existe un $N \geq 1$ tal que $I_N = I_{N+1} = I_{N+2} = \ldots$.*

En el anillo $K[X_1, \ldots, X_n]$ el teorema de la base de Hilbert es una consecuencia de la condición de cadena ascendente.
En efecto, supongamos que existe un ideal $I \subset K[X_1, \ldots, X_n]$ que no tiene un conjunto finito de generadores. Sea $f_1 \in I$ y consideremos $I_1 = (f_1)$. Como I no está finitamente generado existe $f_2 \in I$ tal que $f_2 \notin I_1$. Luego llamando $I_2 = (f_1, f_2)$, como I no está finitamente generado resulta $I_1 \subset I_2 \subset I$. Continuando con este procedimiento obtenemos la cadena ascendente

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

que no es estacionaria. Contradicción.

Del teorema 4.2.4 y la observación anterior resulta que **el teorema de la base de Hilbert** es equivalente a la **condición de cadena ascendente.**

A continuación introducimos el concepto de base de Gröbner y vemos que estas bases sí solucionan el problema de pertenencia a un ideal.

Definición 4.2.10 *Fijado un orden monomial, un subconjunto finito $G = \{g_1, \ldots, g_t\}$ de un ideal I se dice una* **base de Gröbner** *(o* **base standard***) de I si*

$$LT(I) = (LT(g_1), \ldots, LT(g_t)).$$

Corolario 4.2.2 *Sea $>$ un orden monomial. Entonces todo ideal $I \subset K[X_1, \ldots, X_n]$ distinto del $\{0\}$ tiene una base de Gröbner. Más aún, cualquier base de Gröbner de un ideal I es una base de I.*

Demostración: Dado un ideal no nulo I, el conjunto $G = \{g_1, \ldots, g_t\}$ construido en la demostración del teorema 4.2.3 cumple con la definición de base de Gröbner. Además como $LT(I) = (LT(g_1), \ldots, LT(g_t))$ el argumento dado en el teorema 4.2.3 prueba que $I = (g_1, \ldots, g_t)$. Luego G es una base de I. □

Proposición 4.2.6 *Si $I = (f_1, \ldots, f_s)$, entonces $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.*

A continuación veremos un método para determinar cuando una base de un ideal I es una base de Gröbner.

Al dividir un polinomio por una base de Gröbner el resto queda unívocamente determinado, como lo prueba la proposición que sigue.

Proposición 4.2.7 *Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner de un ideal I de $K[X_1, \ldots, X_n]$ y sea $f \in K[X_1, \ldots, X_n]$. Entonces existe un único $r \in K[X_1, \ldots, X_n]$ tal que r verifica:*
i) Si $r = \sum c_\alpha X^\alpha$ y $c_\alpha \neq 0$ entonces $\alpha \in \bar{\Delta}$.
ii) Existe $g \in I$ tal que $f = g + r$.

Demostración: Utilizando el algoritmo de la división obtenemos la expresión $f = a_1 g_1 + \ldots + a_t g_t + r$, donde r satisface i), y tomando $g = a_1 g_1 + \ldots + a_t g_t$ se satisface la condición ii), lo que prueba la existencia de r.

Para probar la unicidad supongamos que $f = g_1 + r_1 = g_2 + r_2$ donde r_1, r_2 satisfacen i) y ii). Entonces $r_2 - r_1 = g_1 - g_2 \in I$. Si $r_1 \neq r_2$, resulta que $LT(r_2 - r_1) \in LT(I) = (LT(g_1), \ldots, LT(g_t))$ y por el lema 4.2.2, $LT(r_2 - r_1)$ es divisible por algún $LT(g_i)$. Contradicción, pues ningún término de r_1, r_2 es divisible por algún $LT(g_i)$. Luego $r_1 = r_2$. □

Si G es una base de Gröbner de I, y f, G y r son como en la proposición anterior, notaremos **fRG** al resto de la división de f por la base $G = \{g_1, \ldots, g_t\}$. Por la proposición 4.2.7, **fRG** no depende del orden de la sucesión $g_1, \ldots, g_t$ sino del orden monomial elegido.

Corolario 4.2.3 *Si $G = \{g_1, \ldots, g_t\}$ es una base de Gröbner para un ideal I de $K[X_1, \ldots, X_n]$, y $f \in K[X_1, \ldots, X_n]$ entonces $f \in I$ si y sólo si el resto de dividir f por G es cero.*

Demostración: Ya probamos que si el resto es cero, $f \in I$. Recíprocamente dado $f \in I$, $f = f + 0$ satisface las dos condiciones de la proposición 4.2.7. Luego 0 es el resto de dividir f por G. □

El corolario 4.2.3 nos da un algoritmo para resolver el problema de pertenencia a un ideal. Calculando el resto de la división de un polinomio f por G podemos determinar directamente si $f \in I$.

Ahora veamos cuándo un conjunto dado de generadores de un ideal I es una base de Gröbner.

Definición 4.2.11 *Sean $f, g \in K[X_1, \ldots, X_n]$ polinomios no nulos. Llamamos* **S-polinomio** *de f y g a la combinación*

$$fSg = \frac{X^\gamma}{LT(f)} \cdot f - \frac{X^\gamma}{LT(g)} \cdot g,$$

donde $X^\gamma = MCM(LM(f), LM(g))$.

Los S-polinomios nos permiten determinar cuando una base de un ideal es una base de Gröbner como lo prueba el teorema siguiente cuya demostración puede verse en [28].

Teorema 4.2.5 *Sea $I \subset K[X_1, \ldots, X_n]$ un ideal no nulo y $>$ un orden monomial sobre $\mathbb{N}_0^n$. Entonces $G = \{f_1, \ldots, f_s\}$ es una base de Gröbner de I para el orden $>$ si y sólo si para todo $i, j \in \{1, \ldots, s\}$ resulta que $(f_i S f_j) R\{f_1, \ldots, f_s\} = 0$.*

El siguiente ejemplo muestra cómo podemos ver que un conjunto G es una base de Gröbner.

Ejemplo 4.2.4 *El conjunto $G = \{X^3, X^2Y - Y^3, Y^3X, Y^5\}$ es una base de Gröbner del ideal $I = (X^3, X^2Y - Y^3)$ para el orden lex.*

Sean $f_1 = X^3, f_2 = X^2Y - Y^3, f_3 = XY^3$ y $f_4 = Y^5$.

Aplicamos el teorema y calculamos

$f_1 S f_2 = f_3$ *y* $f_3 RG = 0$,
$f_1 S f_3 = 0$,
$f_1 S f_4 = 0$,
$f_2 S f_3 = -f_4$ *y* $f_4 RG = 0$,
$f_2 S f_4 = -Y^7$, $Y^7 RG = 0$,
$f_3 S f_4 = 0$,

Luego G es una base de Gröbner de I.

Ahora veamos cómo obtener una base de Gröbner a partir de un conjunto de generadores $F = \{f_1, \ldots, f_s\}$ de un ideal I. Al calcular el S-polinomio de f_1 y f_2, puede suceder que el resto de dividir $f_1 S f_2$ por F sea no nulo. En este caso debemos agregar a F el resto de esta división como un nuevo generador f_{s+1} y verificar si el nuevo conjunto $F \cup \{f_{s+1}\}$ verifica el teorema 4.2.5. Reiterando este procedimiento con todos los generadores obtendremos una base de Gröbner.

Ilustremos este proceso con un ejemplo:

Ejemplo 4.2.5 *Sea $I = (f_1, f_2) = (X^3 - 2XY, X^2Y - 2Y^2 + X)$ con el orden glex.*
$F = \{f_1, f_2\}$ no es una base de Gröbner para I pues $LT(f_1 S f_2) = -X^2 \notin (LT(f_1), LT(f_2))$.

Como $f_1 S f_2 R\{f_1, f_2\} \neq 0$ hacemos $f_3 = f_1 S f_2$ y extendemos el conjunto F a $F = \{f_1, f_2, f_3\}$.

Calculamos $f_1Sf_3 = -2XY$. *Como* $(f_1Sf_3)RF = -2XY \neq 0$ *debemos agregar* $f_4 = -2XY$ *a nuestro conjunto de generadores, i.e.* $F = \{f_1, f_2, f_3, f_4\}$.

Continuando con este procedimiento hacemos
$(f_1Sf_2)RF = (f_1Sf_3)RF = 0$ *y*
$f_2Sf_3 = -2Y^2 + X$ *y* $(f_2Sf_3)RF = -2Y^2 + X \neq 0$.

Debemos agregar también $f_5 = -2Y^2 + X$ *a* F.

Tomando $F = \{f_1, f_2, f_3, f_4, f_5\}$ *resulta*

$$(f_iSf_j)RF = 0 \text{ para todo } 1 \leq i < j \leq 5.$$

Por el teorema 4.2.5, F *es una base de Gröbner.*

Este procedimiento da un algoritmo para encontrar una base de Gröbner de un ideal I.

Una primera versión del **algoritmo de Buchberger** que puede mejorarse es la siguiente:

Teorema 4.2.6 *Sea* $I = (f_1, \ldots, f_s) \neq \{0\}$ *un ideal polinomial. Entonces una base de Gröbner para* I *puede construirse en un número finito de pasos por el algoritmo siguiente:*

Input: $F = (f_1, \ldots, f_s)$
Output: *Una base de Gröbner* $G = \{g_1, \ldots, g_t\}$ *para* I, *con* $F \subset G$
$G := F$
repeat
  $G' := G$
  for *cada par* $\{p, q\}, p \neq q$ *en* G' **do**
    $S := (pSq)RG'$
    if $S \neq 0$ **then** $G := G \cup \{S\}$
until $G = G'$

Demostración: Debemos ver que $G \subset I$. En el comienzo del algoritmo esto se verifica trivialmente. Cuando extendemos G a G' agregando $S := (pSq)RG'$, como $G \subset I$ y $p, q \in I$ entonces $pSq \in I$. Además al dividir por $G' \subset I$, resulta $G \cup \{S\} \subset I$. Como G contiene la base dada F de I entonces G es también una base de I.

El algoritmo finaliza cuando $G = G'$, es decir cuando $(pSq)RG = 0$ para todo $p, q \in G$. Luego por el teorema 4.2.5, G es una base de Gröbner de I.

Veamos ahora que el algoritmo finaliza. Al terminar cada recorrido del bucle principal el conjunto G queda formado por G', (el viejo G) y los restos no nulos de las divisiones de los S-polinomios por los elementos de G'. Luego

$$(LT(G')) \subset (LT(G)) \tag{4}$$

pues $G \subset G'$. Mas aún, si $G' \neq G$ entonces $(LT(G')$ está contenido estrictamente estrictamente en $(LT(G))$. En efecto supongamos que r es un resto no nulo de un

S-polinomio que se ha adjuntado a G. Como r es un resto de una división por G', $LT(r)$ no es divisible por el término principal de ningún término de los elementos de G' y por lo tanto $LT(r) \notin (LT(G'))$, $LT(r) \in (LT(G))$.

Por (4), los ideales de $(LT(G'))$ de las sucesivas iteraciones del bucle forman una cadena ascendente de ideales en $K[X_1, \ldots, X_n]$. Por el teorema 4.2.4 resulta que luego de un número finito de iteraciones, la cadena es estacionaria. Luego se da la igualdad $(LT(G)) = (LT(G'))$, $G = G'$ y el algoritmo finaliza. □

Las bases de Gröbner calculadas en el teorema 4.2.6 suelen ser más grandes de lo necesario. Para obtener una mejora del algoritmo, debemos eliminar los generadores que sobran.

Lema 4.2.4 *Sea G una base de Gröbner para el ideal I. Sea $p \in G$ un polinomio tal que $LT(p) \in (LT(G - \{p\}))$. Entonces $G - \{p\}$ es también una base de Gröbner para I.*

Demostración: Como $(LT(G)) = LT(I)$, si $LT(p) \in (LT(G - \{p\}))$ entonces $(LT(G - \{p\})) = (LT(G))$. Por definición de base de Gröbner resulta que $G - \{p\}$ también es una base de Gröbner para I. □

El lema anterior permite "mejorar" la base de Gröbner G de un ideal I, eliminando los polinomios p de G que satisfacen $LT(p) \in (LT(G - \{p\})$. Además las constantes pueden acomodarse para obtener coeficientes principales 1.

Definición 4.2.12 *Una* **base de Gröbner minimal** *de un ideal polinomial I es una base de Gröbner G de I que satisface:*
i) $LC(p) = 1$ para todo $p \in G$, y
ii) Para todo $p \in G, LT(p) \notin (LT(G - \{p\}))$.

A partir de una base de Gröbner de I podemos obtener una base de Gröbner minimal de un ideal I eliminando los generadores innecesarios que podrían haber sido incluídos.

En el ejemplo 4.2.5 para el orden *lex* habíamos obtenido la base de Gröbner
$G = \{f_1, f_2, f_3, f_4, f_5\}$, donde

$$f_1 = X^3 - 2XY,\ \ f_2 = X^2Y - 2Y^2 + X,\ \ f_3 = -X^2,\ \ f_4 = -2XY,\ \ f_5 = -2Y^2 + X.$$

Primero multiplicamos los polinomios por constantes adecuadas a fin de hacer 1 los coeficientes principales. Luego como $LT(f_1) = X^3 = -X.LT(f_3)$, podemos eliminar f_1. De manera análoga $LT(f_2) = X^2.Y = -(1/2)X.LT(f_4)$, por lo que también podemos eliminar f_2. Como estas son todas las eliminaciones posibles la base de Gröbner minimal está formada por los polinomios

$$\tilde{f}_3 = X^2, \quad \tilde{f}_4 = XY, \quad \tilde{f}_5 = Y^2 - (1/2)X.$$

Es importante observar que un ideal I puede tener más de una base de Gröbner minimal. En efecto $G = \{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$, donde

$$\tilde{f}_3 = X^2 + aXY, \quad \tilde{f}_4 = XY, \quad \tilde{f}_5 = Y^2 - (1/2)X.$$

es también una base minimal del ideal I dado.

Nuestro próximo objetivo es encontrar *una* base de Gröbner minimal determinada *mejor* que las demás. Esta base de Gröbner existe y se llama **base de Gröbner reducida**.

Definición 4.2.13 *Sea I un ideal no nulo de $K[X_1, \ldots, X_n]$ y $>$ un orden monomial sobre $\mathbb{N}_0^n$. La* **escalera** *de I, respecto de $>$ es el conjunto formado por los multigrados de cualquier base de Gröbner minimal de I respecto de $>$.*

Proposición 4.2.8 *Si $f \in I - \{0\}$ y $\{A_1, \ldots, A_n\} \subset \mathbb{N}_0^n$ es la escalera de I respecto de $>$, entonces $multideg(f) \in A_i + \mathbb{N}_0^n$ para algún $i = 1, \ldots, t$.*

Demostración: Si $f \in I - \{0\}$ entonces $LT(f) \in LT(I)$. Si $\{g_1, \ldots, g_t\}$ es una base de Gröbner minimal de I respecto de $>$, donde $multideg(g_i) = A_i$ para $i = 1, \ldots, t$, entonces $LT(f) \in (LT(g_1), \ldots, LT(g_t))$. Luego $multideg(f) = A_i + \gamma$, para algún $i = 1, \ldots, t$ y $\gamma \in \mathbb{N}_0^n$, i.e. $multideg(f) \in A_i + \mathbb{N}_0^n$, para algún $i = 1, \ldots, t$. □

Definición 4.2.14 *Sea I un ideal no nulo de $K[X_1, \ldots, X_n]$ y $>$ un orden monomial. Llamamos* **multigrado de I** *al conjunto*

$$multideg(I) = \{multideg(f)/f \in I - \{0\}\}.$$

La proposición 4.2.8 nos dice que

$$multideg(I) = \bigcup_{i=1}^{t} A_i + \mathbb{N}_0^n, \tag{5}$$

donde $\{A_1, \ldots, A_t\}$ es la escalera de I. Es claro que $multideg(I) \subset \bigcup_{i=1}^t A_i + \mathbb{N}_0^n$. Para demostrar la otra inclusión consideremos $A_i + \beta \in \bigcup_{i=1}^t A_i + \mathbb{N}_0^n$ y $\{g_1, \ldots, g_t\}$ una base de Gröbner minimal de I tal que $multideg(g_i) = A_i$, para $i = 1, \ldots, t$. Entonces $g_i X^\beta \in I - \{0\}$ y $multideg(g_i X^\beta) = multideg(g_i) + multideg(X^\beta) = A_i + \beta$.

De (5) podemos concluir además que $multideg(I) = \bigcup_{i=1}^k multideg(h_i) + \mathbb{N}_0^n$, para cualquier base de Gröbner $\{h_1, \ldots, h_k\}$ de I para el orden monomial dado.

Ahora estamos en condiciones de definir base de Gröbner reducida.

Definición 4.2.15 *Una* **base de Gröbner reducida** *de un ideal polinomial I es una base G de I tal que:*
i) $LC(p) = 1$ para todo $p \in G$.
ii) Para todo $p \in G$, ningún monomio de p pertenece a $LT(G - \{p\})$.

Proposición 4.2.9 *Sea $I \neq \{0\}$ un ideal polinomial. Entonces, para un orden monomial dado, I tiene una única base de Gröbner reducida.*

4.3. Teorema de los ceros de Hilbert. (Hilbert's Nullstellensatz)

Sabemos que dado un cuerpo K, el anillo de polinomios $K[X]$ es un dominio principal. Todo ideal I puede escribirse $I = (f)$ para algún $f \in K[X]$. Si K es algebraicamente cerrado todo polinomio no constante tiene una raíz. Luego si $\mathbf{V}(I) = \emptyset$, f es una constante no nula. De aquí resulta que $1/f \in K$, y por lo tanto $1 = (1/f) \cdot f \in I$. Luego $I = K[X]$ es el único ideal tal que $\mathbf{V}(I) = \emptyset$ cuando K es un cuerpo algebraicamente cerrado.

Podemos extender esta propiedad al caso de más de una variable. Este resultado se conoce con el nombre de *Weak Nullstellensatz* o *versión débil del teorema de los ceros de Hilbert*. La palabra alemana Nullstellensatz está formada por tres palabras simples: Null(Cero), Stellen(Lugar), Satz(Teorema).

Las demostraciones de las versiones fuerte y débil del Teorema de los ceros de Hilbert pueden verse en [7], [12] y [28].

Teorema 4.3.1 *Sea K un cuerpo algebraicamente cerrado. Todo ideal maximal M de $K[X_1, \ldots, X_n]$ es de la forma $M = (X_1 - a_1, \ldots, X_n - a_n)$ donde $(a_1, \ldots, a_n) \in K^n$.*

Teorema 4.3.2 (Versión débil del teorema de los ceros de Hilbert) *Sea K un cuerpo algebraicamente cerrado e I un ideal de $K[X_1, \ldots, X_n]$ tal que $\mathbf{V}(I) = \emptyset$. Entonces $I = K[X_1, \ldots, X_n]$.*

Aplicando el teorema anterior al caso particular $K = \mathbb{C}$, podemos pensar a la Weak Nullstelensatz como el "Teorema Fundamental del Álgebra para polinomios multivariados". Todo sistema de ecuaciones polinomiales que genera un ideal más pequeño que $\mathbb{C}[X_1, \ldots, X_n]$ tiene un cero en común en $\mathbb{C}^n$.

De la versión débil del teorema de los ceros de Hilbert se deduce un algoritmo para determinar si un sistema de ecuaciones polinomiales en $K[X_1, \ldots, X_n]$ con K algebraicamente cerrado,

$$\begin{aligned} f_1(X_1, \ldots, X_n) &= 0 \\ f_2(X_1, \ldots, X_n) &= 0 \\ &\ldots \\ f_s(X_1, \ldots, X_n) &= 0, \end{aligned}$$

es o no compatible. El algoritmo consiste en:

Calcular la base de Gröbner reducida de $I = (f_1, \ldots, f_s)$ respecto de un orden monomial cualquiera.
Esta base es 1 si y sólo si el sistema es incompatible.

El teorema que sigue, demostrado por Hilbert, es uno de los resultados más importantes obtenidos en el siglo XIX.

Teorema 4.3.3 (Versión fuerte del Teorema de los ceros de Hilbert). *Sea K un cuerpo algebraicamente cerrado. Si $f, f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ son tales que $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, entonces existe un entero $m \geq 1$ tal que*

$$f^m \in (f_1, \ldots, f_s).$$

La versión fuerte del teorema de los ceros de Hilbert se puede enunciar de la forma siguiente:
"Sea K un cuerpo algebraicamente cerrado. Si I es un ideal en $K[X_1, \ldots, X_n]$, entonces

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}."$$

En lo que sigue analizamos la relación existente entre variedades afines e ideales.

Teorema 4.3.4 *Sea K un cuerpo arbitrario.*
i) Las aplicaciones

$$\mathbf{I} : variedades\ afines \longrightarrow\ ideales$$

y

$$\mathbf{V} : ideales \longrightarrow\ variedades\ afines$$

son tales que si $I_1 \subset I_2$ son ideales, entonces $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$ y análogamente si $V_1 \subset V_2$ son variedades, entonces $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$. Más aún, para cualquier variedad V, se tiene

$$\mathbf{V}(\mathbf{I}(V)) = V,$$

luego $\mathbf{I}$ es siempre biunívoca.
ii) Si K es algebraicamente cerrado, y si nos restringimos a ideales radicales, entonces las apicaciones

$$variedades\ afines\ \xrightarrow{\mathbf{I}}\ ideales\ radicales$$

y

$$ideales\ radicales\ \xrightarrow{\mathbf{V}}\ variedades\ afines$$

son biyecciones tales que una es la inversa de la otra.

El teorema anterior nos dice que un problema referente a variedades puede verse como un problema algebraico de ideales radicales y recíprocamente, siempre que estemos trabajando en un cuerpo algebraicamente cerrado.

4.4. Teorema de los ceros de Hilbert para cuerpos finitos

En esta sección aplicaremos los resultados vistos en la sección anterior al anillo de polinomios en n indeterminadas sobre un cuerpo finito. Vimos en el capítulo 2 que si K es un cuerpo finito entonces K tiene p^k elementos, siendo p un entero primo positivo y k un número natural.

Lema 4.4.1 *Sea $F(p^k)$ un cuerpo finito e I un ideal de $F(p^k)[X_1, \ldots, X_n]$. Entonces el ideal $I + (X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n)$ es radical.*

Demostración: Sea $J = (X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n)$. Debemos probar que $\sqrt{I+J} = I + J$. Sabemos que todo ideal está contenido en su radical. Luego sólo resta probar que $\sqrt{I+J} \subset I + J$. Dado $f \in \sqrt{I+J}$, existe un entero m tal que $f^m \in I + J$. Sea

$$\varphi : F(p^k)[X_1, \ldots, X_n] \to F(p^k)[X_1, \ldots, X_n]/J$$

el homomorfismo canónico y $\varphi(f) = f + J$, $\varphi(I) = I + J$ las imágenes de f e I respectivamente. Luego $(f + J)^m \in I + J$.
Si $g + J \in F(p^k)[X_1, \ldots, X_n]/J$ entonces $(g + J)^{p^k} = g^{p^k} + J = g + J$. Supongamos sin pérdida de generalidad que $m < p^k$. Como $f^m + J \in I + J$ entonces

$$f + J = (f + J)^{p^k} = (f + J)^m \cdot (f + J)^{p^k - m} = (f^m + J) \cdot (f + J)^{p^k - m} \in I + J.$$

De aquí resulta $f \in I + J$. □

La versión fuerte del Teorema de los ceros de Hilbert en el caso finito nos la da el teorema siguiente:

Teorema 4.4.1 (Versión fuerte del teorema de los ceros de Hilbert para cuerpos finitos.) *Sea $F(p^k)$ un cuerpo finito e $I \subset F(p^k)[X_1, \ldots, X_n]$. Entonces*

$$\mathbf{I}(\mathbf{V}(I)) = I + (X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n)$$

Demostración: Sea $J = (X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n)$. Dado $I \subset F(p^k)[X_1, \ldots, X_n]$, aplicando el teorema de los ceros de Hilbert a $I + J$ y utilizando el lema anterior tenemos que $\mathbf{I}(\mathbf{V}(I+J)) = I + J$. Como $\mathbf{V}(J) = F(p^k)^n$ entonces $\mathbf{V}(I+J) = \mathbf{V}(I)$. Luego $\mathbf{I}(\mathbf{V}(I)) = I + J$. □

Del teorema anterior surge inmediatamente el siguiente teorema:

Teorema 4.4.2 (Versión débil del teorema de los ceros de Hilbert para cuerpos finitos.) *Sea $F(p^k)$ un cuerpo finito y $f_1, \ldots, f_s$, polinomios en $F(p^k)[X_1, \ldots, X_n]$. Entonces $f_1, \ldots, f_s$ no tienen ceros en común en $F(p^k)^n$ si y sólo si $1 \in (f_1, \ldots, f_s, X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n) \subset F(p^k)[X_1, \ldots, X_n]$.*

Demostración: $\Rightarrow$) Supongamos que $f_1, \ldots, f_s$ no tienen ceros en común. Entonces $\mathbf{V}((f_1, \ldots, f_s)) = \emptyset$. Luego $(f_1, \ldots, f_s, X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n) = \mathbf{I}(\emptyset) = (\{1\}) = F(p^k)[X_1, \ldots, X_n]$.
$\Leftarrow$) Inmediata. □

4.5. El cardinal de $V(I)$

En esta sección analizaremos el caso particular en el que la variedad de un ideal $I \subset K[X_1, \ldots, X_n]$ es finita. Primero estudiaremos el caso en que el cuerpo K es algebraicamente cerrado y luego lo aplicaremos a cuerpos finitos.

Sea K un cuerpo y $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ polinomios no nulos. Sea $I = (f_1, \ldots, f_s) \subset K[X_1, \ldots, X_n]$ y $>$ un orden monomial.

El cociente $K[X_1, \ldots, X_n]/I$ es un K-espacio vectorial con la siguiente ley de composición externa

$$\text{“}\cdot\text{”} : K \times K[X_1, \ldots, X_n]/I \to K[X_1, \ldots, X_n]/I$$

definida por $(\alpha, f + I) \to \alpha f + I$.

En lo que sigue veremos que $dim_K K[X_1, \ldots, X_n]/I = \#\mathbb{N}_0^n - LT(I)$.

Definición 4.5.1 *Sea I un ideal propio de $K[X_1, \ldots, X_n]$ Decimos que I es de* **dimensión cero** *si $K[X_1, \ldots, X_n]/I$ es un K-espacio vectorial de dimensión finita.*

Proposición 4.5.1 *Sea $>$ un orden monomial sobre $\mathbb{N}_0^n$ y sea $I \subset K[X_1, \ldots, X_n]$ un ideal no nulo. Entonces $\#\{X^\alpha + I / X^\alpha \notin LT(I)\} = dim_K K[X_1, \ldots, X_n]/I$.*

Demostración: Probemos que $\{X^\alpha + I / X^\alpha \notin LT(I)\}$ es una base del K-espacio vectorial $K[X_1, \ldots, X_n]/I$.

Sea $f + I \in K[X_1, \ldots, X_n]/I$ y sea $\{g_1, \ldots, g_t\}$ una base de Gröbner de I para el orden dado. Entonces

$$f = q_1 g_1 + \ldots + q_t g_t + fRI$$

y por lo tanto $f + I = (fRI) + I$. Como $fRI = \sum_\alpha c_\alpha X^\alpha$ con $X^\alpha \notin LT(I)$ si $c_\alpha \neq 0$, resulta que $\{X^\alpha + I / X^\alpha \notin LT(I)\}$ es un sistema de generadores del $K-$espacio vectorial $K[X_1, \ldots, X_n]/I$.

Veamos que es linealmente independiente. Si existen $a_i \in K$ no todos nulos tal que

$$a_1(X^{\alpha_1} + I) + \ldots + a_s(X^{\alpha_s} + I) = 0, \quad a_i \in K$$

entonces $a_1 X^{\alpha_1} + \ldots + a_s X^{\alpha_s} \in I - \{0\}$. Luego $LT(a_1 X^{\alpha_1} + \ldots + a_s X^{\alpha_s}) \in LT(I)$ y esto nos dice que existe $i \in \{1, \ldots, s\}$ tal que $X^{\alpha_i} \in LT(I)$. Contradicción. $\square$

De la proposición anterior resulta inmediatamente que

$$\#(\{X^\alpha + I / X^\alpha \notin LT(I)\}) = \#\mathbb{N}_0^n - mutideg(I)$$

En efecto la aplicación $\phi : \{X^\alpha + I / X^\alpha \notin LT(I)\} \longrightarrow \mathbb{N}_0^n - mutideg(I)$ dada por $\phi(X^\alpha + I) = \alpha$ está bien definida y es biyectiva.

Por la proposición 4.5.1, si $>$ es un orden monomial,

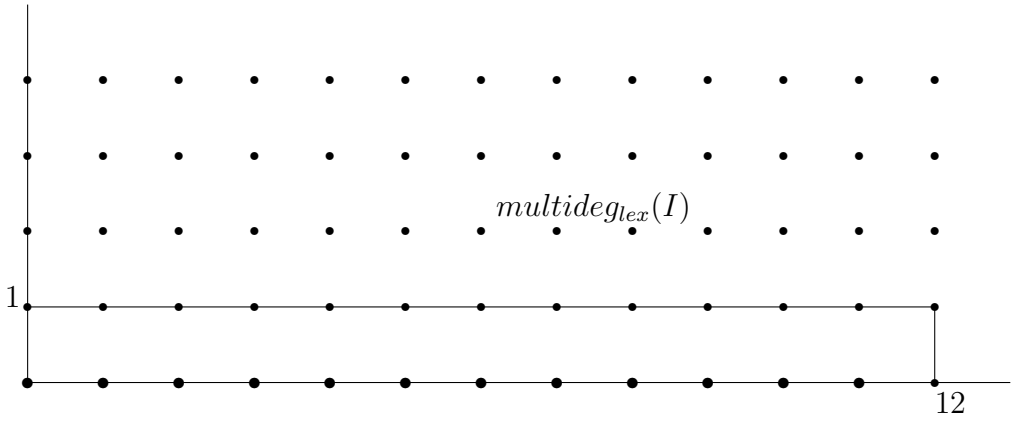
$$dim_K K[X_1, \ldots, X_n]/I = \#\mathbb{N}_0^n - mutideg(I).$$

Corolario 4.5.1 *Si I es un ideal de $K[X_1,\ldots,X_n]$ y $\bar{K}$ es la clausura algebraica de K, entonces $dim_K K[X_1,\ldots,X_n]/I = dim_{\bar{K}} \bar{K}[X_1,\ldots,X_n]/\bar{I}$, donde $\bar{I} = I\bar{K}[X_1,\ldots,X_n]$.*

Demostración: Sea $>$ un orden monomial sobre $\mathbb{N}_0^n$. Entonces que $LT(I) = LT(\bar{I})$. Luego por la proposición 4.5.1 resulta
$dim_K K[X_1,\ldots,X_n]/I = dim_{\bar{K}} \bar{K}[X_1,\ldots,X_n]/\bar{I}$. □

Veamos un ejemplo en donde $V(I)$ es un conjunto finito.

Ejemplo 4.5.1 *Sea $I = (XY^3 - X^2, X^3Y^2 - Y)$.*
Una base de Gröbner de I para el orden lex con $Y > X$ es $\{-X^7 + Y, X^{12} - X^2\}$.



Puede observarse que $\#\mathbb{N}_0^n - multideg_{glex}(I) = \#\mathbb{N}_0^n - multideg_{lex}(I) = 12$.

En el ejemplo anterior $V(I) = \{(a,b) \in \mathbb{C}/a^{12} = a^2 \text{ y } b = a^7\} = \{(0,0)\} \cup \{(a,a^7)/a^{10} = 1\}$ tiene 11 elementos. $V(I)$ es en consecuencia un conjunto finito y su cardinal es menor o igual que 12.

El siguiente teorema prueba este resultado.

Teorema 4.5.1 *Sea I un ideal no nulo de $K[X_1,\ldots,X_n]$ y $>$ un orden monomial. Si $\#\mathbb{N}_0^n - mutideg(I) < \infty$, entonces $\#(V(I)) < \infty$. Además resulta $\#(V(I)) \leq \#\mathbb{N}_0^n - mutideg(I)$.*

Es importante observar que en general $\#(V(I)) < \infty$ no implica que $\#\mathbb{N}_0^n - mutideg(I) < \infty$. En efecto si $I = (X^2 + 1) \subset \mathbb{R}[X,Y]$, resulta $V(I) = \emptyset$, y sin embargo $\#\mathbb{N}_0^2 - mutideg(I)$ es infinito.

La implicación anterior es cierta si K es un cuerpo algebraicamente cerrado.

