Universidad de Valladolid

Curvas monomiales

María Jesús Pisabarro Manteca

Tesis de Doctorado

Facultad: Ciencias

Director: Dra. Carolina Ana Núñez Jiménez

2001

UNIVERSIDAD DE VALLADOLID
FACULTAD DE CIENCIAS
Departamento de Álgebra, Geometría y Topología

Curvas monomiales

María Jesús Pisabarro Manteca

(2001)

Curvas monomiales

Memoria presentada por
María Jesús Pisabarro Manteca
para optar al grado de
Doctora en Matemáticas
por la Universidad de Valladolid

Dña. CAROLINA ANA NÚÑEZ JIMÉNEZ, Profesora Titular de Universidad del área de Geometría y Topología de la Universidad de Valladolid,

CERTIFICA:

que la presente memoria "Curvas monomiales" ha sido realizada por María Jesús Pisabarro Manteca bajo su dirección en la Universidad de Valladolid. Para que conste, en cumplimiento de la legislación vigente, presento y apadrino ante la Comisión de Doctorado de dicha Universidad esta tesis doctoral.

Valladolid, a 4 de Abril de 2001.

Fdo.: Carolina Ana Núñez Jiménez

En primer lugar quiero agradecer a la Dra. Ana Núñez Jiménez, directora de esta tesis, sin cuyos conocimientos y aportaciones hubiera sido imposible la realización de esta memoria, todo su tiempo y esfuerzo empleados en mi formación investigadora.

También agradezco a los Drs. Antonio Campillo López y Félix Delgado de la Mata las ideas que generosamente me han cedido, así como mi inclusión como colaboradora en los proyectos de investigación que dirigen, dándome la posibilidad de contactar con un grupo de trabajo que me ha aportado material fundamental en la obtención de resultados.

Además, agradezco el apoyo de todos mis compañeros del Departamento de Matemáticas de la Universidad de León y, en especial, al Dr. José Ángel Hermida Alonso, por su total atención para solucionar los problemas que le he planteado.

También deseo citar a las Universidades de León y de Valladolid, por los medios económicos que me han aportado durante estos últimos años.

Por último, a todos aquellos que con su confianza y apoyo me han estimulado para la realización de esta memoria.

A mis padres

Índice

Introducción

Con la sistematización y formalización de la Geometría Algebraica, llevada a cabo en los años 50 y 60 del siglo XX, se han entendido y generado gran cantidad de estudios y teorías que afectan a la estructura de las variedades algebraicas y a su clasificación. Muchos de estos avances han sido frecuentemente teóricos o sus contenidos difíciles de discutir y apreciar sobre ejemplos concretos (salvo en ciertos casos de dimensión o codimensión pequeña). Por ello se ha encontrado satisfactoria la localización de clases de variedades sobre las que poder calcular invariantes y comprobar sobre dichos invariantes la profundidad y eficacia de las correspondientes teorías.

Éste ha sido el caso de la geometría tórica, que desde los años 70, y a partir de trabajos de Demazure sobre subgrupos algebraicos maximales de los grupos de Cremona ([Dem]), ha proporcionado a la Geometría Algebraica la amplia clase de variedades tóricas, sobre la que se han podido describir explícitamente muchos de los logros de este campo. A la vez, dicha descripción, influida por la potencia de los métodos algebraico-geométricos, ha dado lugar a gran cantidad de aplicaciones en otros campos de las matemáticas. Así, la geometría tórica se emplea hoy día en Combinatoria, Computación Algebraica, Geometría Computacional, Optimización Combinatoria o Programación Matemática.

La geometría tórica, como disciplina independiente, ha sido popularizada por varios textos sucesivos desde los años 70. En primer lugar, el libro de Knudsen, Kempf, Mumford y Saint Donat de 1973, cuyo impacto se debe a que en él se muestra la descripción explícita de los sistemas lineales de divisores naturales en el caso tórico y se aplican los resultados para obtener un resultado que todavía hoy día se considera de gran alcance, como es el teorema de la reducción semiestable (se ha aplicado recientemente por Abramovich y De Jong para probar versiones cortas del teorema de resolución de singularidades). Por otro lado, el survey de Danilov [Dan] de 1978 en el que se expone con precisión la interrelación entre la geometría tórica y los poliedros de Newton. También el libro de Oda [Oda] de 1998, en el que se sitúa a la geometría tórica como núcleo de la Geometría Algebraica y se muestra cómo ésta se puede beneficiar de los métodos de la Combinatoria y de la Geometría Convexa. En 1993 aparece el libro de Fulton, [Ful2], que convierte ya a la geometría tórica en un útil general para otros campos de las matemáticas (y también para la física, en el momento en el que las implicaciones recíprocas de ambas disciplinas llevan a aplicaciones significativas en ambas direcciones), convirtiéndose entonces la geometría tórica en una rama impulsora del uso de los métodos de la geometría algebraica en otras áreas. Finalmente, el libro de Sturmfels de 1996 [Stu], pone de manifiesto cómo estudiar la geometría tórica, tanto en el caso de variedades proyectivas normales (como se había hecho hasta los años 90) como en los de variedades proyectivas o afines no normales, con una óptica común: basta estudiar variedades tóricas (no normales) sumergidas como ciertos subesquemas del espacio afín.

La presentación de una variedad tórica V como subesquema del espacio afín se realiza identificando su álgebra de coordenadas con el álgebra A de un semigrupo abeliano de generación finita S, en el cual se ha fijado (o "marcado") uno de sus sistemas finitos de (digamos n) generadores. El subesquema que define la variedad tórica está dado, entonces, por el ideal del anillo de polinomios en n indeterminadas que es núcleo del morfismo de álgebras dado por la asignación a cada variable del generador del semigrupo que le corresponde. Un hecho notable es que dicho ideal I está generado por binomios; es decir, se tiene que, módulo I, se identifican dos monomios cuando tienen igual imagen en A. Los ideales I que aparecen en dicho proceso se llaman, en la literatura, tóricos. Cuando V es una variedad irreducible, el semigrupo S puede interpretarse como un subsemigrupo de un grupo abeliano libre de generación finita G (por tanto isomorfo a $\mathbb{Z}^d$ para algún d). Cuando se tiene una variedad proyectiva, la elección de un haz de línea muy amplio que sumerge dicha variedad en el espacio proyectivo $\mathcal{P}^m(k)$, proporciona a la vez una inmersión del cono proyectante de dicha inmersión en $\mathcal{A}^{m+1}(k)$, que resulta ser una variedad afín tórica. El subsemigrupo S de G para dicha inmersión afín se caracteriza por ser uno tal que sus generadores marcados están (todos ellos) en algún subgrupo H de G de corango 1. De esta forma, la geometría tórica proyectiva se puede ver como un caso particular de la afín. Este punto de vista está desarrollado recientemente por Campillo y Pisón en [CP].

Por otro lado, tiene interés en la práctica el caso en el que G (y por tanto S) pueden tener torsión, ya que su tratamiento no muestra diferencias con el caso libre. Ahora G aparece en la práctica presentado como cociente de un grupo abeliano libre (de generación finita) por uno de sus subgrupos L.

El conocimiento de dicho subgrupo L (llamado "retículo" en este contexto) es suficiente para determinar los generadores binomiales del ideal I, ya que I está generado por los binomios cuyos pares de exponentes son, respectivamente, la parte de coordenadas positivas y la de coordenadas negativas de los elementos de L. Tales ideales I se llaman ideales de retículo en la literatura y el propio retículo L aparece como objeto básico en la discusión y tratamiento algebraico geométrico de la correspondiente variedad V, que en este caso puede ser reducible.

La discusión sobre sistemas finitos de generadores de I, es decir de las ecuaciones de las variedades tóricas, ha sido el objeto de mucha investigación reciente. La discusión se produce porque siendo L infinito, en general, lo que se tiene a priori son una cantidad infinita de binomios en I. Por un lado interesan sistemas minimales de generadores de I (es decir conjuntos minimales de binomios que definan la variedad sumergida); por otro lado bases de Gröbner (es fácil ver que toda base de Gröbner reducida de I está también generada por binomios), e incluso bases universales de Gröbner (es decir bases de Gröbner simultáneas para todos los órdenes monomiales). En [Stu] se puede encontrar la discusión sobre la forma y dificultades del cálculo de estas clases de generadores, así como de la aplicación directa de dicho cálculo a problemas clásicos y de gran interés computacional en la actualidad, como el problema de programación lineal entera. Recientemente Bayer y Sturmfels en 1999 ([BStu]) y Campillo y Gimenez en 2000 ([CG]) desarrollaron métodos similares para el cálculo de sicigias para las variedades tóricas afines, por dos procedimientos diferentes y complementarios. En resúmen se ha encontrado una buena y explícita teoría para la familia de ideales tóricos o de ideales de retículo en general.

En 1998 Eisenbud y Sturmfels ([ES]) desarrollaron una teoría general de ideales generados por binomios en anillos de polinomios sobre cuerpos algebraicamente cerrados, mostrando que hay una sorprendentemente buena teoría para ellos. Las propiedades computacionales de dichos ideales son también buenas, y, desde un punto de vista interno su estudio se lleva a cabo por medio de retículos asociados. Este trabajo de Eisenbud y Sturmfels ha sido el punto de partida de esta Memoria, ya que hay muchas preguntas naturales que se derivan del mismo.

En efecto, admitiéndose que los ideales tóricos y de retículo se pueden estudiar a partir de semigrupos con generadores marcados, es natural preguntarse por la existencia y localización de semigrupos u otras estructuras algo más generales a partir de las cuales se puedan estudiar los ideales binomiales en general. Como uno de los resultados principales de esta memoria, veremos que en el caso de dimensión 1 (es decir curvas binomiales) se dispone de dichas estructuras. Otra pregunta natural es estudiar la relación entre las curvas binomiales y las cuasihomogéneas, es decir, aquellas que son tangentes a campos vectoriales de Euler en el espacio afín.

Esta memoria está dividida en cuatro capítulos, cuyo contenido es el siguiente:

El primer capítulo es de tipo introductorio, y en él se repasa el estudio de los ideales binomiales (generados por binomios) hecho por Eisenbud y Sturmfels en [ES]. Se dedica un primer apartado a las bases de Gröbner de un ideal, observándose que la base de Gröbner reducida de un ideal binomial está formada por binomios, hecho que nos permitirá en la práctica saber cuándo un ideal es binomial. Posteriormente se hace un estudio completo de los ideales binomiales (propios) del anillo de polinomios de Laurent, $k[X^{\pm}]$. Estos ideales resultan (Teorema 1.3.5) ser siempre de la forma

$$I(\rho) = \{X^{\underline{m}} - \rho(\underline{m}) \mid \underline{m} \in L_\rho\},$$

donde L_ρ es un subretículo de $\mathbb{Z}^n$ y $\rho : L_\rho \to k$ es un carácter parcial en $\mathbb{Z}^n$. Además el ideal $I(\rho)$ es primo cuando L_ρ es saturado, es decir, tal que $d\underline{m} \in L_\rho \Rightarrow \underline{m} \in L_\rho$. Y en el caso de cuerpos algebraicamente cerrados, la descomposición primaria del ideal $I(\rho)$ está perfectamente determinada en términos de las extensiones de ρ a Sat L_ρ y los ideales asociados.

Estos resultados se aplican al estudio de los ideales binomiales de $k[X_1, \ldots, X_n]$, mediante la consideración de los ideales de retículo

$$I_+(\rho) = \{X^{\underline{m}_+} - \rho(\underline{m})X^{\underline{m}_-} \mid \underline{m}_+ - \underline{m}_- \in L_\rho\} \ .$$

Aunque no todos los ideales binomiales de $k[X_1, \ldots, X_n]$ son de esta forma, se tienen la siguientes descripciones:

Corolario 1.3.13 *Los ideales del anillo de polinomios $k[X]$ de la forma $I_+(\rho)$ son exactamente aquellos ideales binomiales cuyos primos asociados no contienen monomios.*

Corolario 1.3.16 *Sea k un cuerpo algebraicamente cerrado, y sea $\mathcal{P}$ un ideal de $k[X]$. El ideal $\mathcal{P}$ es primo binomial si y sólo si existe un carácter parcial saturado ρ en el retículo $\mathbb{Z}^{\mathcal{Z}}$ tal que $\mathcal{P} = I_+(\rho) + < \{X_i \mid X_i \in \mathcal{P}\} >$.*

Todo lo anterior se utiliza para probar el carácter binomial del radical de un ideal binomial (Teorema 1.4.5). Finalmente se llega al resultado que está en la base de toda esta memoria, y que sirve para caracterizar qué variedades afines son tales que el ideal de los polinomios que se anulan en ellas es binomial (variedades “cortadas por binomios”):

Teorema 1.5.11 *Dado un cuerpo k algebraicamente cerrado, una subvariedad algebraica V de k^n está cortada por binomios si y sólo si se cumplen las tres condiciones siguientes:*

(i) Para cada célula coordenada $(k^*)^{\mathcal{Z}}$, $\overline{V \cap (k^*)^{\mathcal{Z}}}$ es una variedad cortada por binomios.

(ii) La familia de conjuntos $U = \{\mathcal{Z} \subseteq \{1, \dots, n\} \mid V \cap (k^*)^{\mathcal{Z}} \neq \emptyset\}$ es cerrada por intersecciones.

(iii) Si $\mathcal{Z}$, $\mathcal{Z}' \in U$ y $\mathcal{Z} \subseteq \mathcal{Z}'$ entonces la proyección $(k^*)^{\mathcal{Z}'} \to (k^*)^{\mathcal{Z}}$ aplica $V \cap (k^*)^{\mathcal{Z}'}$ en $V \cap (k^*)^{\mathcal{Z}}$.

En el Capítulo 2 pasamos a centrarnos en el estudio de ideales binomiales de codimensión 1, con el fin de aplicarlo al estudio de las curvas afines en $\mathcal{A}^n(k)$, siendo k algebraicamente cerrado y de característica 0. Comenzamos por examinar un resultado ya conocido, que es que en el caso de curvas irreducibles, la binomialidad del ideal se corresponde con la existencia de una parametrización monomial de la curva ("curva monomial"), parametrización que entenderemos definida a partir de un vector de exponentes, $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ y uno de coeficientes $\underline{\lambda} \in k^n$, por $X_i = \lambda_i t^{h_i}$. Va a cobrar en el desarrollo posterior especial relevancia la "célula asociada a la curva", definida por $\mathcal{Z} = \{i \mid \lambda_i \neq 0\}$. Puesto que hablamos de curvas inmersas en $\mathcal{A}^n(k)$, pediremos que los monomios de una tal parametrización tengan exponentes no negativos, lo que nos llevará a exigir a los ideales una condición adicional: que sean "combinatoriamente finitos" (Definición 2.1.10). De esta forma, en esta memoria se denominará en general (no sólo en el caso irreducible) "curva monomial" en $\mathcal{A}^n(k)$ a aquellas curvas C tales que $I := \mathcal{I}(C)$ es binomial y combinatoriamente finito.

El carácter binomial de los primos asociados a un ideal binomial, nos llevará a observar que si una curva C es monomial, entonces sus componentes irreducibles son monomiales, por lo que el problema que nos planteamos, y al que se dedica el resto del capítulo, es entender cuándo una curva cuyas componentes irreducibles son monomiales es a su vez monomial. Utilizaremos para ello el Teorema 1.5.11, caracterizando en primer lugar qué curvas tienen asociado un ideal de retículo (es decir, del tipo $I_+(\rho)$), y pasando después al caso general. El teorema de caracterización es el Teorema 2.2.33. Por simplicidad, enunciaremos aquí la versión correspondiente al caso en que todas las componentes de C pasan por el origen (Teorema 2.2.23):

Teorema 2.2.23 *Sea C una curva cuyas componentes irreducibles, $C_1, \dots$, C_d, son monomiales y pasan por el origen y sea $I := \mathcal{I}(C)$. Consideremos,* *para cada componente monomial irreducible C_j, una parametrización monomial dada por los vectores $(\underline{h}_j, \underline{\lambda}_j)$, su célula asociada $\mathcal{Z}_j$ y su retículo asociado $L_j = \langle(\underline{h}_j)_{\mathcal{Z}_j}\rangle^{\perp}$. Se definen, para cada $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$, $A_{\mathcal{Z}} = \{j \in \{1, \dots, d\} \mid \mathcal{Z}_j = \mathcal{Z}\}$ y $d_{\mathcal{Z}} = |A_{\mathcal{Z}}|$. Entonces, son equivalentes:*

(1) *I es binomial.*

(2) *Se cumplen las condiciones D1, D2 y D3 siguientes:*

D1 *Para todo $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$ se cumple:*

- *Existe $\underline{h}_{\mathcal{Z}} \in (\mathbb{Z}_{\geq 0})^{\mathcal{Z}}$ tal que $(\underline{h}_j)_{\mathcal{Z}} = \underline{h}_{\mathcal{Z}}$ para todo $j \in A_{\mathcal{Z}}$.*
- *Si consideramos los subretículos de $\mathbb{Z}^{\mathcal{Z}}$, $\widetilde{L}_{\mathcal{Z}} = \langle \underline{h}_{\mathcal{Z}}\rangle^{\perp}$ y $L_{\mathcal{Z}} = \{\underline{m} \in \widetilde{L}_{\mathcal{Z}} \mid (\underline{\lambda}_{j\mathcal{Z}})^{\underline{m}} = (\underline{\lambda}_{k\mathcal{Z})}^{\underline{m}}, \forall j, k \in A_{\mathcal{Z}}\}$ entonces $|\widetilde{L}_{\mathcal{Z}}/L_{\mathcal{Z}}| = d_{\mathcal{Z}}$.*

D2 *Para cualesquiera $j, k \in \{1, \dots, d\}$, o bien $\mathcal{Z}_j \cap \mathcal{Z}_k = \emptyset$, o bien existe $l \in \{1, \dots, d\}$ de forma que $\mathcal{Z}_j \cap \mathcal{Z}_k = \mathcal{Z}_l$.*

D3 *Para cualesquiera $j, k \in \{1, \dots, d\}$ tal que $\mathcal{Z}_j \subset \mathcal{Z}_k$ se cumple:*

- *Existe $a \in \mathbb{Z}^*$ tal que $ah_{ji} = h_{ki}$, para todo $i \in \mathcal{Z}_j$ (es decir, los vectores $(\underline{h}_k)_{\mathcal{Z}_j}$ y $(\underline{h}_j)_{\mathcal{Z}_j}$ son proporcionales).*
- *Existe $l \in \{1, \dots, d\}$ tal que $\mathcal{Z}_l = \mathcal{Z}_j$ y $(\underline{\lambda}_{l\mathcal{Z}_j})^{\underline{m}} = (\underline{\lambda}_{k\mathcal{Z}_j})^{\underline{m}}$, para todo $\underline{m} \in L_j$.*

Aunque no es el propósito de esta memoria el profundizar en los aspectos computacionales que se derivan de la combinatoria de las curvas monomiales, el capítulo 2 termina con un apéndice en el que se desarrollan algunos algoritmos que sirven para determinar cuándo una unión de curvas monomiales irreducibles resulta ser una curva monomial, y calcular, caso de que así sea, todos los ideales de retículo y la descomposición celular del ideal de la curva.

El Capítulo 3 se dedica a determinar qué curvas monomiales son curvas integrales de un campo de Euler, es decir de un campo del tipo $\sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}$ con coeficientes $a_i \in \mathbb{Z}$. En la segunda sección se probará algo que ya era conocido, y es que la monomialidad de una curva irreducible es, esencialmente, equivalente a la existencia de un campo de Euler tangente. Más concretamente, se tienen los siguientes resultados:

Proposición 3.2.2 *Sea C una curva monomial irreducible, con célula asociada $\mathcal{Z}$ y vector de exponentes $\underline{h}$. Sea δ el campo de Euler $\delta = \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}$. Son equivalentes:*

(a) δ es tangente a la curva C.

(b) Los vectores $\underline{a}_{\mathcal{Z}}$ y $\underline{h}_{\mathcal{Z}}$ son proporcionales.

Teorema 3.2.11 *Sean I un ideal de $k[X_1, \ldots, X_n]$ primo y de altura $n-1$ y C la curva que define I. Son equivalentes:*

1. *Existe un campo de Euler tangente a C con todos sus coeficientes no negativos.*

2. *C es monomial irreducible.*

Este resultado no es cierto en el caso de curvas monomiales no irreducibles. Es claro por lo anterior que, dado que una curva es curva integral de un campo si y sólo si lo son sus componentes, la existencia de un campo tangente a una curva con componentes monomiales sólo dice algo sobre los exponentes de las parametrizaciones, no sobre los coeficientes, por lo que difícilmente va a implicar la monomialidad de la curva. Pero a la inversa, la particular combinatoria de las curvas monomiales puede hacer pensar que sí deben ser curvas integrales de un campo de Euler. Esto no es cierto, como se ve en el Ejemplo 3.3.11, pero lo que sí es posible es caracterizar mediante un algoritmo cuándo esto ocurre, y esto se hace con el Algoritmo 3.4.8, según se explica en el Teorema 3.4.9:

Teorema 3.4.9 *Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles y sea $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\}$ el conjunto de exponentes asociados a las parametrizaciones monomiales de sus componentes. Si aplicamos el Algoritmo 3.4.8 a $\mathcal{E}$, la salida es $\emptyset$ si y sólo si no existe campo de Euler tangente a C. Si la salida es $F = \{\underline{a}\}$, entonces el campo de Euler con coeficientes $\underline{a}$ es tangente a la curva C.*

Finalmente, en el Capítulo 4 se aborda el problema de estudiar si el álgebra $k[X_1, \ldots, X_n]/\mathcal{I}(C)$ asociada a una curva monomial es, al igual que en el caso de curvas monomiales irreducibles, un álgebra de semigrupo. El propósito último de esto es encontrar una forma combinatoria de estudiar este álgebra (y así, por ejemplo, los sistemas minimales de generadores del ideal, su resolución libre minimal, sus sicigeas...) de manera análoga a lo que se hace para curvas irreducibles ([Bre], [BCMP2], [CG],...).

El primer problema para ello es construir un semigrupo asociado a una curva monomial. Esto se hace de forma natural en el caso de curvas cuyo ideal asociado es del tipo $I_+(\rho)$, considerando el semigrupo asociado al retículo:

Definición 4.1.12 *Sean* $\underline{h} \in \mathbb{Z}^n_{\geq 0}$ *un vector no nulo tal que* m.c.d.$\{h_i \mid h_i \neq 0\} = 1$, L *un subretículo de* $\mathbb{Z}^n$ *de rango* $n-1$ *tal que* $\mathrm{Sat}\ L = \langle \underline{h} \rangle^{\perp}$ *y* $\underline{\alpha} \in \mathbb{Z}^n$ *tal que* $\underline{h}\,\underline{\alpha} = 1$. *Consideremos el homomorfismo,*

$$\begin{array}{rcl} \overline{\varphi} : \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \oplus \mathrm{Sat}\ L/L \\ \underline{m} & \longmapsto & (\underline{m}\,\underline{h}, \underline{m} - (\underline{m}\,\underline{h})\underline{\alpha} + L) \end{array} .$$

Sea $\{\underline{e}_i\}_{i=1}^n$ *la base canónica de* $\mathbb{Z}^n$. *Llamaremos semigrupo asociado a* L *al semigrupo* $S_L = \overline{\varphi}((\mathbb{Z}_{\geq 0})^n)$. *Denotaremos por* Λ_L *al sistema de generadores de* S_L, $\Lambda_L = \{g_1, \ldots , g_n\}$ *siendo* $g_i := \overline{\varphi}(\underline{e}_i) = (h_i, t(g_i))$ *para todo* i.

Dado que el ideal de una curva monomial admite (según el Teorema 1.5.11) una descomposición "celular" como intersección de ideales que, esencialmente, son del tipo anterior, los semigrupos asociados a los retículos que aparecen en esta descomposición nos permiten definir en 4.2.21, un semigrupo asociado a una curva monomial C, marcando en él un sistema de generadores con n elementos. Nos limitaremos aquí, por simplicidad, a explicar el caso de una curva monomial cuyas componentes pasan todas por el origen. Si $C = C_1 \cup \ldots \cup C_r$ es su descomposición celular (cada C_i es unión de componentes irreducibles con la misma célula asociada, $\mathcal{Z}_i$), S_i es el semigrupo asociado, según la definición anterior, a C_i y se define $\widetilde{S}_i = S_i \cup \{\infty\}$, se tiene:

Definición 4.2.21 *Llamaremos semigrupo asociado a la curva* C *al subsemigrupo de* $\widetilde{S}_1 \times \ldots \times \widetilde{S}_r$ *generado por los elementos,*

$$\begin{array}{rc} \underline{g}_1 = & (g_{11} \cdots g_{1\,r}) \\ \vdots & \vdots \\ \underline{g}_n = & (g_{n1} \cdots g_{n\,r}) \end{array}$$

donde

$$g_{ij} = \left\{ \begin{array}{ll} (h_{ji}, t(g_{ij})) & si\ i \in \mathcal{Z}_j \\ \infty & si\ (i \notin \mathcal{Z}_j) \end{array} \right. .$$

Resulta que asignando a X_i grado $\underline{g}_i$, se obtiene una graduación en $k[X_1, \ldots , X_n]$ para la cuál $\mathcal{I}(C)$ es homogéneo, y además se construye, para cada $\underline{\gamma} \in S$ una subálgebra $A_{\underline{\gamma}}$ de $A = k^r$ y la k-álgebra S-graduada $\widetilde{A}_C = \bigoplus_{\underline{\gamma} \in S} A_{\underline{\gamma}} \chi^{\underline{\gamma}} \subseteq A[S]$, probándose lo siguiente (los elementos λ_{ij} del enunciado se construyen también asociados a la curva):

Corolario 4.2.39 *Sean C una curva monomial, S el semigrupo asociado a C y $\{\underline{g}_1, \dots, \underline{g}_n\}$ el sistema de generadores de S dado en la Definición 4.2.21. Entonces, si I es el ideal asociado a C, el homomorfismo $\Psi : k[X]/I \to \widetilde{A}_C / \langle \varepsilon\chi^{\underline{\infty}} \rangle$ dado por $\Psi(X_i + I) = (\lambda_{1i}, \dots, \lambda_{ri})\chi^{\underline{g}_i} + \langle \varepsilon\chi^{\underline{\infty}} \rangle$ es un isomorfismo.*

Previamente a este resultado se demuestra otro similar para el caso en que se cumple determinada hipótesis, (H) (Corolario 4.2.29). La particularidad es que la condición impuesta sobre la curva hace que la estructura de k-álgebra S-graduada sea ahora más sencilla, lo cual indica que en casos particulares el resultado 4.2.39 puede ser simplificado, facilitando una mejor comprensión de la k-álgebra. En todo caso, queda abierto el problema de aprovechar el carácter combinatorio de la estructura encontrada para profundizar en el estudio de la curva: sistemas minimales de generadores, sicigeas...

Para finalizar se incluyen dos apéndices al capítulo 4. En el primero de ellos nos planteamos la viabilidad del lema de Nakayama en los anillos S-graduados (siendo S el semigrupo asociado a una curva monomial), encontrando una versión débil del mismo. Vemos también un ejemplo de un ideal de curva monomial con dos sistemas minimales de generadores con distinto número de elementos. En el segundo apéndice, el estudio de la hipótesis (H) anteriormente mencionada sirve de excusa para estudiar alguna cosa nueva sobre los ideales de carácter parcial.

Capítulo 1

Ideales binomiales

El estudio realizado en esta tesis es relativo a variedades de dimensión uno cuyo ideal radical asociado es binomial, siendo la condición de binomial fundamental en su desarrollo. Para poder entender y justificar los métodos utilizados, es necesario conocer algunos aspectos de la teoría combinatoria sobre ideales binomiales desarrollada por Eisenbud y Sturmfels en [ES], labor que realizaremos en este capítulo.

1.1 Órdenes monomiales y bases de Gröbner

Para poder demostrar los resultados referentes a ideales binomiales que ocupan esta sección es necesario utilizar métodos de bases de Gröbner. Por ello, vamos a comenzar mencionando alguno de los resultados relativos a las mismas. Sus demostraciones se pueden encontrar, por ejemplo, en los capítulos 2 y 3 de [CLO1].

Cuando no dé lugar a dudas, denotaremos por $k[X]$ el anillo de polinomios en n indeterminadas $k[X_1, \ldots, X_n]$. Dado $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, denotaremos por $X^{\underline{\alpha}}$ el *monomio* $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, y dado $\lambda \in k$ diremos que $\lambda X^{\underline{\alpha}}$ es un *término* de $k[X]$. A un orden $<$ en $(\mathbb{Z}_{\geq 0})^n$, le asociaremos un orden en el conjunto de los monomios de $k[X]$, que denotaremos igual, siguiendo el criterio $X^{\underline{\alpha}} < X^{\underline{\beta}} \Leftrightarrow \underline{\alpha} < \underline{\beta}$.

Definición 1.1.1 *Un orden monomial sobre $k[X_1, \ldots, X_n]$ es cualquier relación binaria $<$ sobre $(\mathbb{Z}_{\geq 0})^n$ o, equivalentemente, cualquier relación sobre el conjunto de los monomios de $k[X_1, \ldots, X_n]$, cumpliendo:*

1. *$<$ es un buen orden sobre $(\mathbb{Z}_{\geq 0})^n$.*

2. Si $\underline{\alpha} < \underline{\beta}$ entonces $\underline{\alpha} + \underline{\gamma} < \underline{\beta} + \underline{\gamma}$ para todo $\underline{\gamma} \in (\mathbb{Z}_{\geq 0})^n$.

Definición 1.1.2 *Sea $<$ un orden monomial sobre $k[X]$. Dados un conjunto finito de vectores de $\mathbb{Z}^n$, Γ, y un polinomio $f = \sum_{\underline{\alpha} \in \Gamma} a_{\underline{\alpha}} X^{\underline{\alpha}} \in k[X]$ distinto de 0, denotaremos:*

- $\mathrm{LM}(f) = X^{\underline{\alpha}^*}$, *donde* $\underline{\alpha}^* = \max\,\{\underline{\alpha} \in \Gamma \mid a_{\underline{\alpha}} \neq 0\}$.
- $\mathrm{LT}(f) = a_{\underline{\alpha}^*} X^{\underline{\alpha}^*}$. *Diremos que* $\mathrm{LT}(f)$ *es el término principal de* f.

Y dado un ideal $I \subset k[X]$ denotaremos

- $\mathrm{in}(I) = \langle \{\mathrm{LT}(f) \mid f \in I\} \rangle$.

Definición 1.1.3 *Se dice que un conjunto finito de polinomios de un ideal I, $G = \{g_1, \ldots, g_r\}$, es una base de Gröbner de I para el orden monomial $<$ si $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle = \mathrm{in}(I)$.*

Proposición 1.1.4 *Si G es una base de Gröbner de un ideal $I \subset k[X]$ para un orden monomial $<$, entonces G es un sistema de generadores de I.*

En el resto de la sección se supondrá fijado un orden monomial $<$ sobre $k[X]$. Este orden nos va a permitir definir una operación de división para polinomios en varias variables.

Proposición 1.1.5 *Sea $F = \{f_1, \ldots, f_s\}$ un conjunto de polinomios en $k[X]$. Para cada $f \in k[X]$ existen $a_1, \ldots, a_s, r \in k[X]$ cumpliendo:*

P1 $f = a_1 f_1 + \ldots + a_s f_s + r$.

P2 *Si $r \neq 0$, ninguno de los monomios de r es divisible por ninguno de los términos $\mathrm{LT}(f_1)$, ..., $\mathrm{LT}(f_s)$.*

La demostración de esta proposición es constructiva y se realiza mediante el algoritmo de división.

Algoritmo 1.1.6 (Algoritmo de división)
Input: $F = \{f_1, \ldots, f_s\}, f$
Output: $a_1, \ldots, a_s, r$

```
a_1 := 0; ... ; a_s := 0; r := 0
p := f
WHILE p ≠ 0 DO
    i := 1
```

divisionhecha:=false
WHILE $i \leq s$ *AND divisionhecha=false DO*
  IF $\mathrm{LT}(f_i)$ *divide a* $\mathrm{LT}(p)$ *THEN*
    $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
    $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
    divisionhecha=true
  ELSE
    $i := i + 1$
IF divisionhecha=false THEN
  $r := r + \mathrm{LT}(p)$
  $p := p - \mathrm{LT}(p)$

Teorema 1.1.7 *Si* $F = \{f_1, \ldots, f_s\}$ *es un conjunto de polinomios de* $k[X]$ *y* f *es un polinomio cualquiera, entonces el algoritmo de división aplicado a* (F, f) *devuelve polinomios* $a_1, \ldots, a_s, r$ *cumpliendo P1 y P2.*

En general no hay unicidad de a_1, ... ,a_s, r, cumpliendo las condiciones P1 y P2. Es claro, por ejemplo, que el algoritmo depende de la forma en que se ordenen $f_1, \ldots, f_s$. En lo que sigue, llamaremos resto de la división de f por el conjunto *ordenado* $F = \{f_1, \ldots, f_s\}$ al polinomio r que proporciona el Algoritmo 1.1.6 aplicado a (F, f), y lo denotaremos por $r = \overline{f}^F$.

Proposición 1.1.8 *Sea* $G = \{g_1, \ldots, g_s\}$ *una base de Gröbner de un ideal* $I \subset k[X]$ *y sea* $f \in k[X]$*. Entonces, existe único polinomio* $r \in k[X]$ *con las siguientes propiedades:*

1. *Ningún término de* r *es divisible por ninguno de los términos* $\mathrm{LT}(g_1)$, ... , $\mathrm{LT}(g_s)$.

2. $f - r \in I$.

En particular, r *es el resto de la división de* f *por* G *(ordenado de cualquier forma), es decir* $r = \overline{f}^G$*. Además* $f \in I$ *si y sólo si* $\overline{f}^G = 0$.

Definición 1.1.9 *Dados una base de Gröbner* G *del ideal* $I \subset k[X]$ *y un polinomio* f *de* $k[X]$*, llamaremos forma normal de* f *módulo* G *al resto* $\overline{f}^G$ *(que, por 1.1.8, no depende de la forma en que se ordene* G*).*

Proposición 1.1.10 *Se considera el polinomio* $f = \sum_{i=1}^t f_i \in k[X]$ *donde los* f_i *son polinomios en* $k[X]$*. Si* G *es una base de Gröbner de* I*, entonces* $\overline{f}^G = \sum_{i=1}^t \overline{f_i}^G$.

Dem. Supongamos que G es el conjunto de polinomios $G = \{g_1, \ldots, g_s\}$. Aplicando la Proposición 1.1.5 a f_i y G, para cada $i \in \{1, \ldots, t\}$, se obtiene $f_i = q_{i1}g_1 + \ldots + q_{is}g_s + r_i$, donde ningún término de r_i es divisible por ninguno de los términos principales de g_j para $j \in \{1, \ldots, s\}$, es decir $r_i = \overline{f_i}^G$. Se tiene, entonces

$$f = (\sum_{i=1}^{t} g_{i1})g_1 + \ldots + (\sum_{i=1}^{t} g_{is})g_s + \sum_{i=1}^{t} r_i.$$

Además $\sum_{i=1}^{t} r_i$ es un polinomio cuyos términos no son divisibles por ninguno de los términos principales de los g_i, luego, debido a la unicidad de la Proposición 1.1.8, $\sum_{i=1}^{t} r_i = \overline{f}^G$.

□

Para aplicar en la práctica la Proposición 1.1.8, es imprescindible obtener un método para construir bases de Gröbner para cualquier ideal de polinomios. Este problema se soluciona con el algoritmo de Buchberger, basado en la caracterización de dichas bases mediante condiciones que afectan a los S-polinomios.

Definición 1.1.11 *Dados dos polinomios f y g en $k[X]$, se define el S-polinomio de f y g como:*

$$S(f,g) = \frac{X^{\underline{\gamma}}}{\mathrm{LT}(f)}f - \frac{X^{\underline{\gamma}}}{\mathrm{LT}(g)}g \quad \textit{donde} \quad X^{\underline{\gamma}} = \mathrm{m.c.m.}(\mathrm{LM}(f), \mathrm{LM}(g)).$$

Proposición 1.1.12 *Un conjunto de polinomios $G = \{g_1, \ldots, g_r\}$ de un ideal I es una base de Gröbner de dicho ideal si y sólo si $\overline{S(g_i, g_j)}^G = 0$ para cualesquiera $i, j \in \{1, \ldots, r\}$.*

Teniendo en cuenta este resultado se justifica el cálculo de bases de Gröbner para ideales del anillo de polinomios usando el algoritmo de Buchberger.

Algoritmo 1.1.13 (Algoritmo de Buchberger)
Input: $F = \{f_1, \ldots, f_s\}$
Output: $G = \{g_1, \ldots, g_r\}$

$G := F$
REPEAT
$G' := G$

FOR cada par $\{p, q\}$, $p \neq q$, *en* G' *DO*
  $S := \overline{S(p,q)}^{G'}$
  IF $S \neq 0$ *THEN* $G := G \cup \{S\}$
UNTIL $G = G'$

Teorema 1.1.14 *Si el conjunto* $F = \{f_1, \ldots, f_s\}$ *es un sistema de generadores del ideal* $I \subset k[X]$*, entonces el algoritmo de Buchberger aplicado al conjunto* F *devuelve, en un número finito de pasos, una base de Gröbner para el ideal* I*.*

Fijado un orden monomial $<$ y un ideal I, no tenemos una única base de Gröbner de I. Sin embargo, si añadimos alguna condición adicional a las bases, tendremos asegurada la unicidad.

Definición 1.1.15 *Se dice que una base de Gröbner* G *es minimal cuando, para todo* $g \in G$*, se cumple que:*

- *Su término principal es un monomio* $(\mathrm{LT}(g) = \mathrm{LM}(g))$.
- $\mathrm{LT}(g) \notin \langle \{\mathrm{LT}(h) \mid h \in G - \{g\}\} \rangle$.

Lema 1.1.16 *Si* G *es base de Gröbner y* $\mathrm{LT}(g) \in \langle \mathrm{LT}(G - \{g\}) \rangle$ *entonces* $G - \{g\}$ *también es base de Gröbner.*

Definición 1.1.17 *Se dice que una base de Gröbner* G *es reducida cuando, para todo* $g \in G$*, se cumple:*

- *Su término principal es un monomio.*
- *Ningún término de* g *está en el ideal* $\langle \{\mathrm{LT}(h) \mid h \in G - \{g\}\} \rangle$.

Proposición 1.1.18 *Dados un orden monomial* $<$ *y un ideal* I*, existe una única base de Gröbner reducida de* I *para el orden* $<$.

La construcción de bases de Gröbner reducidas se realiza mediante el algoritmo de reducción.

Algoritmo 1.1.19 (Algoritmo de reducción)
Input: $G' = \{g_1, \ldots, g_t\}$
Output: $G^* = \{\tilde{g}_1, \ldots, \tilde{g}_t\}$
  $G^* := G'$
  $i := 1$

WHILE $i \leq t$ *DO*
$\tilde{g}_i := \overline{g_i}^{G^* - \{g_i\}}$
$G^* := (G^* - \{g_i\}) \cup \{\tilde{g}_i\}$
$i := i + 1$

Teorema 1.1.20 *Sea $G' = \{g_1, \ldots, g_t\}$ una base de Gröbner minimal del ideal $I \subset k[X]$ tal que todos los términos principales de los polinomios de G' tienen coeficiente 1. Entonces el algoritmo de reducción aplicado al conjunto G' devuelve la base de Gröbner reducida para el orden $<$ del ideal I.*

Por último, enunciaremos el teorema de eliminación para bases de Gröbner, resultado imprescindible para desarrollar la teoría de ideales binomiales.

Definición 1.1.21 *Dado un entero $0 \leq r \leq n$, diremos que un orden monomial $<$ sobre $k[X]$ es de eliminación de tipo r, si cualquier monomio de $k[X]$ que contenga alguna indeterminada de $\{X_{r+1}, \ldots, X_n\}$ es mayor que todos los monomios de $k[X_1, \ldots, X_r]$.*

Ejemplo 1.1.22 Consideremos el orden lexicográfico $<_{\text{lex}}$ en $k[X_1, \ldots, X_n]$ donde $X_1 <_{\text{lex}} X_2 <_{\text{lex}} \cdots <_{\text{lex}} X_n$; es decir, $X^{\underline{\alpha}} <_{\text{lex}} X^{\underline{\beta}}$ si la primera coordenada no nula desde la derecha del vector $\underline{\beta} - \underline{\alpha} \in \mathbb{Z}^n$ es positiva. Es claro que el orden monomial $<_{\text{lex}}$ es de eliminación de tipo r, para cualquier $r \in \{0, \ldots, n\}$.

Ejemplo 1.1.23 Dado un orden monomial $<$ en $k[X_1, \ldots, X_n]$, se define el orden monomial $<'$ en $k[X_1, \ldots, X_n, Z_1, \ldots, Z_n]$ por:

$$X^a Z^b <' X^c Z^d \iff \text{ o bien } Z^b < Z^d \text{ o bien } Z^b = Z^d \text{ y } X^a < X^c.$$

El orden $<'$ así definido es un orden de eliminación en $k[X, Z]$ de tipo n.

Teorema 1.1.24 (Teorema de eliminación) *Sean I un ideal del anillo de polinomios $k[X_1, \ldots, X_n]$ y G una base de Gröbner de I respecto a un orden monomial $<$ de eliminación de tipo r. Entonces, el conjunto*

$$G_r = G \cap k[X_1, \ldots, X_r]$$

es una base de Gröbner del ideal de eliminación $I \cap k[X_1, \ldots, X_r]$.

1.2 Ideales binomiales y bases de Gröbner

Al igual que ocurre con los ideales monomiales, se ha desarrollado toda una teoría que analiza las propiedades de los ideales binomiales del anillo de polinomios. El resto de este capítulo está destinado a detallar aquellos resultados de esta clase de ideales, esenciales en nuestro planteamiento de la teoría de curvas monomiales. Dichos resultados se pueden encontrar en el artículo "*Binomial Ideals*" [ES].

Llamaremos binomio de $k[X] = k[X_1, \dots, X_n]$ a cualquier polinomio que tenga como mucho dos términos. Es decir, polinomios de la forma $\lambda X^{\underline{m}} - \mu X^{\underline{n}}$ donde $\lambda, \mu \in k$ y $\underline{m}, \underline{n} \in (\mathbb{Z}_{\geq 0})^n$.

Definición 1.2.1 *Dado un ideal I del anillo de polinomios $k[X]$, diremos que I es binomial si admite un sistema de generadores formado por binomios.*

Fijemos un orden monomial $<$ sobre el anillo de polinomios $k[X]$.

Proposición 1.2.2 *Sea I un ideal binomial de $k[X]$ y sea G la base de Gröbner reducida de I para el orden $<$. Se cumple:*

(a) G está formada por binomios.

(b) La forma normal módulo G de un término de $k[X]$ es, de nuevo, un término.

Dem.

(a) Como I es un ideal binomial, admite un sistema de generadores formado por binomios. Aplicamos a dicho sistema los algoritmos de Buchberger y de reducción para la obtención de la base de Gröbner reducida de I (Algoritmos 1.1.13 y 1.1.19). Como tanto los S-polinomios como los restos de las divisiones de binomios por binomios siguen siendo binomios, obtenemos el resultado.

(b) En el algoritmo de división, cada división parcial de un término entre binomios devuelve un término (Algoritmo 1.1.6).

□

Corolario 1.2.3 *Sea I un ideal de $k[X]$. Son equivalentes:*

- *I es binomial (nótese que esta condición no depende de $<$).*

- *La base de Gröbner reducida de I para el orden monomial $<$ está formada por binomios.*

Corolario 1.2.4 *Si $I \subset k[X_1, \dots, X_n]$ es un ideal binomial, entonces, para $r \in \{0, \dots, n\}$ el ideal de eliminación $I \cap k[X_1, \dots, X_r]$ es binomial.*

Dem. Sea G la base de Gröbner de I para el orden lexicográfico con $X_1 < \ldots < X_n$. Se tiene que el conjunto $G_r := G \cap k[X_1, \dots, X_r]$ es una base de Gröbner del ideal de eliminación $I \cap k[X_1, \dots, X_r]$ (Teorema 1.1.24), y por tanto este es un ideal binomial.

□

Basándonos en estos resultados, podemos decir algo acerca de la intersección de ideales binomiales, que en general no resulta ser un ideal binomial. Sin embargo, sí se cumple que:

Corolario 1.2.5 *Si I, I', J_1, ... ,J_s son ideales de $k[X]$ cumpliendo que I, I' son binomiales y J_1, ... ,J_s son monomiales (generados por monomios), entonces*

$$(I + I') \cap (I + J_1) \cap \ldots \cap (I + J_s)$$

es un ideal binomial.

Dem. Supongamos que $s = 1$. Consideremos el anillo de polinomios $k[X_1, \dots, X_n, t]$ y el ideal $L = I + tI' + (1-t)J_1$, dentro de dicho anillo. Como L es binomial, su ideal de eliminación $L \cap k[X_1, \dots, X_n]$ es binomial (Corolario 1.2.4). Veamos que este es el ideal del enunciado. Si $f \in (I + I') \cap (I + J_1)$, entonces f se puede escribir $f = f_1 + g_1$, donde $f_1 \in I$ y $g_1 \in (I + I') \cap J_1$. Como $f = f_1 + tg_1 + (1-t)g_1$, escribiendo $g_1 = f^* + g^*$ con $f^* \in I$ y $g^* \in I'$, se tiene $f = f_1 + tf^* + tg^* + (1-t)g_1$. Además, teniendo en cuenta que $f_1 + tf^* \in Ik[X_1, \dots, X_n, t]$, $g^* \in I'$ y $g_1 \in J_1$, se tiene que $f \in L \cap k[X_1, \dots, X_n]$. Recíprocamente, si $f(X)$ es un polinomio de $L \cap k[X_1, \dots, X_n]$, existen polinomios $f_1(X, t)$, $f_2(X, t)$ y $f_3(X, t)$ en los ideales I, I' y J_1 extendidos al anillo $k[X_1, \dots, X_n, t]$, cumpliendo

$$f(X) = f_1(X, t) + tf_2(X, t) + (1-t)f_3(X, t).$$

Haciendo en la expresión $t = 0$ y teniendo en cuenta que si $h(X, t)$ pertenece a $\mathcal{J}k[X_1, \dots, X_n, t]$, donde $\mathcal{J}$ es un ideal de $k[X]$, entonces $h(X, \lambda) \in \mathcal{J}$ para cualquier $\lambda \in k$, obtenemos que $f(X)$ pertenece a $I + J_1$. Haciendo ahora $t = 1$, tenemos $f(X) \in I + I'$.

Sea ahora $s > 1$. El resultado se deduce de escribir

$$\begin{aligned} (I+I') \cap (I+J_1) \cap \ldots \cap (I+J_s) &= \\ = \big(I + ((I+I') \cap (I+J_1) \cap \ldots \cap (I+J_{s-1}))\big) \cap (I+J_s) & \end{aligned}$$

y aplicar hipótesis de inducción.

$\square$

Corolario 1.2.6 *Si I es un ideal binomial de $k[X]$ y $J_1, \ldots ,J_s$ son ideales monomiales de $k[X]$, se cumple:*

1. *La intersección $(I + J_1) \cap \ldots \cap (I + J_s)$ está generada por monomios módulo I.*

2. *Cualquier monomio de la suma $I + J_1 + \ldots + J_s$ está en uno de los ideales $I + J_i$. En particular, si $m, m_1, \ldots , m_s$ son monomios y $m \in I + \langle m_1, \ldots , m_s\rangle$ entonces $m \in I + \langle m_i\rangle$ para algún $i \in \{1, \ldots , s\}$.*

Dem. Sea $G = \{g_1, \ldots , g_r\}$ la base de Gröbner reducida de I respecto de un orden monomial $<$ sobre $k[X]$. Sea μ el conjunto de monomios de $k[X]$ que no están en $\mathrm{in}(I)$, denominados monomios estándar módulo I. Denotaremos por $\overline{\mu}$ a la imagen de μ por la aplicación de paso al cociente módulo I. Es cierto que el conjunto $\overline{\mu}$ es base del k-espacio vectorial $k[X]/I$. En efecto, sea f un polinomio que no está en I y denotemos por r la forma normal de f módulo G. Sabemos que $\mathrm{in}(I) = \langle \mathrm{LT}(g_1), \ldots , \mathrm{LT}(g_r)\rangle$ y que ningún término de r es divisible por ninguno de los términos $\mathrm{LT}(g_i)$, luego ninguno de los términos de r están en $\mathrm{in}(I)$. Por lo tanto, si el conjunto $\{\lambda_1 m_1, \ldots , \lambda_t m_t\}$ son los términos de r, entonces $f + I = \sum_{i=1}^{t} \lambda_i m_i + I$, donde $m_i + I \in \overline{\mu}$ para todo $i \in \{1, \ldots , t\}$. Luego $\overline{\mu}$ es sistema de generadores de $k[X]/I$. Además, es claro que se trata de un conjunto libre.

Como para cada $i \in \{1, \ldots , s\}$ el ideal J_i es monomial, entonces, si denotamos por B_i al conjunto de monomios de J_i, se tiene que B_i es un sistema de generadores de J_i y pasando al cociente módulo I, el conjunto $\overline{B_i}$ genera $\overline{J_i}$. Aplicando la Proposición 1.2.2 (b), se deduce que todas las clases en $\overline{B_i}$ o tienen un representante que es un término que no está en $\mathrm{in}(I)$ o son la clase cero, luego $\overline{B_i}\backslash\{\overline{0}\} \subset \overline{\mu}$ y por tanto $\overline{B_i}\backslash\{\overline{0}\}$ es base de $\overline{J_i}$. Además $\bigcap_{i=1}^{s}(\overline{B_i}\backslash\{\overline{0}\})$ es una base de $\bigcap_{i=1}^{s} \overline{J_i}$ y el apartado 1 queda demostrado.

Utilizando, de nuevo, la Proposición 1.2.2 (b), si $m + I$ es un monomio contenido en $I + \sum_{i=1}^{s} J_i$ entonces su clase módulo I está representada por un monomio estándar. Por lo tanto $m + I \in \sum_{i=1}^{s} \overline{J_i} \cap \overline{\mu}$. Puesto que $\bigcup_{i=1}^{s} \overline{B_i} \backslash \{\overline{0}\}$ es una base de $\sum_{i=1}^{s} \overline{J_i}$ y el conjunto $\{m + I\} \cup (\bigcup_{i=1}^{s} \overline{B_i} \backslash \{\overline{0}\})$ es libre (por estar contenido en una base, $\overline{\mu}$), $m + I \in \bigcup_{i=1}^{s} \overline{B_i}$; es decir, existe $i \in \{1, \ldots, s\}$ tal que $\overline{m} \in \overline{B_i}$ y entonces $m \in I + J_i$.

□

Corolario 1.2.7 *Sean $I \subset k[X]$ un ideal binomial, $m_1, \ldots, m_t$ monomios y $f_1, \ldots, f_t$ polinomios tales que $\sum_{i=1}^{t} f_i m_i \in I$. Si llamamos f_{ij} a los términos de f_i, entonces, para todos i, j, $f_{ij} m_i \in I$ o existen términos f_{ij} y $f_{i'j'}$ distintos y un escalar $a \in k^*$ tales que $f_{ij} m_i + a f_{i'j'} m_{i'} \in I$. En particular, para cualquier monomio m, los ideales cocientes $(I : m)$ y $(I : m^{\infty}) := \bigcup_{s=1}^{\infty} (I : m^s)$, son binomiales.*

Dem. Sean $<$ un orden monomial sobre $k[X]$, G la base de Gröbner reducida de I respecto de $<$ y $f = \sum_{i=1}^{t} f_i m_i \in I$. Como $f \in I$ entonces $\overline{f}^G = 0$ y aplicando la Proposición 1.1.10 se tiene $\sum_{i,j} \overline{f_{ij} m_i}^G = 0$. Si denotamos $\mu_{ij} := \overline{f_{ij} m_i}^G$, los polinomios μ_{ij} son términos (Proposición 1.2.2) y $\sum \mu_{ij} = 0$. Tenemos, por tanto, una suma de términos igual a cero, con lo cual, dado (i, j) o bien $\mu_{ij} = 0$; es decir, $f_{ij} m_i \in I$, o bien existen $(i', j') \neq (i, j)$ y $a \in k^*$ tales que $\mu_{ij} = a \mu_{i'j'}$; es decir, $f_{ij} m_i - a f_{i'j'} m_{i'} \in I$.

Además, los ideales $(I : m)$ y $(I : m^{\infty})$ son binomiales. En efecto, sea $f \in (I : m)$, $f = \sum_{i=1}^{r} f_i$ donde los f_i son términos. Sea B el conjunto de binomios de $(I : m)$, incluidos monomios, y $r > 1$. Puesto que $\sum_{i=1}^{r} f_i m \in I$, por el enunciado anterior, o bien $f_r \in (I : m)$, en cuyo caso $f = \tilde{f} + f_r$ con $f_r \in B$ y $\tilde{f} = \sum_{i=1}^{r-1} f_i \in (I : m)$, o bien existen $j < r$ y $a \in k^*$ con $f_r + a f_j \in B$, en cuyo caso $f = \tilde{f} + (f_r + a f_j)$ con $f_r + a f_j \in B$ y $\tilde{f} = f_1 + \ldots + (1 - a) f_j + \ldots + f_{r-1} \in (I : m)$. En ambos casos, aplicando hipótesis de inducción sobre el número de términos a $\tilde{f}$, polinomio que tiene como mucho $r-1$ términos, demostramos que f está generado por polinomios de B.

□

El último resultado técnico que necesitamos para el estudio posterior de los ideales binomiales del anillo de polinomios y del anillo de polinomios de Laurent, está recogido en la siguiente proposición.

Proposición 1.2.8 *Sean I un ideal binomial y M un ideal monomial en $k[X]$. Si $f \in I + M$ y f' es la suma de los términos de f que no están individualmente contenidos en $I + M$, entonces $f' \in I$.*

Dem. Por comodidad en la notación, podemos suponer que $f = f'$. Sean $<$ un orden monomial sobre $k[X]$, G la base de Gröbner reducida de I respecto de $<$ y G_M un conjunto finito de monomios que generen el ideal engendrado por todos los monomios contenidos en $I + M$. G_M es base de Gröbner de dicho ideal. Aplicando la Proposición 1.1.12, $G \cup G_M$ es base de Gröbner de $I + M$ ya que:

- Los S-polinomios que se forman con binomios de G, se reducen a cero módulo G, y por lo tanto también lo harán módulo $G \cup G_M$. Lo mismo ocurre con los S-polinomios que se formen con monomios de G_M, ya que G_M es base de Gröbner del ideal engendrado por todos los monomios contenidos en $I + M$.

- Sean $g \in G$ y $m \in G_M$. El S-polinomio $S(g, m)$ produce un monomio que pertenece a $I + M$. Pero G_M es una base de Gröbner del ideal generado por estos monomios, luego $\overline{S(g,m)}^{G_M} = 0$ y por tanto se tiene $\overline{S(g,m)}^{G \cup G_M} = 0$.

Sea t un término de f. Por la Proposición 1.2.2, $\overline{t}^{G \cup G_M}$ es un término no nulo, pues ninguno de los términos de f están en $I + M$ (por hipótesis). Además, al ir dividiendo t por binomios de G se obtienen como restos parciales términos que tampoco pueden pertenecer a $I + M$, y por lo tanto tampoco pueden dividirse por ningún monomio de M. Luego en el proceso de división de t por $G \cup G_M$ sólo intervienen polinomios de G, y por tanto $\overline{t}^{G \cup G_M} = \overline{t}^G$ para todos los términos de f. Aplicando la Proposición 1.1.10, $\overline{f}^G = \overline{f}^{G \cup G_M}$, que vale cero ya que $f \in I + M$. Por lo tanto $f \in I$.

□

1.3 El anillo de polinomios de Laurent

El estudio de los ideales binomiales del anillo de polinomios de Laurent nos va a aportar información privilegiada para obtener resultados combinatorios de ideales binomiales del anillo de polinomios ([ES]).

Sea k un cuerpo; se considera el anillo $k[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]$, denominado anillo de polinomios de Laurent en n indeterminadas con coeficientes en k. En lo que sigue lo denotaremos por $k[X^{\pm}]$ o $k[\mathbb{Z}^n]$. Veamos cómo caracterizar los ideales binomiales de Laurent, es decir ideales de $k[X^{\pm}]$ que admitan un sistema de generadores formado por binomios.

Definición 1.3.1 *Llamaremos retículo a cualquier $\mathbb{Z}$-módulo libre de rango finito.*

Definición 1.3.2 *Dado un subretículo L de $\mathbb{Z}^n$, llamaremos saturación de L al retículo*

$$\mathrm{Sat}\ L := \{\underline{m} \in \mathbb{Z}^n \mid \exists d \in \mathbb{Z} \text{ con } d\underline{m} \in L\}.$$

Además, diremos que L es saturado si $L = \mathrm{Sat}\ L$.

Definición 1.3.3 *Un carácter parcial sobre $\mathbb{Z}^n$ es un homomorfismo de grupos $\rho : L_\rho \to k^*$, donde L_ρ es algún subretículo de $\mathbb{Z}^n$. Diremos que ρ es saturado cuando L_ρ lo sea.*

Definición 1.3.4 *Dado un carácter parcial ρ, se define el ideal binomial de Laurent asociado a ρ como*

$$I(\rho) := \langle \{X^{\underline{m}} - \rho(\underline{m}) \mid \underline{m} \in L_\rho\} \rangle.$$

Estos no sólo son un tipo de ideales binomiales de $k[X^\pm]$, sino que constituyen el conjunto de todos sus ideales binomiales propios. Este importante hecho así como ciertas propiedades de los ideales asociados a caracteres, se tratan en el siguiente teorema. Para entender los ideales binomiales de $k[X^\pm]$, hay que tener en cuenta que, salvo producto por unidades, cualquier binomio no nulo y no unidad en $k[X^\pm]$ puede ser escrito de la forma $X^{\underline{m}} - c_{\underline{m}}$ donde $\underline{m} \in \mathbb{Z}^n$ y $c_{\underline{m}} \in k^*$.

Teorema 1.3.5 *Sea $k[X^\pm]$ el anillo de polinomios de Laurent sobre k. Se cumple:*

1. *Si $\rho : L_\rho \to k^*$ es un carácter parcial y $X^{\underline{m}} - c \in I(\rho)$, entonces $\underline{m} \in L_\rho$ y $c = \rho(\underline{m})$.*

2. *Si I es un ideal binomial propio de $k[X^\pm]$, entonces existe un único carácter parcial ρ sobre $\mathbb{Z}^n$ con $I = I(\rho)$.*

3. *Si $\underline{m}_1, \ldots, \underline{m}_r$ es una base de L_ρ, los binomios $X^{\underline{m}_1} - \rho(\underline{m}_1), \ldots, X^{\underline{m}_r} - \rho(\underline{m}_r)$ generan $I(\rho)$ y forman una sucesión regular en $k[X^\pm]$. Además,*

$$\mathrm{ht}(I(\rho)) = \mathrm{rango}(L_\rho).$$

Supongamos ahora que k es algebraicamente cerrado.

4. *$I(\rho)$ es primo si y sólo si L_ρ es saturado.*

5. *Sean $p \geq 0$ la característica de k y $\rho : L_\rho \to k^*$ un carácter parcial sobre $\mathbb{Z}^n$. Si L es un subretículo de $\mathbb{Z}^n$ tal que el grupo L/L_ρ es finito de orden g primo con p, entonces existen exactamente g extensiones distintas $\tilde{\rho}_1, \ldots, \tilde{\rho}_g$ de ρ a L, cumpliéndose además*

$$I(\rho) = \bigcap_{i=1}^{g} I(\tilde{\rho}_i).$$

Si g es una potencia de p, entonces existen una única extensión ρ', de ρ a L, y una filtración por $k[X^\pm]$-módulos de $k[X^\pm]/I(\rho)$,

$$k[X^\pm]/I(\rho) = M_0 \supset M_1 \supset \ldots \supset M_g = 0$$

tal que $M_i/M_{i+1} \cong k[X^\pm]/I(\rho')$ para $0 \leq i \leq g-1$.

Dem.
1. Sea J el ideal de $k[X_1, \ldots, X_n, Z_1, \ldots, Z_n]$ generado por $\{X_i Z_i - 1 \mid i = 1, \ldots, n\}$. Con la identificación $k[X^\pm] = k[X_1, \ldots, X_n, Z_1, \ldots, Z_n]/J$, sea $I'(\rho)$ el ideal de $k[X, Z]$ (conteniendo a J), tal que $I(\rho) = I'(\rho)/J$. Entonces, el conjunto

$$G = \{X^a Z^b - \rho(a - b - c + d) X^c Z^d \mid a, b, c, d \in \mathbb{N}^n \text{ y } a - b - c + d \in L_\rho\},$$

es sistema de generadores de $I'(\rho)$. En efecto, como

$$\begin{aligned} &(X^a Z^b - \rho(a - b - c + d) X^c Z^d) + J = \\ &= \ X^{c-d}(X^{a-b-c+d} - \rho(a - b - c + d)) \in I(\rho), \end{aligned}$$

se tiene $G \subseteq I'(\rho)$. Por otra parte, dado $\underline{m} \in L_\rho$ pongamos $\underline{m} = \underline{m}_+ - \underline{m}_-$ donde $\underline{m}_+, \underline{m}_- \in (\mathbb{Z}_{\geq 0})^n$. Entonces $X^{\underline{m}} - \rho(\underline{m}) = X^{\underline{m}_+} Z^{\underline{m}_-} - \rho(\underline{m}) + J$, de donde $I'(\rho)$ está generado por $\{X^{\underline{m}_+} Z^{\underline{m}_-} - \rho(\underline{m}_+ - \underline{m}_-) \mid \underline{m} \in L_\rho\} \cup \{X_i Z_i - 1 \mid 1 \leq i \leq n\}$, que es un subconjunto de G.

Además, si $<$ es cualquier orden monomial en $k[X, Z]$, G es una base de Gröbner (aunque infinita) de $I(\rho)$ para dicho orden. Para demostrarlo consideremos dos polinomios cualesquiera de G:

$$\begin{aligned} p_1 &= X^{a_1} Z^{b_1} - \rho(a_1 - b_1 - c_1 + d_1) X^{c_1} Z^{d_1} \\ p_2 &= X^{a_2} Z^{b_2} - \rho(a_2 - b_2 - c_2 + d_2) X^{c_2} Z^{d_2} \ . \end{aligned}$$

Podemos suponer que los términos principales para $<$ de estos dos polinomios son los que aparecen en primer lugar. Sean $a = \max(\mathrm{a}_1, \mathrm{a}_2)$ y $b = \max(\mathrm{b}_1, \mathrm{b}_2)$. El S-polinomio de p_1 y p_2 es

$$S(p_1, p_2) = X^{a-a_1} Z^{b-b_1} p_1 - X^{a-a_2} Z^{b-b_2} p_2 = X^{\tilde{a}} Z^{\tilde{b}} - \rho(\tilde{a} - \tilde{b} - \tilde{c} + \tilde{d}) X^{\tilde{c}} Z^{\tilde{d}}$$

donde $\tilde{a} = a - a_2 + c_2$, $\tilde{b} = b - b_2 + d_2$, $\tilde{c} = a - a_1 + c_1$ y $\tilde{d} = b - b_1 + d_1$. Ahora bien, $\tilde{a} - \tilde{b} - \tilde{c} + \tilde{d} \in L_\rho$, luego $S(p_1, p_2) \in G$ y en consecuencia G es base de Gröbner (el resultado de la Proposición 1.1.12 también es válido para conjuntos infinitos).

Sea $X^{\underline{m}} - c$ un binomio cualquiera de $I(\rho)$. Si consideramos como antes, $\underline{m} = \underline{m}_+ - \underline{m}_-$ donde $\underline{m}_+, \underline{m}_- \in (\mathbb{Z}_{\geq 0})^n$, entonces $X^{\underline{m}} - c = X^{\underline{m}_+} Z^{\underline{m}_-} - c + J$, es decir, $X^{\underline{m}_+} Z^{\underline{m}_-} - c \in I'(\rho)$. Como G es base de Gröbner de $I'(\rho)$, $\overline{X^{\underline{m}_+} Z^{\underline{m}_-}}^G = c$. Pero en el proceso de división por G de $X^{\underline{m}_+} Z^{\underline{m}_-}$, los restos en cada paso, y por tanto el resto final, tienen la forma $\rho(a - b - c + d) X^{\underline{m}_+ - a + c} Z^{\underline{m}_- - b + d}$ donde $a - b - c + d \in L_\rho$. En consecuencia, tendremos $c = \rho(a - b - c + d) X^{\underline{m}_+ - a + c} Z^{\underline{m}_- - b + d}$ con $a - b - c + d \in L_\rho$. Luego $\underline{m}_+ - a + c = 0$, $\underline{m}_- - b + d = 0$ y $c = \rho(a - b - c + d)$. Por lo tanto $\underline{m} = a - b - c + d \in L_\rho$ y $c = \rho(\underline{m})$.

2. Por ser I un ideal binomial propio de $k[X^\pm]$, está generado por binomios de la forma $X^{\underline{m}} - c_{\underline{m}}$ con $\underline{m} \in \mathbb{Z}^n$ y $c_{\underline{m}} \in k^*$, y por tanto, si definimos $L_\rho = \{\underline{m} \in \mathbb{Z}^n \mid \exists c_{\underline{m}} \in k^* \text{ con } X^{\underline{m}} - c_{\underline{m}} \in I\}$, entonces $L_\rho \neq \emptyset$. Además, es cierta la igualdad

$$X^{\underline{m}+\underline{m}'} - c_{\underline{m}} c_{\underline{m}'} = (X^{\underline{m}} - c_{\underline{m}}) X^{\underline{m}'} + c_{\underline{m}} (X^{\underline{m}'} - c_{\underline{m}'}), \tag{1.1}$$

y por tanto si $X^{\underline{m}} - c_{\underline{m}}$ y $X^{\underline{m}'} - c_{\underline{m}'}$ son polinomios de I, entonces $X^{\underline{m}+\underline{m}'} - c_{\underline{m}} c'_{\underline{m}}$ está en I, luego L_ρ es un retículo. Además, el valor $c_{\underline{m}}$ tal que $X^{\underline{m}} - c_{\underline{m}} \in I$ es único para cada $\underline{m} \in L_\rho$, pues en caso contrario existirían dos binomios distintos $X^{\underline{m}} - c$, $X^{\underline{m}} - d$ en I, luego $c - d \in I$ en contra de que I es propio. Teniendo en cuenta esto, se puede considerar la aplicación $\rho : L_\rho \to k^*$ definida por $\rho(\underline{m}) = c_{\underline{m}}$, que resulta ser un carácter parcial (ecuación 1.1). Por lo tanto, hemos encontrado un carácter parcial ρ cumpliendo:

$$I = \langle \{X^{\underline{m}} - c_{\underline{m}} \mid \underline{m} \in L_\rho\} \rangle = \langle \{X^{\underline{m}} - \rho(\underline{m}) \mid \underline{m} \in L_\rho\} \rangle = I(\rho).$$

La unicidad de ρ se deduce del apartado 1.

3. Consideremos una base de L_ρ, $\{\underline{m}_1, \ldots, \underline{m}_r\}$, y un binomio de $I(\rho)$,

$X^{\underline{m}} - \rho(\underline{m})$. Como $\underline{m} \in L_\rho$, existen enteros a_i con $\underline{m} = \sum_{i=1}^r a_i \underline{m}_i$. Así

$$X^{\underline{m}} - \rho(\underline{m}) = X^{a_1 \underline{m}_1 + \ldots + a_r \underline{m}_r} - \rho(\sum_{i=1}^r a_i m_i).$$

De la ecuación (1.1) se deduce entonces que para comprobar que el conjunto $C = \{X^{\underline{m}_i} - \rho(\underline{m}_i) \mid 1 \leq i \leq r\}$ es un sistema de generadores de $I(\rho)$, basta ver que para todo i, $X^{\underline{m}_i} - \rho(\underline{m}_i)$ y $X^{-\underline{m}_i} - \rho(-\underline{m}_i)$ están en el ideal generado por C. Esto es obvio pues $X^{-\underline{m}_i} - \rho(-\underline{m}_i) = -\rho(-\underline{m}_i) X^{-\underline{m}_i}(X^{\underline{m}_i} - \rho(\underline{m}_i))$.

Veamos que este sistema de generadores forma una sucesión regular en $k[X^\pm]$. Denotemos $J = \langle X_1 Z_1 - 1, \ldots, X_n Z_n - 1\rangle$ y sea $\overline{\mathcal{M}} = \mathcal{M}/J$ uno de los ideales maximales de $k[X^\pm]$. Entonces

$$k[X^\pm]_{\overline{\mathcal{M}}} = \frac{k[X,Z]_{\mathcal{M}}}{Jk[X,Z]_{\mathcal{M}}}.$$

$k[X,Z]_{\mathcal{M}}$ es un anillo Cohen-Macaulay (CM) por ser k un cuerpo ([Mat], th.17.7). Por otra parte, $\{X_1 Z_1 - 1, \ldots, X_n Z_n - 1\}$ es una sucesión regular en $k[X,Z]_{\mathcal{M}}$, pues $k[X,Z]_{\mathcal{M}}/Jk[X,Z]_{\mathcal{M}}$ es dominio de integridad. Como consecuencia $k[X,Z]_{\mathcal{M}}/Jk[X,Z]_{\mathcal{M}} = k[X^\pm]_{\overline{\mathcal{M}}}$ es CM para todo maximal $\overline{\mathcal{M}}$ ([Mat], th.17.3), luego $k[X^\pm]$ es CM. Así que para ver que $\{X^{\underline{m}_i} - \rho(\underline{m}_i) \mid 1 \leq i \leq r\}$ es una sucesión regular, basta ver que $\mathrm{ht}(I(\rho)) = r$ (como $I(\rho)$ es un ideal propio, podemos localizar en un maximal que lo contenga y aplicar [Mat], th.17.4).

Por otra parte, como el ideal J está generado por una sucesión regular de n elementos,

$$\dim(k[X^\pm]) = \dim(k[X,Z]) - \mathrm{ht}(J) = 2n - n = n,$$

y, análogamente, si L es un subretículo de $\mathbb{Z}^n$ entonces $k[L] = \bigoplus_{\underline{m} \in L} kX^{\underline{m}}$ es un anillo de dimensión rango(L). Denotemos $L = \mathrm{Sat}\ L_\rho$ y sea L' el complementario de L en $\mathbb{Z}^n$. Sea $\widetilde{I}(\rho) = I(\rho) \cap k[L]$. Puesto que $I(\rho) \cap k[L'] = \langle 0 \rangle$ (ya que $I(\rho)$ está generado por elementos de $k[L]$), se tiene

$$k[X^\pm]/I(\rho) = k[\mathbb{Z}^n]/I(\rho) \cong k[L]/\widetilde{I}(\rho) \otimes_k k[L']. \tag{1.2}$$

Por lo tanto $\dim(k[X^\pm]) - \mathrm{ht}(I(\rho)) = \dim(k[X^\pm]/I(\rho)) = \dim(k[L]/\widetilde{I}(\rho)) +$ rango(L'); es decir, si $r =$ rango(L), $\mathrm{ht}(I(\rho)) = n - (n-r) + \dim(k[L]/\widetilde{I}(\rho)) = r + \dim(k[L]/\widetilde{I}(\rho))$. Pero la extensión $k \subset k[L]/\widetilde{I}(\rho)$ es entera, pues si $\underline{m} \in L$ entonces existe $h \in \mathbb{Z}$ de forma que $h\underline{m} \in L_\rho$ ($L = \mathrm{Sat}\ L_\rho$) y podemos suponer $h > 0$, con lo cual $X^{\underline{m}} + \widetilde{I}(\rho)$ es raíz del polinomio $T^h - \rho(h\underline{m})$. Luego $\dim(k[L]/\widetilde{I}(\rho)) = 0$ y por tanto $\mathrm{ht}(I(\rho)) = r$, luego la sucesión es regular y $\mathrm{ht}(I(\rho)) = \mathrm{rango}(L_\rho)$.

4. Si L_ρ es un retículo saturado $k[L]/\widetilde{I}(\rho) \cong k$ y de (1.2) se deduce $k[X^{\pm}]/I(\rho) \cong k[L']$, que es dominio de integridad. Por lo tanto $I(\rho)$ es primo.

Recíprocamente, supongamos que $I(\rho)$ es primo. Si $\underline{m}$ es un elemento del saturado de L_ρ, existe un entero positivo d cumpliendo $d\underline{m} \in L_\rho$. Sea $\xi \in k^*$ una raíz primitiva d-ésima de la unidad (estamos suponiendo k algebraicamente cerrado). Entonces, si $a \in k$,

$$Y^d - a^d = \prod_{i=1}^{d}(Y - \xi^i a),$$

y por tanto, se tiene

$$X^{d\underline{m}} - \rho(d\underline{m}) = \prod_{i=1}^{d}(X^{\underline{m}} - \xi^i \rho(\underline{m})). \tag{1.3}$$

Como $I(\rho)$ es primo, existe i tal que $X^{\underline{m}} - \xi^i\rho(\underline{m}) \in I(\rho)$, con lo cual según se vió en el apartado 1, $\underline{m} \in L_\rho$. Luego el retículo es saturado.

5. Como L/L_ρ es un grupo abeliano finito, aplicando el teorema de estructura de grupos abelianos, L/L_ρ es suma directa de grupos cíclicos. Luego, sin pérdida de generalidad, podemos suponer que se trata de un grupo cíclico de orden g. Diagonalizando la matriz de inclusión de L_ρ en L encontramos una base $\{\underline{m}_1, \ldots, \underline{m}_r\}$ de L con $\{\underline{m}_1, \ldots, \underline{m}_{r-1}, g\underline{m}_r\}$ base de L_ρ, siendo r el rango de los dos $\mathbb{Z}$-módulos. Entonces, para cualquier extensión ρ' de ρ a L, el elemento $\rho'(\underline{m}_r)$ es una raíz g-ésima de $\rho(g\underline{m}_r)$, pues

$$(\rho'(\underline{m}_r))^g = \rho'(g\underline{m}_r) = \rho(g\underline{m}_r).$$

Sea $c \in k^*$ una de estas raíces g-ésimas. Variando ξ en el conjunto de las raíces g-ésimas de la unidad, ξc nos da todos los posibles valores para $\rho'(\underline{m}_r)$. Si definimos $J = \langle X^{\underline{m}_1} - \rho(\underline{m}_1), \ldots, X^{\underline{m}_{r-1}} - \rho(\underline{m}_{r-1})\rangle$, por el apartado 3, los ideales asociados a las extensiones, ρ', de ρ son de la forma $I(\rho') = J + \langle X^{\underline{m}_r} - \xi c\rangle$, donde ξ varía en las raíces de orden g de la unidad.

En el anillo $R = k[X^{\pm}]/J$, se cumple:

$$I(\rho)/J = \langle X^{g\underline{m}_r} - c^g\rangle R = \prod_{\xi}\langle X^{\underline{m}_r} - \xi c\rangle R = \bigcap_{\xi}\langle X^{\underline{m}_r} - \xi c\rangle R = \bigcap_{\rho'} I(\rho')/J.$$

Por lo tanto $I(\rho) = \bigcap_{\rho'} I(\rho')$. Si la característica de k no divide a g, existen g raíces g-ésimas de la unidad distintas y tendremos g extensiones distintas de ρ.

En el caso de que $g = p^r$, existe una única raíz g-ésima de la unidad en k, con lo cual hay una única extensión ρ', de ρ a L. Según lo que acabamos de ver, tenemos la filtración

$$k[X^{\pm}] \supset I(\rho') = J + \langle X^{\underline{m}_r} - c\rangle \supset \ldots \supset J + \langle X^{\underline{m}_r} - c\rangle^{p^r} = I(\rho) \qquad (1.4)$$

Además la aplicación $\phi : k[X^{\pm}]/I(\rho') \to J + \langle X^{\underline{m}_r} - c\rangle^i / J + \langle X^{\underline{m}_r} - c\rangle^{i+1}$ definida al multiplicar por $(X^{\underline{m}_r} - c)^i$, es un isomorfismo. Esto es debido a que $X^{\underline{m}_r} - c$ es un no divisor de cero módulo J (apartado 3). Reduciendo la cadena de contenciones (1.4) módulo $I(\rho)$, y llamando $M_i = J + \langle X^{\underline{m}_r} - c\rangle^i / I(\rho)$, obtenemos

$$\frac{k[X^{\pm}]}{I(\rho)} = M_0 \supset M_1 \supset \ldots \supset M_g = \frac{I(\rho)}{I(\rho)} = \langle 0\rangle,$$

siendo los sucesivos cocientes,

$$\frac{M_i}{M_{i+1}} = \frac{J + \langle X^{\underline{m}_r} - c\rangle^i / I(\rho)}{J + \langle X^{\underline{m}_r} - c\rangle^{i+1} / I(\rho)} = \frac{J + \langle X^{\underline{m}_r} - c\rangle^i}{J + \langle X^{\underline{m}_r} - c\rangle^{i+1}},$$

cocientes que, como hemos visto, son isomorfos a $k[X^{\pm}]/I(\rho')$.

□

Utilizando este teorema, podemos describir la descomposición primaria y el ideal radical de los ideales binomiales de $k[X^{\pm}]$, en términos de operaciones con retículos enteros.

Definición 1.3.6 *Si L es un retículo de $\mathbb{Z}^n$ y p es un número primo, se define* $\mathrm{Sat}_p\ L$ *como el mayor subretículo de* $\mathrm{Sat}\ L$ *que contiene a L y tal que el orden de* $\mathrm{Sat}_p\ L/L$ *es una potencia de p. Si $p = 0$ entonces* $\mathrm{Sat}_p\ L = L$.

Definición 1.3.7 *Si L es un retículo de $\mathbb{Z}^n$ y p es un número primo, se define* $\mathrm{Sat}'_p\ L$ *como el mayor subretículo de* $\mathrm{Sat}\ L$ *que contiene a L y tal que el orden de* $\mathrm{Sat}'_p\ L/L$ *es primo con p. Si $p = 0$ entonces* $\mathrm{Sat}'_p\ L = \mathrm{Sat}\ L$.

La unicidad de estos retículos es debida a la unicidad de los p-subgrupos de Sylow en el caso abeliano.

Corolario 1.3.8 *Sean k un cuerpo algebraicamente cerrado de característica p y $\rho : L_\rho \to k^*$ un carácter parcial sobre $\mathbb{Z}^n$. Si g es el orden de $\mathrm{Sat}'_p\ L_\rho/L_\rho$, existen g extensiones de ρ a $\mathrm{Sat}'_p\ L_\rho$, $\rho_1, \dots, \rho_g$, y para cada j un único carácter ρ'_j extensión de ρ_j a $\mathrm{Sat}\ L_\rho$. Además hay un único carácter parcial, ρ', extensión de ρ a $\mathrm{Sat}_p\ L_\rho$, y $\rho'_j, \dots, \rho'_g$ son las extensiones de ρ' a $\mathrm{Sat}\ L_\rho$. Con esta notación, el radical, los primos asociados y la descomposición primaria (minimal e irredundante) de $I(\rho)$, vienen dados por:*

$$\sqrt{I(\rho)} = I(\rho') \quad ; \quad \mathrm{Ass}(I(\rho)) = \{I(\rho'_j) \mid 1 \leq j \leq g\} \quad ; \quad I(\rho) = \bigcap_{j=1}^{g} I(\rho_j)$$

En particular, si $p = 0$, el ideal $I(\rho)$ es radical y los primos asociados son todos minimales.

Dem. Supongamos que $p > 0$ y sea $p^r g$ con m.c.d.$(p, g) = 1$ el orden de $\mathrm{Sat}\ L_\rho/L_\rho$. Como $|\mathrm{Sat}'_p\ L_\rho/L_\rho| = g$ y $|\mathrm{Sat}_p\ L_\rho/L_\rho| = p^r$ (Definición 1.3.6), se tiene $|\mathrm{Sat}\ L_\rho/\mathrm{Sat}'_p\ L_\rho| = p^r$ y $|\mathrm{Sat}\ L_\rho/\mathrm{Sat}_p\ L_\rho| = g$. Siguiendo el apartado 5 del Teorema 1.3.5, denotemos por ρ' a la única extensión de ρ a $\mathrm{Sat}_p\ L_\rho$ y por $\{\tilde{\rho}_1, \dots, \tilde{\rho}_g\}$ al conjunto de las extensiones de ρ' a $\mathrm{Sat}\ L_\rho$. Consideremos, también, el conjunto $\{\rho_1, \dots, \rho_g\}$ de las extensiones de ρ a $\mathrm{Sat}'_p\ L_\rho$ y para cada $j \in \{1, \dots, g\}$ sea ρ'_j la única extensión de ρ_j al $\mathrm{Sat}\ L_\rho$. Es decir, se tiene el siguiente cuadro de extensiones de caracteres:

$$\begin{tikzcd}
 & \tilde{\rho}_1, \dots, \tilde{\rho}_g \arrow[ddl, dotted, dash] & & \rho'_1, \dots, \rho'_g \arrow[ddr, dotted, dash] & \\
 & & \mathrm{Sat}\, L_\rho \arrow[dl, dash, "g"'] \arrow[dr, dash, "p^r"] & & \\
\rho' \arrow[ddrr, dotted, dash] & \mathrm{Sat}_p\, L_\rho \arrow[dr, dash, "p^r"'] & & \mathrm{Sat}'_p\, L_\rho \arrow[dl, dash, "g"] & \rho_1, \dots, \rho_g \arrow[ddll, dotted, dash] \\
 & & L_\rho & & \\
 & & \rho & &
\end{tikzcd}$$

Extensiones de un carácter parcial

Los conjuntos de extensiones $\{\tilde{\rho}_1, \dots, \tilde{\rho}_g\}$ y $\{\rho'_1, \dots, \rho'_g\}$ son iguales, pues al restringir ρ'_j a $\mathrm{Sat}_p\ L_\rho$ se tiene una extensión de ρ a $\mathrm{Sat}_p\ L_\rho$, por lo tanto ρ'_j es una de las extensiones de ρ' a $\mathrm{Sat}\ L_\rho$.

Aplicando el apartado 4 del Teorema 1.3.5, se deduce que los ideales $I(\rho'_j)$ son primos, y del apartado 5 obtenemos que $I(\rho') = \cap_{j=1}^{g} I(\rho'_j)$ (por tanto $I(\rho')$ es radical) y que $I(\rho) = \cap_{j=1}^{g} I(\rho_j)$. Denotemos por τ bien el carácter ρ o bien uno de los caracteres ρ_j. En la demostración del apartado 5 del Teorema 1.3.5 se construían un ideal J, un binomio b del anillo $k[X^{\pm}]$, no divisor de cero módulo J, y un natural $N \geq 1$ tales que $I(\tau) = J + \langle b^N \rangle$ e $I(\tau') = J + \langle b \rangle$. Por lo tanto $\sqrt{I(\tau)} = I(\tau')$; es decir, $\sqrt{I(\rho)} = I(\rho')$ y $\sqrt{I(\rho_j)} = I(\rho'_j)$. Además, $I(\rho_j)$ es $I(\rho'_j)$-primario. En efecto, sea b un binomio de $k[X^{\pm}]$ tal que $I(\rho_j) = J + \langle b^N \rangle$ e $I(\rho'_j) = J + \langle b \rangle$. Supongamos que $xy \in I(\rho_j)$ con $x \notin I(\rho'_j)$. $I(\rho'_j)$ es un ideal primo, luego $y \in I(\rho'_j)$. Se tiene

$$\begin{array}{ll} y \in I(\rho'_j) \Rightarrow y = z_1 + \lambda_1 b & \text{con } z_1 \in J \text{ y } \lambda_1 \in k[X^{\pm}] \\ xy \in I(\rho_j) \Rightarrow xy = z_2 + \lambda_2 b^N & \text{con } z_2 \in J \text{ y } \lambda_2 \in k[X^{\pm}] \ . \end{array}$$

Sustituyendo y en la segunda ecuación se tiene $xz_1 - z_2 = b(\lambda_2 b^{N-1} - \lambda_1 x)$, y puesto que b es un no divisor de cero módulo J, $\lambda_2 b^{N-1} - \lambda_1 x \in J$, luego $\lambda_1 x \in J + \langle b^{N-1} \rangle$. Pero x no pertenece a $I(\rho'_j)$ y por un razonamiento de inducción sobre N, se tendría que $J + \langle b^{N-1} \rangle$ es $I(\rho'_j)$-primario, luego $\lambda_1 \in J + \langle b^{N-1} \rangle$. Por lo tanto, $y = z_1 + \lambda_1 b \in I(\rho_j)$ y tenemos que $I(\rho_j)$ es $I(\rho'_j)$-primario. Por lo tanto,

$$I(\rho) = \bigcap_{j=1}^{g} I(\rho_j)$$

es la descomposición primaria de $I(\rho)$ y sus primos asociados son $\{I(\rho'_j) \mid j \in \{1, \ldots, g\}\}$. La descomposición es minimal ya que no puede haber igualdades del tipo $I(\rho'_i) = I(\rho'_j)$ con $i \neq j$ pues ρ'_i y ρ'_j son extensiones distintas de ρ a un mismo retículo, Sat L_ρ. Además, como las extensiones de ρ a $\mathrm{Sat}'_p\ L_\rho$, $\{\rho_1, \ldots, \rho_g\}$, son distintas, entonces para cada $j \in \{1, \ldots, g-1\}$ existe un elemento $\underline{m}_j \in \mathrm{Sat}'_p\ L_\rho$ cumpliendo que $\rho_j(\underline{m}_j) \neq \rho_g(\underline{m}_j)$. Es decir, si para cada j denotamos $b_j = X^{\underline{m}_j} - \rho_j(\underline{m}_j)$ entonces $b_j \in I(\rho_j)$ y puesto que ρ'_g es la extensión de ρ_g a Sat L_ρ, $b_j \notin I(\rho'_g)$. Luego

$$\prod_{j=1}^{g-1} b_j \in \bigcap_{j=1}^{g-1} I(\rho_j) \text{ y } \prod_{j=1}^{g-1} b_j \notin I(\rho'_g)$$

ya que $I(\rho'_g)$ es un ideal primo. Por lo tanto $\bigcap_{j=1}^{g-1} I(\rho_j) \not\subseteq I(\rho_g)$ y la descomposición es irredundante.

$\square$

Los últimos resultados que hemos expuesto son relativos a los ideales binomiales del anillo de polinomios de Laurent. Estos resultados tienen una traducción inmediata para ciertos ideales binomiales del anillo de polinomios, llamados ideales de carácter parcial.

En lo que sigue, dado $\underline{m} \in \mathbb{Z}^n$, denotaremos $\underline{m}_+$ y $\underline{m}_-$ a las partes positiva y negativa de $\underline{m}$, de forma que $\underline{m} = \underline{m}_+ - \underline{m}_-$. Ambos son vectores con n coordenadas enteras no negativas.

Definición 1.3.9 *Dado un carácter parcial ρ sobre $\mathbb{Z}^n$, se denomina ideal de carácter parcial asociado a ρ al ideal binomial del anillo de polinomios $k[X]$ dado por*

$$I_+(\rho) := \langle \{X^{\underline{m}_+} - \rho(\underline{m})X^{\underline{m}_-} \mid \underline{m} \in L_\rho\}\rangle.$$

Proposición 1.3.10 *$I_+(\rho) = I(\rho) \cap k[X]$ y el sistema de generadores dado en la definición anterior es base de Gröbner de $I_+(\rho)$ para cualquier orden monomial en $k[X]$.*

Dem. Consideremos la cadena de homomorfismos,

$$k[X] \xrightarrow{i} k[X,Z] \xrightarrow{c} k[X,Z]/\langle\{X_iZ_i - 1\}\rangle = k[X^{\pm}]$$

donde i es el homomorfismo inclusión y c es el homomorfismo de paso al cociente módulo $\langle\{X_iZ_i - 1\}\rangle$. Consideremos el ideal de $k[X,Z]$, $I'(\rho) = c^{-1}(I(\rho))$. Dado un orden monomial $<$ en $k[X]$, se define el orden monomial $<'$ en $k[X,Z]$ por:

$$X^aZ^b <' X^cZ^d \iff \text{ o bien } Z^b < Z^d \text{ o bien } Z^b = Z^d \text{ y } X^a < X^c.$$

El orden $<'$ así definido es un orden de eliminación para las indeterminadas $Z_1, \ldots, Z_n$ (Ejemplo 1.1.23). Luego si G es base de Gröbner de $I'(\rho)$ para $<'$, entonces $G \cap k[X]$ es base de Gröbner de $I'(\rho) \cap k[X]$ para $<$ (Teorema 1.1.24).

Ahora bien, en la demostración del apartado 2 del Teorema 1.3.5 vimos que el conjunto $G = \{X^aZ^b - \rho(a-b-c+d)X^cZ^d \mid a-b-c+d \in L_\rho\}$ es base de Gröbner de $I'(\rho)$ para cualquier orden, en particular para $<'$. Por lo tanto $G \cap k[X]$ es base de Gröbner de $I'(\rho) \cap k[X]$ para el orden $<$. Denotemos $G^* = \{X^{\underline{m}_+} - \rho(\underline{m})X^{\underline{m}_-} \mid \underline{m} \in L_\rho\}$. Es claro que $G \cap k[X] = \{mb \mid m \text{ es monomio de } k[X] \text{ y } b \in G^*\}$ y como G^* genera $I_+(\rho)$, también lo hace $G \cap k[X]$. Luego $I_+(\rho) = I'(\rho) \cap k[X]$ y $G \cap k[X]$ es base de Gröbner de $I_+(\rho)$. Además

$$\langle\{\mathrm{LT}(b) \mid b \in G^*\}\rangle = \langle\{\mathrm{LT}(b) \mid b \in G \cap k[X]\}\rangle = \mathrm{in}(I),$$

luego G^* es base de Gröbner de $I_+(\rho)$. Por último, $I_+(\rho) = i^{-1}(I'(\rho) \cap k[X]) = i^{-1} \circ c^{-1}(I(\rho)) = I(\rho) \cap k[X]$ ya que $c \circ i$ es la inclusión de $k[X]$ en $k[X^{\pm}]$.

□

Corolario 1.3.11 *Si I es un ideal binomial de $k[X]$ que no contiene ningún monomio, entonces existe un único carácter parcial ρ, sobre $\mathbb{Z}^n$, tal que $(I : (X_1 \cdots X_n)^\infty) = I_+(\rho)$.*

Dem. En primer lugar observemos que $Ik[X^{\pm}] \cap k[X] = (I : (X_1 \cdots X_n)^\infty)$, ya que si $(X_1 \cdots X_n)^s f \in I$ entonces $f = (X_1 \cdots X_n)^s (X_1 \cdots X_n)^{-s} f \in Ik[X^{\pm}]$. Recíprocamente, si $f \in Ik[X^{\pm}] \cap k[X]$, se tiene $f = \sum_{i=1}^t g_i h_i$ con $g_i \in k[X^{\pm}]$ y $h_i \in I$. Eligiendo $s > 0$ tal que para todo $i \in \{1, \ldots, t\}$ se cumpla $(X_1 \cdots X_n)^s g_i \in k[X]$, se tendrá $f(X_1 \cdots X_n)^s \in I$. Puesto que I es binomial y no contiene monomios, el ideal $Ik[X^{\pm}]$ es binomial propio, luego existe un único carácter parcial ρ tal que $Ik[X^{\pm}] = I(\rho)$ (Teorema 1.3.5, apartado 2). Pero, por la Proposición 1.3.10, se tiene que $I(\rho) \cap k[X] = I_+(\rho)$, de donde se deduce este corolario.

□

Corolario 1.3.12 *Si k es un cuerpo algebraicamente cerrado, el radical, la descomposición primaria y los primos asociados de $I_+(\rho)$ se obtienen como indica el Corolario 1.3.8, cambiando $I(-)$ por $I_+(-)$.*

Dem. No hay más que tener en cuenta que $I_+(\rho) = I(\rho) \cap k[X]$ (Proposición 1.3.10) y utilizar los dos resultados siguientes:

- Si B es un subanillo de A e I un ideal de A entonces $\sqrt{I \cap B} = \sqrt{I} \cap B$.
- Si $\mathcal{Q}$ es un ideal de A, $\mathcal{P}$-primario, entonces $\mathcal{Q} \cap B$ es $\mathcal{P} \cap B$-primario.

□

En el Teorema 1.3.5 vimos que lo ideales binomiales propios del anillo de polinomios de Laurent son exactamente aquellos asociados a caracteres parciales $I(\rho)$. Sin embargo, en el caso del anillo de polinomios el resultado es más débil, como demostraremos a continuación.

Corolario 1.3.13 *Los ideales del anillo de polinomios $k[X]$ de la forma $I_+(\rho)$ son exactamente aquellos ideales binomiales cuyos primos asociados no contienen monomios.*

Dem. Sea $I = \cap_{j=1}^{d} \mathcal{Q}_j$ la descomposición primaria de un ideal binomial I de $k[X]$. Denotemos $\mathcal{P}_j = \sqrt{\mathcal{Q}_j}$ para $j \in \{1, \ldots, d\}$. Si suponemos que los $\mathcal{P}_j$ no contienen monomios, tampoco los contiene I, luego existe un carácter parcial ρ, sobre $\mathbb{Z}^n$, tal que $(I : (X_1 \cdots X_n)^\infty) = I_+(\rho)$ (Corolario 1.3.11). Ahora bien, si $(X_1 \cdots X_n)^s f \in I$ entonces para todo j, $(X_1 \cdots X_n) f^s \in \mathcal{Q}_j$ y $(X_1 \cdots X_n)^s \notin \mathcal{P}_j$, luego $f \in \mathcal{Q}_j$ y por tanto $f \in I$. Luego $I = I_+(\rho)$. Recíprocamente, los primos asociados a $I_+(\rho)$ no contienen monomios, ya que según vimos en el Corolario 1.3.12, estos primos son ideales asociados a un carácter parcial y si contuvieran monomios no serían propios (Proposición 1.3.10).

$\square$

Este resultado nos va a permitir caracterizar, usando ideales asociados a caracteres parciales, todo el conjunto de ideales primos binomiales del anillo de polinomios, lo cual será fundamental en nuestro estudio de las curvas monomiales.

Definición 1.3.14 *Dado un ideal I de $k[X]$, llamaremos célula asociada a I al conjunto $\mathcal{Z}_I := \{i \in \{1, \ldots, n\} \mid X_i \notin I\}$.*

Notación 1.3.15 Dado $\mathcal{Z} \subseteq \{1, \ldots, n\}$, denotaremos $\mathbb{Z}^{\mathcal{Z}} := \{(a_1, \ldots, a_n) \mid a_i = 0$ para todo $i \notin \mathcal{Z}\}$, $k[\mathcal{Z}]$ será el anillo de polinomios $k[\{X_i\}_{i \in \mathcal{Z}}]$ y $M(\mathcal{Z})$ el ideal de $k[X]$ generado por el conjunto $\{X_i \mid i \notin \mathcal{Z}\}$. En ocasiones trabajaremos con la identificación natural $\mathbb{Z}^{\mathcal{Z}} \equiv \mathbb{Z}^{|\mathcal{Z}|}$.

Corolario 1.3.16 *Sea k un cuerpo algebraicamente cerrado, y sean $\mathcal{P}$ un ideal de $k[X]$ y $\mathcal{Z}$ su célula asociada. El ideal $\mathcal{P}$ es primo binomial si y sólo si existe un carácter parcial saturado ρ en el retículo $\mathbb{Z}^{\mathcal{Z}}$ tal que $\mathcal{P} = I_+(\rho) + M(\mathcal{Z})$.*

Dem. Si $\mathcal{P}$ es un ideal primo binomial, el ideal $\overline{\mathcal{P}} = \mathcal{P}/M(\mathcal{Z})$, en el anillo $k[\mathcal{Z}]$, es también binomial y no contiene monomios. Aplicando el Corolario 1.3.11, existe un carácter parcial ρ sobre $\mathbb{Z}^{\mathcal{Z}}$ cumpliendo $(\overline{\mathcal{P}} : (\prod_{i \in \mathcal{Z}} X_i)^\infty) = I_+(\rho)$. Además $\overline{\mathcal{P}} = (\overline{\mathcal{P}} : (\prod_{i \in \mathcal{Z}} X_i)^\infty)$ pues $\overline{\mathcal{P}}$ es primo y $X_i + M(\mathcal{Z}) \notin \overline{\mathcal{P}}$ para $i \in \mathcal{Z}$. Por lo tanto $\mathcal{P} = I_+(\rho) + M(\mathcal{Z})$.

Recíprocamente, es claro que si $\mathcal{P} = I_+(\rho) + M(\mathcal{Z})$ entonces $\mathcal{P}$ es binomial. Denotemos ahora $\{Z_1, \ldots, Z_t\} = \{X_i \mid X_i \notin \mathcal{P}\}$ y $\{Y_1, \ldots, Y_s\} = \{X_i \mid X_i \in \mathcal{P}\}$. Según esta notación, L_ρ es un subretículo de $\mathbb{Z}^t$. Para ver que el ideal $\mathcal{P}$ es primo, veamos que es el núcleo del homomorfismo sobreyectivo de anillos

$$\phi : k[Z_1, \ldots, Z_t, Y_1, \ldots, Y_s] \longrightarrow k[T^{\pm}],$$

definido por $\phi(Y_i) = 0$ y $\phi(Z^{\underline{m}}) = \tilde{\rho}(\underline{m})T^{\overline{m}}$, donde $\overline{m} = \underline{m} + L_\rho \in \mathbb{Z}^t/L_\rho$, $k[T^\pm]$ es el anillo de Laurent asociado al retículo $\mathbb{Z}^t/L_\rho$ (como L_ρ es saturado, $\mathbb{Z}^t/L_\rho$ es subretículo de $\mathbb{Z}^t$) y $\tilde{\rho}$ es una extensión cualquiera de ρ a $\mathbb{Z}^t$.

Consideremos el homomorfismo sobreyectivo $\varphi : k[Z^\pm] \to k[T^\pm]$ dado por $\varphi(Z^{\underline{m}}) = \tilde{\rho}(\underline{m})T^{\overline{m}}$. El núcleo contiene al ideal primo $I(\rho)$, ya que para $\underline{m} \in L_\rho$ se tiene $\varphi(Z^{\underline{m}} - \rho(\underline{m})) = \tilde{\rho}(\underline{m})T^{\overline{m}} - \rho(\underline{m}) = \rho(\underline{m}) - \rho(\underline{m}) = 0$. Además se tiene que $I(\rho)$ es un ideal primo de altura el rango de L_ρ (Teorema 1.3.5, apartados 3 y 4), y $t - \text{rango}(L_\rho) = \dim(k[T^\pm]) = \dim(k[Z^\pm]) - \text{ht}(\ker\varphi) = t - \text{ht}(\ker(\varphi))$. Por lo tanto, tenemos dos ideales primos de igual altura, con $I(\rho) \subseteq \ker(\varphi)$, luego son iguales.

Si ahora consideramos el homomorfismo $\alpha : k[Z, Y] \to k[Z^\pm]$ definido por $\alpha(Z_i) = Z_i$ y $\alpha(Y_k) = 0$, entonces $\alpha^{-1}(I(\rho)) = I_+(\rho) + M(\mathcal{Z}) = \mathcal{P}$. En efecto, puesto que $I_+(\rho) \subseteq I(\rho)$ y $\alpha(M(\mathcal{Z})) = 0$ entonces se tiene $I_+(\rho) + M(\mathcal{Z}) \subseteq \alpha^{-1}(I(\rho))$. Recíprocamente, sea $f \in k[Z, Y]$ tal que $\alpha(f) \in I(\rho)$. Si escribimos $f = f_1 + f_2$ donde $f_1 \in k[Z]$ y $f_2 \in \langle\{Y_k \mid 1 \leq k \leq s\}\rangle$, como $\alpha(f_2) = 0$ entonces $f_1 = \alpha(f_1) \in I(\rho)$ y se tiene $f_1 \in I(\rho) \cap k[\mathcal{Z}]$. Por el Corolario 1.3.11, $I(\rho) \cap k[\mathcal{Z}] = I_+(\rho)$, luego $f_1 \in I_+(\rho)$ y $f \in I_+(\rho) + M(\mathcal{Z})$.

Además como $\varphi \circ \alpha = \phi$ entonces $\ker(\phi) = \ker(\varphi \circ \alpha) = \alpha^{-1}(I(\rho)) = \mathcal{P}$ y se tiene que $\mathcal{P}$ es un ideal primo.

□

Otra propiedad necesaria en nuestro estudio posterior de las curvas monomiales, es que el carácter binomial de un ideal se translada a sus primos asociados.

Proposición 1.3.17 *Si I es un ideal propio binomial del anillo de polinomios $k[X]$, sus primos asociados son también binomiales.*

Dem. Si existe un carácter parcial ρ en $\mathbb{Z}^n$ con $I = I_+(\rho)$, el resultado se obtiene aplicando los Corolarios 1.3.12 y 1.3.8. Si ahora suponemos que $(I : X_i) = I$ para todo $i \in \{1, \ldots, n\}$, entonces I no contiene monomios y además se tiene $(I : (X_1 \cdots X_n)^\infty) = I$. Luego aplicando el Corolario 1.3.11, existe un carácter parcial ρ sobre $\mathbb{Z}^n$ con $I = I_+(\rho)$, y el enunciado es cierto. Supongamos, finalmente, que existe un índice $i \in \{1, \ldots, n\}$ con $(I : X_i) \neq I$. Además, podemos suponer que $X_i \notin I$, ya que en caso contrario, reduciendo módulo X_i, obtenemos un ideal binomial en una indeterminada menos, y aplicando hipótesis de inducción se tiene el resultado. En estas condiciones, se tiene una sucesión exacta,

$$0 \longrightarrow k[X]/(I : X_i) \xrightarrow{\cdot X_i} k[X]/I \longrightarrow k[X]/(I, X_i) \longrightarrow 0,$$

y por tanto $\mathrm{Ass}(I) \subseteq \mathrm{Ass}(I : X_i) \cup \mathrm{Ass}(I, X_i)$. Pero como I es binomial, $(I : X_i)$ también lo es (Corolario 1.2.7). Además $I \subsetneq (I : X_i)$ e $I \subsetneq (I, X_i)$, luego aplicando inducción noetheriana se obtiene el resultado.

□

1.4 El radical de un ideal binomial

Veremos en esta sección que el radical de un ideal binomial del anillo de polinomios es binomial. Para ello consideramos los siguientes lemas previos:

Lema 1.4.1 *Sean R un anillo conmutativo, y $X_1, \ldots, X_n$ elementos de R. Si I es un ideal de R, entonces*

$$\sqrt{I} = \sqrt{(I : (X_1 \cdots X_n)^\infty)} \cap \sqrt{I + \langle X_1 \rangle} \cap \ldots \cap \sqrt{I + \langle X_n \rangle}.$$

Dem. Sea $\mathcal{P}$ un primo que contiene a I. Si $(I : (X_1 \cdots X_n)^\infty) \not\subseteq \mathcal{P}$, entonces existen un elemento f del anillo y un entero positivo d, con $(X_1 \cdots X_n)^d f \in I$ y $f \notin \mathcal{P}$. Pero como $\mathcal{P}$ es primo, X_i pertenece a $\mathcal{P}$ para algún i. Luego $\mathcal{P}$ contiene a $I + \langle X_i \rangle$ para algún i y la igualdad del lema es inmediata.

□

Lema 1.4.2 *Sean $A = k[X_1, \ldots, X_n]$ y $A' = k[X_1, \ldots, X_{n-1}]$. Si I' es un ideal de A' entonces $I' = (I'A + \langle X_n \rangle) \cap A'$. Además, si I' es radical, $I'A + \langle X_n \rangle$ también lo es.*

Dem. Si $f \in (I'A + \langle X_n \rangle) \cap A'$, entonces existen $h_i \in A$, $g_i \in I'$ y $h \in A$ tales que $f = \sum h_i g_i + hX_n$. Escribiendo $h_i = h_{i1} + h_{i2}X_n$ con $h_{i1} \in A'$, se tiene $f = \sum h_{i1} g_i + (\sum h_{i2} g_i + h)X_n$, y puesto que $f \in A'$, se deduce $f = \sum h_{i1} g_i \in I'$.

Supongamos ahora que I' es radical. Si $f = (f_1 + f_2 X_n) \in \sqrt{I'A + \langle X_n \rangle}$, entonces existe $N \in \mathbb{Z}_{>0}$ tal que $f^N \in I'A + \langle X_n \rangle$, con lo cual $f_1^N \in (I'A + \langle X_n \rangle) \cap A' = I'$. Como estamos suponiendo I' radical, $f_1 \in I'$ y por lo tanto $f \in I'A + \langle X_n \rangle$.

□

Lema 1.4.3 *Sean $A = k[X_1, \ldots, X_n]$ y $A' = k[X_1, \ldots, X_{n-1}]$. Si I es un ideal binomial de A y denotamos por I' al ideal binomial $I \cap A'$, entonces $I + \langle X_n \rangle$ es la suma de $I'A + \langle X_n \rangle$ más un ideal generado por monomios de A'.*

Dem. Se deduce de forma inmediata del hecho de que cada binomio de I o pertenece a I', o al ideal $\langle X_n\rangle$, o es congruente módulo $\langle X_n\rangle$ con un monomio de A'.

$\square$

Proposición 1.4.4 *Sea I un ideal radical binomial de $k[X]$. Si M es un ideal monomial, entonces existe un ideal monomial M_1 con $\sqrt{I+M} = I + M_1$.*

Dem. Si $M = \langle 0\rangle$ no hay nada que probar, luego podemos suponer que M contiene a algún monomio, con lo cual $((I+M) : (X_1 \dots X_n)^\infty) = k[X]$. Aplicando el Lema 1.4.1 al ideal $I+M$,

$$\sqrt{I+M} = \bigcap_{i=1}^{n} \sqrt{I+M+\langle X_i\rangle}.$$

Si vemos que para todo i existe un ideal monomial M_i tal que $\sqrt{I+M+\langle X_i\rangle} = I + M_i$, utilizando el Corolario 1.2.6 se deduce la proposición.

Para simplificar la notación supongamos que $i = n$ y sean $A = k[X_1, \dots, X_n]$ y $A' = k[X_1, \dots, X_{n-1}]$. Como I es binomial, por el Lema 1.4.3 existe un ideal monomial J^* en A' de forma que $I+\langle X_n\rangle = I'A+J^*A+\langle X_n\rangle$ donde $I' = I\cap A'$. Por lo tanto, por ser M monomial, existe un ideal monomial J en A' con $I+M+\langle X_n\rangle = I'A+JA+\langle X_n\rangle$. I' es un ideal radical binomial de A', luego aplicando hipótesis de inducción sobre el número de indeterminadas, se deduce que existe un ideal monomial J_1 en A', cumpliendo $\sqrt{I'+J} = I'+J_1$. Aplicando el Lema 1.4.2, $(\sqrt{I'+J})A + \langle X_n\rangle$ es radical. Entonces:

$$\begin{aligned} \sqrt{I+M+\langle X_n\rangle} &= \sqrt{I'A+JA+\langle X_n\rangle} \subseteq \\ \subseteq \quad &\sqrt{(\sqrt{I'+J})A+\langle X_n\rangle} = (\sqrt{I'+J})A+\langle X_n\rangle \end{aligned} \tag{1.5}$$

Por lo que hemos visto, se tiene,

$$\begin{aligned} (\sqrt{I'+J})A+\langle X_n\rangle = I'A+J_1A+\langle X_n\rangle \subseteq I+J_1A+\langle X_n\rangle \subseteq \\ \subseteq \sqrt{I+M+\langle X_n\rangle}+J_1A = \sqrt{I'A+JA+\langle X_n\rangle}+J_1A = \\ = \sqrt{I'A+JA+\langle X_n\rangle} = \sqrt{I+M+\langle X_n\rangle}. \end{aligned} \tag{1.6}$$

De (1.5) y (1.6) se tiene que $\sqrt{I+M+\langle X_n\rangle} = (\sqrt{I'+J})A+\langle X_n\rangle$ y de (1.6) se deduce $\sqrt{I+M+\langle X_n\rangle} = I+J_1A+\langle X_n\rangle$, luego $J_1A+\langle X_n\rangle$ es el ideal monomial que estábamos buscando.

□

Estamos ya en condiciones de demostrar que el carácter binomial de ideales del anillo de polinomios, se conserva por radicales.

Teorema 1.4.5 *Si $I \subseteq k[X]$ es un ideal binomial, entonces $\sqrt{I}$ es binomial.*

Dem. Veamos la demostración razonando por inducción sobre el número de indeterminadas. Para $n = 0$ el resultado es trivial.

Consideremos, para cada $j \in \{1, \ldots, n\}$, el anillo $A_j = k[X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n]$ y el ideal $I_j = I \cap A_j$. Aplicando inducción sobre el número de indeterminadas se tiene que $\sqrt{I_j}$ es binomial. Si definimos $\tilde{I} = I + \sum_{j=1}^{n}(\sqrt{I_j})k[X]$ e $\tilde{I}_j = \tilde{I} \cap A_j$, entonces $\tilde{I}$ es binomial, $\sqrt{\tilde{I}} = \sqrt{I}$ y $\sqrt{\tilde{I}_j} = \sqrt{I_j} \subseteq \tilde{I}_j$. Luego substituyendo I por $\tilde{I}$ podemos suponer que los I_j son radicales.

Se tiene (Lema 1.4.1)

$$\sqrt{I} = \sqrt{(I : (X_1 \cdots X_n)^\infty)} \cap \sqrt{I + \langle X_1 \rangle} \cap \ldots \cap \sqrt{I + \langle X_n \rangle},$$

y el ideal $I' = \sqrt{(I : (X_1 \cdots X_n)^\infty)}$ es binomial (Corolarios 1.3.11 y 1.3.12). Además, $I' = I + I'$. Si encontramos para cada j un ideal monomial M_j tal que $\sqrt{I + \langle X_j \rangle} = I + M_j$, se deducirá del Corolario 1.2.5 que $\sqrt{I}$ es binomial.

Usando el Lema 1.4.3, existe un ideal monomial J en A_j, con

$$I + \langle X_j \rangle = I_j k[X] + Jk[X] + \langle X_j \rangle.$$

Puesto que I_j es radical, por el Lema 1.4.2 también lo es $I_j k[X] + \langle X_j \rangle$, y por la Proposición 1.4.4 existe un ideal monomial M_1 tal que

$$\sqrt{I_j k[X] + \langle X_j \rangle + Jk[X]} = I_j k[X] + \langle X_j \rangle + M_1.$$

Entonces $\sqrt{I + \langle X_j \rangle} = I_j k[X] + \langle X_j \rangle + M_1 \subseteq I + \langle X_j \rangle + M_1 \subseteq \sqrt{I + \langle X_j \rangle} + M_1 \subseteq \sqrt{I + \langle X_j \rangle}$. Luego se tiene $\sqrt{I + \langle X_j \rangle} = I + \langle X_j \rangle + M_1$ y el ideal $M_j = \langle X_j \rangle + M_1$ es el buscado.

□

1.5 Variedades cortadas por binomios

Hasta ahora nos hemos ocupado de estudiar algunas propiedades de los ideales binomiales. Ahora estamos en condiciones de obtener una caracterización de aquellas variedades algebraicas afines cuyo ideal asociado es binomial.

Sea k un cuerpo algebraicamente cerrado y V una subvariedad algebraica afín de k^n, es decir, el conjunto de ceros de un ideal I del anillo $k[X]$, $V = \mathcal{V}(I)$. En estas condiciones, diremos que I es un ideal de definición de la variedad V.

Definición 1.5.1 *Diremos que V es una variedad cortada por binomios si su ideal radical asociado, $\mathcal{I}(V)$, es binomial.*

La condición de que V esté cortada por binomios es equivalente a que algún ideal de definición de V sea binomial (Teorema 1.4.5).

Definición 1.5.2 *Sea $\mathcal{Z}$ un conjunto de subíndices de $\{1, \ldots, n\}$. Llamaremos célula coordenada asociada a $\mathcal{Z}$ al toro*

$$(k^*)^{\mathcal{Z}} := \{(x_1, \ldots, x_n) \in k^n \mid x_i \neq 0 \Leftrightarrow i \in \mathcal{Z}\}.$$

Proposición 1.5.3 *La clausura para la topología de Zariski en k^n de la célula coordenada $(k^*)^{\mathcal{Z}}$ es la subvariedad algebraica de k^n definida por el ideal*

$$M(\mathcal{Z}) := \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle \subseteq k[X_1, \ldots, X_n].$$

Dem. Es claro que $M(\mathcal{Z}) = \{f \in k[X] \mid f(P) = 0, \forall P \in (k^*)^{\mathcal{Z}}\} = \mathcal{I}((k^*)^{\mathcal{Z}})$.

$\square$

Consideremos la subvariedad algebraica de k^n definida por un ideal I, $V = \mathcal{V}(I)$. Se cumple:

Proposición 1.5.4 *La clausura para la topología de Zariski en k^n de la intersección de V con la célula coordenada $(k^*)^{\mathcal{Z}}$, denotada $\overline{V \cap (k^*)^{\mathcal{Z}}}$, es la variedad definida por el ideal*

$$\tilde{I}_{\mathcal{Z}} := \left((I + M(\mathcal{Z})) : \left(\prod_{i \in \mathcal{Z}} X_i \right)^{\infty} \right).$$

Dem. Por comodidad en la notación, supongamos $\mathcal{Z} = \{1, \ldots, d\}$. Sean $P = (x_1, \ldots, x_d, 0, \ldots, 0) \in V \cap (k^*)^{\mathcal{Z}}$ y $f \in \widetilde{I}_{\mathcal{Z}}$. Sea $N \in \mathbb{Z}_{>0}$ con $f(\prod_{i \in \mathcal{Z}} X_i)^N \in I + M(\mathcal{Z})$. Entonces existen polinomios $f_1 \in I$, $f_2 \in M(\mathcal{Z})$ con $f(\prod_{i \in \mathcal{Z}} X_i)^N = f_1 + f_2$. Pero I es un ideal que define V, luego

$f_1(P) = 0$. Además como $f_2 \in M(\mathcal{Z})$, $f_2(P) = 0$. Por lo tanto $f(P) = 0$ y $\overline{V \cap (k^*)^{\mathcal{Z}}} \subseteq \mathcal{V}(\tilde{I}_{\mathcal{Z}})$.

Por otra parte, de

$$\mathcal{I}(V \cap (k^*)^{\mathcal{Z}}) = \mathcal{I}(\mathcal{V}(I) \cap \mathcal{V}(M(\mathcal{Z}))) = \mathcal{I}\mathcal{V}(I + M(\mathcal{Z})) = \sqrt{I + M(\mathcal{Z})} \subseteq \subseteq \sqrt{\widetilde{I}_{\mathcal{Z}}}$$

se deduce la otra contención.

□

Notación 1.5.5 Sean I un ideal de $k[X]$, V la variedad algebraica definida por I y $(k^*)^{\mathcal{Z}}$ una célula coordenada. Denotaremos

$$I_{\mathcal{Z}} := \mathcal{I}(\overline{V \cap (k^*)^{\mathcal{Z}}})$$

e $\widetilde{I}_{\mathcal{Z}}$ como en la Proposición 1.5.4.

Corolario 1.5.6 *$I_{\mathcal{Z}} = \sqrt{\tilde{I}_{\mathcal{Z}}}$. Además, si I es binomial entonces $I_{\mathcal{Z}}$ también lo es.*

Dem. La primera afirmación es consecuencia de la Proposición 1.5.4 (recuérdese que k es algebraicamente cerrado). Además, por el Corolario 1.2.7, $\tilde{I}_{\mathcal{Z}}$ es binomial, luego su radical también lo es (Teorema 1.4.5).

□

Los ideales $I_{\mathcal{Z}}$ que acabamos de definir serán utilizados para realizar la denominada descomposición celular del ideal I. Dicha descomposición es menos fina que la descomposición minimal usual, y como veremos, es primordial para determinar el carácter binomial de I.

Proposición 1.5.7 *Sea V una subvariedad algebraica de k^n y sea $I := \mathcal{I}(V)$. Entonces,*

$$I = \bigcap_{\mathcal{Z} \subseteq \{1,\dots,n\}} I_{\mathcal{Z}}.$$

Dem. Es claro que $V = \bigcup_{\mathcal{Z}} (V \cap (k^*)^{\mathcal{Z}})$, luego $\mathcal{I}(V) = \mathcal{I}\left(\bigcup_{\mathcal{Z}} (V \cap (k^*)^{\mathcal{Z}})\right)$ y por tanto $I = \bigcap_{\mathcal{Z}} \mathcal{I}(\overline{V \cap (k^*)^{\mathcal{Z}}})$.

□

Como hemos dicho, la caracterización de la variedades cortadas por monomios es el resultado fundamental no sólo de esta sección, sino del capítulo que estamos terminando. Para su demostración necesitaremos algunos resultados previos.

Lema 1.5.8 *Sea U un conjunto finito parcialmente ordenado, cumpliendo que todo subconjunto finito no vacío $\{u_1, \ldots, u_r\}$ de U tiene un extremo inferior en U (que denotaremos por $u_1 \wedge \ldots \wedge u_r$), y sea R cualquier anillo conmutativo. Supongamos que para cada $u \in U$ se tienen ideales J_u y M_u de forma que:*

(a) Si $u \leq v$ entonces $J_u \subseteq J_v$.

(b) $\sqrt{M_{u\wedge v}} \subseteq \sqrt{M_u + M_v}$.

En estas condiciones, los ideales

$$I_1 = \bigcap_{u\in U} (J_u + M_u) \quad e \quad I_2 = \left(\bigcap_{u\in U} M_u\right) + \sum_{u\in U} \left(J_u \cap \bigcap_{t\not\geq u} M_t\right),$$

tienen igual radical.

Dem. Veamos primero que $J_u \cap (\bigcap_{t\not\geq u} M_t) \subseteq (J_v + M_v)$ para cualesquiera $u, v \in U$. Si $u \leq v$, por (a) la contención es clara. Si $u \not\leq v$, v es uno de los t que aparecen en la intersección de la izquierda, luego también se tiene la contención. Por lo tanto $I_2 \subseteq I_1$ y $\sqrt{I_2} \subseteq \sqrt{I_1}$.

Sea ahora $\mathcal{P}$ un primo conteniendo a I_2. Consideremos el subconjunto de U dado por $V = \{v \in U \mid M_v \subseteq \mathcal{P}\}$. Si $v, v' \in V$, por la hipótesis (b), $v \wedge v' \in V$. Además $V \neq \emptyset$ pues $\mathcal{P} \supseteq \cap_{u\in U} M_u$, intersección finita. Luego V tiene un mínimo, $w \in V$. Como $\mathcal{P} \supseteq I_2$, en particular se cumple

$$\mathcal{P} \supseteq J_w \cap (\bigcap_{t\not\geq w} M_t),$$

y por definición de w, para $t \not\geq w$, $\mathcal{P} \not\supseteq M_t$, luego $\mathcal{P} \supseteq J_w$ y por tanto $\mathcal{P} \supseteq I_1$. Con esto demostramos que $\sqrt{I_1} \subseteq \sqrt{I_2}$, lo cual concluye la prueba del lema.

□

Lema 1.5.9 *Se consideran el anillo de polinomios de Laurent $R = k[Z_1, Z_1^{-1}, \ldots, Z_r, Z_r^{-1}]$, y el anillo $R' = R[Y_1, \ldots, Y_s]$. Si I es un ideal binomial de R' y M es un ideal monomial de R' de forma que $I + M$ es un ideal propio, entonces $(I + M) \cap R = I \cap R$.*

Dem. Supongamos que $f \in (I + M) \cap R$. Entonces, los términos de f son invertibles en R'. Como $I + M$ es un ideal propio de R', ningún término de f puede estar en $I + M$, luego $f \in I$ (Proposición 1.2.8) y por tanto $f \in I \cap R$.

□

Lema 1.5.10 *Se consideran el anillo de polinomios de Laurent $R = k[Z_1, Z_1^{-1}, \ldots, Z_r, Z_r^{-1}]$, y el anillo $R' = R[Y_1, \ldots, Y_s]$. Si I es un ideal de $k[Z, Y]$ y $f \in IR'$, entonces existe $N > 0$ tal que $f(\prod_{i=1}^t Z_i)^N \in I$.*

Dem. Si $f \in IR'$ entonces existen $g_1, \ldots, g_t \in I$ y $h_1, \ldots, h_t \in R'$ con $f = \sum_{j=1}^t g_j h_j$. Es claro que para cada $j \in \{1, \ldots, t\}$ existe un natural $N_j > 0$ tal que $(\prod_{i=1}^t Z_i)^{N_j} h_j \in k[Z, Y]$. Entonces, si elegimos un natural $N > \max\{N_1, \ldots, N_t\}$ se tiene $f(\prod_{i=1}^t Z_i)^N \in I$.

$\square$

Teorema 1.5.11 *Dado un cuerpo k algebraicamente cerrado, una subvariedad algebraica V de k^n está cortada por binomios si y sólo si se cumplen las tres condiciones siguientes:*

(i) Para cada célula coordenada $(k^*)^{\mathcal{Z}}$, $\overline{V \cap (k^*)^{\mathcal{Z}}}$ es una variedad cortada por binomios.

(ii) La familia de conjuntos $U = \{\mathcal{Z} \subseteq \{1, \ldots, n\} \mid V \cap (k^*)^{\mathcal{Z}} \neq \emptyset\}$ es cerrada por intersecciones.

(iii) Si $\mathcal{Z}$, $\mathcal{Z}' \in U$ y $\mathcal{Z} \subseteq \mathcal{Z}'$ entonces la proyección $(k^*)^{\mathcal{Z}'} \to (k^*)^{\mathcal{Z}}$ aplica $V \cap (k^*)^{\mathcal{Z}'}$ en $V \cap (k^*)^{\mathcal{Z}}$.

Dem. Como hicimos en 1.3.15, denotemos por $k[\mathcal{Z}]$ el anillo de polinomios $k[\{X_i\}_{i\in\mathcal{Z}}]$. Veamos primero que la condición (iii) es equivalente a la condición (iii') siguiente:

(iii') Si $\mathcal{Z}, \mathcal{Z}' \in U$ y $\mathcal{Z} \subseteq \mathcal{Z}'$, entonces $I_{\mathcal{Z}} \cap k[\mathcal{Z}] \subseteq I_{\mathcal{Z}'}$.

Podemos suponer sin pérdida de generalidad que $\mathcal{Z} = \{1, \ldots, d\} \subseteq \mathcal{Z}' = \{1, \ldots, s\}$. Supongamos que se cumple (iii'). Elijamos $P = (p_1, \ldots, p_s, 0, \ldots, 0) \in V \cap (k^*)^{\mathcal{Z}'}$ y sea $P^* = (p_1, \ldots, p_d, 0, \ldots, 0)$ su proyeción en $(k^*)^{\mathcal{Z}}$. Sea $f \in I_{\mathcal{Z}} = I(\overline{V \cap (k^*)^{\mathcal{Z}}})$; podemos escribir $f = f_1 + f_2$ con $f_1 \in k[X_1, \ldots, X_d]$ y $f_2 \in M(\mathcal{Z})$. Como $f_2 \in I_{\mathcal{Z}}$ (consecuencia de 1.5.4) entonces $f_1 \in I_{\mathcal{Z}} \cap k[\mathcal{Z}] \subseteq I_{\mathcal{Z}'}$ (condición (iii')). Además $P \in \mathcal{V}(I_{\mathcal{Z}'})$, luego $f_1(P) = 0$. Por otro lado $f_1 \in k[\mathcal{Z}]$, con lo cual $f_1(P) = f_1(P^*)$ y se tiene $f(P^*) = 0$. Por tanto $P^* \in \overline{V \cap (k^*)^{\mathcal{Z}}} \subseteq V$, y puesto que $P \in (k^*)^{\mathcal{Z}'}$ y $\mathcal{Z} \subseteq \mathcal{Z}'$, $P^* \in V \cap (k^*)^{\mathcal{Z}}$ con lo cual la condición (iii) se cumple.

Recíprocamente, supongamos que (iii) es cierta. Sean $f \in I_{\mathcal{Z}} \cap k[\mathcal{Z}]$ y $(p_1, \ldots, p_s, 0, \ldots, 0) \in V \cap (k^*)^{\mathcal{Z}'}$. Por hipótesis, $(p_1, \ldots p_d, 0, \ldots, 0) \in V \cap (k^*)^{\mathcal{Z}}$, y, como $f \in I_{\mathcal{Z}}$, se tiene $f(p_1, \ldots, p_d, 0, \ldots, 0) = 0$. Pero f es un polinomio en las indeterminadas $\{X_1, \ldots, X_d\}$ y $d \leq s$, luego

$f(p_1, \dots, p_s, 0, \dots, 0) = 0$. Por lo tanto $f \in \mathcal{I}(V \cap (k^*)^{\mathcal{Z}'}) = \mathcal{I}(\overline{V \cap (k^*)^{\mathcal{Z}'}}) = I_{\mathcal{Z}'}$.

Supongamos que V es una variedad cortada por binomios. Si denotamos $I = \mathcal{I}(V) \subseteq k[X]$, entonces I es binomial y por el Corolario 1.5.6, $I_{\mathcal{Z}}$ es binomial y la condición (i) es cierta.

Sean ahora $\mathcal{Z}_1, \mathcal{Z}_2 \in U$. Si $\mathcal{Z}_1 \cap \mathcal{Z}_2 \notin U$ entonces, por la Proposición 1.5.4, $\tilde{I}_{\mathcal{Z}_1 \cap \mathcal{Z}_2} = k[X]$, luego existiría un entero d de forma que $(\prod_{i \in \mathcal{Z}_1 \cap \mathcal{Z}_2} X_i)^d \in I + M(\mathcal{Z}_1 \cap \mathcal{Z}_2) = I + M(\mathcal{Z}_1) + M(\mathcal{Z}_2)$. Aplicando el Corolario 1.2.6, o bien $(\prod_{i \in \mathcal{Z}_1 \cap \mathcal{Z}_2} X_i)^d \in I + M(\mathcal{Z}_1)$ o bien $(\prod_{i \in \mathcal{Z}_1 \cap \mathcal{Z}_2} X_i)^d \in I + M(\mathcal{Z}_2)$. Así pues, o $\widetilde{I}_{\mathcal{Z}_1} = k[X]$ o $\widetilde{I}_{\mathcal{Z}_2} = k[X]$, en contra de que $\mathcal{Z}_1$ y $\mathcal{Z}_2$ están en U. Por lo tanto la condición (ii) es cierta.

Veamos que se cumple (iii'). Consideremos el anillo $R' = k[\mathcal{Z}^{\pm}][\{X_i\}_{i \notin \mathcal{Z}}]$. Se tiene

$$(I + M(\mathcal{Z}))R' \cap k[\mathcal{Z}^{\pm}] \subseteq I_{\mathcal{Z}'}R' \tag{1.7}$$

En efecto, como $\mathcal{Z} \in U$, el ideal $I_{\mathcal{Z}}$ es propio, luego $\tilde{I}_{\mathcal{Z}} = ((I + M(\mathcal{Z})) : (\prod_{i \in \mathcal{Z}} X_i)^{\infty})$ también lo es ya que $I_{\mathcal{Z}} = \sqrt{\tilde{I}_{\mathcal{Z}}}$ (Corolario 1.5.6). Entonces $(I + M(\mathcal{Z}))R'$ es también un ideal propio, pues en caso contrario $1 \in (I + M(\mathcal{Z}))R'$ y, aplicando el Lema 1.5.10, existe un natural $N > 0$ tal que $(\prod_{j \in \mathcal{Z}} X_j)^N \in I + M(\mathcal{Z})$ en contra de que $\tilde{I}_{\mathcal{Z}}$ es propio. Podemos entonces aplicar el Lema 1.5.9 y resulta $(I + M(\mathcal{Z}))R' \cap k[\mathcal{Z}^{\pm}] \subseteq IR' \cap k[\mathcal{Z}^{\pm}]$. Como además $I \subseteq I_{\mathcal{Z}'}$, se tiene $IR' \cap k[\mathcal{Z}^{\pm}] \subseteq I_{\mathcal{Z}'}R'$, con lo cual la condición (1.7) es cierta.

Sean $\mathcal{Z}, \mathcal{Z}' \in U$ con $\mathcal{Z} \subseteq \mathcal{Z}'$. Si $f \in I_{\mathcal{Z}} \cap k[\mathcal{Z}]$, entonces existe $N \in \mathbb{Z}_{>0}$ tal que $f^N \prod_{i \in \mathcal{Z}} X_i \in I + M(\mathcal{Z})$, luego por (1.7), $f^N \prod_{i \in \mathcal{Z}} X_i \in I_{\mathcal{Z}'}R'$, y puesto que $\prod_{i \in \mathcal{Z}} X_i$ es inversible en R', $f^N \in I_{\mathcal{Z}'}R'$. Aplicando el Lema 1.5.10, existe $M \in \mathbb{Z}_{>0}$ cumpliendo que $f^N(\prod_{i \in \mathcal{Z}} X_i)^M \in I_{\mathcal{Z}'}$. Es decir, $f^N \in I_{\mathcal{Z}'}$ ya que $I_{\mathcal{Z}'} = (I_{\mathcal{Z}'} : (\prod_{i \in \mathcal{Z}} X_i)^{\infty})$ puesto que $\mathcal{Z} \subseteq \mathcal{Z}'$. Por lo tanto $f \in I_{\mathcal{Z}'}$ y la condición (iii') se cumple.

Recíprocamente, supongamos ahora que V cumple las condiciones (i), (ii) y (iii) (y por tanto (iii')) y veamos que I es binomial. El conjunto U está parcialmente ordenado, con el orden dado por la inclusión, y además es cerrado por intersecciones. Para cada $\mathcal{Z} \in U$ se considera el ideal $J(\mathcal{Z}) = (I_{\mathcal{Z}} \cap k[\mathcal{Z}])k[X]$. Como se cumple la condición (i), $I_{\mathcal{Z}}$ es binomial, luego aplicando el Corolario 1.2.4 resulta $J_{\mathcal{Z}}$ binomial. Estamos en condiciones de aplicar el Lema 1.5.8, ya que:

(a) Como consecuencia de la condición (iii'), si $\mathcal{Z} \subseteq \mathcal{Z}'$, entonces $I_{\mathcal{Z}} \cap k[\mathcal{Z}] \subseteq I_{\mathcal{Z}'}$ y por tanto $J(\mathcal{Z}) \subseteq J(\mathcal{Z}')$.

(b) Puesto que $M(\mathcal{Z}_1 \cap \mathcal{Z}_2) = M(\mathcal{Z}_1) + M(\mathcal{Z}_2)$, se cumple $\sqrt{M(\mathcal{Z}_1 \cap \mathcal{Z}_2)} \subseteq \sqrt{M(\mathcal{Z}_1) + M(\mathcal{Z}_2)}$.

Como en el Lema 1.5.8, se consideran los ideales

$$I_1 = \bigcap_{\mathcal{Z} \in U} (J(\mathcal{Z}) + M(\mathcal{Z})) \;\; I_2 = \left(\bigcap_{\mathcal{Z} \in U} M(\mathcal{Z}) \right) + \sum_{\mathcal{Z} \in U} \left(J(\mathcal{Z}) \cap \bigcap_{\mathcal{Z}' \not\supseteq \mathcal{Z}} M(\mathcal{Z}') \right),$$

que cumplen $\sqrt{I_1} = \sqrt{I_2}$.

Aplicando el Corolario 1.2.5, se tiene que los ideales $\bigcap_{\mathcal{Z} \in U} M(\mathcal{Z})$ y $J(\mathcal{Z}) \cap (\bigcap_{\mathcal{Z}' \not\supseteq \mathcal{Z}} M(\mathcal{Z}'))$ son binomiales ($J(\mathcal{Z})$ es binomial para todo $\mathcal{Z} \in U$). Luego I_2 es binomial y por el Teorema 1.4.5 $\sqrt{I_2}$ es binomial. Por otra parte, $J(\mathcal{Z}) + M(\mathcal{Z}) = I_{\mathcal{Z}}$. En efecto, de las definiciones es claro que $J(\mathcal{Z}) + M(\mathcal{Z}) \subseteq I_{\mathcal{Z}}$. Recíprocamente, sea $f \in I_{\mathcal{Z}}$ y sean $f_1 \in k[\mathcal{Z}]$, $f_2 \in M(\mathcal{Z})$ cumpliendo $f = f_1 + f_2$. Entonces $f_1 \in I_{\mathcal{Z}} \cap k[\mathcal{Z}]$, luego $f_1 \in J(\mathcal{Z})$.