Teorema 4.5.2 *Sea K un cuerpo algebraicamente cerrado, I un ideal no nulo de $K[X_1,\ldots,X_n]$ y $>$ un orden monomial. Si $\mathbf{V}(I)$ es finito entonces resulta $\#\mathbb{N}_0^n - mutideg(I) < \infty$.*

Corolario 4.5.2 *Si $I = (f_1, \ldots, f_s)$ es un ideal de $K[X_1, \ldots, X_n]$ y $\bar{K}$ es su clausura algebraica, las siguientes condiciones son equivalentes:*
a) I es de dimensión cero.
b) El conjunto de soluciones en $\bar{K}$ del sistema

$$f_1(X_1, \ldots, X_n) = 0,$$

$$f_2(X_1, \ldots, X_n) = 0,$$

$$\ldots$$

$$f_s(X_1, \ldots, X_n) = 0,$$

es finito.

Ahora aplicaremos lo visto anteriormente para poder contar los ceros de un ideal $I = (f_1, \ldots, f_s) \in F(p^k)[X_1, \ldots X_n]$.

Por la proposición 4.5.1, dado un cuerpo K cualquiera, $\{X^\alpha + I / X^\alpha \notin LT(I)\}$ es una base del K- espacio vectorial $K[X_1, \ldots, X_n]/I$. Tomando $K = F(p^k)$ obtenemos una base del $F(p^k)$-espacio vectorial $F(p^k)[X_1, \ldots X_n]/I$.

Lema 4.5.1 *Sea $V = \{\alpha_1, \ldots, \alpha_m\}$ una variedad de $F(p^k)^n$ e $I = I(V)$. Si consideramos al espacio vectorial sobre $F(p^k)$, $F(p^k)[X_1, \ldots, X_n]/I$, entonces $dim(F(p^k)[X_1, \ldots X_n]/I) = m$.*

Demostración: Dado $a \in F(p^k)^n$, sea a_i la i-esima coordenada de a.

Si $m = 1$ entonces I se anula en un único punto a si y sólo si I es de la forma $(X_1 - a_1, \ldots, X_n - a_n)$.

En efecto, si $f \in (X_1 - a_1, \ldots, X_n - a_n)$ entonces $f(a) = 0$. Por otro lado si $f \in I$, al dividir f por el conjunto $\{X_1 - a_1, \ldots, X_n - a_n\}$, se tiene

$$f = \sum_{i=1}^{n} h_i(X_i - a_i) + r,$$

donde $h_i \in F(p^k)[X_1, \ldots X_n]$ y $r \in F(p^k)$. Como $f(a) = 0$ entonces $r = 0$. Luego

$$f \in (X_1 - a_1, \ldots, X_n - a_n)$$

y $dim(F(p^k)[X_1, \ldots X_n]/I) = 1$.

Sea $m > 1$ y consideremos $\alpha_1 \in V$. Supongamos que cualquiera sea α_j con $j \in \{2, \ldots, n\}$, α_1 y α_j difieren en la i-ésima coordenada. Construimos

$$g_j(x) = \frac{x_i - \alpha_{ji}}{\alpha_{1i} - \alpha_{ji}}$$

y sea

$$f_1(x) = \prod_{j=2}^{n} g_j(x).$$

Entonces

$$f_1(\alpha_1) = 1 \text{ y } f_1(\alpha_2) = \ldots = f_1(\alpha_m) = 0.$$

Sea $\{f_1, f_2, \ldots, f_m\}$ el conjunto de funciones definidas especialmente para cada elemento de V, i.e. tales que $f_j(\alpha_i) = 1$ si $j = i$ y $f_j(\alpha_i) = 0$ si $j \neq i$.

Veamos que $\{f_1 + I, \ldots, f_m + I\}$ es una base de $F(p^k)[X_1, \ldots X_n]/I$.

Sea $b_i \in F(p^k)$ con $i \in \{1, \ldots, m\}$ tal que

$$b_1(f_1 + I) + \ldots + b_m(f_m + I) = 0 + I.$$

Entonces $b_1 f_1 + \ldots + b_m f_m \in I$. Luego, para cada $i \in \{1, \ldots, m\}$,
$b_1 f_1(\alpha_i) + \ldots + b_m f_m(\alpha_i) = 0$, pero como $f_j(\alpha_j) = 1$ y $f_j(\alpha_i) = 0$ si $i \neq j$ entonces $b_1 f_1(\alpha_i) + \ldots + b_m f_m(\alpha_i) = b_j$. Luego $b_j = 0$ para todo $j \in \{1, \ldots, m\}$.

Sea $h + I \in F(p^k)[X_1, \ldots, X_n]/I$ y $q_i = h(\alpha_i) \in F(p^k)$. Entonces

$$h - (q_1 f_1 + \ldots + q_m f_m) \in I = I(V).$$

Luego $h + I - (q_1(f_1 + I) + \ldots + q_m(f_m + I)) = 0 + I$ y el conjunto $\{f_1 + I, \ldots, f_m + I\}$ genera $F(p^k)[X_1, \ldots X_n]/I$.

Hemos probado que $dim_{F(p^k)}(F(p^k)[X_1, \ldots X_n]/I) = m$. □

Ejemplo 4.5.2 *Sea* $I = (X^2 + X + 1, X \cdot Y, Y^2 + Y, Y^2) \subset F(3^2)[X, Y]$. *Una base de Gröbner minimal para el orden lex de* I *es*

$$\{X^2 + X + 1, Y\}.$$

$V(I) = \{(1, 0)\}$, *donde* $(1, 0)$ *es raíz doble y* $\#(N_0^2 - multideg_{lex}(I)) = 2$

Teorema 4.5.3 *Sea* I *un ideal de* $F(p^k)[X_1, \ldots X_n]$ *y* $G = \{g_1, \ldots, g_s\}$ *una base de Gröbner de* $I + (X_1^{p^k} - X_1, \ldots, X_n^{p^k} - X_n)$. *Si* $\#(\{X^\alpha + I / X^\alpha \notin LT(I)\}) = m$, *entonces* I *se anula en exactamente* m *puntos distintos en* $F(p^k)^n$.

Demostración: Por el teorema 4.4.1, resulta $I(V(I)) = (g_1, \ldots, g_s)$. y por el lema 4.5.1 se tiene

$$dim(F(p^k)[X_1, \ldots X_n]/I(V(I)) = dim(F(p^k)[X_1, \ldots X_n]/(g_1, \ldots, g_s)) = \#(V(I))$$

y por lo tanto $\#(V(I)) = \#(\{X^\alpha + I / X^\alpha \notin LT(I)\}) = m$. □

Ejemplo 4.5.3 *Sea* $I = (X^2 \cdot Y + X + Y, X + X \cdot Y^2) \subset F(2^2)[X, Y]$. *Una base de Gröbner minimal para el orden lex de* I *es*

$$\{Y^3 + Y, X + X \cdot Y^2, X \cdot Y + Y^2 + X^2\}.$$

$V(I) = \{(0,0); (\alpha + 1, 1); (\alpha, 1)\}$ *siendo* α *raíz de* $X^2 + X + 1$ *y* $(\alpha + 1, 1); (\alpha, 1)$ *raíces dobles. Luego* $\#(V(I)) = 5 = \#(N_0^2 - multideg_{lex}(I))$.

El ideal radical $I + \sqrt{I} = (X^2 \cdot Y + X + Y, X + X \cdot Y^2, X^4 - X, Y^4 - Y)$, *tiene a*

$$G = \{Y^2 + Y, X + X \cdot Y, X + Y + X^2\}$$

como base de Gröbner minimal para el orden lex.

$V(I) = \{(0,0); (\alpha + 1, 1); (\alpha, 1)\}$ *siendo* α *raíz de* $X^2 + X + 1$ *y*
$\#(N_0^2 - multideg_{lex}(I)) = \#(V(I)) = 3$.

Capítulo 5

Resolución de sistemas de ecuaciones sobre las álgebras de Post k-cíclicas.

En los capítulos 3, 5 y 6 se concentran los resultados originales de esta tesis. Ahora nos ocuparemos de mostrar cómo podemos resolver sistemas de ecuaciones algebraicas sobre un álgebra de Post k-cíclica de orden p con p primo, utilizando la interpretación dada en el capítulo 3, las bases de Gröbner definidas en el capítulo 4 y algoritmos programados en Maple que pueden verse en el apéndice.

En la primera sección damos la forma normal disyuntiva de una función de Post en n variables [15] y el teorema que da una condición de consistencia para determinar cuando una ecuación algebraica postiana en n variables tiene solución [38].

En la segunda sección aplicamos la interpretación dada en el capítulo 3 para obtener la expresión de una ecuación algebraica postiana en el anillo $F(p^k)[X_1, \ldots, X_n]$, donde $F(p^k)$ es un cuerpo con p^k elementos. Esta interpretación nos permite ver un sistema de ecuaciones en $F(p^k)[X_1, \ldots, X_n]$, buscar una base de Gröbner del ideal formado por los polinomios del sistema, analizar la existencia de soluciones y abordar su búsqueda. Para ilustrar este proceso presentamos cuatro ejemplos en donde explicamos detalladamente nuestro método para resolver sistemas de ecuaciones polinomiales en las álgebras de Post k-cíclicas de orden p.

5.1. Ecuaciones algebraicas postianas.

Comenzamos dando la definición de función de Post en n variables y algunos resultados probados por G. Epstein y M. Serfati en [15], [38] que nos permitirán analizar una ecuación algebraica en n variables.

Definición 5.1.1 *Una* **función de Post** *en n variables es una función que puede obtenerse a partir de las funciones constantes* $E_i(X_1, \ldots, X_n) = e_i$ *y la función*

identidad $I_j(X_1,\ldots,X_n) = X_j$ *mediante un número finito de operaciones* $\vee$, $\wedge$ *y* C_i, *para* $0 \leq i \leq r-1$.

Las funciones I_j llamadas identidades por Epstein son para nosotros proyecciones.

La reducción de una función de Post a una forma dada es una herramienta muy útil para resolver sistemas de ecuaciones algebraicas. El siguiente teorema muestra que toda función de Post en n variables satisface la forma normal disyuntiva.

Teorema 5.1.1 (Epstein) *Si* f *es una función de Post en* n *variables* $X_1,\ldots,X_n$, *entonces*

$$f(X_1,\ldots,X_n) = \bigvee_{0\leq i_j\leq r-1} f(e_{i_1},\ldots,e_{i_n}) \wedge C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n).$$

Demostración: Los r^n términos de la forma $C_{i_1}(X_1), C_{i_2}(X_2),\ldots,C_{i_n}(X_n)$ se denominan los fundamentos de las n variables. Por el axioma (P3) de la definición 1.2.2 del capítulo 1, resulta que los fundamentos son disjuntos y el supremo de todos ellos es $\mathbf{1}$. El ínfimo de dos fundamentos distintos debe incluir un ínfimo de la forma $C_i(X_j) \wedge C_k(X_j) = 0$, con $i \neq k$ para algún j, y

$$\bigvee_{0\leq i_j\leq r-1} C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n) = \bigwedge_{j=1}^{n} (\bigvee_{i_j=0}^{r-1} C_{i_j}(X_j)) = \bigwedge_{j=1}^{n} 1 = 1$$

Como el supremo de todos los fundamentos es $\mathbf{1}$, el teorema es válido para todas las funciones constantes E_i y por (P7) para las funciones identidad I_j. Además si f, g satisfacen el teorema entonces $f \vee g$ lo satisface, y como los fundamentos son disjuntos, $f \wedge g$ también.

Supongamos que f es una función de Post que verifica el teorema. Por el axioma (P4) y por el teorema 1.2.2, cada término $f(e_{i_1},\ldots,e_{i_n})$ es igual a algún e_j, con $0 \leq j \leq r-1$. Luego

$$f(X_1,\ldots,X_n) = \bigvee_{k=0}^{r-1} e_k \wedge T_k,$$

donde $T_k = \bigvee_{(i_1,\ldots,i_n)/f(e_{i_1},\ldots,e_{i_n})=e_k} C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n)$. Como los fundamentos son disjuntos dos a dos y el supremo es $\mathbf{1}$, el teorema 1.2.2 nos dice que $C_k(f(X_1,\ldots,X_n)) = T_k$. Pero por el teorema 1.2.2

$$\bigvee_{0\leq i_j\leq n-1} C_k(f(e_{i_1},\ldots,e_{i_n}))C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n) = T_k.$$

Luego $C_k(f(e_{i_1},\ldots,e_{i_n}))$ satisface el teorema, lo que completa la demostración. □

Serfati introduce en [38] la siguiente definición de polinomio postiano.

Definición 5.1.2 *Un polinomio postiano en n variables sobre un álgebra de Post L de orden r, es un elemento f de la subálgebra de Post de $P^{(P^n)}$ generada por la familia de proyecciones $(p_1, \ldots, p_n)$, donde $p_i(X_1, \ldots, X_n) = X_i$.*

A partir de esta definición resulta que si f es un polinomio postiano entonces f satisface la forma normal disyuntiva del teorema 5.1.1. Además Serfati prueba en [38] que recíprocamente, toda función de Post que verifica la forma normal disyuntiva del teorema 5.1.1 pertenece a la subálgebra generada por la familia de las proyecciones.

La forma normal disyuntiva es única y tiene propiedades de "transparencia" con respecto a las operaciones usuales de un álgebra de Post, resultados que se demustran mediante los teoremas 1.2.3, 1.2.7 y 1.2.9 del capítulo 1.

Proposición 5.1.1 *El conjunto de todos los polinomios postianos en n variables sobre un álgebra de Post P de orden r es una r-álgebra de Post, notada por $\Omega_n(P)$.*

Si f es un polinomio postiano, entonces la ecuación

$$f(X) = 0$$

es una ecuación algebraica postiana. Comenzamos analizando la solución de esta ecuación algebraica en una sóla variable.

Aplicando el teorema 5.1.1 vemos que si f es una función de Post en una variable entonces f puede expresarse en la forma

$$f(X) = \bigvee_{0 \leq i \leq r-1} f(e_i) \wedge C_i(X).$$

M. Serfati da en [38] una condición de consistencia que permite determinar si una ecuación en una variable tiene solución, y una fórmula para encontrarla cuando ésta existe.

Teorema 5.1.2 (Serfati) *Una condición necesaria y suficiente para que la ecuación*

$$f(X) = \bigvee_{i=0}^{r-1} C_i(X) \wedge f(e_i) = 0 \quad \text{(I)}$$

sea consistente es que

$$\bigwedge_{i=0}^{r-1} f(e_i) = 0. \quad \text{(C1)}$$

Una solución de la ecuación está dada por

$$\hat{X} = \bigvee_{i=0}^{r-1} C_0(f(e_i)) \wedge e_i.$$

A esta solución se la denomina **solución fundamental**.

Corolario 5.1.1 *Las componentes postianas de la solución fundamental son las siguientes*

$$C_{r-1}(\hat{X}) = C_0(f(e_{r-1})), \quad C_0(\hat{X}) = \bigwedge_{1\leq s\leq r-1} (C_0(f(e_s))'$$

y para $1 \leq j \leq r-2$,

$$C_j(\hat{X}) = C_0(f(e_j)) \wedge \bigwedge_{j+1\leq s\leq r-1} (C_0(f(e_s)))'.$$

Ahora daremos el teorema que estudia la consistencia de una ecuación algebraica en n variables

$$f(X_1, \ldots, X_n) = 0.$$

Teorema 5.1.3 *[38] Una condición necesaria y suficiente para que la ecuación*

$$f(X_1, \ldots, X_n) = \bigvee_{0\leq i_j\leq r_-1} f(e_{i_1}, \ldots, e_{i_n}) \wedge C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n) = 0 \quad \text{(II)}$$

tenga solución está dada por la condición

$$\bigwedge_{0\leq i_j\leq r_-1} f(e_{i_1}, \ldots, e_{i_n}) = 0 \qquad \text{(C2)}$$

Demostración: El teorema es válido para $n = 1$ por el teorema 5.1.2. Supongamos que es cierto para cualquier elemento de $\Omega_{n-1}(P)$ y sea $f \in \Omega_n(P)$. Entonces

$$f(X_1, \ldots, X_n) = \bigvee_{0\leq i_j\leq r_-1} f(e_{i_1}, \ldots, e_{i_n}) \wedge C_{i_1}(X_1) \wedge \ldots \wedge C_{i_n}(X_n) = 0.$$

Luego

$$\bigvee_{0\leq i_1\leq r-1} C_{i_1}(X_1) \wedge (\bigvee_{0\leq i_j\leq r-1} (f(e_{i_1}, \ldots, e_{i_n}) \wedge C_{i_2}(X_2) \wedge \ldots \wedge C_{i_n}(X_n))) = 0,$$

y por la condición de consistencia relativa a X_1 dada en el teorema 5.1.2 resulta

$$0 = \bigwedge_{0\leq i_1\leq r-1} (\bigvee_{0\leq i_j\leq r-1} f(e_{i_1}, \ldots, e_{i_n}) \wedge C_{i_2}(X_2) \wedge \ldots \wedge C_{i_n}(X_n)).$$

Esta última expresión tiene la forma

$$\bigvee_{0\leq i_j\leq r-1} (C_{i_2}(X_2) \wedge \ldots \wedge C_{i_n}(X_n) \wedge (\bigwedge_{0\leq i_1\leq r-1} f(e_{i_1}, \ldots, e_{i_n}))) = g_1(X_2, \ldots, X_n) = 0.$$

Por la hipótesis de inducción, esta ecuación relativa a $X_2, \ldots, X_n$ es consistente si y sólo si

$$\bigwedge_{0\leq i_j\leq r-1, 2\leq j\leq n} (\bigwedge_{0\leq i_1\leq r-1} (f(e_{i_1}, \ldots, e_{i_n})) = 0 = \bigwedge_{0\leq i_j\leq r-1} f(e_{i_1}, \ldots, e_{i_n}).$$

□

Una aplicación del teorema 5.1.3 es el método de las eliminaciones sucesivas. Si la condición $(C2)$ se satisface en la ecuación

$$f(X_1, \ldots, X_n) = 0,$$

podemos escribirla como una ecuación relativa a X_1. Eliminando esta primer variable obtenemos una ecuación algebraica en $n-1$ variables, $g_1(X_2, \ldots, X_n) = 0$, y repitiendo este procedimiento sucesivas veces llegamos a la ecuación algebraica en una sola variable

$$g_{n-1}(X_n) = 0,$$

que puede resolverse paramétricamente.

Sin embargo este método tiene dos problemas. En primer lugar nada puede hacerse cuando la condición $(C1)$ no se satisface, y en segundo lugar, aún cumpliendo con esta condición, puede resultar muy complicado obtener su solución. En la próxima sección veremos una forma más efectiva y completa de estudiar las soluciones no sólo de una ecuación, sino de un sistema de ecuaciones cuando r es un número primo.

5.2. Ecuaciones algebraicas sobre las álgebras de Post k-cíclicas de orden p.

En esta sección estudiamos ecuaciones algebraicas en las álgebras de Post k-cíclicas de orden p con p primo. La interpretación dada en el capítulo 3 y las bases de Gröbner descriptas en el capítulo 4 permitirán analizar la existencia y búsqueda de soluciones de diferentes sistemas.

Si las condiciones de consistencia dadas en los teoremas 5.1.2 y 5.1.3 no se satisfacen entonces no es posible resolver una ecuación algebraica dada. En estos casos surgen de manera natural preguntas que iremos respondiendo en este capítulo y en el siguiente.

- ¿Qué podemos hacer si un polinomio f no satisface la condición (C1) o (C2)?.
- ¿Cuándo un sistema de ecuaciones es compatible?.
- ¿Qué caminos podemos utilizar para encontrar la solución cuando sabemos que existe?.

En el capítulo 3 demostramos en el teorema 3.2.2 y en el corolario 3.2.1 que existe una interpretación Φ_1 de $\mathcal{V}(L_{p,k})$ en $\mathcal{V}(F(p^k))$ y una interpretación Φ_2 de $\mathcal{V}(F(p^k))$ en $\mathcal{V}(L_{p,k})$ tal que $\Phi_1\Phi_2(B) = B$, cualquiera sea $B \in \mathcal{V}(L_{p,k})$ y $\Phi_2\Phi_1(R) = R$ para todo $R \in \mathcal{V}(F(p^k))$, [1].

El teorema 3.2.2 da un método constructivo para encontrar las operaciones del cuerpo $F(p^k)$ en términos de las operaciones de un álgebra de Post k-cíclica $L_{p,k}$ y recíprocamente. Los algoritmos programados en MAPLE dados en el apéndice nos muestran cómo obtener de manera efectiva estas operaciones fijados p y k. Si la condición (C1) o (C2) no se satisface podemos interpretar la ecuación $f(X) = 0$ en el lenguaje del cuerpo $F(p^k)$. De esta manera obtenemos un polinomio f que tendrá sus soluciones en una extensión $F(p^t)$ de $F(p^k)$. Finalmente, utilizando nuevamente la interpretación mencionada, buscamos la expresión del polinomio postiano f sobre la nueva álgebra de Post t-cíclica de orden p, $L_{p,t}$.

Comencemos dando un ejemplo de una ecuación algebraica en una variable.

Ejemplo 5.2.1 *Dado el polinomio*

$$f(X) = C_0(X) \vee (C_1(X) \wedge e_1) \vee (C_2(X) \wedge e_1) \in L_{3,1}[X],$$

como $e_2 \wedge e_1 \wedge e_1 \neq 0$ *la ecuación* $f(X) = 0$ *no satisface la condición* $(C1)$ *y en consecuencia no tiene solución en* $L_{3,1}$.

Vimos en el capítulo 3 que podemos obtener a partir del cuerpo $F(3) = \{0, 1, 2\}$ *una estructura de álgebra de Post* L_3 *sobre el conjunto* $\{0, 1, 2\}$.

Aplicando el teorema 3.2.2 y los algoritmos **xinfy3**, **xsupy3** *y* $\mathbf{C_i3}$ *dados en el apéndice habíamos obtenido en el capítulo 3, las operaciones* $\wedge, \vee, \sim, C_0, C_1$ *y* C_2 *como términos en el lenguaje de* F_3. *Éstas eran:*

$x \wedge y = x^2y^2 + 2x^2y + 2xy^2 + 2xy,$
$x \vee y = 2x^2y^2 + x^2y + xy^2 + xy + x + y,$
$\sim x = 2x + 1,$
$C_0(x) = 2x^2 + 1,\ C_1(x) = 2x^2 + x,\ C_2(x) = 2x^2 + 2x,$
$T(x) = x.$

Por otra parte el algoritmo **polinf(x,y)** *nos da el polinomio en* $F(3)[X]$*:*

$$f(X) = X^2 + 1.$$

Las soluciones de la ecuación algebraica $f(X) = 0$ *están en el cuerpo* $F(3^2)$, *lo que hace necesario construir sobre* $F(3^2)$ *la estructura de álgebra de Post* k*-cíclica* $L_{3,2}$.

Los algoritmos **infimo32**, **supremo32**, **T32** *and* $\mathbf{C_i32}$ *nos permiten obtener las operaciones de* $L_{3,2}$ *como términos en el lenguaje de* $F(3^2)$.

$$x \wedge y = x^6[y^6 + 2y^4 + 2y^3 + 2y^2] + x^4[2y^6 + 2y^4 + y^2 + 2y]$$

$$+x^3[2y^6+y^3+y^2+2y]+x^2[2y^6+y^4+y^3+y^2]$$
$$+x[2y^4+2y^3+2y],$$
$$x\vee y=x^6[2y^6+y^4+y^3+y^2]+x^4[y^6+y^4+2y^2+y]$$
$$+x^3[y^6+2y^3+2y^2+y]+x^2[y^6+2y^4+2y^3+2y^2]$$
$$+x[y^4+y^3+y+1]+y,$$

$\sim x=2x+2$,
$C_0(x)=x^6+x^4+2x^2+2$, $C_1(x)=x^6+x^4+2x^2+x$, $C_2(x)=x^6+x^4+2x^2+2x$,
$T(x)=x^3$.

El algoritmo **xdely32(terxL32(x,2),[2,2])** *dado en el apéndice nos da la expresión de* $f(X)=X^2+1$ *en* $L_{3,2}[X]$

$$f(X)=(C_0(X)\wedge C_0(T(X))\wedge \mathbf{e_1})\vee(C_0(X)\wedge C_2(T(X)))\vee(C_0(X)\wedge C_1(T(X)))\vee$$
$$\vee(C_1(X)\wedge C_1(T(X)))\vee(C_2(X)\wedge C_2(T(X))),$$

siendo $\mathbf{e_1}=[2,2]$.

Como $f(X)$ *satisface la condición* (C1), *la ecuación algebraica* $f(X)=0$ *tiene solución y se anula en* $\langle 1,2\rangle$ *and* $\langle 2,1\rangle$, *que son las raíces* ε^2 *y* ε^6 *del polinomio* $f(X)=X^2+1=0$ *en* $F(3^2)[X,Y]$.

El próximo ejemplo es un sistema de dos ecuaciones algebraicas en dos variables.

Ejemplo 5.2.2 *Consideremos el siguiente sistema de ecuaciones en* $L_3[X,Y]$,

$f(X)=C_0(X)\vee(C_1(X)\wedge e_1)\vee(C_2(X)\wedge e_1)=0$.
$g(X,Y)=(C_1(X)\wedge C_2(Y)\wedge e_1)\vee(C_2(X)\wedge C_1(Y)\wedge e_1)\vee(C_1(X)\wedge C_1(Y))\vee$
$\vee(C_2(X)\wedge C_2(Y))=0$.

Vimos en el ejemplo anterior que si bien la primera ecuación algebraica no satisface la condición (C1), sí lo hace la ecuación buscada en $L_{3,2}[X,Y]$.

Por otra parte, la ecuación $g(X,Y)=0$ *verifica la condición (C2), pero aún debemos analizar la compatibilidad del sistema en* $L_{3,2}[X,Y]$ *y hallar las soluciones en caso de que existan.*

Utilizando los algoritmos del apéndice **polinf(x)** *y* **poling(x,y)** *vemos que el sistema de ecuaciones correspondiente en* $F(3)[X,Y]$ *es*

$f(X)=X^2+1=0$
$g(X,Y)=X\cdot Y=0$.

Para saber si el sistema tiene solución sobre $F(3^2)$ *buscamos una base de Gröbner del ideal* $I=(f,g)$. *Utilizando el software Maple obtenemos:*

$I=(X\cdot Y,X^2+1)$;
$GB=Groebner[Basis](I,plex(X,Y),characteristic=3)$;

$$GB = \{Y, X^2 + 1\}$$

Por lo visto en el capítulo 4 el sistema original y el sistema

$f(X) = X^2 + 1 = 0$
$t(Y) = Y = 0$

tienen el mismo conjunto solución en la extensión $F(3^2)$ *de* $F(3)$. *Las soluciones del sistema son* $(\epsilon^2, 0)$ *y* $(\epsilon^6, 0)$.

Utilizando los algoritmos **xdely32(terxL32(x,2),[2,2])** *y* **terxyL32(x,y)** *obtenemos las ecuaciones correspondientes del sistema original en* $L_{3,2}[X, Y]$*:*

$$g(X,Y) = \{[(C_2(X) \wedge C_2(T(X)) \wedge C_2(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_1(Y)) \vee$$

$$\vee (C_2(X) \wedge C_1(T(X)) \wedge C_2(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_1(T(Y))) \vee$$

$$\vee (C_0(X) \wedge C_2(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee (C_0(X) \wedge C_1(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee$$
$$\vee (C_1(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee$$
$$\vee (C_0(X) \wedge C_1(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee (C_1(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee$$
$$\vee (C_2(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee$$
$$\vee (C_1(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_1(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_2(T(Y))) \vee$$
$$\vee (C_0(X) \wedge C_1(T(X)) \wedge C_1(Y) \wedge C_2(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_2(Y) \wedge C_1(T(Y)))] \wedge \mathbf{e_1}\} \vee$$

$$[(C_2(X) \wedge C_1(T(X)) \wedge C_1(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_2(T(Y))) \vee$$

$$(C_2(X) \wedge C_2(T(X)) \wedge C_1(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_2(Y)) \vee$$

$$(C_0(X) \wedge C_2(T(X) \wedge C_0(Y)) \wedge C_1(T(Y))) \vee (C_0(X) \wedge C_1(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee$$
$$(C_0(X) \wedge C_1(T(X)) \wedge C_2(Y) \wedge C_1(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_1(Y) \wedge C_2(T(Y))) \vee$$
$$(C_1(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee$$
$$(C_1(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_2(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_1(T(Y))) \vee$$
$$(C_1(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee$$
$$(C_0(X) \wedge C_1(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_2(Y) \wedge C_0(T(Y)))].$$

$$f(X) = (C_0(X) \wedge C_0(T(X)) \wedge \mathbf{e_1}) \vee (C_0(X) \wedge C_1(T(X))) \vee (C_0(X) \wedge C_2(T(X))) \vee$$

$$(C_1(X) \wedge C_1(T(X))) \vee (C_2(X) \wedge C_2(T(X))) = 0.$$

El sistema original es equivalente en $L_{3,2}[X, Y]$ al siguiente:

$f(X) = (C_0(X) \wedge C_0(T(X)) \wedge \mathbf{e_1}) \vee (C_0(X) \wedge C_1(T(X))) \vee (C_0(X) \wedge C_2(T(X))) \vee$
$\vee (C_1(X) \wedge C_1(T(X))) \vee (C_2(X) \wedge C_2(T(X))) = 0,$

$t(Y) = (C_1(Y) \wedge \mathbf{e_1}) \vee C_2(Y) = 0.$

Este último sistema resulta mucho más simple de resolver y tiene el mismo conjunto solución

$$X = (1,2), Y = (0,0); \qquad X = (2,1), Y = (0,0).$$

En los dos ejemplos anteriores fue posible hallar las soluciones del problema planteado. Sin embargo, podemos encontrarnos con un problema sin solución, es decir que no exista un álgebra $L_{p,t} \in \mathcal{V}(L_{p,k})$ sobre la cual un sistema sea compatible. Para ilustrarlo veamos el siguiente ejemplo:

Ejemplo 5.2.3 *Dado el sistema*

$h(X,Y) = C_0(X) \vee C_0(Y) \vee (C_1(X) \wedge C_1(Y) \wedge e_1) \vee (C_2(X) \wedge C_2(Y) \wedge e_1) = 0$
$g(X,Y) = (C_1(X) \wedge C_2(Y) \wedge e_1) \vee (C_2(X) \wedge C_1(Y) \wedge e_1) \vee (C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y)) = 0,$

puede observarse que ambas ecuaciones satisfacen la condición (C1).

El sistema equivalente en $F(3)$ es

$h(X,Y) = X \cdot Y + 1 = 0$
$g(X,Y) = X \cdot Y = 0.$

Calculando una base de Gröbner del ideal $I = (f,g)$ obtenemos:
$I = (X \cdot Y, X \cdot Y + 1);$
$GB = Groebner[Basis](I, pleX(X,Y), characteristic = 3);$

$$GB = \{1\}$$

Por la versión débil del teorema de los ceros de Hilbert (teorema 4.3.2), el sistema no tiene solución. No existe una extensión $L_{3,k}$ de L_3, cualquiera sea $k \in N$ tal que el sistema sea compatible.