Por lo tanto $I_1 = \bigcap_{\mathcal{Z} \in U} (J(\mathcal{Z}) + M(\mathcal{Z})) = \bigcap_{\mathcal{Z} \in U} I_{\mathcal{Z}} = I$, y se tiene $\sqrt{I_1} = \sqrt{I} = I$. Luego $I = \sqrt{I_2}$ es binomial.

$\square$

Capítulo 2

Curvas monomiales

Como se dijo en la introducción, el tema central de esta tesis es el estudio de las curvas afines cuyo ideal asociado es binomial. En el caso irreducible, es conocido que estas curvas son, esencialmente, aquellas que admiten una parametrización dada por monomios. Comenzaremos analizando este caso para poder entender mejor la extensión que hemos hecho al caso general.

2.1 Curvas monomiales irreducibles

Consideremos el espacio afín de dimensión n, $\mathcal{A}^n(k)$, sobre un cuerpo algebraicamente cerrado, k, de característica cero. En este espacio, las curvas monomiales irreducibles son aquellas que admiten un parametrización dada por monomios.

Definición 2.1.1 *Sea C una curva en el espacio $\mathcal{A}^n(k)$. Se dice que C es monomial si admite una parametrización dada por monomios. Es decir, si existen $h_1, \ldots, h_n \in \mathbb{Z}_{\geq 0}$ y $\lambda_1, \ldots, \lambda_n \in k$, con* m.c.d.$\{h_i \mid \lambda_i \neq 0\} = 1$, *tales que C es la imagen del morfismo de variedades,*

$$\begin{array}{rccl} \Psi: & \mathcal{A}^1(k) & \longrightarrow & \mathcal{A}^n(k) \\ & t & \longmapsto & (\lambda_1 t^{h_1}, \ldots, \lambda_n t^{h_n}) \end{array} .$$

En la situación de la definición, escribiremos:

$$C \equiv \left\{ \begin{array}{c} x_1 = \lambda_1 t^{h_1} \\ \vdots \\ x_n = \lambda_n t^{h_n} \end{array} \right. .$$

Cada parametrización monomial Ψ queda determinada si conocemos los vectores $\underline{h} = (h_1, \ldots, h_n)$, que llamaremos vector de exponentes de la parametrización Ψ, y $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n)$, vector de coeficientes de la parametrización Ψ.

A diferencia del caso irreducible, cuando trabajemos con curvas con varias componentes monomiales, los vectores coeficientes van a ser decisivos para comprobar si la curva tiene asociado un ideal binomial. Por ello, y a pesar de que los resultados referentes a curvas monomiales irreducibles se podrían deducir restringiéndonos a curvas con todos sus coeficientes iguales a uno, trabajaremos desde un principio con un vector de coeficientes genérico.

Notación 2.1.2 En lo que sigue, dados $\mathcal{Z} \subseteq \{1, \ldots, n\}$, un conjunto cualquiera S y $\underline{\alpha} \in S^n$, denotaremos por $\underline{\alpha}_{\mathcal{Z}}$ el vector obtenido al proyectar $\underline{\alpha}$ en las coordenadas en $\mathcal{Z}$.

Definición 2.1.3 *Sean $C \subset \mathcal{A}^n(k)$ una curva monomial irreducible y Ψ una parametrización monomial de C dada por los vectores $(\underline{h}, \underline{\lambda})$. Llamaremos célula asociada a C al conjunto $\mathcal{Z} = \{i \in \{1, \ldots, n\} \mid \lambda_i \neq 0\}$. Además, denotaremos por $C_{\mathcal{Z}}$ a la curva monomial irreducible de $\mathcal{A}^{|\mathcal{Z}|}(k)$ con parametrización dada por los vectores $(\underline{\lambda}_{\mathcal{Z}}, \underline{h}_{\mathcal{Z}})$.*

Nota 2.1.4 La célula $\mathcal{Z}$ no depende de la parametrización monomial elegida para C, pues $i \in \mathcal{Z}$ si y sólo si $X_i \notin \mathcal{I}(C)$; es decir, $\mathcal{Z}$ es la célula asociada a $\mathcal{I}(C)$ según la Definición 1.3.14 .

Proposición 2.1.5 *El ideal asociado a $C_{\mathcal{Z}}$ es un ideal primo, de altura $|\mathcal{Z}| - 1$, que no contiene monomios y binomial.*

Dem. Por comodidad en la notación supongamos que $\mathcal{Z} = \{1, \ldots, n\}$; es decir, $C_{\mathcal{Z}} = C$ y $\lambda_i \neq 0$ para todo $i \in \{1, \ldots, n\}$. $I = \mathcal{I}(C)$ es un ideal de $k[X_1, \ldots, X_n]$ primo y con altura $n-1$, ya que C es una variedad irreducible de dimensión uno. Supongamos que existiese algún monomio en I. Por ser I un ideal primo, tendríamos $X_i \in I$ para algún $i \in \{1, \ldots, n\}$, en contra de que $\{1, \ldots, n\}$ es la célula asociada a I.

Como $I = \mathcal{I}(C)$, es claro que I es el núcleo del homomorfismo de k-álgebras,

$$\begin{array}{rrcl} \Phi: & k[X_1, \ldots, X_n] & \longrightarrow & k[T] \\ & X_i & \longmapsto & \lambda_i T^{h_i}. \end{array}$$

Sea $f \in I$. Escribamos $f = f_0 + f_1 + \ldots + f_s$ siendo f_i la suma de los términos de f con exponente $\underline{m}$ tal que $\underline{h}\,\underline{m} = i$. Entonces $\Phi(f_i) = bT^i$ con $b \in k$, luego $0 = \Phi(f) = b_0 + b_1 T + \ldots + b_s T^s$. Por lo tanto $b_i = 0$ para todo i, y tenemos que los polinomios f_i pertenecen también al núcleo de Φ, que es el ideal I. Teniendo en cuenta esto, tomemos un polinomio $f \in I$, $f = a_1 X^{\underline{m}_1} + \ldots + a_r X^{\underline{m}_r}$, de forma que existe un número natural N con $\underline{h}\,\underline{m}_i = N$ para todo i. Como $f \in \ker(\Phi)$, $a_1 \underline{\lambda}^{\underline{m}_1} + \ldots + a_r \underline{\lambda}^{\underline{m}_r} = 0$, luego

$$f = \sum_{i=1}^{r-1} (a_1 \underline{\lambda}^{\underline{m}_1} + \ldots + a_i \underline{\lambda}^{\underline{m}_i}) \left(\frac{1}{\underline{\lambda}^{\underline{m}_i}} \right) \left(X^{\underline{m}_i} - \frac{\underline{\lambda}^{\underline{m}_i}}{\underline{\lambda}^{\underline{m}_{i+1}}} X^{\underline{m}_{i+1}} \right),$$

y el polinomio f es combinación de los binomios $X^{\underline{m}_i} - \frac{\underline{\lambda}^{\underline{m}_i}}{\underline{\lambda}^{\underline{m}_{i+1}}} X^{\underline{m}_{i+1}}$, que a su vez están en el núcleo. Por lo tanto,

$$I = \left\langle \left\{ X^{\underline{m}_1} - \frac{\underline{\lambda}^{\underline{m}_1}}{\underline{\lambda}^{\underline{m}_2}} X^{\underline{m}_2} \mid \underline{m}_1 \underline{h} = \underline{m}_2 \underline{h} \right\} \right\rangle$$

y el ideal I es binomial.

$\square$

Usando este resultado, podemos demostrar que los ideales asociados a curvas monomiales irreducibles son la suma del ideal asociado a un carácter parcial con un ideal generado por indeterminadas. Por lo tanto, podremos tratar combinatoriamente las curvas monomiales irreducibles, estudiando los retículos asociados.

Antes de seguir, recordemos que en la Nota 1.3.15 se definieron, dado $\mathcal{Z} \subseteq \{1, \ldots, n\}$, el ideal $M(\mathcal{Z}) = \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle$, el anillo de polinomios $k[\mathcal{Z}] = k[\{X_i\}_{i \in \mathcal{Z}}]$ y el $\mathbb{Z}$-módulo $\mathbb{Z}^{\mathcal{Z}} = \{(a_1, \ldots, a_n) \mid a_i = 0, \forall i \notin \mathcal{Z}\}$ con la identificación natural $\mathbb{Z}^{\mathcal{Z}} \equiv \mathbb{Z}^{|\mathcal{Z}|}$.

Además, dado un ideal $I \subseteq k[X^{\pm}]$ denotaremos $\mathcal{V}(I) := \{P \in (k^*)^n \mid f(P) = 0, \forall f \in I\}$.

Proposición 2.1.6 *Sean C una curva monomial irreducible y $\mathcal{Z}$ su célula asociada. Se cumple:*

1. *Existe un único carácter parcial $\rho : L_\rho \to k^*$ tal que $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$, donde L_ρ es un retículo saturado de $\mathbb{Z}^{\mathcal{Z}}$.*

2. $\underline{h}$ *es el vector de exponentes de una parametrización monomial de la curva* C *si y sólo si* $L_\rho = \langle \underline{h}_{\mathcal{Z}} \rangle^\perp$. *Por lo tanto,* $\operatorname{rango}(L_\rho) = |\mathcal{Z}| - 1$ *y* $\underline{h}_{\mathcal{Z}}$ *está unívocamente determinado si exigimos que el máximo común divisor de sus coordenadas sea uno.*

3. $\underline{\lambda}$ *es el vector de coeficientes de una parametrización monomial para la curva* C *si y sólo si* $\underline{\lambda}_{\mathcal{Z}} \in \mathcal{V}(I(\rho)) \subset (k^*)^{\mathcal{Z}}$ *y* $\lambda_i = 0$ *para todo* $i \notin \mathcal{Z}$.

Dem. Sea $\mathcal{Z}$ la célula asociada a C. Por la definición de $C_{\mathcal{Z}}$ es claro que $\mathcal{I}(C) = \mathcal{I}(C_{\mathcal{Z}}) + \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle$. Por lo tanto, usando la Proposición 2.1.5 y el Corolario 1.3.16, se deduce que existe un único carácter parcial saturado ρ sobre un subretículo de $\mathbb{Z}^{\mathcal{Z}}$, L_ρ, con $\mathcal{I}(C_{\mathcal{Z}}) = I_+(\rho)$. Luego $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$.

Es evidente que $(\underline{h}, \underline{\lambda})$ son los vectores de una parametrización monomial para la curva C si y sólo si $\mathcal{I}(C)$, que es el ideal $I_+(\rho) + M(\mathcal{Z})$, es el núcleo del homomorfismo

$$\begin{array}{rccll} \Phi : & k[\mathcal{Z}] & \longrightarrow & k[T] & \\ & X_i & \longmapsto & \lambda_i T^{h_i} & \text{si } i \in \mathcal{Z} \\ & X_i & \longmapsto & 0 & \text{si } i \notin \mathcal{Z} \end{array} .$$

Por lo tanto, si $(\underline{h}, \underline{\lambda})$ son vectores de una parametrización monomial para C, como $I_+(\rho)$ está generado por el conjunto $G = \{X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-} \mid \underline{m} \in L_\rho\}$ entonces para todo $\underline{m} \in L_\rho$, $\Phi(X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-}) = 0$, luego $\underline{m}\, \underline{h}_{\mathcal{Z}} = 0$ y $\rho(\underline{m}) = (\underline{\lambda}_{\mathcal{Z}})^{\underline{m}}$. Por lo tanto $L_\rho \subseteq \langle \underline{h}_{\mathcal{Z}} \rangle^\perp$ y $\underline{\lambda}_{\mathcal{Z}} \in \mathcal{V}(I(\rho))$. Además, si $\underline{m} \in \mathbb{Z}^{\mathcal{Z}}$ cumple que $\underline{m}\, \underline{h}_{\mathcal{Z}} = 0$, entonces el binomio $X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-} \in I_+(\rho)$. Según las definiciones de $I(\rho)$ e $I_+(\rho)$ se tiene $I_+(\rho) k[X^{\pm}] \subset I(\rho)$, luego $X^{\underline{m}} - \rho(\underline{m}) \in I(\rho)$. Pero los únicos binomios de $I(\rho)$ son de la forma $X^{\underline{m}} - \rho(\underline{m})$ con $\underline{m} \in L_\rho$ (Teorema 1.3.5), por lo tanto $\underline{m} \in L_\rho$ y se deduce $\langle \underline{h}_{\mathcal{Z}} \rangle^\perp \subseteq L_\rho$. Luego $L_\rho = \langle \underline{h}_{\mathcal{Z}} \rangle^\perp$ y el retículo L_ρ tiene rango $|\mathcal{Z}| - 1$. Además, si $i \in \mathcal{Z}$ entonces $X_i \in \mathcal{I}(C)$, luego $\lambda_i = 0$ y h_i puede tomar cualquier valor.

Recíprocamente, si los vectores $(\underline{h}, \underline{\lambda})$ cumplen las condiciones del enunciado, entonces es claro que $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z}) \subseteq \ker(\Phi)$. Por lo tanto, la curva monomial irreducible de vectores $(\underline{h}, \underline{\lambda})$ está contenida en C, luego deben coincidir.

□

Definición 2.1.7 *Sea* C *una curva monomial irreducible con célula asociada* $\mathcal{Z}$. *Llamaremos carácter parcial asociado a* C *al único carácter* $\rho : L_\rho \to k^*$ *en* $\mathbb{Z}^{\mathcal{Z}}$ *tal que* $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$. *Además, diremos que* L_ρ *es el retículo asociado a la curva* C.

Notación 2.1.8 Como consecuencia del apartado 2 de la Proposición 2.1.6 se deduce que si $i \notin \mathcal{Z}$ entonces h_i puede tomar cualquier valor. En lo sucesivo representaremos este hecho escribiendo $h_i = \infty$. Además, la parametrización de la curva queda determinada si conocemos la terna $(\mathcal{Z}, \underline{h}_{\mathcal{Z}}, \underline{\lambda}_{\mathcal{Z}})$.

Veamos a continuación cuáles son los cambios de parámetro permitidos entre las parametrizaciones monomiales de una curva monomial.

Proposición 2.1.9 *Sea C una curva monomial irreducible. Si Ψ y $\widetilde{\Psi}$ son dos parametrizaciones monomiales de la curva C, entonces existe $\alpha \in k^*$ tal que $\widetilde{\Psi}(t) = \Psi(\alpha t)$.*

Dem. Podemos suponer, sin pérdida de generalidad, que la célula asociada a la curva C es la total. Denotemos por $(\underline{h}, \underline{\lambda})$ los vectores de la parametrización Ψ y por $(\underline{\widetilde{h}}, \underline{\widetilde{\lambda}})$ los vectores de $\widetilde{\Psi}$. Aplicando la Proposición 2.1.6, se cumple que $\underline{h} = \underline{\widetilde{h}}$ y $\underline{\lambda}^{\underline{m}} = \underline{\widetilde{\lambda}}^{\underline{m}}$ para todo $\underline{m}$ ortogonal a $\underline{h}$. Consideremos un vector de coordenadas enteras $\underline{a}$ tal que $\underline{a}\,\underline{h} = 1$ y sea $\alpha = (\underline{\widetilde{\lambda}}/\underline{\lambda})^{\underline{a}}$. Como $a_1 h_1 + \ldots + a_n h_n = 1$ entonces, para cada $i \in \{1, \ldots, n\}$ se tiene $a_1 h_1 h_i + \ldots + (a_i h_i h_i - h_i) + \ldots + a_n h_n h_i = 0$; es decir, $h_i \underline{a} - \underline{e}_i \in L_\rho = \langle \underline{h} \rangle^\perp$ donde $\underline{e}_i$ denota el i-ésimo vector de la base canónica de $\mathbb{Z}^n$. Por lo tanto, $\underline{\lambda}^{h_i \underline{a} - \underline{e}_i} = \underline{\widetilde{\lambda}}^{h_i \underline{a} - \underline{e}_i}$ y

$$\alpha^{h_i} = \left(\frac{\underline{\widetilde{\lambda}}^{\underline{a}}}{\underline{\lambda}^{\underline{a}}} \right)^{h_i} = \frac{\widetilde{\lambda}_i}{\lambda_i}, \ \forall i \in \{1, \ldots, n\}.$$

De estas igualdades es inmediato que $\widetilde{\Psi}(t) = \Psi(\alpha t)$.

□

Como consecuencia de la Proposición 2.1.5, si C es una curva monomial irreducible, entonces el ideal $\mathcal{I}(C)$, que es primo y de altura $n-1$, es además binomial. Pero estas propiedades no son suficientes para caracterizar los ideales asociados a curvas monomiales irreducibles. Veamos cuál es la otra condición necesaria para establecer dicha caracterización.

Definición 2.1.10 *Sea I un ideal primo del anillo de polinomios $k[X]$ y $\mathcal{Z}$ la célula asociada a I. Diremos que I es combinatoriamente finito si no contiene binomios de la forma $X^{\underline{m}} - c$ con $m_i > 0$ para todo $i \in \mathcal{Z}$ y $m_i = 0$ para todo $i \notin \mathcal{Z}$.*

Nota 2.1.11 El término "combinatoriamente finito" cobra sentido cuando se aplica a ideales de carácter parcial. Como se verá en el capítulo 4, un retículo L_ρ cumpliendo determinadas condiciones tiene asociado un semigrupo S, y el ideal $I_+(\rho)$ cumple la condición de la definición anterior si y sólo si el semigrupo S es combinatoriamente finito (en el sentido de la teoría de semigrupos, [BCMP1]).

Proposición 2.1.12 *Si I es el ideal de una curva monomial irreducible, entonces I es combinatoriamente finito.*

Dem. Sean C la curva que define I, $\mathcal{Z}$ su célula asociada y $(\underline{h}, \underline{\lambda})$ los vectores de una parametrización monomial para C. Si I no es combinatoriamente finito, entonces existe $\underline{m} \in \mathbb{Z}^{\mathcal{Z}}$ tal que $m_i > 0$ para todo $i \in \mathcal{Z}$ y $X^{\underline{m}} - c \in I$. Luego $\underline{\lambda}_{\mathcal{Z}}^{\underline{m}} T^{\underline{h}_{\mathcal{Z}}\, \underline{m}} = c$ y por tanto $\underline{h}_{\mathcal{Z}}\, \underline{m} = 0$. Pero como $\underline{h}_{\mathcal{Z}} \neq 0$ (pues C es una curva), entonces existe $i \in \mathcal{Z}$ tal que $h_i > 0$ y por tanto $\underline{h}_{\mathcal{Z}}\, \underline{m} > 0$, lo cual es absurdo.

$\square$

Veamos cómo afecta al retículo la condición de combinatoriamente finito.

Proposición 2.1.13 *Sea $\rho : L_\rho \to k^*$ un carácter parcial sobre $\mathbb{Z}^n$. Si el ideal $I_+(\rho) \subset k[X]$ es primo y combinatoriamente finito, entonces el retículo $L_\rho \subseteq \mathbb{Z}^n$ no contiene vectores con todas las coordenadas estrictamente positivas (o todas estrictamente negativas).*

Dem. Basta tener en cuenta que $I_+(\rho) = \langle \{X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-} \mid \underline{m} \in L_\rho\} \rangle$ y su célula asociada es $\{1, \ldots, n\}$, pues no contiene monomios.

$\square$

Corolario 2.1.14 *Si C es una curva monomial irreducible con célula asociada $\mathcal{Z}$ y $\rho : L_\rho \to k^*$ es el carácter parcial asociado a C, entonces el retículo L_ρ no admite vectores con todas las coordenadas estrictamente positivas (o estrictamente negativas). Además, si $\underline{h}$ es el vector de exponentes de C y se cumple que $h_i > 0$ para todo $i \in \mathcal{Z}$, entonces $L_\rho \cap (\mathbb{Z}_{\geq 0})^{\mathcal{Z}} = \langle \underline{0} \rangle$.*

Dem. Por la Proposición 2.1.12, el ideal $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$ es combinatoriamente finito. Por lo tanto, aplicando la proposición anterior, la primera afirmación es cierta.

Si $h_i > 0$ para todo $i \in \mathcal{Z}$ entonces $L_\rho \cap (\mathbb{Z}_{\geq 0})^{\mathcal{Z}} = \langle \underline{0} \rangle$. En caso contrario, existiría un vector no nulo $\underline{m} \in L_\rho$ con $m_i \geq 0$ para todo i. Entonces

$X^{\underline{m}} - \rho(\underline{m}) \in \mathcal{I}(C)$, luego $\underline{h}\,\underline{m} = 0$. Pero $\underline{h}\,\underline{m} > 0$, pues $h_i > 0$ para todo $i \in \mathcal{Z}$ y $\underline{m}$ es un vector de $(\mathbb{Z}_{\geq 0})^{\mathcal{Z}}$ no nulo.

□

Ahora queremos dar la vuelta a estos resultados, es decir si $I \subset k[X]$ es un ideal primo y de altura $n-1$, veamos como las condiciones de ser binomial y combinatoriamente finito son suficientes para que I defina una curva monomial irreducible en $\mathcal{A}^n(k)$.

Sabemos que si un ideal primo de carácter parcial es combinatoriamente finito, entonces su retículo asociado cumple la condición de no contener vectores con todas sus coordenadas estrictamente positivas. Esta condición sobre el retículo va a ser determinante para asegurar la existencia de un vector con coordenadas enteras no negativas ortogonal a dicho retículo (candidato a vector de exponentes de la parametrización monomial). Para demostrar este resultado vamos a utilizar el método de Fourier-Motzkin, técnica de eliminación para conos ([Gun], cap.1).

Se consideran una matriz $B \in \mathcal{M}_{m\times n}(\mathbb{Q})$, un entero $k \in \{1, \ldots, n\}$ y se construye, como se explica a continuación, la matriz B_k obtenida tras hacer la eliminación k-ésima de Fourier-Motzkin (F-M) a la matriz B. Si denotamos por $\underline{b}_i$, donde $i \in \{1, \ldots, m\}$, a las filas de B, entonces B_k se obtiene (salvo reordenación de las filas) mediante los siguientes pasos:

(a) Para todo $i \in \{1, \ldots, m\}$ tal que $b_{ik} = 0$, se añade a B_k la fila $\underline{b}_i$.

(b) Para cualesquiera $i, j \in \{1, \ldots, m\}$ distintos tales que $b_{ik} > 0$ y $b_{jk} < 0$, se añade a B_k la fila $b_{ik}\underline{b}_j + (-b_{jk})\underline{b}_i$.

Lema 2.1.15 *Sean $B \in \mathcal{M}_{m\times n}(\mathbb{Q})$, y S el sistema de inecuaciones $B\underline{x} \leq \underline{0}$. Si B_k es la matriz obtenida al hacer la eliminación k-ésima de Fourier-Motzkin en el sistema S y P, P_k son los conjuntos*

$$P := \{\underline{x} \in \mathbb{Q}^n \mid B\underline{x} \leq \underline{0}\} \quad P_k := \{\underline{x} \in \mathbb{Q}^n \mid B_k\underline{x} \leq \underline{0}\},$$

entonces $P_k = \{\underline{x} + \lambda\underline{e}_k \mid \underline{x} \in P \text{ y } \lambda \in \mathbb{Q}\}$, donde $\underline{e}_k$ denota el k-ésimo vector de la base canónica de $\mathbb{Q}^n$.

Dem. Sea $\underline{x} \in P_k$. Si $i, j \in \{1, \ldots, m\}$ son tales que $b_{ik} > 0$ y $b_{jk} < 0$ entonces $b_{ik}(\underline{b}_j) + (-b_{jk})\underline{b}_i$ es una fila de la matriz B_k. Como $\underline{x} \in P_k$, entonces $B_k\underline{x} \leq \underline{0}$, luego $[b_{ik}\underline{b}_j + (-b_{jk})\underline{b}_i]\underline{x} \leq 0$ y por tanto $\left(\frac{1}{b_{ik}}\right)\underline{b}_i\underline{x} \leq \left(\frac{1}{b_{jk}}\right)\underline{b}_j\underline{x}$.

Entonces existe $\lambda \in \mathbb{Q}$ tal que

$$\max_i \left\{ \left(\frac{1}{b_{ik}}\right) \underline{b_i}\underline{x} \mid b_{ik} > 0 \right\} \leq \lambda \leq \min_j \left\{ \left(\frac{1}{b_{jk}}\right) \underline{b_j}\underline{x} \mid b_{jk} < 0 \right\}.$$

Además, para todo $i \in \{1, \ldots, m\}$ se tiene que $\underline{b_i}\,\underline{x} \leq \lambda b_{ik}$, ya que si $b_{ik} > 0$ entonces $(\frac{1}{b_{ik}})\underline{b_i}\underline{x} \leq \lambda$, si $b_{jk} < 0$ entonces $(\frac{1}{b_{jk}})\underline{b_j}\underline{x} \geq \lambda$ y si $b_{ik} = 0$ entonces $\underline{b_i}$ es una fila de la matriz B_k y $\underline{x} \in P_k$ luego $\underline{b_i}\underline{x} \leq \underline{0}$. Por lo tanto, $B(\underline{x} - \lambda\underline{e_k}) \leq 0$ y tenemos $\underline{x} - \lambda\underline{e_k} \in P$.

La contención $\{\underline{x} + \lambda\underline{e_k} \mid \underline{x} \in P \text{ y } \lambda \in \mathbb{Q}\} \subseteq P_k$ se deduce de forma inmediata de la construcción de B_k.

□

Proposición 2.1.16 *Sea L un subretículo de $\mathbb{Z}^n$ que no contiene ningún vector con todas las coordenadas estrictamente positivas. Entonces, existe un vector no nulo $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ tal que $\underline{h}\,\underline{m} = 0$ para todo $\underline{m} \in L$.*

Dem. Sean r el rango del retículo L y $\{\underline{v}_1, \ldots, \underline{v}_r\}$ una base de L como $\mathbb{Z}$-módulo. Consideremos el $\mathbb{Q}$-subespacio vectorial de $\mathbb{Q}^n$, $L_{\mathbb{Q}}$, generado por $\{\underline{v}_1, \ldots, \underline{v}_r\}$. Si $\underline{v}_i = (a_{1i}, \ldots, a_{ni})$ para todo $i \in \{1, \ldots, r\}$, entonces $L_{\mathbb{Q}} = \{-A\underline{\lambda} \mid \underline{\lambda} \in \mathbb{Q}^r\}$ siendo

$$A = \begin{pmatrix} -a_{11} & \ldots & -a_{1r} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \ldots & -a_{nr} \end{pmatrix}.$$

Por hipótesis se tiene que no existe $\underline{\lambda} \in \mathbb{Z}^r$ con $-A\underline{\lambda} > \underline{0}$, o equivalentemente, $A\underline{\lambda} < \underline{0}$. Pero esto es lo mismo que decir que no existe $\underline{\lambda} \in \mathbb{Q}^r$ con $-A\underline{\lambda} > \underline{0}$, o equivalentemente, $A\underline{\lambda} < \underline{0}$.

Denotemos por b_{ij} los coeficientes de la matriz A y consideremos el sistema de inecuaciones,

$$S \equiv \left\{ \begin{array}{c} b_{11}X_1 + \ldots + b_{1r}X_r + X_0 \leq 0 \\ \vdots \\ b_{n1}X_1 + \ldots + b_{nr}X_r + X_0 \leq 0 \end{array} \right. .$$

La condición anterior se traduce en que S no tiene solución con $X_0 > 0$. Denotemos $\underline{z} = (-1, \ldots, -1)$ y sea $\widetilde{B} = (B, -\underline{z})$ la matriz del sistema S. Si hacemos la primera eliminación de F-M a la matriz $\widetilde{B}$, obtenemos una matriz $\widetilde{B}_1$ con un determinado número, m_1, de filas, $r+1$ columnas y primera columna igual a cero (es decir, en el nuevo sistema de inecuaciones con matriz $\widetilde{B}_1$, no aparece X_1). Además, existe una matriz C_1, producto de matrices elementales, con m_1 filas y n columnas tal que $C_1\widetilde{B} = \widetilde{B}_1$. Por lo tanto, si $\widetilde{B}_1 = (B_1, -\underline{z}_1)$ (separando la última columna) entonces $C_1 B = B_1$ y $C_1\underline{z} = \underline{z}_1$. Por las operaciones elementales realizadas en la eliminación de F-M, la matriz C_1 no tiene ningún coeficiente negativo. Aplicando el Lema 2.1.15, el conjunto de soluciones del sistema $\widetilde{B}_1\underline{x} \leq \underline{0}$ está contenido en el conjunto

$$\{\underline{x} + \lambda\underline{e}_1 \mid \underline{x} \text{ solución de S y } \lambda \in \mathbb{Q}\},$$

donde $\underline{e}_1$ representa el primer vector de la base canónica de $\mathbb{Q}^{r+1}$.

Repetimos el proceso eliminando sucesivamente $X_2, \ldots, X_r$ y encontramos una matriz C con coeficientes enteros no negativos, m_r filas y n columnas cumpliendo:

1. $CB = 0$.
2. Si $\overline{P}$ es el conjunto de soluciones del sistema $C\widetilde{B} \leq \underline{0}$, entonces $\overline{P}$ está contenido en el conjunto,

$$\begin{aligned}\{\underline{x} + \lambda_1\underline{e}_1 + \ldots + \lambda_r\underline{e}_r \mid \underline{x} \text{ solución de S y } \lambda_i \in \mathbb{Q}\} &= \\ = \{(\underline{x}, x_0) \mid \underline{x} \in \mathbb{Q}^r \text{ y } \exists \underline{y} \in \mathbb{Q}^r \text{ tal que } (\underline{y}, x_0) \text{ es solución de } S\}\end{aligned}$$

Luego $\overline{P} \subseteq \mathbb{Q}^r \times \mathbb{Q}_{\leq 0}$ ya que, por hipótesis, el sistema S no admite soluciones con $X_0 > 0$. Ahora bien, si denotamos por c_{ij} a los coeficientes de la matriz C, el sistema $C\widetilde{B} \leq \underline{0}$ resulta ser (ya que $CB = 0$)

$$\left\{\begin{array}{c} 0 \leq (-\sum_{j=1}^n c_{1j})X_0 \\ \vdots \\ 0 \leq (-\sum_{j=1}^n c_{m_r j})X_0 \end{array}\right. .$$

Consideremos los valores enteros no positivos, $\gamma_1 = -\sum_{j=1}^n c_{1j}, \ldots, \gamma_{m_r} = -\sum_{j=1}^n c_{m_r j}$. Como P está contenido en $\mathbb{Q}^r \times \mathbb{Q}_{\leq 0}$, debe existir $i \in \{1, \ldots, m_r\}$ con $\gamma_i < 0$. Tomando $\underline{h} = (c_{i1}, \ldots, c_{in})$, se tiene:

1. Puesto que $CB = 0$, $\underline{h}B = \underline{0}$, luego $\underline{h}\,\underline{m} = 0$ para todo $\underline{m} \in L$.
2. Puesto que $\gamma_i < 0$, $\underline{h}$ es un vector no nulo (de coordenadas enteras no negativas).

Por lo tanto, $\underline{h}$ cumple las condiciones del enunciado.

□

Proposición 2.1.17 *Sea I un ideal del anillo de polinomios $k[X]$, primo, de altura $n-1$, binomial y combinatoriamente finito. Entonces I es el ideal asociado a una curva monomial irreducible.*

Dem. Sea $\mathcal{Z}$ la célula asociada a I. Como I es un ideal binomial primo, podemos aplicar el Corolario 1.3.16, luego existe un carácter parcial saturado en $\mathbb{Z}^{\mathcal{Z}}$, ρ, tal que $I = I_+(\rho) + M(\mathcal{Z})$. Como I es combinatoriamente finito, entonces $I_+(\rho)$ también lo es y por la Proposición 2.1.13 el retículo $L_\rho \subseteq \mathbb{Z}^{\mathcal{Z}}$ no contiene vectores con todas sus coordenadas estrictamente positivas. Por lo tanto, aplicando la Proposición 2.1.16, existe un vector $\underline{h}_{\mathcal{Z}} \in \mathbb{Z}^{\mathcal{Z}}$ con todas sus coordenadas no negativas y no nulo, cumpliendo que

$$\underline{h}_{\mathcal{Z}}\, \underline{m} = 0,\ \forall \underline{m} \in L_\rho,$$

y es claro que se puede suponer m.c.d.$\{h_i \mid i \in \mathcal{Z}\} = 1$.

Además, como $I(\rho)$ es un ideal propio (en caso contrario $I_+(\rho)$ no sería propio) y el cuerpo k es algebraicamente cerrado, entonces existe $\underline{\lambda}_{\mathcal{Z}} \in \mathcal{V}(I(\rho))$. Por lo tanto,

$$(\underline{\lambda}_{\mathcal{Z}})^{\underline{m}} = \rho(\underline{m}),\ \forall \underline{m} \in L_\rho.$$

Consideremos la curva monomial irreducible C con parametrización monomial dada por $(\mathcal{Z}, \underline{h}_{\mathcal{Z}}, \underline{\lambda}_{\mathcal{Z}})$. Es decir,

$$C \equiv \left\{ \begin{array}{ll} x_i = \lambda_i t^{h_i} & \text{si } i \in \mathcal{Z} \\ x_i = 0 & \text{si } i \notin \mathcal{Z} \end{array} \right. .$$

Puesto que $\mathcal{I}(C)$ es el núcleo del homomorfismo,

$$\begin{array}{rrcll} \Phi: & k[X_1, \ldots, X_n] & \longrightarrow & k[T] & \\ & X_i & \longmapsto & \lambda_i T^{h_i} & \text{si } i \in \mathcal{Z} \\ & X_i & \longmapsto & 0 & \text{si } i \notin \mathcal{Z} \end{array},$$

se tiene $I = I_+(\rho) + M(\mathcal{Z}) \subset \mathcal{I}(C)$, y por ser primos de la misma altura, $I = \mathcal{I}(C)$.

□

Hemos caracterizado, dentro de los ideales primos de altura $n-1$, aquellos asociados a curvas monomiales irreducibles:

Teorema 2.1.18 *Sea I un ideal primo de altura $n-1$ en el anillo de polinomios $k[X]$. Son equivalentes:*

1. *I es binomial y combinatoriamente finito.*

2. *I es el ideal asociado a una curva monomial irreducible.*

Dem. El resultado es consecuencia de las Proposiciones 2.1.5, 2.1.12 y 2.1.17.

$\square$

Debido a su utilización en las siguientes secciones, vamos a destacar otros elementos asociados a una curva monomial irreducible, aparte de los ya considerados.

Notación 2.1.19 Sea C una curva monomial irreducible con célula asociada $\mathcal{Z}$ y Ψ una parametrización monomial de C dada por los vectores $(\underline{h}, \underline{\lambda})$. Se define el conjunto,

$$\widetilde{\mathcal{Z}} := \{i \in \mathcal{Z} \mid h_i = 0\}.$$

El conjunto definido, $\widetilde{\mathcal{Z}}$, no depende de la elección de la parametrización monomial, ya que tanto la célula $\mathcal{Z}$ como el vector $\underline{h}$ están unívocamente determinados por la curva C (Proposición 2.1.6).

Además, como punto destacado de la curva C, se considera $P := \Psi(0)$. Aunque el vector de coeficientes $\underline{\lambda}_{\mathcal{Z}}$ puede variar según la parametrización monomial elegida, sus coordenadas para índices $i \in \widetilde{\mathcal{Z}}$ sí están unívocamente determinadas (consecuencia de la Proposición 2.1.9), luego el punto P también lo está.

Veamos especificados sobre un ejemplo todos los elementos que hemos asociado a una curva monomial irreducible.

Ejemplo 2.1.20 Consideremos la curva C dada por:

$$C \equiv \left\{ \begin{array}{l} x_1 = t \\ x_2 = 0 \\ x_3 = -4 \\ x_4 = 3t^2 \end{array} \right. .$$

La parametrización monomial dada para C queda determinada por los vectores exponente y coeficiente, que en el ejemplo son:

$$\underline{h} = (1, \infty, 0, 2) \quad \text{y} \quad \underline{\lambda} = (1, 0, -4, 3)$$

(recordemos que la coordenada $h_2 = \infty$ quiere decir que $\lambda_2 = 0$ y por tanto el exponente h_2 puede tomar cualquier valor). Ahora bien, otra forma de determinar la parametrización monomial es conocer la célula asociada a C y los vectores reducidos, que en este caso son:

$$\mathcal{Z} = \{1, 3, 4\} \quad \underline{h}_{\mathcal{Z}} = (1, 0, 2) \quad \underline{\lambda}_{\mathcal{Z}} = (1, -4, 3).$$

Para calcular el ideal asociado a C, recuérdese que si $I := \mathcal{I}(C)$ entonces $I = I_+(\rho) + M(\mathcal{Z})$, donde

- $L_\rho = \langle \underline{m}_1 = (-2, 1, 1), \underline{m}_2 = (-2, 0, 1)\rangle$ $(= \underline{h}_{\mathcal{Z}}^{\perp})$.
- $\rho(-2, 1, 1) = -12$ $(= (\underline{\lambda}_{\mathcal{Z}})^{\underline{m}_1})$ y $\rho(-2, 0, 1) = 3$ $(= (\underline{\lambda}_{\mathcal{Z}})^{\underline{m}_2})$.

Por último, los otros elementos que destacamos para esta curva monomial (independientes de la parametrización monomial elegida), son:

$$\widetilde{\mathcal{Z}} = \{3\} \quad \text{y} \quad P = (0, 0, -4, 0).$$

En los desarrollos posteriores necesitaremos dar un tratamiento similar al que hemos visto para curvas monomiales irreducibles, al caso de variedades formadas por un punto. Para ello tenemos que tener en cuenta el siguiente resultado.

Proposición 2.1.21 *Sea $P = (\lambda_1, \ldots, \lambda_n)$ un punto en el espacio $\mathcal{A}^n(k)$. Asociados a P consideramos:*

1. *La célula $\mathcal{Z} = \{i \in \{1, \ldots, n\} \mid \lambda_i \neq 0\}$.*
2. *El retículo $L_\rho = \mathbb{Z}^{|\mathcal{Z}|}$.*
3. *El carácter $\rho : L_\rho \to k^*$ definido $\rho(\underline{m}) = (\underline{\lambda}_{\mathcal{Z}})^{\underline{m}}$ para todo $\underline{m} \in L_\rho$. En particular, si $i \in \mathcal{Z}$, $\rho(\underline{e}_i) = \lambda_i$, siendo $\underline{e}_i \in L_\rho$, el i-ésimo vector de la base canónica de $\mathbb{Z}^{|\mathcal{Z}|}$.*

Entonces, si $I := \mathcal{I}(\{P\})$ se tiene $I = I_+(\rho) + M(\mathcal{Z})$.

Dem. Es claro, puesto que $I = \langle X_1 - \lambda_1, \ldots, X_n - \lambda_n\rangle$ y, por lo dicho en 3, se tiene $X_i - \lambda_i \in I_+(\rho)$ para todo $i \in \mathcal{Z}$.

$\square$

2.2 Curvas monomiales

Si queremos dar una definición de curva monomial (no necesariamente irreducible) coherente con lo que hemos visto para el caso irreducible, podemos o bien extender la definición teniendo en cuenta las ecuaciones implícitas, o bien fijarnos en las paramétricas. Según la segunda opción, una curva sería monomial si y sólo si sus componentes irreducibles son monomiales, pero esta definición es demasiado general, en el sentido que estas curvas pierden muchas de las propiedades de las curvas monomiales irreducibles.

En este trabajo se ha optado por extender la definición teniendo en cuenta las ecuaciones implícitas, y de esta forma conservar la propiedad de binomialidad para los ideales, lo cual nos permite obtener resultados en gran medida combinatorios. El primer problema que nos planteamos es dar una interpretación de dicha definición atendiendo a las parametrizaciones.

Definición 2.2.1 *Dado un ideal I del anillo de polinomios $k[X]$, diremos que I es combinatoriamente finito si sus primos asociados lo son (Definición 2.1.10).*

Definición 2.2.2 *Sea C una curva de $\mathcal{A}^n(k)$ e $I := \mathcal{I}(C)$ su ideal asociado. Diremos que C es monomial si I es binomial y combinatoriamente finito.*

Según esta definición y teniendo en cuenta las propiedades de los ideales binomiales, se deduce que las componentes irreducibles de una curva monomial son monomiales.

Proposición 2.2.3 *Las componentes irreducibles de una curva monomial C son curvas monomiales irreducibles.*

Dem. Las componentes irreducibles de C son las variedades definidas por los primos asociados de I. Pero estos primos son binomiales por serlo I (Proposición 1.3.17), tienen altura $n-1$ y son combinatoriamente finitos. Luego, aplicando el Teorema 2.1.18, son ideales asociados a curvas monomiales irreducibles.

$\square$

Por lo tanto, si partimos de C una curva monomial en $\mathcal{A}^n(k)$, C es unión de curvas monomiales irreducibles. Además, si llamamos I al ideal asociado a C y consideramos su descomposición minimal

$$I = \mathcal{P}_1 \cap \mathcal{P}_2 \cap \ldots \cap \mathcal{P}_d,$$

cada primo $\mathcal{P}_j$ es el ideal de una curva monomial irreducible. Denotando $C_j := \mathcal{V}(\mathcal{P}_j)$ para todo $j \in \{1, \ldots, d\}$, se tiene la descomposición en componentes irreducibles de C,

$$C = C_1 \cup C_2 \cup \ldots \cup C_d.$$

Como acabamos de ver, toda curva monomial es unión de componentes monomiales irreducibles. Sin embargo, el recíproco no es cierto, como se puede ver en el siguiente ejemplo:

Ejemplo 2.2.4 Sea C la unión de las curvas monomiales irreducibles C_1 y C_2, definidas por las parametrizaciones:

$$C_1 \equiv \left\{ \begin{array}{l} x = t^2 \\ y = t^3 \end{array} \right. \qquad C_2 \equiv \left\{ \begin{array}{l} x = t^3 \\ y = t^5 \end{array} \right. .$$

La base de Gröbner reducida para el orden lexicográfico ($Y < X$) del ideal $I := \mathcal{I}(C)$ es $\{(Y^2 - X^3)(Y^3 - X^5)\}$, que no está formada por binomios. Luego el ideal I no es binomial (Proposición 1.2.2) y la curva C no es monomial.

Como dijimos al comienzo de la sección, queremos dar una interpretación de la definición de curva monomial en términos de las ecuaciones paramétricas. Para ello tenemos que:

"Buscar condiciones sobre las parametrizaciones de las componentes monomiales irreducibles de una curva, para que el ideal asociado a su unión sea binomial"

Sin duda la caracterización de las variedades cortadas por binomios (variedades con ideal asociado binomial), dada en el Teorema 1.5.11, es esencial para nuestro objetivo. Recordemos que C es una variedad de $\mathcal{A}^n(k)$ con ideal asociado binomial si y sólo si se cumplen:

C1 Para cada conjunto $\mathcal{Z} \subseteq \{1, \ldots, n\}$, el ideal de $\overline{C \cap (k^*)^{\mathcal{Z}}}$ es binomial.

C2 El conjunto $U = \{\mathcal{Z} \subseteq \{1, \ldots, n\} \mid C \cap (k^*)^{\mathcal{Z}} \neq \emptyset\}$ es cerrado por intersecciones.

C3 Si $\mathcal{Z}$, $\mathcal{Z}' \in U$ y $\mathcal{Z} \subseteq \mathcal{Z}'$ entonces la proyección $(k^*)^{\mathcal{Z}'} \to (k^*)^{\mathcal{Z}}$ lleva puntos de C en puntos de C.

Por lo tanto, nuestro trabajo consistirá en interpretar las condiciones C1, C2 y C3 en términos de las parametrizaciones de las componentes de la curva C.

Sea C una unión de curvas monomiales irreducibles distintas, $C = C_1 \cup \ldots \cup C_d$. Consideremos la descomposición minimal de $I := \mathcal{I}(C)$,

$$I = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_d, \quad \text{donde } \mathcal{P}_j := \mathcal{I}(C_j); \text{ para } j \in \{1, \ldots, d\}.$$

Para cada una de las componentes C_j de la curva C, sea $\mathcal{Z}_j$ su célula asociada y consideremos una parametrización monomial Ψ_j dada por los vectores $(\underline{h}_j, \underline{\lambda}_j)$. Como hicimos en 2.1.19, se consideran el punto $P_j = \Psi_j(0)$ y el subconjunto de la célula $\mathcal{Z}_j$, $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_{ji} = 0\}$, elementos que no dependen de la parametrización elegida Ψ_j. Teniendo en cuenta estas notaciones, es claro que,

Proposición 2.2.5 *Para todo $\mathcal{Z} \subseteq \{1, \ldots, n\}$,*

$$C \cap (k^*)^{\mathcal{Z}} = \left(\bigcup_{\mathcal{Z}_j = \mathcal{Z}} (C_j \backslash \{P_j\}) \right) \cup \left(\bigcup_{\widetilde{\mathcal{Z}}_j = \mathcal{Z}} \{P_j\} \right).$$

Dem. Se deduce sin más que tener en cuenta la forma de las parametrizaciones monomiales de las componentes C_j y las definiciones de $\mathcal{Z}_j$, $\widetilde{\mathcal{Z}}_j$ y P_j.

$\square$

2.2.1 Curvas monomiales por el origen

Antes de buscar condiciones sobre las parametrizaciones en el caso general, trataremos el caso de curvas cuyas componentes pasen por el origen. En este caso la notación resulta mucho más cómoda, lo cual facilita la interpretación de las condiciones C1, C2 y C3.

En lo que sigue, C será una curva cuyas componentes irreducibles $C_1, \ldots,$ C_d, son monomiales. Para $1 \leq j \leq d$, sean $\mathcal{Z}_j$ la célula asociada a C_j, $(\underline{h}_j, \underline{\lambda}_j)$ los vectores de una parametrización monomial de C_j y $\widetilde{\mathcal{Z}}_j = \{i \in \{1, \ldots, n\} \mid h_{ji} = 0\}$.

Definición 2.2.6 *Diremos que C es una curva por el origen si se cumple*

$$\widetilde{\mathcal{Z}}_j = \emptyset \quad \textit{para todo } j \in \{1, \ldots, d\}$$

(o equivalentemente, todas las componentes irreducibles de C pasan por el origen).

Bajo esta hipótesis se tiene,

Proposición 2.2.7 *Si C es una curva por el origen y $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$, entonces se cumple*

$$C \cap (k^*)^{\mathcal{Z}} = \bigcup_{\mathcal{Z}_j = \mathcal{Z}} (C_j \backslash \{\underline{0}\}).$$

Además $C \cap (k^*)^{\mathcal{Z}} \neq \emptyset$ si y sólo si o bien existe $j \in \{1, \dots, d\}$ tal que $\mathcal{Z} = \mathcal{Z}_j$, o bien $\mathcal{Z} = \emptyset$.

Dem. Como C es una curva por el origen, entonces $\widetilde{\mathcal{Z}}_j = \emptyset$ para todo $j \in \{1, \dots, d\}$. Además, como $\underline{0}$ es un punto de C, se tiene $C \cap (k^*)^{\emptyset} \neq \emptyset$, luego el enunciado se deduce de la Proposición 2.2.5.

□

Vamos entonces a analizar las condiciones del Teorema 1.5.11 una por una, dejando para el final la que requiere mayor trabajo, que es la C1.

$\boxed{\textbf{C2}}$ *El conjunto $U = \{\mathcal{Z} \subseteq \{1, \dots, n\} \mid C \cap (k^*)^{\mathcal{Z}} \neq \emptyset\}$ es cerrado por intersecciones.*

Teorema 2.2.8 *La condición C2 es equivalente a la siguiente condición:*

$$\forall j, k \in \{1, \dots, d\}, \quad \mathcal{Z}_j \cap \mathcal{Z}_k = \begin{cases} \mathcal{Z}_l \text{ para algún } l \in \{1, \dots, d\} \\ \text{ó} \\ \emptyset \end{cases}.$$

Dem. Como consecuencia de la proposición anterior, $U = \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\} \cup \{\emptyset\}$.

□

Esta es una condición combinatoria referida a las células de las componentes. Veamos su comprobación sobre un ejemplo:

Ejemplo 2.2.9 Consideremos la curva $C = C_1 \cup C_2$, donde C_1, C_2 son las curvas monomiales irreducibles definidas por:

$$\begin{array}{cc} C_1 \equiv \left\{ \begin{array}{c} x = 0 \\ y = t^2 \\ z = t^3 \end{array} \right. & C_2 \equiv \left\{ \begin{array}{c} x = t^2 \\ y = 0 \\ z = t^5 \end{array} \right. \\ \downarrow & \downarrow \\ \mathcal{Z}_1 = \{2, 3\} & \mathcal{Z}_2 = \{1, 3\} \end{array}.$$

Como C es una curva por el origen, el conjunto U resulta $\{\mathcal{Z}_1, \mathcal{Z}_2, \emptyset\}$ que claramente no es cerrado para intersecciones. Por lo tanto C no es monomial. En efecto, sean $\mathcal{P}_1 = \mathcal{I}(C_1)$ y $\mathcal{P}_2 = \mathcal{I}(C_2)$. La base de Gröbner reducida de $\mathcal{P}_1 \cap \mathcal{P}_2$, con respecto al orden lexicográfico ($Z < Y < X$) es $\{Y^4 - YZ^2, XY, X^5 + Y^3 - Z^2\}$, con lo cual el ideal asociado a C no es binomial. Pero si añadimos a C la componente,

$$C_3 \equiv \left\{ \begin{array}{c} x = 0 \\ y = 0 \\ z = t \end{array} \right. ,$$

con célula $\mathcal{Z}_3 = \{3\}$, la base de Gröbner reducida para el ideal asociado a $\widetilde{C} = C \cup C_3$ es $\{Y^4 - YZ^2, XY, X^6 - XZ^2\}$, luego $\widetilde{C}$ es monomial, aunque esto no se debe sólo a que se cumpla la condición C2.

$\boxed{\textbf{C3}}$ *Si $\mathcal{Z}$, $\mathcal{Z}' \in U$ y $\mathcal{Z} \subset \mathcal{Z}'$, entonces la proyección $(k^*)^{\mathcal{Z}'} \to (k^*)^{\mathcal{Z}}$ debe llevar puntos de C en puntos de C.*

Proposición 2.2.10 *La condición C3 es equivalente a que para cualesquiera $j, k \in \{1, \ldots, d\}$ tales que $\mathcal{Z}_j \subseteq \mathcal{Z}_k$, exista $l \in \{1, \ldots, d\}$ con $\mathcal{Z}_l = \mathcal{Z}_j$ y tal que $\pi(C_k) = C_l$, siendo π la proyección $\pi : (k^*)^{\mathcal{Z}_k} \to (k^*)^{\mathcal{Z}_j}$.*

Dem. Como C es una curva por el origen, entonces $U = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\} \cup \{\emptyset\}$. Es evidente que la proyección $(k^*)^{\mathcal{Z}} \to (k^*)^{\emptyset} = \{\underline{0}\}$ cumple la condición. Consideremos, por tanto, dos células $\mathcal{Z}_j$, $\mathcal{Z}_k$ con $\mathcal{Z}_j \subseteq \mathcal{Z}_k$ y sea π la proyección $\pi : (k^*)^{\mathcal{Z}_k} \to (k^*)^{\mathcal{Z}_j}$. Se tiene

$$C \cap (k^*)^{\mathcal{Z}_k} = \bigcup_{\mathcal{Z}_i = \mathcal{Z}_k} (C_i \backslash \{\underline{0}\})$$

(Proposición 2.2.7), con lo cual $\pi(C \cap (k^*)^{\mathcal{Z}_k}) \subseteq C$ si y sólo si para cualquier componente C_i tal que $\mathcal{Z}_i = \mathcal{Z}_k$, su imagen mediante π está contenida en la curva C. Veamos, por tanto, qué significa que $\pi(C_k) \subseteq C$. Considerando una parametrización monomial de C_k y teniendo en cuenta que $\widetilde{\mathcal{Z}}_k = \emptyset$ y $\emptyset \neq \mathcal{Z}_j \subseteq \mathcal{Z}_k$, es claro que $\pi(C_k)$ es a su vez una curva monomial irreducible, con célula asociada $\mathcal{Z}_j$. Luego $\pi(C_k) \subseteq C$ si y sólo si $\pi(C_k)$ es una de las componentes de C con célula asociada $\mathcal{Z}_j$.

$\square$

Teorema 2.2.11 *La condición C3 es equivalente a la siguiente condición:*

Para cualesquiera $j, k \in \{1, \ldots, d\}$ con $\mathcal{Z}_j \subseteq \mathcal{Z}_k$, existe $l \in \{1, \ldots, d\}$ tal que $\mathcal{Z}_l = \mathcal{Z}_j$ y cumpliendo:

1. *Existe* $a \in \mathbb{Z}^*$ *tal que* $ah_{li} = h_{ki}$ *para todo* $i \in \mathcal{Z}_j$.
2. $((\underline{\lambda}_l)_{\mathcal{Z}_j})^{\underline{m}} = ((\underline{\lambda}_k)_{\mathcal{Z}_j})^{\underline{m}}$ *para todo* $\underline{m} \in L_l = \langle (\underline{h}_l)_{\mathcal{Z}_l} \rangle^{\perp} \subset \mathbb{Z}^{\mathcal{Z}_l}$.

Dem. Después de lo dicho en la proposición anterior sólo queda interpretar la condición $\pi(C_k) = C_l$.

Si denotamos por $\widetilde{\underline{h}}_k$ el vector obtenido al dividir $(\underline{h}_k)_{\mathcal{Z}_j}$ (Nota 2.1.2) por el máximo común divisor de sus coordenadas y denotamos $\widetilde{\underline{\lambda}}_k = (\underline{\lambda}_k)_{\mathcal{Z}_j}$, entonces $\pi(C_k)$ es la curva monomial irreducible asociada a la terna $(\mathcal{Z}_j, \widetilde{\underline{h}}_k, \widetilde{\underline{\lambda}}_k)$. Además C_l es una componente asociada a $(\mathcal{Z}_j, (\underline{h}_l)_{\mathcal{Z}_j}, (\underline{\lambda}_l)_{\mathcal{Z}_j})$. Entonces, aplicando la Proposición 2.1.6, se tiene que $\pi(C_k) = C_l$ equivale a que $\widetilde{\underline{h}}_k = (\underline{h}_l)_{\mathcal{Z}_j}$ y $(\widetilde{\underline{\lambda}}_k)^{\underline{m}} = ((\underline{\lambda}_l)_{\mathcal{Z}_j})^{\underline{m}}$ para todo $\underline{m} \in L_l$, de donde se deduce el enunciado.

$\square$

Ejemplo 2.2.12 Busquemos una curva unión de componentes monomiales irreducibles que no cumple esta doble condición. Sea $C = C_1 \cup C_2$ donde

$$\begin{array}{ccc} C_1 \equiv \left\{ \begin{array}{c} x = t \\ y = t^2 \\ z = t^3 \end{array} \right. & \qquad & C_2 \equiv \left\{ \begin{array}{c} x = 0 \\ y = t^2 \\ z = t^5 \end{array} \right. . \\ \downarrow & & \downarrow \\ \mathcal{Z}_1 = \{1,2,3\} & & \mathcal{Z}_2 = \{2,3\} \end{array}$$

Se cumple que $\mathcal{Z}_2 \subseteq \mathcal{Z}_1$ y por tanto la condición C2, pero si hacemos la proyección de C_1 en la célula coordenada correspondiente a los índices 2 y 3, la curva resultante no es C_2 ya que los vectores $(2,3)$ y $(2,5)$ no son proporcionales (Proposición 2.1.6). Por lo tanto la condición C3 no se cumple y C no es monomial. En efecto, si calculamos la base de Gröbner reducida para el orden lexicográfico con $Z < Y < X$ del ideal $I := \mathcal{I}(C)$, resulta $\{-X^4 + XZ, -X^3 + XY, -X^6 + X^{10} - Y^5 + Z^2\}$, que no es binomial (Proposición 1.2.2). Sin embargo, si ahora consideramos la componente,

$$C_3 \equiv \left\{ \begin{array}{c} x = 0 \\ y = t^2 \\ z = t^3 \end{array} \right.$$

y la curva $\widetilde{C} = C_1 \cup C_3$, entonces se cumple C3, y además $\widetilde{C}$ es monomial ya que la base de Gröbner reducida para su ideal asociado es $\{-X^4 + XZ, -X^3 + XY, Y^3 - Z^2\}$ (aunque, de nuevo, la razón de que sea monomial no es sólo que se cumplan C2 y C3).

Una vez analizadas las condiciones C2 y C3, empecemos ya el estudio de C1:

$\boxed{\textbf{C1}}$ *Para cada conjunto $\mathcal{Z} \subseteq \{1, \ldots, n\}$, el ideal $I_{\mathcal{Z}} = \mathcal{I}(\overline{C \cap (k^*)^{\mathcal{Z}}})$ es binomial.*

Para analizar este enunciado en términos combinatorios, hay que establecer quién es $\overline{C \cap (k^*)^{\mathcal{Z}}}$; es decir, el mínimo cerrado para la topología de Zariski en $\mathcal{A}^n(k)$ que contiene a $C \cap (k^*)^{\mathcal{Z}}$. Pero como vimos en la Proposición 2.2.7, $C \cap (k^*)^{\mathcal{Z}} \neq \emptyset$ si y sólo si $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\} \cup \{\emptyset\}$. Para el caso $\mathcal{Z} = \emptyset$ resulta $\overline{C \cap (k^*)^{\emptyset}} = \{\underline{0}\}$, luego $I_{\mathcal{Z}} = \langle X_1, \ldots, X_n \rangle$, que es un ideal binomial. Veamos qué ocurre cuando $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$.

Proposición 2.2.13 *Sea $\mathcal{P}_j = \mathcal{I}(C_j)$, para cada $j \in \{1, \ldots, d\}$. Si C es una curva por el origen y $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$, se tiene*

$$I_{\mathcal{Z}} = \bigcap_{\mathcal{Z}_j = \mathcal{Z}} \mathcal{P}_j,$$

y esta es la descomposición primaria minimal de $I_{\mathcal{Z}}$.

Dem. La demostración es inmediata teniendo en cuenta la Proposición 2.2.7.

□

Denotemos como en la sección anterior, $M(\mathcal{Z}) := \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle$.

Proposición 2.2.14 *Dado $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$, se definen $J_{\mathcal{Z}} = I_{\mathcal{Z}} \cap k[\mathcal{Z}]$ y, para cada j tal que $\mathcal{Z}_j = \mathcal{Z}$, $\widetilde{\mathcal{P}}_j = \mathcal{P}_j \cap k[\mathcal{Z}]$. Entonces se tiene:*

1. *$J_{\mathcal{Z}} = \cap_{\mathcal{Z}_j = \mathcal{Z}} \widetilde{\mathcal{P}}_j$, descomposición primaria minimal de $J_{\mathcal{Z}}$.*
2. *$I_{\mathcal{Z}} = J_{\mathcal{Z}} + M(\mathcal{Z})$ (suma en $k[X]$).*
3. *$\mathcal{P}_j = \widetilde{\mathcal{P}}_j + M(\mathcal{Z})$ (suma en $k[X]$).*
4. *$\widetilde{\mathcal{P}}_j$ es primo de altura $|\mathcal{Z}| - 1$.*
5. *$J_{\mathcal{Z}} = (J_{\mathcal{Z}} : (\prod_{i \in \mathcal{Z}} X_i)^{\infty})$.*

Dem. Puesto que $I_{\mathcal{Z}} = \bigcap_{\mathcal{Z}_j = \mathcal{Z}} \mathcal{P}_j$, 1 es evidente.

Si $\mathcal{Z} = \mathcal{Z}_j = \{i \mid X_i \notin \mathcal{P}_j\}$, entonces $M(\mathcal{Z}) \subseteq \mathcal{P}_j$, luego $M(\mathcal{Z}) \subseteq I_{\mathcal{Z}}$. Teniendo en cuenta que todo polinomio $f \in k[X]$ se escribe de forma única como $f = f_1 + f_2$ con $f_1 \in k[\mathcal{Z}]$ y $f_2 \in M(\mathcal{Z}) \subseteq I_{\mathcal{Z}}$, entonces es claro que $I_{\mathcal{Z}} = J_{\mathcal{Z}} + M(\mathcal{Z})$. De forma análoga se tiene que si $\mathcal{Z}_j = \mathcal{Z}$ entonces $\mathcal{P}_j = M(\mathcal{Z}) + \widetilde{\mathcal{P}}_j$. Además $\widetilde{\mathcal{P}}_j$ es la imagen de $\mathcal{P}_j/M(\mathcal{Z})$ vía el isomorfismo $k[X]/M(\mathcal{Z}) \cong k[\mathcal{Z}]$, y como $\mathrm{ht}(\mathcal{P}_j) = n-1$ entonces la altura de $\widetilde{\mathcal{P}}_j$ es $|\mathcal{Z}| - 1$.

Finalmente, consideremos un polinomio $h \in (J_{\mathcal{Z}} : (\prod_{i\in\mathcal{Z}} X_i)^\infty) \subset k[\mathcal{Z}]$. Entonces existe un monomio $X^{\underline{m}} \in k[\mathcal{Z}]$ tal que $hX^{\underline{m}} \in J_{\mathcal{Z}}$. Si suponemos que $h \notin J_{\mathcal{Z}}$ existirá $j \in \{1, \dots, d\}$ tal que $h \notin \widetilde{\mathcal{P}}_j$, luego $X^{\underline{m}} \in \widetilde{\mathcal{P}}_j$, en contra de que $\widetilde{\mathcal{P}}_j$ no contiene indeterminadas. Luego $J_{\mathcal{Z}} = (J_{\mathcal{Z}} : (\prod_{i\in\mathcal{Z}} X_i)^\infty)$.

□

Nota 2.2.15 El ideal $\widetilde{\mathcal{P}}_j$ es el ideal asociado a la curva $C_{j,\mathcal{Z}_j} = \mathrm{pr}_{\mathcal{Z}_j}(C_j) \subset (k)^{\mathcal{Z}_j}$, que se definió en 2.1.3. Luego $J_{\mathcal{Z}}$ es el ideal asociado a una unión de curvas monomiales irreducibles todas ellas con célula asociada $\mathcal{Z}$.

Proposición 2.2.16 *La condición C1 se cumple si y sólo si*

$$J_{\mathcal{Z}} \textit{ es binomial para todo } \mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\} \qquad (*)$$

Dem. La condición C1 exige que los ideales $I_{\mathcal{Z}}$ sean binomiales para todo $\mathcal{Z}$, lo que, como acabamos de ver, equivale a que $I_{\mathcal{Z}}$ sea binomial cuando $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$. La proposición se deduce de que $I_{\mathcal{Z}} = J_{\mathcal{Z}} + M(\mathcal{Z})$, $J_{\mathcal{Z}} = I_{\mathcal{Z}} \cap k[\mathcal{Z}]$ (Proposición 2.2.14) y $M(\mathcal{Z}) = \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle$.

□

Por lo tanto, el problema consiste en establecer, en términos de las parametrizaciones de la componentes, las condiciones necesarias y suficientes para que se cumpla $(*)$. Es decir, hemos reducido el problema a considerar una curva C cuyas componentes irreducibles son monomiales, todas con la misma célula asociada, y caracterizar, en términos de las parametrizaciones, cuándo $\mathcal{I}(C)$ es binomial.

2.2.2 Curvas monomiales en una célula

Veamos qué condiciones caracterizan cuándo una unión de curvas monomiales irreducibles, todas con célula asociada la total, es una curva monomial. Aunque estábamos viendo qué pasaba en el caso de que la curva pasa por el origen, los resultados de esta subsección son independientes de este hecho, y válidos con la única condición de que la célula asociada a todas las componentes sea $\{1, \dots, n\}$.

Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de curvas monomiales irreducibles distintas tales que la célula asociada a C_j es $\mathcal{Z} = \{1, \ldots, n\}$ para todo $j \in \{1, \ldots, d\}$. Sean $I = \mathcal{I}(C)$ y $\mathcal{P}_j = \mathcal{I}(C_j)$ para todo j. Entonces, de la Proposición 2.2.7 se deduce que $I = I_{\mathcal{Z}}$, y de la Proposición 2.2.14, que $I = (I : (\prod_{i=1}^n X_i)^\infty)$.

Denotemos por $(\underline{h}_j, \underline{\lambda}_j)$ a los vectores de una parametrización monomial de C_j y por (L_j, ρ_j) el retículo saturado de rango $n-1$ y el carácter parcial $\rho_j : L_j \to k^*$ tales que $\mathcal{P}_j = I_+(\rho_j)$ (Proposición 2.1.6). Se tiene $L_j = \langle \underline{h}_j \rangle^\perp$ y $\rho_j(\underline{m}) = \underline{\lambda}_j^{\underline{m}}$ para todo $\underline{m} \in L_j$.

Con estas notaciones, veamos condiciones necesarias y suficientes para que la curva C sea monomial.

Proposición 2.2.17 *Si I es binomial entonces existe un carácter parcial $\rho : L_\rho \to k^*$ tal que $I = I_+(\rho)$. Además:*

1. $\operatorname{Sat} L_\rho = L_j$ *para todo* $j \in \{1, \ldots, d\}$ *y por tanto* $\underline{h}_j = \underline{h}_1$ *para todo* $j \in \{2, \ldots, d\}$.
2. $\rho_1, \ldots, \rho_d$ *son las extensiones de* ρ *a* $\operatorname{Sat} L_\rho$. *En particular,* $|\operatorname{Sat} L_\rho / L_\rho| = d$.
3. $L_\rho = \{\underline{m} \in \operatorname{Sat} L_\rho \mid \underline{\lambda}_j^{\underline{m}} = \underline{\lambda}_1^{\underline{m}}, \forall j \in \{2, \ldots, d\}\}$ *y* $\rho(\underline{m}) = \underline{\lambda}_1^{\underline{m}}$ *para todo* $\underline{m} \in L_\rho$.