Los **algoritmos** *correspondiente a los polinomios de este ejemplo se encuentran en el apéndice.*

Ejemplo 5.2.4 *El siguiente sistema de ecuaciones polinomiales tiene expresiones complicadas en algunas de sus ecuaciones.*

$f_1(X) = (C_1(X) \wedge C_0(T(X)) \wedge \mathbf{e_1}) \vee (C_1(X) \wedge C_2(T(X)) \wedge \mathbf{e_1}) \vee (C_0(X) \wedge \mathbf{e_1}) \vee (C_2(X) \wedge \mathbf{e_1}) \vee$

$(C_2(X) \wedge C_0(T(X)) \vee (C_2(X) \wedge C_1(T(X))) \vee (C_0(X) \wedge C_2(T(X))) \vee (C_0(X) \wedge C_1(T(X))) = 0.$

$f_2(X,Y) = \{[(C_2(X) \wedge C_2(T(X)) \wedge C_2(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_1(Y)) \vee$

$$\vee(C_2(X) \wedge C_1(T(X)) \wedge C_2(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_1(T(Y)))\vee$$
$$\vee(C_0(X)\wedge C_2(T(X))\wedge C_0(Y)\wedge C_2(T(Y)))\vee(C_0(X)\wedge C_1(T(X))\wedge C_0(Y)\wedge C_1(T(Y)))\vee$$
$$\vee(C_1(X)\wedge C_0(T(X))\wedge C_0(Y)\wedge C_2(T(Y)))\vee(C_2(X)\wedge C_0(T(X))\wedge C_0(Y)\wedge C_1(T(Y)))\vee$$
$$\vee(C_0(X)\wedge C_1(T(X))\wedge C_2(Y)\wedge C_0(T(Y)))\vee(C_1(X)\wedge C_0(T(X))\wedge C_2(Y)\wedge C_0(T(Y)))\vee$$
$$\vee(C_2(X)\wedge C_0(T(X))\wedge C_1(Y)\wedge C_0(T(Y)))\vee(C_0(X)\wedge C_2(T(X))\wedge C_1(Y)\wedge C_0(T(Y)))\vee$$
$$\vee(C_1(X)\wedge C_0(T(X))\wedge C_1(Y)\wedge C_1(T(Y)))\vee(C_2(X)\wedge C_0(T(X))\wedge C_2(Y)\wedge C_2(T(Y)))\vee$$
$$\vee(C_0(X)\wedge C_1(T(X))\wedge C_1(Y)\wedge C_2(T(Y)))\vee(C_0(X)\wedge C_2(T(X))\wedge C_2(Y)\wedge C_1(T(Y)))]\wedge\mathbf{e_1}\}\vee$$
$$[(C_2(X) \wedge C_1(T(X)) \wedge C_1(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_2(T(Y)))\vee$$
$$(C_2(X) \wedge C_2(T(X)) \wedge C_1(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_2(Y))\vee$$
$$(C_0(X)\wedge C_2(T(X)\wedge C_0(Y))\wedge C_1(T(Y)))\vee(C_0(X)\wedge C_1(T(X))\wedge C_0(Y)\wedge C_2(T(Y)))\vee$$
$$(C_0(X)\wedge C_1(T(X))\wedge C_2(Y)\wedge C_1(T(Y)))\vee(C_0(X)\wedge C_2(T(X))\wedge C_1(Y)\wedge C_2(T(Y)))\vee$$
$$(C_1(X)\wedge C_0(T(X))\wedge C_0(Y)\wedge C_1(T(Y)))\vee(C_2(X)\wedge C_0(T(X))\wedge C_0(Y)\wedge C_2(T(Y)))\vee$$
$$(C_1(X)\wedge C_0(T(X))\wedge C_2(Y)\wedge C_2(T(Y)))\vee(C_2(X)\wedge C_0(T(X))\wedge C_1(Y)\wedge C_1(T(Y)))\vee$$
$$(C_1(X)\wedge C_0(T(X))\wedge C_1(Y)\wedge C_0(T(Y)))\vee(C_2(X)\wedge C_0(T(X))\wedge C_2(Y)\wedge C_0(T(Y)))\vee$$
$$(C_0(X)\wedge C_1(T(X))\wedge C_1(Y)\wedge C_0(T(Y)))\vee(C_0(X)\wedge C_2(T(X))\wedge C_2(Y)\wedge C_0(T(Y)))].$$

$$f_3(Y) = \{[(C_0(Y) \wedge C_2(T(Y))) \vee (C_0(Y) \wedge C_1(T(Y))) \vee (C_2(Y) \wedge C_1(T(Y)))\vee$$
$$\vee(C_2(Y) \wedge C_0(T(Y)))] \wedge \mathbf{e_1}\} \vee (C_1(Y) \wedge C_1(T(Y))) = 0.$$

$$f_4(Y) = \{[(C_0(Y) \wedge C_2(T(Y))) \vee (C_0(Y) \wedge C_1(T(Y))) \vee (C_1(Y) \wedge C_1(T(Y)))\vee$$
$$\vee(C_2(Y) \wedge C_2(T(Y)))] \wedge \mathbf{e_1}\} \vee (C_1(Y) \wedge C_2(T(Y))) \vee (C_2(Y) \wedge C_1(T(Y)))\vee$$
$$\vee(C_1(Y) \wedge C_0(T(Y))) \vee (C_2(Y) \wedge C_0(T(Y))) = 0.$$

Todas las ecuaciones satisfacen (C1) o (C2), y el sistema equivalente en $F(3^2)[X, Y]$ *es:*

$f_1(X) = X^2 + X + 1 = 0$
$f_2(X, Y) = X \cdot Y = 0$
$f_3(Y) = Y^2 + Y = 0$
$f_4(Y) = Y^2 = 0.$

Una base de Gröbner del ideal $I = (X^2 + X + 1, X \cdot Y, Y^2 + Y, Y^2)$ *es*

$$GB = \{Y, X^2 + X + 1\}.$$

Luego el sistema tiene el mismo conjunto de soluciones que el siguiente:

$f_1(X) = X^2 + X + 1 = 0$
$t(Y) = Y = 0.$

El sistema equivalente en $L_{3,2}$ es

$$f_1(X) = (C_1(X) \wedge C_0(T(X)) \wedge \mathbf{e_1}) \vee (C_1(X) \wedge C_2(T(X)) \wedge \mathbf{e_1}) \vee (C_0(X) \wedge \mathbf{e_1}) \vee$$
$$\vee (C_2(X) \wedge \mathbf{e_1}) \vee (C_2(X) \wedge C_0(T(X))) \vee (C_2(X) \wedge C_1(T(X))) \vee (C_0(X) \wedge C_2(T(X))) \vee$$
$$\vee (C_0(X) \wedge C_1(T(X))) = 0$$
$$t(Y) = (C_1(X) \wedge \mathbf{e_1}) \vee C_2(Y) = 0,$$

un sistema muy simple con una solución doble $X = (2, 2),\ Y = (0, 0)$.

A los efectos de encontrar las soluciones de un sistema dado o bien probar la incompatibilidad del mismo, utilizamos en los ejemplos anteriores la interpretación dada en el capítulo 3, algoritmos programados en Maple y una poderosa herramienta del álgebra conmutativa, como son las bases de Gröbner. Ante las dificultades que se presentan al hacerse necesaria una doble programación de algoritmos, surge de modo natural la siguiente pregunta:

¿Podemos resolver un sistema de ecuaciones sobre una extensión $L_{p,t}$ de $L_{p,k}$ hallando una base de Gröbner en $L_{p,t}[X_1, \ldots, X_n]$, definiendo este nuevo concepto sobre un álgebra de Post k-cíclica de orden p?.

Este es el desafío que afrontamos en el próximo capítulo, en donde analizaremos las nuevas dificultades que se presentan al abordar este camino.

Capítulo 6

Bases de Gröbner en $L_{p,k}[X_1, \ldots, X_n]$

En el capítulo 4 vimos cómo obtener una base de Gröbner en el anillo de polinomios $F(p^k)[X_1, \ldots, X_n]$. En este capítulo imitamos ese proceso para construir una base en $L_{p,k}[X_1, \ldots, X_n]$, mostrando algunos ejemplos para $p = 2$ y $p = 3$.

En la primera sección damos la definición de base de Gröbner de un ideal I de $L_{p,k}[X_1, \ldots, X_n]$ siguiendo el camino descripto en el capítulo 4 y teniendo en cuenta la interpretación dada en el capítulo 3. Indicamos cómo se calcula un producto, damos la definición de algunos órdenes monomiales y de ideal monomial, y mostramos en un ejemplo cómo calcular efectivamente una base de Gröbner de un ideal en $L_{3,1}[X, Y]$.

En la segunda sección estudiamos algunos ejemplos concretos de bases de Gröbner en $L_{2,k}[X_1, \ldots, X_n]$. Damos el algoritmo de división cuando $k = 1$ y un teorema para calcular los S-polinomios en $L_2[X, Y]$. También calculamos una base de Gröbner minimal de un ideal de $L_{2,2}[X, Y]$.

En la tercera y última sección terminamos de responder las preguntas formuladas en el capítulo 5 y detallamos distintas dificultades que se presentan al resolver un sistema de ecuaciones polinomiales en $L_{p,k}[X_1, \ldots, X_n]$. Las conclusiones obtenidas en esta tesis son consecuencia de las ideas originales desarrolladas en los capítulos 3, 5 y 6, y de los algoritmos programados en Maple incluidos en el apéndice.

6.1. Bases de Gröbner en $L_{p,k}[X_1, \ldots, X_n]$.

El teorema 3.2.2 del capítulo 3 demuestra la equivalencia entre las álgebras de Post k-cíclicas y los cuerpos con p^k elementos, siendo p un entero primo positivo. En esta sección utilizamos esta interpretación para definir una base de Gröbner de un ideal I en $L_{p,k}[X_1, \ldots, X_n]$ siguiendo el proceso descripto en el capítulo 4.

Notaremos si $k = 1$ al álgebra de Post k-cíclica $L_{p,k}$ por L_p.

Comenzamos definiendo las nociones de ideal generado y de variedad algebraica afín de manera análoga a la dada en el capítulo 4.

Definición 6.1.1 *Dados $f_1, \ldots, f_s$ polinomios en $L_{p,k}[X_1, \ldots, X_n]$, llamamos* **ideal** *de $L_{p,k}[X_1, \ldots, X_n]$ generado por $f_1, \ldots, f_s$ al conjunto*

$$(f_1, \ldots, f_s) = \{\sum_{i=1}^{s} h_i \cdot f_i : h_1, \ldots, h_s \in L_{p,k}[X_1, \ldots, X_n]\},$$

donde las operaciones $+$ y $\cdot$ del cuerpo $F(p^k)$ son términos en el lenguaje del álgebra de Post k-cíclica $L_{p,k}$ dados por la interpretación Φ_2.

Los ideales de $L_{p,k}[X_1, \ldots, X_n]$ **están finitamente generados** ya que $L_{p,k}$ es un álgebra finita. Decimos que $f_1, \ldots, f_s$ es una **base** de I.

Definición 6.1.2 *Sea $L_{p,k}$ el álgebra de Post k-cíclica con p^k elementos y sean $f_1, \ldots, f_s$ polinomios en $L_{p,k}[X_1, \ldots, X_n]$. El conjunto*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in L_{p,k}^n : f_i(a_1, \ldots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}$$

se llama **variedad algebraica afín** *definida por $f_1, \ldots, f_s$.*

Lema 6.1.1 *Si $V, W \subset L_{p,k}^n$ son variedades afines, entonces también lo son $V \cup W$ y $V \cap W$.*

Demostración: La demostracción de este lema resulta del teorema 3.2.2 y del lema 4.1.1 de los capítulos 3 y 4 respectivamente. □

Nuestro objetivo es buscar una base de Gröbner para un ideal I de $L_{p,k}[X_1, \ldots, X_n]$. El primer paso consiste en identificar los monomios. Un orden en los monomios de $L_{p,k}[X_1, \ldots, X_n]$ debe ser *total*. Recordemos que es necesario que el orden monomial posea la siguiente propiedad

$$Si\ X^\alpha > X^\beta\ y\ \gamma \in \mathbb{N}_0^n\ entonces\ X^\alpha \cdot X^\gamma > X^\beta \cdot X^\gamma,$$

donde la operación "$\cdot$" es función de las operaciones del álgebra de Post k-cíclica $L_{p,k}$.

En particular un **orden monomial** sobre $L_{p,k}[X_1, \ldots, X_n]$ es una relación $>$ sobre $\mathbb{N}_0^n$, que satisface:
i) $>$ es un orden total sobre $\mathbb{N}_0^n$.
ii) Si $\alpha > \beta$ y $\gamma \in \mathbb{N}_0^n$, entonces $\alpha + \gamma > \beta + \gamma$.
iii) $>$ es un buen orden sobre $\mathbb{N}_0^n$.

En el caso particular en que $p = 2$ y $k = 1$, el producto en $L_2[X_1, \ldots, X_n]$ es el ínfimo. Luego los monomios son de la forma

$$X^\alpha = X_1^{\alpha_1} \wedge \ldots \wedge X_n^{\alpha_n}.$$

En este caso identificamos estos monomios con las n-uplas $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.

Moisil introdujo en [31] la siguiente fórmula del producto para $p = 2$ y $k = 2$:

$$X \cdot Y = (X \wedge Y \wedge T(X) \wedge T(Y)) \vee (-X \wedge -Y \wedge T(X) \wedge T(Y)) \vee (X \wedge -T(X) \wedge T(Y)) \vee \\ \vee (Y \wedge T(X) \wedge -T(Y)),$$

Si $p = 3$ y $k = 1$ puede verse en el algoritmo **terxyL3(x,1,y,1)** dado en el apéndice que

$$X \cdot Y = \{[(C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y))] \wedge e_2\} \vee [(C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y))],$$

y si $p = 3$ y $k = 2$ entonces **terxyL32(x,y)** nos da

$$X \cdot Y = \{[(C_2(X) \wedge C_2(T(X)) \wedge C_2(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_1(Y)) \vee$$

$$\vee (C_2(X) \wedge C_1(T(X)) \wedge C_2(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_1(T(Y)) \vee$$

$$\vee (C_0(X) \wedge C_2(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee (C_0(X) \wedge C_1(T(X)) \wedge C_0(Y)) \wedge C_1(T(Y))) \vee$$

$$\vee (C_1(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee$$

$$\vee (C_0(X) \wedge C_1(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee (C_1(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee$$

$$\vee (C_2(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee$$

$$\vee (C_1(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_1(T(Y)) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_2(T(Y))) \vee$$

$$\vee (C_0(X) \wedge C_1(T(X)) \wedge C_1(Y) \wedge C_2(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_2(Y) \wedge C_1(T(Y)))] \wedge \mathbf{e_1}\} \vee$$

$$[(C_2(X) \wedge C_1(T(X)) \wedge C_1(T(Y))) \vee (C_1(X) \wedge C_2(T(X)) \wedge C_2(T(Y))) \vee$$

$$(C_2(X) \wedge C_2(T(X)) \wedge C_1(Y)) \vee (C_1(X) \wedge C_1(T(X)) \wedge C_2(Y)) \vee$$

$$(C_0(X) \wedge C_2(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee (C_0(X) \wedge C_1(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee$$

$$(C_0(X) \wedge C_1(T(X)) \wedge C_2(Y) \wedge C_1(T(Y))) \vee (C_0(X) \wedge C_2(T(X)) \wedge C_1(Y) \wedge C_2(T(Y))) \vee$$

$$(C_1(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_1(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_0(Y) \wedge C_2(T(Y))) \vee$$

$$(C_1(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_2(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_1(T(Y))) \vee$$

$$(C_1(X) \wedge C_0(T(X)) \wedge C_1(Y) \wedge C_0(T(Y))) \vee (C_2(X) \wedge C_0(T(X)) \wedge C_2(Y) \wedge C_0(T(Y))) \vee$$

$$(C_0(X) \wedge C_1(T(X)) \wedge C_1(Y)) \wedge C_0(T(Y))) \vee (C_0(X) \wedge C_2(T(X) \wedge C_2(Y) \wedge C_0(T(Y)))].$$

Para identificar los monomios X^α debemos obtener previamente la fórmula del producto utilizando el teorema 3.2.2 y realizar el programa correspondiente. En el apéndice se presentan los programas que permiten calcular algunos productos en

$L_{p,k}[X,Y]$ en los casos $p=2$, $p=3$ y $k=1$, $k=2$. Queda claro a partir de estas ecuaciones que la fórmula del producto es más complicada a medida que crecen los valores de p y k, lo que dificultará aún más el proceso de búsqueda de la base de Gröbner.

Algunos órdenes monomiales que ya hemos definido en el capítulo 4 son los siguientes:

Orden lexicográfico.

Dado $\alpha=(\alpha_1,\ldots,\alpha_n)$ y $\beta=(\beta_1,\ldots,\beta_n)$ en $\mathbb{N}_0^n$, decimos que $\alpha >_{lex} \beta$ si y sólo si existe $i\in\{1,\ldots,n\}$ que verifica:
$\alpha_1=\beta_1,\ldots,\alpha_{i-1}=\beta_{i-1}$ y $\alpha_i>\beta_i$.
Notaremos $X^\alpha >_{lex} X^\beta$ si $\alpha >_{lex} \beta$.

Las variables $X_1,\ldots,X_n$ se ordenan de manera usual usando el orden $>_{lex}$.

$$(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} \ldots >_{lex} (0,\ldots,0,1),$$

luego $X_1 >_{lex} X_2 >_{lex} \ldots >_{lex} X_n$.

Es importante observar que existen otros órdenes *lex*, según como se ordenen las variables.

El conjunto de monomios en $L_2[X,Y]$ es
$\{0,1,C_1(X),C_1(Y),C_1(X)\wedge C_1(Y)\}=\{0,1,X,Y,X\cdot Y\}$
mientras que las expresiones
$C_0(X)=X+1$,
$C_1(X)\vee C_1(Y)=X\cdot Y+X+Y$,
$C_0(X)\wedge C_1(Y)=X\cdot Y+X$,
son ejemplos de términos.

En $L_{2,2}[X,Y]$ son ejemplos de monomios
$C_1(X)=X$,
$C_1(Y)=Y$,
$C_1(T(X))=X^2$,
$C_1(T(Y))=Y^2$,
$(C_1(X)\wedge C_1(Y)\wedge C_1(T(X))\wedge C_1(T(Y)))\vee(C_0(X)\wedge C_0(Y)\wedge C_1(T(X))\wedge C_1(T(Y)))\vee$
$(C_1(X)\wedge C_0(T(X))\wedge C_1(T(Y)))\vee(C_1(Y)\wedge C_1(T(X))\wedge C_0(T(Y)))=X\cdot Y$,
y las expresiones
$C_0(X)\wedge C_1(Y))\vee(C_1(X)\wedge C_0(Y)=X+Y$,
$C_0(X)=X+1$,
$C_1(X)\vee C_1(Y)=X^2Y^2+X^2Y+XY^2+X+Y$,
son términos.

Son monomios en $L_3[X,Y]$,
$C_1(X)=X$,
$C_1(Y)=Y$,

$C_1(T(X)) = X^2$,
$\{[(C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y))] \wedge e_1\} \vee [(C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y))] =$
$= X \cdot Y$,
mientras que la expresión
$\{[(C_0(X) \wedge C_1(Y)) \vee (C_1(X) \wedge C_0(Y)) \vee (C_2(X) \wedge C_2(Y))] \wedge e_1\} \vee$
$\vee [(C_0(X) \wedge C_2(Y)) \vee (C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_0(Y))] = X + Y$
es un término.

Vimos en el capítulo 4 la existencia de otros órdenes más eficientes computacionalmente que el orden *lex*, los llamados órdenes de grado, entre los que mencionamos:

Orden Lexicográfico Graduado:

Dados α y $\beta \in \mathbb{N}_0^n$, decimos que $\alpha >_{glex} \beta$ si

$$\mid \alpha \mid = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = \mid \beta \mid, \ o \ \mid \alpha \mid = \mid \beta \mid \ y \ \alpha >_{lex} \beta.$$

Las variables se ordenan de acuerdo al orden lex, i.e.

$$X_1 >_{glex} X_2 >_{glex} \ldots >_{glex} X_n.$$

Orden Lexicográfico Graduado Inverso:

Dados $\alpha, \beta \in \mathbb{N}_0^n$, decimos que $\alpha >_{rlex} \beta$ si

$$\mid \alpha \mid = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = \mid \beta \mid,$$

$$o \ \mid \alpha \mid = \mid \beta \mid \ y \ existe \ i \in \{1, \ldots, n\} : \alpha_{i+1} = \beta_{i+1}, \ldots \alpha_n = \beta_n \ y \ \alpha_i < \beta_i.$$

Las definiciones de multigrado, coeficiente principal, monomio principal y el término principal correspondientes son las siguientes:

Definición 6.1.3 *Dado un polinomio no nulo en $L_{p,k}[X_1, \ldots, X_n]$ escrito en la notación de Epstein,*
$f(X_1, \ldots, X_n) = \bigvee_{0 \leq i_j \leq p-1, 0 \leq t_s \leq k-1} f(e_{i_1}, \ldots, e_{i_n}) \wedge C_{i_1}(T^{t_1}(X_1)) \wedge \ldots \wedge C_{i_n}(T^{t_n}(X_n))$
y $>$ un orden monomial, por el teorema 3.2.2 el polinomio $f \in F(p^k)[X_1, \ldots, X_n]$ queda expresado en la forma $f = \sum_\alpha a_\alpha X^\alpha$. Llamamos
i) el **multigrado** *de f (relativo a $>$) a*

$$multideg(f) = max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\},$$

ii) el **coeficiente principal** *de f a*

$$LC(f) = a_{multideg(f)} \in F(p^k),$$

iii) el **monomio principal** *de f a*

$$LM(f) = X^{multideg(f)}, \quad y$$

iv) la **término principal** *de f a*

$$LT(f) = a_{multideg(f)X^{multideg(f)}},$$

donde las fórmulas ii), iii) y iv) tienen su expresión correspondiente en $L_{p,k}[X_1, \ldots, X_n]$.

Es claro que si $p = 2$ y $k = 1$ los tres órdenes definidos anteriormente coinciden.

Veamos los siguientes ejemplos de la definición 6.1.3:

Dado el polinomio en $L_2[X, Y]$, $\quad f(X, Y) = C_1(X) \vee C_1(Y) = X \cdot Y + X + Y$ con $X > Y$, resulta:

$multideg(f) = (1, 1)$,
$LC(f) = 1$,
$LM(f) = C_1(X) \wedge C_1(Y)$ y
$LT(f) = C_1(X) \wedge C_1(Y)$.

En $L_{2,2}[X, Y]$ el polinomio $f(X, Y) = (C_1(T(X)) \wedge C_1(Y)) \vee (\alpha \wedge C_0(X)) =$
$= X^3Y^2 + \alpha X^3Y + X^3Y + \alpha X^2Y^2 + \alpha X^2Y + X^2 + \alpha XY^2 + XY^2 + \alpha X + X + \alpha$.
Considerando $X > Y$ se tiene:

$multideg(f) = (3, 2)$,
$LC(f) = 1$,
$LM(f) = (C_1(X) \wedge C_1(Y) \wedge C_1(T(Y))) \vee (C_1(T(X)) \wedge C_1(Y) \wedge C_1(T(Y))) \vee$
$\vee (C_1(T(X)) \wedge C_1(T(Y)) \wedge C_0(Y)) \vee (C_1(X) \wedge C_0(Y) \wedge C_1(T(Y)))$ y
$LT(f) = LM(f)$.

El polinomio $f(X, Y) = (C_0(X) \wedge C_1(Y)) \vee C_2(Y) = X^2Y^2 + 2X^2Y + Y^2$ en $L_3[X, Y]$ con $X > Y$ tiene:

$multideg(f) = (2, 2)$,
$LC(f) = 1$,
$LM(f) = (C_1(X) \wedge C_1(Y)) \vee (C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y))$,
$LT(f) = LM(f)$.

A continuación veremos el problema de la descripción de un ideal en el caso particular de ideales monomiales.

La definición de ideal monomial en $L_{p,k}[X_1, \ldots, X_n]$ es la siguiente:

Definición 6.1.4 *Sea $I \subset L_{p,k}[X_1, \ldots, X_n]$. Decimos que I es un* **ideal monomial** *si existe un subconjunto $A \subset \mathbb{N}_0^n$ tal que I consiste en todos los polinomios de la forma $\sum_{\alpha \in A} h_\alpha \cdot X^\alpha$ donde $h_\alpha \in L_{p,k}[X_1, \ldots, X_n]$ y las operaciones " + " y "·" son términos en lenguaje del álgebra de Post k-cíclica $L_{p,k}$ vía la interpretación Φ_2. Notamos $I = (\{X^\alpha : \alpha \in A\})$.*

Ejemplos 6.1.1 *El ideal* $I = (C_1(X)) = \{0, C_1(X), C_1(X) \wedge C_1(Y), C_1(X) \wedge C_0(Y)\}$ *es un ideal monomial de* $L_2[X, Y]$.

Sea $I = (C_1(X))$ *un ideal monomial en* $L_{2,2}[X, Y]$. *Los polinomios*
$f = 0, \quad g(X) = C_1(X) = X, \quad h(X) = C_1(T(X)) = X^2$ *y*
$p(X, Y) = (C_1(X) \wedge C_1(Y) \wedge C_1(T(X)) \wedge C_1(T(Y))) \vee (C_0(X) \wedge C_0(Y) \wedge C_1(T(X)) \wedge C_1(T(Y))) \vee (C_1(X) \wedge C_0(T(X)) \wedge C_1(T(Y))) \vee (C_1(Y) \wedge C_1(T(X)) \wedge C_0(T(Y))) = X \cdot Y$, *son algunos de los polinomios que están en* I.

En $L_3[X, Y]$ *el ideal* $I = (X)$ *tiene entre sus polinomios además de* X *a*
$f(X, Y) = [(C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y))] \wedge e_1\} \vee (C_1(X) \wedge C_1(Y)) \vee \vee (C_2(X) \wedge C_2(Y)) = X \cdot Y$,
$g(X, Y) = C_1(X) \vee C_2(X) = X^2$,
$h(X, Y) = (C_1(X) \wedge C_1(Y)) \vee (C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y)) = X^2 Y^2$.

El lema equivalente al lema 4.2.2 en $L_{p,k}[X_1, \ldots, X_n]$ es el siguiente:

Lema 6.1.2 *Sea* $I = (\{X^\alpha : \alpha \in A\}), A \subset \mathbb{N}_0^n$ *un ideal monomial. Entonces un monomio* $X^\beta \in I$ *si y sólo si* X^β *es divisible por* X^α *para algún* $\alpha \in A$, *i.e. si* $X^\beta = X^\alpha \cdot X^\gamma$ *para algún* $\gamma \in \mathbb{N}_0^n$, *siendo la operación "*$\cdot$*" función de las operaciones del álgebra de Post k-cíclica* $L_{p,k}$, *luego de aplicar la interpretación* Φ_2.

Vimos en el capítulo 4 que el lema de Dickson resuelve el problema de la descripción de un ideal cuando éste es monomial. En nuestro caso el lema cuya demostración es consecuencia del teorema 3.2.2 y del lema 4.2.1 de los capítulos 3 y 4 repectivamente, es el siguiente:

Lema 6.1.3 (Lema de Dickson) *Sea* $I = (\{X^\alpha : \alpha \in A\})$ *un ideal monomial de* $L_{p,k}[X_1, \ldots, X_n]$. *Entonces* I *puede escribirse en la forma* $I = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$, *donde* $\alpha(1), \ldots, \alpha(s) \in A$.

Utilizando nuevamente el teorema 3.2.2 del capítulo 3 y el teorema 4.2.2 del capítulo 4 obtenemos un algoritmo de división en $L_{p,k}[X_1, \ldots, X_n]$. En la próxima sección mostraremos la interpretación de este algoritmo en $L_2[X_1, \ldots, X_n]$.

Teorema 6.1.1 (Algoritmo de División en $L_{p,k}[X_1, \ldots, X_n]$**)** *Sea* $>$ *un orden monomial sobre el anillo* $L_{p,k}[X_1, \ldots, X_n]$ *y* $F = \{f_1, \ldots, f_s\}$ *una s-upla ordenada de polinomios en* $L_{p,k}[X_1, \ldots, X_n]$. *Entonces para cada* $f \in L_{p,k}[X_1, \ldots, X_n]$, *existen únicos* $q_1, \ldots, q_s$ *y* $r \in L_{p,k}[X_1, \ldots, X_n]$ *tales que:*
i) $f = q_1 f_1 + \ldots + q_s f_s + r$,
ii) Si $q_i = \sum c_\alpha X^\alpha$ *y* $c_\alpha \neq 0$ *entonces* $\alpha + multideg(f_i) \in \Delta_i$,
iii) Si $r = \sum c_\alpha X^\alpha$ *y* $c_\alpha \neq 0$ *entonces* $\alpha \in \bar{\Delta}$.
Además si $q_i \neq 0$, $multideg(q_i) + multideg(f_i) \leq multideg(f)$ *y si* $r \neq 0$, $multideg(r) \leq multideg(f)$.
Las operaciones suma y producto son términos en el lenguaje del álgebra $L_{p,k}$.

Ejemplo 6.1.1 *Veamos el siguiente ejemplo de división en L_3 del polinomio*

$f(X,Y) = (C_0(X) \wedge C_1(Y)) \vee C_2(Y) = X^2Y^2 + 2X^2Y + Y^2$ *por los polinomios* $f_1(X,Y) = (C_2(X) \wedge C_0(Y)) \vee (C_1(X) \wedge C_1(Y)) = 2X^2Y^2 + 2X^2Y + XY + 2X^2 + 2X$ *y* $f_2(X,Y) = (C_0(X) \vee C_1(Y)) \wedge e_1 = XY + 2$.

Utilizando el algoritmo de división y el orden lexicográfico con $X > Y$ obtenemos que

$f = q_1 f_1 + q_2 f_2 + r$ *donde*
$q_1 = e_1 = 2, \quad q_2(X) = (C_2(X) \wedge e_1) \vee C_0(X) = X + 1$ *y*
$r(X,Y) = (C_0(X) \wedge C_1(Y) \wedge e_1) \vee (C_0(X) \wedge C_2(Y) \wedge e_1) \vee (C_0(X) \wedge C_0(Y)) \vee$
$\vee (C_1(X) \wedge C_1(Y)) \vee (C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_1(Y)) \vee (C_0(X) \wedge C_0(Y)) \vee$
$\vee (C_2(X) \wedge C_2(Y)) = 2X^2 + Y^2 + 1 \quad y$
las operaciones suma y producto de $F(3)$ son términos en el lenguaje de L_3.

El próximo paso es definir el *ideal principal de I.*

Definición 6.1.5 *Sea $I \in L_{p,k}[X_1, \ldots, X_n]$ un ideal no nulo y $>$ un orden monomial fijo. Llamamos* **ideal principal de I** *al ideal generado por los términos principales de los polinomios $f \in I - \{0\}$, i.e.*

$$LT(I) = (\{LT(f)/f \in I - \{0\}\}).$$

Sabemos que si $I = (f_1, \ldots, f_s)$ entonces el ideal $(LT(f_1), \ldots, LT(f_s)) \subset LT(I)$ pero la igualdad no vale en general como puede verse en el ejemplo siguiente.

Ejemplo 6.1.2 *Sea $I = (f_1, f_2)$ donde $f_1 = X \vee Y$ y $f_2 = (-X \wedge Y) \vee (X \wedge -Y)$, y lex el orden monomial en $L_2[X,Y]$ con $X > Y$.*
El monomio $Y \in I$ pues, $Y = (X \vee Y) \wedge Y$ con $X \vee Y \in I$ e $Y \in L_2[X,Y]$.
Sin embargo $Y \notin (LT(f_1), LT(f_2)) = (X \wedge Y, X)$ pues no es divisible por $LT(f_1) = X \wedge Y$ o $LT(f_2) = X$.

De manera análoga a la vista en el capítulo 4 puede observarse que $LT(I)$ es un ideal monomial.

Proposición 6.1.1 *Sea $I \subset L_{p,k}[X_1, \ldots, X_n]$ un ideal. Entonces*
i) $LT(I)$ es un ideal monomial.
ii) Existen $g_1, \ldots, g_t \in I$ tales que $LT(I) = (LT(g_1), \ldots, LT(g_t))$.

En nuestro caso como las álgebras de Post k-cíclicas son finitas tendremos siempre bases finitas en los ideales de $L_{p,k}[X_1, \ldots, X_n]$ y en consecuencia el teorema de la base de Hilbert se verifica trivialmente.

Teorema 6.1.2 (Teorema de la base de Hilbert) *Todo ideal I de $L_{p,k}[X_1, \ldots, X_n]$ tiene un conjunto de generadores $\{g_1, \ldots, g_t\}$ con $g_1, \ldots, g_t \in I$.*

Nuevamente, la base que nos interesa buscar es la **base de Gröbner**.

Definición 6.1.6 *Fijado un orden monomial, un subconjunto finito* $G = \{g_1, \ldots, g_t\}$ *de un ideal* I *se dice una* **base de Gröbner** *si*

$$LT(I) = (LT(g_1), \ldots, LT(g_t)).$$

El próximo corolario asegura su existencia y se sigue de los teoremas 3.2.2 y 6.1.2.

Corolario 6.1.1 *Sea* $>$ *un orden monomial. Entonces todo ideal* $I \subset L_{p,k}[X_1, \ldots, X_n]$ *distinto del* $\{0\}$ *tiene una base de Gröbner.*

La variedad afín definida por un *ideal* $I \subset L_{p,k}[X_1, \ldots, X_n]$ la da la proposición siguiente:

Proposición 6.1.2 *Si* $I = (f_1, \ldots, f_s)$, *entonces* $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

En lo que sigue estudiaremos las bases de Gröbner en $L_{p,k}[X_1, \ldots, X_n]$. Daremos un método para determinar cuando una base de un ideal I de $L_{p,k}[X_1, \ldots, X_n]$ es una base de Gröbner siguiendo el proceso descripto en el capítulo 4.

Vimos en la proposición 4.2.7 que al "dividir" un polinomio por una base de Gröbner el resto queda unívocamente determinado.

Proposición 6.1.3 *Sea* $G = \{g_1, \ldots, g_t\}$ *una base de Gröbner de un ideal* I *de* $L_{p,k}[X_1, \ldots, X_n]$ *y sea* $f \in L_{p,k}[X_1, \ldots, X_n]$. *Entonces existe un único polinomio* $r \in L_{p,k}[X_1, \ldots, X_n]$ *tal que* r *verifica:*
i) Si $r = \sum c_\alpha X^\alpha$ *y* $c_\alpha \neq 0$ *entonces* $\alpha \in \bar{\Delta}$, *donde las operaciones del cuerpo* $F(p^k)$ *son términos en el lenguaje del álgebra de Post k-cíclica* $L_{p,k}$.
ii) Existe $g \in I$ *tal que* $f = g + r$, *siendo "+" función de las operaciones del álgebra de Post k-cíclica* $L_{p,k}$, *aplicando la interpretación* Φ_2.