Dem. La existencia de ρ está garantizada por el Corolario 1.3.11. Por los resultados 1.3.12 y 1.3.8, conocemos la descomposición primaria minimal del ideal $I_+(\rho)$ que, por tratarse de un ideal radical, es la intersección de los ideales primos $I_+(\widetilde{\rho}_j)$, donde $\widetilde{\rho}_j$ son las extensiones de ρ a $\operatorname{Sat} L_\rho$ (de las cuales hay $|\operatorname{Sat} L_\rho / L_\rho|$). Puesto que $I = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_d$ es la descomposición primaria minimal de I, se tiene $d = |\operatorname{Sat} L_\rho / L_\rho|$ y, salvo reordenación, $\mathcal{P}_j = I_+(\widetilde{\rho}_j)$. Puesto que $\mathcal{P}_j = I_+(\rho_j)$, se tendrá $\rho_j = \widetilde{\rho}_j$ y $L_j = \operatorname{Sat} L_\rho$ para todo j. Por tanto $\rho_1, \ldots, \rho_d$ son las extensiones de ρ a $\operatorname{Sat} L_\rho$ y $\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$. Además, si $L = \{\underline{m} \in \operatorname{Sat} L_\rho \mid \rho_j(\underline{m}) = \rho_1(\underline{m}), \forall j \in \{2, \ldots, d\}\}$ entonces $\rho_1, \ldots, \rho_d$ son extensiones distintas del carácter $\rho_1|_L$ al retículo $\operatorname{Sat} L_\rho$, luego $|\operatorname{Sat} L_\rho / L| \geq d$ y puesto que $L_\rho \subseteq L$ y $|\operatorname{Sat} L_\rho / L_\rho| = d$, se tiene $L = L_\rho$ (recuérdese que $\rho_j(\underline{m}) = \underline{\lambda}_j^{\underline{m}}$).

□

Definición 2.2.18 *En estas condiciones diremos que L_ρ es el retículo asociado a la curva C.*

Nota 2.2.19 El carácter ρ que aparece en la proposición anterior puede definirse a través de cualquiera de los vectores coeficientes $\underline{\lambda}_1, \ldots, \underline{\lambda}_d$ ya que para todo $\underline{m} \in L_\rho$ se tiene $\underline{\lambda}_j^{\underline{m}} = \underline{\lambda}_1^{\underline{m}}$ para todo $j \in \{2, \ldots, d\}$.

Teorema 2.2.20 *En las condiciones anteriores, se consideran los subretículos $\widetilde{L} = \langle \underline{h}_1 \rangle^\perp$ y $L = \{\underline{m} \in \widetilde{L} \mid (\underline{\lambda}_j)^{\underline{m}} = (\underline{\lambda}_1)^{\underline{m}}, \forall j \in \{2, \ldots, d\}\}$. Entonces I es binomial si y sólo si se cumplen las dos condiciones siguientes:*

1. *$\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$.*

2. *$|\widetilde{L}/L| = d$.*

Dem. Si I es binomial, por la proposición anterior, $\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$. Además existe un carácter parcial $\rho : L_\rho \to k^*$ tal que $I = I_+(\rho)$ donde $L_\rho = L$, Sat $L_\rho = \widetilde{L}$ y $|\text{Sat } L_\rho / L_\rho| = d$.

Recíprocamente, supongamos que se cumplen 1 y 2. Consideremos el carácter $\rho : L \to k^*$ dado por $\rho(\underline{m}) = \underline{\lambda}_1^{\underline{m}}$ para todo $\underline{m} \in L$. Debido a la condición 1, para todo $j \in \{1, \ldots, d\}$, $L_j = \widetilde{L}$, luego ρ_j es una extensión de ρ a $\widetilde{L}$, y como $|\widetilde{L}/L| = d$ se tiene que $\rho_1, \ldots, \rho_d$ son todas las extensiones de ρ a $\widetilde{L}$. Además, la condición $|\widetilde{L}/L| = d$ implica que $\widetilde{L} \subseteq$ Sat L, luego $\widetilde{L} =$ Sat L ya que $\widetilde{L}$ es saturado. Por lo tanto $I_+(\rho) = \cap_{j=1}^d I_+(\rho_j)$ (Corolarios 1.3.12 y 1.3.8), luego $I = I_+(\rho)$ y el ideal I es binomial.

$\square$

El teorema que acabamos de ver caracteriza, en el caso de única célula, qué uniones de curvas monomiales irreducibles son monomiales. El siguiente resultado nos proporciona otra caracterización, más complicada pero con más información con vistas a la construcción de curvas monomiales, pues de hecho lo que hace es detallar un procedimiento de cálculo de L, así como encontrar relaciones entre las distintas componentes de C.

Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles, cuyas componentes tienen asociada la célula $\{1, \ldots, n\}$ y sea $I := \mathcal{I}(C)$. Consideremos, para cada $j \in \{1, \ldots, d\}$, los vectores $(\underline{h}_j, \underline{\lambda}_j)$ que definen una parametrización monomial de C_j y su retículo asociado, L_j.

Teorema 2.2.21 *Se consideran los subretículos $\widetilde{L} = \langle \underline{h}_1 \rangle^\perp$ y $L = \{\underline{m} \in \widetilde{L} \mid (\underline{\lambda}_j)^{\underline{m}} = (\underline{\lambda}_1)^{\underline{m}}, \forall j \in \{2, \ldots, d\}\}$. Entonces I es binomial si y sólo si se cumplen las dos condiciones siguientes:*

1. *$\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$.*

2. *Existen:*

   (a) *Una factorización* $d = d_1 \cdots d_{n-1}$*, tal que* $d_1 / \dots / d_{n-1}$*.*

   (b) *Una base de* $\widetilde{L}$*,* $\mathcal{B} = \{\underline{m}_1, \dots, \underline{m}_{n-1}\}$*, tal que para todo* $i \in \{1, \dots, n-1\}$ *se tiene*

$$(\underline{\lambda}_j)^{d_i \underline{m}_i} = (\underline{\lambda}_1)^{d_i \underline{m}_i} \quad , \forall j \in \{2, \dots, d\}$$

   (es decir, $d_i \underline{m}_i \in L$*, para todo* i*).*

Además, si se cumplen 1 *y* 2*,* $\{d_1 \underline{m}_1, \dots, d_{n-1}\underline{m}_{n-1}\}$ *es base de* L *y fijada, para cada* $i \in \{1, \dots, n-1\}$*, una raíz primitiva* d_i*-ésima de la unidad,* ξ_i*, la aplicación*

$$\beta : \{1, \dots, d\} \to \mathbb{Z}/(d_1) \times \dots \times \mathbb{Z}/(d_{n-1})$$

dada por $\beta(j) = (j_1, \dots, j_{n-1})$ *donde* $\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = \xi_i^{j_i}$ *para cada* $i \in \{1, \dots, n-1\}$ *y para cada* $j \in \{1, \dots, d\}$*, es biyección.*

Dem. Si I es binomial, por el Teorema 2.2.20 se cumple 1 y se tiene $I = I_+(\rho)$, donde $L_\rho = L$, Sat $L_\rho = \widetilde{L}$ y $\rho(\underline{m}) = (\underline{\lambda}_1)^{\underline{m}}$ para todo $\underline{m} \in L_\rho$. Además, $|\text{Sat } L_\rho / L_\rho| = d$, luego aplicando el teorema de estructura de grupos abelianos existen una base de Sat L_ρ, $\{\underline{m}_1, \dots, \underline{m}_{n-1}\}$, y enteros positivos, $\{d_1, \dots, d_{n-1}\}$, de forma que $d = d_1 \dots d_{n-1}$, $d_1 / \dots / d_{n-1}$ y el conjunto $\{d_1 \underline{m}_1, \dots, d_{n-1}\underline{m}_{n-1}\}$ es una base de L_ρ. Pero para todo $j \in \{1, \dots, d\}$, ρ_j es una extensión de ρ al retículo Sat L_ρ, y para cada $i \in \{1, \dots, n-1\}$ $d_i \underline{m}_i \in L_\rho$, luego $(\underline{\lambda}_j)^{d_i \underline{m}_i} = \rho_j(d_i \underline{m}_i) = \rho_1(d_i \underline{m}_i) = (\underline{\lambda}_1)^{d_i \underline{m}_i}$, y se cumple 2.

Recíprocamente, la condición 2 implica que para todo $i \in \{1, \dots, n-1\}$, $d_i \underline{m}_i \in L$, y por tanto, para todo $j \in \{1, \dots, d\}$, $\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i}$ es una raíz d_i-ésima de la unidad. Luego existe j_i, $0 \leq j_i < d_i$ tal que

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = \xi_i^{j_i} \quad \begin{array}{l} , \forall i \in \{1, \dots, n-1\} \\ , \forall j \in \{1, \dots, d\} \ . \end{array}$$

La aplicación $\beta : \{1, \dots, d\} \to \mathbb{Z}/(d_1) \times \dots \times \mathbb{Z}/(d_{n-1})$ dada por $\beta(j) = (j_1, \dots, j_{n-1})$ es inyectiva ya que si $\beta(j) = \beta(k)$ entonces $(\underline{\lambda}_j)^{\underline{m}} = (\underline{\lambda}_k)^{\underline{m}}$ para todo $\underline{m} \in \widetilde{L}$. Pero por la condición 1, $\widetilde{L} = L_j$ para todo $j \in \{1, \dots, d\}$, luego $\rho_j = \rho_k$ y $j = k$. Por tanto, puesto que $d_1 \cdots d_{n-1} = d$, β es biyección.

Para ver que $\{d_1 \underline{m}_1, \dots, d_{n-1}\underline{m}_{n-1}\}$ es sistema de generadores de L, tomemos un vector $\underline{m} \in L$. Como $\underline{m} \in \widetilde{L}$, entonces existen enteros $a_1, \dots,$

a_{n-1} tales que $\underline{m} = \sum_{i=1}^{n-1} a_i \underline{m}_i$. Si para todo $i \in \{1, \ldots, n-1\}$ denotamos por r_i al resto de la división euclídea de a_i por d_i $(0 \leq r_i < d_i)$, se tiene:

$$1 = \left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}} = \left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\sum\limits_{i=1}^{n-1} a_i \underline{m}_i} = \prod_{i=1}^{n-1} (\xi_i^{j_i})^{a_i} = \prod_{i=1}^{n-1} (\xi_i^{j_i})^{r_i} = \left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\sum\limits_{i=1}^{n-1} r_i \underline{m}_i},$$

y por tanto $\sum_i r_i \underline{m}_i \in L$ y L está generado por

$$\{d_i \underline{m}_i,\ 1 \leq i \leq n-1\} \cup \left(\left\{\sum_{i=1}^{n-1} r_i \underline{m}_i \mid 0 \leq r_i < d_i\right\} \cap L\right).$$

Si vemos que la segunda parte de esta unión es el conjunto formado por el vector nulo, hemos terminado. Supongamos que tenemos un vector en L de la forma $\sum_i r_i \underline{m}_i$ donde $0 \leq r_i < d_i$ para todo $i \in \{1, \ldots, n-1\}$. Entonces se cumple que para todo $j \in \{1, \ldots, d\}$,

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\sum\limits_{i=1}^{n-1} r_i \underline{m}_i} = \prod_{i=1}^{n-1} (\xi_i^{j_i})^{r_i} = 1.$$

Fijemos un índice $s \in \{1, \ldots, n-1\}$. Puesto que β es sobre, la igualdad anterior se cumplirá, en particular, siendo $j_i = 0$ para todo $i \neq s$ y $j_s = 1$. Con lo cual $\xi_s^{r_s} = 1$, donde ξ_s es una raíz d_s-ésima primitiva de la unidad y $r_s < d_s$. Luego $r_s = 0$ para cualquier $s \in \{1, \ldots, n-1\}$ y deducimos que el conjunto $\{d_1 \underline{m}_1, \ldots, d_{n-1} \underline{m}_{n-1}\}$ es un sistema de generadores de L. Además es libre ya que $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ es base de $\widetilde{L}$.

Como $\{d_1 \underline{m}_1, \ldots, d_{n-1} \underline{m}_{n-1}\}$ es base de L se tiene $\widetilde{L}/L \cong \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$, luego $|\widetilde{L}/L| = d$ y, aplicando el Teorema 2.2.20, I es binomial.

□

Veamos a continuacion cómo se puede utilizar este teorema para construir unos ejemplos de curvas monomiales en una célula.

Ejemplo 2.2.22 Pretendemos construir una curva monomial en $\mathcal{A}^2(\mathbb{C})$, con dos componentes, y tal que su ideal asociado sea un ideal de carácter parcial, $I_+(\rho)$; es decir, las dos componentes deben tener por célula asociada la total (no hay ceros en las parametrizaciones monomiales). Fijamos los exponentes de las parametrizaciones, que por la condición 1 del Teorema 2.2.21 tienen que ser vectores iguales. Por ejemplo:

$$\begin{array}{ccc} C_1 \equiv \left\{ \begin{array}{l} x = \alpha_1 t \\ y = \beta_1 t^2 \end{array} \right. & & C_2 \equiv \left\{ \begin{array}{l} x = \alpha_2 t \\ y = \beta_2 t^2 \end{array} \right. \\ \downarrow & & \downarrow \\ \mathcal{Z}_1 = \{1,2\} & & \mathcal{Z}_2 = \{1,2\} \end{array}.$$

En este caso sólo aparece una célula coordenada $\mathcal{Z} = \{1,2\}$. Consideremos

1. $d = 2 = d_1$ (la única factorización de d en $n-1$ factores).

2. Una base de $\widetilde{L} = \langle \underline{h}_1 \rangle^{\perp}$, $\underline{m}_1 = (-2,1)$ (única posible salvo el signo).

Si denotamos $\underline{\lambda}_1 = (\alpha_1, \beta_1)$ y $\underline{\lambda}_2 = (\alpha_2, \beta_2)$, para que tengamos la condición 2 del Teorema 2.2.21, se debe cumplir

$$(\underline{\lambda}_2)^{2\underline{m}_1} = (\underline{\lambda}_1)^{2\underline{m}_1}.$$

Para ello, si ξ_1 es una raíz cuadrada primitiva de la unidad ($\xi_1 = -1$), entonces se debe cumplir que:

$$\frac{\alpha_2^{-2}\beta_2}{\alpha_1^{-2}\beta_1} = (\xi_1)^1 = -1.$$

Teniendo en cuenta esta relación, obtenemos distintos valores para los coeficientes que hacen que la curva C sea monomial. Por ejemplo:

1. Si $\alpha_1 = 1$, $\alpha_2 = 1$ y $\beta_1 = 2$, entonces β_2 debe ser -2. Según estos valores construimos la curva plana compleja monomial $C = C_1 \cup C_2$ con componentes

$$C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = 2t^2 \end{array} \right. \quad \text{y} \quad C_2 \equiv \left\{ \begin{array}{l} x = t \\ y = -2t^2 \end{array} \right. ,$$

que resulta monomial.

2. Si $\alpha_1 = 2$, $\alpha_2 = 3$ y $\beta_1 = 5$, entonces β_2 tiene que ser $\frac{-45}{4}$. Por lo tanto si consideramos la curva plana compleja $C = C_1 \cup C_2$, donde

$$C_1 \equiv \left\{ \begin{array}{l} x = 2t \\ y = 5t^2 \end{array} \right. \quad \text{y} \quad C_2 \equiv \left\{ \begin{array}{l} x = 3t \\ y = \frac{-45}{4} t^2 \end{array} \right. ,$$

entonces C es monomial.

Veamos cuáles son los ideales de las curvas en estos dos casos. Denotemos por L_ρ y ρ el retículo y el carácter asociados a la curva C. Entonces $L_\rho = \langle(-4,2)\rangle$, ya que es el único subretículo contenido en $\widetilde{L}$, cumpliendo que Sat $L_\rho = \widetilde{L}$ y $|\widetilde{L}/L_\rho| = 2$. Además, usando la Proposición 2.2.17 se tiene que $\rho(\underline{m}) = \underline{\lambda}_1^{\underline{m}}$, para todo $\underline{m} \in L_\rho$. Por lo tanto, los ideales de las curvas en los dos ejemplos considerados son:

1. $\mathcal{I}(C) = I_+(\rho)$, donde

$$\begin{array}{rcl} \rho : L_\rho & \longrightarrow & k^* \\ (-4,2) & \longmapsto & 4 = \alpha_1^{-4}\beta_1^2 = \alpha_2^{-4}\beta_2^2 \end{array}.$$

2. $\mathcal{I}(C) = I_+(\rho)$, donde

$$\begin{array}{rcl} \rho : L_\rho & \longrightarrow & k^* \\ (-4,2) & \longmapsto & \frac{25}{16} = \alpha_1^{-4}\beta_1^2 = \alpha_2^{-4}\beta_2^2 \end{array}.$$

De este hecho se puede deducir fácilmente que en estos casos (consecuencia de 1.1),

1. $\mathcal{I}(C) = \langle Y^2 - 4X^4\rangle$.
2. $\mathcal{I}(C) = \langle Y^2 - \frac{25}{16}X^4\rangle$.

En el apéndice 1 de este capítulo, volveremos sobre el problema de construir curvas mononmiales asociadas a una única célula.

2.2.3 Caracterización de las curvas monomiales por el origen

Teniendo en cuenta las interpretaciones que hemos hecho de las condiciones C1, C2 y C3, en términos de los vectores de las parametrizaciones, estamos en condiciones de enunciar el siguiente teorema:

Teorema 2.2.23 *Sea C una curva cuyas componentes irreducibles, $C_1, \ldots,$ C_d, son monomiales y pasan por el origen y sea $I := \mathcal{I}(C)$. Consideremos, para cada componente monomial irreducible C_j, una parametrización monomial dada por los vectores $(\underline{h}_j, \underline{\lambda}_j)$, su célula asociada $\mathcal{Z}_j$ y su retículo asociado $L_j = \langle(\underline{h}_j)_{\mathcal{Z}_j}\rangle^\perp$. Se definen, para cada $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$, $A_\mathcal{Z} = \{j \in \{1, \ldots, d\} \mid \mathcal{Z}_j = \mathcal{Z}\}$ y $d_\mathcal{Z} = |A_\mathcal{Z}|$. Entonces, son equivalentes:*

(1) *I es binomial.*

(2) *Se cumplen las condiciones D1, D2 y D3 siguientes:*

D1 *Para todo $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$ se cumplen:*

- *Existe $\underline{h}_{\mathcal{Z}} \in (\mathbb{Z}_{\geq 0})^{\mathcal{Z}}$ tal que $(\underline{h}_j)_{\mathcal{Z}} = \underline{h}_{\mathcal{Z}}$ para todo $j \in A_{\mathcal{Z}}$.*
- *Si consideramos los subretículos de $\mathbb{Z}^{\mathcal{Z}}$, $\widetilde{L}_{\mathcal{Z}} = \langle \underline{h}_{\mathcal{Z}} \rangle^{\perp}$ y $L_{\mathcal{Z}} = \{\underline{m} \in \widetilde{L}_{\mathcal{Z}} \mid (\underline{\lambda}_j)_{\mathcal{Z}}^{\underline{m}} = (\underline{\lambda}_k)_{\mathcal{Z}}^{\underline{m}}, \forall j, k \in A_{\mathcal{Z}}\}$ entonces $|\widetilde{L}_{\mathcal{Z}}/L_{\mathcal{Z}}| = d_{\mathcal{Z}}$.*

D2 *Para cualesquiera $j, k \in \{1, \dots, d\}$, o bien $\mathcal{Z}_j \cap \mathcal{Z}_k = \emptyset$, o bien existe $l \in \{1, \dots, d\}$ de forma que $\mathcal{Z}_j \cap \mathcal{Z}_k = \mathcal{Z}_l$.*

D3 *Para cualesquiera $j, k \in \{1, \dots, d\}$ tal que $\mathcal{Z}_j \subset \mathcal{Z}_k$ se cumple:*

- *Existe $a \in \mathbb{Z}^*$ tal que $ah_{ji} = h_{ki}$, para todo $i \in \mathcal{Z}_j$ (es decir, los vectores $(\underline{h}_k)_{\mathcal{Z}_j}$ y $(\underline{h}_j)_{\mathcal{Z}_j}$ son proporcionales).*
- *Existe $l \in \{1, \dots, d\}$ tal que $\mathcal{Z}_l = \mathcal{Z}_j$ y $(\underline{\lambda}_l)_{\mathcal{Z}_j}^{\underline{m}} = (\underline{\lambda}_k)_{\mathcal{Z}_j}^{\underline{m}}$, para todo $\underline{m} \in L_j$.*

Dem. Por el Teorema 1.5.11, sabemos que I es binomial si y sólo si se cumplen las condiciones C1, C2 y C3. Estas condiciones son equivalentes a las expresadas en los apartados D1, D2 y D3 del teorema anterior ya que:

- En la Proposición 2.2.16 hemos visto que C1 es equivalente a que para todo $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$, el ideal $J_{\mathcal{Z}} = I_{\mathcal{Z}} \cap k[\mathcal{Z}]$ sea binomial. Como se explicó en la Nota 2.2.15, $J_{\mathcal{Z}}$ es el ideal de la unión de las curvas monomiales irreducibles, $\mathrm{pr}_{\mathcal{Z}}(C_j)$, con j variando en $A_{\mathcal{Z}}$, todas ellas con célula asociada $\mathcal{Z}$. Por lo tanto, aplicando el Teorema 2.2.20, $J_{\mathcal{Z}}$ es binomial si y sólo si se cumplen las condiciones impuestas en D1.
- Por el Teorema 2.2.8, C2 es equivalente a D2.
- Como consecuencia del Teorema 2.2.11, C3 y D3 son equivalentes si se cumple D1 ya que en este caso, si $\mathcal{Z}_l = \mathcal{Z}_j$ entonces $(\underline{h}_l)_{\mathcal{Z}_j} = (\underline{h}_j)_{\mathcal{Z}_j}$.

□

El teorema que acabamos de ver nos va a proporcionar un método computacional que determina cuándo la unión de curvas monomiales por el origen es una curva monomial.

Veamos un ejemplo de una curva por el origen que cumple las condiciones del teorema anterior y, por tanto, es monomial.

Ejemplo 2.2.24 Consideremos las curvas monomiales construidas en el Ejemplo 2.2.22

$$C^1 = C_1^1 \cup C_2^1$$

donde

$$C_1^1 \equiv \begin{cases} x = t \\ y = 2t^2 \end{cases} \qquad C_2^1 \equiv \begin{cases} x = t \\ y = -2t^2 \end{cases},$$

y

$$C^2 = C_1^2 \cup C_2^2$$

donde

$$C_1^2 \equiv \begin{cases} x = 2t \\ y = 5t^2 \end{cases} \qquad C_2^2 \equiv \begin{cases} x = 3t \\ y = \frac{-45}{4}t^2 \end{cases}.$$

Consideramos ahora la curva $C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$ donde:

$$C_1 \equiv \begin{cases} x = t \\ y = 2t^2 \\ z = 0 \end{cases}, \; C_2 \equiv \begin{cases} x = t \\ y = -2t^2 \\ z = 0 \end{cases},$$
$$C_3 \equiv \begin{cases} x = 0 \\ y = 2t \\ z = 5t^2 \end{cases}, \; C_4 \equiv \begin{cases} x = 0 \\ y = 3t \\ z = \frac{-45}{4}t^2 \end{cases} \text{ y } C_5 \equiv \begin{cases} x = 0 \\ y = t \\ z = 0 \end{cases}.$$

Si denotamos $\mathcal{Z}_1 = \{1, 2\}$, $\mathcal{Z}_2 = \{2, 3\}$ y $\mathcal{Z}_3 = \{2\}$, entonces $U = \{\mathcal{Z}_1, \mathcal{Z}_2, \mathcal{Z}_3\}$. Pero como C^1 y C^2 son monomiales, la condición D1 se cumple para $\mathcal{Z} = \mathcal{Z}_1$ y para $\mathcal{Z} = \mathcal{Z}_2$. Además $|A_{\mathcal{Z}_3}| = 1$ luego D1 también se cumple para $\mathcal{Z} = \mathcal{Z}_3$. Por último, es claro que C satisface D2 y D3, luego C es monomial.

El enunciado del Teorema 2.2.23 se simplifica considerablemente en el caso de que las componentes de la curva sean monomiales irreducibles puras (curvas irreducibles que admiten una parametrización monomial cumpliendo que todos los coeficientes que corresponden a índices de la célula sean uno). En este caso sólo aparecen condiciones que implican a los exponentes de las parametrizaciones y a las células de las componentes, por lo que la caracterización es puramente combinatoria.

Teorema 2.2.25 *Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de curvas monomiales irreducibles puras distintas, y sea $I := \mathcal{I}(C)$. Consideremos, para cada componente irreducible C_j, el vector de exponentes $\underline{h}_j$ y su célula asociada $\mathcal{Z}_j$. Definimos, para cada $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$, $A_{\mathcal{Z}} = \{j \in \{1, \ldots, d\} \mid \mathcal{Z}_j = \mathcal{Z}\}$. Entonces, son equivalentes:*

(1) *I es binomial.*

(2) *Se cumplen las condiciones D1', D2' y D3' siguientes:*

- **D1'** *Para cada $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$ se tiene $|A_{\mathcal{Z}}| = 1$.*
- **D2'** *Para cualesquiera $j, k \in \{1, \ldots, d\}$, o bien $\mathcal{Z}_j \cap \mathcal{Z}_k = \emptyset$, o bien existe $l \in \{1, \ldots, d\}$ de forma que $\mathcal{Z}_j \cap \mathcal{Z}_k = \mathcal{Z}_l$.*
- **D3'** *Para cualesquiera $j, k \in \{1, \ldots, d\}$ tal que $\mathcal{Z}_j \subset \mathcal{Z}_k$, existe $a \in \mathbb{Z}^*$ tal que $ah_{ji} = h_{ki}$ para todo $i \in \mathcal{Z}_j$.*

Dem. Sabemos que I es binomial si y sólo si se cumplen las condiciones D1, D2 y D3 del 2.2.23. Si se cumple D1 entonces, para todo $j \in A_{\mathcal{Z}}$, $(\underline{h}_j)_{\mathcal{Z}} = \underline{h}_{\mathcal{Z}}$, y como todas las componentes de C son puras y distintas entonces $|A_{\mathcal{Z}}| = 1$ y $L_{\mathcal{Z}} = \widetilde{L}_{\mathcal{Z}}$. Además, si $|A_{\mathcal{Z}}| = 1$ es claro que $J_{\mathcal{Z}}$ es binomial. Por lo tanto la condición D1 del Teorema 2.2.23 es equivalente a D1'. La condición D2 es igual que la D2' y teniendo en cuenta que si $\mathcal{Z} \subset \mathcal{Z}_j$ entonces $(\underline{\lambda}_j)_{\mathcal{Z}}^{\underline{m}} = 1$ para todo $\underline{m} \in \mathbb{Z}^{\mathcal{Z}}$, la condición D3 se escribe ahora como D3'.

$\square$

2.2.4 Curvas monomiales. Caso general

En el apartado 2.2.3 hemos caracterizado qué uniones de curvas monomiales irreducibles son curvas monomiales, a través de condiciones combinatorias sobre las parametrizaciones de las componentes. Dichas condiciones fueron determinadas cuando todas las componentes de la curva pasan por el origen. Veamos en esta subsección las condiciones que hay que imponer cuando permitimos que las componentes no pasen por el origen.

Sea $C \subset \mathcal{A}^n(k)$ una unión de las curvas monomiales irreducibles distintas $C_1, \ldots, C_d$. Consideremos la descomposición minimal de $I := \mathcal{I}(C)$,

$$I = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_d, \quad \text{donde } \mathcal{P}_j = \mathcal{I}(C_j) \;\; \forall j \in \{1, \ldots, d\}.$$

Para cada $j \in \{1, \dots, d\}$ denotemos por $\mathcal{Z}_j$ la célula asociada a la curva C_j y consideremos una parametrización monomial Ψ_j de C_j de vectores $(\underline{h}_j, \underline{\lambda}_j)$. Como hicimos en 2.1.19, se consideran el punto $P_j = \Psi_j(0)$ y el subconjunto de la célula $\mathcal{Z}_j$, $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_{ji} = 0\}$, elementos que no dependen de la parametrización elegida Ψ_j.

En la Proposición 2.2.5 vimos que dado un conjunto $\mathcal{Z} \subseteq \{1, \dots, n\}$ se cumple

$$C \cap (k^*)^{\mathcal{Z}} = \left(\bigcup_{\mathcal{Z}_j = \mathcal{Z}} (C_j \setminus \{P_j\}) \right) \cup \left(\bigcup_{\widetilde{\mathcal{Z}}_j = \mathcal{Z}} \{P_j\} \right).$$

Por tanto, si consideramos el ideal $I_{\mathcal{Z}} = \mathcal{I}(\overline{C \cap (k^*)^{\mathcal{Z}}})$ y denotamos por $\mathcal{M}_j$ al ideal maximal $\mathcal{M}_j = \mathcal{I}(\{P_j\})$, se tiene,

$$I_{\mathcal{Z}} = (\bigcap_{\mathcal{Z}_j = \mathcal{Z}} \mathcal{P}_j) \cap (\bigcap_{\widetilde{\mathcal{Z}}_j = \mathcal{Z}} \mathcal{M}_j).$$

Luego $I_{\mathcal{Z}}$ es un ideal propio si y sólo si $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d, \widetilde{\mathcal{Z}}_1, \dots, \widetilde{\mathcal{Z}}_d\}$.

Proposición 2.2.26 *Dado $\mathcal{Z} \in \{\mathcal{Z}_1, \dots, \mathcal{Z}_d, \widetilde{\mathcal{Z}}_1, \dots, \widetilde{\mathcal{Z}}_d\}$ se definen $J_{\mathcal{Z}} = I_{\mathcal{Z}} \cap k[\mathcal{Z}]$, $\widetilde{\mathcal{P}}_j = \mathcal{P}_j \cap k[\mathcal{Z}]$ para cada j tal que $\mathcal{Z} = \mathcal{Z}_j$ y $\widetilde{\mathcal{M}}_j = \mathcal{M}_j \cap k[\mathcal{Z}]$ para cada j tal que $\mathcal{Z} = \widetilde{\mathcal{Z}}_j$. Entonces, se tiene que*

1. *$J_{\mathcal{Z}} = (\cap_{\mathcal{Z}_j = \mathcal{Z}} \widetilde{\mathcal{P}}_j) \cap (\cap_{\widetilde{\mathcal{Z}}_j = \mathcal{Z}} \widetilde{\mathcal{M}}_j)$, y esta expresión es una descomposición primaria de $J_{\mathcal{Z}}$ (no necesariamente minimal).*

2. *$I_{\mathcal{Z}} = J_{\mathcal{Z}} + M(\mathcal{Z})$ (suma en $k[X]$).*

3. *Para cada j tal que $\mathcal{Z} = \mathcal{Z}_j$, $\mathcal{P}_j = \widetilde{\mathcal{P}}_j + M(\mathcal{Z})$.*

4. *$\widetilde{\mathcal{P}}_j$ es primo de altuna $|\mathcal{Z}| - 1$.*

5. *Para cada j tal que $\mathcal{Z} = \widetilde{\mathcal{Z}}_j$, $\mathcal{M}_j = \widetilde{\mathcal{M}}_j + M(\mathcal{Z})$.*

6. *$\widetilde{\mathcal{M}}_j$ es maximal en $k[\mathcal{Z}]$.*

7. *$J_{\mathcal{Z}} = (J_{\mathcal{Z}} : (\prod_{i \in \mathcal{Z}} X_i)^\infty)$.*

Dem. Análoga a la demostración de la Proposición 2.2.14, teniendo en cuenta las consideraciones sobre el caso especial de ideales de puntos dadas en la Proposición 2.1.21.

□

Nota 2.2.27 El ideal $\widetilde{\mathcal{P}}_j$ es el ideal asociado a la curva monomial irreducible $C_{j,\mathcal{Z}_j} = \mathrm{pr}_{\mathcal{Z}_j}(C_j) \subset k^{\mathcal{Z}_j}$. Luego el retículo asociado a $\widetilde{\mathcal{P}}_j$ es $\langle(\underline{h}_j)_{\mathcal{Z}_j}\rangle^\perp$.

Nota 2.2.28 El ideal $\widetilde{\mathcal{M}}_j$ es el ideal asociado al punto $P_j = \mathrm{pr}_{\widetilde{\mathcal{Z}}_j}(C_j) \in (k)^{\widetilde{\mathcal{Z}}_j}$. Luego el retículo asociado a $\widetilde{\mathcal{M}}_j$ es $\mathbb{Z}^{\widetilde{\mathcal{Z}}_j}$ (Proposición 2.1.21).

Según el teorema de caracterización de las variedades cortadas por binomios (Teorema 1.5.11), la condición de I binomial es equivalente a que se cumplan las condiciones C1, C2 y C3 de dicho teorema. La condición C1, que exige que los ideales $I_\mathcal{Z}$ sean binomiales, equivale a que para todo $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d, \widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_d\}$ el ideal $J_\mathcal{Z}$ sea binomial (Proposición 2.2.26). Como consecuencia, se tiene:

Proposición 2.2.29 *Si I es binomial, entonces:*

1. *Para todo $\mathcal{Z} \in \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d, \widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_d\}$ existe un carácter parcial $\rho_\mathcal{Z}$, definido sobre un subretículo $L_{\rho_\mathcal{Z}}$ de $\mathbb{Z}^\mathcal{Z}$, con $J_\mathcal{Z} = I_+(\rho_\mathcal{Z})$ y por tanto*
$$I_\mathcal{Z} = I_+(\rho_\mathcal{Z}) + M(\mathcal{Z}).$$
2. *Si existen j, k tales que $\mathcal{Z}_j = \widetilde{\mathcal{Z}}_k$, entonces existe l tal que $\mathcal{Z}_j = \mathcal{Z}_l$ y $\mathcal{P}_l \subseteq \mathcal{M}_k$.*
3. *Si existe $j \in \{1, \ldots, d\}$ tal que $\mathcal{Z} = \mathcal{Z}_j$ entonces $J_\mathcal{Z} = \cap_{\mathcal{Z}_j=\mathcal{Z}}\widetilde{\mathcal{P}}_j$ (es decir, $I_\mathcal{Z} = \cap_{\mathcal{Z}_j=\mathcal{Z}}\mathcal{P}_j$), $L_{\rho_\mathcal{Z}}$ es un subretículo de $\mathbb{Z}^\mathcal{Z}$ de rango $|\mathcal{Z}| - 1$ y existe un vector $\underline{h}_\mathcal{Z} \in \mathbb{Z}^\mathcal{Z}$ con coordenadas no negativas tal que* $\mathrm{Sat}\, L_{\rho_\mathcal{Z}} = \langle \underline{h}_\mathcal{Z}\rangle^\perp$.
4. *Si no existe $j \in \{1, \ldots, d\}$ tal que $\mathcal{Z} = \mathcal{Z}_j$, entonces, $L_{\rho_\mathcal{Z}}$ es un subretículo de $\mathbb{Z}^\mathcal{Z}$ de rango $|\mathcal{Z}|$, y* $\mathrm{Sat}\, L_{\rho_\mathcal{Z}} = \mathbb{Z}^\mathcal{Z}$.

Dem. Como I es el ideal de una curva monomial, $I_\mathcal{Z}$, y por tanto $J_\mathcal{Z}$, son binomiales. Además $J_\mathcal{Z}$ no contiene monomios y $J_\mathcal{Z} = (J_\mathcal{Z} : (\prod_{i\in\mathcal{Z}} X_i)^\infty)$ (Proposición 2.2.26). Luego, por el Corolario 1.3.11, debe existir un carácter parcial $\rho_\mathcal{Z}$, definido sobre un subretículo $L_{\rho_\mathcal{Z}}$ de $\mathbb{Z}^\mathcal{Z}$, con $J_\mathcal{Z} = I_+(\rho_\mathcal{Z})$.

Entonces, usando el Corolario 1.3.12, la descomposición primaria minimal de $J_{\mathcal{Z}}$ es $J_{\mathcal{Z}} = \cap I_+(\rho_j)$, donde ρ_j denotan las extensiones de $\rho_{\mathcal{Z}}$ a Sat $L_{\rho_{\mathcal{Z}}}$. Pero puesto que

$$J_{\mathcal{Z}} = (\bigcap_{\mathcal{Z}_j=\mathcal{Z}} \widetilde{\mathcal{P}}_j) \cap (\bigcap_{\widetilde{\mathcal{Z}}_j=\mathcal{Z}} \widetilde{\mathcal{M}_j}), \tag{2.1}$$

cada ideal $I_+(\rho_j)$ es, o bien uno de los primos $\widetilde{\mathcal{P}}_j$, o bien uno de los maximales $\widetilde{\mathcal{M}}_j$. Ahora bien, no es posible que en la descomposición $J_{\mathcal{Z}} = \cap I_+(\rho_j)$ aparezcan a la vez primos $\widetilde{\mathcal{P}}_j$ (ideales de curvas monomiales irreducibles, y por tanto asociados a retículos de rango $|\mathcal{Z}| - 1$) e ideales maximales $\widetilde{\mathcal{M}}_j$ (ideales de puntos, y por tanto asociados a retículos de rango $|\mathcal{Z}|$, Proposición 2.1.21), pues el retículo Sat $L_{\rho_{\mathcal{Z}}}$ es común a todos los ideales $I_+(\rho_j)$. Por tanto, si se tiene $\mathcal{Z}_j = \widetilde{\mathcal{Z}}_k = \mathcal{Z}$, en (2.1) aparecen $\widetilde{\mathcal{P}}_j$ y $\widetilde{\mathcal{M}}_k$, y por tanto $\widetilde{\mathcal{M}}_k$ debe desaparecer, es decir, $\cap_{\mathcal{Z}_l=\mathcal{Z}} \widetilde{\mathcal{P}}_l \subseteq \widetilde{\mathcal{M}}_k$ luego existe l tal que $\mathcal{Z}_j = \mathcal{Z}_l$ y $\mathcal{P}_l \subseteq \mathcal{M}_k$ y se tiene 2.

Los apartados 3 y 4 se deducen de todo lo anterior, teniendo en cuenta que $\widetilde{\mathcal{P}}_j$ es el ideal de la curva $C_{j,\mathcal{Z}_j}$ y por tanto Sat $(L_{\rho_{\mathcal{Z}}}) = \langle \underline{h}_{\mathcal{Z}} \rangle^{\perp}$ siendo $\underline{h}_{\mathcal{Z}} = (\underline{h}_j)_{\mathcal{Z}_j}$ para algún j con $\mathcal{Z}_j = \mathcal{Z}$.

□

Como consecuencia del apartado 2 de la proposición anterior, se tiene que las curvas monomiales deben cumplir:

$\boxed{\textbf{D0}}$ Si existen j, k tales que $\mathcal{Z}_j = \widetilde{\mathcal{Z}}_k$ entonces debe existir l tal que $\mathcal{Z}_j = \mathcal{Z}_l$ y $P_k \in C_l$.

Obsérvese que si se cumple $P_k \in C_l$ con $\mathcal{Z}_l = \widetilde{\mathcal{Z}}_k$, entonces $P_k \neq P_l$ pues siempre $\widetilde{\mathcal{Z}}_l \neq \mathcal{Z}_l$.

La condición D0 es necesaria para que los ideales $J_{\mathcal{Z}}$ sean binomiales, y hay que añadirla en el enunciado del teorema análogo a 2.2.23. Además, también es necesario modificar las condiciones D1, D2 y D3 de dicho teorema, como veremos a continuación.

Distinguiremos dos tipos de índices en $\{1, \ldots, d\}$: los índices del primer tipo serán aquellos k tales que existe $j \in \{1, \ldots, d\}$ con $\mathcal{Z}_j = \widetilde{\mathcal{Z}}_k$; el resto serán del segundo tipo. Supongamos, tras una reordenación, que los índices del segundo tipo son $\{1, \ldots, s\}$, $s \leq d$. Se considera el conjunto,

$$U = \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\} \cup \{\widetilde{\mathcal{Z}}_1, \dots, \widetilde{\mathcal{Z}}_s\}. \tag{2.2}$$

Proposición 2.2.30 *En estas condiciones se tiene que si C es una curva monomial, entonces $C \cap (k^*)^{\mathcal{Z}} \neq \emptyset$ si y sólo si $\mathcal{Z} \in U$. Además,*

$$C \cap (k^*)^{\mathcal{Z}_k} = \bigcup_{\mathcal{Z}_j = \mathcal{Z}_k} (C_j \backslash \{P_j\}), \quad 1 \le k \le d$$
$$C \cap (k^*)^{\widetilde{\mathcal{Z}}_k} = \bigcup_{\widetilde{\mathcal{Z}}_j = \widetilde{\mathcal{Z}}_k} \{P_j\}, \quad 1 \le k \le s.$$

Dem. Basta tener en cuenta la condición D0 y la Proposición 2.2.5.

□

Nota 2.2.31 $C \cap (k^*)^{\emptyset} \neq \emptyset$ si y sólo si alguna componente pasa por el origen, es decir, si existe $j \in \{1, \dots, d\}$ tal que $\widetilde{\mathcal{Z}}_j = \emptyset$ (el caso $\mathcal{Z}_j = \emptyset$ no se puede dar pues C_j es una curva).

Teniendo en cuenta estos resultados, es fácil ver, de forma similar al caso de curvas por el origen, que ahora las condiciones C2, C3 y C1 del Teorema 1.5.11 se traducen en:

$\boxed{\textbf{D2}}$ El conjunto U es cerrado para intersecciones.

Por la proposición anterior $\{\mathcal{Z} \subseteq \{1, \dots, n\} \mid C \cap (k^*)^{\mathcal{Z}} \neq \emptyset\} = U$, luego la condición C2 del Teorema 1.5.11 es equivalente a D2.

$\boxed{\textbf{D3}}$

- Si $\mathcal{Z}_j \subseteq \widetilde{\mathcal{Z}}_k$ con $1 \le j \le d$ y $1 \le k \le s$, entonces existe l tal que $\mathcal{Z}_l = \mathcal{Z}_j$ y $\pi_{\mathcal{Z}_j}(P_k) \in C_l$.

- Si $\mathcal{Z}_j \subseteq \mathcal{Z}_k$ con $1 \le j, k \le d$, y $\mathcal{Z}_j \not\subseteq \widetilde{\mathcal{Z}}_k$ entonces existe l tal que $\mathcal{Z}_l = \mathcal{Z}_j$ y $\pi_{\mathcal{Z}_j}(C_k) = C_l$.

- Si $\widetilde{\mathcal{Z}}_j \subseteq \widetilde{\mathcal{Z}}_k$ con $1 \le j, k \le s$, entonces existe l tal que $\widetilde{\mathcal{Z}}_l = \widetilde{\mathcal{Z}}_j$ y $\pi_{\widetilde{\mathcal{Z}}_j}(P_k) = P_l$.

- Si $\widetilde{\mathcal{Z}}_j \subseteq \mathcal{Z}_k$ con $1 \le j \le s$ y $1 \le k \le d$, entonces existe l tal que $\widetilde{\mathcal{Z}}_l = \widetilde{\mathcal{Z}}_j$ y $\pi_{\widetilde{\mathcal{Z}}_j}(C_k) = \{P_l\}$ (y en particular, $\widetilde{\mathcal{Z}}_j \subseteq \widetilde{\mathcal{Z}}_k$).

Estos cuatro puntos tienen una inmediata traducción sobre los vectores de las parametrizaciones, como veremos en el teorema de caracterización de las curvas monomiales. Obsérvese que, en presencia del punto tercero, el cuarto punto se puede sustituir por:

- Si $\widetilde{\mathcal{Z}}_j \subseteq \mathcal{Z}_k$ entonces $\widetilde{\mathcal{Z}}_j \subseteq \widetilde{\mathcal{Z}}_k$.

$\boxed{\textbf{D1}}$ Es equivalente a que para todo $\mathcal{Z} \in U$, el ideal $J_{\mathcal{Z}}$ sea binomial.

Ahora los ideales $J_{\mathcal{Z}}$ son de dos tipos:

1. $J_{\mathcal{Z}_k} = \cap_{\mathcal{Z}_j=\mathcal{Z}_k}\widetilde{\mathcal{P}}_j$, es decir, $I_{\mathcal{Z}_k} = \cap_{\mathcal{Z}_j=\mathcal{Z}_k}\mathcal{P}_j$, si $1 \leq k \leq d$.
2. $J_{\widetilde{\mathcal{Z}}_k} = \cap_{\widetilde{\mathcal{Z}}_j=\widetilde{\mathcal{Z}}_k}\widetilde{\mathcal{M}}_j$, es decir, $I_{\widetilde{\mathcal{Z}}_k} = \cap_{\widetilde{\mathcal{Z}}_j=\widetilde{\mathcal{Z}}_k}\mathcal{M}_j$, si $1 \leq k \leq s$.

(consecuencia de las Proposiciones 2.2.29 y 2.2.30). La situación 1 es totamente análoga a la del caso de curvas por el origen. Para el caso 2, el procedimiento es completamente paralelo, salvo que ahora el retículo saturado a considerar es $\mathbb{Z}^{\mathcal{Z}}$. Concretamente, en el caso 2, se tiene:

Proposición 2.2.32 *Para todo $\mathcal{Z} \in \{\widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_s\}$ definimos $A_{\mathcal{Z}} = \{j \mid \widetilde{\mathcal{Z}}_j = \mathcal{Z}\}$, $B_{\mathcal{Z}} = \{P_j \mid j \in A_{\mathcal{Z}}\}$, $d_{\mathcal{Z}} = |\mathcal{B}_{\mathcal{Z}}|$ (es decir, $d_{\mathcal{Z}} = |\mathcal{V}(J_{\mathcal{Z}})|$) y $L_{\mathcal{Z}} = \{\underline{m} \in \mathbb{Z}^{\mathcal{Z}} \mid (\underline{\lambda}_j)^{\underline{m}}_{\mathcal{Z}} = (\underline{\lambda}_k)^{\underline{m}}_{\mathcal{Z}}$ para cualesquiera $j,k \in A_{\mathcal{Z}}\}$. Entonces $J_{\mathcal{Z}}$ es binomial si y sólo si $|\mathbb{Z}^{\mathcal{Z}}/L_{\mathcal{Z}}| = d_{\mathcal{Z}}$.*

Dem. Totalmente análoga a la demostración del Teorema 2.2.20, teniendo en cuenta que si $\mathcal{V}(J_{\mathcal{Z}}) = \{P_{i_1}, \ldots, P_{i_{d_{\mathcal{Z}}}}\}$ (tras eliminar los puntos repetidos) entonces la descomposición primaria minimal de $J_{\mathcal{Z}}$ es $J_{\mathcal{Z}} = \widetilde{\mathcal{M}}_{i_1} \cap \ldots \cap \widetilde{\mathcal{M}}_{i_{d_{\mathcal{Z}}}}$.

$\square$

Teniendo en cuenta estas consideraciones, el teorema de caracterización de las curvas monomiales desde el punto de vista de las parametrizaciones resulta:

Teorema 2.2.33 *Sea C una curva cuyas componentes irreducibles, $C_1, \ldots,$ C_d, son monomiales y sea $I := \mathcal{I}(C)$. Consideremos, para cada componente monomial irreducible C_j, una parametrización monomial ψ_j dada por los vectores $(\underline{h}_j, \underline{\lambda}_j)$, su célula asociada $\mathcal{Z}_j$ y el conjunto $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_i = 0\}$. Consideremos, además, el punto $P_j = \psi_j(0)$ y el retículo asociado a C_j, $L_j = \langle(\underline{h}_j)_{\mathcal{Z}_j}\rangle^{\perp}$. Tras una reordenación de las componentes, supongamos* *que* $j \in \{1, \ldots, s\}$ *(*$s \leq d$*) si y sólo si no existe* $k \in \{1, \ldots, d\}$ *con* $\widetilde{\mathcal{Z}}_j = \mathcal{Z}_k$*. Definimos*

$$U = U_1 \sqcup U_2 \text{ donde } U_1 = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\} \text{ y } U_2 = \{\widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_s\}.$$

Para todo $\mathcal{Z} \in U_1$ *se definen* $A_{\mathcal{Z}} = \{j \mid \mathcal{Z}_j = \mathcal{Z}\}$ *y* $d_{\mathcal{Z}} = |A_{\mathcal{Z}}|$*. Para todo* $\mathcal{Z} \in U_2$ *se definen* $A_{\mathcal{Z}} = \{j \mid \widetilde{\mathcal{Z}}_j = \mathcal{Z}\}$, $B_{\mathcal{Z}} = \{P_j \mid \widetilde{\mathcal{Z}}_j = \mathcal{Z}\}$ *y* $d_{\mathcal{Z}} = |B_{\mathcal{Z}}|$*. Entonces, son equivalentes:*

(1) *I es binomial.*

(2) *Se cumplen las condiciones D0, D1, D2 y D3 siguientes:*

D0 *Si existen* j, k *tales que* $\mathcal{Z}_j = \widetilde{\mathcal{Z}}_k$ *entonces debe existir* l *tal que* $\mathcal{Z}_j = \mathcal{Z}_l$ *y* $P_k \in C_l$*.*

D1 *Para todo* $\mathcal{Z} \in U$ *se cumple:*

1. *Si* $\mathcal{Z} \in U_1$*, existe* $\underline{h}_{\mathcal{Z}} \in \mathbb{Z}^{\mathcal{Z}}$ *tal que* $\underline{h}_{\mathcal{Z}} = (\underline{h}_j)_{\mathcal{Z}}$ *para todo* $j \in A_{\mathcal{Z}}$*.*
2. *Sean* $j \in A_{\mathcal{Z}}$, $\widetilde{L}_{\mathcal{Z}} = \langle(\underline{h}_j)_{\mathcal{Z}}\rangle^{\perp}$ *y* $L_{\mathcal{Z}} = \{\underline{m} \in \widetilde{L}_{\mathcal{Z}} \mid (\underline{\lambda}_j)_{\mathcal{Z}}^{\underline{m}} = (\underline{\lambda}_k)_{\mathcal{Z}}^{\underline{m}}, \forall j, k \in A_{\mathcal{Z}}\}$*. Entonces* $|\widetilde{L}_{\mathcal{Z}}/L_{\mathcal{Z}}| = d_{\mathcal{Z}}$*.*

D2 *El conjunto* U *es cerrado para intersecciones.*

D3
- *Para cualesquiera* $j \in \{1, \ldots, d\}$ *y* $k \in \{1, \ldots, s\}$ *tales que* $\mathcal{Z}_j \subseteq \widetilde{\mathcal{Z}}_k$ *existe* $l \in \{1, \ldots, d\}$ *tal que* $l \in A_{\mathcal{Z}_j}$ *y* $((\underline{\lambda}_l)_{\mathcal{Z}_j})^{\underline{m}} = ((\underline{\lambda}_k)_{\mathcal{Z}_j})^{\underline{m}}$ *para todo* $\underline{m} \in L_j$*.*
- *Para cualesquiera* $j, k \in \{1, \ldots, d\}$ *tales que* $\mathcal{Z}_j \subseteq \mathcal{Z}_k$ *y* $\mathcal{Z}_j \not\subseteq \widetilde{\mathcal{Z}}_k$*, se tiene:*
  Existe $a \in \mathbb{Z}^*$ *tal que* $ah_{ji} = h_{ki}$*, para todo* $i \in \mathcal{Z}_j$*.*
  Existe $l \in \{1, \ldots, d\}$ *tal que* $l \in A_{\mathcal{Z}_j}$ *y* $((\underline{\lambda}_l)_{\mathcal{Z}_j})^{\underline{m}} = ((\underline{\lambda}_k)_{\mathcal{Z}_j})^{\underline{m}}$ *para todo* $\underline{m} \in L_j$*.*
- *Para cualesquiera* $j, k \in \{1, \ldots, s\}$ *tales que* $\widetilde{\mathcal{Z}}_j \subseteq \widetilde{\mathcal{Z}}_k$ *existe* $l \in \{1, \ldots, s\}$ *tal que* $l \in A_{\widetilde{\mathcal{Z}}_j}$ *y* $(\underline{\lambda}_l)_{\widetilde{\mathcal{Z}}_j} = (\underline{\lambda}_k)_{\widetilde{\mathcal{Z}}_j}$*.*
- *Para cualesquiera* $j \in \{1, \ldots, s\}$ *y* $k \in \{1, \ldots, d\}$ *tales que* $\widetilde{\mathcal{Z}}_j \subseteq \mathcal{Z}_k$*, se tiene* $\widetilde{\mathcal{Z}}_j \subseteq \widetilde{\mathcal{Z}}_k$*.*

Nota 2.2.34 En particular, si C es una curva monomial y denotamos por $\mathcal{Z}_j^*$ a los elementos de U ($\mathcal{Z}_j^* = \mathcal{Z}_j$ o $\mathcal{Z}_j^* = \widetilde{\mathcal{Z}}_j$), se cumple que si $\mathcal{Z}_j^* \subseteq \mathcal{Z}_k^*$ entonces existe $a \in \mathbb{Z}$ tal que $ah_{ji} = h_{ki}$ para todo $i \in \mathcal{Z}_j^*$.

2.3 Algoritmos

Existe una forma obvia de saber, computacionalmente, cuándo una unión de curvas dadas por parametrizaciones monomiales es monomial: el cálculo de una base de Gröbner del ideal asociado a dicha curva. Los pasos a seguir serían:

1. Dada la parametrización monomial de cada componente C_j, $(\underline{h}_j, \underline{\lambda}_j)$, buscar una base de Gröbner del ideal $\langle X_1 - \lambda_{j1} t^{h_{j1}}, \ldots, X_n - \lambda_{jn} t^{h_{jn}} \rangle \subset k[X_1, \ldots, X_n, t]$ para el orden lexicográfico donde $X_1 < \ldots < X_n < t$, y selecionar, dentro de ella, los polinomios en $k[X_1, \ldots, X_n]$. El conjunto obtenido es una base de Gröbner de $\mathcal{I}(C_j)$.

2. Una vez obtenidas una base de Gröbner de $\mathcal{I}(C_j)$, G_j, y una de $\mathcal{I}(C_k)$, G_k, se calcula una base de Gröbner del ideal $\langle \{tg \mid g \in G_j\} \cup \{(1-t)g \mid g \in G_k\} \rangle \subset k[X_1, \ldots, X_n, t]$ para el orden lexicográfico donde $X_1 < \ldots < X_n < t$. Haciendo la intersección de dicha base con $k[X_1, \ldots, X_n]$, obtenemos una base de Gröbner de $\mathcal{I}(C_j) \cap \mathcal{I}(C_k)$.

A pesar de esto, en esta sección intentaremos aprovechar los aspectos combinatorios del Teorema 2.2.33 para construir un método alternativo, que también servirá para poner de manifiesto los elementos (retículos y caracteres parciales) asociados a la curva.

Por comodidad en la notación expondremos, en primer lugar, el método para el caso de una curva unión de curvas monomiales irreducibles, que pase por el origen (todas las componentes irreducibles contienen al origen). Por lo tanto, el algoritmo deberá comprobar cuándo se cumplen las condiciones D1, D2 y D3 del Teorema 2.2.23.

Comenzaremos estableciendo un algoritmo que compruebe cuándo se cumple la condición D1. Para ello necesitamos determinar cuándo una unión de curvas monomiales irreducibles, todas con célula asociada la total, es una curva monomial.

2.3.1 Construcción de una base del ortogonal en $\mathbb{Z}^n$ a un vector

Consideremos un vector $\underline{h} = (h_1, \ldots, h_n) \in (\mathbb{Z}_{\geq 0})^n$ no nulo. Vamos a calcular una base del retículo saturado de $\mathbb{Z}^n$ dado por $L = \langle \underline{h} \rangle^\perp = \{\underline{m} \in \mathbb{Z}^n \mid \underline{m}\,\underline{h} = 0\}$.

Consideramos la aplicación $\mathbb{Z}$-lineal φ dada por

$$\begin{array}{rcl}\varphi : \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ \underline{m} & \longmapsto & \sum_{i=1}^n m_i h_i \end{array} .$$

Es obvio que $L = \ker(\varphi)$, luego si encontramos una base $\{\underline{v}_1, \dots, \underline{v}_n\}$ de $\mathbb{Z}^n$ tal que la matriz de φ en dicha base sea $(a, 0, \dots, 0)$ con $a \neq 0$, tendremos que $\{\underline{v}_2, \dots, \underline{v}_n\}$ será una base de L. Puesto que la matriz de φ en la base canónica es $(h_1, \dots, h_n)$, necesitamos encontrar una matriz inversible $M \in \mathcal{M}_{n\times n}(\mathbb{Z})$ tal que

$$(h_1, \dots, h_n)M = (a, 0, \dots, 0),$$

y la base de L estará dada por las $n-1$ últimas columnas de M.

Empecemos por suponer que para todo i, $h_i \neq 0$, y sea $d = \text{m.c.d.}\{h_i \mid 1 \leq i \leq n\}$. Para buscar M seguiremos los siguientes pasos:

Paso 1: Usando el algoritmo de Euclides, calculamos $d_1 = \text{m.c.d.}(h_1, h_2)$ y enteros a_{11}, a_{12} tales que $d_1 = a_{11}h_1 + a_{12}h_2$, y definimos $h'_1 = \frac{h_1}{d_1}$, $h'_2 = \frac{h_2}{d_1}$. Con estos valores construimos la matriz,

$$A_1 = \begin{pmatrix} a_{11} & -h'_2 & 0 & \cdots & 0 \\ a_{12} & h'_1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

que resulta inversible sobre $\mathbb{Z}$.

Se cumple $(h_1, \dots, h_n)A_1 = (d_1, 0, h_3, \dots, h_n)$.

Paso 2: Calculamos $d_2 = \text{m.c.d.}(d_1, h_3)$ y enteros a_{21}, a_{22} tales que $d_2 = a_{21}h_1 + a_{22}h_2$. Definimos $d'_1 = \frac{d_1}{d_2}$ y $h'_3 = \frac{h_3}{d_2}$. Para estos valores construimos la matriz,

$$A_2 = \begin{pmatrix} a_{21} & 0 & -h'_3 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ a_{22} & 0 & d'_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

que resulta inversible sobre $\mathbb{Z}$.

Se cumple $(d_1, 0, h_3 \dots, h_n)A_2 = (d_2, 0, 0, h_4, \dots, h_n)$.

Así, hasta llegar al último paso:

Paso $\mathbf{n-1}$: Calculamos $d_{n-1} = \text{m.c.d.}(d_{n-2}, h_n) = d$ y enteros $a_{n-1,1}$, $a_{n-1,2}$ tales que $d_{n-1} = a_{n-1,1}d_{n-2} + a_{n-1,2}h_n$. Definimos $d'_{n-2} = \frac{d_{n-2}}{d_{n-1}}$ y $h'_n = \frac{h_n}{d_{n-1}}$ y construimos la matriz,

$$A_{n-1} = \begin{pmatrix} a_{n-11} & 0 & 0 & \cdots & -h'_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-12} & 0 & 0 & \cdots & d'_{n-2} \end{pmatrix},$$

que resulta inversible sobre $\mathbb{Z}$.

Se cumple $(d_{n-2}, 0, \ldots, 0, h_n)A_2 = (d, 0, \ldots, 0)$.

Entonces la matriz $M = A_1A_2 \ldots A_{n-1}$ es inversible sobre $\mathbb{Z}$ y $(h_1, \ldots, h_n)$ $M = (d, 0, \ldots, 0)$ con $d \neq 0$ ya que $\underline{h} \neq \underline{0}$. Luego M es la matriz que buscábamos. Sus últimas $n-1$ columnas se pueden aislar multiplicando por la matriz con n filas y $n-1$ columnas,

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Por lo tanto, las columnas de MC proporcionan una base para el retículo L. Además la primera columna de M es un vector $\underline{\alpha} \in \mathbb{Z}^n$ con $\underline{\alpha}\,\underline{h} = d$ y, en particular, $\mathbb{Z}^n = L \oplus \langle\underline{\alpha}\rangle$.

Teniendo en cuenta el método descrito y adaptándolo al caso en que $\underline{h}$ tenga alguna coordenada nula, es claro que el siguiente algoritmo nos proporciona una base de $\langle\underline{h}\rangle^\perp$.

Algoritmo 2.3.1
Input: $\underline{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_{\geq 0}$.
Output: $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\} \subset \mathbb{Z}^n$.
Inicialización: *Definimos* $d^{(0)} = h_1$, $A = I_n$, $j = 0$.
Iteración: *Mientras* $1 \leq j \leq n-1$,

- *si* $h_{j+1} = 0$ *entonces* $j := j+1$

- *si* $h_{j+1} \neq 0$ *entonces, usando el algoritmo de Euclides, se calculan* $d^{(j)} = \text{m.c.d.}(d^{(j-1)}, h_{j+1})$ *y enteros* λ_j, μ_j, a_j *y* b_j *tales que,*

$$d^{(j)} = \lambda_j d^{(j-1)} + \mu_j h_{j+1} \quad y \quad d^{(j-1)} = d^{(j)} a_j,\ h_{j+1} = d^{(j)} b_j.$$

Se construye la matriz $A^{(j)} \in \mathcal{M}_n(\mathbb{Z})$ *tal que* $a^{(j)}_{1,1} = \lambda_j$, $a^{(j)}_{1,j+1} = -b_j$, $a^{(j)}_{j+1,1} = \mu_j$, $a^{(j)}_{j+1,j+1} = a_j$ *y el resto de coeficientes como en la matriz identidad. Se redefine* $A := A\,A^{(j)}$.

Salida: *El algoritmo devuelve* $\mathcal{B} = \{\underline{c}_2, \ldots, \underline{c}_n\}$*, siendo* $\{\underline{c}_1, \ldots, \underline{c}_n\}$ *las columnas de la matriz* A.

Teorema 2.3.2 *Sean* $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ *no nulo y* $L = \langle \underline{h} \rangle^{\perp}$*. Si el Algoritmo 2.3.1 aplicado al vector* $\underline{h}$ *devuelve* $\mathcal{B}$ *entonces* $\mathcal{B}$ *es una base del* $\mathbb{Z}$*-módulo* L*. Además, si* $\underline{\alpha} = \underline{c}_1$ *es la primera columna de la matriz* $A^{(1)} \cdots A^{(n-1)}$ *construida en dicho algoritmo, entonces* $\underline{\alpha}\,\underline{h} = d$*, siendo* $d = \text{m.c.d.}\{h_i \mid h_i \neq 0\}$.

Dem. Se deduce de la explicación previa al algoritmo.

$\square$

Ejemplo 2.3.3 Vamos a calcular una base de $L = \langle \underline{h} \rangle^{\perp}$, siendo $\underline{h} = (1, 2, 3)$. Como $\text{m.c.d.}(1, 2) = 1$ y $1 = (-1)1 + (1)2$ entonces,

$$A_1 = \begin{pmatrix} -1 & -2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Además teniendo en cuenta que $\text{m.c.d.}(1, 3) = 1$ y $1 = (-2)1 + (1)3$,

$$A_2 = \begin{pmatrix} -2 & 0 & -3 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Entonces la matriz M resulta

$$M = \begin{pmatrix} 2 & -2 & 3 \\ -2 & 1 & -3 \\ 1 & 0 & 1 \end{pmatrix}$$

y el conjunto $\{(-2, 1, 0), (3, -3, 1)\}$ es una base del $\mathbb{Z}$-módulo L. Además, la primera columna de M es un vector cuyo producto escalar con $\underline{h}$ es 1.

2.3.2 Cálculo del retículo asociado a una curva monomial en una célula

Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de curvas monomiales irreducibles tal que $\mathcal{Z}_j = \{1, \ldots, n\}$ para todo $j \in \{1, \ldots, d\}$. Consideremos, para cada j, una parametrización monomial de C_j, dada por los vectores $(\underline{h}_j, \underline{\lambda}_j)$.

Recordemos que si C es monomial se tiene que $\underline{h}_j = \underline{h}_1$ para todo $j \in \{1, \ldots, d\}$ y que si $I := \mathcal{I}(C)$ entonces $I = I_+(\rho)$, siendo

$$L_\rho = \{\underline{m} \in \langle \underline{h}_1 \rangle^\perp \mid \underline{\lambda}_j^{\underline{m}} = \underline{\lambda}_1^{\underline{m}},\ \forall j \in \{2, \ldots, d\}\},$$

Sat $L_\rho = \langle \underline{h}_1 \rangle^\perp$ y $\rho(\underline{m}) = \underline{\lambda}_1^{\underline{m}}$ (Proposición 2.2.17).

En la sección anterior vimos un método para calcular una base de Sat L_ρ. Veamos ahora cómo calcular un sistema de generadores de L_ρ, retículo asociado a la curva monomial C. Para ello necesitamos considerar el siguiente resultado técnico (en el cual, teniendo en cuenta que k es algebraicamente cerrado y de característica cero, utilizamos notación compleja):

Teorema 2.3.4 *Sea $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ no nulo y sean $\underline{\lambda}_1, \ldots, \underline{\lambda}_d \in (k^*)^n$. Definimos los subretículos de $\mathbb{Z}^n$, $\widetilde{L} = \langle \underline{h} \rangle^\perp$ y*

$$L = \{\underline{m} \in \widetilde{L} \mid \underline{\lambda}_j^{\underline{m}} = \underline{\lambda}_1^{\underline{m}},\ \forall j \in \{2, \ldots, d\}\}.$$

Consideremos un base de $\widetilde{L}$, $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$. Supongamos que $|\widetilde{L}/L| < \infty$. Con esta condición, definimos para cada $i \in \{1, \ldots, n-1\}$, $d_i = \min\{a \in \mathbb{Z}_{>0} \mid a\underline{m}_i \in L\}$. De esta forma, para cualesquiera $i \in \{1, \ldots, n-1\}$ y $j \in \{2, \ldots, d\}$ existe un único $k_i^{(j)}$, con $0 \leq k_i^{(j)} < d_i$ y tal que $\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = e^{\frac{2k_i^{(j)}\pi I}{d_i}}$.

Además, definimos $d^* = \text{m.c.m.}\{d_1, \ldots, d_{n-1}\}$ y $\widetilde{d}_i = d^*/d_i$ para todo i, y consideramos el sistema de congruencias S, dado por las ecuaciones

$$\sum_{i=1}^{n-1} k_i^{(j)} \widetilde{d}_i X_i \equiv 0 \bmod d^*, \quad 2 \leq j \leq d.$$

Entonces, si $\{\underline{f}_1, \ldots, \underline{f}_r\}$ es un sistema de generadores del conjunto de soluciones de S y $\underline{g}_i$ es el vector de coordenadas $\underline{f}_i$ en la base $\mathcal{B}$, se tiene que $\{\underline{g}_1, \ldots, \underline{g}_r\}$ es sistema de generadores de L.

Dem. Sea $i \in \{1, \dots, n-1\}$. Como $d_i \underline{m}_i \in L$, entonces para cada $j \in \{2, \dots, d\}$ se tiene que $\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i}$ es una raíz d_i-ésima de la unidad. Luego, usando notación compleja, para cada $j \in \{2, \dots, d\}$ existe un único entero $k_i^{(j)}$ con $0 \leq k_i^{(j)} < d_i$ y tal que

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = e^{\frac{2k_i^{(j)}\pi I}{d_i}}$$

(como k tiene característica cero y es algebraicamente cerrado, contiene a un subcuerpo de $\mathbb{C}$ que contiene a las raíces de la unidad, por lo tanto tiene sentido utilizar notación compleja).

Sea $\underline{m} \in \widetilde{L}$, $\underline{m} = a_1\underline{m}_1 + \ldots + a_{n-1}\underline{m}_{n-1}$. Por definición de L se tiene que $\underline{m} \in L$ si y sólo si

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}} = 1; \quad \forall j \in \{2, \dots, d\}$$

que equivale a

$$1 = \prod_{i=1}^{n-1} e^{\frac{2a_i k_i^{(j)}\pi I}{d_i}} = e^{\sum\limits_{i=1}^{n-1} \frac{2a_i k_i^{(j)}\pi I}{d_i}}; \quad \forall j \in \{2, \dots, d\},$$

que es lo mismo que

$$\sum_{i=1}^{n-1} \frac{a_i k_i^{(j)}}{d_i} \in \mathbb{Z}; \quad \forall j \in \{2, \dots, d\}.$$

Por lo tanto, $\underline{m} = a_1\underline{m}_1 + \ldots + a_{n-1}\underline{m}_{n-1} \in L$ si y sólo si para cada $j \in \{2, \dots, d\}$ se cumple

$$\sum_{i=1}^{n-1} k_i^{(j)} \widetilde{d}_i a_i \equiv 0 \bmod d^*.$$

Luego $(a_1, \dots, a_{n-1})$ son las coordenadas de un vector de L en la base $\{\underline{m}_1, \dots, \underline{m}_{n-1}\}$ si y sólo si $(a_1, \dots, a_{n-1})$ es solución del sistema de congruencias con $d-1$ ecuaciones y $n-1+d-1$ incógnitas,

$$\sum_{i=1}^{n-1} k_i^{(j)} \widetilde{d}_i X_i \equiv 0 \bmod d^*, \quad 2 \leq j \leq d,$$

de lo cual se deduce el resultado.

□

Teniendo en cuenta este resultado, podemos construir un algoritmo que nos permita calcular un sistema de generadores de L_ρ, retículo asociado a una curva monomial, en el caso de única célula coordenada.

Algoritmo 2.3.5
Input: $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\} \subset \mathbb{Z}^n, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset (k^*)^n$.
Output: $F = \emptyset$ *o* $F = \{\underline{g}_1, \ldots, \underline{g}_r\} \subset \mathbb{Z}^n$.
Paso 1: *Si existen* $i \in \{1, \ldots, n-1\}$ *y* $j \in \{2, \ldots, d\}$ *tales que* $\underline{\lambda}_j^{d\underline{m}_i} \neq \underline{\lambda}_1^{d\underline{m}_i}$, *entonces el algoritmo termina y devuelve* $F = \emptyset$. *En caso contrario, para cada* $i \in \{1, \ldots, n-1\}$ *se calcula* $d_i = \min\{a \in \mathbb{Z}_{>0} \mid \underline{\lambda}_j^{a\underline{m}_i} = \underline{\lambda}_1^{a\underline{m}_i}, \forall j \in \{2, \ldots, d\}\}$.
Paso 2: *Para cada* $i \in \{1, \ldots, n-1\}$ *y para cada* $j \in \{2, \ldots, d\}$ *se calcula un entero* $0 \leq k_i^{(j)} < d_i$ *tal que*

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = e^{\frac{2k_i^{(j)}\pi I}{d_i}}.$$

Paso 3: *Calculamos* $d^* = \text{m.c.m.}\{d_1, \ldots, d_{n-1}\}$, $\widetilde{d_i} = d^*/d_i$ *para cada* $i \in \{1, \ldots, n-1\}$, *y, por último, una matriz con coeficientes enteros y dimensión* $(n-1) \times r$, $(f_{ij})_{i,j}$, *cuyas columnas generen las soluciones del sistema de congruencias*

$$\sum_{i=1}^{n-1} k_i^{(j)} \widetilde{d}_i X_i \equiv \mod d^*, \quad 2 \leq j \leq d.$$

Paso 4: *Para cada* $i \in \{1, \ldots, r\}$ *se construye* $\underline{g}_i = \sum_{j=1}^{n-1} f_{ji}\underline{m}_j$. *El algoritmo devuelve* $F = \{\underline{g}_1, \ldots, \underline{g}_r\}$.

Teorema 2.3.6 *En las condiciones del Teorema 2.3.4, el algoritmo anterior aplicado a* $(\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$ *devuelve* $\emptyset$ *si existe* $\underline{m} \in \widetilde{L}$ *tal que* $d\underline{m} \notin L$ *y un sistema de generadores* $\{\underline{g}_1, \ldots, \underline{g}_r\}$ *de* L, *en caso contrario.*

Dem. Consecuencia del Teorema 2.3.4.

□

Teorema 2.3.7 *Sea C curva monomial y sean $C_1, \ldots, C_d$ las componentes irreducibles de C. Supongamos que $\mathcal{Z}_j = \{1, \ldots, n\}$ para todo $j \in \{1, \ldots, d\}$, y consideremos el carácter parcial $\rho : L_\rho \to k^*$ tal que $\mathcal{I}(C) = I_+(\rho)$. Entonces se cumple:*

1. *$\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$.*

Apliquemos el Algoritmo 2.3.1 a $\underline{h}_1$ y sea $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ la salida. Apliquemos 2.3.5 a $(\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$ y sea $\{\underline{g}_1, \ldots, \underline{g}_r\}$ la salida. Entonces:

2. *$\{\underline{g}_1, \ldots, \underline{g}_r\}$ es sistema de generadores del retículo L_ρ.*

3. *Si los factores invariantes de la extensión $\langle \underline{g}_1, \ldots, \underline{g}_r \rangle \subset \langle \underline{m}_1, \ldots, \underline{m}_{n-1} \rangle$ son $\widetilde{d}_1, \ldots, \widetilde{d}_{n-1}$, entonces $\prod_{i=1}^{n-1} \widetilde{d}_i = d$.*

Dem. El apartado 1 se deduce del Teorema 2.2.20. También se tiene Sat $L_\rho = \langle \underline{h}_1 \rangle^\perp = \widetilde{L}$ y $L_\rho = \{\underline{m} \in \text{Sat } L_\rho \mid (\underline{\lambda}_j)^{\underline{m}} = (\underline{\lambda}_1)^{\underline{m}}, \forall j \in \{2, \ldots, d\}\}$ $= L$ (Proposición 2.2.17). Además, $|\text{Sat } L_\rho / L_\rho| = d$, luego $d\underline{m} \in L_\rho$ para todo $\underline{m} \in \text{Sat } L_\rho$ y aplicando los Teoremas 2.3.2 y 2.3.6 se demuestra el apartado 2.

Puesto que $\{\underline{g}_1, \ldots, \underline{g}_r\}$ es sistema de generadores de L y $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ es base de $\widetilde{L}$, $\widetilde{d}_1, \ldots, \widetilde{d}_{n-1}$ son los factores invariantes de la extensión $\widetilde{L} \subseteq L$ y por tanto $\widetilde{d}_1 \cdots \widetilde{d}_{n-1} = |\widetilde{L}/L| = d$.

□

Ejemplo 2.3.8 Consideremos la curva $C = C_1 \cup C_2 \cup C_3 \cup C_4$ en $\mathbb{C}^3$, cuyas componentes vienen definidas por las parametrizaciones:

$$C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = 2t^2 \\ z = 8t^3 \end{array} \right. \quad C_2 \equiv \left\{ \begin{array}{l} x = t \\ y = 2It^2 \\ z = -8It^3 \end{array} \right. \quad C_3 \equiv \left\{ \begin{array}{l} x = t \\ y = -2t^2 \\ z = -8t^3 \end{array} \right. \quad C_4 \equiv \left\{ \begin{array}{l} x = t \\ y = -2It^2 \\ z = 8It^3 \end{array} \right. .$$

C es una curva cuyas componentes tienen asociada la célula total. Además C es monomial, como comprobaremos más adelante. Por lo tanto existe un carácter parcial ρ sobre $\mathbb{Z}^3$ tal que $\mathcal{I}(C) = I_+(\rho)$. Veamos cómo calcular un sistema de generadores del retículo L_ρ.

$\mathcal{B} = \{\underline{m}_1 = (-2, 1, 0), \underline{m}_2 = (3, -3, 1)\}$ es la base de Sat L_ρ $(= \langle (1, 2, 3) \rangle^\perp)$ calculada en el Ejemplo 2.3.3. Consideremos los vectores coeficientes de las parametrizaciones fijadas para las componentes, $\underline{\lambda}_1 = (1, 2, 8)$, $\underline{\lambda}_2 =$

$(1, 2I, -8I)$, $\underline{\lambda}_3 = (1, -2, -8)$ y $\underline{\lambda}_4 = (1, -2I, 8I)$. Para cada $i \in \{1, 2\}$ calculamos

$$d_i = \min \{a \in \mathbb{Z}_{>0} \mid (\underline{\lambda}_j)^{a\underline{m}_i} = (\underline{\lambda}_1)^{a\underline{m}_i},\ \forall j \in \{2, 3, 4\}\},$$

resultando $d_1 = 4$ y $d_2 = 1$ (en particular los vectores $4\underline{m}_1$ y $\underline{m}_2$ están en L_ρ). Como

$$\left(\frac{\underline{\lambda}_2}{\underline{\lambda}_1}\right)^{\underline{m}_1} = I \quad \left(\frac{\underline{\lambda}_3}{\underline{\lambda}_1}\right)^{\underline{m}_1} = -1 \quad \left(\frac{\underline{\lambda}_4}{\underline{\lambda}_1}\right)^{\underline{m}_1} = -I$$

y

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_2} = 1,\ \forall j \in \{2, 3, 4\}$$

entonces, con la notación del Teorema 2.3.4, $k_1^2 = 1$, $k_1^3 = 2$, $k_1^4 = 3$ y $k_2^j = 0$ para $j \in \{2, 3, 4\}$. Además, en este caso $d^* = 4$, $\widetilde{d_1} = 1$ y $\widetilde{d_2} = 4$, luego el sistema en congruencias que tenemos que resolver es:

$$\begin{aligned} 1X_1 + 0X_2 &\equiv 0 \bmod 4 \\ 2X_1 + 0X_2 &\equiv 0 \bmod 4 \\ 3X_1 + 0X_2 &\equiv 0 \bmod 4 \end{aligned}$$

cuya solución es

$$X_1 = 4\lambda,\ X_2 = \mu; \quad \lambda, \mu \in \mathbb{Z}.$$

Por lo tanto, las coordenadas en la base $\{\underline{m}_1, \underline{m}_2\}$ de un sistema de generadores para L_ρ son $(4, 0)$ y $(0, 1)$. Luego $L_\rho = \langle(-8, 4, 0), (3, -3, 1)\rangle$.

2.3.3 Determinación de curvas monomiales irreducibles iguales

Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles. Supongamos que, para todo j, la célula asociada a C_j es $\{1, \ldots, n\}$ y su vector de exponentes es $\underline{h}$. Veamos un algoritmo para obtener las componentes irreducibles de la curva C, es decir, eliminar las curvas repetidas.

Algoritmo 2.3.9
Input: $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\} \subset \mathbb{Z}^n, \mathcal{C} = \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset (k^*)^n$.
Output: $(d^*, F = \{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\})$.
Proceso: *Se definen $d^* = d$ y $F = \mathcal{C}$. Para cada $j \in \{1, \ldots, d^*\}$, si existe $k \in \{1, \ldots, d\}$ tal que $\underline{\lambda}_j^{\underline{m}_i} = \underline{\lambda}_k^{\underline{m}_i}$ para todo $i \in \{1, \ldots, n-1\}$, entonces $d^* := d - 1$, $\mathcal{C} := \{\underline{\lambda}_j \mid j \neq k\}$ y se aplica el algoritmo a $(\mathcal{B}, \mathcal{C})$. En caso contrario, el algoritmo devuelve (d^*, F) y termina.*

Teorema 2.3.10 *Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles. Supongamos que, para todo j, la célula asociada a C_j es $\{1, \ldots, n\}$ y los vectores $(\underline{h}, \underline{\lambda}_j)$ definen una parametrización monomial de C_j. Sea $\mathcal{B}$ una base de $\langle \underline{h} \rangle^\perp$. En estas condiciones, si el Algoritmo 2.3.9 aplicado a $(\mathcal{B}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$ devuelve $(d^*, F = \{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\})$ y, para cada $j \in \{1, \ldots, d^*\}$, denotamos por C_j^* a la curva monomial irreducible con parametrización dada por $(\underline{h}, \underline{\lambda}_j^*)$, entonces $C_1^*, \ldots, C_{d^*}^*$ son las componentes irreducibles de la curva C.*

Dem. Es obvio, pues sabemos que las componentes C_j y C_k son iguales si y sólo si $\underline{\lambda}_j^{\underline{m}} = \underline{\lambda}_k^{\underline{m}}$ para todo $\underline{m} \in \langle \underline{h} \rangle^\perp$ (Proposición 2.1.6).

$\square$

2.3.4 Algoritmo de caracterización de curvas monomiales en una célula

Sea C una curva unión de curvas monomiales irreducibles, todas con célula asociada $\{1, \ldots, n\}$. Estamos en condiciones de construir un algoritmo que, a partir de las parametrizaciones de las componentes de C, determine cuándo C es o no es monomial, y en caso afirmativo, calcule una base del retículo asociado a C.

Algoritmo 2.3.11
Input: $\{\underline{h}_1, \ldots, \underline{h}_d\} \subset (\mathbb{Z}_{\geq 0})^n, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset (k^*)^n$.
Output: $F = \emptyset$ *o* $F = \{\underline{v}_1, \ldots, \underline{v}_{n-1}\}$.
Paso 1: *Si existe $j \in \{2, \ldots, d\}$ tal que $\underline{h}_j \neq \underline{h}_1$, entonces el algoritmo devuelve $F = \emptyset$.*
Paso 2: *Se aplica el Algoritmo 2.3.1 a $\underline{h}_1$. Sea $\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}$ el conjunto de vectores obtenidos como salida.*
Paso 3: *Se aplica el Algoritmo 2.3.9 a $(\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$. Sea $(d^*, \{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\})$ el par obtenido como salida.*
Paso 4: *Aplicamos el Algoritmo 2.3.5 al par $(\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}, \{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\})$. Si devuelve $\emptyset$, entonces el algoritmo termina y devuelve $F = \emptyset$. En caso contrario sea $\{\underline{g}_1, \ldots, \underline{g}_r\}$ el resultado obtenido.*
Paso 5: *Calculamos el conjunto de factores invariantes de la extensión $\langle \{\underline{g}_j\}_j \rangle \subseteq \langle \{\underline{n}_i\}_i \rangle$, $\{d_1, \ldots, d_{n-1}\}$, y una base de diagonalización, $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$. Si $\prod_{i=1}^{n-1} d_i \neq d^*$, entonces el algoritmo devuelve $F = \emptyset$.*
Paso 6: *Se definen $\underline{v}_i = d_i \underline{m}_i$ para todo $i \in \{1, \ldots, n-1\}$ y el algoritmo devuelve $F = \{\underline{v}_1, \ldots, \underline{v}_{n-1}\}$.*

Teorema 2.3.12 *Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles tal que todas sus componentes tienen como célula asociada $\{1, \ldots, n\}$. Sea $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\}$ el conjunto de exponentes asociados a las parametrizaciones monomiales de sus componentes, y $\mathcal{C} = \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$ el conjunto de coeficientes. Si aplicamos el algoritmo anterior a $(\mathcal{E}, \mathcal{C})$, la salida es $\emptyset$ si y sólo si la curva C no es monomial. Además, si la salida es $\{\underline{v}_1, \ldots, \underline{v}_{n-1}\}$ entonces $\mathcal{I}(C) = I_+(\rho)$, donde $L_\rho = \langle \underline{v}_1, \ldots, \underline{v}_{n-1} \rangle$ y $\rho(\underline{m}) = (\underline{\lambda}_1)^{\underline{m}}$ para todo $\underline{m} \in L_\rho$.*

Dem. Observemos, en primer lugar, que si el Paso 5 se llega a realizar es porque $\widetilde{L}/L$ es finito, y por tanto el conjunto de factores invariantes de la extensión (incluyendo los posibles unos) tiene cardinal $n-1$.

Si C es monomial, se tiene $\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$. Sea $\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}$ el conjunto de vectores obtenido al aplicar el Algoritmo 2.3.1 a $\underline{h}_1$, que resulta una base de $\langle \underline{h}_1 \rangle^\perp$ (Teorema 2.3.2). Denotemos por $\{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\}$ el conjunto de vectores obtenido al aplicar el Algoritmo 2.3.9 a $(\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$. Por el Teorema 2.3.10, se tiene que si C_j^* es la curva monomial irreducible con parametrización dada por $(\underline{h}, \underline{\lambda}_j^*)$ entonces $C_1^*, \ldots, C_{d^*}^*$ son las componentes irreducibles de C. Como estamos en las condiciones del Teorema 2.3.7, al aplicar el Algoritmo 2.3.5 al par $(\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}, \{\underline{\lambda}_1^*, \ldots, \underline{\lambda}_{d^*}^*\})$, la salida es un sistema de generadores de L_ρ. Por lo tanto, los enteros $d_1, \ldots, d_{n-1}$ obtenidos en el Paso 5 cumplen $\prod_{i=1}^{n-1} d_i = d^*$ y la salida no es $\emptyset$.

Recíprocamente, supongamos que la salida es $\{\underline{v}_1, \ldots, \underline{v}_{n-1}\}$. Entonces $\underline{h}_j = \underline{h}_1$ para todo $j \in \{2, \ldots, d\}$. Además, por el Teorema 2.3.2, $\{\underline{n}_1, \ldots, \underline{n}_{n-1}\}$ es base de $\widetilde{L} = \langle \underline{h}_1 \rangle^\perp$ y por el Teorema 2.3.6, $\{\underline{g}_1, \ldots, \underline{g}_r\}$ es sistema de generadores del retículo $L = \{\underline{m} \in \widetilde{L} \mid (\underline{\lambda}_j^*)^{\underline{m}} = (\underline{\lambda}_1^*)^{\underline{m}}, \forall j \in \{1, \ldots, d^*\}\}$. Por lo tanto, como $\prod_{i=1}^{n-1} d_i = d^*$, se tiene que $|\widetilde{L}/L| = d$. Luego se cumplen las condiciones del Teorema 2.2.20 y C es monomial. Además, la salida del algoritmo es $\{d_1\underline{m}_1, \ldots, d_{n-1}\underline{m}_{n-1}\}$, y por tanto una base de L_ρ (Teorema 2.2.21). Si definimos $\rho(\underline{m}) = (\underline{\lambda}_1)^{\underline{m}}$ para todo $\underline{m} \in L_\rho$, entonces $\mathcal{I}(C) = I_+(\rho)$ (Proposición 2.2.17).

□

Ejemplo 2.3.13 Consideremos la curva del Ejemplo 2.3.8, $C = C_1 \cup C_2 \cup C_3 \cup C_4$ contenida en $\mathbb{C}^3$, cuyas componentes vienen definidas por las parametrizaciones:

$$C_1 \equiv \begin{cases} x = t \\ y = 2t^2 \\ z = 8t^3 \end{cases} C_2 \equiv \begin{cases} x = t \\ y = 2It^2 \\ z = -8It^3 \end{cases} C_3 \equiv \begin{cases} x = t \\ y = -2t^2 \\ z = -8t^3 \end{cases} C_4 \equiv \begin{cases} x = t \\ y = -2It^2 \\ z = 8It^3 \end{cases} .$$

Vamos a aplicar el Algoritmo 2.3.11 a los vectores $\underline{h} = (1, 2, 3)$, $\underline{\lambda}_1 = (1, 2, 8)$, $\underline{\lambda}_2 = (1, 2I, -8I)$, $\underline{\lambda}_3 = (1, -2, -8)$ y $\underline{\lambda}_4 = (1, -2I, 8I)$, para ver si la curva C es monomial. La condición del Paso 1 se cumple ya que todos los vectores exponentes de las parametrizaciones son el mismo, $\underline{h} = (1, 2, 3)$. Consideremos la base de $\widetilde{L} = \langle \underline{h} \rangle^{\perp}$, $\{\underline{n}_1 = (-2, 1, 0), \underline{n}_2 = (3, -3, 1)\}$, obtenida en el Ejemplo 2.3.3 tras aplicar el Algoritmo 2.3.1 al vector $\underline{h} = (1, 2, 3)$, y el sistema de generadores de L obtenido en el Ejemplo 2.3.8, $\{\underline{g}_1 = (-8, 4, 0), \underline{g}_2 = (3, -3, 1)\}$. Si diagonalizamos la extensión $\langle \underline{g}_1, \underline{g}_2 \rangle \subset \langle \underline{n}_1, \underline{n}_2 \rangle$, resulta que el conjunto $\{\underline{n}_1, \underline{n}_2\}$ es una base de diagonalización, siendo los factores invariantes $d_1 = 4$ y $d_2 = 1$. Puesto que $4 = d_1 \cdot d_2$, la curva C es monomial.

Además $\mathcal{I}(C) = I_+(\rho)$ donde $L_\rho = \langle (-8, 4, 0), (3, -3, 1) \rangle$ y $\rho : L_\rho \to k^*$ donde $\rho(m_1, m_2, m_3) = 1^{m_1} 2^{m_2} 8^{m_3}$ para todo $\underline{m} = (m_1, m_2, m_3) \in L_\rho$ (para definir el carácter ρ podemos tomar cualquiera de los vectores coeficientes de las componentes).

2.3.5 Algoritmo de caracterización de curvas monomiales por el origen

Consideremos ahora, una curva $C = C_1 \cup \ldots \cup C_d$ unión de curvas monomiales, con células asociadas arbitrarias, todas ellas pasando por el origen. Sean, para cada $j \in \{1, \ldots, d\}$, los vectores $(\underline{h}_j, \underline{\lambda}_j)$ que definen una parametrización monomial para C_j, y $\mathcal{Z}_j$ la célula asociada a C_j. Veamos un algoritmo para determinar si C es monomial. Obsérvese que por las condiciones impuestas, ahora todas las coordenadas de $\underline{h}_j$ son estrictamente positivas o valen ∞.

Algoritmo 2.3.14
Input: $\{\underline{h}_1, \ldots, \underline{h}_d\} \subset (\mathbb{Z}_{>0} \cup \{\infty\})^n, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset k^n$.
Output: $F = SI$ *o* $F = NO$.
Paso 0: *Para cada* $j \in \{1, \ldots, d\}$ *calculamos el conjunto* $\mathcal{Z}_j = \{i \in \{1, \ldots, n\} \mid \lambda_i \neq 0\}$. *Definimos el conjunto* $U = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$.
Paso 1: *Para todos* $j, k \in \{1, \ldots, d\}$ *distintos calculamos* $\mathcal{Z}_{jk} = \mathcal{Z}_j \cap \mathcal{Z}_k$. *Si existen* j *y* k *tales que* $\mathcal{Z}_{jk} \neq \emptyset$ *y* $\mathcal{Z}_{jk} \notin U$, *entonces el algoritmo devuelve* $F = NO$ *y termina.*

Paso 2: *Para todos* $j, k \in \{1, \ldots, d\}$ *distintos tales que* $\mathcal{Z}_j \subset \mathcal{Z}_k$*, si existen* $i_1, i_2 \in \mathcal{Z}_j$ *tales que*

$$\frac{h_{k,i_1}}{h_{j,i_1}} \neq \frac{h_{k,i_2}}{h_{j,i_2}},$$

entonces el algoritmo devuelve $F = NO$ *y termina.*
Paso 3: *Para todos* $j, k \in \{1, \ldots, d\}$ *distintos tales que* $\mathcal{Z}_j \subset \mathcal{Z}_k$*, aplicamos el Algoritmo 2.3.1 al vector* $(\underline{h}_j)_{\mathcal{Z}_j}$*. Sea* $\{\underline{m}_1, \ldots, \underline{m}_{|\mathcal{Z}_j|-1}\}$ *el conjunto de vectores obtenido. Si no existe* $l \in A_{\mathcal{Z}_j}$ *tal que* $((\underline{\lambda}_l)_{\mathcal{Z}_j})^{\underline{m}_i} = ((\underline{\lambda}_k)_{\mathcal{Z}_j})^{\underline{m}_i}$ *para todo* $i \in \{1, \ldots, |\mathcal{Z}_j| - 1\}$*, entonces el algoritmo devuelve* $F = NO$ *y termina.*
Paso 4: *Para cada* $\mathcal{Z} \in U$*, se construye* $A_{\mathcal{Z}} = \{j \in \{1, \ldots, d\} \mid \mathcal{Z}_j = \mathcal{Z}\}$ *y se aplica el Algoritmo 2.3.11 a* $(\{(\underline{h}_j)_{\mathcal{Z}} \mid j \in A_{\mathcal{Z}}\}, \{(\underline{\lambda}_j)_{\mathcal{Z}} \mid j \in A_{\mathcal{Z}}\})$*. Si para algún* $\mathcal{Z}$*, este algoritmo devuelve* $\emptyset$*, entonces* $F = NO$ *y el algoritmo termina.*
Paso 5: *El algoritmo devuelve* $F = SI$*.*

Teorema 2.3.15 *Sea* $C = C_1 \cup \ldots \cup C_d$ *una curva unión de curvas monomiales irreducibles que pasa por el origen. Consideremos para cada* $j \in \{1, \ldots, d\}$ *los vectores* $(\underline{h}_j, \underline{\lambda}_j)$ *que definen una parametrización monomial de* C_j*. Entonces el Algoritmo 2.3.14 aplicado a* $(\{\underline{h}_j\}_{j=1}^d, \{\underline{\lambda}_j\}_{j=1}^d)$ *devuelve* $F = SI$ *si y sólo si* C *es monomial.*

Dem. C es monomial si y sólo si se cumplen las condiciones D1, D2 y D3 del Teorema 2.2.23 y tras el Teorema 2.3.12, es evidente que dichas condiciones se cumplen si y sólo si la salida del algoritmo es $F = SI$.

$\square$

Nota 2.3.16 Si incluimos en la salida del Algoritmo 2.3.11 el conjunto de vectores $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ (obtenido en su desarrollo) y reordenamos adecuadamente los pasos del algoritmo anterior, entonces en el Paso 3 no es necesario aplicar el Algoritmo 2.3.1 para calcular el conjunto $\{\underline{m}_1, \ldots, \underline{m}_{|\mathcal{Z}_j|-1}\}$, pues se calcularía en el Paso 4.

Nota 2.3.17 Por otra parte, es obvio que una pequeña modificación del Algoritmo 2.3.14 nos permitiría hacer que la salida, caso de ser la curva monomial, fuese la descomposición celular $I = \cap I_{\mathcal{Z}}$ (Proposición 1.5.7).

2.3.6 Algoritmo de caracterización de curvas monomiales

Consideremos, para terminar, una curva $C = C_1 \cup \ldots \cup C_d$ unión de curvas monomiales. Sea, para cada $j \in \{1, \ldots, d\}$, $(\underline{h}_j, \underline{\lambda}_j)$ un vector que define una parametrización monomial para C_j, y sea $\mathcal{Z}_j$ la célula asociada a C_j. Veamos un algoritmo que determine cuándo C es monomial, a partir de $(\{\underline{h}_j\}_{j=1}^d, \{\underline{\lambda}_j\}_{j=1}^d)$, es decir, que compruebe cuándo se satisfacen las condiciones del Teorema 2.2.33.

Para ello veamos primero cómo determinar cuándo una unión de puntos, todos con célula asociada la total, cumple que su ideal asociado es binomial. El método es muy parecido al descrito en el Algoritmo 2.3.11.

Algoritmo 2.3.18
Input: $\mathcal{C} = \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset (k^*)^n$.
Output: $F = \emptyset$ *o* $F = \{\underline{v}_1, \ldots, \underline{v}_n\}$.
Paso 1: *Se eliminan en* $\mathcal{C}$ *los puntos repetidos.*
Paso 2: *Sea* $\{\underline{e}_1, \ldots, \underline{e}_n\}$ *la base canónica de* $\mathbb{Z}^n$. *Aplicamos el Algoritmo 2.3.5 al par* $(\{\underline{e}_1, \ldots, \underline{e}_n\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$. *Si devuelve* $\emptyset$, *entonces el algoritmo devuelve* $F = \emptyset$ *y termina. En caso contrario sea* $\{\underline{g}_1, \ldots, \underline{g}_r\}$ *el resultado obtenido.*
Paso 3: *Calculamos el conjunto de factores invariantes de la extensión* $\langle\{\underline{g}_j\}_j\rangle \subseteq \langle\{\underline{e}_i\}_i\rangle$, $\{d_1, \ldots, d_n\}$, *y una base de diagonalización,* $\{\underline{m}_1, \ldots, \underline{m}_n\}$. *Si* $\prod_{i=1}^n d_i \neq d$, *entonces el algoritmo devuelve* $F = \emptyset$.
Paso 4: *Se definen* $\underline{v}_i = d_i \underline{m}_i$ *para todo* $i \in \{1, \ldots, n\}$ *y el algoritmo devuelve* $F = \{\underline{v}_1, \ldots, \underline{v}_n\}$.

Teorema 2.3.19 *Sea* $\mathcal{V} = P_1 \cup \ldots \cup P_d$ *una unión de puntos distintos con* $P_j \in (k^*)^n$ *para todo* j. *Para cada* j, *denotemos por* $\underline{\lambda}_j$ *al vector de las coordenadas de* P_j. *Entonces el Algoritmo 2.3.18 aplicado a* $\{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$ *devuelve* $F = \emptyset$ *si y sólo si* $\mathcal{I}(\mathcal{V})$ *no es binomial. Además, si la salida es* $\{\underline{v}_1, \ldots, \underline{v}_n\}$ *entonces* $\mathcal{I}(C) = I_+(\rho)$, *donde* $L_\rho = \langle \underline{v}_1, \ldots, \underline{v}_n\rangle$ *y* $\rho(\underline{m}) = (\underline{\lambda}_1)^{\underline{m}}$ *para todo* $\underline{m} \in L_\rho$.

Dem. Teniendo en cuenta la Proposición 2.2.32, la demostración es paralela a la del Teorema 2.3.12.

□

Con el fin de comprobar la condición D0 del Teorema 2.2.33 necesitamos obtener un algoritmo que determine cuándo un punto, con todas sus coordenadas no nulas, pertenece a una curva monomial irreducible con célula asociada la célula total.

Algoritmo 2.3.20
Input: $\underline{v} \in (k^*)^n, \underline{h} \in (\mathbb{Z}_{>0})^n, \underline{\lambda} \in (k^*)^n$.
Output: $F = SI$ o $F = NO$.
Paso 0: *Aplicamos el Algoritmo 2.3.1 al vector* $\underline{h}$. *Sea* $\{\underline{m}_1, \dots, \underline{m}_{n-1}\}$ *el conjunto de vectores obtenido.*
Paso 1: *Si para todo* $i \in \{1, \dots, n-1\}$, $\underline{v}^{\underline{m}_i} = \underline{\lambda}^{\underline{m}_i}$, *entonces el algoritmo devuelve* $F = SI$. *En caso contrario, el algoritmo devuelve* $F = NO$.

Teorema 2.3.21 *Sean* C *una curva monomial irreducible con célula asociada la total y* $P \in (k^*)^n$. *Sea* $(\underline{h}, \underline{\lambda})$ *un vector de una parametrización monomial para* C *y* $\underline{v}$ *el vector de coordenadas de* P. *Entonces, el Algoritmo 2.3.20 aplicado a* $(\underline{v}, \underline{h}, \underline{\lambda})$ *devuelve* $F = SI$ *si y sólo si* $P \in C$.

Dem. Sea $\rho : L_\rho \to k^*$ dado por $\rho(\underline{m}) = \underline{\lambda}^{\underline{m}}$ donde $L_\rho = \langle \underline{h} \rangle^\perp$. Por la Proposición 2.1.6 se tiene que $\mathcal{I}(C) = I_+(\rho)$. Además sabemos que si $\{\underline{m}_1, \dots, \underline{m}_{n-1}\}$ es una base de $\langle \underline{h} \rangle^\perp$, entonces $I(\rho) = \langle X^{\underline{m}_1} - \rho(\underline{m}_1), \dots, X^{\underline{m}_{n-1}} - \rho(\underline{m}_{n-1})\rangle$, luego el resultado se deduce de que $\mathcal{V}(I_+(\rho)) \cap (k^*)^n = \mathcal{V}(I(\rho))$.

$\square$

Utilizando todos los algoritmos que hemos definido se puede construir:

Algoritmo 2.3.22 (Caracterización de curvas monomiales)
Input: $\{\underline{h}_1, \dots, \underline{h}_d\} \subset (\mathbb{Z}_{\geq 0} \cup \{\infty\})^n, \{\underline{\lambda}_1, \dots, \underline{\lambda}_d\} \subset k^n$.
Output: $F = SI$ o $F = NO$.
Paso 0: *Calculamos, para cada* $j \in \{1, \dots, d\}$, $\mathcal{Z}_j = \{i \in \{1, \dots, n\} \mid \lambda_i \neq 0\}$, $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_{ji} = 0\}$, *y* $\Lambda = \{j \in \{1, \dots, d\} \mid \exists k \in \{1, \dots, d\}$ *con* $\widetilde{\mathcal{Z}}_j = \mathcal{Z}_k\}$. *Sean* $U_1 = \{\mathcal{Z}_1, \dots, \mathcal{Z}_d\}$, $U_2 = \{\widetilde{\mathcal{Z}}_j \mid j \notin \Lambda\}$ *y* $U = U_1 \cup U_2$. *Se reordenan* $\mathcal{Z}_1, \dots, \mathcal{Z}_d$ *para que* $U_2 = \{\widetilde{\mathcal{Z}}_1, \dots, \widetilde{\mathcal{Z}}_s\}$. *Para cada* $\mathcal{Z} \in U_1$, *se define* $A_{\mathcal{Z}} = \{j \in \{1, \dots, d\} \mid \mathcal{Z}_j = \mathcal{Z}\}$. *Para cada* $\mathcal{Z} \in U_2$, *definimos* $A_{\mathcal{Z}} = \{j \in \{1, \dots, s\} \mid \widetilde{\mathcal{Z}}_j = \mathcal{Z}\}$.
Paso 1: *Denotemos, para cada* $j \in \{1, \dots, d\}$, $\mathcal{Z}_j^* = \mathcal{Z}_j$ *y para cada* $j \in \{d+1, \dots, d+s\}$, $\mathcal{Z}_j^* = \widetilde{\mathcal{Z}}_{j-d}$. *Entonces, si existen* $j, k \in \{1, \dots, d+s\}$ *distintos tales que* $\mathcal{Z}_j^* \cap \mathcal{Z}_k^* \notin U$, *el algoritmo devuelve* $F = NO$ *y termina.*
Paso 2: *Para todos* $j \in \{1, \dots, s\}$ *y* $k \in \{1, \dots, d\}$ *tales que* $\widetilde{\mathcal{Z}}_j \subset \mathcal{Z}_k$, *si* $\widetilde{\mathcal{Z}}_j \not\subseteq \widetilde{\mathcal{Z}}_k$ *entonces el algoritmo devuelve* $F = NO$ *y termina.*
Paso 3: *Para todos* $j, k \in \{1, \dots, s\}$ *tales que* $\widetilde{\mathcal{Z}}_j \subset \widetilde{\mathcal{Z}}_k$, *si no existe* $l \in A_{\widetilde{\mathcal{Z}}_j}$ *tal que* $(\underline{\lambda}_l)_{\widetilde{\mathcal{Z}}_j} = (\underline{\lambda}_k)_{\widetilde{\mathcal{Z}}_j}$ *entonces el algoritmo devuelve* $F = NO$ *y termina.*
Paso 4: *Para todos* $j, k \in \{1, \dots, d\}$ *tales que* $\mathcal{Z}_j \subset \mathcal{Z}_k$ *y* $\mathcal{Z}_j \not\subseteq \widetilde{\mathcal{Z}}_k$, *si existe*

$i \in \mathcal{Z}_j$ tal que $h_{ji} \neq 0$ y $h_{ki} = 0$ entonces el algoritmo devuelve $F = NO$ y termina. En caso contrario, si existen $i_1, i_2 \in \mathcal{Z}_j \setminus \widetilde{\mathcal{Z}}_j$ tales que $\frac{h_{k,i_1}}{h_{j,i_1}} \neq \frac{h_{k,i_2}}{h_{j,i_2}}$ entonces el algoritmo devuelve $F = NO$ y termina.

Paso 5: *Para todos $j, k \in \{1, \dots, d\}$ tales que $\mathcal{Z}_j \subset \mathcal{Z}_k$ y $\mathcal{Z}_j \not\subseteq \widetilde{\mathcal{Z}}_k$, si no existe $l \in A_{\mathcal{Z}_j}$ tal que 2.3.20 aplicado a $(\underline{\lambda}_k)_{\mathcal{Z}_j}, (\underline{h}_j)_{\mathcal{Z}_j}, (\underline{\lambda}_l)_{\mathcal{Z}_j}$ devuelve SI, entonces el algoritmo termina y devuelve $F = NO$.*

Paso 6: *Para todos $j \in \{1, \dots, d\}, k \in \{1, \dots, s\}$ tales que $\mathcal{Z}_j \subset \widetilde{\mathcal{Z}}_k$, si no existe $l \in A_{\mathcal{Z}_j}$ tal que 2.3.20 aplicado a $(\underline{\lambda}_k)_{\mathcal{Z}_j}, (\underline{h}_j)_{\mathcal{Z}_j}, (\underline{\lambda}_l)_{\mathcal{Z}_j}$ devuelve SI, entonces el algoritmo termina y devuelve $F = NO$.*

Paso 7: *Para todo $j \in \Lambda$, si no existe $k \in \{1, \dots, d\}$ tal que $\mathcal{Z}_k = \widetilde{\mathcal{Z}}_j$ y el Algoritmo 2.3.20 aplicado a $((\underline{\lambda}_j)_{\mathcal{Z}_k}, (\underline{h}_k)_{\mathcal{Z}_k}, (\underline{\lambda}_k)_{\mathcal{Z}_k})$ devuelve SI, entonces el algoritmo devuelve $F = NO$ y termina.*

Paso 8: *Si existe $\mathcal{Z} \in U_1$ tal que el Algoritmo 2.3.11 aplicado a $(\{(\underline{h}_j)_{\mathcal{Z}} \mid j \in A_{\mathcal{Z}}\}, \{(\underline{\lambda}_j)_{\mathcal{Z}} \mid j \in A_{\mathcal{Z}}\})$ devuelve $\emptyset$, entonces el algoritmo devuelve $F = NO$ y termina.*

Paso 9: *Si existe $\mathcal{Z} \in U_2$ tal que el Algoritmo 2.3.18 aplicado al conjunto $\mathcal{C} = \{(\underline{\lambda}_j)_{\mathcal{Z}} \mid j \in A_{\mathcal{Z}}\})$ devuelve $\emptyset$, entonces el algoritmo devuelve $F = NO$ y termina.*

Paso 10: *El algoritmo devuelve $F = SI$.*

Teorema 2.3.23 *Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de curvas monomiales irreducibles. Consideremos, para cada $j \in \{1, \dots, d\}$, los vectores $(\underline{h}_j, \underline{\lambda}_j)$ que definen una parametrización monomial de C_j. Entonces el Algoritmo 2.3.22 aplicado a $(\{\underline{h}_j\}_{j=1}^d, \{\underline{\lambda}_j\}_{j=1}^d)$ devuelve $F = SI$ si y sólo si C es monomial.*

Dem. C es monomial si y sólo si se cumplen las condiciones D0, D1, D2 y D3 del Teorema 2.2.33, y tras los Teoremas 2.3.12, 2.3.19 y 2.3.21, es evidente que dichas condiciones se cumplen si y sólo si la salida del algoritmo es $F = SI$ (el paso 7 controla D0, los pasos 8 y 9 controlan D1, el 1 controla D2 y 6,4,5,3 y 2 controlan D3).

$\square$

Nota 2.3.24 Una pequeña modificación del Algoritmo 2.3.22, nos permite hacer que la salida, caso de ser la curva monomial, fuese la descomposición celular $I = \cap I_{\mathcal{Z}}$ de I (Proposición 1.5.7).

2.4 Apéndice: Curvas monomiales en una célula

En esta sección vamos a profundizar, basándonos en el Teorema 2.2.21, en el estudio de las curvas monomiales en una célula. Veremos cuántas hay y cómo se pueden construir.

Sea $C = C_1 \cup \ldots \cup C_d$ una curva monomial en una célula, es decir, para todo j, $\mathcal{Z}_j = \{1, \ldots, n\}$ e $\mathcal{I}(C) = I_+(\rho)$. Sean $d_1, \ldots, d_{n-1}$ los factores invariantes de la extensión $L_\rho \subseteq \text{Sat } L_\rho$.

Recordemos que el Teorema 2.2.21 asegura que si $\mathcal{B} := \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ es una base de diagonalización de la extensión (es decir, una base de Sat L_ρ tal que $\{d_1\underline{m}_1, \ldots, d_{n-1}\underline{m}_{n-1}\}$ es base de L_ρ) y si $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$ es un conjunto de raíces de la unidad, donde ξ_i es un raíz primitiva d_i-ésima de la unidad, entonces la aplicación

$$\begin{array}{rcl} \beta : \{1, \ldots, d\} & \longrightarrow & \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1}) \\ j & \longmapsto & (j_1, \ldots, j_{n-1}) \ , \end{array}$$

siendo

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = \xi_i^{j_i}; \qquad \begin{array}{l} \forall i \in \{1, \ldots, n-1\} \\ \forall j \in \{1, \ldots, d\} \end{array} \ ,$$

es una biyección.

La biyección β lo que hace, esencialmente, es reordenar las componentes $C_1, \ldots, C_d$ para tener información directa sobre sus coeficientes. Así, si denotamos por $C_{j_1,\ldots,j_{n-1}}$ a la componente $C_{\beta^{-1}(j_1,\ldots,j_{n-1})}$ y por $\underline{\lambda}_{j_1,\ldots,j_{n-1}}$ a su vector de coeficientes, entonces,

$$\left(\frac{\underline{\lambda}_{j_1,\ldots,j_{n-1}}}{\underline{\lambda}_{0,\ldots,0}}\right)^{\underline{m}_i} = \xi_i^{j_i}; \qquad \begin{array}{l} \forall i \in \{1, \ldots, n-1\} \\ \forall (j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1}) \end{array} .$$

Obviamente, β, y por tanto la ordenación de $C_1, \ldots, C_d$, dependen de la elección de las raíces de la unidad, y de la base $\mathcal{B}$. También de la elección de una componente "origen", pues hemos elegido β con $\beta(1) = (0, \ldots, 0)$ de forma arbitraria, y de la misma forma se podría construir β con la condición

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_k}\right)^{\underline{m}_i} = \xi_i^{j_i},$$

donde k es cualquier índice previamente fijado. De esta forma, la componente $C_{0,\ldots,0}$ sería C_k.

Veamos en primer lugar, cómo varía β al variar el origen, las raíces de la unidad y la base elegida.

Proposición 2.4.1 *Fijemos el conjunto* $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$*, donde* ξ_i *es una raíz primitiva* d_i*-ésima de la unidad, y una base de diagonalización de la extensión* $L_\rho \subseteq \mathrm{Sat}\ L_\rho$*,* $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$*. Denotemos por* $\{C_{j_1,\ldots,j_{n-1}}\}$ *a la ordenación de las componentes que se obtiene usando como origen* C_1*, y por* $\{\widetilde{C}_{j_1,\ldots,j_{n-1}}\}$ *la que se se obtiene usando como origen* C_k*. En esta situación, si* $C_{0,\ldots,0} = \widetilde{C}_{k_1,\ldots,k_{n-1}}$ *entonces* $C_{j_1,\ldots,j_{n-1}} = \widetilde{C}_{j_1+k_1,\ldots,j_{n-1}+k_{n-1}}$ *para todo* $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$*.*

Dem. Si $C_{0,\ldots,0} = \widetilde{C}_{k_1,\ldots,k_{n-1}}$ se cumple

$$\left(\frac{\underline{\lambda}_1}{\underline{\lambda}_k}\right)^{\underline{m}_i} = \xi_i^{k_i},\ \forall i \in \{1, \ldots, n-1\}.$$

Sea $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$ y supongamos $C_j = C_{j_1,\ldots,j_{n-1}}$. Entonces,

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_k}\right)^{\underline{m}_i} = \frac{\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i}}{\left(\frac{\underline{\lambda}_k}{\underline{\lambda}_1}\right)^{\underline{m}_i}} = \xi_i^{j_i+k_i}; \quad \forall i \in \{1, \ldots, n-1\},$$

luego $C_{j_1,\ldots,j_{n-1}} = \widetilde{C}_{j_1+k_1,\ldots,j_{n-1}+k_{n-1}}$.

□

A partir de ahora, fijaremos como origen la componente C_1.

Proposición 2.4.2 *Consideremos una base de diagonalización de la extensión* $L_\rho \subseteq \mathrm{Sat}\ L_\rho$*,* $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$*. Denotemos por* $\{C_{j_1,\ldots,j_{n-1}}\}$ *a la ordenación de las componentes que se obtiene usando como raíces de la unidad* $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$*, y por* $\{\widetilde{C}_{j_1,\ldots,j_{n-1}}\}$ *a la que se se obtiene usando como raíces de la unidad* $\widetilde{\Lambda} = \{\widetilde{\xi}_1, \ldots, \widetilde{\xi}_{n-1}\}$*. En esta situación, si* $\widetilde{\xi}_i = \xi_i^{r_i}$ *para cada* $1 \leq i \leq n-1$*, entonces* $C_{j_1,\ldots,,j_{n-1}} = \widetilde{C}_{r_1 j_1,\ldots,r_{n-1}j_{n-1}}$ *para todo* $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$*.*

Dem. Dado $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$, sea j tal que $C_j = C_{j_1,\ldots,j_{n-1}}$. Como para cada $i \in \{1, \ldots, n-1\}$, $\widetilde{\xi}_i = \xi_i^{\widetilde{r}_i}$ (con m.c.d.$(\widetilde{r}_i, d_i) = 1$), entonces

$$\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = \xi_i^{\widetilde{j}_i} = \widetilde{\xi}_i^{r_i \widetilde{j}_i},$$

y $C_{j_1,\ldots,,j_{n-1}} = \widetilde{C}_{r_1 j_1,\ldots,r_{n-1}j_{n-1}}$.

$\square$

Sea ξ una raíz primitiva d_{n-1}-ésima de la unidad, y para cada $1 \leq i \leq n-1$ definamos $\xi_i = \xi^{\frac{d_{n-1}}{d_i}}$. Entonces, ξ_i es una raíz primitiva d_i-ésima de la unidad y si $i \leq h$

$$\xi_h^{\frac{d_h}{d_i}} = \xi^{\frac{d_{n-1}}{d_h}\frac{d_h}{d_i}} = \xi_i.$$

Definamos $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$.

Proposición 2.4.3 *Consideremos el conjunto de raíces de la unidad* $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$ *que acabamos de definir. Denotemos por* $\{C_{j_1,\ldots,j_{n-1}}\}$ *a la ordenación de las componentes que se obtiene usando la base de diagonalización* $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$*, y por* $\{\widetilde{C}_{j_1,\ldots,j_{n-1}}\}$ *la que se se obtiene según la base de diagonalización* $\widetilde{\mathcal{B}} = \{\underline{n}_1, \ldots, \underline{n}_{n-1}\}$*. Escribamos, para cada* $1 \leq i \leq n-1$*,* $d_i\underline{m}_i = \sum_{h=1}^{n-1} b_{ih} d_h \underline{n}_h$*, y consideremos la matriz* $B := (b_{ih})_{i,h}$*. Si para* $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$*, se tiene* $C_{j_1,\ldots,j_{n-1}} = \widetilde{C}_{\widetilde{j}_1,\ldots,\widetilde{j}_{n-1}}$*, entonces* $(\widetilde{j}_1, \ldots, \widetilde{j}_{n-1}) = (j_1, \ldots, j_{n-1})B^{-1}$.

Dem. Como $\mathcal{B}$ y $\widetilde{\mathcal{B}}$ son bases del mismo retículo, Sat L_ρ, entonces, para todo i, $\underline{m}_i = \sum_{h=1}^{n-1} a_{ih}\underline{n}_h$. Pero como $d_i\underline{m}_i = \sum_{h=1}^{n-1} b_{ih}d_h\underline{n}_h$, se tiene $d_i a_{ih} = b_{ih} d_h$, y, si $i \geq h$ entonces $d_i / b_{ih} d_h$.

Teniendo en cuenta estas consideraciones se tiene,

$$\xi_h^{a_{ih}} = \begin{cases} \left(\xi_h^{\frac{d_h}{d_i}}\right)^{b_{ih}} = \xi_i^{b_{ih}} & \text{si } i \leq h \\ \xi_h^{\frac{b_{ih}d_h}{d_i}} = \left(\xi_i^{\frac{d_i}{d_h}}\right)^{\frac{b_{ih}d_h}{d_i}} = \xi_i^{b_{ih}} & \text{si } i \geq h \end{cases}.$$

Sea $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$ y sea j con $C_j = C_{j_1,\ldots,j_{n-1}} = \widetilde{C}_{\widetilde{j}_1,\ldots,\widetilde{j}_{n-1}}$. Como

$$\xi_i^{j_i} = \left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{\underline{m}_i} = \prod_{h=1}^{n-1}\left(\frac{\underline{\lambda}_j}{\underline{\lambda}_1}\right)^{a_{ih}\underline{n}_h} = \prod_{h=1}^{n-1}\xi_h^{\widetilde{j}_h a_{ih}} = \prod_{h=1}^{n-1}\xi_i^{b_{ih}\widetilde{j}_h} = \xi_i^{\sum_{h=1}^{n-1} b_{ih}\widetilde{j}_h},$$

entonces $(\widetilde{j}_1, \ldots, \widetilde{j}_{n-1}) = (j_1, \ldots, j_{n-1})B^{-1}$.

□

Nos planteamos ahora el problema de la construcción de curvas con ideal asociado de la forma $I_+(\rho)$ tales que d sea el número de componentes, n el número de coordenadas, $\underline{h}$ el vector de exponentes. Fijemos una componente, que denotaremos por C_1, parametrizable por $(\underline{\lambda}, \underline{h})$. En este sentido contestaremos a las preguntas: ¿existen curvas con estas condiciones? De ser así, ¿cuántas hay?, ¿cómo construirlas?

Proposición 2.4.4 *Sean C y $\widetilde{C}$ dos curvas monomiales en $\mathcal{A}^n(k)$ con d componentes irreducibles, todas ellas con vector de exponentes asociado, $\underline{h}$. Sean L_ρ y $\widetilde{L}_\rho$ los retículos asociados a C y a $\widetilde{C}$ respectivamente (Definición 2.2.18). Si los factores invariantes de las extensiones $L_\rho \subset \langle \underline{h} \rangle^\perp$ y $\widetilde{L}_\rho \subset \langle \underline{h} \rangle^\perp$ son distintos entonces $C \neq \widetilde{C}$.*

Dem. Obvio pues si $C = \widetilde{C}$, entonces $L_\rho = \widetilde{L}_\rho$ (pues los retículos sólo dependen de la curva), luego las extensiones son la misma.

□

Así pues, fijaremos también la factorización $d = d_1 \cdots d_{n-1}$ con $d_1 / \ldots / d_{n-1}$.

Proposición 2.4.5 *Sean $n \geq 1$, $d \in (\mathbb{Z}_{>0})^n$, $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$, $\underline{\lambda} \in (k^*)^n$, y $d = d_1 \cdots d_{n-1}$ con $d_1 / \ldots / d_{n-1}$. Entonces existe una curva monomial C en $\mathcal{A}^n(k)$ con d componentes irreducibles, una de las cuales es C_1, cuyo ideal asociado es de la forma $I_+(\rho)$, con* Sat $L_\rho = \langle \underline{h} \rangle^\perp$ *y los factores invariantes $d_1, \ldots, d_{n-1}$.*

Dem. Sea $\mathcal{B} = \{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ una base de $\langle \underline{h} \rangle^\perp$ y sea L_ρ el retículo generado por $\{d_1 \underline{m}_1, \ldots, d_{n-1} \underline{m}_{n-1}\}$. Elijamos un conjunto de raíces primitivas de la unidad, $\Lambda = \{\xi_1, \ldots, \xi_{n-1}\}$. Entonces, para todo $(j_1, \ldots, j_{n-1}) \in \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$, por el teorema de los ceros de Hilbert, podemos elegir $\underline{\lambda}_{j_1, \ldots, j_{n-1}} \in (k^*)^n$ tal que

$$\left(\frac{\underline{\lambda}_{j_1, \ldots, j_{n-1}}}{\underline{\lambda}} \right)^{\underline{m}_i} = \xi_i^{j_i}, \ \forall i \in \{1, \ldots, n-1\} \ .$$

Denotemos por $C_{j_1, \ldots, j_{n-1}}$ la curva monomial irreducible con parametrización dada por los vectores $(\underline{h}, \underline{\lambda}_{j_1, \ldots, j_{n-1}})$ y consideremos la curva $C = \cup C_{j_1, \ldots, j_{n-1}}$. Por el Teorema 2.2.21, C es una curva monomial en una célula, con retículo asociado L_ρ. Además, su componente $C_{0,\dots,0}$ es C_1 y $\mathcal{B}$ es base de diagonalización de la extensión $L_\rho \subseteq \text{Sat } L_\rho = \langle \underline{h} \rangle^\perp$.

$\square$

Nota 2.4.6 En la construcción anterior, la curva $C_{j_1,\dots,j_{n-1}}$ no depende de la elección de $\underline{\lambda}_{j_1,\dots,j_{n-1}}$, pues de la condición

$$\left(\frac{\underline{\lambda}_{j_1,\dots,j_{n-1}}}{\underline{\lambda}}\right)^{\underline{m}_i} = \xi_i^{j_i}, \ \forall i \in \{1,\dots,n-1\}$$

se determina de forma única $\rho_{j_1,\dots,j_{n-1}}$ (por $\rho_{j_1,\dots,j_{n-1}}(\underline{m}) = \underline{\lambda}_{j_1,\dots,j_{n-1}}{}^{\underline{m}}$) y por tanto $I_+(\rho_{j_1,\dots,j_{n-1}})$.

De hecho, podemos dar un algoritmo para el cálculo de $\underline{\lambda}_{j_1,\dots,j_{n-1}}$ para cada $(j_1,\dots,j_{n-1}) \in \mathbb{Z}/(d_1) \times \dots \times \mathbb{Z}/(d_{n-1})$, y, como consecuencia, otro para la construcción de la curva calculada en la Proposición 2.4.5.

Algoritmo 2.4.7
Input: $\{\underline{m}_1,\dots,\underline{m}_r\}, \{\gamma_1,\dots,\gamma_r\} \subset k^*$, *donde* S *es un conjunto libre de* $\mathbb{Z}^n$.
Output: $F = \{\underline{\lambda}\} \subset (k^*)^n$.
Paso 1: *Ampliamos el conjunto* S *hasta obtener una base de* $\mathbb{Z}^n$, $\{\underline{m}_1,\dots,\underline{m}_n\}$.
Paso 2: *Construimos la matriz* M *cuyas columnas son los vectores* $\{\underline{m}_1,\dots,\underline{m}_n\}$ *y sea*

$$A = M^{-1} = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix}.$$

Paso 3: *Para cada* $i \in \{1,\dots,n\}$ *construimos* $\lambda_i := \prod_{j=1}^{r} \gamma_j^{a_{ji}}$. *El algoritmo devuelve* $F = \underline{\lambda}$ *donde* $\underline{\lambda} = (\lambda_1,\dots,\lambda_n)$.

Teorema 2.4.8 *Sean* $S = \{\underline{m}_1,\dots,\underline{m}_r\}$ *un conjunto libre de vectores de* $\mathbb{Z}^n$ *y* $T = \{\gamma_1,\dots,\gamma_r\} \subseteq k^*$. *Consideremos el retículo* $L_\rho = \langle\{\underline{m}_1,\dots,\underline{m}_r\}\rangle \subseteq \mathbb{Z}^n$ *y el carácter* $\rho : L_\rho \to k^*$ *dado por* $\rho(\underline{m}_i) = \gamma_i$ *para todo* i. *Entonces el Algoritmo 2.4.7 aplicado a* (S,T) *devuelve un vector* $\underline{\lambda} \in \mathcal{V}(I(\rho))$.

Dem. Consideremos el vector $\underline{\lambda}$ obtenido en el Algoritmo 2.4.7. Para todo $j \in \{1,\dots,n-1\}$ se tiene

$$\underline{\lambda}^{\underline{m}_j} = \prod_{i=1}^{n}\left(\prod_{k=1}^{r}\gamma_k^{a_{ki}}\right)^{m_{ji}} = \prod_{k=1}^{r}\gamma_k^{\sum_{i=1}^{n} a_{ki}m_{ji}}.$$

Teniendo en cuenta que M es la matriz que tiene por columnas los vectores $\{\underline{m}_1, \ldots, \underline{m}_n\}$, y $M = A^{-1}$ se obtiene $\lambda^{\underline{m}_j} = \gamma_j$.

$\square$

Algoritmo 2.4.9
Input: *$\underline{h} \in (\mathbb{Z}_{\geq 0})^n$, $\underline{\lambda}_1 \in (k^*)^n$ y $d \in \mathbb{Z}_{>0}$*
Output: *$F = \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$, donde $\underline{\lambda}_j \in (k^*)^n$*
Paso 1: *Aplicamos el Algoritmo 2.3.1 al vector $\underline{h}$. Sea $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ el conjunto de vectores obtenido.*
Paso 2: *Elegimos enteros $d_1, \ldots, d_{n-1}$ tales que $d = d_1 \cdots d_{n-1}$ y un vector $\underline{\lambda}_1 \in (k^*)^n$.*
Paso 3: *Para cada $i \in \{1, \ldots, n-1\}$ escogemos una raíz primitiva d_i-ésima de la unidad, ξ_i. Fijamos una biyección $\beta : \{1, \ldots, d\} \to \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_{n-1})$ tal que $\beta(1) = (0, \ldots, 0)$. Denotemos $\beta(j) = (j_1, \ldots, j_{n-1})$, para todo $j \in \{1, \ldots, d\}$.*
Paso 4: *Para cada $j \in \{2, \ldots, d\}$:*

(a) *Se construye, para cada $i \in \{1, \ldots, n-1\}$, $\gamma_i = \xi_i^{j_i} \underline{\lambda}_1^{\underline{m}_i}$.*

(b) *Aplicamos el Algoritmo 2.4.7 al par $(\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}, \{\gamma_1, \ldots, \gamma_{n-1}\})$. Sea $\underline{\lambda}_j$ el vector obtenido.*

Paso 5: *El algoritmo devuelve $F = \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$ y termina.*

Teorema 2.4.10 *Sean $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ no nulo, $\underline{\lambda}_1 \in (k^*)^n$, $d \in \mathbb{Z}_{>0}$ y $\{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$ el conjunto de vectores obtenido al aplicar el Algoritmo 2.4.9 a $(\underline{h}, \underline{\lambda}_1, d)$. Consideremos, para cada $j \in \{1, \ldots, d\}$, la curva monomial irreducible C_j con parametrización dada por el par de vectores $(\underline{h}, \underline{\lambda}_j)$. Entonces la curva $C := C_1 \cup \ldots \cup C_d$ es monomial.*

Dem. Sea $\{\underline{m}_1, \ldots, \underline{m}_{n-1}\}$ el conjunto de vectores obtenido al aplicar el Algoritmo 2.3.1 al vector $\underline{h}$ y consideremos el conjunto $\{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\}$ como en el enunciado. Entonces, si $d = d_1 \cdots d_{n-1}$ es la factorización utilizada en el Algoritmo 2.4.9 aplicado a $(\underline{h}, \underline{\lambda}_1, d)$, se tiene que, para todo $i \in \{1, \ldots, n-1\}$,

$$(\underline{\lambda}_j)^{d_i \underline{m}_i} = (\underline{\lambda}_1)^{d_i \underline{m}_i}, \ \forall j \in \{2, \ldots, d\}.$$

Por lo tanto, la curva C, definida en el enunciado, cumple las condiciones del Teorema 2.2.21, luego es monomial.

$\square$

Ejemplo 2.4.11 Supongamos que queremos construir una curva monomial con 8 componentes, en un espacio de dimensión 3, y con vector de exponentes $\underline{h} = (1, 2, 3)$. Siguiendo los pasos del Algoritmo 2.4.9, escogemos una factorización $8 = 2 \cdot 4$ y un vector $\underline{\lambda}_1 = (1, 1, 1) \in (k^*)^3$. Utilizando el Algoritmo 2.3.1, calculamos una base de $\langle \underline{h} \rangle^\perp$, $\{\underline{m}_1 = (-2, 1, 0\}, \underline{m}_2 = (3, -3, 1)\}$, y utilizando el algoritmo de Euclides calculamos $\underline{m}_3 = (2, -2, 1)$ que cumple $\underline{m}_3\, \underline{h} = 1$, entonces $\{\underline{m}_1, \underline{m}_2, \underline{m}_3\}$ es base de $\mathbb{Z}^3$. Como en el Algoritmo 2.4.7, construimos

$$M = \begin{pmatrix} -2 & 3 & 2 \\ 1 & -3 & -2 \\ 0 & 1 & 1 \end{pmatrix}$$

y calculamos

$$A = M^{-1} = \begin{pmatrix} -1 & -1 & 0 \\ -1 & -2 & -2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Fijamos $\xi_1 = -1$ y $\xi_2 = I$ y consideramos la biyección,

$$\begin{array}{rcl} \beta : \{1, \dots, 8\} & \longrightarrow & \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \\ j & \longmapsto & (j_1, j_2) \end{array}$$

donde j_1 y j_2 son el cociente y el resto de la división de $j - 1$ por 4. La biyección β cumple $\beta(1) = (0, \dots, 0)$.

Para cada $j \in \{2, \dots, n\}$ calculamos $\gamma_1 = \xi_1^{j_1}$, $\gamma_2 = \xi_2^{j_2}$ y $\underline{\lambda}_j = (\gamma_1^{a_{11}}\gamma_2^{a_{21}}, \gamma_1^{a_{12}}\gamma_2^{a_{22}}, \gamma_1^{a_{13}}\gamma_2^{a_{23}})$. Así obtenemos:

$$\begin{array}{lll} \underline{\lambda}_2 = (-I, -1, -1) & & \\ \underline{\lambda}_3 = (-1, 1, 1) & \underline{\lambda}_5 = (-1, -1, 1) & \underline{\lambda}_7 = (1, -1, 1) \\ & \underline{\lambda}_6 = (-I, 1, -1) & \underline{\lambda}_8 = (I, 1, -1) \\ \underline{\lambda}_4 = (I, -1, -1) & & \end{array}.$$

Por lo tanto, si consideramos la curva $C = C_1 \cup \ldots \cup C_8$ donde

$$C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = t^2 \\ z = t^3 \end{array} \right. C_2 \equiv \left\{ \begin{array}{l} x = -It \\ y = -1t^2 \\ z = -1t^3 \end{array} \right. C_3 \equiv \left\{ \begin{array}{l} x = -1t \\ y = t^2 \\ z = t^3 \end{array} \right. C_4 \equiv \left\{ \begin{array}{l} x = It \\ y = -1t^2 \\ z = -1t^3 \end{array} \right.$$

$$C_5 \equiv \left\{ \begin{array}{l} x = -1t \\ y = -1t^2 \\ z = t^3 \end{array} \right. C_6 \equiv \left\{ \begin{array}{l} x = -It \\ y = t^2 \\ z = -1t^3 \end{array} \right. C_7 \equiv \left\{ \begin{array}{l} x = t \\ y = -1t^2 \\ z = t^3 \end{array} \right. C_8 \equiv \left\{ \begin{array}{l} x = It \\ y = t^2 \\ z = -1t^3 \end{array} \right.$$

resulta que C es monomial (Teorema 2.4.10). Además $\mathcal{I}(C) = I_+(\rho)$ donde $L_\rho = \langle (-4, 2, 0), (12, -12, 1) \rangle$ (Teorema 2.2.21) y $\rho(\underline{m}) = 1$ para todo $\underline{m} \in L_\rho$ (Proposición 2.2.17).

Volvamos a la cuestión de cuántas curvas diferentes se construyen por el proceso anterior. La construcción de la Proposición 2.4.5 depende de la elección de un conjunto de raíces de la unidad, Λ, y de una base de diagonalización, $\mathcal{B}$. Veamos qué ocurre cuando cambiamos $\mathcal{B}$ y Λ.

Proposición 2.4.12 *Consideremos dos conjuntos de raíces de la unidad $\Lambda = \{\xi_1, \dots, \xi_{n-1}\}$ y $\widetilde{\Lambda} = \{\widetilde{\xi}_1, \dots, \widetilde{\xi}_{n-1}\}$, y una base de $\langle \underline{h} \rangle^\perp$, $\mathcal{B} = \{\underline{m}_1, \dots, \underline{m}_{n-1}\}$. Entonces las curvas monomiales obtenidas en la Proposición 2.4.5 para $\Lambda, \mathcal{B}$ y para $\widetilde{\Lambda}, \mathcal{B}$ son la misma.*

Dem. Para cada $i \in \{1, \dots, n-1\}$ existe r_i con $0 \leq r_i \leq d_i - 1$ tal que $\widetilde{\xi}_i = \xi_i^{r_i}$. Por lo tanto, para todo $(j_1, \dots, j_{n-1})$, si denotamos por $C_{j_1,\dots,j_{n-1}}$ la componente obtenida para $\Lambda, \mathcal{B}$, y por $\widetilde{C}_{j_1,\dots,j_{n-1}}$ la componente obtenida para $\widetilde{\Lambda}, \mathcal{B}$, entonces

$$\left(\frac{\widetilde{\underline{\lambda}}_{j_1,\dots,j_{n-1}}}{\underline{\lambda}} \right)^{\underline{m}_i} = \widetilde{\xi}_i^{j_i} = \xi_i^{r_i j_i},$$

luego $\widetilde{C}_{j_1,\dots,j_{n-1}} = C_{r_1 j_1,\dots,r_{n-1}j_{n-1}}$ de donde se deduce el resultado.