Dada una base de Gröbner G de un ideal I, y un polinomio postiano f, notamos **fRG** al resto de la división de f por la base $G = \{g_1, \ldots, g_t\}$. Por la proposición 4.2.7 del capítulo 4, **fRG** no depende del orden de los polinomos $g_1, \ldots, g_t$ sino del orden monomial elegido.

El corolario 4.2.3 en nuestro caso es el siguiente:

Corolario 6.1.2 *Si* $G = \{g_1, \ldots, g_t\}$ *es una base de Gröbner para un ideal* I *de* $L_{p,k}[X_1, \ldots, X_n]$ *y* $f \in L_{p,k}[X_1, \ldots, X_n]$, *entonces* $f \in I$ *si y sólo si el resto de dividir* f *por* G *es cero.*

El corolario 6.1.2 da un algoritmo para resolver el problema de pertenencia a un ideal cuando se tiene una base de Gröbner G del ideal I. Calculando el resto de la división de un polinomio f por G podemos determinar directamente si $f \in I$.

Utilizando los S-polinomios nuevamente obtenemos un criterio para determinar cuando una base de un ideal es una base de Gröbner.

Definición 6.1.7 *Dados $f, g \in L_{p,k}[X_1, \ldots, X_n]$ polinomios no nulos, el* **S-polinomio** *de f y g es la combinación*

$$fSg = \frac{X^\gamma}{LT(f)} \cdot f - \frac{X^\gamma}{LT(g)} \cdot g.$$

donde $X^\gamma = MCM(LM(f), LM(g))$ y las operaciones de $F(p^k)$ son términos en el lenguaje del álgebra $L_{p,k}$ vía la interpretación Φ_2.

Recordemos que los S-polinomios nos permiten determinar cuando una base de un ideal es una base de Gröbner.

Teorema 6.1.3 *Sea $I \subset L_{p,k}[X_1, \ldots, X_n]$ un ideal no nulo y $>$ un orden monomial sobre $\mathbb{N}_0^n$. Entonces $G = \{f_1, \ldots, f_s\}$ es una base de Gröbner de I para el orden $>$ si y sólo si para todo $i, j \in \{1, \ldots, s\}$ resulta que $(f_i S f_j) R\{f_1, \ldots, f_s\} = 0$.*

En el corolario 6.1.1 vimos que todo ideal I no nulo de $L_{p,k}[X_1, \ldots, X_n]$ admite una base de Gröbner. Sin embargo éste no nos dice cómo calcular la base de manera algorítmica.

Para obtener una base de Gröbner, debemos ir extendiendo el conjunto de generadores $F = \{f_1, \ldots, f_s\}$ de I. Al calcular el S-polinomio $f_i S f_j$, el resto de dividirlo por F puede ser no nulo, por lo que debemos agregar a F el resto de la división como un nuevo generador f_{s+1} y verificar si el nuevo conjunto $F' = F \cup \{f_{s+1}\}$ verifica el teorema 6.1.3.

Este procedimiento, que ya describimos en el capítulo 4, nos da un algoritmo para encontrar una base de Gröbner de un ideal I en $L_{p,k}[X_1, \ldots X_n]$.

Algoritmo de Buchberger en $L_{p,k}[X_1, \ldots, X_n]$

Presentamos a continuación una versión simple del algoritmo de Buchberger para $L_{p,k}[X_1, \ldots, X_n]$.

Dado $I = (f_1, \ldots, f_s) \neq \{0\} \in L_{p,k}[X_1, \ldots, X_n]$ podemos encontrar una base de Gröbner para I en un número finito de pasos utilizando el siguiente algoritmo:

Input: $F = (f_1, \ldots, f_s)$
Output: Una base de Gröbner $G = \{g_1, \ldots, g_t\}$ para I, con $F \subset G$
$G := F$
REPEAT

$G' := G$
FOR cada par $\{f_i, f_j\}, f_i \neq f_j$ en G' **DO**
$S := (f_i S f_j) R G'$
IF $S \neq 0$ **THEN** $G := G \cup \{S\}$
UNTIL $G = G'$

Ilustremos este proceso con un ejemplo:

Ejemplo 6.1.3 *Consideremos en* $L_3[X,Y]$ *el ideal* $I = (f_1, f_2)$ *donde*

$f_1(X,Y) = \{[(C_1(X) \wedge C_0(Y)) \vee (C_2(X) \wedge C_0(Y))] \wedge e_1\} \vee [C_0(X) \vee (C_1(X) \wedge C_1(Y)) \vee \vee (C_2(X) \wedge C_1(Y))]$ *y*

$f_2(X,Y) = \{[C_0(X) \vee (C_1(X) \wedge C_0(Y)) \vee (C_2(X) \wedge C_0(Y)) \vee (C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_1(Y))] \wedge e_1\} \vee (C_1(X) \wedge C_2(Y)) \vee (C_2(X) \wedge C_2(Y))$.

Los polinomios f_1 *y* f_2 *en* $F(3)[X,Y]$ *son los siguientes:*
$f_1(X,Y) = X^2Y + X^2 + 1$ *y*
$f_2(X,Y) = X^2Y^2 + X^2Y + 2$.

Al calcular $f_1 S f_2$ *obtenemos*

$f_3(X,Y) = f_1(X,Y) S f_2(X,Y) = Y + 1$, *siendo su expresión en* $L_3[X,Y]$,

$f_3(X,Y) = C_0(Y) \vee (C_2(Y) \wedge e_1)$.

Luego obtenemos
$f_1 S f_2 R\{f_1, f_2\} = f_3$ *y*
$f_1 S f_3 R\{f_1, f_2\} = 1$.
Hacemos $f_4 = 1$ *y la base de Gröbner que obtenemos es* $G = \{f_1, f_2, f_3, f_4\}$. *Por lo visto en el capítulo 4 resulta* $I = L_3[X,Y]$.

Las bases de Gröbner calculadas en el algoritmo suelen ser más grandes de lo necesario. El objetivo es, igual que en el capítulo 4, eliminar los generadores que sobran utilizando el siguiente lema cuya demostración se basa en el lema 4.2.4 del capítulo 4 y el teorema 3.2.2 del capítulo 3.

Lema 6.1.4 *Sea* G *una base de Gröbner para el ideal* I *de* $L_{p,k}[X_1, \ldots, X_n]$. *Sea* $f \in G$ *un polinomio tal que* $LT(f) \in (LT(G - \{f\}))$. *Entonces* $G - \{f\}$ *es también una base de Gröbner para* I.

Este lema nos permite "mejorar" la base de Gröbner G de un ideal I, eliminando los polinomios f de G que satisfacen $LT(f) \in (LT(G - \{f\})$. Además pueden obtenerse polinomios con coeficiente principal 1.

Recordemos que una **base de Gröbner minimal** de un ideal polinomial I es una base de Gröbner G de I que satisface:
1) $LC(f) = 1$ para todo $f \in G$,
2) para todo $f \in G, LT(f) \notin (LT(G - \{f\}))$.

Para construir una base de Gröbner minimal de un ideal polinomial no nulo I aplicamos el algoritmo, y utilizando el lema 6.1.4, eliminamos los generadores innecesarios que podrían haberse incluído.

En el ejemplo 6.1.3, $G = \{1\}$ es una base de Gröbner minimal de I.

Es importante recordar que un ideal I puede tener más de una base de Gröbner minimal. Existe una **una** base de Gröbner minimal **mejor** que las demás y se llama **base de Gröbner reducida**.

Una **base de Gröbner reducida** de un ideal polinomial I es una base G de I tal que
1) $LC(f) = 1$ para todo $f \in G$,
2) para todo $f \in G$, ningún monomio de f pertenece a $LT(G - \{f\})$.

De la proposición 4.2.9 del capítulo 4 y el teorema 3.2.2 resulta la unicidad de la base de Gröbner reducida.

Proposición 6.1.4 *Sea $I \neq \{0\}$ un ideal de $L_{p,k}[X_1, \ldots, X_n]$. Entonces I tiene una única base de Gröbner reducida para un orden monomial dado.*

En la búsqueda de una base de Gröbner de un ideal I de $L_{p,k}[X_1, \ldots, X_n]$ es necesario obtener la expresión de algunos polinomios en $F(p^k)[X_1, \ldots, X_n]$, calcular S-polinomios y divisiones en este anillo y luego buscar la expresión en $L_{p,k}[X_1, \ldots, X_n]$ de los polinomios que irán formando la base. Es claro que este proceso puede resultar largo y complicado, no sólo por los cálculos involucrados, sino también por el tamaño de p, k y n. En la próxima sección daremos algunos algoritmos para $p = 2$ y $k \in \{1, 2\}$

6.2. Bases de Gröbner en $L_{2,k}[X_1, \ldots, X_n]$

En esta sección utilizamos la interpretación dada en el capítulo 3 en el caso en que $p = 2$. Damos un algoritmo de división en $L_2[X_1, \ldots, X_n]$ y un teorema para calcular los S-polinomios en $L_2[X, Y]$.

El teorema 3.2.2 es una generalización del teorema siguiente dado por H. Cendra en [10].

Teorema 6.2.1 *Sea C un conjunto con 2^k elementos, $k \in \mathbf{N}, k \geq 2$ y $\langle F(2^k), +, \cdot, 0, 1\rangle$ un cuerpo. Entonces podemos definir una estructura de álgebra de Boole simple k-periódica (B, T) sobre C de tal manera que:*

(a) El primer y último elemento de B son 0 y 1 respectivamente.

(b) $T(x) = x^2$, $x \in B$; T permuta cíclicamente los átomos de B.

(c) $x + y = (x' \wedge y) \vee (x \wedge y')$, x, $y \in B$, $x' = 1 + x$, $x \in B$.

(d) $\wedge$, $\vee$ son composiciones iteradas de $+$ y "$\cdot$".

(e) "$\cdot$" es un cierta composición iterada de $', \wedge, \vee, T$.

Notaremos $L_{2,k}$ al álgebra de Boole (B, T) del teorema 6.2.1.

Vimos en la sección anterior que el producto en $L_2[X_1, \ldots, X_n]$ es el ínfimo y que los monomios son de la forma

$$X^\alpha = X_1^{\alpha_1} \wedge \ldots \wedge X_n^{\alpha_n}.$$

Además los órdenes *lex*, *glex* y *rlex* coinciden para $k = 1$.

Veamos un ejemplo en $L_2[X, Y]$.

Ejemplo 6.2.1 *Consideremos el polinomio genérico* $f(X, Y) \in L_2[X, Y]$,

$$f(X,Y) = (a \wedge C_0(X) \wedge C_0(Y)) \vee (b \wedge C_0(X) \wedge C_1(Y)) \vee (c \wedge C_1(X) \wedge C_0(Y)) \vee (d \wedge C_1(X) \wedge C_1(Y)).$$

Teniendo en cuenta que $C_0(X) = X'$ *y* $C_1(X) = X$, *notando* $X' = -X$ *podemos escribir al polinomio* $f(X, Y)$ *como*

$$f(X,Y) = (a \wedge -X \wedge -Y) \vee (b \wedge -X \wedge Y) \vee (c \wedge X \wedge -Y) \vee (d \wedge X \wedge Y).$$

Utilizando la interpretación existente entre L_2 *y* $F(2)$, *el polinomio* $f(X, Y)$ *en* $F(2)[X, Y]$ *tiene la siguiente expresión:*

$$f(X,Y) = (a+b+c+d)XY + (a+c)X + (a+b)Y + a.$$

Llamando
$a_{11} = (a + b + c + d)$, $a_{10} = a + c$,
$a_{01} = a + b$, *y* $a_{00} = a$.
El polinomio f *queda expresado en la forma:*

$$f(X,Y) = a_{11}XY + a_{10}X + a_{01}Y + a_{00}.$$

Luego
$multideg(f) = max\{\alpha = (i, j)/a_{ij} \neq 0\}$.
$LC(f) = 1$ *y*
$LM(f) = LT(f) = (XY)^{multideg(f)}$.

Al buscar la forma general de un polinomio f dado en $L_{2,2}[X, Y]$ en el anillo $F(2^2)[X, Y]$, problemas de capacidad de memoria durante el procedimiento hacen imposible la finalización de los cálculos. Por esta razón daremos sólo algunos ejemplos particulares.

A continuación veremos cómo interpretar la división de un polinomio f por un conjunto de polinomios $\{f_1, f_2, \ldots, f_s\}$ en $L_2[X_1, X_2, \ldots, X_n]$. A los efectos de aclarar la interpretación de esta división, comenzamos dando un ejemplo en $L_2[X, Y]$.

Ejemplo 6.2.2 *Supongamos que queremos interpretar la división del polinomio*

$$f(X,Y) = X \vee Y$$

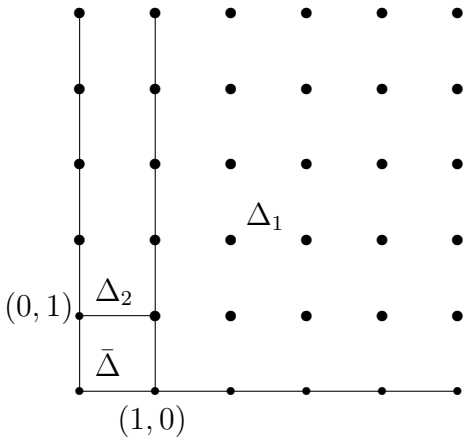
por el conjunto de polinomios $\{f_1, f_2\}$ *donde* $f_1(X,Y) = (-X \wedge Y) \vee (X \wedge -Y)$ *y* $f_2(Y) = -Y$.

Eligiendo un orden monomial con $X > Y$, *los polinomios en* $F_2[X,Y]$ *tienen las siguientes expresiones:*

$f(X,Y) = X \cdot Y + X + Y$ *y* $multideg(f) = (1,1)$,
$f_1(X,Y) = X + Y$ *y* $multideg(f_1) = (1,0)$
$f_2(Y) = Y + 1$ *y* $multideg(f_2) = (0,1)$

Para realizar la división en $F_2[X,Y]$ *hacemos una partición de* $\mathbb{N}_0^2$ *teniendo en cuenta lo explicado en el capítulo 4.*

$\Delta_1 = multideg(f_1) + \mathbb{N}_0^2 = (1,0) + \mathbb{N}_0^2$,
$\Delta_2 = multideg(f_2) + \mathbb{N}_0^2 - \Delta_1 = (0,1) + \mathbb{N}_0^2 - \Delta_1$ *y*
$\bar{\Delta} = \mathbb{N}_0^2 - (\Delta_1 \cup \Delta_2)$



Como $multideg(f) = (1,1) \in \Delta_1$ *entonces*
$f^{(1)} = f - Y \cdot f_1 = X \cdot Y + X + Y - Y \cdot (X + Y) = X$,
$multideg(f^{(1)}) = (1,0) \in \Delta_1$,
$f^{(2)} = f^{(1)} - f_1 = X - (X + Y) = Y$,
$multideg(f^{(2)}) = (0,1) \in \Delta_2$,
$f^{(3)} = f^{(2)} - f_2 = Y - (Y + 1) = 1$,
$multideg(f^{(3)}) = (0,0) \in \bar{\Delta}$.

Despejando obtenemos $f = (Y + 1) \cdot f_1 + f_2 + 1$.

En $L_2[X,Y]$ *obtenemos lo siguiente:*
$f = f^{(1)} + Y \cdot f_1 = (-f^{(1)} \wedge Y \wedge f_1) \vee [f^{(1)} \wedge -(Y \wedge f_1)]$,
$f^{(1)} = f^{(2)} + f_1 = (-f^{(2)} \wedge f_1) \vee (f^{(2)} \wedge -f_1)$,

$f^{(2)} = f^{(3)} - f_2 = (-1 \wedge f_2) \vee (1 \wedge -f_2) = -f_2,$

y obtenemos $f(X,Y) = [(-Y \wedge f_1) \wedge (1 \wedge f_2)] \vee [-(-Y \wedge f_1) \wedge -(f_2 \wedge 1)] =$
$= [(Y \vee -f_2) \wedge f_1] \vee (-f_1 \wedge f_2).$

El teorema que sigue nos muestra cómo interpretar el algoritmo de división en $L_2[X_1, \ldots, X_n]$.

Teorema 6.2.2 (Interpretación del Algoritmo de División en $L_2[X_1, \ldots, X_n]$) *Sea $>$ un orden monomial en $L_2[X_1, \ldots, X_n]$ y $F = \{f_1, \ldots, f_s\}$ una s-upla ordenada de polinomios en $L_2[X_1, \ldots, X_n]$. Entonces para cada $f \in L_2[X_1, \ldots, X_n]$, existen únicos $q_1, \ldots, q_s$ y $r \in L_2[X_1, \ldots, X_n]$ tales que:*
i) a) Si $s = 2k, k \in N$ (i.e. s es par) entonces $f(X_1, \ldots, X_n) = (-A \wedge r) \vee (A \wedge -r)$ donde

$A = [(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})] \vee$
$\vee [(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})] \vee$

$$\ldots \qquad P_{2k}^{2k-1(+),1(-)}$$

$\vee [-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})] \vee$

$$\ldots \qquad P_{2k}^{2k-3(+),3(-)}$$

$$\ldots$$

$$\ldots \qquad P_{2k}^{3(+),2k-3(-)}$$

$[(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})] \vee$
$\vee [-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})] \vee$

$$\ldots \qquad P_{2k}^{1(+),2k-1(-)}$$

$\vee [-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})].$

i) b) Si $s = 2k+1$ (i.e s es impar) entonces
$f(X_1, \ldots, X_n) = (-A \wedge r) \vee (A \wedge -r)$ *donde*
$A = [(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})] \vee$
$\vee [(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})] \vee$

$$\ldots \qquad P_{2k+1}^{2k-1(+),2(-)}$$

$\vee [-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})] \vee$

$$\ldots \qquad P_{2k+1}^{2k-3(+),4(-)}$$

$$\ldots$$

$$\ldots \qquad P_{2k+1}^{3(+),2k-4(-)}$$

$$\vee[(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})] \vee$$

$$\ldots \qquad P_{2k+1}^{1(+),2k(-)}$$

$$\vee[-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})].$$

ii) Si $q_i = \bigvee b_\beta \wedge X^\beta$ *y* $b_\beta \neq 0$ *entonces* $\beta + multideg(f_i) \in \Delta_i$, *donde* β *es el definido en la definición 6.1.3.*
iii) Si $r = \bigvee b_\beta \wedge X^\beta$ *y* $b_\beta \neq 0$ *entonces* $\beta \in \bar{\Delta}$.
Además si $q_i \neq 0$, $multideg(q_i) + multideg(f_i) \leq multideg(f)$ *y*
si $r \neq 0$, $multideg(r) \leq multideg(f)$.

Demostración: Sea $s = 2$ y $f = q_1 f_1 + q_2 f_2 + r$. Llamando
$A = q_1 f_1 + q_2 f_2 = [(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2)] \vee [-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2)]$ resulta
$f = (-A \wedge r) \vee (A \wedge -r)$.

Si $s = 3$, $f = (-A \wedge r) \vee (A \wedge -r)$ y
$A = [(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge (q_3 \wedge f_3)] \vee [-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge (q_3 \wedge f_3)] \vee$
$\vee[-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge -(q_3 \wedge f_3)] \vee [(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge -(q_3 \wedge f_3)]$.

Continuando con este razonamiento puede observarse que si s es par, es decir $s = 2k,\ k \in N$, tendremos en la descomposición de A el supremo de las siguientes expresiones:

- todas las permutaciones del supremo de $2k$ elementos donde $2k-1$ son de la forma $(q_i \wedge f_i)$ y un sólo elemento es el complemento booleano de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k}^{2k-1(+),1(-)}$:

  $[(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})]$,

  $[(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})]$,

  $\ldots$

  $[-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})]$,

- todas las permutaciones del supremo de $2k$ elementos donde $2k-3$ son de la forma $(q_i \wedge f_i)$ y tres de ellos son los complementos booleanos de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k}^{2k-3(+),3(-)}$,

- y continuamos aumentando de dos en dos los complementos booleanos, hasta obtener,

- todas las permutaciones del supremo de $2k$ elementos donde uno es de la forma $(q_i \wedge f_i)$ y $2k-1$ de ellos son complementos booleanos de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k}^{1(+),2k-1(-)}$:

  $[(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})]$,

$$[-(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})],$$
$$\ldots$$
$$[-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})].$$

Si s es impar, es decir $s = 2k+1,\ k \in N$, tendremos en la descomposición de A el supremo de las siguientes expresiones:

- la expresión
  $[(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})]$,
- todas las permutaciones del supremo de $2k+1$ elementos donde $2k-1$ son de la forma $(q_i \wedge f_i)$ y dos de ellos son los complementos booleanos de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k+1}^{2k-1(+),2(-)}$:
  $[(q_1 \wedge f_1) \wedge (q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})]$,
  $\ldots$
  $[-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (+) \ldots \wedge (q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})]$,
- todas las permutaciones del supremo de $2k+1$ elementos donde $2k-3$ son de la forma $(q_i \wedge f_i)$ y cuatro de ellos son los complementos booleanos de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k+1}^{2k-3(+),4(-)}$,
- y continuamos aumentando de dos en dos los complementos booleanos, hasta obtener,
- todas las permutaciones del supremo de $2k+1$ elementos donde uno de ellos es $(q_i \wedge f_i)$ y $2k$ de ellos son los complementos booleanos de $(q_i \wedge f_i)$, $-(q_i \wedge f_i)$. Simbolizamos a esta expresión por $P_{2k+1}^{1(+),2k(-)}$,
  $[(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge -(q_{2k} \wedge f_{2k})]$,
  $\ldots$
  $[-(q_1 \wedge f_1) \wedge -(q_2 \wedge f_2) \wedge \ldots (-) \ldots \wedge -(q_{2k-1} \wedge f_{2k-1}) \wedge (q_{2k} \wedge f_{2k})]$.

  Los incisos ii) y iii) se deducen de los teoremas 4.2.2 y 6.2.1.

□

En el ejemplo 6.2.2 obtuvimos $f(X,Y) = [(Y \vee -f_2) \wedge f_1] \vee (-f_1 \wedge f_2) =$
$= [(-Y \wedge f_1) \wedge (1 \wedge f_2)] \vee [-(-Y \wedge f_1) \wedge -(f_2 \wedge 1)]$ como indica el teorema.
Además $q_1 = -Y, q_2 = 1$ y $r = 1$ verifican las condiciones ii) y iii) ya que:
$multideg(q_1) + multideg(f_1) = multideg(-Y) + multideg[(-X \wedge Y) \vee (X \wedge -Y)] =$
$(0,1) + (1,0) = (1,1) \in \Delta_1$,
$multideg(q_2) + multideg(f_2) = multideg(1) + multideg(-Y) = (0,0) + (0,1) =$
$(0,1) \in \Delta_2$ y

$multideg(r) = multideg(1) = (0,0) \in \bar{\Delta}$.

La interpretación del algoritmo de división en $L_2[X_1, \ldots, X_n]$ nos muestra que la complejidad de las expresiones obtenidas aumentará para los valores de $k > 1$. Estas dificultades implicarán que, más allá de ser posible, será necesario analizar cómo hallar una base de Gröbner de un ideal en $L_{2,k}[X_1, \ldots, X_n]$, ya que en general resultará recomendable utilizar el camino descripto en el capítulo 5.

En lo que sigue damos un teorema para calcular los S**-polinomios** en $L_2[X, Y]$.

Supongamos que queremos calcular el S-polinomio entre los polinomios $f(X,Y)$ y $f'(X,Y)$ en $L_2[X,Y]$ donde

$f(X,Y) = (a \wedge -X \wedge -Y) \vee (b \wedge -X \wedge Y) \vee (c \wedge X \wedge -Y) \vee (d \wedge X \wedge Y)$, y
$f'(X,Y) = (a' \wedge -X \wedge -Y) \vee (b' \wedge -X \wedge Y) \vee (c' \wedge X \wedge -Y) \vee (d' \wedge X \wedge Y)$.

Sabiendo que el cálculo de $f(X,Y)Sf'(X,Y)$ viene dado por la fórmula

$$fSf' = \frac{X^\gamma}{LT(f)} \cdot f + \frac{X^\gamma}{LT(f')} \cdot f' \quad (S).$$

donde $X^\gamma = MCM(LM(f), LM(f'))$, obtenemos utilizando las operaciones del teorema 6.2.1 el siguiente teorema:

Teorema 6.2.3 *Dados dos polinomios f y f' en $L_2[X,Y]$ el S-polinomio $f(X,Y)Sf'(X,Y)$ tiene la siguiente expresión:*

Caso I
En los casos siguientes $LM(f) = LM(f')$.
a) Si $a_{11} = 1 = a'_{11}$ ó,
b) si $a_{11} = 0 = a'_{11}$ y $a_{10} = 1 = a'_{10}$ ó,
c) si $a_{11} = 0 = a'_{11}$, $a_{10} = 0 = a'_{10}$ y $a_{01} = 1 = a'_{01}$ ó,
d) si $f(X,Y) = 1 = f'(X,Y)$,
entonces

$$f(X,Y)Sf'(X,Y) = f(X,Y) + f'(X,Y) = (-f \wedge f') \vee (f \wedge -f').$$

Caso II
a) Si $a_{11} = 1$, $a'_{11} = 0$ y $a'_{10} = 1$, i.e. $LM(f) = X \cdot Y$ y $LM(f') = X$, o
b) $a_{11} = 0 = a_{10}$, $a_{01} = 1$ y $f'(X,Y) = 1$, i.e. $LM(f) = Y$, y $f'(X,Y) = 1$,

entonces

$$f(X,Y)Sf'(X,Y) = f(X,Y) + Y \cdot f'(X,Y) =$$

a) $= (-Y \wedge f) \vee (Y \wedge -f \wedge f') \vee (f \wedge -f')$,
b) $= (Y \wedge -f) \vee (-Y \wedge f)$.

Caso III

a) Si $a_{11} = 1$, $a'_{11} = 0 = a'_{10}$ *y* $a'_{01} = 1$, *i.e* $LM(f) = X \cdot Y$ *y* $LM(f') = Y$, *o*
b) $a_{11} = 0, a_{10} = 1$, *i.e* $LM(f) = X$, *y* $f'(X,Y) = 1$,
entonces

$$f(X,Y)Sf'(X,Y) = f(X,Y) + X \cdot f'(X,Y) =$$

a) $= (-X \wedge f) \vee (X \wedge -f \wedge f') \vee (f \wedge -f')$,
b) $= (X \wedge -f) \vee (-X \wedge f)$.

Caso IV
Si $a_{11} = 0$, $a_{10} = 1$, $a'_{11} = 0 = a'_{10}$ *y* $a'_{01} = 1$, *i.e* $LM(f) = X$ *y* $LM(f') = Y$,
entonces

$$f(X,Y)Sf'(X,Y) = Y \cdot f(X,Y) + X \cdot f'(X,Y) =$$
$$= (-X \wedge f \wedge Y) \vee (-f' \wedge Y \wedge f) \vee (X \wedge f' \wedge -Y) \vee (X \wedge f' \wedge -f).$$

Caso V
Si $a_{11} = 1$ *y* $f'(X,Y) = 1$ *i.e.* $LM(f) = X \cdot Y$ *entonces*

$$f(X,Y)Sf'(X,Y) = f(X,Y) + X \cdot Y \cdot f'(X,Y) = f + X \cdot Y =$$
$$= (-X \wedge f) \vee (-Y \wedge f) \vee (X \wedge Y \wedge -f).$$

Caso VI
Si $f'(X,Y) = 0$ *entonces*

$$f(X,Y)Sf'(X,Y) = f(X,Y).$$

Demostración: La demostración del corolario resulta del teorema 6.2.2 y de la fórmula (S). □

Como el S-polinomio $f(X,Y)Sf'(X,Y) = f'(X,Y)Sf(X,Y)$, todos los casos han sido considerados.

Ejemplo 6.2.3 *Si* $f(X,Y) = X \vee Y$ *y* $f'(X,Y) = -X \vee -Y$ *entonces teniendo en cuenta las fórmulas del ejemplo 6.2.1 resulta*

$a = 0$, $b = c = d = 1$,
$a_{11} = a_{10} = a_{01} = 1, a_{00} = 0$,
$a' = b' = c' = 1$, $d' = 0$,
$a'_{11} = 1 = a'_{00}$, $a'_{10} = 0 = a'_{01}$.

Luego estamos en el caso I a) y por lo tanto el polinomio $f(X,Y)Sf'(X,Y)$ *es* $(-f \wedge f') \vee (f \wedge -f') = (-X \wedge -Y) \vee (X \wedge Y)$.

Utilizando las fórmulas dadas en el teorema 6.2.1, los polinomios correspondientes en $F(2)$ *son los siguientes:*

$f(X,Y) = X \cdot Y + X + Y$, $f'(X,Y) = X \cdot Y + 1$ y
$f(X,Y)Sf'(X,Y) = X + Y + 1$.

Ejemplo 6.2.4 *Si* $f(X,Y) = X \vee -Y$ *y* $f'(X,Y) = -X$ *entonces tenemos*

$a = c = d = 1, b = 0$,
$a_{11} = 1$, $a_{10} = 0$, $a_{01} = 1 = a_{00}$,
$a' = b' = 1, c' = d' = 0$,
$a'_{11} = 0$, $a'_{10} = 1 = a'_{00}$, $a'_{01} = 0$.

En este ejemplo estamos en el caso II a) y por lo tanto el polinomio $f(X,Y)Sf'(X,Y) = (-Y \wedge f) \vee (Y \wedge -f \wedge f') \vee (f \wedge -f') = 1$.

Los polinomios correspondientes en $F(2)$ *son*

$f(X,Y) = X \cdot Y + Y + 1$, $f'(X,Y) = X + 1$ y
$f(X,Y)Sf'(X,Y) = 1$.

Vimos que utilizando los S-polinomios podemos determinar cuando una base de un ideal es una base de Gröbner.

Ejemplo 6.2.5 *El conjunto* $G = \{X, -X \wedge Y, Y\}$ *es una base de Gröbner del ideal* $I = (X, -X \wedge Y)$ *para el orden lexicográfico.*
Sean $f_1 = X$, $f_2 = -X \wedge Y$ *y* $f_3 = Y$.

Teniendo en cuenta que $f_1Sf_2 = f_2Sf_1$ *aplicando el caso II a) del teorema 6.2.3 tenemos que:*
$f_1Sf_2 = (-Y \wedge f_2) \vee (Y \wedge -f_2 \wedge f_1) \vee (f_2 \wedge -f_1) = f_3$ y
$f_1Sf_2RG = 0$.

Aplicando el caso VI resulta
$f_1Sf_3 = (-X \wedge f_1 \wedge Y) \vee (-f_3 \wedge Y \wedge f_1) \vee (X \wedge f_3 \wedge -Y) \vee (X \wedge f_3 \wedge -f_1) = 0$ y
$f_1Sf_3RG = 0$.

Por último utilizando el caso III a)
$f_2Sf_3 = (-X \wedge f_2) \vee (X \wedge -f_2 \wedge f_3) \vee (f_2 \wedge -f_3) = Y$ y
$f_2Sf_3RG = 0$.

Luego por el teorema 6.1.3, G *es una base de Gröbner de* I.

En el ejemplo anterior el conjunto $F = \{f_1, f_2\}$ no es una base de Gröbner para el ideal $I = (f_1, f_2) = (X, -X \wedge Y)$ pues $LT(f_1Sf_2) = Y \notin (LT(f_1), LT(f_2))$.

Como $f_1Sf_2RF \neq 0$ hacemos $f_3 = f_1Sf_2RF$. Extendemos el conjunto F a un nuevo conjunto $G = \{f_1, f_2, f_3\}$. Cómo ahora $f_3 \in G$ resulta $(f_1Sf_2)RG = 0$.

Luego calculamos f_1Sf_3 y como $(f_1Sf_3)RG = 0$ continuamos con este procedimiento haciendo f_2Sf_3 y calculando $(f_2Sf_3)RG$.

El nuevo conjunto $G = \{f_1, f_2, f_3\}$ verifica que $(f_iSf_j)RG = 0$ para todo $1 \leq i < j \leq 3$. Luego por el teorema 6.1.3, G es una base de Gröbner de I.

Recordemos que una **base de Gröbner minimal** de un ideal polinomial I en $L_2[X_1, \ldots, X_n]$ es una base de Gröbner G de I que satisface:

Para todo $f \in G,\ LT(f) \notin (LT(G - \{f\}))$.

En el ejemplo 6.2.5, como $LT(f_2) = X \wedge Y = X \wedge LT(f_3)$, podemos eliminar f_2 y la base de Gröbner minimal está formada por los polinomios
$\tilde{f}_1 = X, \quad \tilde{f}_3 = Y$.

Veamos el siguiente ejemplo en $L_{2,2}[X, Y]$.