□

Proposición 2.4.13 *Consideremos dos bases de $\langle \underline{h} \rangle^\perp$, $\mathcal{B} = \{\underline{m}_1, \dots, \underline{m}_{n-1}\}$ y $\widetilde{\mathcal{B}} = \{\underline{n}_1, \dots, \underline{n}_{n-1}\}$. Sea $(a_{ij})_{ij}$ la matriz de cambio de base de $\mathcal{B}$ a $\widetilde{\mathcal{B}}$. Entonces las curvas monomiales obtenidas en la Proposición 2.4.5 para $\mathcal{B}$ y para $\widetilde{\mathcal{B}}$ son la misma si y sólo si $d_j / d_i a_{ij}$ para todo i, j.*

Dem. Sea L_1 el subretículo de $\langle \underline{h} \rangle^\perp$ generado por $\{d_1 \underline{m}_1, \dots, d_{n-1}\underline{m}_{n-1}\}$ y sea L_2 el generado por $\{d_1 \underline{n}_1, \dots, d_{n-1}\underline{n}_{n-1}\}$. Puesto que los caracteres quedan determinados por la condición $\rho(\underline{m}) = \underline{\lambda}^{\underline{m}}$ para $\underline{m} \in L_\rho$ (Proposición 2.2.17), las curvas son la misma si y sólo si $L_1 = L_2$. Si $L_1 = L_2$ debe existir una matriz $(b_{ij})_{ij}$ con coeficientes enteros tal que $d_i \underline{m}_i = \sum_{j=1}^{n-1} b_{ij} d_j \underline{n}_j$, y por tanto, puesto que además $\underline{m}_i = \sum_{j=1}^{n-1} a_{ij} \underline{n}_j$, $b_{ij} = \dfrac{d_i a_{ij}}{d_j}$.

Recíprocamente, si se define $b_{ij} = \dfrac{d_i a_{ij}}{d_j}$ entonces es fácil comprobar que $\det(b_{ij})_{ij} = \det(a_{ij})_{ij}$, y evidentemente $d_i \underline{m}_i = \sum_{j=1}^{n-1} b_{ij} d_j \underline{n}_j$, luego $L_1 = L_2$.

□

Teorema 2.4.14 *Sean* $n \geq 1$*,* $d \in \mathbb{Z}_{>0}$*,* $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$*,* $\underline{\lambda} \in (k^*)^n$*, y* $d = d_1 \cdots d_{n-1}$ *con* $d_1 / \ldots / d_{n-1}$*. Fijemos una curva mnoomial irreducible* C_1*. Entonces existe una curva monomial* C *en* $\mathcal{A}^n(k)$ *con* d *componentes, una de las cuales es* C_1*, y cuyo ideal asociado es de la forma* $I_+(\rho)$ *tal que* $\operatorname{Sat} L_\rho = \langle \underline{h} \rangle^\perp$ *y* $\operatorname{Sat} L_\rho / L_\rho \cong \mathbb{Z}/(d_1) \oplus \ldots \oplus \mathbb{Z}/(d_{n-1})$*. Dos de tales curvas,* $I_+(\rho_1)$*,* $I_+(\rho_2)$ *son iguales si y sólo si* $L_{\rho_1} = L_{\rho_2}$*.*

Dem. La existencia es debida a la Proposición 2.4.5. Además, en las condiciones del enunciado, una vez determinado el retículo, el carácter parcial ρ también lo está, ya que $\rho(\underline{m}) = \underline{\lambda}^{\underline{m}}$ para todo $\underline{m} \in L_\rho$ (Proposición 2.2.17).

□

Capítulo 3

Curvas monomiales y campos de Euler

Es un resultado conocido que la existencia de un campo de Euler (tipo especial de k-derivación) tangente a una curva irreducible se corresponde, en cierto sentido, con la propiedad de binomialidad del su ideal asociado. Por otro lado, en el capítulo anterior hemos establecido, bajo ciertas condiciones, una equivalencia entre ideales binomiales y curvas monomiales. Cabe por tanto pensar en la posibilidad de una relación entre la existencia de un campo de Euler tangente a una curva C y su carácter monomial. El objetivo de este capítulo es estudiar esta posible relación.

3.1 Ideales y derivaciones

Para comenzar recordaremos algunos resultados clásicos sobre el anillo de las k-derivaciones.

Sea k un cuerpo algebraicamente cerrado y de característica cero, y denotemos por A o bien a $k[X]$, el anillo de polinomios en n indeterminadas con coeficientes en k, o bien a $k[[X]]$, el anillo de series en n indeterminadas con coeficientes en k, o bien el cuerpo de fracciones de cualquiera de los dos casos.

Definición 3.1.1 *Una k-derivación sobre el anillo A es una aplicación k-lineal $\delta : A \to A$ que cumple la regla de Leibnitz,*

$$\delta(fg) = f\delta(g) + g\delta(f), \text{ para todos } f, g \in A.$$

Denotaremos por $\mathrm{Der}_k(A, A)$ al A-módulo libre de las k-derivaciones sobre A. Para cada $i \in \{1, \ldots, n\}$, la derivada parcial respecto de la variable X_i, $\frac{\partial}{\partial X_i}$, es una k-derivación de A. De hecho $\mathrm{Der}_k(A, A) = \bigoplus_{i=1}^n A \frac{\partial}{\partial X_i}$. Es decir, cualquier derivación δ se puede escribir de forma única como

$$\delta = \sum_{i=1}^{n} f_i \frac{\partial}{\partial X_i}$$

con $f_i \in A$ para todo i (de hecho, $f_i = \delta(X_i)$).

Definición 3.1.2

1. *Dado $I \subset A$, diremos que una k-derivación de A, δ, es tangente a I si se cumple $\delta(I) \subseteq I$.*

2. *Sea $\mathcal{V} \subset \mathcal{A}^n(k)$ una variedad algebraica y sea $I = \mathcal{I}(\mathcal{V})$. Diremos que una k-derivación δ es tangente a $\mathcal{V}$ si se cumple que $\delta(I) \subseteq I$.*

Es decir, δ es tangente a $\mathcal{V}$ si δ induce una k-derivación en el anillo de coordenadas de la variedad. La condición de tangencia se puede expresar en términos de los primos asociados, como se ve en la siguiente proposición:

Proposición 3.1.3 *Sea I un ideal radical del anillo A y sea $\{\mathcal{P}_1, \ldots, \mathcal{P}_d\}$ el conjunto de sus primos asociados. Si $\delta \in \mathrm{Der}_k(A, A)$, entonces $\delta(I) \subseteq I \Leftrightarrow \delta(\mathcal{P}_j) \subseteq \mathcal{P}_j$, para todo $j \in \{1, \ldots, d\}$.*

Dem. Puesto que $I = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_d$, es evidente que si $\delta(\mathcal{P}_j) \subseteq \mathcal{P}_j$ para todo $j \in \{1, \ldots, d\}$, entonces $\delta(I) \subseteq I$. Recíprocamente, supongamos que δ es tangente a I. Fijemos un índice $j \in \{1, \ldots, d\}$ y consideremos $f \in \mathcal{P}_j$. Como I es radical, si $k \neq j$ entonces $\mathcal{P}_k \not\subseteq \mathcal{P}_j$, luego existe $g_k \in \mathcal{P}_k$ tal que $g_k \notin \mathcal{P}_j$. Consideremos $f \prod_{k \neq j} g_k \in I$. Aplicando la regla de Leibnitz, se tiene,

$$\delta\left(f \prod_{k \neq j} g_k\right) = \delta(f) \prod_{k \neq j} g_k + f\delta\left(\prod_{k \neq j} g_k\right) \in I \subseteq \mathcal{P}_j$$

entonces $\delta(f) \prod_{k \neq j} g_k \in \mathcal{P}_j$ luego $\delta(f) \in \mathcal{P}_j$ ya que $\mathcal{P}_j$ es un ideal primo. Por tanto, δ es tangente a $\mathcal{P}_j$.

□

Corolario 3.1.4 *Se consideran una variedad algebraica $\mathcal{V} \subset \mathcal{A}^n(k)$, y una k-derivación de $k[X]$, δ. Entonces δ es tangente a $\mathcal{V}$ si y sólo si es tangente a todas sus componentes irreducibles.*

A partir de ahora consideraremos sólo una clase especial de k-derivaciones, los denominados campos de Euler.

Definición 3.1.5 *Diremos que una k-derivación δ sobre A es un campo de Euler si existen números enteros $a_1, \dots, a_n$ tales que*

$$\delta = \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}.$$

En este caso, llamaremos vector de coeficientes del campo δ al vector con coordenadas enteras, $\underline{a} = (a_1, \dots, a_n)$.

Veamos el significado geométrico que tiene la existencia de un campo de Euler tangente a una curva.

Proposición 3.1.6 *Dadas series $x_1, \dots, x_n \in k[[t]]$ con $\mathrm{ord}(x_i) > 0$, consideremos el homomorfismo de k-álgebras*

$$\begin{array}{rcl} \phi : k[[X_1, \dots, X_n]] & \longrightarrow & k[[t]] \\ X_i & \longmapsto & x_i(t) \end{array},$$

y sea $I := \ker(\phi)$. Si $\delta = \sum_i a_i X_i \frac{\partial}{\partial X_i}$ es una derivación sobre $k[[X]]$, con $a_i \in \mathbb{Z}$ para todo i, entonces son equivalentes:

1. *Existe $h(t) \in k[[t]]$ tal que $(a_1 x_1(t), \dots, a_n x_n(t)) = h(t)(\dot{x}_1(t), \dots, \dot{x}_n(t))$ (donde $\dot{x}_i(t) = \frac{\partial}{\partial t}(x_i(t))$).*
2. *$\delta(I) \subseteq I$.*

Dem. Como $\ker(\phi) = I$, se tiene, a partir de ϕ, una inyección,

$$i : k[[X]]/I \hookrightarrow k[[t]]$$

que prolongada al cuerpo de fracciones, nos proporciona la extensión de cuerpos,

$$i : \mathrm{Fr}(k[[X]]/I) \hookrightarrow k((t)).$$

Además, dicha extensión resulta separable, pues k tiene característica cero.

Veamos primero $2 \Rightarrow 1$. Supongamos, por lo tanto, que δ es un campo de Euler tangente a I. Como $\delta(I) \subseteq I$, la derivación δ induce una derivación $\widetilde{\delta}$ sobre $k[[X]]/I$, que se extiende (utilizando la regla de derivación del cociente) a una derivación sobre el cuerpo de fracciones $\mathrm{Fr}(k[[X]]/I)$,

$$\widetilde{\delta} : \mathrm{Fr}(k[[X]]/I) \to \mathrm{Fr}(k[[X]]/I).$$

Como la extensión $i : \mathrm{Fr}(k[[X]]/I) \hookrightarrow k((t))$ es separable, $\widetilde{\delta}$ se puede prolongar a $k((t))$ (Lema 16.15 [Eis]), es decir, existe una k-derivación $\overline{\delta}$ sobre $k((t))$, haciendo el siguiente diagrama conmutativo:

$$\begin{array}{ccc}
\mathrm{Fr}(k[[X]]/I) & \overset{i}{\hookrightarrow} & k((t)) \\
\widetilde{\delta} \downarrow & & \downarrow \overline{\delta} \\
\mathrm{Fr}(k[[X]]/I) & \overset{i}{\hookrightarrow} & k((t))
\end{array}$$

Además, debido a que $\overline{\delta}$ es una derivación sobre $k((t))$, existe $h(t) \in k((t))$ tal que $\overline{\delta} = h(t)\frac{\partial}{\partial t}$. Por lo tanto, para cada $i \in \{1, \dots, n\}$ se tiene:

$$\begin{aligned}
h(t)\dot{x}_i(t) = \overline{\delta}(x_i(t)) = \overline{\delta}(i(X_i + I)) = i(\widetilde{\delta}(X_i + I)) = \\
= i(\delta(X_i) + I) = i(a_i X_i + I) = a_i x_i(t) \ .
\end{aligned}$$

En particular, $\mathrm{ord}(h(t)) > 0$ y por tanto $h(t) \in k[[t]]$ y se tiene 1.

Recíprocamente, supongamos que existe $h(t) \in k[[t]]$ cumpliendo

$$(a_1 x_1(t), \dots, a_n x_n(t)) = h(t)(\dot{x}_1(t), \dots, \dot{x}_n(t)).$$

Se define sobre $k[[t]]$ la derivación $\overline{\delta} = h(t)\frac{\partial}{\partial t}$, y se considera la composición $\overline{\delta} \circ i$, donde i es la inclusión de $k[[X]]/I$ en $k[[t]]$. Entonces, para cada $f \in k[[X]]$, se tiene

$$\begin{aligned}
\overline{\delta} \circ i(f + I) = \overline{\delta}(f(x_1(t), \dots, x_n(t))) &= \sum_{i=1}^{n} \overline{\delta}(x_i(t)) \frac{\partial f}{\partial X_i}(x_1(t), \dots, x_n(t)) \\
&= \sum_{i=1}^{n} h(t)\dot{x}_i(t) \frac{\partial f}{\partial X_i}(x_1(t), \dots, x_n(t)) \\
&= \sum_{i=1}^{n} a_i x_i(t) \frac{\partial f}{\partial X_i}(x_1(t), \dots, x_n(t)) \ .
\end{aligned}$$

Por tanto, dada una serie $f \in k[[X]]$, se tiene que

$$\begin{aligned} i(\delta(f)+I) &= i(\sum_{i=1}^{n} a_i X_i \frac{\partial f}{\partial X_i} + I) = \\ &= \sum_{i=1}^{n} a_i x_i(t) \frac{\partial f}{\partial X_i}(x_1(t), \dots, x_n(t)) = \overline{\delta} \circ i(f+I). \end{aligned}$$

Entonces, si $f \in I$ se tiene $i(\delta(f)+I) = 0$ y por tanto $\delta(f) \in I$. Es decir, $\delta(I) \subseteq I$.

□

3.2 Campos de Euler y curvas monomiales irreducibles

En esta sección veremos que la existencia de un campo de Euler tangente a una curva irreducible C implica el carácter monomial de dicha curva. Más aún, en el resultado central de la sección obtendremos, bajo ciertas condiciones, una equivalencia entre las curvas monomiales irreducibles y las curvas irreducibles que admiten un campo de Euler tangente.

Sea C una curva monomial irreducible con parametrización

$$C \equiv \begin{cases} x_1 = \lambda_1 t^{h_1} \\ \quad\vdots \\ x_n = \lambda_n t^{h_n} \end{cases}$$

dada por los vectores $(\underline{h}, \underline{\lambda})$, y célula asociada $\mathcal{Z} = \{i \in \{1, \dots, n\} \mid \lambda_i \neq 0\}$. Como vimos en la Proposición 2.1.6, el vector $\underline{h}_{\mathcal{Z}}$ (resultado de la restricción de $\underline{h}$ a las coordenadas en $\mathcal{Z}$), es único si se impone la condición m.c.d.$\{h_i \mid i \in \mathcal{Z}\} = 1$. Además, los exponentes correspondientes a índices $i \notin \mathcal{Z}$ pueden tomar cualquier valor, hecho que expresamos escribiendo $h_i = \infty$ (Notación 2.1.8). Con esta notación, el vector $\underline{h} \in (\mathbb{Z}_{\geq 0} \cup \{\infty\})^n$ asociado a C es único, y considerando el conjunto de índices $\widetilde{\mathcal{Z}} = \{i \in \mathcal{Z} \mid h_i = 0\}$ se tiene:

1. $\widetilde{\mathcal{Z}} \subset \mathcal{Z}$
2. $h_i = 0 \Leftrightarrow i \in \widetilde{\mathcal{Z}}$
3. $h_i = \infty \Leftrightarrow i \notin \mathcal{Z}$

El vector de coeficientes $\underline{\lambda}$ sí depende de la parametrización elegida, sin embargo no va a intervenir en el problema de la existencia de campo de Euler. Veamos que toda curva monomial irreducible admite un campo de Euler tangente, cuya construcción depende del vector exponentes de la parametrización.

Definición 3.2.1 *Dados $\underline{a}, \underline{b} \in (\mathbb{Z} \cup \{\infty\})^n$, diremos que $\underline{a}$ y $\underline{b}$ son proporcionales en la intersección, y lo denotaremos $\underline{a} \mathrel{\wr\!\!\cap} \underline{b}$, si existen enteros p, q con $(p, q) \neq (0, 0)$ de forma que $pa_i = qb_i$ para todo i tal que $a_i, b_i \in \mathbb{Z}$.*

Proposición 3.2.2 *Sea C una curva monomial irreducible, con célula asociada $\mathcal{Z}$ y vector de exponentes $\underline{h}$. Sea δ el campo de Euler $\delta = \sum\limits_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}$. Son equivalentes:*

(a) δ es tangente a la curva C.

(b) Los vectores $\underline{a}$ y $\underline{h}$ son proporcionales en la intersección, $\underline{a} \mathrel{\wr\!\!\cap} \underline{h}$ (es decir, puesto que $\underline{a} \in \mathbb{Z}^n$, son proporcionales en las coordenadas que están en $\mathcal{Z}$).

Dem. Sea $I \subset k[X]$ el ideal asociado a la curva C. Entonces I es binomial y existe un carácter parcial ρ definido sobre L_ρ, subretículo de $\mathbb{Z}^{\mathcal{Z}}$, con $I = I_+(\rho) + \langle \{X_i \mid i \notin \mathcal{Z}\} \rangle$ (Proposición 2.1.6), donde $I_+(\rho) \subset k[\mathcal{Z}]$. Consideremos un campo de Euler sobre $k[X]$, $\delta = \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}$. Como $\delta(X_i) = a_i X_i$, entonces $\delta(X_i) \in I$ si $i \notin \mathcal{Z}$, cualquiera que sea a_i. Por tanto, δ es tangente a I si y sólo si $\widetilde{\delta}(I_+(\rho)) \subseteq I_+(\rho)$, siendo $\widetilde{\delta} = \sum_{i \in \mathcal{Z}} a_i X_i \frac{\partial}{\partial X_i}$. Es decir, esta propiedad es independiente del valor que toman los coeficientes para índices que no estén en $\mathcal{Z}$.

Por comodidad en la notación, supongamos que $\mathcal{Z} = \{1, \ldots, n\}$ y por tanto $I = I_+(\rho)$. Hagamos actuar el campo δ sobre el sistema de generadores de $I_+(\rho)$, $\{X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-} \mid \underline{m} \in L_\rho\}$:

$$\delta\left(X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-}\right) = \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}(X^{\underline{m}_+}) - \rho(\underline{m}) \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}(X^{\underline{m}_-}).$$

Denotando $P = \{i \mid m_i > 0\}$ y $N = \{j \mid m_j < 0\}$, podemos escribir

$$\begin{aligned} \delta\left(X^{\underline{m}_+} - \rho(\underline{m}) X^{\underline{m}_-}\right) &= \sum_{i \in P} a_i X_i \frac{\partial}{\partial X_i}(X^{\underline{m}_+}) - \rho(\underline{m}) \sum_{j \in N} a_j X_j \frac{\partial}{\partial X_j}(X^{\underline{m}_-}) \\ &= (\sum_{i \in P} a_i m_i) X^{\underline{m}_+} - \rho(\underline{m}) (\sum_{j \in N} a_j m_j) X^{\underline{m}_-} \\ &= \underline{a}\, \underline{m}_+ X^{\underline{m}_+} - \rho(\underline{m})\, \underline{a}\, \underline{m}_- X^{\underline{m}_-}, \end{aligned}$$

polinomio que pertenece a $I = I_+(\rho)$ si y sólo si se cumple $\underline{a}\,\underline{m}_+ = \underline{a}\,\underline{m}_-$ (Teorema 1.3.5). Por lo tanto δ es tangente a I si y sólo si $\underline{a}\,\underline{m} = 0$ para todo $\underline{m} \in L_\rho$. Pero sabemos que $L_\rho = \langle \underline{h} \rangle^\perp$, luego δ es tangente a I si y sólo si $\underline{a}$ es cualquiera de los vectores con coordenadas enteras que están en la recta que define el vector $\underline{h}$.

$\square$

Corolario 3.2.3 *Toda curva monomial irreducible admite un campo de Euler tangente con todos sus coeficientes no negativos.*

Dem. En efecto, sea $\underline{h}$ el vector de exponentes de la curva. Definimos $a_i = h_i$ cuando $i \in \mathcal{Z}$ y asignamos a a_i cualquier entero no negativo, cuando $i \notin \mathcal{Z}$. Entonces el campo de Euler $\delta = \sum_{i=1}^n a_i X_i \frac{\partial}{\partial X_i}$ es, por la proposición anterior, tangente a C.

$\square$

Nota 3.2.4 Puesto que para todo $i \notin \mathcal{Z}$, a_i puede tomar cualquier valor entero, en lo sucesivo consideraremos $\underline{a} \in (\mathbb{Z} \cup \{\infty\})^n$, denotando por $a_i = \infty$ el hecho de que a_i pueda tomar cualquier valor.

Corolario 3.2.5 *Sean C una curva monomial irreducible con célula $\mathcal{Z}$ y vector de exponentes $\underline{h}$ y δ un campo de Euler con vector de coeficientes $\underline{a} = (a_1, \ldots, a_n)$. Si δ es tangente a C, entonces para $i \in \mathcal{Z}$ se tiene $a_i = 0$ si y sólo si $i \in \widetilde{\mathcal{Z}}$.*

Dem. Inmediata de la Proposición 3.2.2.

$\square$

También es cierto que la existencia de un campo de Euler con coeficientes positivos tangente a una curva irreducible C, implica que C es monomial. Primero, veamos la demostración cuando la curva pasa por el origen.

Teorema 3.2.6 *Sea I un ideal en el anillo de polinomios $k[X]$, primo, de altura $n-1$ y sea $C := \mathcal{V}(I)$ la curva que define I. Supongamos que C pasa por el origen. En estas condiciones, si existe un campo de Euler δ (no trivial) tangente a la curva irreducible C, entonces C es monomial.*

Dem. Sea $\widetilde{I} := Ik[[X]]$, la extensión de I al anillo de series de potencias. Consideremos la descomposición primaria del ideal $\widetilde{I}$, $\widetilde{I} = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_d$ (por ser $k[X]$ un G-anillo, $\widetilde{I}$ es radical y los primos que aparecen en la descomposición primaria de $\widetilde{I}$ tienen también altura $n-1$, [Mat]). Sea δ un campo de Euler tangente a I. Puesto que I genera $\widetilde{I}$ y $\delta(I) \subseteq I$ entonces $\delta(\widetilde{I}) \subseteq \widetilde{I}$, y en particular $\delta(\mathcal{P}_1) \subseteq \mathcal{P}_1$ (Proposición 3.1.3).

Tras una reordenación de las coordenadas podemos suponer que $a_1 \neq 0$ (el campo de Euler es no trivial). Como k es un cuerpo de característica cero y $\mathcal{P}_1$ es un ideal de $k[[X]]$ primo y de altura $n-1$, entonces si denotamos por C_1 a la curva algebroide que define $\mathcal{P}_1$, existe una parametrización de Puiseux para C_1,

$$C_1 \equiv \begin{cases} x_1 = t^{h_1} \\ x_2 = \sum_{i \geq 0} \lambda_i t^{h_2+i} \\ \vdots \end{cases},$$

con $h_1 > 0$ (es decir, $\mathcal{P}_1$ es el núcleo del homomorfismo $\phi : k[[X]] \to k[[t]]$ dado por $\phi(f) = f(x_1(t), \ldots, x_n(t))$).

Supongamos que esta parametrización no es monomial. Salvo reordenación, podemos suponer que $\lambda_0 \neq 0$ y existe $m > 0$ tal que $\lambda_m \neq 0$. Sea m el primero en estas condiciones.

Como el campo de Euler δ es tangente a la curva C_1, si $\underline{a} = (a_1, \ldots, a_n)$ es el vector de coeficientes de δ, entonces el vector $(a_1 x_1(t), \ldots, a_n x_n(t))$ está en la dirección del vector tangente a la curva $(\dot{x}_1(t), \ldots, \dot{x}_n(t))$ (Proposición 3.1.6). Es decir, existe $h(t) \in k[[t]]$ tal que

$$(a_1 x_1(t), \ldots, a_n x_n(t)) = h(t)(\dot{x}_1(t), \dot{x}_2(t), \ldots, \dot{x}_n(t)).$$

En particular, igualando las primeras coordenadas de estos vectores se tiene $a_1 t^{h_1} = h(t) h_1 t^{h_1 - 1}$, luego $h(t) = \frac{a_1}{h_1} t$. Si ahora igualamos las segundas coordenadas resulta

$$a_2(\lambda_0 t^{h_2} + \lambda_m t^{h_2+m} + \ldots) = \frac{a_1}{h_1} t(h_2 \lambda_0 t^{h_2-1} + (h_2+m)\lambda_m t^{h_2+m-1} + \ldots),$$

y por lo tanto

$$\begin{array}{l} a_2 \lambda_0 = \frac{a_1}{h_1} h_2 \lambda_0 \\ a_2 \lambda_m = \frac{a_1}{h_1}(h_2+m)\lambda_m \end{array}.$$

Además $\lambda_0, \lambda_m \neq 0$ y por tanto

$$\frac{a_1}{h_1} h_2 = \frac{a_1}{h_1}(h_2+m)$$

luego $h_2 = h_2 + m$, lo cual es absurdo. Así pues, la parametrización dada es monomial.

Ahora, obviamente $\mathcal{P}_1 \cap k[X_1, \ldots, X_n]$ es el núcleo de la aplicación

$$\begin{array}{rcl} \phi : k[X_1, \ldots, X_n] & \longrightarrow & k[t] \\ X_i & \longmapsto & x_i(t) \end{array},$$

luego es el ideal de la curva monomial

$$C_1 \equiv \left\{ \begin{array}{c} x_1 = x_1(t) \\ \vdots \\ x_n = x_n(t) \end{array} \right. .$$

Como $I \subseteq \mathcal{P}_1 \cap k[X]$, y se trata de dos ideales primos de altura $n-1$, entonces son iguales y la curva C es monomial.

□

Nota 3.2.7 El resultado anterior es válido cuando el campo de Euler es no trivial, ya que la derivación trivial es tangente a cualquier ideal. De aquí en adelante consideraremos derivaciones no triviales, aunque no se especifique.

Como acabamos de ver, toda curva irreducible que pase por el origen y admita un campo de Euler tangente es una curva monomial. Para demostrar el resultado sin la condición de que la curva pase por el origen, necesitamos asegurarnos la existencia de un punto que nos permita un cambio de coordenadas que conserve el carácter monomial de la curva.

Lema 3.2.8 *Sea $\delta = \sum_{i=1}^n a_i X_i \frac{\partial}{\partial X_i}$ un campo de Euler con todos los coeficientes positivos. Si δ es tangente a $I \subset k[X]$, entonces existe un punto $P = (p_1, \ldots, p_n)$ en la variedad que define I, cumpliendo $p_i = 0$ si $a_i \neq 0$.*

Dem. El enunciado asegura la existencia de un elemento $P \in \mathcal{V}(I) \cap \mathcal{V}(\langle\{X_i \mid a_i \neq 0\}\rangle)$, luego basta probar que $I + \langle\{X_i \mid a_i \neq 0\}\rangle \neq k[X]$. Supongamos que no fuera así; entonces existirían $f \in I$ y $g \in \langle\{X_i \mid a_i \neq 0\}\rangle$ tales que $1 = f + g$.

Fijamos un orden monomial $<$ en $k[X]$, y de todas las expresiones del tipo $1 = f + g$ en las condiciones de antes, elegimos una tal que $\mathrm{LM}(g)$ sea mínimo para el orden $<$. Tras una reordenación de las indeterminadas, podemos suponer que los índices correspondientes a coeficientes no nulos en δ son los s primeros ($s \leq n$). Si denotamos por $j_1, \ldots, j_n$ los exponentes del monomio $\mathrm{LM}(g)$, entonces el elemento $\lambda = \sum_{k=1}^s a_k j_k$ es no nulo, ya que $a_k > 0$ para todo $k \in \{1, \ldots, s\}$ y $g \in \langle\{X_i \mid 1 \leq i \leq s\}\rangle$. Para este valor de λ se tiene $\mathrm{LM}(g - \delta(g/\lambda)) < \mathrm{LM}(g)$ y $g - \delta(g/\lambda) \in \langle\{X_i \mid a_i \neq 0\}\rangle$. Se construye el polinomio $f - \delta(f/\lambda)$, que, puesto que $\delta(I) \subseteq I$, cumple

$$f - \delta(f/\lambda) \in I$$

y además, puesto que $1 = f + g$,

$$1 = (f - \delta(f/\lambda)) + (g - \delta(g/\lambda))$$

lo cual va en contra de lo que habíamos supuesto.

□

Proposición 3.2.9 *Sea I un ideal de $k[X]$ primo y de altura $n-1$. Si existe un campo de Euler $\delta = \sum_{i=1}^{n} a_i X_i \frac{\partial}{\partial X_i}$ tangente a I con todos sus coeficientes no negativos, entonces la curva irreducible $C := \mathcal{V}(I)$ es monomial.*

Dem. Por el Lema 3.2.8 sabemos que existe un punto $P = (p_1, \ldots, p_n)$ que pertenece a $C \cap \mathcal{V}(\{X_i \mid a_i \neq 0\})$. Consideremos el cambio de coordenadas dado por $Y_i = X_i - p_i$ para todo $i \in \{1, \ldots, n\}$, que translada el punto P al origen. Denotamos por δ^* al campo de Euler $\sum_{i=1}^{n} a_i Y_i \frac{\partial}{\partial Y_i}$, por I^* al ideal que resulta de aplicarle a I el cambio de coordenadas y por C^* la curva obtenida al aplicarle el cambio a C. Entonces δ^* es tangente a I^*, pues si $f = \sum f_{i_1,\cdots,i_n} X_1^{i_1} \ldots X_n^{i_n}$ y $f^* = \sum f_{i_1,\cdots,i_n} (Y_1 + p_1)^{i_1} \ldots (Y_n + p_n)^{i_n}$, al hacer actuar el campo de Euler δ^* sobre el polinomio f^*, resulta

$$\delta^*(f^*) = \sum f_{i_1,\cdots,i_n} \sum_{j=1}^{n} a_j Y_j \frac{\partial}{\partial Y_j}((Y_1 + p_1)^{i_1} \ldots (Y_n + p_n)^{i_n}) =$$

$$= \sum f_{i_1,\cdots,i_n} \sum_{j=1}^{n} i_j a_j Y_j (Y_1 + p_1)^{i_1} \ldots (Y_j + p_j)^{i_j - 1} \ldots (Y_n + p_n)^{i_n}$$

$$\stackrel{(a_j \neq 0 \Rightarrow p_j = 0)}{=} \sum f_{i_1,\cdots,i_n} \sum_{j=1}^{n} i_j a_j (Y_1 + p_1)^{i_1} \ldots (Y_n + p_n)^{i_n}$$

$$= \left[\sum f_{i_1,\cdots,i_n} \sum_{j=1}^{n} i_j a_j X_1^{i_1} \ldots X_n^{i_n}\right]^* = [\delta(f)]^*.$$

Por lo tanto, para todo $f^* \in I^*$, $\delta^*(f^*) = [\delta(f)]^*$ y como $f \in I$ entonces $\delta(f) \in I$ y $\delta^*(f^*) \in I^*$.

Así pues, I^* es el ideal asociado a una curva irreducible que pasa por el origen y que admite un campo de Euler tangente, δ^*. Entonces, aplicando el Teorema 3.2.6, C^* es monomial.

Consideremos una parametrización monomial para dicha curva,

$$C^* \equiv \begin{cases} y_1 = \lambda_1 t^{h_1} \\ \vdots \\ y_n = \lambda_n t^{h_n} \end{cases}.$$

Puesto que C^* pasa por el origen, $h_i > 0$ para todo i y por el Corolario 3.2.5 se tiene que si $\lambda_i \neq 0$ entonces $a_i \neq 0$ y por tanto $p_i = 0$.

Deshaciendo el cambio de coordenadas, obtenemos una parametrización para C,

$$C \equiv \begin{cases} x_1 = \lambda_1 t^{h_1} + p_1 \\ \vdots \\ x_n = \lambda_n t^{h_n} + p_n \end{cases},$$

que es monomial pues si $\lambda_i = 0$ entonces $x_i = p_i$ y en caso contrario $p_i = 0$ y por tanto $x_i = \lambda_i t^{h_i}$.

□

La condición de que los coeficientes del campo de Euler tangente tengan todos el mismo signo ha sido necesaria en la demostración del Lema 3.2.8 y por tanto de la Proposición 3.2.9. Mas aún, es una condición imprescindible para obtener el propio resultado, como se demuestra en el siguiente ejemplo.

Ejemplo 3.2.10 Consideremos la curva plana C sobre el cuerpo de los números complejos con ideal asociado $I = \langle XY - 1\rangle$ y el campo de Euler $\delta = X\frac{\partial}{\partial X} - Y\frac{\partial}{\partial Y}$. Es claro que el campo δ es tangente a la curva C. Sin embargo, aunque el ideal I es binomial, la curva C no es monomial ya que falla la condición de que I sea combinatoriamente finito.

Según lo que hemos visto podemos establecer una relación entre campos de Euler y curvas monomiales irreducibles.

Teorema 3.2.11 *Sean I un ideal de $k[X_1, \dots, X_n]$ primo y de altura $n-1$ y C la curva que define I. Son equivalentes:*

1. *Existe un campo de Euler tangente a C con todos sus coeficientes no negativos.*

2. *C es monomial irreducible.*

Dem. Consecuencia de la Proposición 3.2.9 y del Corolario 3.2.3.

□

3.3 Campos de Euler y curvas monomiales

La relación que hemos obtenido entre curvas monomiales irreducibles y campos de Euler desaparece al intentar extenderla al caso general. Es claro que la existencia de un campo de Euler, con coeficientes positivos, tangente a una curva C, implica que todas las componentes de C son monomiales (consecuencia del Corolario 3.1.4 y de la Proposición 3.2.9). Sin embargo, no asegura el carácter monomial de C. Además, existen curvas monomiales que no admiten campo de Euler tangente con coeficientes positivos, aunque estas curvas monomiales son detectables mediante un algoritmo.

El objetivo de esta sección es, dada una curva $C = C_1 \cup \ldots \cup C_d$, unión de componentes monomiales irreducibles, estudiar cuándo la curva admite un campo de Euler tangente.

Primero establezcamos las condiciones que tiene que cumplir el vector de coeficientes de un campo de Euler tangente a una unión de curvas monomiales irreducibles.

Proposición 3.3.1 *Consideremos una curva $C = C_1 \cup \ldots \cup C_d$ donde cada C_j es una curva monomial irreducible con célula asociada $\mathcal{Z}_j$ y vector de exponentes $\underline{h}_j$. Si δ es el campo de Euler con vector de coeficientes $\underline{a}$, son equivalentes:*

(a) δ es tangente a C.

(b) $\underline{a} \overset{\frown}{\sim} \underline{h}_j$ para todo $j \in \{1, \ldots, d\}$.

Dem. Es evidente teniendo en cuenta las Proposiciones 3.1.3 y 3.2.2.

□

Por tanto, la existencia de un campo de Euler tangente a una unión de curvas monomiales irreducibles no impone ninguna condición a los vectores coeficientes de las parametrizaciones monomiales de las curvas, mientras que las condiciones para que C sea monomial sí afectan a dichos vectores. Así, resulta sencillo construir uniones de curvas monomiales irreducibles que admitan un campo de Euler tangente, incluso con coeficientes positivos, y que, sin embargo, incumplan las condiciones dadas en el Teorema 2.2.23 para que dichas uniones sean monomiales.

Vamos a ver unos ejemplos en los que existe un campo de Euler tangente a la curva, pero esta no cumple las distintas condiciones del Teorema 2.2.23.

Ejemplo 3.3.2 Consideremos la curva plana $C = C_1 \cup C_2$ sobre el cuerpo $\mathbb{C}$, donde

$$\begin{array}{cc} C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = t^2 \end{array} \right. & C_2 \equiv \left\{ \begin{array}{l} x = 2t \\ y = 2t^2 \end{array} \right. \\ \downarrow & \downarrow \\ \underline{h} = (1,2) & \underline{h} = (1,2) \\ \underline{\lambda}_1 = (1,1) & \underline{\lambda}_2 = (2,2) \end{array}.$$

La curva C admite un campo de Euler tangente con coeficientes positivos $\delta = X\frac{\partial}{\partial X} + 2Y\frac{\partial}{\partial Y}$. Sin embargo no cumple la condición D1 del Teorema 2.2.23 ya que en este caso $\widetilde{L} = \langle(-2,1)\rangle$ $(= \langle(1,2)\rangle^{\perp})$ y $L = \{\underline{m} \in \widetilde{L} \mid \underline{\lambda}_1^{\underline{m}} = \underline{\lambda}_2^{\underline{m}}\} = \{(-2a,a) \mid 1 = 2^{-2a}2^a,\ a \in \mathbb{Z}\} = \{(-2a,a) \mid a = 0\} = \langle\underline{0}\rangle$. Luego $|\widetilde{L}/L| = \infty$ y C no es monomial.

Ejemplo 3.3.3 Consideremos la curva compleja en el espacio, $C = C_1 \cup C_2$, donde

$$\begin{array}{cc} C_1 \equiv \left\{ \begin{array}{l} x = 0 \\ y = t^2 \\ z = t^3 \end{array} \right. & C_2 \equiv \left\{ \begin{array}{l} x = t^2 \\ y = 0 \\ z = t^5 \end{array} \right. \\ \downarrow & \downarrow \\ \underline{h}_1 = (\infty,2,3) & \underline{h}_2 = (2,\infty,5) \end{array}.$$

La célula asociada a la componente C_1 es $\mathcal{Z}_1 = \{2,3\}$, mientras que para C_2 resulta $\mathcal{Z}_2 = \{1,3\}$. El campo de Euler $\delta = 6X\frac{\partial}{\partial X} + 10Y\frac{\partial}{\partial Y} + 15Z\frac{\partial}{\partial Z}$ es tangente a C. En efecto, el vector $\underline{a} = (6,10,15)$ cumple: $\underline{a}_{\mathcal{Z}_1} = (10,15)$ es proporcional a $(\underline{h}_1)_{\mathcal{Z}_1} = (2,3)$ y $\underline{a}_{\mathcal{Z}_2} = (6,15)$ es proporcional a $(\underline{h}_2)_{\mathcal{Z}_2} = (2,5)$. Sin embargo, el conjunto $U = \{\mathcal{Z}_1, \mathcal{Z}_2\}$ no es cerrado para intersecciones, y por tanto la curva C no es monomial, pues no se cumple la condición D2 del Teorema 2.2.23.

Ejemplo 3.3.4 Consideremos la curva $C = C_1 \cup C_2$ donde,

$$\begin{array}{cc} C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = t^2 \\ z = t^3 \end{array} \right. & C_2 \equiv \left\{ \begin{array}{l} x = 2t \\ y = 2t^2 \\ z = 0 \end{array} \right. \\ \downarrow & \downarrow \\ \underline{h}_1 = (1,2,3) & \underline{h}_2 = (1,2,\infty) \end{array}.$$

La célula asociada a la componente C_1 es $\mathcal{Z}_1 = \{1,2,3\}$, mientras que para C_2 resulta $\mathcal{Z}_2 = \{1,2\}$. El campo de Euler $\delta = X\frac{\partial}{\partial X} + 2Y\frac{\partial}{\partial Y} + 3Z\frac{\partial}{\partial Z}$ es tangente a C. En efecto, se tiene $\underline{a}_{\mathcal{Z}_1} = (1,2,3) = (\underline{h}_1)_{\mathcal{Z}_1}$ y $\underline{a}_{\mathcal{Z}_2} = (1,2) = (\underline{h}_2)_{\mathcal{Z}_2}$. Sin embargo, el punto $P = (1,1,1)$ está en C y su proyección en la célula $\mathcal{Z}_2 = \{1,2\}$) no está. Por lo tanto la condición D3 del Teorema 2.2.23 no se cumple y C no es monomial.

Recíprocamente, a pesar de las condiciones tan fuertes que tienen que cumplir las componentes irreducibles de una curva monomial, tampoco vamos a poder asegurar la existencia de un campo Euler tangente en todos los casos. Sin embargo, la búsqueda de contraejemplos no es trivial, pues las condiciones de las que hablamos están cerca de lo que se busca.

Sea $C = C_1 \cup \ldots \cup C_d$ una curva monomial y consideremos, para cada $j \in \{1,\ldots,d\}$ el vector $\underline{h}_j$ de exponentes de C_j. Como vimos en la Proposición 3.3.1, la existencia o no de un campo de Euler δ tangente a una curva equivale a la existencia de un vector $\underline{a} \in (\mathbb{Z}_{\geq 0} \cup \{\infty\})^n$ tal que $\underline{a} \stackrel{\cap}{\sim} \underline{h}_j$ para todo j. Pero como la curva C con la que trabajamos es monomial, esta condición se puede debilitar, según se ve en el siguiente resultado; que también explica porqué la condición D2 no tiene relevancia en cuanto a la existencia de campos de Euler tangentes.

Proposición 3.3.5 *Sean $C = C_1 \cup ... \cup C_d$ una curva monomial y δ un campo de Euler tangente a la componente C_k. Si $j \in \{1,\ldots,d\}$ cumple que $\mathcal{Z}_j \subseteq \mathcal{Z}_k$, entonces δ también es tangente a la componente C_j.*

Dem. Sea $\delta = \sum_i a_i X_i \frac{\partial}{\partial X_i}$ un campo de Euler tangente a la curva monomial irreducible C_k con vector de exponentes $\underline{h}_k$. Por la Proposición 3.2.2, $\underline{a} \stackrel{\cap}{\sim} \underline{h}_k$; es decir, existen enteros α, β con $(\alpha,\beta) \neq (0,0)$ de forma que $\alpha a_i = \beta h_{ki}$ para todo $i \in \mathcal{Z}_k$. Denotemos por $\underline{h}_j$ el vector de exponentes de la componente irreducible C_j. Como $\mathcal{Z}_j \subseteq \mathcal{Z}_k$ y C es monomial, entonces existe un entero λ no nulo tal que $\lambda h_{ji} = h_{ki}$ para todo $i \in \mathcal{Z}_j$ (Nota 2.2.34). Por tanto, para todo $i \in \mathcal{Z}_j$ se tiene $\alpha a_i = \beta h_{ki} = \lambda\beta h_{ji}$ siendo $(\alpha, \lambda\beta) \neq (0,0)$, luego $\underline{a} \stackrel{\cap}{\sim} \underline{h}_j$.

$\square$

Como acabamos de decir, el problema de la existencia del campo de Euler tangente a C afecta solamente a los exponentes de las parametrizaciones. Por ello, a partir de ahora trataremos el problema en términos de los vectores $\underline{h}_1, \ldots, \underline{h}_d$.

Veamos primero una condición de proporcionalidad que cumplen los vectores $\underline{h}_1, \ldots, \underline{h}_d$ cuando C es monomial y que va a ser fundamental en las siguientes construcciones.

Proposición 3.3.6 *Sea $C = C_1 \cup \ldots \cup C_d$ una curva monomial. Para cada $j \in \{1, \ldots, d\}$, denotemos por $\underline{h}_j$ el vector de exponentes de C_j. Entonces $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ para cualesquiera $j, k \in \{1, \ldots, d\}$.*

Dem. Como C es una curva monomial, el conjunto $\{\mathcal{Z}_1, \ldots, \mathcal{Z}_d, \widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_d\}$ es cerrado para intersecciones. Luego dados $j, k \in \{1, \ldots, d\}$, existe $s \in \{1, \ldots, d\}$ cumpliendo que, o bien $\mathcal{Z}_j \cap \mathcal{Z}_k$ es $\mathcal{Z}_s$, o bien es $\widetilde{\mathcal{Z}}_s$. Entonces, denotando $\mathcal{Z}_s^* = \mathcal{Z}_s$ cuando $\mathcal{Z}_j \cap \mathcal{Z}_k = \mathcal{Z}_s$ y $\mathcal{Z}_s^* = \widetilde{\mathcal{Z}}_s$ cuando $\mathcal{Z}_j \cap \mathcal{Z}_k = \widetilde{\mathcal{Z}}_s$, se tiene que $\mathcal{Z}_s^* \subseteq \mathcal{Z}_j$ y $\mathcal{Z}_s^* \subseteq \mathcal{Z}_k$. Por lo tanto, según la Nota 2.2.34, existen enteros no nulos λ, μ tales que para todo $i \in \mathcal{Z}_s^*$ se tiene $\lambda h_{si}^* = h_{ji}$ y $\mu h_{si}^* = h_{ki}$, de donde $\mu h_{ji} = \lambda h_{ki}$ con $(\lambda, \mu) \neq (0, 0)$, y se tiene $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$.

$\square$

Comenzaremos nuestro análisis preguntándonos qué ocurre en el caso de curvas *por el origen.* En este caso, para todo $j \in \{1, \ldots, d\}$, $\underline{h}_j \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$.

Por lo tanto, en lo que sigue, consideraremos vectores $\underline{h}_1, \ldots, \underline{h}_d \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$. Definamos para cada $j \in \{1, \ldots, d\}$, el conjunto $\mathcal{Z}_j = \{i \mid h_{ji} \in \mathbb{Z}_{>0}\}$. Se tienen los siguientes resultados:

Lema 3.3.7 *Sean $\underline{a}, \underline{b} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$, $\mathcal{Z}_{\underline{a}} := \{i \mid a_i \neq \infty\}$ y $\mathcal{Z}_{\underline{b}} := \{i \mid b_i \neq \infty\}$. Entonces son equivalentes:*

1. *$\underline{a} \overset{\cap}{\sim} \underline{b}$.*
2. *Para cualesquiera $i, m \in \mathcal{Z}_{\underline{a}} \cap \mathcal{Z}_{\underline{b}}$ se cumple $\dfrac{a_i}{b_i} = \dfrac{a_m}{b_m}$.*

Dem. Es obvio, teniendo en cuenta que $\underline{a}$ y $\underline{b}$ no tienen coordenadas nulas.

$\square$

Proposición 3.3.8 *Si $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ para cualesquiera $j, k \in \{1, \ldots, d\}$ y $\bigcap_{j=1}^d \mathcal{Z}_j \neq \emptyset$, entonces existe un vector $\underline{a} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ tal que $\mathcal{Z}_{\underline{a}} = \bigcup_{j=1}^d \mathcal{Z}_j$ y, para todo $j \in \{1, \ldots, d\}$, $\underline{a} \overset{\cap}{\sim} \underline{h}_j$.*

Dem. La demostración es constructiva. Los pasos que debemos seguir para el cálculo de los coeficientes son:

1. Elegimos $m \in \displaystyle\bigcap_{j=1}^{d} \mathcal{Z}_j$.
2. Calculamos $\alpha = \text{m.c.m.}\{h_{jm} \mid j \in \{1, \ldots, d\}\}$.

3. Para cada $j \in \{1, \dots, d\}$, definimos $\lambda_j = \dfrac{\alpha}{h_{jm}}$ ($h_{jm} \in \mathbb{Z}_{>0}$, pues $m \in \mathcal{Z}_j$).

Obsérvese que si $i \in \mathcal{Z}_j \cap \mathcal{Z}_k$, como $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ y $m \in \mathcal{Z}_j$ para todo j, entonces se tiene

$$\frac{h_{ji}}{h_{ki}} = \frac{h_{jm}}{h_{km}} = \frac{\lambda_k}{\lambda_j}$$

luego $\lambda_j h_{ji} = \lambda_k h_{ki}$.

4. Para $i \in \bigcup_{j=1}^{d} \mathcal{Z}_j$ definimos $a_i = \lambda_j h_{ji}$ donde j es cualquier índice tal que $i \in \mathcal{Z}_j$.

5. Si $i \notin \bigcup_{j=1}^{d} \mathcal{Z}_j$ definimos $a_i = \infty$.

El vector $\underline{a}$ construido cumple que $\underline{a} \overset{\cap}{\sim} \underline{h}_j$ para todo j. En efecto, si $j \in \{1, \dots, d\}$ y $l, i \in \mathcal{Z}_j$,

$$\frac{h_{ji}}{h_{jl}} = \frac{\lambda_j h_{ji}}{\lambda_j h_{jl}} = \frac{a_i}{a_l},$$

y por tanto, aplicando el Lema 3.3.7, se tiene que $\underline{a} \overset{\cap}{\sim} \underline{h}_j$.

□

Este resultado nos proporciona una condición suficiente para que una curva monomial, que pasa por el origen, admita un campo de Euler tangente. Aunque esta condición es demasiado restrictiva, va a servir para realizar las siguientes construcciones y determinar una condición necesaria en el caso general.

Corolario 3.3.9 *Supongamos que $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ para todos $j, k \in \{1, \dots, d\}$. Se definen los conjuntos $A_1 = \{j \mid 1 \in \mathcal{Z}_j\}$ y $A_k = \{j \mid 1 \notin \mathcal{Z}_j, \dots, k-1 \notin \mathcal{Z}_j, k \in \mathcal{Z}_j\}$ para $k \in \{2, \dots, n\}$. Entonces, para todo $k \geq 1$ existe $\underline{h}^k = (h_1^k, \dots, h_n^k) \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ tal que $\mathcal{Z}_{\underline{h}^k} = \bigcup_{j \in A_k} \mathcal{Z}_j$ y, para todo $j \in A_k$, $\underline{h}^k \overset{\cap}{\sim} \underline{h}_j$.*

Dem. Es consecuencia de la Proposición 3.3.8, puesto que $k \in \bigcap_{j \in A_k} \mathcal{Z}_k$.

□

Proposición 3.3.10 *En las condiciones y con las notaciones del corolario anterior, si existe* $\underline{a} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ *con* $\mathcal{Z}_{\underline{a}} \supseteq \bigcup_{j=1}^{d} \mathcal{Z}_j$ *y de forma que* $\underline{a} \stackrel{\cap}{\sim} \underline{h}_j$ *para todo* $j \in \{1, \dots, d\}$*, entonces:*

1. *Para todo* $k \in \{1, \dots, n\}$ *tal que* $A_k \neq \emptyset$*,* $\underline{a} \stackrel{\cap}{\sim} \underline{h}^k$ *(y* $\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_{\underline{h}^k}$*) .*

2. *Para todos* k_1, k_2 *tales que* $A_{k_1} \neq \emptyset$ *y* $A_{k_2} \neq \emptyset$*, se tiene que* $\underline{h}^{k_1} \stackrel{\cap}{\sim} \underline{h}^{k_2}$*.*

Dem.

1. Por el Lema 3.3.7, hay que comprobar que para todo $i, m \in \mathcal{Z}_{\underline{h}^k}$,

$$\frac{h_i^k}{a_i} = \frac{h_m^k}{a_m}.$$

Dado $i \in \mathcal{Z}_{\underline{h}^k}$, existe $j \in A_k$ tal que $i \in \mathcal{Z}_j$. Puesto que $j \in A_k$ se tiene además $k \in \mathcal{Z}_j$, $\underline{h}^k \stackrel{\cap}{\sim} \underline{h}_j$ y $\mathcal{Z}_j \subseteq \mathcal{Z}_{\underline{h}^k}$. Por tanto, $\frac{h_i^k}{h_{ji}} = \frac{h_k^k}{h_{jk}}$. Además, por hipótesis $\underline{h}_j \stackrel{\cap}{\sim} \underline{a}$, luego $\frac{a_i}{h_{ji}} = \frac{a_k}{h_{jk}}$, de lo que se deduce $\frac{h_i^k}{a_i} = \frac{h_k^k}{a_k}$ y se tiene el resultado.

2. Por lo anterior, si $i, m \in \mathcal{Z}_{\underline{h}^{k_1}} \cap \mathcal{Z}_{\underline{h}^{k_2}}$ se tiene $\frac{h_i^{k_1}}{a_i} = \frac{h_m^{k_1}}{a_m}$ y $\frac{h_i^{k_2}}{a_i} = \frac{h_m^{k_2}}{a_m}$, luego $\frac{h_i^{k_1}}{h_i^{k_2}} = \frac{h_m^{k_1}}{h_m^{k_2}}$ y se cumple 2.

$\square$

La proposición anterior nos proporciona una condición necesaria para la existencia de un campo de Euler tangente a una curva monomial por el origen, y nos da una pauta para construir una curva monomial que no admita campo de Euler tangente.

Ejemplo 3.3.11 Consideremos la curva $C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_7$, donde

$$C_1 \equiv \begin{cases} x_1 = t \\ x_2 = 0 \\ x_3 = t \\ x_4 = t \\ x_5 = 0 \end{cases} \qquad C_2 \equiv \begin{cases} x_1 = t^2 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = t \end{cases} \qquad C_3 \equiv \begin{cases} x_1 = 0 \\ x_2 = t \\ x_3 = t \\ x_4 = 0 \\ x_5 = t \end{cases}$$

$$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$$

$$\mathcal{Z}_1 = \{1,3,4\} \qquad \mathcal{Z}_2 = \{1,5\} \qquad \mathcal{Z}_3 = \{2,3,5\}$$

$$\underline{h}_1 = (1,\infty,1,1,\infty) \qquad \underline{h}_2 = (2,\infty,\infty,\infty,1) \qquad \underline{h}_3 = (\infty,1,1,\infty,1)$$

$$C_4 \equiv \begin{cases} x_1 = t \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = 0 \end{cases} \quad C_5 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = t \\ x_4 = 0 \\ x_5 = 0 \end{cases} \quad C_6 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = t \end{cases} \quad C_7 \equiv \begin{cases} x_1 = 0 \\ x_2 = t \\ x_3 = t \\ x_4 = 0 \\ x_5 = 0 \end{cases}$$

$$\updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow \qquad\qquad \updownarrow$$

$$\mathcal{Z}_4 = \{1\} \qquad \mathcal{Z}_5 = \{3\} \qquad \mathcal{Z}_6 = \{5\} \qquad \mathcal{Z}_7 = \{2,3\}$$

La curva C es monomial ya que se cumplen las condiciones D1', D2' y D3' del Teorema 2.2.25.

Como $\mathcal{Z}_4 \subseteq \mathcal{Z}_1$, $\mathcal{Z}_5 \subseteq \mathcal{Z}_1$, $\mathcal{Z}_6 \subseteq \mathcal{Z}_2$ y $\mathcal{Z}_7 \subseteq \mathcal{Z}_3$, para encontrar un campo de Euler tangente hay que buscar un vector $\underline{a}$ proporcional a $\underline{h}_1$, $\underline{h}_2$ y a $\underline{h}_3$ (Proposición 3.3.5). En este caso tenemos $A_1 = \{1,2\}$, $A_2 = \{3\}$, y aplicando la Proposición 3.3.8, $\underline{h}^1 = (2,\infty,2,2,1)$ y $\underline{h}^2 = (\infty,1,1,\infty,1)$. Como $\underline{h}^1 \not\approx \underline{h}^2$ (basta fijarse en sus coordenadas 3 y 5), no puede existir un campo de Euler tangente a la curva (Proposición 3.3.10).

3.4 Algoritmo

Ya sabemos que no todas las curvas monomiales admiten un campo de Euler tangente, luego es conveniente establecer criterios para determinar cuándo una curva monomial admite campo de Euler tangente. La respuesta la daremos mediante un algoritmo que además calcule el vector de coeficientes de un campo tangente, caso de que éste exista. Para simplificar el problema, comenzaremos dando la solución en el caso de curvas monomiales por el origen.

Consideremos vectores $\underline{h}_1, \dots, \underline{h}_d \in (\mathbb{Z}_{>0} \cup \infty)^n$ y definimos para cada $j \in \{1, \dots, d\}$, el conjunto $\mathcal{Z}_j = \{i \mid h_{ji} \in \mathbb{Z}_{>0}\}$.

Lema 3.4.1 *Si $\mathcal{Z}_j \cap \mathcal{Z}_k = \emptyset$ para todo $j, k \in \{1, \ldots, d\}$ con $j \neq k$, entonces existe $\underline{a} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ de forma que $\mathcal{Z}_{\underline{a}} = \cup_{j=1}^{d} \mathcal{Z}_j$ y $\underline{a} \frown \underline{h}_j$ para todo $j \in \{1, \ldots, d\}$.*

Dem. Dado $i \in \{1, \ldots, n\}$, si existe $j \in \{1, \ldots, d\}$ tal que $i \in \mathcal{Z}_j$, por hipótesis este es único, luego definimos $a_i = h_{ji}$. En otro caso, a_i puede tomar cualquier valor entero y escribimos $a_i = \infty$. El vector $\underline{a}$ así construido cumple la condición de ser proporcional en la intersección a los vectores $\{\underline{h}_1, \ldots, \underline{h}_d\}$.

□

Supongamos, a partir de ahora, que para cualesquiera $j, k \in \{1, \ldots, d\}$ se cumple que $\underline{h}_j \frown \underline{h}_k$. Entonces se tiene:

Lema 3.4.2 *En las condiciones y con las notaciones del Corolario 3.3.9, si $\underline{a} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ entonces son equivalentes:*

1. *$\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_j$ y $\underline{a} \frown \underline{h}_j$ para todo $j \in \{1, \ldots, d\}$.*
2. *$\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_{\underline{h}^k}$ y $\underline{a} \frown \underline{h}^k$ para todo k con $A_k \neq \emptyset$.*

Dem. Es claro que $\{1, \ldots, d\}$ es la unión disjunta de los conjuntos A_k no vacíos, luego por una parte, $\cup_{j=1}^{d} \mathcal{Z}_j = \cup_{A_k \neq \emptyset} \mathcal{Z}_{\underline{h}^k}$ (consecuencia de 3.3.9), y, por otra parte, para todo $j \in \{1, \ldots, d\}$, existe $k \in \{1, \ldots, n\}$ tal que $j \in A_k$. Si $\underline{a} \frown \underline{h}^k$, puesto que $\underline{h}^k \frown \underline{h}_j$ y $\mathcal{Z}_j \subseteq \mathcal{Z}_{\underline{h}^k} \subseteq \mathcal{Z}_{\underline{a}}$, se tiene $\underline{h}_j \frown \underline{a}$.

El recíproco es la Proposición 3.3.10.

□

Teniendo en cuenta las construcciones dadas para el vector $\underline{a}$ en el caso de que la intersección de todas las células sea no vacía (Proposición 3.3.8), en el caso de células disjuntas (Lema 3.4.1) y el resultado que acabamos de demostrar, podemos construir el algoritmo de existencia y cálculo de campos de Euler, para una curva unión de curvas monomiales irreducibles por el origen.

Algoritmo 3.4.3
Input: $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\} \subset (\mathbb{Z}_{>0} \cup \{\infty\})^n$
Output: $F = \emptyset$ o $F = \{\underline{a}\} \subset (\mathbb{Z}_{>0} \cup \{\infty\})^n$
Paso 1: *Se comprueba si existen $j, k \in \{1, \ldots, d\}$ tales que $\underline{h}_j \not\frown \underline{h}_k$. Si es así, el algoritmo devuelve $F = \emptyset$ y termina.*
Paso 2: *Se construyen, para cada $j \in \{1, \ldots, d\}$, los conjuntos $\mathcal{Z}_j = \{i \in \{1, \ldots, n\} \mid h_{ji} \neq \infty\}$.*

Paso 3: *Se comprueba si para todos $j, k \in \{1, \ldots, d\}$ con $j \neq k$ se tiene $\mathcal{Z}_j \cap \mathcal{Z}_k = \emptyset$. Si es así, se construye $\underline{a}$ como en el Lema 3.4.1, el algoritmo devuelve $F = \{\underline{a}\}$ y termina.*
Paso 4: *Elegimos $j, k \in \{1, \ldots, d\}$, con $j \neq k$ y $\mathcal{Z}_j \cap \mathcal{Z}_k \neq \emptyset$. Se reordenan las coordenadas para que $1 \in \mathcal{Z}_j \cap \mathcal{Z}_k$. Se construyen, para cada $k \in \{1, \ldots, n\}$, los conjuntos A_k, y si $A_k \neq \emptyset$ se calcula $\underline{h}^k$ como en el Corolario 3.3.9. Se redefine $\mathcal{E} = \{\underline{h}^k \mid A_k \neq \emptyset\}$ y se aplica el algoritmo a $\mathcal{E}$.*

Lema 3.4.4 *Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de componentes monomiales irreducibles por el origen y sea $\{\underline{h}_1, \ldots, \underline{h}_d\}$ el conjunto de exponentes asociados a las parametrizaciones monomiales de sus componentes. Si existe $\underline{a} \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ tal que $\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_j$ y $\underline{a} \overset{\cap}{\sim} \underline{h}_j$ para todo j, entonces $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ para cualesquiera $j, k \in \{1, \ldots, d\}$.*

Dem. Sean $i, m \in \mathcal{Z}_j \cap \mathcal{Z}_k$. Como $\underline{a} \in \mathbb{Z}^n$, $\underline{a} \overset{\cap}{\sim} \underline{h}_j$ y $\underline{a} \overset{\cap}{\sim} \underline{h}_k$, entonces $\frac{h_{ji}}{a_i} = \frac{h_{jm}}{a_m}$ y $\frac{h_{ki}}{a_i} = \frac{h_{km}}{a_m}$, luego $\frac{h_{ji}}{h_{ki}} = \frac{h_{jm}}{h_{km}}$, por lo tanto $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$.

□

Teorema 3.4.5 *Sea $C = C_1 \cup \ldots \cup C_d$ una curva unión de componentes monomiales irreducibles por el origen y sea $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\}$ el conjunto de exponentes asociados a las parametrizaciones monomiales de sus componentes. Si aplicamos el Algoritmo 3.4.3 a $\mathcal{E}$, la salida es $\emptyset$ si y sólo si no existe un campo de Euler tangente a C. Si la salida es $F = \{\underline{a}\}$, entonces el campo de Euler con coeficientes $\underline{a}$ es tangente a la curva C.*

Dem. Como vimos en el lema anterior, para que C admita un campo de Euler tangente es necesario que $\underline{h}_j \overset{\cap}{\sim} \underline{h}_k$ para cualesquiera $j, k \in \{1, \ldots, d\}$, condición que se comprueba en el Paso 1. Es claro que el conjunto $\{1, \ldots, d\}$ es unión disjunta de los conjuntos A_k cuando k varía en $\{1, \ldots, n\}$. Por lo tanto, si ejecutamos el Paso 4, como A_1 contiene por lo menos dos elementos, el nuevo conjunto defininido, $\mathcal{E}$, contiene menos de d vectores. Luego el algoritmo termina en un número finito de pasos. Además, sabemos que $\underline{a}$ es el vector de coeficientes de un campo de Euler tangente a C, si y sólo si $\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_j$ y $\underline{a} \overset{\cap}{\sim} \underline{h}_j$ para todo j y como vimos en el Lema 3.4.2, esta condición es equivalente a que $\mathcal{Z}_{\underline{a}} \supseteq \mathcal{Z}_{\underline{h}^k}$ y $\underline{a} \overset{\cap}{\sim} \underline{h}^k$ para todo $k \in \{1, \ldots, n\}$ con $A_k \neq \emptyset$. Teniendo en cuenta esto, la Proposición 3.3.8, el Corolario 3.3.9 y el Lema 3.4.1, el teorema queda demostrado.

□

Nota 3.4.6 Si aplicamos el Algoritmo 3.4.3 a los vectores exponentes de una curva *monomial* por el origen, entonces $\underline{h}_j \overset{\frown}{\sim} \underline{h}_k$ para cualesquiera $j, k \in \{1, \ldots, d\}$ (Proposición 3.3.6), y la primera comprobación del Paso 1 no sería necesaria. Además, se puede hacer una reducción en el conjunto de vectores de entrada $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\}$, quedándonos sólo con aquellos que corresponden a células maximales para la contención (Proposición 3.3.5), como se hizo en el Ejemplo 3.3.11.

Si quitamos la condición de que las curvas monomiales irreducibles pasen por el origen, el algoritmo no se complica demasiado, basta tener en cuenta el siguiente resultado.

Lema 3.4.7 *Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles. Si existe un campo de Euler tangente a C, entonces, para cualesquiera $j, k \in \{1, \ldots, d\}$ se cumple que $\widetilde{\mathcal{Z}}_j \cap \mathcal{Z}_k \subseteq \widetilde{\mathcal{Z}}_k$.*

Dem. Por hipótesis, existe un vector $\underline{a}$ proporcional a los $\underline{h}_j$ para todo $j \in \{1, \ldots, d\}$. Si existe $i \in \widetilde{\mathcal{Z}}_j \cap (\mathcal{Z}_k \backslash \widetilde{\mathcal{Z}}_k)$, entonces, por el Corolario 3.2.5, como $i \in \widetilde{\mathcal{Z}}_j$, $a_i = 0$. Pero $\underline{a}$ tambien es proporcional a $\underline{h}_k$, con lo cual $h_{ki} = 0$ y tendríamos $i \in \widetilde{\mathcal{Z}}_k$, lo cual es absurdo.