Ejemplo 6.2.6 *Para encontrar una base de Gröbner del ideal generado por los polinomios de* $L_{2,2}[X, Y]$,
$f_1(X, Y) = (C_1(X) \wedge C_0(T(Y))) \vee (C_0(T(X)) \wedge C_1(T(X)) \wedge C_1(T(Y)))$ *y*
$f_2(X, Y) = (C_0(T(X)) \wedge C_1(T(Y))) \vee (C_1(T(X)) \wedge C_0(T(Y)))$
comenzamos buscando el polinomio $f_1 S f_2$ *y calculando* $f_1 S f_2 R\{f_1, f_2\}$.
En este caso particular resulta ser $f_1 S f_2 = f_1 S f_2 R\{f_1, f_2\}$. *Llamamos* f_3 *a* $f_1 S f_2$, *i.e.,*
$f_3 = (C_1(X) \wedge C_0(Y) \wedge C_1(T(X)) \wedge C_0(T(Y))) \vee (C_0(T(X)) \wedge C_1(Y) \wedge C_1(X) \wedge C_0(T(Y))) \vee (C_1(X) \wedge C_0(T(X))) \wedge C_0(T(Y))) \vee (C_0(Y) \wedge C_1(T(Y))) \wedge C_1(T(X)))$.

Continuamos con el procedimiento que nos permite encontrar la base de Gröbner haciendo $f_1 S f_3 R\{f_1, f_2, f_3\}$ *y* $f_2 S f_3 R\{f_1, f_2, f_3\}$ *y obtenemos*
$f_1 S f_3 R\{f_1, f_2, f_3\} = 0$ *y*
$f_2 S f_3 R\{f_1, f_2, f_3\} = f_4$, *donde*
$f_4 = C_1(Y) \wedge C_0(T(Y))$.

Ahora obtenemos
$f_1 S f_4 R\{f_1, f_2, f_3, f_4\} = 0$,
$f_2 S f_4 R\{f_1, f_2, f_3, f_4\} = 0$ *y*
$f_3 S f_4 R\{f_1, f_2, f_3\} = 0$.

Luego $\{f_1, f_2, f_3, f_4\}$ *es una base de Gröbner del ideal generado por los polinomios* f_1 *y* f_2.

Una base de Gröbner minimal es $G = \{f_2, f_3, f_4\}$.

6.3. Conclusiones

En la sección 2 del capítulo 5 planteamos distintas preguntas referidas a la solución de un sistema de ecuaciones polinomiales en $L_{p,k}[X_1, \ldots, X_n]$. Explicamos cómo buscar las soluciones de una ecuación postiana cuando no satisface la condición (C1) o (C2) y dimos una condición necesaria y suficiente para que un sistema de ecuaciones sea compatible. Cuando la solución existe, mostramos un camino para obtenerla.

En este capítulo definimos el concepto de base de Gröbner de un ideal I en $L_{p,k}[X_1, \ldots, X_n]$. Las dificultades computacionales que presenta el cálculo de estas bases, muestra que, en general, no resulta conveniente abordar la solución de un sistema de ecuaciones buscando directamente las bases de Gröbner en $L_{p,k}[X_1, \ldots, X_n]$. Una primera dificultad se presenta en la expresión del producto, que es más complicada a medida que los valores de p y k aumentan. A esta complicación deben

sumarse las que resultan del cálculo de los S-polinomios y las divisiones a efectuarse durante el proceso del cálculo de las bases. En la sección anterior dimos el teorema 6.2.2 que interpreta el algoritmo de división en $L_2[X_1, \ldots, X_n]$. En este caso, al ser $k = 1$ el producto coincide con el ínfimo y esto simplifica los cálculos. En el ejemplo 6.2.1 obtuvimos a partir de un polinomio genérico en $L_2[X, Y]$ la expresión de un polinomio en $F(2)[X, Y]$, lo que nos permitió dar el teorema 6.2.3 que calcula los S-polinomios en $L_2[X, Y]$. Se programó un algoritmo en Maple para encontrar la expresión de un polinomio en $F(2^2)[X, Y]$ a partir de su expresión en $L_{2,2}[X, Y]$. Sin embargo, la complejidad de los cálculos hizo imposible imitar el proceso anterior.

Resolver sistemas de ecuaciones polinomiales no es una tarea simple, y nuestro caso obviamente no es una excepción. Es importante analizar el sistema original y establecer una estrategia que permita obtener la solución, en caso de que exista. El camino descripto en el capítulo 5 es teóricamente el óptimo, aunque requiera de una doble programación en el cálculo de los polinomios, ya que ésta también es necesaria al calcular una base de Gröbner en $L_{p,k}[X_1, \ldots X_n]$. Sin embargo, resulta muy interesante definir estas bases en $L_{p,k}[X_1, \ldots X_n]$ pues esto permite, entre otras operaciones, **dividir** expresiones postianas, lo que resulta original y novedoso.

El sistema de ecuaciones polinomiales del ejemplo 5.2.4 permite observar que el camino utilizado para obtener su solución es el indicado. Es claro que resultaría mucho más complicado calcular las bases de Gröbner directamente en $L_{3,2}[X, Y]$ que hacerlo en $F(3^2)[X, Y]$, debido a los cálculos que involucra el proceso de obtención de las mismas en $L_{3,2}[X, Y]$.

Ahora supongamos que queremos resolver el sistema de ecuaciones polinomiales
$f_1(X, Y) = 0$
$f_2(X, Y) = 0,$
donde f_1 y f_2 son los polinomios del ejemplo 6.2.6. Las expresiones de los mismos en $F(2^2)[X, Y]$ son,
$f_1(X, Y) = X^3Y^2 + X,$
$f_2(X, Y) = X^2 + Y^2,$
y una base de Gröbner minimal de $\{f_1, f_2\}$ es $G = \{f_2, f_3, f_4\}$ donde
$f_3(X, Y) = XY + X$ y
$f_4(X, Y) = Y^3 + Y^2.$

Las expresiones de los polinomios de la base G en $L_{2,2}[X, Y]$ son:
$f_2(X, Y) = (C_0(T(X)) \wedge C_1(T(Y))) \vee (C_1(T(X)) \wedge C_0(T(Y))),$
$f_3(X, Y) = (C_1(X) \wedge C_0(Y) \wedge C_1(T(X)) \wedge C_0(T(Y))) \vee (C_0(X) \wedge C_1(Y) \wedge C_1(T(X)) \wedge C_0(T(Y))) \vee (C_1(X) \wedge C_0(T(X))) \wedge C_0(T(Y))) \vee (C_0(Y) \wedge C_1(T(Y))) \wedge C_1(T(X)))),$
$f_4(X, Y) = C_1(Y) \wedge C_0(T(Y)),$
y las soluciones del sistema son $(0, 0)$ con orden de multiplicidad 2 y $(0, 1)$.

Puede observarse en este último ejemplo que, calcular la base de Gröbner en $F(2^2)[X, Y]$ y luego buscar las expresiones de los polinomios de las bases en $L_{2,2}[X, Y]$, es un camino más directo que buscarlas en $L_{2,2}[X, Y]$. Sin embargo, el proceso de obtención de las mismas, detallado en la segunda sección de este capítulo, no presenta complicaciones en los cálculos.

En el apéndice se presentan numerosos algoritmos programados en Maple que permitieron elaborar los ejemplos de esta tesis.

Bibliografía

[1] Abad, M., J. P. Díaz Varela, B. F. López Martinolich, M. C. Vannicola and M. Zander, *An equivalence between Varieties of ciclic Post Algebras and Varieties generate by a finite field*. Central European Journal of Mathematics, Vol. **4**, (2006), 547-561.

[2] Abad, M., *Cyclic Post Algebras of Order n*, An. Acad. brasil. Ciênc. **53**(2), (1981), 243-246.

[3] Adams, W. and P. Loustaunau, *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics. **3**, AMS, Providence, (1994).

[4] Allgower, E. L. and K. Georg, *Computational Solution of Nonlinear Systems of Equations.* Lectures in Applied Mathematics, vol. **26**, AMS, (1990).

[5] Atiyah, M. F. and I. G. Macdonald, *Introduction to Commutative Algebra.* Addison-Wesley, (1969).

[6] Balbes, R. and A. Dwinger, *Distributive Lattices*, University of Missouri Press, Columbia, MO, (1974).

[7] Becker, T. and V. Weispfenning, *Gröbner Bases*. Graduate Texts in Mathematics 141, Springer-Verlag, (1993).

[8] Boicescu, V., A. Filipoiu, G. Georgescu and S. Rudeanu, *Lukasiewica-Moisil Algebras*, Annals of Discrete Mathematics, vol. **49**, Norh-Holland, Amsterdam, (1991).

[9] Burris, S. and H. P. Sankappanavar, *A course in Universal Algebra*. Graduate Texts in Mathematics 78, Springer-Verlag, (1981).

[10] Cendra, H. *Cyclic Boolean algebras and Galois fields* $F(2^k)$, Portugal Math. **39**, 1-4, (1980), 435-440.

[11] Cignoli, R. *Moisil Algebras*, Notas de Lógica Matemática **27**, Universidad Nacional del Sur, Bahía Blanca, (1970).

[12] Cox, D., J. Little and D. O'Shea, *Ideals, Varieties and Algorithms.* Undergraduate Texts in Mathematics, Springer-Verlag (1992, 1997 Second Edition).

[13] Díaz Varela. J. P. and B. F. López Martinolich, *Resolution of Algebraic Systems of Equations in the Variety of Cyclic Post Algebras.* To appear in Studia Logica.

[14] Eisenbud, D., *Conmutative Algebra with a view toward Geometry*, Springer-Verlag, (1995).

[15] Epstein,G. *The lattice theory of Post algebras*, Trans. Amer. Math. Soc. **95**, (1960), 300-317.

[16] Faugère, J.C., P. Gianni, D. Lazard and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering.* Technical Report LIPT 89-52, (1988).

[17] Faugère, J.C., *Comparison of XL and Gröbner basis algorithms over Finite Fields.* Rapport de recherche N° 5251, (2004).

[18] Gaal, L., *Classical Galois Theory.* AMS Chelsea Publishing, (1998).

[19] Gander, W. and J. Hrebicek, *Solving Problems in Scientific Computing Using Maple and MatLab.* Springer-Verlag, (1993).

[20] Gräbe, H. G., *On factorized Gröbner bases.* Computer Algebra in Science and Ingenieering, World Scientific, Singapore, S. 77-89, (1995).

[21] Hungerford, T. *Algebra*, Springer-Verlag, (1984).

[22] Lejeune-Jalabert, M., *Effectivité de calculs polynomiaux*, Cours de DEA, Grenoble, (1984-1985).

[23] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston (1985).

[24] Lang, S., *Algebra.* Addison-Wesley Publishing Company, Inc., (1984).

[25] Lazard, D., *Solving zero-dimensional algebraic systems.* J. Symbolic Computation **13**, 117-131, (1992).

[26] Lewin, R. *Interpretability into Lukasiewicz algebras*, Rev. Un. Mat. Argentina **42**(3),(1999), 81-89.

[27] Lidl, R. and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, (1997).

[28] López Martinolich, Blanca Fernanda, *Resolución de sistemas de ecuaciones polinomiales*, Tesis de Magister, Biblioteca Central Universidad Nacional del Sur, (1998).

[29] Matsumura H., *Commutative Ring Theory*, Cambridge University Press (1986).

[30] McKenzie, R., G. McNulty and W. Taylor, *Algebras, Lattices, Varieties*, Vol I, Wadsworth and Brooks, Monterey, CA, (1987).

[31] Moisil, G., *The Algebraic Theory of Switching Circuits*, Pergamon Press, Editura Tehnică, Bucharest, (1969).

[32] Moisil, G., *Algebra schemelor cu elemente ventil*, Rev. Universitatti C.I. Parhon, Bucharest, Seria St. nat. 4-5, (1954), 9-15.

[33] Moisil, G., *Algèbres universelles et automates, in "Essais sur les Logiques non Chrysippiennes"*, Editions de L'Academie de la Republique Socialiste de Roumanie, Bucharest, (1972).

[34] Möller, H.M., *On decomposing systems of polinomial equations with finitely many solutions*. J. AAECC **4**, 217-230, (1993).

[35] Monteiro, A., *Algèbres de Boole cycliques*, Rev. Roumaine de Mathématiques Pures Appl. **23**(1),(1978), 71-76.

[36] Rotman, J., *Galois Theory*, Springer-Verlag, (1990).

[37] Rudeanu, S., *Boolean Functions Equations*, North Holland, Elsevier, Amsterdam, New York, (1974).

[38] Serfati, M., *On Postian Algebraic Equations*, Discrete Math. **152**, (1996), 269-285.

[39] Serfati, M., *The lattice theory of r-ordered partitions*. Discrete Mathematics **194** (1999), 205-227.

[40] Spindler, K., *Abstract Algebra with Applications*, Volumen II, Marcelb Dekker, Inc. (1994).

[41] Seidenberg, A., *On the Lasker-Noether decomposition theorem*. Am. J. Math **106**, 611-638, (1984).

[42] Stewart, I., *Galois Theory*. ChapmanHall/CRC. (2004).

[43] Traczyk,T., *Axioms and some Properties of Post Algebras*, Coll. Math. **10** (1963). 198-209.

[44] Vasconcelos, W., *Computational methods in Commutative Algebra and Algebraic Geometry.* Springer, Berlin-Heidelberg-New York, (1998).

[45] Winkler, F., *Polynomial algorithms in Computer Algebra*. Springer, Wien-New-York, (1996).

[46] Zariski, O. and P. Samuel, *Commutative Algebra I,II*. Graduate Texts in Mathematics 28, 29. Springer-Verlag, (1979).

Apéndice:Algoritmos programados en Maple

Los algoritmos incluídos en esta sección han sido programados en Maple para los valores de $p = 3$, $k = 1$ y $k = 2$. Éstos pueden implementarse, y siguiendo estos ejemplos es posible elaborar programas para otros valores de p y k siempre que la complejidad computacional de los mismos permita su ejecución.

Polinomios con coeficientes en $F(3)$ y L_3

Cálculo del ínfimo

```
inf3 := proc(r,s)
local x, y;
    if r = 0 or s = 0 then inf3(r, s) := 0
          else
             if r = 1 then inf3(r, s) := s
                    else
                       if s = 2 and r = 2 then inf3(r, s) := 2
                             else
                                   x := r;
                                   y := s;
                                         if x = y then return x
                                                  else 'inf3(r, s)'
                                         end if
                       end if
             end if
    end if;
end proc:
```

Cálculo del Supremo

```
sup3 := proc(r,s)
local supremo, x, y;
    if r = 1 or s = 1 then sup3(r, s) := 1
          else
             if r = 0 then sup3(r, s) := s
                   else
                         if r = 2 and s = 2 then sup3(r, s) := 2
                               else
                                     x := r;
                                     y := s;
                                           if x = y then return x
                                                    else 'sup3(r, s)'
                                           end if
                         end if
```

```
            end if
    end if
end proc:
```

Cálculo de las constantes

```
e3 := proc(i)
    if i = 0 then e3(i) := 0
            else
               if i = 1 then e3(i) := 2
                        else
                        if i = 2 then e3(i) := 1
                                 else return'e3(i)'
                        end if
               end if
    end if
end proc:
```

Cálculos de los C_i3

```
C := proc(i,z)
local c;
if i = 0 then if z = 0 then c := 1
          elif z = 1 or z = 2 then c := 0
          elif z = sup3(x, y) then return 'inf3(C(0, x), C(0, y))'
          elif z = inf3(x, y) then return 'sup3(C(0, x), C(0, y))
                                          else return 'C(0, z)'
          end if
       else if i = 1 then if z = 2 then c := 1
          elif z = 0 or z = 1 then c := 0
          elif z = sup3(x, y) then return
            'sup3(sup3(inf3(C(1, x), C(0, y)), inf3(C(1, x), C(1, y))), inf3(C(0, x), C(1, y)))'
          elif z = inf3(x, y) then return
            'sup3(sup3(inf3(C(1, x), C(2, y)), inf3(C(1, x), C(1, y))), inf3(C(2, x), C(1, y)))'
                                    else return 'C(1, z)'
          end if
       else if i = 2 then if z = 1 then c := 1
          elif z = 0 or z = 2 then c := 0
          elif z = sup3(x, y) then return 'sup3(C(2, x), C(2, y))'
          elif z = inf3(x, y) then return 'inf3(C(2, x), C(2, y))'
                           else return 'C(2, z)'
       end if
          else return'C(i, z)'
          end if;
end if;
```

Declaraciones para una biblioteca

$C(0, C(0, x)) := sup3(C(1, x), C(2, x));$
$C(0, C(1, x)) := sup3(C(0, x), C(2, x));$
$C(0, C(2, x)) := sup3(C(0, x), C(1, x));$
$C(1, C(0, x)) := 0;$
$C(1, C(1, x)) := 0;$
$C(1, C(2, x)) := 0;$
$C(2, C(0, x)) := C(0, x)$
$C(2, C(1, x)) := C(1, x);$
$C(2, C(2, x)) := C(2, x);$
$C(0, sup3(C(0, x), C(0, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(0, x), C(1, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(0, x), C(2, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(0, x), C(0, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(0, x), C(1, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(0, x), C(2, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, sup3(C(1, x), C(0, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(1, x), C(1, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(1, x), C(2, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(1, x), C(0, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(1, x), C(1, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(1, x), C(2, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, sup3(C(2, x), C(0, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(2, x), C(1, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(2, x), C(2, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(2, x), C(0, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(2, x), C(1, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(2, x), C(2, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(1, y)));$
$C(1, sup3(C(0, x), C(0, y))) := 0;$
$C(1, sup3(C(0, x), C(1, y))) := 0;$
$C(1, sup3(C(0, x), C(2, y))) := 0;$
$C(1, inf3(C(0, x), C(0, y))) := 0;$
$C(1, inf3(C(0, x), C(1, y))) := 0;$
$C(1, inf3(C(0, x), C(2, y))) := 0;$
$C(1, sup3(C(1, x), C(0, y))) := 0;$
$C(1, sup3(C(1, x), C(1, y))) := 0;$
$C(1, sup3(C(1, x), C(2, y))) := 0;$
$C(1, inf3(C(1, x), C(0, y))) := 0;$
$C(1, inf3(C(1, x), C(1, y))) := 0;$
$C(1, inf3(C(1, x), C(2, y))) := 0;$
$C(1, sup3(C(2, x), C(0, y))) := 0;$
$C(1, sup3(C(2, x), C(1, y))) := 0;$

$C(1, sup3(C(2,x), C(2,y))) := 0;$
$C(1, inf3(C(2,x), C(0,y))) := 0;$
$C(1, inf3(C(2,x), C(1,y))) := 0;$
$C(1, inf3(C(2,x), C(2,y))) := 0;$
$C(2, sup3(C(0,x), C(0,y))) := sup3(C(0,x), C(0,y));$
$C(2, sup3(C(0,x), C(1,y))) := sup3(C(0,x), C(1,y));$
$C(2, sup3(C(0,x), C(2,y))) := sup3(C(0,x), C(2,y));$
$C(2, inf3(C(0,x), C(0,y))) := inf3(C(0,x), C(0,y));$
$C(2, inf3(C(0,x), C(1,y))) := inf3(C(0,x), C(1,y));$
$C(2, inf3(C(0,x), C(2,y))) := inf3(C(0,x), C(2,y));$
$C(2, sup3(C(1,x), C(0,y))) := sup3(C(1,x), C(0,y));$
$C(2, sup3(C(1,x), C(1,y))) := sup3(C(1,x), C(1,y));$
$C(2, sup3(C(1,x), C(2,y))) := sup3(C(1,x), C(2,y));$
$C(2, inf3(C(1,x), C(0,y))) := inf3(C(1,x), C(0,y));$
$C(2, inf3(C(1,x), C(1,y))) := inf3(C(1,x), C(1,y));$
$C(2, inf3(C(1,x), C(2,y))) := inf3(C(1,x), C(2,y));$
$C(2, sup3(C(2,x), C(0,y))) := sup3(C(2,x), C(0,y));$
$C(2, sup3(C(2,x), C(1,y))) := sup3(C(2,x), C(1,y));$
$C(2, sup3(C(2,x), C(2,y))) := sup3(C(2,x), C(2,y));$
$C(2, inf3(C(2,x), C(0,y))) := inf3(C(2,x), C(0,y));$
$C(2, inf3(C(2,x), C(1,y))) := inf3(C(2,x), C(1,y));$
$C(2, inf3(C(2,x), C(2,y))) := inf3(C(2,x), C(2,y));$
$C(0, sup3(C(1,x), C(2,x))) := C(0,x);$
$C(1, sup3(C(1,x), C(2,x))) := 0;$
$C(2, sup3(C(1,x), C(2,x))) := sup3(C(1,x), C(2,x));$
$C(0, sup3(C(1,y), C(2,y))) := C(0,y);$
$C(1, sup3(C(1,y), C(2,y))) := 0;$
$C(2, sup3(C(1,y), C(2,y))) := sup3(C(1,y), C(2,y));$
$C(0, sup3(inf3(sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(1,y))), 2),$
$sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(2,y))))) := sup3(C(0,x), C(0,y));$
$C(1, sup3(inf3(sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(1,y))), 2),$
$sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(2,y))))) := 0;$
$C(2, sup3(inf3(sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(1,y))), 2),$
$sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(2,y))))) :=$
$sup3(inf3(sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(1,y))), 2),$
$sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(2,y))));$
$C(0, sup3(inf3(inf3(sup3(C(1,x), C(2,x)), C(1,y)), 2),$
$inf3(sup3(C(1,x), C(2,x)), C(2,y)))) := sup3(C(0,x), C(0,y));$
$C(1, sup3(inf3(inf3(sup3(C(1,x), C(2,x)), C(1,y)), 2),$
$inf3(sup3(C(1,x), C(2,x)), C(2,y)))) := sup3(inf3(C(1,x), C(1,y)), (C(2,x), C(1,y)));$
$C(2, sup3(inf3(inf3(sup3(C(1,x), C(2,x)), C(1,y)), 2),$
$inf3(sup3(C(1,x), C(2,x)), C(2,y)))) := sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(2,y)));$
$C(0, sup3(inf3(sup3(C(1,x), C(2,x)), 2), C(0,x))) := 0;$

$C(1, sup3(inf3(sup3(C(1,x), C(2,x)), 2), C(0,x))) := sup3(C(1,x), C(2,x))$;
$C(2, sup3(inf3(sup3(C(1,x), C(2,x)), 2), C(0,x))) := C(0,x)$;
$inf3(sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(2,y))), C(0,x))) := 0$;
$inf3(sup3(C(0,x), C(0,y)), sup3(C(1,x), C(2,x))) :=$
$= sup3(inf3(C(1,x), C(0,y)), inf3(C(2,x), C(0,y)))$;
$inf3(sup3(C(0,x), C(0,y)), C(0,x)) := C(0,x)$;
$inf3(sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y))), sup3(C(1,x), C(2,x))) :=$
$= sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y)))$;
$C(0, inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y)))) := sup3(C(0,x), C(0,y))$;
$C(1, inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y)))) := 0$;
$C(2, inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y)))) :=$
$inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y)))$;
$C(0, sup3(inf3(sup3(C(0,x), C(0,y)), 2), sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y))))) :=$
$= sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(2,y)))$;
$C(1, sup3(inf3(sup3(C(0,x), C(0,y)), 2), sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y))))) :=$
$= sup3(C(0,x), sup3(inf3(C(1,x), C(0,y)), inf3(C(2,x), C(0,y))))$;
$C(2, sup3(inf3(sup3(C(0,x), C(0,y)), 2), sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y))))) :=$
$= sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y)))$;
$inf3(sup3(C(0,x), C(0,y)), sup3(C(0,x), sup3(inf3(C(1,x), C(0,y)), inf3(C(2,x), C(0,y))))) :=$
$= sup3(sup3(C(0,x), inf3(C(1,x), C(0,y))), inf3(C(2,x), C(0,y)))$;
$inf3(inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y)))sup3(inf3(C(1,x), C(1,y)),$
$inf3(C(2,x), C(1,y)))) := sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y)))$;
$inf3(sup3(C(0,x), C(0,y)), sup3(inf3(C(1,x), C(1,y)), inf3(C(2,x), C(1,y)))) :=$
$= 0$;
$inf3(inf3(sup3(C(1,x), C(2,x)), sup3(C(1,y), C(2,y))), sup3(inf3(C(1,x), C(2,y)),$
$inf3(C(2,x), C(2,y)))) := sup3(inf3(C(1,x), C(2,y)), inf3(C(2,x), C(2,y)))$;

```
    c;
    end proc:
```

Cálculo de $C_i3(x\Delta y)$

```
    Cixdely3 := proc(i,x,y)
    local resul, s, t;
    resul:=0;
        for s from 0 to 2 do
            for t from 0 to 2 do
                if modp(s+t-i,3)=0 then
                    resul:=sup3(resul,inf3(C(s,x),C(t,y)));
                end if;
                if s <> t and x = y then inf3(C(s,x), C(t,y)) := 0;
                end if;
                if s <> t and x = y then inf3(C(t,y), C(x,s)) := 0;
                end if;
            end do
```

```
    end do;
resul
end proc:
```

Cálculo de $x\Delta y$

```
xdely3:= proc(x,y)
local i, suma;
      for i from 0 to 2 do
            suma:= sup3(suma,inf3(Cixdely3(i,x,y),e3(i)))
      end do;
suma
end proc:
```

xdely3(x,y);

$$sup3(inf3(sup3(sup3(inf3(C(0,x),C(1,y)),inf3(C(1,x),C(0,y)))inf3(C(2,x),C(2,y)),2),$$

$$sup3(sup3(inf3(C(0,x),C(2,y)),inf3(C(1,x),C(1,y))),inf3(C(2,x),C(0,y))))$$

La salida del programa es la siguiente:

$$x\Delta y = (C_0(x) \wedge C_1(y)) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_2(y))] \wedge e_1\} \vee$$

$$\vee (C_0(x) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_0(y)).$$

Cálculo de $C_i3(x \odot y)$

```
Cixody3:= proc(i,x,y)
local resul, s, t, u, v;
resul:= 0;
    for s from 0 to 2 do
       for t from 0 to 2 do
          if (modp(s*t+i,3)=0) then resul:= sup3(resul,inf3(C(s,x),C(t,y)))
          end if;
          if resul = inf3(C(s,x),C(t,y)) and s <> t and x = y then resul:=0
          end if;
          if resul = sup3(C(s,x),inf3(C(s,x),C(t,y))) then resul:=C(s,x)
          end if;
          if resul = sup3(C(t,y),inf3(C(s,x),C(t,y))) then resul:=C(t,y)
          end if;
       end do
    end do;
if resul = sup3(inf3(C(1,x),C(2,y)),inf3(C(1,x),C(2,y))) then
                        resul:= inf3(C(1,x),(C(2,y)))
end if;
if resul = sup3(sup3(C(0,x),C(1,x)),C(2,x)) or resul = sup3(sup3(C(0,y),C(1,y)),C(2,y))
```

```
                then resul:= 1
end if;
resul;
end proc:
```

Cálculo de $x \odot y$

```
xody3:= proc(x,y)
local i, suma;
      for i from 0 to 2 do
            suma:= sup3(suma,inf3(Cixody3(i,x,y),e3(i)))
      end do;
suma
end proc:
xody3(x,y);
```

$$sup3(inf3(sup3(inf3(C(1,x),C(2,y)),inf3(C(2,x),C(1,y))),2),$$
$$sup3(inf3(C(1,x),C(1,y)),inf3(C(2,x),C(2,y)))).$$

Luego
$x \odot y = \{[(C_1(x) \wedge C_2(y)) \vee (C_2(x) \wedge C_1(y))] \wedge e_1\} \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y))$.

Cálculo del elemento primitivo

```
readlib(GF):
G:= GF(3,1):
ep:= G[ConvertOut](G[PrimitiveElement]());
```

$$ep := 2$$

Cálculo de los coeficientes

```
coef:= proc(a)
    if a = 1 then e3(a):= 2
             else e3(a):= 1
    end if
end proc:
```

Cálculo de los polinomios de Lagrange en F_3

```
L0 := proc(p,k,x)
(p - 1) * x^(p^k-1) + 1;
end proc:
L0(3,1,x);
```

$$2x^2 + 1$$

```
L := proc(p,k,i,x)
```

```
local polilag;
    if i = 0 then polilag:=(p − 1) ∗ x^(p^k−1) + 1;
             else polilag:= L0(p, k, x + (p − 1) ∗ i);
    end if;
polilag;
end proc:

L := proc(p, k, i, x)
local polilag, pol, j;
    if i = 0 then polilag:=(p − 1) ∗ x^(p^k−1) + 1
             else polilag:= L0(p, k, x + (p − 1) ∗ i);
    end if;
pol:= 0;
for j from 0 to 2 do
pol:= pol + x^j∗(coeff(polilag,x,j) mod p);
end do;
pol;
end proc:
L(3,1,0,x);
L(3,1,1,x);
L(3,1,2,x);
```

$$2x^2 + 1$$

$$2x^2 + 2x$$

$$2x^2 + x$$

Cálculo del ínfimo en L_3

```
xinfy3:= proc(x,y)
local suma, i, j;
suma:=0;
for i from 0 to 2 do
      for j from 0 to 2 do
            suma:= suma + inf3(i,j)∗L(3,1,i,x)∗L(3,1,j,y) mod 3;
      end do;
end do;
end proc:

xinfy3:= proc(x,y)
local suma, pol, i, j;
suma:= 0;
for i from 0 to 2 do
      for j from 0 to 2 do
```

```
            suma:= suma + inf3(i,j)*L(3,1,i,x)*L(3,1,j,y) mod 3;
        end do;
end do;
pol:= 0 ;
for j from 0 to 2 do
pol:= pol + x^j*(coeff(suma,x,j) mod 3);
end do;
pol;
end proc:
xinfy3(x,y);
```

$$x(2y + 2y^2) + x^2(2y + y^2)$$

Cálculo del supremo en L_3

```
xsupy3:= proc(x,y)
local suma, i, j;
suma:=0;
for i from 0 to 2 do
        for j from 0 to 2 do
            suma:= suma + sup3(i,j)*L(3,1,i,x)*L(3,1,j,y) mod 3;
        end do;
end do;
end proc:

xsupy3:= proc(x,y)
local suma, pol, i, j;
suma:= 0;
for i from 0 to 2 do
        for j from 0 to 2 do
            suma:= suma + sup3(i,j)*L(3,1,i,x)*L(3,1,j,y) mod 3;
        end do;
end do;
pol:= 0 ;
for j from 0 to 2 do
pol:= pol + x^j*(coeff(suma,x,j) mod 3);
end do;
pol;
end proc:
xsupy3(x,y);
```

$$y + x(y^2 + 1 + y) + x^2(y + 2y^2)$$

Cálculo de los polinomios de Lagrange en L_3

```
L0 := proc(p,x)
```

$e3(2) + (p-1) * x^{p-1}$;
end proc:
L0(3,x);

$$2x^2 + 1$$

El polinomio obtenido es $\mathcal{L}_0(x) = 2 \odot x^2 \Delta 1$

```
L := proc(p,i,x)
local polag;
    if i = 0 then polag:=e3(2) + (p-1) * x^(p-1)
             else polag:= L0(p, x + (p-1) * i);
    end if;
polag;
end proc:
```

```
L := proc(p, i, x)
local polag, pol, j;
    if i = 0 then polag:=e3(2) + (p-1) * x^(p-1)
             else polag:= L0(p, x + (p-1) * i);
    end if;
pol:= 0;
for j from 0 to 2 do
pol:= pol + x^j*(coeff(polag,x,j) mod p);
end do;
pol;
end proc:
```

L(3,0,x);
L(3,1,x);
L(3,2,x);

$$2x^2 + 1$$
$$2x^2 + 2x$$
$$2x^2 + x$$

Los polinomios obtenidos son:
$\mathcal{L}_0(x) = 2 \odot x^2 \Delta 1$
$\mathcal{L}_1(x) = 2 \odot x^2 \Delta 2 \odot x$ y
$\mathcal{L}_2(x) = 2 \odot x^2 \Delta x$.

Cálculo del producto en $\langle L_3; \Delta, \odot \rangle$

```
prodanillo3:= proc(x,y)
local suma, i, j;
suma:=0;
for i from 0 to 2 do
```

```
        for j from 0 to 2 do
              suma:= suma + e3(i)*e3(j)*L(3,e3(i),x)*L(3,e3(j),y) mod 3;
        end do;
end do;
suma;
end proc:
prodanillo3(x,y);

prodanillo3:= proc(x,y)
local suma, sum, i, j, k;
suma:=0;
for i from 0 to 2 do
        for j from 0 to 2 do
              suma:= suma + e3(i)*e3(j)*L(3,e3(i),x)*L(3,e3(j),y) mod 3;
        end do;
end do;
suma;
sum:=0;
for k from 0 to 2 do
sum:= sum + x^k * (coeff(suma, x, k)mod3);
end do;
sum;
end proc:
prodanillo3(x,y);
```

$$xy$$

El resultado obtenido es $x \cdot y = x \odot y$

Cálculo de la suma en $\langle L_3; \Delta, \odot \rangle$

```
sumanillo3:= proc(x,y)
local suma, i, j;
suma:=0;
for i from 0 to 2 do
        for j from 0 to 2 do
              suma:= suma + (e3(i) + e3(j)) * L(3,e3(i),x)*L(3,e3(j),y) mod 3;
        end do;
end do;
suma;
end proc:
sumanillo3(x,y);

sumanillo3:= proc(x,y)
local suma, sum, i, j, k;
suma:=0;
```

```
for i from 0 to 2 do
      for j from 0 to 2 do
            suma:= suma + e3(i) + e3(j)*L(3,e3(i),x)*L(3,e3(j),y) mod 3;
      end do;
end do;
suma;
sum:=0;
for k from 0 to 2 do
sum:= sum + x^k * (coeff(suma, x, k)mod3);
end do;
sum;
end proc:
sumanillo3(x,y);
```

$$x + y$$

El resultado obtenido es $x + y = x\Delta y$.

Cálculo de una expresión dada en $L_3[X, Y]$ en $F(3)[X, Y]$

$C0x := 2 * x^2 + 1;$
$C1x := 2 * x^2 + x;$
$C2x := 2 * x^2 + 2 * x;$

$C0y := 2 * y^2 + 1;$
$C1y := 2 * y^2 + y;$
$C2y := 2 * y^2 + 2 * y;$

C1xinf3e1:=proc(x)
local res1, res2, resul;
res1:=$C1x^2 * 2^2 + 2 * C1x^2 * 2 + 2 * C1x * 2^2 + 2 * C1x * 2$ mod 3;
res2:=expand(res1) mod 3;
resul:=algsubs($x^3 = x$,res2) mod 3;
resul;
end proc:

C2xinf3e1:=proc(x)
local res1, res2, resul;
res1:=$C2x^2 * 2^2 + 2 * C2x^2 * 2 + 2 * C2x * 2^2 + 2 * C2x * 2$ mod 3;
res2:=expand(res1) mod 3;
resul:=algsubs($x^3 = x$,res2) mod 3;
resul;
end proc:

C1xinf3C2y:=proc(x,y)
local res1, res2, resul1,resul2, resul;
res1:=$C1x^2 * C2y^2 + 2 * C1x^2 * C2y + 2 * C1x * C2y^2 + 2 * C1x * C2y$ mod 3;
res2:=expand(res1) mod 3;

resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=expand(resul2) mod 3;
end proc:

C2xinf3C1y:=proc(x,y)
local res1, res2, resul1, resul2, resul;
res1:=$C2x^2 * C1y^2 + 2 * C2x^2 * C1y + 2 * C2x * C1y^2 + 2 * C2x * C1y$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=expand(resul2) mod 3;
end proc:

C1xinf3C1y:=proc(x,y)
local res1, res2, resul1, resul2, resul ;
res1:=$C1x^2 * C1y^2 + 2 * C1x^2 * C1y + 2 * C1x * C1y^2 + 2 * C1x * C1y$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=expand(resul2) mod 3;
end proc:

C2xinf3C2y:=proc(x,y)
local res1, res2, resul1, resul2, resul;
res1:=$C2x^2 * C2y^2 + 2 * C2x^2 * C2y + 2 * C2x * C2y^2 + 2 * C2x * C2y$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=expand(resul2) mod 3;;
end proc:

C1xinf3C2yinf3e1:=proc(x,y)
local res1, res2, resul1, resul2, resul, resfin;
res1:=$C1xinf3C2y(x,y)^2 * 2^2 + 2 * C1xinf3C2y(x,y)^2 * 2+$
$2 * C1xinf3C2y(x,y) * 2^2 + 2 * C1xinf3C2y * 2(x,y)$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=algsubs($y^3 = y$,resul2) mod 3;
resfin:=expand(resul) mod 3;
end proc:

C2xinf3C1yinf3e1:=proc(x,y)
local res1, res2, resul1, resul2, resul, resfin;
res1:=$C2xinf3C1y(x,y)^2 * 2^2 + 2 * C2xinf3C1y(x,y)^2 * 2+$

$2 * C2xinf3C1y(x,y) * 2^2 + 2 * C2xinf3C1y(x,y) * 2$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=algsubs($y^3 = y$,resul2) mod 3;
resfin:=expand(resul) mod 3;
end proc:

C1xinf3C1yinf3e1:=proc(x,y)
local res1, res2, resul1, resul2, resul, resfin;
res1:=$C1xinf3C1y(x,y)^2 * 2^2 + 2 * C1xinf3C1y(x,y)^2 * 2+$
$2 * C1xinf3C1y(x,y) * 2^2 + 2 * C1xinf3C1y(x,y) * 2$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=algsubs($y^3 = y$,resul2) mod 3;
resfin:=expand(resul) mod 3;
end proc:

C2xinf3C2yinf3e1:=proc(x,y)
local res1, res2, resul1, resul2, resul, resfin;
res1:=$C2xinf3C2y(x,y)^2 * 2^2 + 2 * C2xinf3C2y(x,y)^2 * 2+$
$2 * C2xinf3C2y(x,y) * 2^2 + 2 * C2xinf3C2y * 2(x,y)$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($y^3 = y$,resul1) mod 3;
resul:=algsubs($y^3 = y$,resul2) mod 3;
resfin:=expand(resul) mod 3;
end proc:

Polinomios en $F(3)[X,Y]$

Los ejemplos que se dan a continuación muestran la expresión en $F(3)[X,Y]$ de polinomios dados en $L_3[X,Y]$.

polinf:=proc(x)
local res1, res2, resul1, resul2, resul3, resul4, res, resfin;
res1:=$2 * C1xinf3e1(x)^2 * C2xinf3e1(x)^2 + C1xinf3e1(x)^2 * C2xinf3e1(x)+$
$+C1xinf3e1(x) * C2xinf3e1(x)^2 + C1xinf3e1(x) * C2xinf3e1(x) + C1xinf3e1(x)+$
$+C2xinf3e1(x)$ mod 3;
res2:=expand(res1) mod 3;
resul1:=algsubs($x^3 = x$,res2) mod 3;
resul2:=algsubs($x^3 = x$,resul1) mod 3;
resul3:=$2 * C0x * resul2^2 + C0x^2 * resul2 + C0x * resul2^2 + C0x * resul2+$
$+C0x + resul2$ mod 3;
resul4:=expand(resul3) mod 3;

res:=algsubs($x^3 = x$,resul4) mod 3;
resfin:=algsubs($x^3 = x$,res) mod 3;
end proc:
polinf(x);

$$x^2 + 1.$$

El polinomio $f(X) = C_0(X) \vee (C_1(X) \wedge e_1) \vee (C_2(X) \wedge e_1) \in L_3[X]$ corresponde a $f(X) = X^2 + 1$ en $F(3)[X]$.

poling(x,y):=proc(x,y)
local res1, res2, res3, res4, res5, res6, resul1, resul2, resul3, resul4, resul5, res, resfin, resfin2;
$res1:=2 * C1xinf3C2yinf3e1(x,y)^2 * C2xinf3C1yinf3e1(x,y)^2+$
$+C1xinf3C2yinf3e1(x,y)^2 * C2xinf3C1yinf3e1(x,y)+$
$+C1xinf3C2yinf3e1(x,y) * C2xinf3C1yinf3e1(x,y)^2+$
$+C1xinf3C2yinf3e1(x,y) * C2xinfC1yinf3e1(x,y)+$
$+C1xinf3C2yinf3e1(x,y) + C2xinf3C1yinf3e1(x,y)$ mod 3;
res2:=expand(res1) mod 3;
res3:=algsubs($x^3 = x$,res2) mod 3;
resul1:=algsubs($y^3 = y$,res3) mod 3;
$res4:=2 * C1xinf3C1y^2 * C2xinf3C2y^2 + C1xinf3C1y^2 * C2xinf3C2y+$
$+C1xinf3C1y * C2xinf3C2y^2 + C1xinf3C1y * C2xinfC2y+$
$+C1xinf3C1y + C2xinf3C2y$ mod 3;
res5:=expand(res4) mod 3;
res6:=algsubs($x^3 = x$,res5) mod 3;
resul2:=algsubs($y^3 = y$,res6) mod 3;
$resul3:=2*resul1^2*resul2^2+resul1^2*resul2+resul1*resul2^2+resul1*resul2+$
$+resul1 + resul2$ mod 3;
resul4:=expand(resul3) mod 3;
resul5:=algsubs($x^3 = x$,resul4) mod 3;
res:=algsubs($y^3 = y$,resul5) mod 3;
resfin:=algsubs($x^3 = x$,res) mod 3;
resfin2:=algsubs($y^3 = y$,resfin) mod 3;
end proc:

poling(x,y);

$$xy$$

El polinomio $g(X,Y) = (C_1(X) \wedge C_2(Y) \wedge e_1) \vee (C_2(X) \wedge C_1(Y) \wedge e_1) \vee$
$\vee (C_1(X) \wedge C_1(Y)) \vee (C_2(X) \wedge C_2(Y)) = 0$ es el polinomio $g(X,Y) = X \cdot Y$ en $F(3)[X,Y]$

polinh:=proc(x,y)
local res1, res2, res3, res4, res5, res6, resul1, resul2, resul3, resul4, resul5, res, resfin, resfin2;
$res1:=2 * C1xinf3C1yinf3e1(x,y)^2 * C2xinf3C2yinf3e1(x,y)^2+$

$+C1xinf3C1yinf3e1(x,y)^2 * C2xinf3C2yinf3e1(x,y)+$
$+C1xinf3C1yinf3e1(x,y) * C2xinf3C2yinf3e1(x,y)^2+$
$+C1xinf3C1yinf3e1(x,y) * C2xinfC2yinf3e1(x,y)+$
$+C1xinf3C1yinf3e1(x,y) + C2xinf3C2yinf3e1(x,y)$ mod 3;
res2:=expand(res1) mod 3;
res3:=algsubs($x^3 = x$,res2) mod 3;
resul1:=algsubs($y^3 = y$,res3) mod 3;
res4:=$2 * C0x^2 * C0y^2 + C0x^2 * C0y + C0x * C0y^2 + C0x * C0y + C0x + C0y$ mod 3;
res5:=expand(res4) mod 3;
res6:=algsubs($x^3 = x$,res5) mod 3;
resul2:=algsubs($y^3 = y$,res6) mod 3;
resul3:=$2*resul1^2*resul2^2+resul1^2*resul2+resul1*resul2^2+resul1*resul2+$
$+resul1 + resul2$ mod 3;
resul4:=expand(resul3) mod 3;
resul5:=algsubs($x^3 = x$,resul4) mod 3;
res:=algsubs($y^3 = y$,resul5) mod 3;
resfin:=algsubs($x^3 = x$,res) mod 3;
resfin2:=algsubs($y^3 = y$,resfin) mod 3;
resfin3:=algsubs($y^3 = y$,resfin) mod 3;
end proc:

polinh(x,y);

$$x \cdot y + 1.$$

La expresión del polinomio $h(X,Y) = C_0(X) \vee C_0(Y) \vee (C_1(X) \wedge C_1(Y) \wedge e_1) \vee$
$\vee (C_2(X) \wedge C_2(Y) \wedge e_1) = 0 \in L_3[X,Y]$ corresponde a $h(X,Y) = X \cdot Y + 1$ en F(3)[X,Y].

Cálculo de un término dado en $F(3)[X,Y]$ en $L_3[X,Y]$

terxy:=proc(x,n,y,m,a)
local terx, s, tery, t, ter;
s:= $G[ConvertOut](G[`](G[ConvertIn](ep), n-1))$;
terx:= x^s;
t:= $G[ConvertOut](G[`](G[ConvertIn](ep), m-1))$;
tery:= y^t;
if $a = 1$ then e3(a):=2
else e3(a):=1
end if;
ter:= e3(a)*terx*tery;
ter;
end proc:

terxL3:=proc(x,n)

```
local s, tex, i;
s:= G[ConvertOut](G[‘](G[ConvertIn](ep), n − 1));
tex:=x;
for i from 2 to s do
    tex:=xody3(tex,x)
end do;
tex;
end proc:

teryL3:=proc(y,m)
local t, tey, j;
t:= G[ConvertOut](G[‘](G[ConvertIn](ep), m − 1));
tey:=y;
for j from 2 to t do
    tey:=xody3(tey,y)
end do;
tey;
end proc:

terxyL3:=proc(x,n,y,m)
local terx, tery, terxy;
terx:= terxL3(x,n);
tery:= teryL3(y,m);
terxy:= xody3(terx,tery);
terxy;
end proc:
```

Polinomios en $L_3[X, Y]$

Los siguientes ejemplos nos muestran la expresión en $L_3[X, Y]$ de algunos polinomios dados en $F(3)[X, Y]$.

terxyL3(x,1,y,1);

$$sup3(inf3(sup3(inf3(C(1,x),C(2,y)),inf3(C(2,x),C(1,y))),2),$$

$$sup3(inf3(C(1,x),C(1,y)),inf3(C(2,x),C(2,y)))),$$

esto es $x \cdot y =$
$= \{[(C_1(x) \wedge C_2(y)) \vee (C_2(x) \wedge C_1(y))] \wedge e_1\} \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y))$.

terxL3(x,2);

$$sup3(C(1,x),C(2,x)),$$

i.e. $x^2 = C_1(x) \vee C_2(x)$

terxyL3(x,2,y,2);

$$inf3(sup3(C(1,x),C(2,x)),sup3(C(1,y),C(2,y))).$$

Luego $x^2 \cdot y^2 = (C_1(x) \vee C_2(x)) \wedge (C_1(y) \vee C_2(y))$.

terxyL3(x,2,y,1);

$$sup3(inf3(inf3(sup3(C(1,x),C(2,x)),C(1,y)),2),inf3(sup3(C(1,x),C(2,x)),C(2,y))).$$

Aquí obtenemos
$x^2 \cdot y = [(C_1(x) \vee C_2(x)) \wedge C_1(y) \wedge e_1] \vee [(C_1(x) \vee C_2(x)) \wedge C_2(y)]$.

xdely3(terxL3(x,2),1);

$$sup3(inf3(sup3(C(1,x),C(2,x)),2),C(0,x)),$$

Luego $x^2 + 1 = [(C_1(x) \vee C_2(x)) \wedge e_1] \vee C_0(x)$.

xdely3(x,y);

$$sup3(inf3(sup3(sup3(inf3(C(0,x),C(1,y)),inf3(C(1,x),C(0,y))),inf3(C(2,x),C(2,y))),2),$$

$$sup3(sup3(inf3(C(0,x),C(2,y)),inf3(C(1,x),C(1,y))),inf3(C(2,x),C(0,y)))).$$

La expresión es
$x + y = \{[(C_0(x) \wedge C_1(y)) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_2(y))] \wedge e_1\} \vee$
$\vee [(C_0(x) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_0(y))$.

xdely3(terxyL3(x,1,y,1),2);

$$inf3(sup3(C(0,x),C(0,y)),2),$$

i.e. $x \cdot y + 2 = (C_0(x) \vee C_0(y)) \wedge e_1$.

xdely3(x,1);

$$sup3(inf3(C(2,x),2),C(0,x)).$$

El polinomio correspondiente es
$x + 1 = (C_2(x) \wedge e_1) \vee C_0(x)$.

xdely3(terxyL3(x,2,y,1),xdely3(terxL3(x,2),1));

$$sup3(inf3(sup3(inf3(C(1,x),C(0,y)),inf3(C(2,x),C(0,y))),2),$$

$$sup3(C(0,x),sup3(inf3(C(1,x),C(1,y)),inf3(C(2,x),C(1,y))))).$$

La expresión $x^2y + x^2 + 1 =$
$= \{[(C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_0(y))] \wedge e_1\} \vee [(C_0(x) \vee (C_1(x) \wedge C_1(y)) \vee$
$\vee (C_2(x) \wedge C_1(y))$.

xdely3(terxy(x,2,y,1,2);

$$sup3(inf3(sup3(C(0,x),C(0,y)),2),sup3(inf3(C(1,x),C(1,y)),inf3(C(2,x),C(1,y)))).$$

La salida es
$x^2y + 2 = [(C_0(x) \vee C_0(y)) \wedge e_1] \vee [(C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_1(y))]$

xdely3(terxyL3(x,2,y,2),xdely3(terxyL3(x,2,y,1),2));

$$sup3(inf3(sup3(sup3(sup3(sup3(sup3(C(0,x),inf3(C(1,x),C(0,y))),$$

$$inf3(C(2,x),C(0,y))),inf3(C(1,x),C(1,y))),inf3(C(2,x),C(1,y)))),2),$$

$$sup3(inf3(C(1,x),C(2,y)),inf3(C(2,x),C(2,y)))).$$

Luego
$x^2y^2 + x^2y + 2 = \{[C_0(x) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_0(y)) \vee (C_1(x) \wedge C_1(y)) \vee$
$\vee (C_2(x) \wedge C_1(y))] \wedge e_1\} \vee (C_1(x) \wedge C_2(y)) \vee (C_2(x) \wedge C_2(y))$.

Polinomios con coeficientes en $F(3^2)$ y $L_{3,2}$

Cálculo del ínfimo

```
inf3 := proc(r,s)
local x, y;
    if r = 0 or s = 0 then inf3(r,s):=0
          else
             if r = 1 then inf3(r,s):=s
                   else
                         if s = 1 then inf3(r,s):=r
                               else
                                     x:=r;
                                     y:=s;
                                           if x = y then return x
                                                 else 'inf3(r,s)'
                                           end if
                         end if
             end if
    end if;
end proc:
```

```
inf32:= proc(x,y)
```

```
local infimo;
infimo:= [inf3(x[1],y[1]),inf3(x[2],y[2])];
infimo;
end proc:
```

Cálculo del Supremo

```
sup3 := proc(r,s)
local supremo, x, y;
    if r = 1 or s = 1 then sup3(r,s):=1
          else
             if r = 0 then sup3(r,s):=s
                   else
                         if r = 2 and s = 2 then sup3(r,s):=2
                               else
                                     x:=r;
                                     y:=s;
                                           if x = y then return x
                                                 else 'sup3(r,s)'
                                           end if
                         end if
             end if
    end if
end proc:
```

```
sup32:= proc(x,y)
local supremo;
supremo:= [sup3(x[1],y[1]),sup3(x[2],y[2])];
supremo;
end proc:
```

Cálculo de la negación

```
if r = 2 then neg3(r):= 2
    else
       if r = 1 then neg3(r):= 2
             else neg3(r):= 1
       end if
end if;
end proc:
```

```
neg32:= proc(x)
[neg3(x[1],x[2])];
end proc:
```

Cálculo de las constantes

```
e3 := proc(i)
```

```
    if i = 0 then e3(i):=0
          else
             if i = 1 then e3(i):=2
                   else
                         if i = 2 then e3(i):=1
                                  else return'e3(i)'
                         end if
             end if
    end if
end proc:

e32:=proc(x)
[e3(x[1],e3(x[2]))];
end proc:
```

Cálculo del operador T

```
T32:= proc(x)
[x[2],x[1]];
end proc:
```

Cálculo de los C_i32

```
C := proc(i,z)
local c;
if i = 0 then if z = 0 then c:=1
          elif z = 1 or z = 2 then c:=0
          elif z = sup3(x, y) then return 'inf3(C(0,x),C(0,y))'
          elif z = inf3(x, y) then return 'sup3(C(0,x),C(0,y))'
                         else return 'C(0,z)'
             end if
          else if i = 1 then if z = 2 then c:=1
             elif z = 0 or z = 1 then c:=0
             elif z = sup3(x, y) then return
                'sup3(sup3(inf3(C(1,x),C(0,y)),inf3(C(1,x),C(1,y))),inf3(C(0,x),C(1,y)))'
             elif z = inf3(x, y) then return
                'sup3(sup3(inf3(C(1,x),C(2,y)),inf3(C(1,x),C(1,y))),inf3(C(2,x),C(1,y)))'
                         else return 'C(1,z)'
             end if
          else if i = 2 then if z = 1 then c:=1
             elif z = 0 or z = 2 then c:=0
             elif z = sup3(x, y) then return 'sup3(C(0,x),C(0,y))'
             elif z = inf3(x, y) then return 'inf3(C(0,x),C(0,y))'
             else return 'C(2, z)'
             end if
             else return'C(i, z)'
```

end if;
end if;

Declaraciones para una biblioteca

$C(0, C(0, x)) := sup3(C(1, x), C(2, x));$
$C(0, C(1, x)) := sup3(C(0, x), C(2, x));$
$C(0, C(2, x)) := sup3(C(0, x), C(1, x));$
$C(1, C(0, x)) := 0;$
$C(1, C(1, x)) := 0;$
$C(1, C(2, x)) := 0;$
$C(2, C(0, x)) := C(0, x);$
$C(2, C(1, x)) := C(1, x);$
$C(2, C(2, x)) := C(2, x);$
$C(0, sup3(C(0, x), C(0, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(0, x), C(1, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(0, x), C(2, y))) := inf3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(0, x), C(0, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(0, x), C(1, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(0, x), C(2, y))) := sup3(sup3(C(1, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, sup3(C(1, x), C(0, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(1, x), C(1, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(1, x), C(2, y))) := inf3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(1, x), C(0, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(1, x), C(1, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(1, x), C(2, y))) := sup3(sup3(C(0, x), C(2, x)), sup3(C(0, y), C(1, y)));$
$C(0, sup3(C(2, x), C(0, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(1, y), C(2, y)));$
$C(0, sup3(C(2, x), C(1, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(2, y)));$
$C(0, sup3(C(2, x), C(2, y))) := inf3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(1, y)));$
$C(0, inf3(C(2, x), C(0, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(1, y), C(2, y)));$
$C(0, inf3(C(2, x), C(1, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(2, y)));$
$C(0, inf3(C(2, x), C(2, y))) := sup3(sup3(C(0, x), C(1, x)), sup3(C(0, y), C(1, y)));$
$C(1, sup3(C(0, x), C(0, y))) := 0;$
$C(1, sup3(C(0, x), C(1, y))) := 0;$
$C(1, sup3(C(0, x), C(2, y))) := 0;$
$C(1, inf3(C(0, x), C(0, y))) := 0;$
$C(1, inf3(C(0, x), C(1, y))) := 0;$
$C(1, inf3(C(0, x), C(2, y))) := 0;$
$C(1, sup3(C(1, x), C(0, y))) := 0;$
$C(1, sup3(C(1, x), C(1, y))) := 0;$
$C(1, sup3(C(1, x), C(2, y))) := 0;$
$C(1, inf3(C(1, x), C(0, y))) := 0;$
$C(1, inf3(C(1, x), C(1, y))) := 0;$

$C(1, inf3(C(1,x), C(2,y))) := 0;$
$C(1, sup3(C(2,x), C(0,y))) := 0;$
$C(1, sup3(C(2,x), C(1,y))) := 0;$
$C(1, sup3(C(2,x), C(2,y))) := 0;$
$C(1, inf3(C(2,x), C(0,y))) := 0;$
$C(1, inf3(C(2,x), C(1,y))) := 0;$
$C(1, inf3(C(2,x), C(2,y))) := 0;$
$C(2, sup3(C(0,x), C(0,y))) := sup3(C(0,x), C(0,y));$
$C(2, sup3(C(0,x), C(1,y))) := sup3(C(0,x), C(1,y));$
$C(2, sup3(C(0,x), C(2,y))) := sup3(C(0,x), C(2,y));$
$C(2, inf3(C(0,x), C(0,y))) := inf3(C(0,x), C(0,y));$
$C(2, inf3(C(0,x), C(1,y))) := inf3(C(0,x), C(1,y));$
$C(2, inf3(C(0,x), C(2,y))) := inf3(C(0,x), C(2,y));$
$C(2, sup3(C(1,x), C(0,y))) := sup3(C(1,x), C(0,y));$
$C(2, sup3(C(1,x), C(1,y))) := sup3(C(1,x), C(1,y));$
$C(2, sup3(C(1,x), C(2,y))) := sup3(C(1,x), C(2,y));$
$C(2, inf3(C(1,x), C(0,y))) := inf3(C(1,x), C(0,y));$
$C(2, inf3(C(1,x), C(1,y))) := inf3(C(1,x), C(1,y));$
$C(2, inf3(C(1,x), C(2,y))) := inf3(C(1,x), C(2,y));$
$C(2, sup3(C(2,x), C(0,y))) := sup3(C(2,x), C(0,y));$
$C(2, sup3(C(2,x), C(1,y))) := sup3(C(2,x), C(1,y));$
$C(2, sup3(C(2,x), C(2,y))) := sup3(C(2,x), C(2,y));$
$C(2, inf3(C(2,x), C(0,y))) := inf3(C(2,x), C(0,y));$
$C(2, inf3(C(2,x), C(1,y))) := inf3(C(2,x), C(1,y));$
$C(2, inf3(C(2,x), C(2,y))) := inf3(C(2,x), C(2,y));$
$C(0, sup3(C(1,x), C(2,x))) := C(0,x);$
$C(1, sup3(C(1,x), C(2,x))) := 0;$
$C(2, sup3(C(1,x), C(2,x))) := sup3(C(1,x), C(2,x));$
$C(0, sup3(C(1,y), C(2,y))) := C(0,y);$
$C(1, sup3(C(1,y), C(2,y))) := 0;$
$C(2, sup3(C(1,y), C(2,y))) := sup3(C(1,y), C(2,y));$

```
    c;
    end proc:

    C32:= proc(i,r)
    local c;
    c:=[C(i,r[1]),C(i,r[2])];
```

$C(0, C(0, x[1])) := sup3(C(1, x[1]), C(2, x[1]));$
$C(0, C(0, x[2])) := sup3(C(1, x[2]), C(2, x[2]));$
$C(0, C(1, x[1])) := sup3(C(0, x[1]), C(2, x[1]));$
$C(0, C(1, x[2])) := sup3(C(0, x[2]), C(2, x[2]));$
$C(0, C(2, x[1])) := sup3(C(0, x[1]), C(1, x[1]));$
$C(0, C(2, x[2])) := sup3(C(0, x[2]), C(1, x[2]));$

$C(1, C(0, x[1])) := 0;$
$C(1, C(0, x[2])) := 0;$
$C(1, C(1, x[1])) := 0;$
$C(1, C(1, x[2])) := 0;$
$C(1, C(2, x[1])) := 0;$
$C(1, C(2, x[2])) := 0;$
$C(2, C(0, x[1])) := C(0, x[1]);$
$C(2, C(0, x[2])) := C(0, x[2]);$
$C(2, C(1, x[1])) := C(1, x[1]);$
$C(2, C(1, x[2])) := C(1, x[2]);$
$C(2, C(2, x[1])) := C(2, x[1]);$
$C(2, C(2, x[1])) := C(2, x[1]);$
$C(0, sup3(x[1], y[1])) := inf3(C(0, x[1]), C(0, y[1]));$
$C(0, sup3(x[2], y[2])) := inf3(C(0, x[2]), C(0, y[2]));$
$C(0, inf3(x[1], y[1])) := sup3(C(0, x[1]), C(0, y[1]));$
$C(0, inf3(x[2], y[2])) := sup3(C(0, x[2]), C(0, y[2]));$
$C(1, sup3(x[1], y[1])) := sup3(sup3(inf3(C(0, x[1]), C(1, y[1])),$
$inf3(C(1, x[1]), C(0, y[1]))), inf3(C(1, x[1]), C(1, y[1])));$
$C(1, sup3(x[2], y[2])) := sup3(sup3(inf3(C(0, x[2]), C(1, y[2])),$
$inf3(C(1, x[2]), C(0, y[2]))), inf3(C(1, x[2]), C(1, y[2])));$
$C(1, inf3(x[1], y[1])) := sup3(sup3(inf3(C(1, x[1]), C(2, y[1])),$
$inf3(C(1, x[1]), C(1, y[1]))), inf3(C(2, x[1]), C(1, y[1])));$
$C(1, inf3(x[2], y[2])) := sup3(sup3(inf3(C(1, x[2]), C(2, y[2])),$
$inf3(C(1, x[2]), C(1, y[2]))), inf3(C(2, x[2]), C(1, y[2])));$
$C(2, sup3(x[1], y[1])) := sup3(C(2, x[1]), C(2, y[1]));$
$C(2, sup3(x[2], y[2])) := sup3(C(2, x[2]), C(2, y[2]));$
$C(2, inf3(x[1], y[1])) := inf3(C(2, x[1]), C(2, y[1]));$
$C(2, inf3(x[2], y[2])) := sup3(C(2, x[2]), C(2, y[2]));$
$C(0, sup3(C(0, x)[1], C(0, y)[1])) := inf3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(1, y[1]), C(2, y[1])));$
$C(0, sup3(C(0, x)[2], C(0, y)[2])) := inf3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(1, y[2]), C(2, y[2])));$
$C(0, sup3(C(0, x)[1], C(1, y)[1])) := inf3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(0, y[1]), C(2, y[1])));$
$C(0, sup3(C(0, x)[2], C(1, y)[2])) := inf3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(0, y[2]), C(2, y[2])));$
$C(0, sup3(C(0, x)[1], C(2, y)[1])) := inf3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(0, y[1]), C(1, y[1])));$
$C(0, sup3(C(0, x)[2], C(2, y)[2])) := inf3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(0, y[2]), C(1, y[2])));$
$C(0, inf3(C(0, x)[1], C(0, y)[1])) := sup3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(1, y[1]), C(2, y[1])));$
$C(0, inf3(C(0, x)[2], C(0, y)[2])) := sup3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(1, y[2]), C(2, y[2])));$
$C(0, inf3(C(0, x)[1], C(1, y)[1])) := sup3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(0, y[1]), C(2, y[1])));$
$C(0, inf3(C(0, x)[2], C(1, y)[2])) := sup3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(0, y[2]), C(2, y[2])));$
$C(0, inf3(C(0, x)[1], C(2, y)[1])) := sup3(sup3(C(1, x[1]), C(2, x[1])), sup3(C(0, y[1]), C(1, y)[1]));$
$C(0, inf3(C(0, x)[2], C(2, y)[2])) := sup3(sup3(C(1, x[2]), C(2, x[2])), sup3(C(0, y[2]), C(1, y)[2]));$
$C(0, sup3(C(1, x)[1], C(0, y)[1])) := inf3(sup3(C(0, x[1]), C(2, x[1])), sup3(C(1, y[1]), C(2, y)[1]));$
$C(0, sup3(C(1, x)[2], C(0, y)[2])) := inf3(sup3(C(0, x[2]), C(2, x[2])), sup3(C(1, y[2]), C(2, y)[2]));$
$C(0, sup3(C(1, x)[1], C(1, y)[1])) := inf3(sup3(C(0, x[1]), C(2, x[1])), sup3(C(0, y[1]), C(2, y)[1]));$

$C(0, sup3(C(1,x)[2], C(1,y)[2])) := inf3(sup3(C(0,x[2]), C(2,x[2])), sup3(C(0,y[2]), C(2,y)[2]));$
$C(0, sup3(C(1,x)[1], C(2,y)[1])) := inf3(sup3(C(0,x[1]), C(2,x[1])), sup3(C(0,y[1]), C(1,y)[1]));$
$C(0, sup3(C(1,x)[2]), C(2,y[2])) := inf3(sup3(C(0,x[2]), C(2,x[2])), sup3(C(0,y[2]), C(1,y[2])));$
$C(0, inf3(C(1,x)[1], C(0,y)[1])) := sup3(sup3(C(0,x[1]), C(2,x[1])), sup3(C(1,y[1]), C(2,y[1])));$
$C(0, inf3(C(1,x)[2], C(0,y)[2])) := sup3(sup3(C(0,x[2]), C(2,x[2])), sup3(C(1,y[2]), C(2,y[2])));$
$C(0, inf3(C(1,x)[1], C(1,y)[1])) := sup3(sup3(C(0,x[1]), C(2,x[1])), sup3(C(0,y[1]), C(2,y[1])));$
$C(0, inf3(C(1,x)[2], C(1,y)[2])) := sup3(sup3(C(0,x[2]), C(2,x[2])), sup3(C(0,y[2]), C(2,y[2])));$
$C(0, inf3(C(1,x)[1], C(2,y)[1])) := sup3(sup3(C(0,x[1]), C(2,x[1])), sup3(C(0,y[1]), C(1,y[1])));$
$C(0, inf3(C(1,x)[2], C(2,y)[2])) := sup3(sup3(C(0,x[2]), C(2,x[2])), sup3(C(0,y[2]), C(1,y[2])));$
$C(0, sup3(C(2,x)[1], C(0,y)[1])) := inf3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(1,y[1]), C(2,y[1])));$
$C(0, sup3(C(2,x)[2], C(0,y)[2])) := inf3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(1,y[2]), C(2,y[2])));$
$C(0, sup3(C(2,x)[1], C(1,y)[1])) := inf3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(0,y[1]), C(2,y[1])));$
$C(0, sup3(C(2,x)[2], C(1,y)[2])) := inf3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(0,y[2]), C(2,y[2])));$
$C(0, sup3(C(2,x)[1], C(2,y)[1])) := inf3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(0,y[1]), C(1,y[1])));$
$C(0, sup3(C(2,x)[2], C(2,y)[2])) := inf3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(0,y[2]), C(1,y[2])));$
$C(0, inf3(C(2,x)[1], C(0,y)[1])) := sup3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(1,y[1]), C(2,y[1])));$
$C(0, inf3(C(2,x)[2], C(0,y)[2])) := sup3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(1,y[2]), C(2,y[2])));$
$C(0, inf3(C(2,x)[1], C(1,y)[1])) := sup3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(0,y[1]), C(2,y[1])));$
$C(0, inf3(C(2,x)[2], C(1,y)[2])) := sup3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(0,y[2]), C(2,y[2])));$
$C(0, inf3(C(2,x)[1], C(2,y)[1])) := sup3(sup3(C(0,x[1]), C(1,x[1])), sup3(C(0,y[1]), C(1,y[1])));$
$C(0, inf3(C(2,x)[2], C(2,y)[2])) := sup3(sup3(C(0,x[2]), C(1,x[2])), sup3(C(0,y[2]), C(1,y[2])));$
$C(1, (sup3(inf3(C(2,x[1]), 2), C(1,x[1]))) := C(2,x[1]);$
$C(1, (sup3(inf3(C(2,x[2]), 2), C(1,x[2]))) := C(2,x[2]);$
$C(2, (sup3(inf3(C(2,x[1]), 2), C(1,x[1]))) := C(1,x[1]);$
$C(2, (sup3(inf3(C(2,x[2]), 2), C(1,x[2]))) := C(1,x[2]);$
$sup3(sup3(C(0,x[1]), C(1,x[1])), C(2,x[1]) := 1;$
$sup3(sup3(C(0,x[2]), C(1,x[2])), C(2,x[2]) := 1;$
$inf3(C(0,x[1]), C(1,x[1])) := 0;$
$inf3(C(0,x[2]), C(1,x[2])) := 0;$
$inf3(C(0,x[1]), C(2,x[1])) := 0;$
$inf3(C(0,x[2]), C(2,x[2])) := 0;$
$inf3(C(1,x[1]), C(0,x[1])) := 0;$
$inf3(C(1,x[2]), C(0,x[2])) := 0;$
$inf3(C(1,x[1]), C(2,x[1])) := 0;$
$inf3(C(1,x[2]), C(2,x[2])) := 0;$
$inf3(C(2,x[1]), C(0,x[1])) := 0;$
$inf3(C(2,x[2]), C(0,x[2])) := 0;$
$inf3(C(2,x[1]), C(1,x[1])) := 0;$
$inf3(C(2,x[2]), C(1,x[2])) := 0;$
$inf3(C(0,y[1]), C(1,y[1])) := 0;$
$inf3(C(0,y[2]), C(1,y[2])) := 0;$
$inf3(C(0,y[1]), C(2,y[1])) := 0;$
$inf3(C(0,y[2]), C(2,y[2])) := 0;$