$\square$

Por lo tanto el algoritmo en el caso general quedaría modificado de la siguiente manera:

Algoritmo 3.4.8
Input: $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\} \subset (\mathbb{Z}_{\geq 0} \cup \infty)^n$
Output: $F = \emptyset$ *o* $F = \{\underline{a}\} \subset (\mathbb{Z}_{\geq 0} \cup \{\infty\})^n$
Paso 1: *Se construyen, para cada $j \in \{1, \ldots, d\}$, los conjuntos $\mathcal{Z}_j = \{i \in \{1, \ldots, n\} \mid h_{ji} \neq \infty\}$ y $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_{ji} = 0\}$.*
Paso 2: *Si existen $j, k \in \{1, \ldots, d\}$ tales que $\widetilde{\mathcal{Z}}_j \cap \mathcal{Z}_k \not\subseteq \widetilde{\mathcal{Z}}_k$, entonces el algoritmo devuelve $F = \emptyset$ y termina.*
Paso 3: *Calculamos $\mathcal{Z} = \{1, \ldots, n\} \backslash \bigcup_{j=1}^{d} \widetilde{\mathcal{Z}}_j$ y redefinimos $\mathcal{E} = \{\underline{h}_1^*, \ldots, \underline{h}_d^*\}$ donde $h_{ji}^* = h_{ji}$ para todo $i \in \mathcal{Z}$ y $h_{ji}^* = \infty$ para todo $i \notin \mathcal{Z}$.*
Paso 4: *Aplicamos a $\mathcal{E}$ el Algoritmo 3.4.3. Si devuelve $\emptyset$, entonces $F = \emptyset$. Si devuelve un vector $\underline{a}^*$, entonces se define el vector $\underline{a}$ con coordenadas $a_i = a_i^*$ si $i \in \mathcal{Z}$ y cero en el resto de los casos, devolviendo $F = \{\underline{a}\}$.*

Teorema 3.4.9 *Sea $C = C_1 \cup \ldots \cup C_d$ una unión de curvas monomiales irreducibles y sea $\mathcal{E} = \{\underline{h}_1, \ldots, \underline{h}_d\}$ el conjunto de exponentes asociados a las parametrizaciones monomiales de sus componentes. Si aplicamos el algoritmo anterior a $\mathcal{E}$, la salida es $\emptyset$ si y sólo si no existe campo de Euler tangente a C. Si la salida es $F = \{\underline{a}\}$, entonces el campo de Euler con coeficientes $\underline{a}$ es tangente a la curva C.*

Dem. En primer lugar, por el Lema 3.4.7, si existe un campo de Euler tangente, el algoritmo no termina en el Paso 2. Supongamos por tanto que se ejecuta el Paso 3 (es decir, $\widetilde{\mathcal{Z}}_j \cap \mathcal{Z}_k \subseteq \widetilde{\mathcal{Z}}_k$, para todo j, k) y examinemos los elementos $\underline{h}_j^* \in (\mathbb{Z}_{>0} \cup \{\infty\})^n$ allí construidos. Es claro que tienen por célula asociada $\mathcal{Z}_j^* = \mathcal{Z}_j \cap \mathcal{Z} = \mathcal{Z}_j \setminus \cup_{i=1}^d \widetilde{\mathcal{Z}_i}$ y, por lo anterior, $\mathcal{Z}_j \setminus \mathcal{Z}_j^* = \widetilde{\mathcal{Z}_j}$, así que $\underline{h}_j$ se obtiene completanto $\underline{h}_j^*$ con ceros en las coordenadas de $\widetilde{\mathcal{Z}}_j$. Así, si existe un campo de Euler tangente a C y $\underline{a}$ es su vector de coeficientes, se debe tener $\mathcal{Z}_{\underline{a}} \supset \mathcal{Z}_j$ y $\underline{a} \stackrel{\cap}{\sim} \underline{h}_j^*$. Por lo tanto, el Algoritmo 3.4.3 aplicado a $\{\underline{h}_1^*, \ldots, \underline{h}_d^*\}$ no puede devolver $\emptyset$, y tampoco 3.4.8.

Recíprocamente, supongamos que $\underline{a}$ es la salida de 3.4.8. Entonces $\mathcal{Z}_{\underline{a}^*} \supset \mathcal{Z}_j^*$ y $\underline{a}^* \stackrel{\cap}{\sim} \underline{h}_j^*$ para todo j, luego esto sigue siendo verdad si se completan con ceros en $\mathcal{Z}_j \setminus \mathcal{Z}_j^*$, es decir, $\mathcal{Z}_{\underline{a}} \supset \mathcal{Z}_j$ y $\underline{a} \stackrel{\cap}{\sim} \underline{h}_j$ para todo j, por lo que $\underline{a}$ es el vector de coeficientes de un campo de Euler tangente a C.

$\square$

Ejemplo 3.4.10 Consideremos la curva $C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$, donde

$$
\begin{array}{ccc}
C_1 \equiv \left\{ \begin{array}{c} x_1 = 1 \\ x_2 = t \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = 0 \\ x_6 = t \end{array} \right. &
C_2 \equiv \left\{ \begin{array}{c} x_1 = -1 \\ x_2 = t^2 \\ x_3 = 0 \\ x_4 = 0 \\ x_5 = t \\ x_6 = 0 \end{array} \right. &
C_3 \equiv \left\{ \begin{array}{c} x_1 = -1 \\ x_2 = t^2 \\ x_3 = 0 \\ x_4 = t^3 \\ x_5 = 0 \\ x_6 = 0 \end{array} \right. \\
\downarrow & \downarrow & \downarrow \\
\mathcal{Z}_1 = \{1, 2, 6\} & \mathcal{Z}_2 = \{1, 2, 5\} & \mathcal{Z}_3 = \{1, 2, 4\} \\
\widetilde{\mathcal{Z}}_1 = 1 & \widetilde{\mathcal{Z}}_2 = \{1\} & \widetilde{\mathcal{Z}}_3 = \{1\} \\
\underline{h}_1 = (0, 1, \infty, \infty, \infty, 1) & \underline{h}_2 = (0, 2, \infty, \infty, 1, \infty) & \underline{h}_3 = (0, 2, \infty, 3, \infty, \infty)
\end{array}
$$

$$
\begin{array}{ccc}
C_4 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = t \\ x_4 = t^6 \\ x_5 = 0 \\ x_6 = 0 \end{cases} & C_5 \equiv \begin{cases} x_1 = 1 \\ x_2 = 0 \\ x_3 = t \\ x_4 = 0 \\ x_5 = t^2 \\ x_6 = t^4 \end{cases} & C_6 \equiv \begin{cases} x_1 = -1 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = t^3 \\ x_5 = 0 \\ x_6 = t^2 \end{cases} \\
\downarrow & \downarrow & \downarrow \\
\mathcal{Z}_4 = \{3,4\} & \mathcal{Z}_5 = \{1,3,5,6\} & \mathcal{Z}_6 = \{1,4,6\} \\
\widetilde{\mathcal{Z}}_4 = \emptyset & \widetilde{\mathcal{Z}}_5 = \{1\} & \widetilde{\mathcal{Z}}_6 = \{1\} \\
\underline{h}_4 = (\infty,\infty,1,6,\infty,\infty) & \underline{h}_5 = (0,\infty,1,\infty,2,4) & \underline{h}_6 = (0,\infty,\infty,3,\infty,2)
\end{array}
$$

Siguiendo los pasos del Algoritmo 3.4.8 calculamos $\mathcal{Z} = \{1,\dots,6\} \setminus \bigcup_{i=1}^{6} \widetilde{\mathcal{Z}}_i = \{2,3,4,5,6\}$ y construimos los vectores

$$
\begin{array}{lll}
\underline{h}_1^* = (\infty,1,\infty,\infty,\infty,1) & \underline{h}_2^* = (\infty,2,\infty,\infty,1,\infty) & \underline{h}_3^* = (\infty,2,\infty,3,\infty,\infty) \\
\underline{h}_4^* = (\infty,\infty,1,6,\infty,\infty) & \underline{h}_5^* = (\infty,\infty,1,\infty,2,4) & \underline{h}_6^* = (\infty,\infty,\infty,3,\infty,2)
\end{array}
$$

y les aplicamos el Algoritmo 3.4.3. Usando el método de la Proposición 3.3.8 calculamos:

- el vector $\underline{h}^1 = (\infty,2,\infty,3,1,2)$ que es proporcional a $\underline{h}_1^*$, $\underline{h}_2^*$ y $\underline{h}_3^*$,
- el vector $\underline{h}^2 = (\infty,\infty,1,6,2,4)$ que es proporcional a $\underline{h}_4^*$ y $\underline{h}_5^*$,
- y el vector $\underline{h}_3 = (\infty,\infty,\infty,3,\infty,2)$ que es proporcional a $\underline{h}_6^*$.

Repitiendo el procedimiento descrito en la Proposición 3.3.8, ahora con los vectores $\underline{h}^1$, $\underline{h}^2$ y $\underline{h}^3$, se calcula el vector $\underline{h}^* = (\infty,4,1,6,2,4)$ que es proporcional a dichos vectores. Por lo tanto el vector $\underline{a} = (0,4,1,6,2,4)$ es el vector de coeficientes de un campo de Euler tangente a C.

Capítulo 4

k-álgebras de curvas monomiales

La k-álgebra asociada a una curva monomial irreducible C es del tipo $k[S]$, siendo S el semigrupo numérico asociado a C. Esta estructura facilita el trabajo de calcular efectivamente la resolución libre minimal del ideal de la curva, pues lo convierte en un problema combinatorio. La estructura S-homogénea del álgebra y del ideal son esenciales para ello ([CG]).

El objetivo de este capítulo es extender en lo posible dicha construcción al caso general, encontrando un semigrupo S asociado a una curva monomial C, de forma que el ideal de la curva resulte S-homogéneo y la k-álgebra de la curva sea algo aproximado a $k[S]$.

4.1 Semigrupos y graduaciones

Para comenzar veamos algunos aspectos generales acerca de los semigrupos y de las k-álgebras de semigrupos ([BCMP1]).

Sea S un semigrupo conmutativo y con elemento neutro. Denotaremos por 0 a dicho elemento.

Definición 4.1.1 *Se dice que S es cancelativo si para todos g_1, g_2 y $g \in S$ tales que $g_1 + g = g_2 + g$ se tiene $g_1 = g_2$.*

Definición 4.1.2 *Sea S un semigrupo cancelativo. Se dice que S es combinatoriamente finito si cumple que $S \cap (-S) = \{0\}$.*

Proposición 4.1.3 *Sea S un semigrupo conmutativo, cancelativo y con elemento neutro, 0. Entonces S es combinatoriamente finito si y sólo si no existen $g_1, \ldots, g_r \in S \setminus \{0\}$ tales que $0 = g_1 + \ldots + g_r$.*

Dem. Supongamos que S es combinatoriamente finito. Si existen $g_1, \ldots, g_r \in S \setminus \{0\}$ tales que $0 = g_1 + \ldots + g_r$, entonces $r \geq 2$ y se tiene que $-g_1 = g_2 + \ldots + g_r$. Luego $-g_1 \in S \cap (-S)$ y $-g_1 \neq 0$, en contra de que S es combinatoriamente finito.

Recíprocamente, si S no es combinatoriamente finito entonces existe $g \in S \cap (-S)$ tal que $g \neq 0$. Luego $g, -g \in S$ y $0 = g + (-g)$.

□

Nota 4.1.4 En lo que sigue, todos los semigrupos se consideraran conmutativos y con elemento neutro, aunque no se especifique.

4.1.1 Semigrupos y retículos

Como dijimos al comienzo del capítulo, nuestro objetivo es construir un semigrupo asociado a cada curva monomial. Para establecer esta conexión entre semigrupos y curvas monomiales utilizaremos los retículos asociados a curvas monomiales, estudiadas en el capítulo 2, y la relación entre retículos y semigrupos que veremos a continuación.

Definición 4.1.5 *Dados dos semigrupos cancelativos S y S^*, un sistema de generadores de S, $\Lambda = \{g_1, \ldots, g_n\}$ y un sistema de generadores de S^*, $\Lambda^* = \{g_1^*, \ldots, g_n^*\}$, diremos que (S, Λ) y (S^*, Λ^*) son isomorfos si existe un isomorfismo de semigrupos $\omega : S \to S^*$ cumpliendo $\omega(g_i) = g_i^*$ para todo $i \in \{1, \ldots, n\}$.*

Sea S un semigrupo combinatoriamente finito y finitamente generado, y fijemos un sistema de generadores $\Lambda = \{g_1, \ldots, g_n\}$ para S. Denotemos por $G(S)$ el grupo de Grothendieck de S, es decir, el grupo conmutativo con la propiedad universal respecto de los homomorfismos de S en grupos conmutativos ([Lan]). Como S es cancelativo, S se puede identificar con un subsemigrupo de $G(S)$, y se tiene un homomorfismo sobreyectivo de grupos,

$$\begin{aligned} \phi : \mathbb{Z}^n &\to G(S) \\ \underline{e}_i &\mapsto g_i \end{aligned},$$

siendo $\{\underline{e}_i \mid 1 \leq i \leq n\}$ la base canónica de $\mathbb{Z}^n$. Utilizando este homomorfismo ϕ, que depende del semigrupo S y del sistema de generadores $\Lambda = \{g_1, \ldots, g_n\}$, vamos a definir el retículo asociado a (S, Λ).

Definición 4.1.6 *Sea S un semigrupo cancelativo y finitamente generado y consideremos un sistema de generadores de S, $\Lambda = \{g_1, \ldots , g_n\}$. Llamaremos retículo asociado al par (S, Λ) al $\mathbb{Z}$-módulo libre $L_{S,\Lambda} = \ker(\phi)$, siendo ϕ el homomorfismo de grupos*

$$\begin{array}{c} \phi : \mathbb{Z}^n \to G(S) \\ \underline{e}_i \mapsto g_i \end{array}.$$

Es decir $L_{S,\Lambda} = \{\underline{m} = (m_1, \ldots , m_n) \in \mathbb{Z}^n \mid \sum_{i=1}^{n} m_i g_i = 0\}$.

Veamos que los retículos asociados a pares isomorfos coinciden.

Proposición 4.1.7 *Consideremos un semigrupo S con sistema de generadores $\Lambda = \{g_1, \ldots , g_n\}$ y un semigrupo S^* con sistema de generadores $\Lambda^* = \{g_1^*, \ldots , g_n^*\}$. Si (S, Λ) y (S^*, Λ^*) son isomorfos, entonces $L_{S,\Lambda} = L_{S^*,\Lambda^*}$.*

Dem. En las condiciones del enunciado, existe un isomorfimo de semigrupos $\omega : S \to S^*$ cumpliendo $\omega(g_i) = g_i^*$ para todo $i \in \{1, \ldots , n\}$. Este isomorfismo se prolonga, de forma natural, a un isomorfismo de grupos $\omega : G(S) \to G(S^*)$. Consideremos las aplicaciones

$$\begin{array}{rcl} \phi : \mathbb{Z}^n : & \longrightarrow & G(S) \\ \underline{m} & \longmapsto & \sum_i m_i g_i \end{array} \qquad \begin{array}{rcl} \phi^* : \mathbb{Z}^n : & \longrightarrow & G(S^*) \\ \underline{m} & \longmapsto & \sum_i m_i g_i^* \end{array}.$$

Es claro que $\omega \circ \phi = \phi^*$, luego $\ker(\phi) = \ker(\phi^*)$.

□

Corolario 4.1.8 *En particular, si $\Lambda = \{g_1, \ldots , g_n\}$ y $\Lambda^* = \{g_1^*, \ldots , g_n^*\}$ son dos sistemas de generadores del semigrupo S, entonces $L_{S,\Lambda} = L_{S,\Lambda^*}$.*

La condición para que un semigrupo S sea combinatoriamente finito (que no es necesaria para la construcción de $L_{S,\Lambda}$), se puede interpretar en términos de $L_{S,\Lambda}$.

Proposición 4.1.9 *Sean S un semigrupo cancelativo y finitamente generado, $\Lambda = \{g_1, \ldots , g_n\}$ un sistema de generadores de S formado por elementos no nulos y $L_{S,\Lambda}$ el retículo asociado a (S, Λ). Entonces S es combinatoriamente finito si y sólo si $L_{S,\Lambda} \cap (\mathbb{Z}_{\geq 0})^n = \langle \underline{0} \rangle$.*

Dem. Si $L_{S,\Lambda} \cap (\mathbb{Z}_{\geq 0})^n \neq \langle \underline{0} \rangle$, entonces existe $(a_1, \ldots, a_n) \in L_{S,\Lambda}$ tal que $a_i \geq 0$ para todo i y $a_j > 0$ para algún $j \in \{1, \ldots, n\}$. Por tanto, $a_i g_i \in S$ para todo i, y, como $L_{S,\Lambda} = \ker(\phi)$, entonces $a_1 g_1 + \ldots + a_n g_n = 0$. Pero estamos suponiendo que $g_i \neq 0$ para todo i, en particular $g_j \neq 0$, luego $a_1 g_1 + \ldots + a_n g_n = 0$ es una expresión del 0 como suma de elementos no nulos de S, y por la Proposición 4.1.3, S no es combinatoriamente finito.

Recíprocamente, supongamos que $L_{S,\Lambda} \cap (\mathbb{Z}_{\geq 0})^n = \langle \underline{0} \rangle$. Si $g \in S \cap (-S)$, entonces existen $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0}$ y $b_1, \ldots, b_n \in \mathbb{Z}_{\leq 0}$ cumpliendo $g = a_1 g_1 + \ldots + a_n g_n = b_1 g_1 + \ldots + b_n g_n$. El vector $\underline{v} = (a_1 - b_1, \ldots, a_n - b_n) \in (\mathbb{Z}_{\geq 0})^n$ y cumple que $\phi(\underline{v}) = g - g = 0$, luego $\underline{v} \in L_{S,\Lambda}$. Como estamos suponiendo que $L_{S,\Lambda} \cap (\mathbb{Z}_{\geq 0})^n = \langle \underline{0} \rangle$ entonces $\underline{v} = \underline{0}$, es decir, $g = 0$, y resulta $S \cap (-S) = \{0\}$. □

Si permitimos generadores nulos y suponemos que S es combinatoriamente finito, entonces la condición que deducimos para el retículo $L_{S,\Lambda}$ es más débil.

Proposición 4.1.10 *Sea $S \neq \{0\}$ un semigrupo cancelativo y finitamente generado. Si $\Lambda = \{g_1, \ldots, g_n\}$ un sistema de generadores de S, salvo reordenación, existe un $r \in \{1, \ldots, n\}$ tal que $g_i = 0$ si y sólo si $i > r$. Entonces, si $\widetilde{\Lambda} = \{g_1, \ldots, g_r\}$, se tiene $L_{S,\Lambda} = L_{S,\widetilde{\Lambda}} \times \mathbb{Z}^{n-r}$ y $L_{S,\widetilde{\Lambda}} \cap (\mathbb{Z}_{\geq 0})^r = \langle \underline{0} \rangle$.*

Dem. Esencialmente igual que la demostración de la proposición anterior. □

En lo que sigue consideraremos subretículos L de $\mathbb{Z}^n$, de uno de estos dos tipos:

Tipo 1 rango$(L) = n - 1$ y existe $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ tal que Sat $L = \langle \underline{h} \rangle^{\perp}$ $(n > 0)$.

Tipo 2 rango$(L) = n$ $(n \geq 0)$.

En cada uno de estos casos vamos a construir un semigrupo asociado al retículo L.

Tipo 1

Sea L un subretículo de $\mathbb{Z}^n$ de rango $n - 1$ y tal que existe $\underline{h} \in \mathbb{Z}^n_{\geq 0}$, no nulo, de forma que Sat $L = \langle \underline{h} \rangle^{\perp}$. Elegimos $\underline{h}$ de forma que m.c.d.$\{h_i \mid h_i \neq 0\} = 1$. Dado un vector $\underline{\alpha} \in \mathbb{Z}^n$ cumpliendo que $\underline{h}\,\underline{\alpha} = 1$, se considera el homomorfismo de grupos:

$$\begin{array}{rcl} \varphi_{\underline{\alpha}} : \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \oplus \mathrm{Sat}\ L \\ \underline{m} & \longmapsto & (\underline{m}\,\underline{h}, \underline{m} - (\underline{m}\,\underline{h})\underline{\alpha}) \end{array} .$$

Proposición 4.1.11 *El homomorfismo $\varphi_{\underline{\alpha}}$ es un isomorfismo entre $\mathbb{Z}^n$ y $\mathbb{Z} \oplus \mathrm{Sat}\ L$.*

Dem. Consideremos el homomorfismo de grupos, $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ definido por $\psi(\underline{m}) = \underline{m}\,\underline{h}$. Es caro que $\ker(\psi) = \mathrm{Sat}\ L$. Si ahora consideramos el homomorfismo $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}^n$ donde $\phi(a) = a\underline{\alpha}$, entonces $\psi \circ \phi = \mathrm{Id}_{\mathbb{Z}}$, luego la sucesión exacta $0 \to \mathrm{Sat}\ L \to \mathbb{Z}^n \xrightarrow{\psi} \mathbb{Z} \to 0$ es escindida. Por lo tanto, el homomorfismo $\varphi_{\underline{\alpha}} : \mathbb{Z}^n \to \mathbb{Z} \oplus \mathrm{Sat}\ L$ dado por $\varphi_{\underline{\alpha}}(\underline{m}) = (\psi(\underline{m}), \underline{m} - \phi(\psi(\underline{m}))) = (\underline{m}\,\underline{h}, \underline{m} - (\underline{m}\,\underline{h})\underline{\alpha})$ es isomorfismo.

□

Sea $\overline{\varphi}_{\underline{\alpha}}$ la composición de $\varphi_{\underline{\alpha}}$ con el paso al cociente módulo L,

$$\begin{array}{rcl} \overline{\varphi}_{\underline{\alpha}} : \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \oplus \mathrm{Sat}\ L/L \\ \underline{m} & \longmapsto & (\underline{m}\,\underline{h}, \underline{m} - (\underline{m}\,\underline{h})\underline{\alpha} + L) \end{array} .$$

Es claro que, para $\underline{m}, \underline{n} \in \mathbb{Z}^n$, se tiene

$$\overline{\varphi}_{\underline{\alpha}}(\underline{m}) = \overline{\varphi}_{\underline{\alpha}}(\underline{n}) \Leftrightarrow \underline{m} - \underline{n} \in L. \tag{4.1}$$

En particular, $L = \ker(\overline{\varphi}_{\underline{\alpha}})$.

Definición 4.1.12 *Sean $\underline{h} \in \mathbb{Z}^n_{\geq 0}$ un vector no nulo tal que* $\mathrm{m.c.d.}\{h_i \mid h_i \neq 0\} = 1$*, L un subretículo de $\mathbb{Z}^n$ de rango $n-1$ tal que* $\mathrm{Sat}\ L = \langle \underline{h} \rangle^{\perp}$ *y $\underline{\alpha} \in \mathbb{Z}^n$ tal que $\underline{h}\,\underline{\alpha} = 1$. Consideremos el homomorfismo,*

$$\begin{array}{rcl} \overline{\varphi} : \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \oplus \mathrm{Sat}\ L/L \\ \underline{m} & \longmapsto & (\underline{m}\,\underline{h}, \underline{m} - (\underline{m}\,\underline{h})\underline{\alpha} + L) \end{array} .$$

Sea $\{\underline{e}_i\}_{i=1}^n$ la base canónica de $\mathbb{Z}^n$. Llamaremos semigrupo asociado a L al semigrupo $S_L = \overline{\varphi}((\mathbb{Z}_{\geq 0})^n)$. Denotaremos por Λ_L al sistema de generadores de S_L, $\Lambda_L = \{g_1, \ldots, g_n\}$ siendo $g_i := \overline{\varphi}(\underline{e}_i)$ para todo i.

Notación 4.1.13 Para cada $i \in \{1, \ldots, n\}$ denotaremos $g_i = (h_i, t(g_i))$, donde $t(g_i) = \underline{e}_i - h_i\underline{\alpha} + L \in \mathrm{Sat}\ L/L$ hace referencia a la parte de torsión.

El homomorfismo $\overline{\varphi}$, de la Definición 4.1.12, depende de la elección de un vector $\underline{\alpha}$ tal que $\underline{h}\,\underline{\alpha} = 1$. Veamos qué variación se produce en el semigrupo S_L al cambiar la elección de $\underline{\alpha}$.

Proposición 4.1.14 *Sean $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ un vector no nulo y $L \subset \mathbb{Z}^n$ un retículo de rango $n-1$ tal que* Sat $L = \langle \underline{h} \rangle^{\perp}$. *Se consideran vectores $\underline{\alpha}$ y $\underline{\alpha}^*$ de $\mathbb{Z}^n$ tales que $\underline{h}\,\underline{\alpha} = 1$ y $\underline{h}\,\underline{\alpha}^* = 1$. Se construyen, como en la definición anterior, (S_L, Λ) asociado a $\underline{\alpha}$ y (S_L^*, Λ^*) asociado a $\underline{\alpha}^*$. Entonces (S_L, Λ) y (S_L^*, Λ^*) son isomorfos.*

Dem. Como indica el enunciado,

$$\begin{aligned} S_L &= \overline{\varphi}_{\underline{\alpha}}(\mathbb{Z}^n_{\geq 0}) \subset \mathbb{Z} \oplus \mathrm{Sat}\ L/L \\ S_L^* &= \overline{\varphi}_{\underline{\alpha}^*}(\mathbb{Z}^n_{\geq 0}) \subset \mathbb{Z} \oplus \mathrm{Sat}\ L/L\ . \end{aligned}$$

Definamos $\omega : S_L \longrightarrow S_L^*$ dada por,

$$\omega(\overline{\varphi}_{\underline{\alpha}}(\underline{m})) = \overline{\varphi}_{\underline{\alpha}^*}(\underline{m}).$$

Puesto que

$$\overline{\varphi}_{\underline{\alpha}}(\underline{m}) = \overline{\varphi}_{\underline{\alpha}}(\underline{n}) \Leftrightarrow \underline{m} - \underline{n} \in L \Leftrightarrow \overline{\varphi}_{\underline{\alpha}^*}(\underline{m}) = \overline{\varphi}_{\underline{\alpha}^*}(\underline{n})\ ,$$

ω está bien definida y es un isomorfismo de semigrupos. Además $\omega(\overline{\varphi}_{\underline{\alpha}}(\underline{e}_i)) = \overline{\varphi}_{\underline{\alpha}^*}(\underline{e}_i)$ para todo $i \in \{1, \ldots, n\}$. Luego (S_L, Λ) y (S_L^*, Λ^*) son isomorfos.

□

Según la Definición 4.1.12, el semigrupo S_L es cancelativo (ya que es subsemigrupo de un grupo). Por lo tanto tiene sentido hablar de su retículo asociado. Veamos que este es el propio L.

Proposición 4.1.15 *Sea L un retículo de $\mathbb{Z}^n$ de rango $n-1$ y tal que existe $\underline{h} \in (\mathbb{Z}_{\geq 0})^n$ con* Sat $L = \langle \underline{h} \rangle^{\perp}$. *Consideremos el semigrupo asociado a L, S_L, con sistema de generadores Λ_L. Entonces, el retículo asociado al par (S_L, Λ_L) es L.*

Dem. Como $G(S_L) \subseteq \mathbb{Z} \oplus \mathrm{Sat}\ L/L$ y $\Lambda_L = \{\overline{\varphi}(\underline{e}_1), \ldots, \overline{\varphi}(\underline{e}_n)\}$, entonces el retículo asociado a (S_L, Λ_L) es el núcleo del homomorfismo $\overline{\varphi}$ que, como ya hemos visto, es L.

□

Tipo 2

Sea ahora L un subretículo de $\mathbb{Z}^n$ de rango $n \geq 0$. En este caso denotaremos por $\overline{\varphi}$ el homomorfismo de grupos $\overline{\varphi} : \mathbb{Z}^n \to \mathbb{Z}^n/L$ (aplicación de paso al cociente módulo L). Según esta definición, para $\underline{m}, \underline{n} \in \mathbb{Z}^n$

$$\overline{\varphi}(\underline{m}) = \overline{\varphi}(\underline{n}) \Leftrightarrow \underline{m} - \underline{n} \in L. \tag{4.2}$$

Definición 4.1.16 *Sean L un subretículo de $\mathbb{Z}^n$ de rango n y $\overline{\varphi} : \mathbb{Z}^n \to \mathbb{Z}^n/L$ la aplicación de paso al cociente módulo L. Llamaremos semigrupo asociado a L al semigrupo $S_L = \overline{\varphi}((\mathbb{Z}_{\geq 0})^n)$. Denotaremos por Λ_L al sistema de generadores de S_L, $\Lambda_L = \{g_1, \ldots, g_n\}$ siendo $g_i := \overline{\varphi}(\underline{e}_i)$ y $\{\underline{e}_i\}_{i=1}^n$ la base canónica de $\mathbb{Z}^n$.*

Notación 4.1.17 Como en este caso $S_L \subset \mathbb{Z}^n/L$, sus elementos sólo tienen parte de torsión. Por lo tanto, denotaremos $t(g_i) := g_i$, para cada $i \in \{1, \ldots, n\}$.

El semigrupo S_L es cancelativo y, por tanto, tiene sentido construir su retículo asociado que, como veremos a continuación, coincide con L.

Proposición 4.1.18 *Sea L un subretículo de $\mathbb{Z}^n$ de rango n. Consideremos el semigrupo S_L y el sistema de generadores Λ_L, definidos en 4.1.16. Entonces el retículo asociado a (S_L, Λ_L) es L.*

Dem. Consecuencia directa de la definición de S_L y Λ_L.

□

Nota 4.1.19 Para el caso especial $n = 0$, el retículo resulta $L = \langle 0 \rangle = \mathbb{Z}^{\emptyset}$, y su semigrupo asociado es $S_L = \{0\}$.

Por último, veamos un resultado válido para los semigrupos asociados a retículos de cualquiera de los dos tipos. Este resultado será utilizado en desarrollos teóricos posteriores.

Proposición 4.1.20 *Sea L un subretículo de $\mathbb{Z}^n$ de tipo 1 o tipo 2 y consideremos el semigrupo asociado a L, $S_L = \overline{\varphi}((\mathbb{Z}_{\geq 0})^n)$. Si $\underline{m}, \underline{n} \in (\mathbb{Z}_{\geq 0})^n$, $\gamma = \overline{\varphi}(\underline{m})$ y $\eta = \overline{\varphi}(\underline{n})$, entonces*

$$\gamma = \eta \Leftrightarrow \underline{m} - \underline{n} \in L \ .$$

Dem. Consecuencia de las ecuaciones (4.1) y (4.2).

□

4.1.2 S-Graduaciones

Para entender los isomorfismos que estableceremos en la siguiente sección, es necesario conocer el significado de los anillos, los módulos y los homomorfismos S-graduados.

k-álgebra k[S]

Sea S un semigrupo conmutativo con elemento neutro. Se define $k[S]$ como el conjunto de las aplicaciones $\alpha : S \to k$ tales que $\alpha(g) = 0$ salvo para un número finito de elementos g del semigrupo. El conjunto $k[S]$ tiene una estructura natural de k-algebra con el producto $(\alpha\beta)(g) = \sum\limits_{g_1+g_2=g} \alpha(g_1)\beta(g_2)$. Si denotamos por χ^g a la aplicación

$$\chi^g(g') = \begin{cases} 1 & \text{si } g' = g \\ 0 & \text{si } g' \neq g \end{cases},$$

cada elemento α de $k[S]$ se escribe de forma única como

$$\alpha = \sum_{g\in S} \lambda_g \chi^g, \qquad \text{siendo } \lambda_g = \alpha(\chi^g) \text{ para todo } g \in S.$$

Por lo tanto, $k[S] = \bigoplus_{g\in S} k\chi^g$ y $\sum_{g\in S} \lambda_g\chi^g = 0$ si y sólo si $\lambda_g = 0$ para todo $g \in S$. Además, $\chi^g\chi^{g'} = \chi^{g+g'}$ y $\chi^0 = 1$. De aquí en adelante, utilizaremos la expresión formal $\alpha = \sum_{g\in S} \lambda_g\chi^g$ para trabajar con los elementos de $k[S]$.

Lema 4.1.21 *Consideremos semigrupos S y $\widetilde{S}$ con sistemas de generadores $\Lambda = \{g_1, \ldots, g_n\}$ y $\widetilde{\Lambda} = \langle \widetilde{g}_1, \ldots, \widetilde{g}_n\rangle$ respectivamente. Si $(S, \Lambda) \cong (\widetilde{S}, \widetilde{\Lambda})$, entonces existe un isomorfismo Ω entre las k-álgebras de semigrupo $k[S]$ y $k[\widetilde{S}]$ dado por $\Omega(\chi^{g_i}) = \chi^{\widetilde{g}_i}$.*

Dem. En las condiciones del enunciado, existe un isomorfismo de semigrupos $\omega : \widetilde{S} \to S$ tal que $\omega(\widetilde{g}_i) = g_i$ para todo i y por lo tanto Ω es un isomorfismo de k-álgebras.

$\square$

Estructura S-graduada

Sea ahora $A = \bigoplus_{g\in S} A_g$ un anillo S-graduado. Se dice que un elemento $f \in A$ es homogéneo de grado g cuando $f \in A_g$. Como $A = \bigoplus_{g\in S} A_g$ entonces cualquier elemento $f \in A$ se puede escribir de forma única como suma de elementos homogéneos, $f = \sum_{g\in S} f_g$, donde $f_g \in A_g$ y $f_g \neq 0$ para un número finito de elementos (se dice que f_g es la componente homogénea de f de grado g). Diremos que un ideal $I \subset A$ es homogéneo, cuando admite un sistema de generadores formado por elementos homogéneos. Además, si $M = \bigoplus_{g\in S} M_g$ un A-módulo S-graduado, entonces se dice que $m \in M$ es homogéneo de grado $g \in S$ cuando $m \in M_g$.

Sean $k[X] := k[X_1, \ldots, X_n]$ y $S = \langle g_1, \ldots, g_n \rangle$ un semigrupo. Podemos dotar al anillo $k[X]$ de estructura S-graduada asignando grado g_i a X_i. Es decir, para cada $g \in S$, $k[X]_g$ es el k-subespacio vectorial de $k[X]$ generado por $\{X_1^{a_1} \cdots X_n^{a_n} \mid \sum_{j=1}^n a_j g_j = g\}$.

Definición 4.1.22 *Sean A y B dos anillos S-graduados, $f : A \to B$ un homomorfismo de anillos y $g_0 \in S$. Se dice que f es S-homogéneo de grado g_0 si para todo $x_g \in A_g$ se cumple que $f(x_g) \in B_{g+g_0}$.*

Proposición 4.1.23 *Sean A y B dos anillos S-graduados. Si $f : A \to B$ es un homomorfismo S-graduado de grado 0, entonces $\ker(f)$ es un ideal S-homogéneo de A.*

Dem. Consideremos un elemento $x \in A$ tal que $f(x) = 0$. Escribamos $x = \sum_{g \in S} x_g$, entonces $\sum_{g \in S} f(x_g) = 0$. Pero f es un homomorfismo S-homogéneo de grado cero, luego $f(x_g)$ es homogéneo de grado g, luego $f(x_g) = 0$ para todo $g \in S$. Entonces $x_g \in \ker(f)$ para todo g y $\ker(f)$ es un ideal S-homogéneo.

$\square$

Nota 4.1.24 Si el semigrupo S es cancelativo, el resultado anterior también es cierto para homomorfismos S-graduados de grado distinto de cero.

4.2 Anillos de coordenadas de curvas monomiales como cocientes de k-álgebras de semigrupos

En esta sección construiremos un semigrupo S asociado a cada curva monomial, de forma que el ideal de la curva sea S-homogéneo. Comenzaremos estudiando lo que ocurre en el caso irreducible y en el caso en que todas las componentes de la curva tienen la misma célula asociada. El estudio de estos dos casos particulares permitirá entender mejor la construcción en el caso general, construcción que pasa por considerar una descomposición celular del ideal de la curva.

Para el caso de única célula, el semigrupo que asignaremos a la curva C es cancelativo, combinatoriamente finito y finitamente generado. Por lo tanto podemos utilizar el método desarrollado en [CG] para el cálculo de una resolución libre minimal finita S-graduada de $\mathcal{I}(C)$.

Para comenzar, veamos un resultado fundamental en la justificación de los isomorfismos que vamos a construir. Como venimos haciendo, escribiremos $k[X]$ para denotar el anillo $k[X_1, \ldots, X_n]$.

Proposición 4.2.1 *Sean S un semigrupo cancelativo y finitamente generado y $\Lambda = \{g_1, \ldots, g_n\}$ un sistema de generadores de S. Fijado un vector $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in (k^*)^n$, se define el homomorfismo*

$$\begin{array}{rcl} \phi : k[X] & \longrightarrow & k[S] \\ X_i & \longmapsto & \lambda_i \chi^{g_i}. \end{array}$$

Entonces, $\ker(\phi) = I_+(\rho)$*, donde L es el retículo asociado a S y $\rho : L \to k^*$ es el carácter parcial dado por $\rho(\underline{m}) = \underline{\lambda}^{\underline{m}}$.*

Dem. Sea $\underline{m} \in L$. Denotemos por $\underline{m}\,\underline{g}$ al elemento $\sum_{i=1}^n m_i g_i \in S$. Como L es el retículo asociado a S, entonces $\underline{m}\,\underline{g} = 0$ (Definición 4.1.6), luego $\underline{m}_+\,\underline{g} = \underline{m}_-\,\underline{g}$. Por lo tanto,

$$\phi(X^{\underline{m}_+} - \rho(\underline{m})X^{\underline{m}_-}) = \underline{\lambda}^{\underline{m}_+}\chi^{\underline{m}_+\,\underline{g}} - \rho(\underline{m})\lambda^{\underline{m}_-}\chi^{\underline{m}_-\,\underline{g}} = (\underline{\lambda}^{\underline{m}_+} - \rho(\underline{m})\underline{\lambda}^{\underline{m}_-})\chi^{\underline{m}_+\,\underline{g}}\ .$$

Por definición de ρ, $(\underline{\lambda}^{\underline{m}_+} - \rho(\underline{m})\underline{\lambda}^{\underline{m}_-}) = 0$. Por lo tanto, $I_+(\rho) \subseteq \ker(\phi)$.

Para demostrar la otra contención, consideremos la estructura S-graduada de $k[X]$, obtenida al dar, para cada i, grado g_i a X_i. Esto convierte a ϕ en un homomorfismo S-graduado de grado cero, luego $\ker(\phi)$ es un ideal S-homogéneo (Proposición 4.1.23), y para ver que $\ker(\phi) \subseteq I_+(\rho)$ basta considerar los elementos homogéneos de $\ker(\phi)$. Consideremos un polinomio $f \in \ker(\phi)$ que sea S-homogéneo de grado $\gamma \in S$. Entonces $f = a_{\underline{s}_1}X^{\underline{s}_1} + \ldots + a_{\underline{s}_t}X^{\underline{s}_t}$ donde para cada $j \in \{1, \ldots, t\}$, $a_{\underline{s}_j} \in k$, $\underline{s}_j \in (\mathbb{Z}_{\geq 0})^n$ y $\underline{s}_j\,\underline{g} = \gamma$. Puesto que $f \in \ker(\phi)$,

$$f = \sum_{i=1}^{t-1}(a_{\underline{s}_1}\underline{\lambda}^{\underline{s}_1} + \ldots + a_{\underline{s}_i}\underline{\lambda}^{\underline{s}_i})\left(\frac{1}{\underline{\lambda}^{\underline{s}_i}}X^{\underline{s}_i} - \frac{1}{\underline{\lambda}^{\underline{s}_{i+1}}}X^{\underline{s}_{i+1}}\right).$$

Como L es el retículo asociado a S y $\underline{s}_i\,\underline{g} = \underline{s}_{i+1}\,\underline{g}$ entonces $\underline{s}_{i+1} - \underline{s}_i \in L$. Además, por la definición de ρ, $\rho(\underline{s}_{i+1} - \underline{s}_i) = \frac{\underline{\lambda}^{\underline{s}_{i+1}}}{\underline{\lambda}^{\underline{s}_i}}$. Como

$$\frac{1}{\underline{\lambda}^{\underline{s}_i}}X^{\underline{s}_i} - \frac{1}{\underline{\lambda}^{\underline{s}_{i+1}}}X^{\underline{s}_{i+1}} = -\frac{1}{\underline{\lambda}^{\underline{s}_{i+1}}}(X^{\underline{s}_{i+1}} - \rho(\underline{s}_{i+1} - \underline{s}_i)X^{\underline{s}_i}),$$

entonces $\frac{1}{\underline{\lambda}^{\underline{s}_i}}X^{\underline{s}_i} - \frac{1}{\underline{\lambda}^{\underline{s}_{i+1}}}X^{\underline{s}_{i+1}} \in I_+(\rho)$, para todo i, y $f \in I_+(\rho)$.

$\square$

Corolario 4.2.2 *Sea L un subretículo de $\mathbb{Z}^{\mathcal{Z}}$, bien de rango $|\mathcal{Z}|-1$ y tal que existe $\underline{h} \in (\mathbb{Z}_{\geq 0})^{\mathcal{Z}}$ tal que* Sat $L = \langle \underline{h} \rangle^\perp$*, bien de rango $|\mathcal{Z}|$. Consideremos un vector $\underline{\lambda} \in (k^*)^{\mathcal{Z}}$ y el carácter parcial $\rho : L \to k^*$ dado por $\rho(\underline{m}) = \underline{\lambda}^{\underline{m}}$.*

Si $(S, \Lambda = \{g_1, \dots, g_n\})$ *es el semigrupo asociado a* L *según las Definiciones 4.1.12 o 4.1.16 (según el caso), entonces* $I = I_+(\rho) + M(\mathcal{Z})$ *es el núcleo del homomorfismo*

$$\begin{array}{rcl} \phi : k[X] & \longrightarrow & k[S] \\ X_i & \longmapsto & \lambda_i \chi^{g_i} \ \ si\ i \in \mathcal{Z} \\ X_i & \longmapsto & 0 \ \ si\ i \notin \mathcal{Z} \ . \end{array}$$

Dem. Teniendo en cuenta que L es el retículo asociado a (S, Λ) (Proposición 4.1.15), el resultado se deduce de la proposición anterior.

□

4.2.1 Caso irreducible

Sea $C \subset \mathcal{A}^n(k)$ una curva monomial irreducible con célula asociada $\mathcal{Z}$ y sean $(\underline{h}, \underline{\lambda})$ los vectores de una parametrización monomial de C. Es decir,

$$C \equiv \left\{ \begin{array}{c} X_1 = \lambda_1 t^{h_1} \\ \vdots \\ X_n = \lambda_n t^{h_n} \end{array} \right. .$$

Recordemos que $\mathcal{Z} = \{i \in \{1, \dots, n\} \mid \lambda_i \neq 0\}$ y el vector de exponentes $\underline{h}_{\mathcal{Z}}$ es independiente de la parametrización monomial elegida.

Definición 4.2.3 *Sea* C *una curva monomial irreducible con célula asociada* $\mathcal{Z}$ *y sea* $\underline{h}$ *su vector de exponentes. Llamaremos semigrupo asociado a la curva* C *al semigrupo numérico* S *generado por el conjunto* $\Lambda = \{h_i \mid i \in \mathcal{Z}\}$*, o por extensión, al par* (S, Λ)*.*

Nota 4.2.4 El semigrupo S asociado a una curva monomial irreducible C es un semigrupo numérico (es decir, $S \subseteq \mathbb{N}$), luego tiene las propiedades de ser cancelativo y combinatoriamente finito. Además, por construcción, es finitamente generado. Por lo tanto, cuando los elemento de Λ sean no nulos, podemos utilizar el método desarrollado en [CG] para el cálculo de una resolución libre minimal finita S-graduada de $\mathcal{I}(C)$. En el caso de aparecer algún generador nulo, el cálculo de las sicigeas se reduce también al caso de generadores no nulos, tras resolver un problema de tipo combinatorio.

Sea L_ρ el retículo asociado a C (Definición 2.1.7), es decir, el subretículo de $\mathbb{Z}^{\mathcal{Z}}$ dado por $L_\rho = \langle \underline{h}_{\mathcal{Z}} \rangle^\perp$. Recordemos que si consideramos el carácter parcial $\rho : L_\rho \to k^*$ dado por $\rho(\underline{m}) = \underline{\lambda}_{\mathcal{Z}}^{\underline{m}}$ para todo $\underline{m} \in L_\rho$, entonces $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$ (Proposición 2.1.6).

Lema 4.2.5 *Sea C un curva monomial irreducible con retículo asociado L_ρ y sean (S,Λ) el semigrupo asociado a C y $(S_{L_\rho},\Lambda_\rho)$ el asociado a L_ρ. Entonces $(S,\Lambda)\cong(S_{L_\rho},\Lambda_{L_\rho})$.*

Dem. Sea $\mathcal{Z}$ la célula asociada a C. Entonces $L_\rho=\langle \underline{h}_{\mathcal{Z}}\rangle^\perp$, donde $\underline{h}_{\mathcal{Z}}\in(\mathbb{Z}_{\geq 0})^{\mathcal{Z}}$ es el vector de exponentes de la curva C restringido a las coordenadas en $\mathcal{Z}$. Según la Definición 4.1.12, S_{L_ρ} es la imagen de $(\mathbb{Z}_{\geq 0})^n$ vía el homomorfismo,

$$\begin{array}{rcl}\overline{\varphi}:\mathbb{Z}^{\mathcal{Z}} & \longrightarrow & \mathbb{Z}\oplus L_\rho/L_\rho \\ \underline{m} & \longmapsto & (\underline{m}\,\underline{h}_{\mathcal{Z}},\overline{0})\end{array},$$

y $\Lambda_{L_\rho}=\{(h_i,\overline{0})\mid i\in\mathcal{Z}\}$.

Es claro que la proyección $\pi: S_{L_\rho}\longrightarrow S$ dada por $\pi(a,\overline{0})=a$, para todo $(a,\underline{0})\in S$, es un isomorfismo de semigrupos tal que $\pi(\Lambda_{L_\rho})=\Lambda$, luego $(S,\Lambda)\cong(S_{L_\rho},\Lambda_{L_\rho})$.

□

Proposición 4.2.6 *Sea C una curva monomial irreducible con célula asociada $\mathcal{Z}$, y sean $(\underline{h},\underline{\lambda})$ los vectores de una parametrización monomial de C. Si denotamos por S al semigrupo numérico asociado a C, y consideramos el homomorfismo*

$$\begin{array}{rcl}\phi:k[X] & \longrightarrow & k[S] \\ X_i & \longmapsto & \lambda_i\chi^{h_i}\ si\ i\in\mathcal{Z} \\ X_i & \longmapsto & 0\ si\ i\notin\mathcal{Z}\end{array},$$

entonces ϕ es sobreyectivo y $\ker(\phi)=\mathcal{I}(C)$.

Dem. Como $\Lambda=\{h_i\mid i\in\mathcal{Z}\}$ es un sistema de generadores de S, entonces, para todo $g\in S$, existen $a_i\in\mathbb{Z}_{\geq 0}$ tales que $g=\sum_{i\in\mathcal{Z}}a_ih_i$. Luego $\phi\left(\prod_{i\in\mathcal{Z}}\left(\frac{1}{\lambda_i}\right)^{a_i}X_i^{a_i}\right)=\chi^g$ y ϕ es sobreyectivo. Para ver que $\ker(\phi)=\mathcal{I}(C)$ basta aplicar la Proposición 4.2.1 y los Lemas 4.2.5 y 4.1.21.

□

Como consecuencia, se tiene el siguiente resultado:

Teorema 4.2.7 *Sea C una curva monomial irreducible y sea $I:=\mathcal{I}(C)$. Asociados a C consideramos su célula $\mathcal{Z}$, los vectores de una parametrización* *monomial de C, $(\underline{h}, \underline{\lambda})$, y el semigrupo $S = \langle \{h_i \mid i \in \mathcal{Z}\} \rangle$. Entonces el homomorfismo S-graduado de grado cero,*

$$\begin{array}{rcl} \phi : k[X]/I & \longrightarrow & k[S] \\ X_i + I & \longmapsto & \lambda_i \chi^{h_i} \ \mathit{si}\ i \in \mathcal{Z} \\ X_i + I & \longmapsto & 0 \ \mathit{si}\ i \notin \mathcal{Z} \end{array} ,$$

es un isomorfismo.

Nota 4.2.8 El isomorfismo planteado depende del vector de coeficientes de la parametrización. Como vimos en la Proposición 2.1.6, si $\rho : L_\rho \to k^*$ es el carácter parcial asociado a la curva monomial C con célula $\mathcal{Z}$, entonces $\underline{\lambda}$ es el vector de coeficientes de una parametrización monomial para C, si y sólo si $\underline{\lambda}_{\mathcal{Z}} \in \mathcal{V}(I(\rho))$ y $\lambda_i = 0$ para todo $i \notin \mathcal{Z}$. Por lo tanto, tomando distintos $\underline{\lambda}_{\mathcal{Z}} \in \mathcal{V}(I(\rho))$, obtendremos distintos isomorfismos.

Ejemplo 4.2.9 Consideremos, como en el Ejemplo 2.1.20, la curva monomial irreducible C dada por

$$C \equiv \begin{cases} x_1 = t \\ x_2 = 0 \\ x_3 = -4 \\ x_4 = 3t^2 \end{cases} ,$$

es decir, $\underline{h} = (1, \infty, 0, 2)$ y $\underline{\lambda} = (1, 0, -4, 3)$. El semigrupo asociado a C es $S = \mathbb{Z}_{\geq 0}$ y su sistema de generadores fijado es $\Lambda = \{1, 0, 2\}$. Aplicando el Teorema 4.2.7, se tiene el isomorfismo S-graduado

$$\begin{array}{rcl} \phi : k[X]/I & \longrightarrow & k[S] \\ X_1 + I & \longmapsto & \chi \\ X_2 + I & \longmapsto & 0 \\ X_3 + I & \longmapsto & -4 \\ X_4 + I & \longmapsto & 3\chi^2 \end{array} ,$$

donde I denota el ideal asociado a la curva C.

Además, si $\rho : L_\rho \to k^*$ es el carácter asociado a C, se tiene $L_\rho = \langle (-2, 1, 1), (-2, 0, 1) \rangle$, siendo $\rho(\underline{m}) = 1^{m_1}(-4)^{m_2} 3^{m_3}$, para todo $\underline{m} \in L_\rho$. Por lo tanto, si consideramos el vector de coeficientes $\widetilde{\underline{\lambda}}_{\mathcal{Z}} = (1/\sqrt{3}, -4, 1)$, resulta $\widetilde{\underline{\lambda}}_{\mathcal{Z}}^{\underline{m}} = \rho(\underline{m})$ para todo $\underline{m} \in L_\rho$, luego $\widetilde{\underline{\lambda}}_{\mathcal{Z}} \in \mathcal{V}(I(\rho))$ y el vector $\underline{\lambda}^* = (1/\sqrt{3}, 0, -4, 1)$ es el vector de coeficientes de otra parametrización monomial para C. Por lo tanto, aplicando el Teorema 4.2.7, obtenemos el isomorfismo S-graduado

$$\begin{array}{rcl} \phi^* : k[X]/I & \longrightarrow & k[S] \\ X_1 + I & \longmapsto & \frac{1}{\sqrt{3}}\chi \\ X_2 + I & \longmapsto & 0 \\ X_3 + I & \longmapsto & -4 \\ X_4 + I & \longmapsto & \chi^2 \end{array} .$$

4.2.2 Caso de una célula

Consideremos ahora una curva monomial $C = C_1 \cup \ldots \cup C_d$ tal que todas sus componentes tienen asociada la misma célula $\mathcal{Z} \subseteq \{1, \ldots , n\}$. Para cada $j \in \{1, \ldots , d\}$ denotemos por $(\underline{h}_j, \underline{\lambda}_j)$ los vectores de una parametrización monomial de la curva monomial irreducible C_j y por $C_{j,\mathcal{Z}}$ la curva monomial irreducible definida por la parametrización dada por los vectores $((\underline{h}_j)_{\mathcal{Z}}, (\underline{\lambda}_j)_{\mathcal{Z}})$. Consideremos la curva $C_{\mathcal{Z}} = \cup_{j=1}^{d} C_{j,\mathcal{Z}}$. Es claro que $\mathcal{I}(C) = \mathcal{I}(C_{\mathcal{Z}}) + M(\mathcal{Z})$. Además, como consecuencia del apartado D1 del Teorema 2.2.33, la curva $C_{\mathcal{Z}}$ es monomial y $(\underline{h}_j)_{\mathcal{Z}} = (\underline{h}_1)_{\mathcal{Z}}$ para todo $j \in \{2, \ldots , d\}$. Por lo tanto, si consideramos el retículo $L_\rho = \{\underline{m} \in \langle(\underline{h}_1)_{\mathcal{Z}}\rangle^\perp \mid (\underline{\lambda}_1)^{\underline{m}}_{\mathcal{Z}} = (\underline{\lambda}_j)^{\underline{m}}_{\mathcal{Z}}, \forall j \in \{2, \ldots , d\}\}$ y el carácter parcial $\rho : L_\rho \to k^*$ dado por $\rho(\underline{m}) = (\underline{\lambda}_1)^{\underline{m}}_{\mathcal{Z}}$, entonces $\mathcal{I}(C_{\mathcal{Z}}) = I_+(\rho)$ (Proposición 2.2.17). Recordemos que L_ρ es el retículo asociado a C (Definición 2.2.18).

Como L_ρ es un subretículo de $\mathbb{Z}^{\mathcal{Z}}$ de rango $|\mathcal{Z}|-1$ y cumple que Sat $L_\rho = \langle(\underline{h}_1)_{\mathcal{Z}}\rangle^\perp$, podemos construir el semigrupo S asociado a L_ρ, según la Definición 4.1.12, es decir; se elige $\underline{\alpha} \in (\mathbb{Z})^{\mathcal{Z}}$ tal que $\underline{\alpha}\, \underline{h}_{\mathcal{Z}} = 1$, y si $\overline{\varphi}$ es el homomorfismo

$$\begin{array}{rcl} \overline{\varphi} : \mathbb{Z}^{\mathcal{Z}} & \longrightarrow & \mathbb{Z} \oplus \text{Sat } L_\rho/L_\rho \\ \underline{m} & \longmapsto & (\underline{m}\, \underline{h}_{\mathcal{Z}}, \underline{m} - (\underline{m}\, \underline{h}_{\mathcal{Z}})\underline{\alpha} + L_\rho) \end{array} ,$$

entonces $S = \overline{\varphi}((\mathbb{Z}_{\geq 0})^{\mathcal{Z}})$ y el sistema de generadores fijado para S es $\Lambda = \{\overline{\varphi}(\underline{e}_i) \mid i \in \mathcal{Z}\}$ donde $\{\underline{e}_i \mid i \in \mathcal{Z}\}$ denota la base canónica de $\mathbb{Z}^{\mathcal{Z}}$.

Definición 4.2.10 *Sea C una curva monomial tal que todas sus componentes irreducibles tienen asociada la misma célula, $\mathcal{Z}$, y consideremos el retículo asociado a la curva C, L_ρ. Llamaremos semigrupo asociado a la curva C, al semigrupo asociado a L_ρ, es decir, al generado por $\Lambda = \{\overline{\varphi}(\underline{e}_i) \mid i \in \mathcal{Z}\}$, $S = \langle\Lambda\rangle$, o por extensión, al par (S, Λ).*

Teniendo en cuenta el Lema 4.2.5, es claro que en el caso irreducible, la definición anterior y la definición que dimos en 4.2.3 coinciden, salvo isomorfismo de semigrupos.

Notación 4.2.11 En lo que sigue escribiremos $g_i := \overline{\varphi}(\underline{e}_i)$ para denotar los elementos del sistema de generadores, Λ, del semigrupo asociado a C.

Proposición 4.2.12 *Sea C una curva monomial tal que todas sus componentes irreducibles tienen asociada la misma célula, $\mathcal{Z}$. Sean $\rho : L_\rho \to k^*$ el carácter parcial tal que $\mathcal{I}(C) = I_+(\rho) + M(\mathcal{Z})$, $S = \langle \{g_i \mid i \in \mathcal{Z}\} \rangle$ el semigrupo asociado a C y $\underline{\lambda} \in \mathcal{V}(I(\rho))$. Entonces, el homomorfismo*

$$\begin{array}{rcl} \phi : k[X] & \longrightarrow & k[S] \\ X_i & \longmapsto & \lambda_i \chi^{g_i} \ si \ i \in \mathcal{Z} \\ X_i & \longmapsto & 0 \ si \ i \notin \mathcal{Z} \end{array}$$

es sobreyectivo, y su núcleo es el ideal $\mathcal{I}(C)$.

Dem. Si $g \in S$, como Λ es un sistema de generadores de S, existen $\{a_i \mid i \in \mathcal{Z}\} \subset \mathbb{Z}_{\geq 0}$ tales que $g = \sum_{i \in \mathcal{Z}} a_i g_i$. Luego $\phi\left(\prod_{i\in\mathcal{Z}} \left(\frac{1}{\lambda_i^{a_i}}\right) X_i^{a_i}\right) = \chi^g$ y ϕ es sobreyectivo. Para ver que $\ker(\phi) = \mathcal{I}(C)$ basta aplicar el Corolario 4.2.2. $\square$

Teorema 4.2.13 *En las condiciones de la proposición anterior, el homomorfismo S-graduado de grado cero*

$$\begin{array}{rcl} \phi : k[X]/\mathcal{I}(C) & \longrightarrow & k[S] \\ X_i + \mathcal{I}(C) & \longmapsto & \lambda_i \chi^{g_i} \ si \ i \in \mathcal{Z} \\ X_i + \mathcal{I}(C) & \longmapsto & 0 \ si \ i \notin \mathcal{Z} \ , \end{array}$$

es un isomorfismo.

Veamos en un ejemplo como resulta el isomorfismo.

Ejemplo 4.2.14 Consideremos la curva monomial compleja del Ejemplo 2.3.8, $C = C_1 \cup C_2 \cup C_3 \cup C_4$, cuyas componentes tienen parametrizaciones:

$$C_1 \equiv \left\{ \begin{array}{l} x = t \\ y = 2t^2 \\ z = 8t^3 \end{array} \right. \quad C_2 \equiv \left\{ \begin{array}{l} x = t \\ y = 2It^2 \\ z = -8It^3 \end{array} \right. \quad C_3 \equiv \left\{ \begin{array}{l} x = t \\ y = -2t^2 \\ z = -8t^3 \end{array} \right. \quad C_4 \equiv \left\{ \begin{array}{l} x = t \\ y = -2It^2 \\ z = 8It^3 \end{array} \right.$$

Denotemos por L el retículo asociado a C. Entonces, $\{d_1 = 4, d_2 = 1\}$ son los factores invariantes de la extensión $L \subset \mathrm{Sat}\ L$, y el conjunto $\{\underline{m}_1 = (-2, 1, 0), \underline{m}_2 = (3, -3, 1)\}$ es una base de diagonalización.

Consideremos el isomorfismo $\Gamma := \mathbb{Z} \oplus \mathrm{Sat}\ L/L \to \mathbb{Z} \oplus \mathbb{Z}/(4)$ dado por $\Gamma(a, \underline{m}) = (a, \overline{\gamma}_1)$ donde $\underline{m} = \gamma_1 \underline{m}_1 + \gamma_2 \underline{m}_2$.

Para $\underline{\alpha} = (2, -2, 1)$, se tiene $\underline{\alpha}\,\underline{h} = 1$, y entonces el conjunto $\mathcal{B} = \{(2, -2, 1),\ (-2, 1, 0), (3, -3, 1)\}$ es una base de $\mathbb{Z}^3$. Calculando la matriz de cambio de base de la base canónica $\{\underline{e}_1, \underline{e}_2, \underline{e}_3\}$ en la base $\mathcal{B}$, resulta

$$\begin{pmatrix} 2 & -2 & 3 \\ -2 & 1 & -3 \\ 1 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ -1 & -1 & 0 \\ -1 & -2 & -2 \end{pmatrix}$$

Por lo tanto $\underline{e}_1 - 1\underline{\alpha} = -\underline{m}_1 - \underline{m}_2$, $\underline{e}_2 - 2\underline{\alpha} = -\underline{m}_1 - 2\underline{m}_2$ y $\underline{e}_3 - 3\underline{\alpha} = -2\underline{m}_2$. Luego $\Gamma(\overline{\varphi}(\underline{e}_1)) = (1, \overline{-1}) = (1, \overline{3})$, $\Gamma(\overline{\varphi}(\underline{e}_2)) = (2, \overline{-1}) = (2, \overline{3})$ y $\Gamma(\overline{\varphi}(\underline{e}_3)) = (3, \overline{0})$. Luego el semigrupo $S \subset \mathbb{Z} \oplus \mathbb{Z}/(4)$ generado por $g_1 = (1, \overline{3}), g_2 = (2, \overline{-1}) = (2, \overline{3})$ y $g_3 = (3, \overline{0})$ es isomorfo al semigrupo asociado a la curva C. Por lo tanto, aplicando el Lema 4.1.21 y el Teorema 4.2.13, si denotamos por I el ideal asociado a C, se tiene el isomorfismo

$$\begin{array}{rcl} \phi : k[\underline{X}]/I & \longrightarrow & k[S] \\ X + I & \longmapsto & 1\chi^{g_1} \\ Y + I & \longmapsto & 2\chi^{g_2} \\ Z + I & \longmapsto & 8\chi^{g_3} \end{array} .$$

Nota 4.2.15 Sea C una curva monomial cumpliendo que todas sus componentes tienen asociada la célula $\{1, \dots, n\}$, y cuyo vector de exponentes, $\underline{h}$, cumple que $h_i > 0$ para todo $i \in \{1, \dots, n\}$. Consideremos el retículo asociado a C, L, y el semigrupo asociado a C, S, con sistema de generadores $\Lambda = \{g_1, \dots, g_n\}$. Aplicando el Corolario 2.1.14, se tiene $(\mathrm{Sat}\ L) \cap (\mathbb{Z}_{\geq 0})^{\mathcal{Z}} = \langle \underline{0} \rangle$ y como $L \subset \mathrm{Sat}\ L$ entonces $L \cap (\mathbb{Z}_{\geq 0})^{\mathcal{Z}} = \langle \underline{0} \rangle$. Por la Proposición 4.1.15, L es el retículo asociado a (S, Λ), con lo cual podemos aplicar la Proposición 4.1.10 y obtenemos que S es combinatoriamente finito ($g_i = (h_i, t(g_i))$ para todo i, luego $g_i \neq 0$). Este es el motivo de haber escogido en la Definición 2.1.10 el nombre de "combinatoriamente finito" para hacer referencia a la condición combinatoria que cumplen los ideales asociados a curvas monomiales irreducibles.

Por lo tanto, tenemos un semigrupo conmutativo $S = \langle g_1, \dots, g_n \rangle$, que es cancelativo, combinatoriamente finito y finitamente generado, y un homomorfismo S-graduado de grado cero

$$\begin{array}{rcl} \phi : k[X] & \longrightarrow & k[S] \\ X_i & \longmapsto & \lambda_i \chi^{g_i} \end{array}$$

sobreyectivo y cuyo núcleo es el ideal $\mathcal{I}(C)$ (Proposición 4.2.12). En estas condiciones podemos utilizar el método desarrollado en [CG] para el cálculo de una resolución libre minimal S-graduada y finita de $\mathcal{I}(C)$.

Nota 4.2.16 En el caso en que la curva monomial C cumpla que todas sus componentes tienen asociada la misma célula $\mathcal{Z} \subsetneq \{1, \ldots, n\}$ y el vector de exponentes, $\underline{h}$, cumpla que $h_i > 0$ para todo $i \in \mathcal{Z}$, también podemos calcular, tras resolver de forma combinatoria la aparición de elementos nulos en el sistema de generadores de S, las sicigeas S-graduadas de $\mathcal{I}(C)$, a partir de las sicigeas S-graduadas de $\mathcal{I}(C_{\mathcal{Z}})$ (obtenidas como se indicó en la nota anterior).

Nota 4.2.17 Cuando el vector de exponentes tiene alguna coordenada nula, el semigrupo asociado a la curva C no tiene por qué ser combinatoriamente finito. Basta considerar la curva plana compleja $C = C_1 \cup C_2$ donde

$$C_1 \equiv \left\{ \begin{array}{l} x = 1 \\ y = t \end{array} \right. \quad C_2 \equiv \left\{ \begin{array}{l} x = -1 \\ y = t \end{array} \right. \quad .$$

Es claro que $\mathcal{I}(C) = \langle X^2 - 1 \rangle$, luego la curva C es monomial. Sea $\rho : L_\rho \to k^*$ el carácter parcial tal que $\mathcal{I}(C) = I_+(\rho)$. Como $\underline{h} = (0, 1)$ entonces Sat $L_\rho = \langle (1, 0) \rangle$. Además, como $I_+(\rho) = \langle X^2 - 1 \rangle$, es claro que $L_\rho = \langle (2, 0) \rangle$ y $\rho(\underline{m}) = 1$ para todo $\underline{m} \in L_\rho$. Por lo tanto Sat $L_\rho / L_\rho \cong \mathbb{Z}/(2)$, y el semigrupo asociado a C es $S = \langle (0, \overline{1}), (1, \overline{0}) \rangle \subset \mathbb{Z} \oplus \mathbb{Z}/(2)$, que no es combinatoriamente finito ya que $(0, \overline{0}) = (0, \overline{1}) + (0, \overline{1})$.

4.2.3 Caso general

Una vez analizados los casos irreducible y de única célula coordenada, veamos ahora cómo dotar al ideal de una curva monomial de estructura S-homogénea. Para hacer la construcción de S necesitaremos considerar, al contrario que en el caso de única célula, además de las células asociadas a cada componente, $\mathcal{Z}_j$, los conjuntos $\widetilde{\mathcal{Z}}_j$ (Notación 2.1.19).

Sea $C = C_1 \cup \ldots \cup C_d$ una curva monomial en el espacio afín $\mathcal{A}^n(k)$. Para cada $j \in \{1, \ldots, d\}$ sean, como de costumbre, $\mathcal{Z}_j$ la célula asociada a la componente monomial irreducible C_j, $\underline{h}_j$ el vector de exponentes de la componente C_j y $\widetilde{\mathcal{Z}}_j = \{i \in \mathcal{Z}_j \mid h_{ji} = 0\}$. Para cualquier $\mathcal{Z} \subseteq \{1, \ldots, n\}$, sea $I_{\mathcal{Z}}$ el ideal $\mathcal{I}(\overline{C \cap (k^*)^{\mathcal{Z}}})$, y consideremos el conjunto $U = \{\mathcal{Z} \mid C_{\mathcal{Z}} \cap (k^*)^{\mathcal{Z}} \neq \emptyset\}$. Tras una reordenación de las componentes, podemos suponer $U = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_r, \widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_s\}$, con $s \leq r \leq d$, tales que las células

$\mathcal{Z}_1, \ldots, \mathcal{Z}_r$ son distintas, y $j \in \{1, \ldots, s\}$ si y sólo si no existe $k \in \{1, \ldots, r\}$ con $\widetilde{\mathcal{Z}}_j = \mathcal{Z}_k$, donde además los conjuntos $\widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_s$ son distintos.

Nota 4.2.18 El conjunto U que acabamos de construir se puede obtener apartir del que se definió en el Teorema 2.2.33 eliminando en $U_1 = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_d\}$ y en $U_2 = \{\widetilde{\mathcal{Z}}_1, \ldots, \widetilde{\mathcal{Z}}_s\}$ los elementos repetidos.