$inf3(C(1,y[1]),C(0,y[1])) := 0;$
$inf3(C(1,y[2]),C(0,y[2])) := 0;$
$inf3(C(1,y[1]),C(2,y[1])) := 0;$
$inf3(C(1,y[2]),C(2,y[2])) := 0;$
$inf3(C(2,y[1]),C(0,y[1])) := 0;$
$inf3(C(2,y[2]),C(0,y[2])) := 0;$
$inf3(C(2,y[1]),C(1,y[1])) := 0;$
$inf3(C(2,y[2]),C(1,y[2])) := 0;$
$C(0,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),2),$
$sup3(inf3(C(1,x[2]),C(1,x[1])),inf3(C(2,x[2]),C(2,x[1])))) := sup3(C(0,x[1]),C(0,x[2]));$
$C(1,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),2),$
$sup3(inf3(C(1,x[2]),C(1,x[1])),inf3(C(2,x[2]),C(1,x[1])))) :=$
$sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1])));$
$C(2,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),2),$
$sup3(inf3(C(1,x[2]),C(1,x[1])),inf3(C(2,x[2]),C(2,x[1])))) :=$
$sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2])));$
$C(0,sup3(inf3(sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),$
$C(0,x[1]))),inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),sup3$
$(C(1,x[1]),C(2,x[1])))),2),sup3(inf3(sup3(C(0,x[1]),C(0,x[2])),sup3(C(1,x[1]),C(2,x[1]))),$
$inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),C(0,x[1])))) :=$
$sup3(sup3(C(0,x[1]),inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2])));$
$C(1,sup3(inf3(sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),$
$C(0,x[1]))),inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),sup3$
$(C(1,x[1]),C(2,x[1])))),2),sup3(inf3(sup3(C(0,x[1]),C(0,x[2])),sup3(C(1,x[1]),C(2,x[1]))),$
$inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),C(0,x[1])))) :=$
$sup3(inf3(C(1,x[1]),C(1,x[2]))),inf3(C(2,x[1]),C(2,x[2])));$
$C(2,sup3(inf3(sup3(inf3(sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1]))),$
$C(0,x[1]))),inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),sup3$
$(C(1,x[1]),C(2,x[1])))),2),sup3(inf3(sup3(C(0,x[1]),C(0,x[2])),sup3(C(1,x[1]),C(2,x[1]))),$
$inf3(sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))),C(0,x[1])))) :=$
$sup3(inf3(C(0,x[2]),C(1,x[1]))),inf3(C(0,x[2]),C(2,x[1])));$
$C(0,sup3(inf3(inf3(sup3(sup3(C(0,x[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1])))),2),$
$inf3(sup3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,x[2]),C(2,x[1]))),sup3(C(0,x[1]),C(0,x[2])))) :=$
$= sup3(C(0,x[1]),sup3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,x[1]),C(2,x[2]))));$
$C(1,sup3(inf3(inf3(sup3(sup3(C(0,x[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1])))),2),$
$inf3(sup3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,x[2]),C(2,x[1]))),sup3(C(0,x[1]),C(0,x[2])))) :=$
$= sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1])));$
$C(2,sup3(inf3(inf3(sup3(sup3(C(0,x[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),sup3(inf3(C(1,x[2]),C(2,x[1])),inf3(C(2,x[2]),C(1,x[1])))),2),$
$inf3(sup3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,x[2]),C(2,x[1]))),sup3(C(0,x[1]),C(0,x[2])))) :=$
$= sup3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,x[2]),C(2,x[1])));$

$C(0, inf3(sup3(C(2, x[2]), (C(1, x[2])), 2)) := C(0, x[2]);$
$C(1, inf3(sup3(C(2, x[2]), (C(1, x[2])), 2)) := sup3(C(2, x[2]), C(1, x[2]));$
$C(2, inf3(sup3(C(2, x[2]), (C(1, x[2])), 2)) := 0;$
$inf3(sup3(C(0, x[1]), sup3(inf3(C(1, x[1]), C(1, x[2])), inf3(C(2, x[1]), C(2, x[2])))),$
$sup3(C(2, x[2]), C(1, x[2]))) := sup3(sup3(sup3(inf3(C(0, x[1]), C(2, x[2])),$
$inf3(C(0, x[1]), C(1, x[2]))), inf3(C(1, x[1]), C(1, x[2]))), inf3(C(2, x[1]), C(2, x[2])));$
$sup3(inf3(sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1]))),$
$sup3(C(2, x[2]), C(1, x[2]))), C(0, x[2])) := sup3(sup3(C(0, x[2]), inf3(C(1, x[2]), C(2, x[1]))),$
$inf3(C(2, x[2]), C(2, x[1])));$
$inf3(sup3(C(0, x[2]), sup3(inf3(C(1, x[2]), C(1, x[1])),$
$inf3(C(2, x[2]), C(2, x[1])))), sup3(C(2, x[1]), C(1, x[1]))) :=$
$sup3(sup3(sup3(inf3(C(0, x[2]), C(2, x[1])), inf3(C(0, x[2]), C(1, x[1]))),$
$inf3(C(1, x[2]), C(1, x[1]))), inf3(C(2, x[2]), C(2, x[1])));$
$sup3(inf3(sup3(inf3(C(1, x[1]), C(2, x[2])), inf3(C(2, x[1]), C(1, x[2]))),$
$sup3(C(2, x[1]), C(1, x[1]))), C(0, x[1])) :=$
$sup3(sup3(C(0, x[1]), inf3(C(1, x[1]), C(2, x[2]))), inf3(C(2, x[1]), C(1, x[2])));$
$inf3(sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1]))), C(0, x[2])) := 0;$
$inf3(sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1]))),$
$sup3(C(2, x[2]), C(1, x[2]))) := sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1])));$
$inf3(sup3(inf3(C(0, x[2]), C(1, x[1])), inf3(C(0, x[2]), C(2, x[1]))), C(0, x[2])) :=$
$sup3(inf3(C(0, x[2]), C(1, x[1])), inf3(C(0, x[2]), C(2, x[1])));$
$C(0, sup3(inf3(sup3(sup3(sup3(inf3(C(0, x[1]), C(2, x[2])), inf3(C(0, x[1]), C(1, x[2]))),$
$inf3(C(1, x[1]), C(1, x[2]))), inf3(C(2, x[1]), C(2, x[2]))), 2),$
$sup3(sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1]))),$
$sup3(inf3(C(0, x[2]), C(1, x[1])), inf3(C(0, x[2]), C(2, x[1])))))) := inf3(C(0, x[1]), C(0, x[2]));$
$C(1, sup3(inf3(sup3(sup3(sup3(inf3(C(0, x[1]), C(2, x[2])), inf3(C(0, x[1]), C(1, x[2]))),$
$inf3(C(1, x[1]), C(1, x[2]))), inf3(C(2, x[1]), C(2, x[2]))), 2),$
$sup3(sup3(inf3(C(1, x[2]), C(2, x[1])), inf3(C(2, x[2]), C(1, x[1]))),$
$sup3(inf3(C(0, x[2]), C(1, x[1])), inf3(C(0, x[2]), C(2, x[1])))))) :=$
$sup3(sup3(sup3(inf3(C(0, x[1]), C(2, x[2])), inf3(C(0, x[1]), C(1, x[2]))),$
$inf3(C(1, x[1]), C(1, x[2]))), inf3(C(2, x[1]), C(2, x[2])));$
$C(0, sup3(inf3(sup3(inf3(C(1, x[2]), C(2, y[1])), inf3(C(2, x[2]), C(1, y[1]))), 2),$
$sup3(inf3(C(1, x[2]), C(1, y[1])), inf3(C(2, x[2]), C(2, y[1]))))) := sup3(C(0, x[2]), C(0, y[1]));$
$C(1, sup3(inf3(sup3(inf3(C(1, x[2]), C(2, y[1])), inf3(C(2, x[2]), C(1, y[1]))), 2),$
$sup3(inf3(C(1, x[2]), C(1, y[1])), inf3(C(2, x[2]), C(2, y[1])))) :=$
$sup3(inf3(C(1, x[2]), C(2, y[1])), inf3(C(2, x[2]), C(1, y[1])));$
$C(2, sup3(inf3(sup3(inf3(C(1, x[2]), C(2, y[1])), inf3(C(2, x[2]), C(1, y[1]))), 2),$
$sup3(inf3(C(1, x[2]), C(1, y[1])), inf3(C(2, x[2]), C(2, y[1])))) :=$
$sup3(inf3(C(1, y[1]), C(1, x[2])), inf3(C(2, y[1]), C(2, x[2])));$
$C(0, sup3(inf3(sup3(inf3(C(1, x[1]), C(2, y[1])), inf3(C(2, x[1]), C(1, y[1]))), 2),$
$sup3(inf3(C(1, x[1]), C(1, y[1])), inf3(C(2, x[1]), C(2, y[1]))))) := sup3(C(0, x[1]), C(0, y[1]));$
$C(1, sup3(inf3(sup3(inf3(C(1, x[1]), C(2, y[1])), inf3(C(2, x[1]), C(1, y[1]))), 2),$
$sup3(inf3(C(1, x[1]), C(1, y[1])), inf3(C(2, x[1]), C(2, y[1])))) :=$

$sup3(inf3(C(1,x[1]),C(2,y[1])),inf3(C(2,x[1]),C(1,y[1])));$
$C(2,sup3(inf3(sup3(inf3(C(1,x[1]),C(2,y[1])),inf3(C(2,x[1]),C(1,y[1]))),2),$
$sup3(inf3(C(1,x[1]),C(1,y[1])),inf3(C(2,x[1]),C(2,y[1])))) :=$
$sup3(inf3(C(1,x[1]),C(1,y[1])),inf3(C(2,x[1]),C(2,y[1])));$
$C(0,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))) := sup3(C(0,x[2]),C(0,y[2]));$
$C(1,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))) :=$
$sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2])));$
$C(2,sup3(inf3(sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))) :=$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])));$
$C(0,sup3(inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))) := sup3(C(0,x[1]),C(0,y[2]));$
$C(1,sup3(inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))) :=$
$sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2])));$
$C(2,sup3(inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),2),$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))) :=$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])));$
$C(0,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(2,y[1])),$
$inf3(C(2,x[1]),C(1,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))),$
$sup3(C(0,x[1]),C(0,y[1])))),inf3(sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),$
$sup3(inf3(C(1,x[1]),C(1,y[1])),inf3(C(2,x[1]),C(2,y[1])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(1,y[1])),$
$inf3(C(2,x[1]),C(2,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))),$
$sup3(inf3(C(1,x[1]),C(2,y[1])),inf3(C(2,x[1]),C(1,y[1])))),inf3(sup3(inf3($
$C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),sup3(C(0,x[1]),C(0,y[1]))))) :=$
$sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2]))),$
$inf3(C(0,x[1]),C(0,x[2])));$
$C(1,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(2,y[1])),$
$inf3(C(2,x[1]),C(1,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))),$
$sup3(C(0,x[1]),C(0,y[1])))),inf3(sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),$
$sup3(inf3(C(1,x[1]),C(1,y[1])),inf3(C(2,x[1]),C(2,y[1])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(1,y[1])),$
$inf3(C(2,x[1]),C(2,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),$
$inf3(C(2,x[2]),C(1,y[1]))),sup3(inf3(C(1,x[1]),C(2,y[1])),inf3(C(2,x[1]),C(1,y[1]))))),$
$inf3(sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),$
$sup3(C(0,x[1]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3$
$(C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1])));$
$C(2,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(2,y[1])),$

$inf3(C(2,x[1]),C(1,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))),$
$sup3(C(0,x[1]),C(0,y[1])))),inf3(sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),$
$sup3(inf3(C(1,x[1]),C(1,y[1])),inf3(C(2,x[1]),C(2,y[1])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[2]),C(0,y[1])),sup3(inf3(C(1,x[1]),C(1,y[1])),$
$inf3(C(2,x[1]),C(2,y[1])))),inf3(sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))),$
$sup3(inf3(C(1,x[1]),C(2,y[1])),inf3(C(2,x[1]),C(1,y[1])))),$
$inf3(sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2]))),$
$sup3(C(0,x[1]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1])));$
$C(0,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(2,y[2])),$
$inf3(C(2,x[2]),C(1,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(C(0,x[2]),C(0,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(1,y[2])),$
$inf3(C(2,x[2]),C(2,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2])))),$
$inf3(sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),$
$sup3(C(0,x[2]),C(0,y[2])))))) := sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),$
$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2])));$
$C(1,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(2,y[2])),$
$inf3(C(2,x[2]),C(1,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(C(0,x[2]),C(0,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(1,y[2])),$
$inf3(C(2,x[2]),C(2,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2])))),inf3(sup3(inf3($
$C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),sup3(C(0,x[2]),C(0,y[2]))))) :=$
$sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),$
$inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),$
$inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2])));$
$C(2,sup3(inf3(sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(2,y[2])),$
$inf3(C(2,x[2]),C(1,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(C(0,x[2]),C(0,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),$
$sup3(inf3(C(1,x[2]),C(1,y[2])),inf3(C(2,x[2]),C(2,y[2])))),2),$
$sup3(sup3(inf3(sup3(C(0,x[1]),C(0,y[2])),sup3(inf3(C(1,x[2]),C(1,y[2])),$
$inf3(C(2,x[2]),C(2,y[2])))),inf3(sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))),$
$sup3(inf3(C(1,x[2]),C(2,y[2])),inf3(C(2,x[2]),C(1,y[2])))),inf3(sup3(inf3($
$C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))),sup3(C(0,x[2]),C(0,y[2]))))) :=$
$sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(1,y[2])),$

$inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),$
$inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2])));$
$C(0,sup3(inf3(sup3(inf3(C(2,x[2]),C(2,y[2])),inf3(C(1,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(2,x[2]),C(1,y[2])),inf3(C(1,x[2]),C(2,y[2]))))) := sup3(C(0,x[2]),C(0,y[2]));$
$C(1,sup3(inf3(sup3(inf3(C(2,x[2]),C(2,y[2])),inf3(C(1,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(2,x[2]),C(1,y[2])),inf3(C(1,x[2]),C(2,y[2]))))) :=$
$sup3(inf3(C(2,x[2]),C(2,y[2])),inf3(C(1,x[2]),C(1,y[2])));$
$C(2,sup3(inf3(sup3(inf3(C(2,x[2]),C(2,y[2])),inf3(C(1,x[2]),C(1,y[2]))),2),$
$sup3(inf3(C(2,x[2]),C(1,y[2])),inf3(C(1,x[2]),C(2,y[2]))))) :=$
$sup3(inf3(C(2,x[2]),C(1,y[2])),inf3(C(1,x[2]),C(2,y[2])));$
$C(0,sup3(inf3(sup3(inf3(C(2,x[1]),C(2,y[1])),inf3(C(1,x[1]),C(1,y[1]))),2),$
$sup3(inf3(C(2,x[1]),C(1,y[1])),inf3(C(1,x[1]),C(2,y[1]))))) := sup3(C(0,x[1]),C(0,y[1]));$
$C(1,sup3(inf3(sup3(inf3(C(2,x[1]),C(2,y[1])),inf3(C(1,x[1]),C(1,y[1]))),2),$
$sup3(inf3(C(2,x[1]),C(1,y[1])),inf3(C(1,x[1]),C(2,y[1]))))) :=$
$sup3(inf3(C(2,x[1]),C(2,y[1])),inf3(C(1,x[1]),C(1,y[1])));$
$C(2,sup3(inf3(sup3(inf3(C(2,x[1]),C(2,y[1])),inf3(C(1,x[1]),C(1,y[1]))),2),$
$sup3(inf3(C(2,x[1]),C(1,y[1])),inf3(C(1,x[1]),C(2,y[1]))))) :=$
$sup3(inf3(C(2,x[1]),C(1,y[1])),inf3(C(1,x[1]),C(2,y[1])));$
$C(0,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$
$inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),2),$
$sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),$
$inf3(C(2,y[1]),C(2,x[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1])))),$
$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(1,y[1])),$
$inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),sup3(C(0,x[2]),C(0,y[1])))))) :=$
$sup3(sup3(sup3(sup3(sup3(C(0,y[1]),inf3(C(0,x[1]),C(0,x[2]))),inf3(inf3($
$C(2,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),$

$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1])))$, $inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1])))$;
$C(0,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),$
$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$
$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),$
$C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),inf3(inf3($
$C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3($
$C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3($
$C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))))),2),sup3(sup3(inf3(sup3(sup3(sup3($
$C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3($
$inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2])))))),inf3(sup3(sup3(sup3(sup3(sup3($
$inf3(inf3(C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(C(0,y[2]),$
$inf3(C(0,x[1]),C(0,x[2]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[2]))),inf3(inf3($
$C(1,x[1]),C(1,x[2])),C(2,y[2]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[2])),inf3($
$inf3(C(2,x[1]),C(2,x[2])),C(2,y[2])))$;
$C(1,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$
$inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),$
$C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3($
$C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(1,y[1]),C(1,x[2])),$
$inf3(C(2,y[1]),C(2,x[2])))))),2),sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),$
$inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),$
$sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1])))))),inf3(sup3(sup3(sup3(sup3(sup3($
$inf3(inf3(C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$

$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(C(0,x[2]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(2,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1])));$
$C(1,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),$
$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$
$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),2),sup3(sup3(inf3(sup3($
$sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),$
$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(1,y[2])),$
$inf3(C(2,x[1]),C(2,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3($
$inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3($
$sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$
$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$
$sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$
$inf3(inf3(C(1,x[2]),C(2,x[1])),C(1,y[2]))),$
$inf3(inf3(C(2,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2])));$
$C(2,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$
$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$
$inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$
$sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3($
$inf3(C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$

$$sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),2),sup3(sup3(inf3($$
$$sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2])))),inf3(C(1,x[1]),C(2,x[2]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),$$
$$inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$$
$$inf3(C(2,x[2]),C(1,y[1])))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[2]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(2,x[1]),C(1,x[2])),C(1,y[1])),inf3(inf3(C(1,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1])));$$
$$C(2,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1])))),$$
$$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),2),sup3(sup3(inf3(sup3($$
$$sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1])))),inf3(C(1,x[2]),C(2,x[1]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),$$
$$inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(2,x[2]),C(1,x[1])),C(1,y[2])),inf3(inf3(C(1,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2])));$$
$$C(0,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2])))),$$
$$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3($$

$$inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),2),sup3($$
$$sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),$$
$$inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$sup3(sup3(inf3(C(0,x[1]),C(0,x[2])),inf3(C(0,x[1]),C(0,y[1]))),inf3(C(0,y[1]),C(0,y[2]))),$$
$$inf3(inf3(C(1,x[1]),C(2,x[2])),C(0,y[2]))),inf3(inf3(C(2,x[1]),C(1,x[2])),C(0,y[2]))),$$
$$inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$$
$$inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$
$$inf3(C(2,y[1]),C(2,y[2]))));$$
$$C(0,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),$$
$$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$$
$$inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),2),sup3(sup3(inf3(sup3($$
$$sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),$$
$$inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),$$

$$inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$$
$$inf3(C(2,x[2]),C(1,y[1])))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[2]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$sup3(sup3(sup3(inf3(C(0,x[1]),C(0,x[2])),inf3(C(0,x[2]),C(0,y[2]))),$$
$$inf3(C(0,y[1]),C(0,y[2]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(0,y[1]))),$$
$$inf3(inf3(C(2,x[2]),C(1,x[1])),C(0,y[1]))),inf3(inf3(C(2,x[2]),C(0,x[1])),$$
$$inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(2,y[1])))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[2]),C(0,x[1])),$$
$$inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,y[2]))));$$
$$C(1,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$$
$$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),2),sup3(sup3(inf3(sup3($$
$$sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),$$
$$inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,y[1])),C(2,y[2])),$$
$$inf3(inf3(C(2,x[1]),C(0,y[1])),C(1,y[2]))),inf3(inf3(C(2,x[1]),C(1,x[2])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[1]),C(2,x[2])),C(2,y[2]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$$
$$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(1,y[2])))),$$

$$inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(2,y[2]))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$
$$inf3(C(2,y[1]),C(1,y[2]))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(2,y[2])))));$$
$$C(1,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),$$
$$inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$$
$$inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),2),sup3(sup3(inf3($$
$$sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),$$
$$inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),$$
$$inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),$$
$$inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),$$
$$inf3(C(2,x[2]),C(1,y[1])))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),$$
$$sup3(C(0,x[2]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,y[2])),C(2,y[1])),inf3(inf3($$
$$C(2,x[2]),C(0,y[2])),C(1,y[1]))),inf3(inf3(C(2,x[2]),C(1,x[1])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[2]),C(2,x[1])),C(2,y[1]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$$
$$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$
$$inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(2,y[1]))));$$
$$C(2,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),$$
$$inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(2,y[2])),$$
$$inf3(C(2,x[1]),C(1,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),$$
$$sup3(C(0,x[1]),C(0,y[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),$$

$$sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))))),2),sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[1]),inf3(C(2,x[1]),C(1,x[2]))),inf3(C(1,x[1]),C(2,x[2]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[1]),C(1,y[2])),inf3(C(2,x[1]),C(2,y[2]))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(2,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(1,x[1]),C(2,y[2])),inf3(C(2,x[1]),C(1,y[2]))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),C(1,y[1])),inf3(inf3(C(2,x[1]),C(0,x[2])),C(2,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),sup3(C(0,x[1]),C(0,y[2])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,y[1])),C(1,y[2])),inf3(inf3(C(2,x[1]),C(0,y[1])),C(2,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(0,x[2])),C(2,y[1]))),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1])));$$

$$C(2,sup3(inf3(sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1])))),inf3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2])))),sup3(C(0,x[2]),C(0,y[1])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(1,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(2,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),2),sup3(sup3(inf3(sup3(sup3(sup3(C(0,y[2]),inf3(C(2,x[2]),C(1,x[1]))),inf3(C(1,x[2]),C(2,x[1]))),inf3(C(0,x[1]),C(0,x[2]))),sup3(inf3(C(1,y[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,x[2])))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2])))),sup3(inf3(C(1,x[2]),C(2,y[1])),inf3(C(2,x[2]),C(1,y[1]))))),inf3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),C(2,y[2])),inf3(inf3(C(2,x[2]),C(0,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(2,x[2]),C(2,x[1])),C(2,y[2])))),sup3(C(0,x[2]),C(0,y[1])))))) := sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$

$$sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,y[2])),C(1,y[1])),inf3(inf3(C(2,x[2]),C(0,y[2])),C(2,y[1]))),inf3(inf3(C(2,x[2]),C(1,x[1])),C(2,y[1]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(1,y[1]))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(2,x[2]),C(2,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2])));$$

$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(C(0,x[1]),C(0,x[2])),inf3(C(0,x[1]),C(0,y[1]))),inf3(C(0,y[1]),C(0,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(0,y[2]))),inf3(inf3(C(2,x[1]),C(1,x[2])),C(0,y[2]))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,y[2])))),sup3(inf3(C(2,x[2]),C(2,y[2])),inf3(C(1,x[2]),C(1,y[2])))) :=$$
$$sup3(sup3(sup3(inf3(inf3(C(0,x[1]),C(2,x[2])),inf3(C(0,y[1]),C(2,y[2]))),inf3(inf3(C(0,x[1]),C(1,x[2])),inf3(C(0,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2]))));$$

$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(C(0,x[1]),C(0,x[2])),inf3(C(0,x[2]),C(0,y[2]))),inf3(C(0,y[1]),C(0,y[2]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(0,y[1]))),inf3(inf3(C(2,x[2]),C(1,x[1])),C(0,y[1]))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,y[2])))),sup3(inf3(C(2,x[1]),C(2,y[1])),inf3(C(1,x[1]),C(1,y[1])))) :=$$
$$sup3(sup3(sup3(inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(0,y[2]),C(2,y[1]))),inf3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2]))));$$

$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,y[1])),C(2,y[2])),inf3(inf3(C(2,x[1]),C(0,y[1])),C(1,y[2]))),inf3(inf3(C(2,x[1]),C(1,x[2])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(2,y[2]))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(0,x[2]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(2,y[2])))),sup3(C(0,x[2]),C(0,y[2]))) :=$$

$sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),$
$inf3(C(0,y[1]),C(2,y[2]))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(0,y[1]),C(1,y[2])))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),$
$inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(0,y[2])))),$
$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$
$inf3(C(2,y[1]),C(2,y[2]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,y[2])),C(2,y[1])),inf3(inf3(C(2,x[2]),C(0,y[2])),C(1,y[1]))),$
$inf3(inf3(C(2,x[2]),C(1,x[1])),C(1,y[1]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(2,y[1]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(0,y[1])))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[2]),C(0,y[1])))),$
$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$
$inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(1,y[1])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(2,y[1])))),sup3(C(0,x[1]),C(0,y[1]))) :=$
$sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(0,y[2]),C(2,y[1]))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(0,y[2]),C(1,y[1])))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(0,y[1])))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[2]),C(0,y[1])))),$
$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$
$inf3(C(2,y[2]),C(2,y[1]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,y[1])),C(1,y[2])),inf3(inf3(C(2,x[1]),C(0,y[1])),C(2,y[2]))),$
$inf3(inf3(C(2,x[1]),C(1,x[2])),C(2,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(1,y[2]))),$
$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$
$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(2,y[2])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),$
$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(0,y[2])))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$
$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),$
$inf3(inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),sup3(inf3(C(2,x[2]),C(1,y[2])),$
$inf3(C(1,x[2]),C(2,y[2])))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(2,x[1]),C(1,x[2])),$
$C(2,y[2])),inf3(inf3(C(1,x[1]),C(2,x[2])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(1,y[2])))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(0,x[1]),C(2,x[2])),$
$inf3(C(2,y[1]),C(1,y[2]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($
$sup3(inf3(inf3(C(1,x[2]),C(0,y[2])),C(1,y[1])),inf3(inf3(C(2,x[2]),C(0,y[2])),C(2,y[1]))),$

$$inf3(inf3(C(2,x[2]),C(1,x[1])),C(2,y[1]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[2]),C(2,y[1])))),$$
$$inf3(inf3(C(2,x[2]),C(2,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),$$
$$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(0,y[1])))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[2]),C(2,x[1])),C(2,y[2]))),sup3(inf3(C(2,x[1]),C(1,y[1])),$$
$$inf3(C(1,x[1]),C(2,y[1])))) := sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(2,x[2]),C(1,x[1])),C(2,y[1])),inf3(inf3(C(1,x[2]),C(2,x[1])),C(1,y[1]))),$$
$$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(1,y[2]),C(2,y[1])))),$$
$$inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(2,y[2]),C(1,y[1]))));$$
$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$inf3(C(0,x[1]),C(0,x[2])),inf3(C(0,x[1]),C(0,y[1]))),inf3(C(0,y[1]),C(0,y[2]))),$$
$$inf3(inf3(C(1,x[1]),C(2,x[2])),C(0,y[2]))),inf3(inf3(C(2,x[1]),C(1,x[2])),C(0,y[2]))),$$
$$inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$$
$$inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$
$$inf3(C(2,y[1]),C(2,y[2])))),sup3(inf3(C(2,x[2]),C(1,y[2])),inf3(C(1,x[2]),C(2,y[2])))) :=$$
$$sup3(sup3(sup3(inf3(inf3(C(0,x[1]),C(2,x[2])),inf3(C(0,y[1]),C(1,y[2]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),inf3(C(0,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,y[2]))));$$
$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3($$
$$C(0,x[1]),C(0,x[2])),inf3(C(0,x[2]),C(0,y[2]))),inf3(C(0,y[1]),C(0,y[2]))),$$
$$inf3(inf3(C(1,x[2]),C(2,x[1])),C(0,y[1]))),inf3(inf3(C(2,x[2]),C(1,x[1])),C(0,y[1]))),$$
$$inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(1,y[1])))),$$
$$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$$
$$inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(1,y[2])))),$$
$$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$
$$inf3(C(2,y[1]),C(2,y[2])))),sup3(inf3(C(2,x[1]),C(1,y[1])),inf3(C(1,x[1]),C(2,y[1])))) :=$$
$$sup3(sup3(sup3(inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(0,y[2]),C(1,y[1]))),$$
$$inf3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(0,y[2]),C(2,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$$
$$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(2,y[2]))));$$
$$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($$
$$C(1,x[1]),C(0,y[1])),C(2,y[2])),inf3(inf3(C(2,x[1]),C(0,y[1])),C(1,y[2]))),$$
$$inf3(inf3(C(2,x[1]),C(1,x[2])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(2,y[2]))),$$
$$inf3(inf3(C(0,x[1]),C(1,x[2])),C(2,y[1]))),inf3(inf3(C(1,x[1]),C(0,x[2])),$$
$$inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),$$
$$inf3(inf3(C(0,x[1]),C(2,x[2])),C(1,y[1]))),inf3(inf3(C(1,x[1]),C(1,x[2])),$$

$inf3(C(1,y[1]),C(0,y[2]))))$, $inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(0,y[2])))$,
$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(1,y[2])))$, $inf3(inf3(C(2,x[1]),C(0,x[2]))$,
$inf3(C(2,y[1]),C(2,y[2])))$, $inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(1,y[2])))$,
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(2,y[2])))$, $sup3(inf3(C(2,x[2]),C(2,y[2]))$,
$inf3(C(1,x[2]),C(1,y[2])))) := sup3(sup3(inf3(sup3(sup3(inf3(inf3($
$C(2,x[1]),C(1,x[2])),C(1,y[2])),inf3(inf3(C(1,x[1]),C(2,x[2])),C(2,y[2]))),inf3($
$inf3(C(0,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(0,x[1]),C(2,x[2])),$
$inf3(C(1,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(1,y[2])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(2,y[2]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3($
$C(1,x[2]),C(0,y[2])),C(2,y[1])),inf3(inf3(C(2,x[2]),C(0,y[2])),C(1,y[1]))),$
$inf3(inf3(C(2,x[2]),C(1,x[1])),C(1,y[1]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(2,y[1]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),C(2,y[2]))),inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(0,y[1])))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),C(1,y[2]))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[2]),C(0,y[1])))),$
$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$
$inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(1,y[1])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(2,y[1])))),sup3(inf3(C(2,x[1]),C(2,y[1])),$
$inf3(C(1,x[1]),C(1,y[1])))) := sup3(sup3(inf3(sup3(sup3(inf3(inf3($
$C(2,x[2]),C(1,x[1])),C(1,y[1])),inf3(inf3(C(1,x[2]),C(2,x[1])),C(2,y[1]))),$
$inf3(inf3(C(0,x[2]),C(1,x[1])),inf3(C(2,y[2]),C(1,y[1])))),$
$inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(1,y[2]),C(2,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(2,y[1]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($
$sup3(inf3(inf3(C(1,x[1]),C(0,y[1])),C(1,y[2])),inf3(inf3(C(2,x[1]),C(0,y[1])),C(2,y[2]))),$
$inf3(inf3(C(2,x[1]),C(1,x[2])),C(2,y[2]))),inf3(inf3(C(1,x[1]),C(2,x[2])),C(1,y[2]))),$
$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$
$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(2,y[2])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(2,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),$
$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(0,y[2])))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$
$inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(1,x[2])),C(1,y[1]))),inf3($
$inf3(C(0,x[1]),C(2,x[2])),C(2,y[1]))),sup3(C(0,x[2]),C(0,y[2]))) :=$
$sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[1]),C(0,x[2])),$
$inf3(C(0,y[1]),C(1,y[2]))),inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(0,y[1]),C(2,y[2])))),$
$inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[1]),C(0,x[2])),$
$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(0,x[2])),inf3(C(1,y[1]),C(0,y[2])))),$
$inf3(inf3(C(2,x[1]),C(0,x[2])),inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),$
$inf3(C(2,y[1]),C(0,y[2])))),inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[1]),C(0,y[2])))),$
$inf3(inf3(C(0,x[1]),C(1,x[2])),inf3(C(1,y[1]),C(0,y[2])))),inf3(inf3(C(0,x[1]),C(2,x[2])),$
$inf3(C(2,y[1]),C(0,y[2]))));$
$inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(inf3(}$

$inf3(C(1,x[2]),C(0,y[2])),C(1,y[1])),inf3(inf3(C(2,x[2]),C(0,y[2])),C(2,y[1]))),$
$inf3(inf3(C(2,x[2]),C(1,x[1])),C(2,y[1]))),inf3(inf3(C(1,x[2]),C(2,x[1])),C(1,y[1]))),$
$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$
$inf3(C(1,y[1]),C(1,y[2])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(1,y[2]),C(2,y[1])))),$
$inf3(inf3(C(2,x[2]),C(2,x[1])),inf3(C(2,y[2]),C(1,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(2,y[2]),C(0,y[1])))),$
$inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[1]),C(2,x[2])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(1,x[1])),C(1,y[2]))),inf3(inf3($
$C(0,x[2]),C(2,x[1])),C(2,y[2]))),sup3(C(0,x[1]),C(0,y[1]))) := sup3(sup3(sup3(sup3($
$sup3(sup3(sup3(sup3(sup3(inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(0,y[2]),C(1,y[1]))),$
$inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(0,y[2]),C(2,y[1])))),inf3(inf3(C(1,x[2]),C(0,x[1])),$
$inf3(C(2,y[1]),C(2,y[2])))),inf3(inf3(C(2,x[2]),C(0,x[1])),inf3(C(1,y[1]),C(1,y[2])))),$
$inf3(inf3(C(1,x[2]),C(0,x[1])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(2,x[2]),C(0,x[1])),$
$inf3(C(2,y[2]),C(0,y[1])))),inf3(inf3(C(1,x[1]),C(1,x[2])),inf3(C(2,y[2]),C(0,y[1])))),$
$inf3(inf3(C(2,x[1]),C(2,x[2])),inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(1,x[1])),$
$inf3(C(1,y[2]),C(0,y[1])))),inf3(inf3(C(0,x[2]),C(2,x[1])),inf3(C(2,y[2]),C(0,y[1]))));$

```
c;
end proc:
```

Cálculo de $C_i(x\Delta y)(32)$

```
Cixdely32 := proc(i,x,y)
local resul, s, t;
resul:=[0,0];
    for s from 0 to 2 do
       for t from 0 to 2 do
          if modp(s+t-i,3)=0 then
                resul:=sup32(resul,inf32(C32(s,x),C32(t,y)));
          end if;
       end do
    end do;
resul
end proc:
```

Cálculo de $x\Delta y(32)$

```
xdely32 := proc(x,y)
local i, suma;
suma := 0 :
    for i from 0 to 2 do
            suma:=sup32(suma,inf32(Cixdely32(i,x,y),[e3(i),e3(i)]))
    end do;
suma
end proc:
```

xdely32(x,y);

$$[sup3(inf3(sup3(sup3($$
$$inf3(C(0,x_1),C(1,y_1)),inf3(C(1,x_1),C(0,y_1))),inf3(C(2,x_1),C(2,y_1))),2),$$
$$sup3(sup3(inf3(C(0,x_1),C(2,y_1)),inf3(C(1,x_1),C(1,y_1))),inf3(C(2,x_1),C(0,y_1)))),$$
$$sup3(inf3(sup3(sup3($$
$$inf3(C(0,x_2),C(1,y_2)),inf3(C(1,x_2),C(0,y_2))),inf3(C(2,x_2),C(2,y_2))),2),$$
$$sup3(sup3(inf3(C(0,x_2),C(2,y_2)),inf3(C(1,x_2),C(1,y_2))),inf3(C(2,x_2),C(2,y_2))))]$$

La salida del programa es

$x\Delta y(32) = [\{[(C_0(x) \wedge C_1(y)) \vee (C_1(x) \wedge C_0(y)) \vee (C_2(x) \wedge C_2(y))] \wedge \mathbf{e_1}\} \vee$
$\vee (C_0(x) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_0(y))$.

Cálculo de $C_i(x \odot y)(32)$

```
Cixody3:= proc(i,x,y)
local resul, s, t;
resul:= 0;
    for s from 0 to 2 do
        for t from 0 to 2 do
            if modp(s*t+i,3)=0 then resul:= sup32(resul,inf32(C32(s,x),C32(t,y)))
            end if;
        end do
        end do;
resul;
end proc:
```

Cálculo de $x \odot y(32)$

```
xody32:= proc(x,y)
local i, suma;
suma:= 0;
    for i from 0 to 2 do
    suma:= sup32(suma, inf32(Cixody32(i,x,y),e32([i,i])));
    end do;
suma;
end proc:
```

xody32(x,y);

$$[sup3(inf3(sup3(inf3(C(1,x_1),C(2,y_1)),inf3(C(2,x_1),C(1,y_1))),2),$$
$$sup3(inf3(C(1,x_1),C(1,y_1)),inf3(C(2,x_1),C(2,y_1)))),$$
$$sup3(inf3(sup3(inf3(C(1,x_2),C(2,y_2)),inf3(C(2,x_2),C(1,y_2))),2),$$
$$sup3(inf3(C(1,x_2),C(1,y_2)),inf3(C(2,x_2),C(2,y_2))))]$$

La salida del programa corresponde a la fórmula

$x \odot y(32) = [\{[(C_1(x) \wedge C_2(y)) \vee (C_2(x) \wedge C_1(y))] \wedge \mathbf{e_1}\} \vee$
$\vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y))$.

Cálculo del elemento primitivo

```
readlib(GF):
G:= GF(3, 2, alpha^2 + 1):
ep:= G[ConvertOut](G[PrimitiveElement]());
```

$$ep := 2 + \alpha$$

Expresa los elementos de $F(3^2)$ en L_{32}

```
Polavec:= proc(pol,G,ep)
global w, rep, ecu, sols, vec;
w[0]:= ep;
w[1]:= G[ConvertOut](G[‘](G[ConvertIn](ep), 3)):
rep:= lambda[0]*w[0] + lambda[1]*w[1]:
ecu[1]:= coeff(rep,alpha,0) =coeff(pol, alpha,0):
ecu[2]:= coeff(rep,alpha,1) =coeff(pol, alpha,1):
sols:= msolve({ecu[1],ecu[2]},3):
vec:= [subs(sols,lambda[0]),subs(sols,lambda[1])];
end proc:

xpoti:= proc(x,i,G)
    if i=0 then xpoti(x,i):= 0
          else xpoti(x,i):= G[ConvertOut](G[‘ ‘](G[ConvertIn](x), i))
    end if;
end proc:
```

Cálculo de los polinomios de Lagrange en $F(3^2)$

```
L0 := proc(p, k, x)
    (p - 1) * x^(p^k - 1) + 1
end proc:
```

$$2x^8 + 1$$

```
L := proc(p, k, i, x, l)
local polilag, pol, j;
    if i = 0 then polilag:=(p - 1) * x^(p^k - 1) + 1
              else polilag:= L0(p, k, x + (p - 1) * l^i);
    end if;
pol:= 0;
for j from 0 to 8 do
pol:= pol + x^j * (rem(coeff(polilag, x, j), alpha^2 + 1, alpha) mod 3);
```

```
end do;
pol;
end proc:
```

La salida del programa es la siguiente:

L(3,2,0,x);

$$\varepsilon^4 x^8 + 1,$$

L(3,2,1,x);

$$\varepsilon^4 x^8 + \varepsilon^5 x^7 + \varepsilon^6 x^6 + \varepsilon^7 x^5 + x^4 + \varepsilon x^3 + \varepsilon^2 x^2 + \varepsilon^3 x,$$

L(3,2,2,x);

$$\varepsilon^4 x^8 + \varepsilon^6 x^7 + x^6 + \varepsilon^2 x^5 + \varepsilon^4 x^4 + \varepsilon^6 x^3 + x^2 + \varepsilon^2 x,$$

L(3,2,3,x);

$$\varepsilon^4 x^8 + \varepsilon^7 x^7 + \varepsilon^2 x^6 + \varepsilon^5 x^5 + x^4 + \varepsilon^3 x^3 + \varepsilon^6 x^2 + \varepsilon x,$$

L(3,2,4,x);

$$\varepsilon^4 x^8 + x^7 + \varepsilon^4 x^6 + x^5 + \varepsilon^4 x^4 + x^3 + \varepsilon^4 x^2 + x,$$

L(3,2,5,x);

$$L_{\varepsilon^5}(x) = \varepsilon^4 x^8 + \varepsilon x^7 + \varepsilon^6 x^6 + \varepsilon^3 x^5 + x^4 + \varepsilon^5 x^3 + \varepsilon^2 x^2 + \varepsilon^7 x,$$

L(3,2,6,x);

$$\varepsilon^4 x^8 + \varepsilon^2 x^7 + x^6 + \varepsilon^6 x^5 + \varepsilon^4 x^4 + \varepsilon^2 x^3 + x^2 + \varepsilon^6 x,$$

L(3,2,7,x);

$$\varepsilon^4 x^8 + \varepsilon^3 x^7 + \varepsilon^2 x^6 + \varepsilon x^5 + x^4 + \varepsilon^7 x^3 + \varepsilon^6 x^2 + \varepsilon^5 x,$$

L(3,2,8,x);

$$\varepsilon^4 x^8 + \varepsilon^4 x^7 + \varepsilon^4 x^6 + \varepsilon^4 x^5 + \varepsilon^4 x^4 + \varepsilon^4 x^3 + \varepsilon^4 x^2 + \varepsilon^4 x.$$

Cálculo del ínfimo

```
infalpha := proc(x,y)
local comx, comy, ma, vuelta;
comx := Polavec(x,G,ep);
comy := Polavec(y,G,ep);
ma[1]:= inf3(comx[1],comy[1]);
ma[2]:= inf3(comx[2],comy[2]);
```

vuelta:= ma[1]∗w[0] + ma[2]∗w[1] mod 3;
end proc:

xinfy:= proc(x,y,ep)
local i, j;
add(add(infalpha(xpoti(ep,i,G),xpoti(ep,j,G))∗L(3, 2, i, x, ep)∗L(3, 2, j, y, ep),
$j = 0...(3^2 - 1)), i = 0...(3^2 - 1))$
end proc:

infimo32:=expand(xinfy(x,y,ep)) mod 3:
pin:=0:
for k from 0 to 6 do
$pin := pin + x^k * (algsubs(alpha^2 = 2, coeff(infimo32, x, k))mod3)$;
end do;

$$x(2y + 2y^3 + 2y^4) + x^2(y^2 + y^3 + 2y^6 + y^4) + x^3(2y^6 + 2y + y^3 + y^2)+$$
$$+x^4(2y + 2y^6 + y^2 + 2y^4) + x^6(2y^4 + 2y^2 + 2y^3 + y^6)$$

Cálculo del supremo
supalpha := proc(x,y)
local comx, comy, ma, vuelta;
comx := Polavec(x,G,ep);
comy := Polavec(y,G,ep);
ma[1]:= sup3(comx[1],comy[1]);
ma[2]:= sup3(comx[2],comy[2]);
vuelta:= ma[1]∗w[0] + ma[2]∗w[1] mod 3;
end proc:

xsupy:= proc(x,y,ep)
local i, j;
add(add(supalpha(xpoti(ep,i,G),xpoti(ep,j,G))∗L(3, 2, i, x, ep)∗L(3, 2, j, y, ep),
$j = 0...(3^2 - 1)), i = 0...(3^2 - 1))$
end proc:

supremo32:=expand(xinfy(x,y,ep)) mod 3:
pin:=0:
for k from 0 to 6 do
$pin := pin + x^k * (algsubs(alpha^2 = 2, coeff(supremo32, x, k))mod3)$;
end do;

$$y + x(1 + y + y^3 + y^4) + x^2(2y^3 + 2y^2 + y^6 + 2y^4) + x^3(y + 2y^3 + 2y^2 + y^6)+$$
$$+x^4(y + y^4 + 2y^2 + y^6) + x^6(y^3 + y^2 + 2y^6 + y^4)$$

Cálculo de los polinomios de Lagrange en $L_{3,2}$

L0 := proc(x)
$[x[1]^2 * x[2]^2 + 2 * x[1]^2 + 2 * x[2]^2 + 1 \bmod 3,$
$x[1]^2 * x[2]^2 + 2 * x[1]^2 + 2 * x[2]^2 + 1 \bmod 3];$
end proc:
L:= proc(a,x)
expand(L0($[x[1] + 2 * a[1], x[2] + 2 * a[2]]$)) mod 3
end proc:
L00:= L([0,0],[x,T(x)])[1];
L10:= L([1,0],[x,T(x)])[1];
L12:= L([1,2],[x,T(x)])[1];
L01:= L([0,1],[x,T(x)])[1];
L11:= L([1,1],[x,T(x)])[1];
L20:= L([2,0],[x,T(x)])[1];
L21:= L([2,1],[x,T(x)])[1];
L02:= L([0,2],[x,T(x)])[1];
L22:= L([2,2],[x,T(x)])[1];

$$L00 := x^2Tx^2 + 2x^2 + 2Tx^2 + 1$$

$$L10 := x^2Tx^2 + Tx^2x + 2x^2 + 2x$$

$$L12 := x^2Tx^2 + 2x^2Tx + Tx^2x + 2xTx$$

$$L01 := x^2Tx^2 + x^2Tx + 2Tx^2 + 2Tx$$

$$L11 := x^2Tx^2 + x^2Tx + Tx^2x + xTx$$

$$L20 := x^2Tx^2 + 2xTx^2 + 2x^2 + x$$

$$L21 := x^2Tx^2 + x^2Tx + 2Tx^2x + 2xTx$$

$$L02 := x^2Tx^2 + 2x^2Tx + 2Tx^2 + Tx$$

$$L22 := x^2Tx^2 + 2x^2Tx + 2Tx^2x + xTx$$

Los polinomios obtenidos son los siguientes:

$\mathcal{L}_0(x) = x^2 \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2\Delta\mathbf{e_1} \odot (T(x))^2\Delta\mathbf{1}$,
$\mathcal{L}_\epsilon(x) = x^2 \odot (T(x))^2\Delta x \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2 \odot \mathbf{e_1} \odot x$,
$\mathcal{L}_{\varepsilon^2}(x) = x^2 \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2 \odot T(x)\Delta x \odot (T(x))^2\Delta\mathbf{e_1} \odot x \odot T(x)$,
$\mathcal{L}_{\varepsilon^3}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta\mathbf{e_1} \odot (T(x))^2\Delta\mathbf{e_1} \odot T(x)$,
$\mathcal{L}_{\varepsilon^4}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta x \odot (T(x))^2\Delta x \odot T(x)$,
$\mathcal{L}_{\varepsilon^5}(x) = x^2 \odot (T(x))^2\Delta\mathbf{e_1} \odot x \odot (T(x))^2\Delta x \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2\Delta x$,
$\mathcal{L}_{\varepsilon^6}(x) = x^2 \odot (T(x))^2\Delta x^2 \odot T(x)\Delta\mathbf{e_1} \odot x \odot (T(x))^2\Delta\mathbf{e_1} \odot x \odot T(x)$,
$\mathcal{L}_{\varepsilon^7}(x) = x^2 \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2 \odot T(x)\Delta\mathbf{e_1} \odot (T(x))^2\Delta T(x)$ y
$\mathcal{L}_{\varepsilon^8}(x) = x^2 \odot (T(x))^2\Delta\mathbf{e_1} \odot x^2 \odot T(x)\Delta\mathbf{e_1} \odot x \odot (T(x))^2\Delta x \odot T(x)$.

Cálculo del producto en $\langle L_{3,2}; \Delta, \odot \rangle$
v[0,0]:=0;

```
v[0,1]:=1+alpha;
v[2,1]:=2*alpha;
v[1,0]:=1+2*alpha;
v[1,1]:=2;
v[0,2]:=2+2*alpha;
v[1,2]:=alpha;
v[2,0]:=2+alpha;
v[2,2]:=1;

prodpares32:=proc(x,y,G,ep)
local prod1, prod2, producto, par;
prod1:=v[x[1],x[2]]*v[y[1],y[2]];
prod2:=expand(prod1) mod 3;
producto:=algsubs(alpha^2 = 2,prod2) mod 3;
par:=Polavec(producto,GF(3,2,alpha^2 + 1),2 * alpha + 1);
par;
end proc:

prodani32:= proc(x,y)
local suma, i1, j1, i2, j2;
suma:=0;
for i1 from 0 to 2 do
        for j1 from 0 to 2 do
                for i2 from 0 to 2 do
                        for j2 from 0 to 2 do
suma:=suma+[prodpares32([i1,j1],[i2,j2])[1]*L([i1,j1],[x,Tx])[1]*L([i2,j2],[y,Ty])[1]
mod 3,prodpares32([i1,j1],[i2,j2])[2]*L([i1,j1],[x,Tx])[2]*L([i2,j2],[y,Ty])[2] mod 3];
                        end do;
                end do;
        end do;
end do;
suma;
end proc:
prodani32(x,y);

prodanillo32:=proc(x,y)
expand(prodani32(x,y)) mod 3
end:
prodanillo32(x,y);
```

$$[2TxTy + xy + Txy + xTy, 2TxTy + xy + Txy + xTy]$$

El resultado obtenido es
$x \cdot y = \mathbf{e_1} \odot T(x) \odot T(y) \Delta x \odot y \Delta T(x) \odot y \Delta x \odot T(y)$

Cálculo de la suma en $\langle L_{3,2}; \Delta, \odot \rangle$

```
sumani32:= proc(x,y)
local suma, i1, i2, j1, j2;
suma:=0;
for i1 from 0 to 2 do
        for j1 from 0 to 2 do
                for i2 from 0 to 2 do
                        for j1 from 0 to 2 do
                                for j2 from 0 to 2 do
suma:=suma+[([i1,j1]+[i2,j2])[1]*L([i1,j1],[x,Tx])[1]*L([i2,j2],[y,Ty])[1]
mod 3,([i1,j1]+[i2,j2])[2]*L([i1,j1],[x,Tx])[2]*L([i2,j2],[y,Ty])[2] mod 3];
                                end do;
                        end do;
                end do;
        end do;
suma;
end proc:
sumani32(x,y);
```

```
sumanillo32:= proc(x,y)
expand(sumani32(x,y)) mod 3
end proc:
sumanillo3(x,y);
```

$$[x+y, x+y]$$

El resultado obtenido es $x + y = x\Delta y$.

Cálculo de un término dado en $F(3^2)$ en L_{32}

```
terxL32:=proc(x,n)
local i, s, ter0, ter1, ter2, ter3, terx;
s := G[ConvertOut](G[‘](G[ConvertIn](2), n − 1));
terx := x;
for i from 2 to s do
ter0:= xody32(T32(terx),x);
ter1:= xody32(terx,x);
ter2:= xody32(T32(terx),x);
ter3:= xody32(xody32([2,2],T32(terx)),T32(x));
terx:=xdely32(xdely32(xdely32(ter0,ter1),ter2),ter3);
end do;
terx;
end proc:
```

```
terxyL32:=proc(x,n,y,m)
local s, i, terx, t, j, tery, terxy;
s := G[ConvertOut](G[‘](G[ConvertIn](2), n − 1));
terx:=x;
```

for i from 2 to s do
terx:=xdely32(xdely32(xdely32(xody32(T32(terx),x),xody32(terx,x)),xody32(T32(terx),x)),
xody32(xody32(e32([1,1]),T32(terx)),T32(x)));
end do;
$t := G[ConvertOut](G[`](G[ConvertIn](2), m-1))$;
$tery := y$;
for j from 2 to t do
tery:=xdely32(xdely32(xdely32(xody32(T32(tery),y),xody32(tery,y)),xody32(T32(tery),y)),
xody32(xody32(e32([1,1]),T32(tery)),T32(y)));
end do;
terxy:=xdely32(xdely32(xdely32(xody32(T32(terx),tery),xody32(terx,tery)),
xody32(T32(terx),tery)),xody32(xody32(e32([1,1]),T32(terx)),T32(tery)));
terxy;
end proc:

Polinomios en L_{32}[X,Y]

Los siguientes ejemplos nos muestran la expresión en $L_{32}[X,Y]$ de polinomios dados en $F(3^2)[X,Y]$.

terxL32(x,2);

$$[sup3(inf3(sup3(sup3(sup3(inf3(C(0,x_1),C(2,x_2)),inf3(C(0,x_1),C(1,x_2))),$$
$$inf3(C(1,x_1),C(1,x_2))),inf3(C(2,x_1),C(2,x_2))),2),$$
$$sup3(sup3(inf3(C(1,x_2),C(2,x_1)),inf3(C(2,x_2),C(1,x_1))),$$
$$sup3(inf3(C(0,x_2),C(1,x_1)),inf3(C(0,x_2),C(2,x_1))))),$$
$$sup3(inf3(sup3(sup3(sup3(inf3(C(0,x_2),C(2,x_1)),inf3(C(0,x_2),C(1,x_1))),$$
$$inf3(C(1,x_2),C(1,x_1))),inf3(C(2,x_2),C(2,x_1))),2),$$
$$sup3(sup3(inf3(C(1,x_1),C(2,x_2)),inf3(C(2,x_1),C(1,x_2))),$$
$$sup3(inf3(C(0,x_1),C(1,x_2)),inf3(C(0,x_1),C(2,x_2))))]$$

El polinomio obtenido es

$$x^2 = \{[(C_0(x)\wedge C_2(T(x)))\vee(C_0(x)\wedge C_1(T(x)))\vee(C_1(x)\wedge C_1(T(x)))\vee$$
$$\vee(C_2(x)\wedge C_2(T(x)))]\wedge \mathbf{e_1}\}\vee$$
$$\vee(C_2(x)\wedge C_1(T(x)))\vee(C_1(x)\wedge C_2(T(x)))\vee(C_1(x)\wedge C_0(T(x)))\vee(C_2(x)\wedge C_0(T(x))).$$

xdely32(terxL32(x,2),[2,2]);

$$[sup3(sup3(sup3(sup3(inf3(inf3(C(0,x_1),C(0,x_2)),2),inf3(C(0,x_1),C(2,x_2))),$$
$$inf3(C(0,x_1),C(1,x_2))),inf3(C(1,x_1),C(1,x_2))),inf3(C(2,x_1),C(2,x_2))),$$

$sup3(sup3(sup3(sup3(inf3(inf3(C(0,x_2),C(0,x_1)),2),inf3(C(0,x_2),C(2,x_1))),$
$inf3(C(0,x_2),C(1,x_1))),inf3(C(1,x_2),C(1,x_1))),inf3(C(2,x_2),C(2,x_1)))]$.

La expresión anterior corresponde al polinomio

$x^2+1=(C_0(x)\wedge C_0(T(x))\wedge \mathbf{e_1})\vee(C_0(x)\wedge C_2(T(x)))\vee(C_0(x)\wedge C_1(T(x)))\vee$
$\vee(C_1(x)\wedge C_1(T(x)))\vee(C_2(x)\wedge C_2(T(x)))$

xdely32(terxL32(x,2),xdely32(x,[2,2]));

$[sup3(inf3(sup3(sup3(sup3(sup3(inf3(C(1,x_1),C(0,x_2)),inf3(C(1,x_1),C(2,x_2))),$

$inf3(C(0,x_1),C(2,x_2))),C(0,x_1)),C(2,x)),2),sup3(sup3(sup3(inf3(C(2,x_1),C(0,x_2)),$
$inf3(C(2,x_1),C(1,x_2))),inf3(C(0,x_1),C(2,x_2))),inf3(C(0,x_1),C(1,x_2)))),$
$sup3(inf3(sup3(sup3(sup3(sup3(inf3(C(1,x_2),C(0,x_1)),inf3(C(1,x_2),C(2,x_1))),$
$inf3(C(0,x_2),C(2,x_1))),C(0,x_2)),C(2,x)),2),sup3(sup3(sup3(inf3(C(2,x_2),C(0,x_1)),$
$inf3(C(2,x_2),C(1,x_1))),inf3(C(0,x_2),C(2,x_1))),inf3(C(0,x_2),C(1,x_1))))]$.

Luego
$x^2+x+1=\{[(C_1(x)\wedge C_0(T(x)))\vee(C_1(x)\wedge C_2(T(x)))\vee C_0(x)\vee C_2(x)]\wedge \mathbf{e_1}\}$
$\vee(C_2(x)\wedge C_0(T(x)))\vee(C_2(x)\wedge C_1(T(x)))\vee(C_0(x)\wedge C_2(T(x)))\vee(C_0(x)\wedge C_1(T(x)))$.

xdely32(x,y);

$[sup3(inf3(sup3(sup3(inf3(C(0,x_1),C(1,y_1)),inf3(C(1,x_1),C(0,y_1))),$

$inf3(C(2,x_1),C(2,y_1)))),2),$
$sup3(sup3(inf3(C(0,x_1),C(2,y_1)),inf3(C(1,x_1),C(1,y_1))),inf3(C(2,x_1),C(0,y_1))),$
$sup3(inf3(sup3(sup3(inf3(C(0,x_2),C(1,y_2)),inf3(C(1,x_2),C(0,y_2))),$
$inf3(C(2,x_2),C(2,y_2)))),2),$
$sup3(sup3(inf3(C(0,x_2),C(2,y_2)),inf3(C(1,x_2),C(1,y_2))),inf3(C(2,x_2),C(0,y_2)))]$.

Obtenemos
$x+y=\{[(C_0(x)\wedge C_1(y))\vee(C_1(x)\wedge C_0(y))\vee(C_2(x)\wedge C_2(y))]\wedge \mathbf{e_1}\}\vee$
$\vee(C_0(x)\wedge C_2(y))\vee(C_1(x)\wedge C_1(y))\vee(C_2(x)\wedge C_0(y))$.

terxyL32(x,y);

$[sup3(inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($

$inf3(inf3(C(2,x_1),C(2,x_2)),C(2,y_1))),inf3(inf3(C(1,x_1),C(1,x_2)),C(1,y_1))),$
$inf3(inf3(C(2,x_1),C(1,x_2)),C(2,y_2))),inf3(inf3(C(1,x_1),C(2,x_2)),C(1,y_2))),$

$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(0,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(0,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(0,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(0,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(2,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(2,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(1,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(1,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(1,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(2,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(1,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(2,y_1)),C(1,y_2)))\wedge 2)],$$
$$[sup3(inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$inf3(inf3(C(2,x_1),C(1,x_2)),C(1,y_2))),inf3(inf3(C(1,x_1),C(2,x_2)),C(2,y_2))),$$
$$inf3(inf3(C(2,x_1),C(2,x_2)),C(1,y_1))),inf3(inf3(C(1,x_1),C(1,x_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(0,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(0,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(2,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(1,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(0,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(0,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(2,y_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(1,y_1)),C(1,y_2))),$$
$$inf3(inf3(inf3(C(1,x_1),C(0,x_2)),C(1,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(2,x_1),C(0,x_2)),C(2,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(1,x_2)),C(1,y_1)),C(0,y_2))),$$
$$inf3(inf3(inf3(C(0,x_1),C(2,x_2)),C(2,y_1)),C(0,y_2))),$$
$$sup3(inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$inf3(inf3(C(2,x_2),C(2,x_1)),C(2,y_2))),inf3(inf3(C(1,x_2),C(1,x_1)),C(1,y_2))),$$
$$inf3(inf3(C(2,x_2),C(1,x_1)),C(2,y_1))),inf3(inf3(C(1,x_2),C(2,x_1)),C(1,y_1))),$$

$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(0,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(0,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(0,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(0,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(2,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(2,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(1,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(1,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(1,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(2,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(1,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(2,y_2)),C(1,y_1))) \wedge 2)],$$
$$[sup3(inf3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3(sup3($$
$$inf3(inf3(C(2,x_2),C(1,x_1)),C(1,y_1))),inf3(inf3(C(1,x_2),C(2,x_1)),C(2,y_1))),$$
$$inf3(inf3(C(2,x_2),C(2,x_1)),C(1,y_2))),inf3(inf3(C(1,x_2),C(1,x_1)),C(2,y_2))),$$
$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(0,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(0,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(2,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(1,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(0,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(0,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(2,y_2)),C(2,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(1,y_2)),C(1,y_1))),$$
$$inf3(inf3(inf3(C(1,x_2),C(0,x_1)),C(1,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(2,x_2),C(0,x_1)),C(2,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(1,x_1)),C(1,y_2)),C(0,y_1))),$$
$$inf3(inf3(inf3(C(0,x_2),C(2,x_1)),C(2,y_2)),C(0,y_1))).]$$

La salida del programa es el polinomio

$$x \cdot y = \{[(C_2(x) \wedge C_2(T(x)) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(T(x)) \wedge C_1(y)) \vee$$
$$\vee (C_2(x) \wedge C_1(T(x)) \wedge C_2(T(y))) \vee (C_1(x) \wedge C_2(T(x)) \wedge C_1(T(y))) \vee$$

$$\vee(C_0(x) \wedge C_2(T(x)) \wedge C_0(y) \wedge C_2(T(y))) \vee (C_0(x) \wedge C_1(T(x)) \wedge C_0(y) \wedge C_1(T(y)))\vee$$
$$\vee(C_1(x) \wedge C_0(T(x)) \wedge C_0(y) \wedge C_2(T(y))) \vee (C_2(x) \wedge C_0(T(x)) \wedge C_0(y) \wedge C_1(T(y)))\vee$$
$$\vee(C_0(x) \wedge C_1(T(x)) \wedge C_2(y) \wedge C_0(T(y))) \vee (C_1(x) \wedge C_0(T(x)) \wedge C_2(y) \wedge C_0(T(y)))\vee$$
$$\vee(C_2(x) \wedge C_0(T(x)) \wedge C_1(y) \wedge C_0(T(y))) \vee (C_0(x) \wedge C_2(T(x)) \wedge C_1(y) \wedge C_0(T(y)))\vee$$
$$\vee(C_1(x) \wedge C_0(T(x)) \wedge C_1(y) \wedge C_1(T(y))) \vee (C_2(x) \wedge C_0(T(x)) \wedge C_2(y) \wedge C_2(T(y)))\vee$$
$$\vee(C_0(x)\wedge C_1(T(x))\wedge C_1(y)\wedge C_2(T(y)))\vee(C_0(x)\wedge C_2(T(x))\wedge C_2(y)\wedge C_1(T(y)))]\wedge\mathbf{e_1}\}\vee$$
$$[(C_2(x) \wedge C_1(T(x)) \wedge C_1(T(y))) \vee (C_1(x) \wedge C_2(T(x)) \wedge C_2(T(y)))\vee$$
$$(C_2(x) \wedge C_2(T(x)) \wedge C_1(y)) \vee (C_1(x) \wedge C_1(T(x)) \wedge C_2(y))\vee$$
$$(C_0(x) \wedge C_2(T(x) \wedge C_0(y)) \wedge C_1(T(y))) \vee (C_0(x) \wedge C_1(T(x)) \wedge C_0(y) \wedge C_2(T(y)))\vee$$
$$(C_0(x) \wedge C_1(T(x)) \wedge C_2(y) \wedge C_1(T(y))) \vee (C_0(x) \wedge C_2(T(x)) \wedge C_1(y) \wedge C_2(T(y)))\vee$$
$$(C_1(x) \wedge C_0(T(x)) \wedge C_0(y) \wedge C_1(T(y))) \vee (C_2(x) \wedge C_0(T(x)) \wedge C_0(y) \wedge C_2(T(y)))\vee$$
$$(C_1(x) \wedge C_0(T(x)) \wedge C_2(y) \wedge C_2(T(y))) \vee (C_2(x) \wedge C_0(T(x)) \wedge C_1(y) \wedge C_1(T(y)))\vee$$
$$(C_1(x) \wedge C_0(T(x)) \wedge C_1(y) \wedge C_0(T(y))) \vee (C_2(x) \wedge C_0(T(x)) \wedge C_2(y) \wedge C_0(T(y)))\vee$$
$$(C_0(x) \wedge C_1(T(x)) \wedge C_1(y) \wedge C_0(T(y))) \vee (C_0(x) \wedge C_2(T(x)) \wedge C_2(y) \wedge C_0(T(y)))].$$