Notación 4.2.19 *En lo que sigue, denotaremos* $\mathcal{Z}_j^* = \mathcal{Z}_j$ *para cada* $j \in \{1, \ldots, r\}$ *y* $\mathcal{Z}_{r+j}^* = \widetilde{\mathcal{Z}}_j$ *para cada* $j \in \{1, \ldots, s\}$.

Como vimos en la Proposición 2.2.29, para cada $\mathcal{Z}_j^* \in U$ $(1 \leq j \leq r+s)$ existe un carácter parcial $\rho_j : L_{\mathcal{Z}_j^*} \to k^*$, siendo $L_{\mathcal{Z}_j^*}$ un subretículo de $\mathbb{Z}^{\mathcal{Z}_j^*}$, tal que $I_{\mathcal{Z}_j^*} = I_+(\rho_j) + M(\mathcal{Z}_j^*)$.

Proposición 4.2.20 *Si* $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$, *entonces* $L_{\mathcal{Z}_k^*} \subseteq L_{\mathcal{Z}_j^*}$ *y* $I_+(\rho_k) \subseteq I_+(\rho_j)$.

Dem. Sea π_{jk} la proyección $\pi_{jk} : (k^*)^{\mathcal{Z}_j^*} \to (k^*)^{\mathcal{Z}_k^*}$. Como C es monomial, entonces $\mathcal{I}(C)$ es binomial y, por tanto, $\pi_{jk}(C \cap (k^*)^{\mathcal{Z}_j^*}) \subseteq C \cap (k^*)^{\mathcal{Z}_k^*}$ (Teorema 1.5.11). Luego $I_{\mathcal{Z}_k^*} \cap k[\mathcal{Z}_k^*] \subseteq I_{\mathcal{Z}_j^*} \cap k[\mathcal{Z}_k^*]$ y se tiene $I_+(\rho_k) = I_{\mathcal{Z}_k^*} \cap k[\mathcal{Z}_k^*] \subseteq I_{\mathcal{Z}_j^*} \cap k[\mathcal{Z}_k^*] \subseteq I_{\mathcal{Z}_j^*} \cap k[\mathcal{Z}_j^*] = I_+(\rho_j)$. Entonces, si $\underline{m} \in L_{\mathcal{Z}_k^*}$, se tiene $X^{\underline{m}_+} - \rho_k(\underline{m})X^{\underline{m}_-} \in I_+(\rho_k) \subseteq I_+(\rho_j)$, luego $\underline{m} \in L_{\mathcal{Z}_j^*}$ (Teorema 1.3.5).

□

Además se tiene:

1. Como vimos en la Proposición 2.2.29, si $j \in \{1, \ldots, r\}$ entonces $L_{\mathcal{Z}_j^*}$ es un subretículo de $\mathbb{Z}^{\mathcal{Z}_j^*}$ de rango $|\mathcal{Z}_j^*| - 1$ y Sat $(L_{\mathcal{Z}_j^*}) = \langle \underline{h}_{\mathcal{Z}_j^*} \rangle^\perp$ ($\underline{h}_{\mathcal{Z}_j^*}$ es el vector de exponentes de las componentes con célula asociada $\mathcal{Z}_j^*$). Por lo tanto podemos aplicar la Definición 4.1.12 y calcular el semigrupo asociado a $L_{\mathcal{Z}_j^*}$, $S_j = \overline{\varphi}_j((\mathbb{Z}_{\geq 0})^{\mathcal{Z}_j^*})$, generado por $\{g_{ij} = \overline{\varphi}_j(\underline{e}_i) \mid i \in \mathcal{Z}_j^*\}$, donde $\{\underline{e}_1, \ldots, \underline{e}_n\}$ denota la base canónica de $\mathbb{Z}^n$.

2. Como vimos en la Proposición 2.2.32, si $j \in \{r+1, \ldots, r+s\}$ entonces $L_{\mathcal{Z}_j^*}$ es un subretículo de $\mathbb{Z}^{\mathcal{Z}_j^*}$ de rango $|\mathcal{Z}_j^*|$ y tal que Sat $(L_{\mathcal{Z}_j^*}) = \mathbb{Z}^{\mathcal{Z}_j^*}$. Por lo tanto podemos aplicar la Definición 4.1.16 y calcular el semigrupo asociado a $L_{\mathcal{Z}_j^*}$, $S_j = \overline{\varphi}_j((\mathbb{Z}_{\geq 0})^{\mathcal{Z}_j})$, generado por $\{g_{ij} = \overline{\varphi}_j(\underline{e}_i) \mid i \in \mathcal{Z}_j^*\}$.

Como dijimos en 4.1.13 y 4.1.17, si $1 \leq j \leq r$ denotaremos $g_{ij} = (h_{ji}, t(g_{ij}))$, para todo $i \in \mathcal{Z}_j^*$, y si $r+1 \leq j \leq r+s$ entonces $g_{ij} = t(g_{ij})$, para todo $i \in \mathcal{Z}_j^*$.

Teniendo en cuenta estos elementos, se construye para cada $1 \leq j \leq r+s$, el conjunto $\widetilde{S}_j = S_j \sqcup \{\infty\}$, con la estructura de semigrupo extendida a partir de la de S_j y exigiendo que $g + \infty = \infty$ para todo $g \in S_j$.

Definición 4.2.21 *Sea $C \subset \mathcal{A}^n(k)$ una curva monomial. Llamaremos semigrupo asociado a la curva C al subsemigrupo de $\widetilde{S}_1 \times \ldots \times \widetilde{S}_{r+s}$ generado por los elementos,*

$$\begin{array}{cc} \underline{g}_1 = & (g_{11} \cdots g_{1\,r+s}) \\ \vdots & \vdots \\ \underline{g}_n = & (g_{n1} \cdots g_{n\,r+s}) \end{array}$$

donde

$$g_{ij} = \begin{cases} (h_{ji}, t(g_{ij})) & si\ 1 \leq j \leq r \ \ e\ \ i \in \mathcal{Z}_j = \mathcal{Z}_j^* \\ t(g_{ij}) & si\ r+1 \leq j \ \ e \ \ i \in \widetilde{\mathcal{Z}}_{j-r} = \mathcal{Z}_j^* \\ \infty & en\ otro\ caso\ (i \notin \mathcal{Z}_j^*) \end{cases} .$$

Posteriormente, distinguiremos si $\underline{\infty} := (\infty, \ldots, \infty) \in S$ o no. Empecemos por caracterizar este hecho:

Proposición 4.2.22 *Sea S el semigrupo asociado a la curva monomial C. Entonces, el elemento $\underline{\infty}$ pertenece a S si y sólo si para cada $j \in \{1, \ldots, r\}$ existe $i \in \{1, \ldots, n\}$ tal que $h_{ji} = \infty$ (es decir, tal que $X_i \in I_{\mathcal{Z}_j}$, o equivalentemente, $i \notin \mathcal{Z}_j$).*

Dem. Por la definición de S, $\underline{\infty} \in S$ si y sólo si para todo $j \in \{1, \ldots, r+s\}$ existe $i \in \{1, \ldots, n\}$ tal que $g_{ij} = \infty$. Pero esta condición es equivalente a que para todo $j \in \{1, \ldots, r\}$ exista i tal que $g_{ij} = \infty$ (es decir, $i \notin \mathcal{Z}_j$). En efecto, para todo $k \in \{1, \ldots, s\}$, $\mathcal{Z}_{k+r}^* = \widetilde{\mathcal{Z}}_k \subseteq \mathcal{Z}_k$, y existe $i \in \{1, \ldots, n\}$ tal que $g_{ik} = \infty$, es decir, $i \notin \mathcal{Z}_k$ y, por tanto, $i \notin \widetilde{\mathcal{Z}}_k$, y se tiene $g_{i,k+r} = \infty$. $\square$

Con las notaciones que hemos establecido, vamos a dividir los elementos del semigrupo S según los tipos especificados en la siguiente definición:

Definición 4.2.23 *Dados un elemento $\underline{\gamma} \in S$ y $k \in \{1, \dots, r+s\}$, diremos que $\underline{\gamma}$ es de tipo k si se cumple que:*

$$\gamma_j \neq \infty \Leftrightarrow \mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*.$$

Notación 4.2.24 Para cada $k \in \{1, \dots, r+s\}$ denotaremos $T_k := \{\underline{\gamma} \in S \mid \underline{\gamma}$ es de tipo $k\}$ y $B_k := \{j \in \{1, \dots, r+s\} \mid \mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*\}$ (es decir, los índices de las coordenadas distintas de ∞ para los elementos de T_k).

Veamos que todos los elementos de S salvo el $\underline{\infty}$ (caso de que pertenezca a S) son de uno de los tipos especificados. Es más, el conjunto $S \backslash \{\underline{\infty}\}$ admite una partición dada por los subconjuntos $T_1, \dots, T_{r+s}$. Recordemos que el conjunto U es cerrado por intersecciones.

Proposición 4.2.25

1. *Para cada $1 \leq i \leq n$, si $\underline{g}_i \neq \underline{\infty}$ entonces $\underline{g}_i$ es de tipo k, siendo k el único elemento de $\{1, \dots, r+s\}$ tal que $\bigcap_{\{j \mid i \in \mathcal{Z}_j^*\}} \mathcal{Z}_j^* = \mathcal{Z}_k^* \in U$.*

2. *Dado $\underline{\gamma} = \sum_{i=1}^p \underline{m}_i$, donde el elemento $\underline{m}_i \in S$ es de tipo k_i, se tiene que $\gamma_l \neq \infty \Leftrightarrow \bigcup_{i=1}^p \mathcal{Z}_{k_i}^* \subseteq \mathcal{Z}_l^*$. Además, si $\underline{\gamma} \neq \underline{\infty}$ y $\bigcap_{\gamma_l \neq \infty} \mathcal{Z}_l^* = \mathcal{Z}_t^* \in U$, entonces $\underline{\gamma}$ es de tipo t.*

3. *$S \backslash \{\underline{\infty}\} = T_1 \sqcup \ldots \sqcup T_{r+s}$, unión disjunta y $T_k \neq \emptyset$ para cada $k \in \{1, \dots, r+s\}$.*

4. *Si $\underline{\gamma} \in T_k$, entonces $\underline{\gamma} = \sum_{i \in \mathcal{Z}_k^*} l_i \underline{g}_i$, $l_i \in \mathbb{Z}_{\geq 0}$.*

Dem. Para $i \in \{1, \dots, n\}$, si $\underline{g}_i \neq \underline{\infty}$ entonces existe $j \in \{1, \dots, r\}$ tal que $i \in \mathcal{Z}_j$, y por tanto $\bigcap_{\{i \in \mathcal{Z}_j^*\}} \mathcal{Z}_j^* \in U$. Sea k el único elemento tal que $\bigcap_{\{i \in \mathcal{Z}_j^*\}} \mathcal{Z}_j^* = \mathcal{Z}_k^*$. Para este k es claro que si $g_{ij} \neq \infty$ entonces $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$ ya que en este caso $\mathcal{Z}_j^*$ es uno de los que aparecen en la intersección. Recíprocamente, si $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$, como $i \in \mathcal{Z}_k^*$, entonces $g_{ij} \neq \infty$. Por lo tanto $\underline{g}_i$ es de tipo k.

Sea $\underline{\gamma} = \sum_{i=1}^p \underline{m}_i$, donde $\underline{m}_i \in S$ es de tipo k_i. Es claro que $\gamma_l \neq \infty$ si y sólo si $m_{il} \neq \infty$ para $1 \leq i \leq p$, es decir, puesto que $\underline{m}_i$ es de tipo k_i, si $\mathcal{Z}_{k_i}^* \subseteq \mathcal{Z}_l$. Por lo tanto, tenemos $\{l \in \{1, \dots, r+s\} \mid \gamma_l \neq \infty\} = \{l \in \{1, \dots, r+s\} \mid \bigcup_{i=1}^p \mathcal{Z}_{k_i}^* \subseteq \mathcal{Z}_l^*\}$. En particular, $\bigcup_{i=1}^p \mathcal{Z}_{k_i}^* \subseteq \bigcap_{\gamma_l \neq \infty} \mathcal{Z}_l^*$. Además, si $\underline{\gamma} \neq \underline{\infty}$, entonces existe un único $t \in \{1, \dots, r+s\}$ tal que $\bigcap_{\gamma_l \neq \infty} \mathcal{Z}_l^* = \mathcal{Z}_t^*$. Entonces, si $\mathcal{Z}_t^* \subseteq \mathcal{Z}_j^*$ se tiene $\bigcup_{i=1}^p \mathcal{Z}_{k_i}^* \subseteq \mathcal{Z}_j^*$ y por tanto $\gamma_j \neq \infty$. Recíprocamente, si $\gamma_j \neq \infty$ entonces, por la construcción de $\mathcal{Z}_t^*$, $\mathcal{Z}_t^* \subseteq \mathcal{Z}_j^*$. Con lo cual, $\underline{\gamma}$ es de tipo t.

Como hemos visto en 1, cada generador distinto de $\underline{\infty}$ de S tiene un tipo asociado. Además, si $\underline{\gamma} \in S$ es suma de generadores de S y, si $\underline{\gamma} \neq \underline{\infty}$, aplicando 2 podemos construir su tipo asociado de forma única. Luego $S \backslash \{\underline{\infty}\} = T_1 \sqcup \ldots \sqcup T_{r+s}$. Es más, para todo $k \in \{1, \ldots, r+s\}$, $T_k \neq \emptyset$ pues basta considerar $\underline{\gamma}_k = \sum_{i \in \mathcal{Z}_k^*} \underline{g}_i$ que cumple que, para todo j, $\gamma_{kj} = \infty$ si y sólo si, para todo $i \in \mathcal{Z}_k^*$, $g_{ij} = \infty$ (es decir, $i \in \mathcal{Z}_j^*$). Luego $\gamma_{kj} = \infty$ si y sólo si $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$, por lo tanto $\underline{\gamma}_k$ es de tipo k.

Finalmente, sea $\underline{\gamma} = \sum_{i \in J} l_i \underline{g}_i$ un elemento de tipo k, y supongamos que para cada $i \in J$, $\underline{g}_i$ es de tipo k_i^*. Aplicando 1, se deduce $i \in \mathcal{Z}_{k_i}^*$. Además, como $\underline{\gamma}$ es de tipo k, aplicando 2 tenemos que $\bigcup_{\{i \in J | l_i \neq 0\}} \mathcal{Z}_{k_i}^* \subseteq \mathcal{Z}_k^*$, y por tanto $i \in \mathcal{Z}_k^*$ para todo $i \in J$ con $l_i \neq 0$.

□

Utilizando este resultado, podemos demostrar que la condición necesaria y suficiente para que dos elementos de S de tipo k sean iguales es que su coordenada k-ésima sea igual (esta es la razón básica de la importancia de la construcción de T_k).

Proposición 4.2.26 *Si $\underline{\gamma}$ y $\underline{\eta}$ son elementos en T_k tales que $\gamma_k = \eta_k$, entonces $\underline{\gamma} = \underline{\eta}$.*

Dem. De la Proposición 4.2.25, se tiene

$$\underline{\gamma} = \sum_{i \in \mathcal{Z}_k^*} m_i \underline{g}_i \ \text{ y } \ \underline{\eta} = \sum_{i \in \mathcal{Z}_k^*} n_i \underline{g}_i; \qquad \underline{m}, \underline{n} \in (\mathbb{Z}_{\geq 0})^{\mathcal{Z}_k^*}.$$

Sea $j \in B_k$; es decir, $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$ y por tanto $\gamma_j \neq \infty$ y $\eta_j \neq \infty$. Entonces, $\gamma_j = \overline{\varphi}_j(\underline{m})$ y $\eta_j = \overline{\varphi}_j(\underline{n})$ siendo $\overline{\varphi}_j$ el homomorfismo utilizado para definir el semigrupo S_j (Definición 4.1.12 cuando $1 \leq j \leq r$ y 4.1.16 cuando $r + 1 \leq j \leq r + s$). Como $\gamma_k = \eta_k$, entonces $\underline{m} - \underline{n} \in L_{\mathcal{Z}_k}$ (Proposición 4.1.20). Además, utilizando la Proposición 4.2.20, como $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$ entonces $L_{\mathcal{Z}_k^*} \subseteq L_{\mathcal{Z}_j^*}$ (inclusión a través del embebimiento natural $\mathbb{Z}^{\mathcal{Z}_k^*} \subseteq \mathbb{Z}^{\mathcal{Z}_j^*}$). Por lo tanto $\underline{m} - \underline{n} \in L_{\mathcal{Z}_j^*}$, de donde se deduce que $\gamma_j = \eta_j$ (Proposición 4.1.20). Como $\underline{\gamma}$ y $\underline{\eta}$ son de tipo k, y $\gamma_j = \eta_j$ para todo $j \in B_k$, se tiene $\underline{\gamma} = \underline{\eta}$.

□

Teniendo en cuenta estos resultados podemos demostrar que el anillo de coordenadas de la curva C es isomorfo a un cociente de la k-álgebra $k[S]$. Empecemos por el caso más simple, que es aquel en que se cumpla la condición (H) siguiente:

Existe $\underline{\lambda} \in \mathbb{Z}^n \mid \ \mathrm{pr}_{\mathcal{Z}_j}(\underline{\lambda})^{\underline{m}} = \rho_j(\underline{m}),\ \forall j \in \{1, \ldots, r\},\ \forall \underline{m} \in L_{\mathcal{Z}_j}$ (**H**)

(condición que estudiaremos en el apéndice 2)

Para cada $1 \leq j \leq r + s$, consideremos la k-álgebra asociada a S_j, $k[S_j] = \bigoplus_{\gamma_j \in S_j} k\chi_j^{\gamma_j}$. Del mismo modo, tenemos la k-algebra asociada a S, $k[S] = \bigoplus_{\underline{\gamma} \in S} k\chi^{\underline{\gamma}}$. En adelante, denotaremos $\varepsilon = 1$ si $\underline{\infty} \in S$ y $\varepsilon = 0$ en otro caso. Cuando $\varepsilon = 1$, el ideal de $k[S]$ generado por $\chi^{\underline{\infty}}$ es exactamente $\{\lambda\chi^{\underline{\infty}} \mid \lambda \in k\}$.

Se construye, para cada $j \in \{1, \ldots, r + s\}$, el homomorfismo

$$\begin{array}{rcl} \alpha_j : k[S]/\left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle & \longrightarrow & k[S_j] \\ \chi^{\underline{\gamma}} + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle & \longmapsto & \chi_j^{\gamma_j} \text{ si } \gamma_j \neq \infty \\ \chi^{\underline{\gamma}} + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle & \longmapsto & 0 \text{ si } \gamma_j = \infty \end{array} ,$$

y el homomorfismo

$$\alpha : k[S]/\left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle \to k[S_1] \times \ldots \times k[S_{r+s}] \ , \ \alpha := (\alpha_1, \ldots, \alpha_{r+s}) \ .$$

Proposición 4.2.27 *α es inyectivo.*

Dem. Sea $f = \sum_{\underline{\gamma} \in S \setminus \{\infty\}} \lambda_{\underline{\gamma}} \chi^{\underline{\gamma}}$ tal que $f + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle \in \ker(\alpha)$. Podemos distribuir los términos de f de acuerdo con el tipo de sus exponentes; es decir, $f = \sum_{k=1}^{r+s} f_{T_k}$, donde $f_{T_k} = \sum_{\underline{\gamma} \in T_k} \lambda_{\underline{\gamma}} \chi^{\underline{\gamma}}$. Es claro que si $j \notin B_k$, entonces $\alpha_j(f_{T_k} + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle) = 0$. Por lo tanto,

$$\alpha_j(f + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle) = \sum_{\{k | j \in B_k\}} \sum_{\underline{\gamma} \in T_k} \lambda_{\underline{\gamma}} \chi_j^{\gamma_j} \ .$$

Denotemos:

$$X_{kj} = \sum_{\underline{\gamma} \in T_k} \lambda_{\underline{\gamma}} \chi_j^{\gamma_j} \ .$$

Como $f + \left\langle \varepsilon\chi^{\underline{\infty}} \right\rangle \in \ker(\alpha_j)$, tenemos que, para cada $1 \leq j \leq r + s$:

$$\sum_{\{k | j \in B_k\}} X_{kj} = 0 \tag{4.3}$$

Por la Proposición 4.2.26, cada $\gamma_k \in S_k$ aparece a lo sumo como coordenada k-ésima de un elemento $\underline{\gamma} \in T_k$, luego de $X_{kk} = \sum_{\underline{\gamma} \in T_k} \underline{\lambda}_{\underline{\gamma}} \chi_k^{\gamma_k} = 0$ deducimos $\underline{\lambda}_{\underline{\gamma}} = 0$ para todo $\underline{\gamma} \in T_k$. Así, para ver que $f = 0$ es suficiente probar $X_{kk} = 0$ para todo k. Obsérvese que también hemos probado que $X_{kk} = 0$ implica $X_{kj} = 0$ para todo $j \in B_k$.

Veamos entonces que $X_{kk} = 0$ para todo $k \in \{1, \ldots, r+s\}$. Definamos el nivel de la célula $\mathcal{Z}_j^*$ como el máximo de las longitudes, l, de cadenas $\mathcal{Z}_{t_0}^* \subsetneq \mathcal{Z}_{t_1}^* \subsetneq \ldots \subsetneq \mathcal{Z}_{t_l}^* = \mathcal{Z}_j^*$ en U. En la demostración razonaremos por inducción sobre nivel$(\mathcal{Z}_j^*)$.

Si nivel$(\mathcal{Z}_j^*) = 0$ y $j \in B_k$, entonces $k = j$, ya que $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$. Por lo tanto, la ecuación (4.3) nos dice $X_{jj} = 0$. Supongamos que nivel$(\mathcal{Z}_j) = l > 0$ y elijamos $k \neq j$, de forma que $j \in B_k$. Entonces $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$ y $\mathcal{Z}_k^* \neq \mathcal{Z}_j^*$, luego nivel$(\mathcal{Z}_k^*) < l$. Por lo tanto, como $k \in B_k$, aplicando hipótesis de inducción tenemos que $X_{kk} = 0$ y entonces $X_{kj} = 0$, como hemos dicho en el párrafo anterior. Aplicando la ecuación (4.3) se deduce $X_{jj} = 0$ como queríamos demostrar.

$\square$

Teorema 4.2.28 *Sean C una curva monomial cumpliendo la condición* (H) *e I su ideal asociado. Entonces el núcleo del homomorfismo,*

$$\begin{array}{rcl} \psi : k[X_1, \ldots, X_n] & \longrightarrow & k[S] / \langle \varepsilon \chi^{\underline{\infty}} \rangle \\ X_i & \mapsto & \lambda_i \chi^{\underline{g}_i} + \langle \varepsilon \chi^{\underline{\infty}} \rangle \end{array}$$

es el ideal I.

Dem. Sea $\underline{\lambda}$ un vector que cumpla la hipótesis (H). Consideremos, para cada $j \in \{1, \ldots, r+s\}$, el homomorfismo:

$$\begin{array}{rcl} \phi_j : k[X_1, \ldots, X_n] & \longrightarrow & k[S_j] \\ X_i & \longmapsto & \lambda_i \chi_j^{g_{ij}} \text{ si } i \in \mathcal{Z} \\ X_i & \longmapsto & 0 \text{ si } i \notin \mathcal{Z} \ , \end{array}$$

y el homomorfismo

$$\phi : k[X_1, \ldots, X_n] \longrightarrow k[S_1] \times \ldots \times k[S_{r+s}] \quad , \phi := (\phi_1, \ldots, \phi_{r+s})$$

Por la Proposición 4.2.1, para cada $j \in \{1, \ldots, r+s\}$, $\ker(\phi_j) = I_+(\widetilde{\rho}_j) + M_{\mathcal{Z}_j^*}$, donde $\widetilde{\rho}_j : L_j \to k^*$ está definido por $\widetilde{\rho}_j(\underline{m}) = (\underline{\lambda}_{\mathcal{Z}})^{\underline{m}}$, siendo L_j el retículo asociado a $(S_j, \{g_{ij} \mid i \in \mathcal{Z}_j^*\})$. Por (H), $\widetilde{\rho}_j(\underline{m}) = \rho_j(\underline{m})$ y se tiene que $\ker(\phi_j) = I_{\mathcal{Z}_j^*}$ para cada $j \in \{1, \ldots, r\}$. Por otra parte, debido a la

Proposición 4.2.20, $L_{\mathcal{Z}^*_{r+k}} \subseteq L_{\mathcal{Z}^*_k}$ y $\rho_k(\underline{m}) = \rho_{r+k}(\underline{m})$, para todo $\underline{m} \in \mathcal{Z}^*_{r+k}$. Luego si $\underline{m} \in L_{\mathcal{Z}^*_{r+k}}$ se tiene $(\mathrm{pr}_{\mathcal{Z}^*_{r+k}}(\underline{\lambda}))^{\underline{m}} = (\mathrm{pr}_{\mathcal{Z}^*_k}(\underline{\lambda}))^{\underline{m}} = \rho_k(\underline{m}) = \rho_{r+k}(\underline{m})$ y por tanto, por un razonamiento análogo al anterior, también $\ker(\phi_j) = I_{\mathcal{Z}^*_j}$ para $r+1 \leq j \leq r+s$.

Puesto que, como consecuencia de la Proposición 2.2.30 se tiene $I = \bigcap_{j=1}^{r+s} I_{\mathcal{Z}^*_j}$, se deduce $\ker(\phi) = I$. Por otro lado, es claro que $\alpha \circ \psi = \phi$, luego, como α es inyectiva, $\ker(\psi) = \ker(\phi) = I$.

□

Corolario 4.2.29 *Sean C una curva monomial cumpliendo la condición* (H)*, S el semigrupo asociado a C y $\{\underline{g}_1, \ldots, \underline{g}_n\}$ un sistema de generadores de S como en la Definición 4.2.21. Entonces, si I es el ideal asociado a C, el homomorfismo $\Psi : k[X]/I \to k[S]/\langle \varepsilon\chi^{\underline{\infty}} \rangle$ dado por $\Psi(X_i + I) = \lambda_i \chi^{\underline{g}_i} + \langle \varepsilon\chi^{\underline{\infty}} \rangle$ es un isomorfismo.*

Corolario 4.2.30 *El ideal I es S-homogéneo.*

Nota 4.2.31 De hecho se puede comprobar sin dificultad que todos los binomios de I son homogéneos y que los elementos de grado $\underline{\infty}$ de I (caso de existir) son exactamente suma de monomios que pertenecen a I.

Veamos un ejemplo de una curva monomial que satisface (H), y, en este caso, construiremos el semigrupo asociado y el isomorfismo planteado en el corolario anterior.

Ejemplo 4.2.32 Consideremos la curva monomial compleja $C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$, cuyas componentes tienen parametrizaciones:

$$C_1 \equiv \begin{cases} x_1 = t \\ x_2 = 2t^2 \\ x_3 = 8t^3 \\ x_4 = 0 \end{cases} \quad C_2 \equiv \begin{cases} x_1 = t \\ x_2 = 2It^2 \\ x_3 = -8It^3 \\ x_4 = 0 \end{cases} \quad C_3 \equiv \begin{cases} x_1 = t \\ x_2 = -2t^2 \\ x_3 = -8t^3 \\ x_4 = 0 \end{cases}$$

$$C_4 \equiv \begin{cases} x_1 = t \\ x_2 = -2It^2 \\ x_3 = 8It^3 \\ x_4 = 0 \end{cases} \quad C_5 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = t^3 \\ x_4 = t^2 \end{cases} \quad C_6 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = t \\ x_4 = 0 \end{cases}$$

Con estos datos $U = \{\mathcal{Z}_1, \mathcal{Z}_2, \mathcal{Z}_3, \mathcal{Z}_4\}$, siendo $\mathcal{Z}_1 = \{1,2,3\}$, $\mathcal{Z}_2 = \{3,4\}$, $\mathcal{Z}_3 = \{3\}$ y $\mathcal{Z}_4 = \emptyset$. Para cada $j \in \{1, \ldots, 4\}$ denotemos por $\rho_j : L_j \to$

k^* el carácter parcial cumpliendo $I_{\mathcal{Z}_j} = I_+(\rho_j) + M(\mathcal{Z}_j)$. Como vimos en el Ejemplo 2.3.8, $L_1 = \langle(-8,4,0),(3,-3,1)\rangle \subseteq \mathbb{Z}^{\mathcal{Z}_1}$. Además es fácil comprobar que $L_2 = \langle(-2,3)\rangle \subseteq \mathbb{Z}^{\mathcal{Z}_2}$ y $L_3 = \langle 0\rangle \subseteq \mathbb{Z}^{\mathcal{Z}_3}$. Por último, el caso degenerado $\mathcal{Z}_4 = \emptyset$ se corresponde con $L_4 = \langle 0\rangle \subset \mathbb{Z}^{\emptyset}$ (Nota 4.1.19). Como hicimos en el Ejemplo 4.2.14, calculamos el semigrupo asociado a L_1 que resulta ser $S_1 = \langle(1,\overline{3}),(2,\overline{3}),(3,\overline{0})\rangle \subseteq \mathbb{Z}\oplus\mathbb{Z}/(4)$. Para L_2 y L_3, estamos en la situación de única componente con célula $\mathcal{Z}_2$ y con célula $\mathcal{Z}_3$, y se tiene $S_2 = \langle 3,2\rangle \subseteq \mathbb{Z}_{\geq 0}$ y $S_3 = \langle 1\rangle \subseteq \mathbb{Z}_{\geq 0}$. En el caso degenerado, el semigrupo a considerar es $S_4 = \{0\} = \mathbb{Z}^{\emptyset}$.

Por lo tanto el semigrupo asociado a C es el semigrupo $S \subseteq \widetilde{S}_1 \times \widetilde{S}_2 \times \widetilde{S}_3 \times \widetilde{S}_4$, generado por los vectores fila de la matriz:

$$\begin{pmatrix} (1,\overline{3}) & \infty & \infty & \infty \\ (2,\overline{3}) & \infty & \infty & \infty \\ (3,\overline{0}) & 3 & 1 & \infty \\ \infty & 2 & \infty & \infty \end{pmatrix}$$

El vector $\underline{\lambda} = (1,2,8,1/4)$ cumple que para cada $j \in \{1,2,3,4\}$ se tiene $\mathrm{pr}_{\mathcal{Z}_j}(\underline{\lambda}) \in \mathcal{V}(I(\rho_j))$. En efecto, si $j=1$, el resultado se deduce de lo visto en el Ejemplo 4.2.14. Como $(8,1/4)^{(-2,3)} = 1$, también es válido para $j=2$. Los casos $j=3$ y $j=4$ son triviales. Por lo tanto, aplicando el Corolario 4.2.29, el homomorfismo S-graduado

$$\begin{array}{rcl} \phi : k[X]/I & \longrightarrow & k[S]/\langle \varepsilon\chi^{\infty}\rangle \\ X_1 + I & \longmapsto & 1\chi^{((1,\overline{3}),\infty,\infty,\infty)} \\ X_2 + I & \longmapsto & 2\chi^{((2,\overline{3}),\infty,\infty,\infty)} \\ X_3 + I & \longmapsto & 8\chi^{((3,\overline{0}),3,1,\infty)} \\ X_4 + I & \longmapsto & 1/4\chi^{(\infty,2,\infty,\infty)} \end{array},$$

es un isomorfismo.

Nota 4.2.33 En el caso $\widetilde{\mathcal{Z}}_j = \emptyset$, se puede prescindir en el semigrupo de la coordenada, ∞, correspondiente a $\widetilde{\mathcal{Z}}_j$, obteniendo un semigrupo isomorfo, y por tanto un isomorfismo de k-álgebras (Lema 4.1.21).

Como hemos visto, hemos establecido el isomorfismo cuando las curvas monomiales cumplen la condición (H). Como vemos a continuación, existen casos de curvas monomial que no satisfacen (H).

Ejemplo 4.2.34 Consideremos la curva monomial compleja $C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$, cuyas componentes tienen parametrizaciones:

$$C_1 \equiv \begin{cases} x_1 = t^3 \\ x_2 = 3t \\ x_3 = 4t^2 \\ x_4 = 0 \end{cases} \quad C_2 \equiv \begin{cases} x_1 = 0 \\ x_2 = \frac{3}{2}t^2 \\ x_3 = t^4 \\ x_4 = t \end{cases} \quad C_3 \equiv \begin{cases} x_1 = t^6 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 2t \end{cases}$$

$$C_4 \equiv \begin{cases} x_1 = 0 \\ x_2 = 3t \\ x_3 = 4t^2 \\ x_4 = 0 \end{cases} \quad C_5 \equiv \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = t \end{cases} \quad C_6 \equiv \begin{cases} x_1 = t \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \end{cases}$$

Con estos datos, $U = \{\mathcal{Z}_1, \mathcal{Z}_2, \mathcal{Z}_3, \mathcal{Z}_4, \mathcal{Z}_5, \mathcal{Z}_6, \mathcal{Z}_7\}$, siendo $\mathcal{Z}_1 = \{1,2,3\}$, $\mathcal{Z}_2 = \{2,3,4\}$, $\mathcal{Z}_3 = \{1,4\}$, $\mathcal{Z}_4 = \{2,3\}$, $\mathcal{Z}_5 = \{4\}$, $\mathcal{Z}_6 = \{1\}$ y $\mathcal{Z}_7 = \emptyset$. Para cada $j \in \{1, \ldots, 7\}$ denotemos por $\rho_j : L_j \to k^*$ el carácter parcial cumpliendo $I_{\mathcal{Z}_j} = I_+(\rho_j) + M(\mathcal{Z}_j)$. Si buscamos un vector $\underline{\lambda} \in \mathbb{C}^4$ cumpliendo la condición (H), en particular tiene que cumplir que:

$$\underline{\lambda} \in \mathcal{V}(I(\rho_1)) \cap V(I(\rho_2)) \cap V(I(\rho_3))$$

Como en este caso los ideales $I_{\mathcal{Z}_j} = I_+(\rho_j) + M(\mathcal{Z}_j)$ son ideales de curvas monomiales irreducibles, si dicho vector existe, tiene que ser válido como vector de coeficientes de una parametrización monomial para C_j $(1 \leq j \leq 3)$. Por lo tanto, si existe $\underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathcal{V}(I(\rho_1)) \cap V(I(\rho_2)) \cap V(I(\rho_3))$, entonces el sistema de ecuaciones

$$\begin{matrix} 1 = \lambda_1\alpha^3 \\ 3 = \lambda_2\alpha \\ 4 = \lambda_3\alpha^2 \end{matrix} \qquad \begin{matrix} \frac{3}{2} = \lambda_2\beta^2 \\ 1 = \lambda_3\beta^4 \\ 1 = \lambda_4\beta \end{matrix} \qquad \begin{matrix} 1 = \lambda_1\gamma^6 \\ 2 = \lambda_4\gamma \end{matrix} \quad ,$$

tiene que tener solución en $\mathbb{C}$ (Proposición 2.1.9). Pero este sistema no tiene solución, por lo tanto C no cumple la condición (H).

Veamos ahora qué pasa si no se dispone de la condición (H). En este caso se obtiene un resultado análogo al Corolario 4.2.29 aunque menos "redondo". Vamos a ver que $K[X_1, \ldots, X_n]/I$ es también isomorfo a una k-álgebra S-graduada, cuya estructura es, en general, más complicada que la de $k[S]/\langle \epsilon\chi^{\underline{\infty}} \rangle$. Las demostraciones son, con ciertas precisiones que haremos, completamente análogas a las del caso anterior, por lo que no las detallaremos.

Sea $A = \overbrace{k \times \ldots \times k}^{r+s}$. De forma análoga a la construcción de $k[S]$ se puede construir $A[S]$, que es una k-álgebra S-graduada (de hecho un $k[S]$-módulo graduado).

Para cada $1 \leq j \leq r+s$, elijamos $\underline{\lambda}_j \in k^n$ tal que $(\underline{\lambda}_j)_{\mathcal{Z}_j^*} \in \mathcal{V}(I(\rho_j))$ y $\lambda_{ji} = 0$ si $i \notin \mathcal{Z}_j^*$.

Para cada $\underline{\gamma} \in S$ se considera el subconjunto de A dado por

$$\begin{aligned} C_{\underline{\gamma}} &= \{(\lambda_{11}, \ldots, \lambda_{r+s,1})^{i_1} \cdots (\lambda_{1n}, \ldots, \lambda_{r+s,n})^{i_n} \mid i_1\underline{g}_1 + \ldots + i_n\underline{g}_n = \underline{\gamma}\} \\ &= \{(\lambda_{11}^{i_1} \cdots \lambda_{1n}^{i_n}, \ldots, \lambda_{r+s,1}^{i_1} \cdots \lambda_{r+s,n}^{i_n}) \mid i_1\underline{g}_1 + \ldots + i_n\underline{g}_n = \underline{\gamma}\} \end{aligned}$$

y sea $A_{\underline{\gamma}}$ el k-subespacio vectorial de A generado por $C_{\underline{\gamma}}$. Es claro que

$$A_{\underline{\gamma}} = \left\{ (f(\lambda_{11}, \ldots, \lambda_{1n}), \ldots, f(\lambda_{r+s,1}, \ldots, \lambda_{r+s,n})) \;\middle|\; \begin{array}{l} f \in k[X_1, \ldots, X_n] \\ f \text{ de grado } \underline{\gamma} \end{array} \right\}$$

(donde se considera en $k[X_1, \ldots, X_n]$ la graduación que a X_i le asigna grado $\underline{g}_i$).

Sea $\widetilde{A}_C = \bigoplus_{\underline{\gamma} \in S} A_{\underline{\gamma}} \chi^{\underline{\gamma}} \subseteq A[S]$. Es obvio, por construcción, que $\widetilde{A}_C$ es $k[S]$-subálgebra de $A[S]$.

Lema 4.2.35 *Sean $\underline{\gamma} = (\gamma_1, \ldots, \gamma_{r+s}) \in S$ y $(a_1, \ldots, a_{r+s}) \in A_{\underline{\gamma}}$. Si $\gamma_j = \infty$, entonces $a_j = 0$.*

Dem. La demostración es obvia, pues, por construcción

$$a_j = \sum_{i_1\underline{g}_1 + \ldots + i_n\underline{g}_n = \underline{\gamma}} \alpha_{i_1, \ldots, i_n} \lambda_{j1}^{i_1} \cdots \lambda_{jn}^{i_n} \ ,$$

y, para cada sumando, puesto que $\gamma_j = \infty$, existe k tal que $i_k > 0$ y $g_{kj} = \infty$, con lo que $\lambda_{jk} = 0$ y $\lambda_{j1}^{i_1} \cdots \lambda_{jn}^{i_n} = 0$.

□

Lema 4.2.36 *Si f es homogéneo de grado $\underline{\gamma} = (\gamma_1, \ldots, \gamma_{r+s})$ entonces para todo $\lambda_1, \ldots, \lambda_n \in k$ y para todo $j \in \{1, \ldots, r+s\}$*

$$f(\lambda_1 \chi^{g_{1j}}, \ldots, \lambda_n \chi^{g_{nj}}) = \chi^{\gamma_j} f(\lambda_1, \ldots, \lambda_n) \ .$$

Dem. Basta probarlo para los monomios $f = X_1^{i_1} \cdots X_n^{i_n}$ con $i_1\underline{g}_1 + \ldots + i_n\underline{g}_n = \underline{\gamma}$. Al sustituir resulta,

$$f(\lambda_1 \chi^{g_{1j}}, \ldots, \lambda_n \chi^{g_{nj}}) = \lambda_1^{i_1} \cdots \lambda_n^{i_n} \chi^{i_1 g_{1j} + \ldots + i_n g_{nj}} = f(\lambda_1, \ldots, \lambda_n) \chi^{\gamma_j} \ .$$

□

Proposición 4.2.37 *Sea $\underline{\gamma} = (\gamma_1, \ldots, \gamma_{r+s}) \in S$ con $\gamma_k \neq \infty$ y sea $(a_1, \ldots, a_{r+s}) \in A_{\underline{\gamma}}$. Entonces, si $a_k = 0$ y $\mathcal{Z}_k^* \subset \mathcal{Z}_j^*$ se tiene $a_j = 0$.*

Dem. Puesto que $(a_1, \ldots, a_{r+s}) \in A_{\underline{\gamma}}$, existe $f \in k[X_1, \ldots, X_n]$, suma de monomios de grado $\underline{\gamma}$, tal que $a_i = f(\lambda_{i1}, \ldots, \lambda_{in})$ para todo i. Puesto que $\gamma_k \neq \infty$, si $m_1\underline{g}_1 + \ldots m_n\underline{g}_n = \underline{\gamma}$ entonces no se puede tener $g_{jk} = \infty$ a menos que $m_j = 0$. Por tanto, f es suma de monomios de $k[\mathcal{Z}_k^*]$, y se tiene $a_i = f((\underline{\lambda}_i)_{\mathcal{Z}_k^*})$ para todo i.

Puesto que $a_k = 0$, se tiene $f(\lambda_{k1}, \ldots, \lambda_{kn}) = f((\underline{\lambda}_k)_{\mathcal{Z}_k^*}) = 0$, y por el Lema 4.2.36, $f(\lambda_{k1}\chi^{g_{1k}}, \ldots, \lambda_{kn}\chi^{g_{nk}}) = 0$, con lo cual $f \in I_+(\rho_k)$ (Proposición 4.2.12).

Ahora bien, $\mathcal{Z}_k^* \subset \mathcal{Z}_j^*$, entonces $I_+(\rho_k) \subset I_+(\rho_j)$ (Proposición 4.2.20), así que $f \in I_+(\rho_j)$ y por tanto $a_j = f(\lambda_{j1}, \ldots, \lambda_{jn}) = 0$.

$\square$

Se construye, para cada $j \in \{1, \ldots, r+s\}$, el homomorfismo

$$\alpha_j : \widetilde{A}_c / \langle \varepsilon\chi^{\underline{\infty}} \rangle \longrightarrow k[S_j]$$

$$\begin{array}{rcl} (a_1, \ldots, a_{r+s})\chi^{\underline{\gamma}} + \langle \varepsilon\chi^{\underline{\infty}} \rangle & \longmapsto & a_j\chi_j^{\gamma_j} \quad \text{si } \gamma_j \neq \infty \\ (a_1, \ldots, a_{r+s})\chi^{\underline{\gamma}} + \langle \varepsilon\chi^{\underline{\infty}} \rangle & \longmapsto & 0 \quad \text{si } \gamma_j = \infty \ , \end{array}$$

y el homomorfismo

$$\alpha : \widetilde{A}_C / \langle \varepsilon\chi^{\underline{\infty}} \rangle \to k[S_1] \times \ldots \times k[S_{r+s}] \ , \ \alpha := (\alpha_1, \ldots, \alpha_{r+s}) \ .$$

Proposición 4.2.38 *α es inyectivo.*

Dem. La demostración es similar a la que vimos en la Proposición 4.2.27, salvo que ahora en la ecuación (4.3), $X_{kk} = \sum_{\underline{\gamma} \in T_k} \lambda_{\underline{\gamma}} X_k^{\gamma_k} = 0$ se sustituye por $X_{kk} = \sum_{\gamma \in T_k} \mathrm{pr}_k(\underline{\lambda}_{\underline{\gamma}}) X_k^{\underline{\gamma}_k} = 0$, y se deduce $\mathrm{pr}_k(\underline{\lambda}_{\underline{\gamma}}) = 0$. Pero por ser $\underline{\gamma} \in T_k$ entonces $\gamma_k \neq \infty$, y para todo j con $\gamma_j \neq \infty$ se tiene $\mathcal{Z}_k^* \subseteq \mathcal{Z}_j^*$, luego, por la Proposición 4.2.37, $\mathrm{pr}_j(\underline{\lambda}_{\underline{\gamma}}) = 0$, y teniendo en cuenta también el Lema 4.2.35, $\underline{\lambda}_{\underline{\gamma}} = 0$.

$\square$

Corolario 4.2.39 *Sean C una curva monomial, S el semigrupo asociado a C y $\{\underline{g}_1, \ldots, \underline{g}_n\}$ el sistema de generadores de S dado en la Definición 4.2.21. Entonces, si I es el ideal asociado a C, el homomorfismo $\Psi : k[X]/I \to \widetilde{A}_C / \langle \varepsilon\chi^{\underline{\infty}} \rangle$ dado por $\Psi(X_i + I) = (\lambda_{1i}, \ldots, \lambda_{r+s,i})\chi^{\underline{g}_i} + \langle \varepsilon\chi^{\underline{\infty}} \rangle$ es un isomorfismo.*

Corolario 4.2.40 *El ideal I es S-homogéneo.*

4.3 Apéndice 1: Lema de Nakayama

Cuando S es un semigrupo cancelativo y combinatoriamente finito, entonces se cumple el lema de Nakayama para el anillo S-graduado, $k[X]$, y el ideal irrelevante, $k[X]_+$. Este resultado nos permitirá demostrar que los sistemas de generadores minimales (por contenciones) de $k[X]$-modulos S-graduados, son minimales en número de elementos.

Proposición 4.3.1 *Sean S un semigrupo combinatoriamente finito y A un anillo S-graduado. Entonces el conjunto $A_+ = \bigoplus_{g \in S-\{0\}} A_g$ es un ideal de A.*

Dem. Como S es combinatoriamente finito, por la Proposición 4.1.3, $g + g' \neq 0$ si $g \in S\backslash\{0\}$. Por lo tanto, si $f \in A$ y $h \in A_+$ entonces $f\,h \in A_+$.
$\square$

Definición 4.3.2 *Llamaremos a A_+ ideal irrelevante de A.*

Veamos que si el semigrupo S es cancelativo entonces se cumple el lema de Nakayama para módulos S-graduados.

Lema 4.3.3 (Nakayama) *Sean S un semigrupo cancelativo y combinatoriamente finito y A un anillo S-graduado. Si $M = \oplus_{g\in S} M_g$ es un A-módulo finitamente generado y S-graduado e I es un ideal S-homogéneo contenido en A_+, entonces*

$$M = IM \Rightarrow M = 0.$$

Dem. Sea $\{m_1, \ldots, m_r\}$ un sistema de generadores homogéneos del A-módulo M, donde m_i es homogéneo de grado g_i, para $1 \leq i \leq r$. Como $M = IM$, existen $\lambda_{ij} \in I$ cumpliendo,

$$\begin{array}{c} m_1 = \lambda_{11} m_1 + \ldots + \lambda_{1r} m_r \\ \vdots \\ m_r = \lambda_{r1} m_1 + \ldots + \lambda_{rr} m_r \end{array}.$$

Si consideramos la matriz $C = (\lambda_{ij})$ entonces $(C - I_r)m_i = 0$ para todo $i \in \{1, \ldots, r\}$. Multiplicando la igualdad por la matriz traspuesta de la adjunta de $(C - I_r)$, se tiene que $\det(C - I_r)m_i = 0$ para todo i. Por lo tanto, existe $x \in I$ cumpliendo $(1 + x)m = 0$ para todo $m \in M$.

Supongamos que $M \neq 0$ y elijamos $m \in M$ tal que $m \neq 0$ y m es homogéneo de grado g. Escribamos $x = x_{g_1} + \ldots + x_{g_s}$ con x_{g_i} homogéneo de grado g_i, $g_i \neq 0$ $(I \subset A_+)$. Entonces tendríamos $m = xm = x_{g_1}m + \ldots + x_{g_s}m$, lo cual es imposible pues, por ser S cancelativo, $g_i + g \neq g$ para todo i. Por tanto $M = 0$.

$\square$

Corolario 4.3.4 *Sean M, N dos A-módulos finitamente generados y S-graduados e I un ideal S-homogéneo contenido en A_+. Si $M = N + IM$ entonces $M = N$.*

Dem. Consideremos el A-módulo finitamente generado y S-graduado, M/N. Como $M/N = I(M/N)$, aplicando el lema de Nakayama obtenemos el resultado.

$\square$

Corolario 4.3.5 *Sean S un semigrupo cancelativo y combinatoriamente finito y A un anillo S-graduado. Si M es un A-módulo finitamente generado y S-graduado, entonces*

$$M = N + A_+M \Rightarrow M = N.$$

Dem. Como S es combinatoriamente finito entonces A_+ es un ideal S-homogéneo de A (Proposición 4.3.1), por lo tanto el resultado es consecuencia del corolario anterior.

$\square$

Corolario 4.3.6 *Sean S un semigrupo cancelativo, combinatoriamente finito y finitamente generado, y $\Lambda = \{g_1, \ldots, g_n\}$ un sistema de generadores de S. Consideremos el anillo $k[X]$ con la estructura S-graduada que asigna grado g_i a X_i. Si M es un $k[X]$-módulo S-graduado y finitamente generado, entonces todos los sistemas minimales de generadores de M tienen el mismo número de elementos.*

Dem. Es claro que $k[X]/k[X]_+ \simeq k$. Consideremos el k-espacio vectorial $\overline{M} = M/k[X]_+M$ y sea d su dimensión. Veamos que existe una biyección entre las bases de $\overline{M}$ y los sistemas de generadores minimales de M.

Sea $\mathcal{B} = \{\overline{m}_1, \ldots, \overline{m}_d\}$ una base de $\overline{M}$ y elegimos para cada clase $\overline{m}_i$ un representante m_i. Como $M = \sum_{i=1}^{d} m_i k[X] + k[X]_+M$, aplicando el lema de

Nakayama se tiene $M = \sum_{i=1}^{d} m_i k[X]$ y por tanto el conjunto $\{m_1, \ldots, m_d\}$ es un sistema de generadores de M.

Recíprocamente, es obvio que si $C = \{m_1, \ldots, m_r\}$ es un sistema de generadores de M, el conjunto $\overline{C} = \{\overline{m}_1, \ldots, \overline{m}_r\}$ es un sistema de generadores de $\overline{M}$.

Por tanto, los sistemas minimales de generadores de M se corresponden, vía paso al cociente, con los sistemas minimales de generadores de $\overline{M}$, esto es, las bases de $\overline{M}$, que tienen todas el mismo número de elementos.

$\square$

Nos planteamos si un resultado de este tipo será cierto en el caso de que el semigrupo sea uno de los asociados a curvas monomiales, pues una respuesta afirmativa nos permitiría asegurar que los sistemas minimales de generadores de $\mathcal{I}(C)$ tienen un número de elementos fijo, y aplicar los procedimientos combinatorios de [BCMP1] para calcular una resolución libre minimal de $\mathcal{I}(C)$.

El semigrupo de una curva monomial no es cancelativo ni combinatoriamente finito, (debido a las componentes ∞), pero, en cierto sentido, se aproxima a serlo, al menos en el caso de curvas por el origen. Veremos que en este caso hay un resultado similar al lema de Nakayama, pero que no sirve para establecer un resultado similar a 4.3.6.

Sea C una curva monomial por el origen, es decir, todas las componentes irreducibles de C pasan por el origen y, por tanto, $U = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_r\}$ y $h_{ji} \neq 0$ para todo $j \in \{1, \ldots, r\}$ y para todo $i \in \{1, \ldots, n\}$.

Consideremos el semigrupo $S = \langle \underline{g}_1, \ldots, \underline{g}_n \rangle$ definido en 4.2.21.

Proposición 4.3.7 *Sea A un anillo S-graduado. Entonces el conjunto $A_+ = \bigoplus_{\underline{g} \in S - \{\underline{0}\}} A_{\underline{g}}$ es un ideal de A.*

Dem. Como C es una curva por el origen, si $\underline{g} \in S \backslash \{\underline{0}\}$ entonces existe $j \in \{1, \ldots, r\}$ tal que $g_j = (a, t(g_j))$ con $a \in \mathbb{Z}_{>0}$. Por lo tanto, $\underline{g} + \underline{g}' \neq 0$ si $\underline{g} \in S \backslash \{\underline{0}\}$. Luego si $f \in A$ y $h \in A_+$ entonces $f\, h \in A_+$.

$\square$

Definición 4.3.8 *Llamaremos a A_+ ideal irrelevante de A.*

Lema 4.3.9 (Nakayama) *Sean A un anillo S-graduado, $M = \oplus_{g \in S} M_g$ un A-módulo finitamente generado y S-graduado e I un ideal S- homogéneo contenido en A_+. Entonces*

$$M = A_+ M \Rightarrow M = M_{\underline{\infty}}.$$

Dem. Razonando igual que en la demostración de 4.3.3, existe $x \in I$ cumpliendo $(1+x)m = 0$ para todo $m \in M$.

Supongamos que $M \neq M_{\underline{\infty}}$ y elijamos $m \in M$ tal que $m \neq 0$ y m es homogéneo de grado $\underline{g}$ con $\underline{g} \neq \underline{\infty}$. Escribamos $x = x_{\underline{\gamma}_1} + \ldots + x_{\underline{\gamma}_s}$ con $x_{\underline{\gamma}_i}$ homogéneo de grado $\underline{\gamma}_i$, $\underline{\gamma}_i \neq \underline{0}$ ($I \subset A_+$). Entonces tendríamos $m = xm = x_{\underline{\gamma}_1} m + \ldots + x_{\underline{\gamma}_s} m$, pero esto es imposible ya que, teniendo en cuenta la estructura de S y que $\underline{g} \neq \underline{\infty}$, se tiene $\underline{g} \neq \underline{g} + \underline{\gamma}_i$ para todo i. Por tanto $M = M_{\underline{\infty}}$.

□

Corolario 4.3.10 *Sean A un anillo S-graduado y M, N dos A-módulos finitamente generados y S-graduados. Si $M = N + A_+ M$ y $N_{\underline{\infty}} = M_{\underline{\infty}}$ entonces $M = N$.*

A pesar de estos resultados en general no es cierto que los sistemas minimales de generadores de ideales S-homogéneos tengan el mismo número de elementos, como se comprueba en el siguiente ejemplo.

Ejemplo 4.3.11 Consideremos la curva monomial $C = C_1 \cup C_2 \cup C_3$, donde

$$C_1 \equiv \begin{cases} x = t \\ y = t^2 \\ z = 0 \\ w = 0 \end{cases}, \quad C_2 \equiv \begin{cases} x = t^2 \\ y = 0 \\ z = t \\ w = t^4 \end{cases} \quad \text{y } C_1 \equiv \begin{cases} x = t \\ y = 0 \\ z = 0 \\ w = 0 \end{cases}.$$

Sea $S = \langle (1,2,1), (2,\infty,\infty), (\infty,1,\infty), (\infty,4,\infty) \rangle$. Como la curva C es monomial, $\mathcal{I}(C)$ es S-homogéneo. Se puede comprobar que los conjuntos $M_1 = \{X^2Y - Y^2, ZX - Z^3, ZY, Z^4 - W\}$ y $T2 = \{X^2Y - Y^2, ZX - Z^3, ZY + WY, ZY - WY, Z^4 - W\}$, son sistemas minimales de generadores de $\mathcal{I}(C)$ y tienen distinto número de elementos.

4.4 Apéndice 2: Curvas monomiales con la condición (H)

En este apéndice estudiaremos un poco más la condición (H) de la sección 4.2.3, lo cual nos servirá para decir alguna propiedad más de los ideales binomiales de $k[X^{\pm}]$. De paso, veremos un algoritmo que servirá para comprobar cuándo una curva monomial satisface la condición (H).

Consideremos un conjunto de células $U = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_t\}$ con $\mathcal{Z}_j \subseteq \{1, \ldots, n\}$ para todo $j \in \{1, \ldots, t\}$. Supongamos que para cada j tenemos un carácter parcial ρ_j en $\mathbb{Z}^{\mathcal{Z}_j}$, $\rho_j : L_j \to k^*$. En estas condiciones, nuestro objetivo es determinar cuándo existe un vector $\underline{\lambda} \in k^n$ cumpliendo que para todo $j \in \{1, \ldots, t\}$,

$$\mathrm{pr}_{\mathcal{Z}_j}(\underline{\lambda})^{\underline{m}} = \rho_j(\underline{m}), \quad \forall \underline{m} \in \ L_j;$$

es decir, cuándo se cumple la siguiente condición:

$$\exists \underline{\lambda} \in k^n \mid \ \mathrm{pr}_{\mathcal{Z}_j}(\underline{\lambda}) \in \mathcal{V}(I(\rho_j)) \ (\subset (k^*)^{\mathcal{Z}_j}), \quad \forall j \in \{1, \ldots, t\}. \tag{4.4}$$

Consideremos, a partir de ahora, una curva monomial C con células $\mathcal{Z}_1, \ldots, \mathcal{Z}_t$ tal que $\bigcup_{j=1}^{t} \mathcal{Z}_j = \{1, \ldots, n\}$. Denotemos, para cada $j \in \{1, \ldots, t\}$, $\widetilde{I}(\rho_j)$ a la extensión del ideal $I(\rho_j)$ al anillo $k[X^{\pm}]$, y sea $J = \sum_{j=1}^{t} \widetilde{I}(\rho_j)$.

Teorema 4.4.1 *Con las notaciones anteriores, existe $\underline{\lambda}$ cumpliendo la condición dada en (4.4) si y sólo si J es un ideal propio. Además, en caso de que exista $\underline{\lambda} \in J$.*

Dem. Es claro que $\underline{\lambda}$ cumple la condición dada en (4.4) si y sólo si $\underline{\lambda} \in \sum_{j=1}^{t} \widetilde{I}(\rho_j)$. Entonces, aplicando el teorema de los ceros de Hilbert, se obtiene el resultado.

□

Como vimos en el Teorema 1.3.5, si J es binomial y propio entonces existe un carácter parcial $\rho : L_\rho \to k^*$ con $L_\rho \subseteq \mathbb{Z}^n$ y $L_\rho \neq 0$ tal que $J = I(\rho)$. Recíprocamente, si $J = I(\rho)$ entonces J es binomial y propio.

Por lo tanto, $\underline{\lambda}$ existe si y sólo si J es un ideal de carácter parcial. Vamos a ver cómo son el retículo y el carácter asociados a J en este caso.

Veamos primero cómo calcular el retículo asociado a un ideal binomial propio de $k[X^{\pm}]$, $I(\rho)$, conocido un sistema de generadores de $I(\rho)$. Para ello empezaremos por caracterizar L_ρ en función de cualquier familia de generadores de $I(\rho)$.

Proposición 4.4.2 *Sean $L \subseteq \mathbb{Z}^n$ y $\rho : L \to k^*$ un retículo y un carácter parcial, y supongamos que $S = \{X^{\underline{m}_1} - c_1, \ldots, X^{\underline{m}_r} - c_r\}$ es un sistema de generadores de $I(\rho)$. Entonces $L = \langle \underline{m}_1, \ldots, \underline{m}_r \rangle$.*

Dem. Sea $X^{\underline{m}}-c$ un binomio de $I(\rho)$. Como S es un sistema de generadores para $I(\rho)$, existe un conjunto de binomios $A=\{b_1,\dots,b_p\}$ tales que

$$X^{\underline{m}}-c=\sum_{i=1}^{p} b_i, \tag{4.5}$$

y cada b_i es de la forma $b_i=a_iX^{\underline{\gamma}_i+\underline{m}_{j_i}}-a_ic_{j_i}X^{\underline{\gamma}_i}$ con $1\leq j_i\leq r$. Sean T el conjunto de términos de binomios de A, y E el conjunto de exponentes de los términos $t\in T$.

De (4.5) se deduce que $\underline{m}\in E$. Denotemos $\underline{n}_0=\underline{m}$, marquemos en A los términos de exponente $\underline{m}$ y construyamos el conjunto B_0 formado por los binomios de A con al menos uno de sus términos marcado. Sea T_0 el conjunto de los términos no marcados de los binomios de B_0. Es claro que

$$X^{\underline{m}}=\sum_{b\in B_0} b-\sum_{t\in T_0} t\ .$$

Supongamos construidos $\underline{n}_0,\dots,\underline{n}_{i-1},B_{i-1}$ y T_{i-1}. Si existe algún término en T_{i-1} de exponente distinto de $\underline{0}$, se elige uno de ellos, se denota por $\underline{n}_i$ a su exponente, se marcan (además de los que estaban) los términos de grado $\underline{n}_i$ y se construyen B_i como el conjunto de binomios de A con al menos uno de sus términos marcados y T_i como el conjunto de términos no marcados. Es claro, aplicando inducción, que se tiene

$$X^{\underline{m}}=\sum_{b\in B_i} b-\sum_{t\in T_i} t\ .$$

El proceso termina cuando todos los términos de T_s tienen exponente $\underline{0}$, en cuyo caso, puesto que $X^{\underline{m}}+\sum_{t\in T_s} t\in I(\rho)$, debe ser $\sum_{t\in T_s} t=-c_{\underline{m}}$.

Veamos que para cada $j\in\{0,1,\dots,s\}$, existen $\widetilde{\underline{m}},\underline{m}^*\in L$ tales que $\underline{n}_j-\widetilde{\underline{m}}=\underline{m}-\underline{m}^*$. Razonando por inducción, el resultado es cierto para $j=0$. Supongamos que también lo es cuando $k\in\{0,1,\dots,j-1\}$. Sea $t\in T_j$ con $\exp(t)=\underline{n}_j$ y sea $b\in B_{j-1}$ con $b=t+\widetilde{t}$, $\widetilde{t}$ ya marcado, es decir, $\exp(t)=\underline{n}_k$ con $k<j$. Por hipótesis de inducción, existen $\widetilde{\underline{m}_1},\underline{m}_1^*\in L$ tales que $\underline{n}_k-\widetilde{\underline{m}_1}=\underline{m}-\underline{m}_1^*$. Pero $b\in A$, luego existe $i\in\{1,\dots p\}$ con $b=b_i=a_iX^{\underline{\gamma}_i+\underline{m}_{j_i}}-a_ic_{j_i}X^{\underline{\gamma}_i}$. Razonando con las dos expresiones encontradas para b, se ve que existen dos posibles casos:

(a) $\underline{n}_j=\underline{\gamma}_i+\underline{m}_{j_i}$ y $\underline{n}_k=\underline{\gamma}_i$. Por lo tanto para los valores $\widetilde{\underline{m}}:=\widetilde{\underline{m}}_1+\underline{m}_{j_i}$ y $\underline{m}^*:=\underline{m}_1^*$ se cumple la igualdad deseada.

(b) $\underline{n}_j = \underline{\gamma}_i$ y $\underline{n}_k = \underline{\gamma}_i + \underline{m}_{j_i}$. Por lo tanto para los valores $\underline{\widetilde{m}} := \underline{\widetilde{m}}_1 - \underline{m}_{j_i}$ y $\underline{m}^* := \underline{m}_1^*$ se cumple la igualdad deseada.

En concreto, para el caso $j = s$ se tiene $\underline{n}_s = \underline{0}$, y de la igualdad se obtiene $\underline{m} \in L$.

$\square$

Teniendo en cuenta este resultado podemos caracterizar cuándo la suma de ideales binomiales propios de Laurent es un ideal propio.

Proposición 4.4.3 *Sean $\rho_1 : L_1 \to k^*, \ldots, \rho_r : L_r \to k^*$ caracteres parciales de $\mathbb{Z}^n$ y $L = L_1 + \ldots + L_r$. Entonces $\sum_{j=1}^r I(\rho_j)$ es un ideal propio si y sólo si existe un carácter parcial $\rho : L \to k^*$ que extiende los caracteres ρ_j al retículo L. Además, en el caso de que exista, si $\underline{m} \in L$ y $\underline{m} = \sum_{j=1}^r \underline{m}_j$, con $\underline{m}_j \in L_j$ para todo j, entonces $\rho(\underline{m}) = \prod_{j=1}^r \rho_j(\underline{m}_j)$.*

Dem. Denotemos $J = \sum_{j=1}^r I(\rho_j)$. Si J es binomial y propio, entonces sabemos que existe un carácter $\rho : L_\rho \to k^*$ tal que $J = I(\rho)$. Pero aplicando la Proposición 4.4.2, se tiene $L_\rho = L_1 + \ldots + L_r = L$. Además, para todo $j \in \{1, \ldots, r\}$, si $\underline{m} \in L_j$ entonces $X^{\underline{m}} - \rho_j(\underline{m}) \in J$. Pero como $J = I(\rho)$ entonces $\rho(\underline{m}) = \rho_j(\underline{m})$, y por tanto ρ es una extensión de ρ_j a L.

Recíprocamente, supongamos que existe $\rho : L \to k^*$ tal que para todo $j \in \{1, \ldots, r\}$, $\rho(\underline{m}) = \rho_j(\underline{m})$ cuando $\underline{m} \in L_j$. Veamos que $\sum_{j=1}^r I(\rho_j) = I(\rho)$. La contención $\sum_{j=1}^r I(\rho_j) \subseteq I(\rho)$ es obvia. Sea $\underline{m} \in L$, entonces existen $\underline{m}_1 \in L_1, \ldots, \underline{m}_r \in L_r$ tales que $\underline{m} = \sum_{j=1}^r \underline{m}_j$. Si $r \geq 2$, utilizando la igualdad 1.1 del Capítulo 1, se tiene

$$X^{\sum\limits_{j=1}^{r} \underline{m}_j} - \rho(\sum_{j=1}^{r} \underline{m}_j) = (X^{\sum\limits_{j=1}^{r-1} \underline{m}_j} - \rho(\sum_{j=1}^{r-1} \underline{m}_j))X^{\underline{m}_r} + \rho(\sum_{j=1}^{r-1} \underline{m}_j)(X^{\underline{m}_r} - \rho(\underline{m}_r)).$$

Luego

$$X^{\sum\limits_{j=1}^{r} \underline{m}_j} - \rho(\sum_{j=1}^{r} \underline{m}_j) \in \langle X^{\sum\limits_{j=1}^{r-1} \underline{m}_j} - \rho(\sum_{j=1}^{r-1} \underline{m}_j), X^{\underline{m}_r} - \rho(\underline{m}_r)\rangle$$

y por recurrencia $X^{\sum_{j=1}^r \underline{m}_j} - \rho(\sum_{j=1}^r \underline{m}_j) \in \langle\{X^{\underline{m}_1} - \rho(\underline{m}_1), \ldots, X^{\underline{m}_r} - \rho(\underline{m}_r)\}\rangle$, luego $X^{\underline{m}} - \rho(\underline{m}) \in \sum_{j=1}^r I(\rho_j)$.

Además, si el carácter ρ existe, es claro que se define de forma única a partir de los caracteres $\rho_1, \ldots, \rho_r$, como se indica en el enunciado.

$\square$

Teniendo en cuenta estos resultados, el siguiente algoritmo nos proporciona un método para determinar cuando una curva monomial cumple la condición (H), aunque es un método demasiado complicado, dado que sólo hay que comprobar si $I(\rho)$ es propio.

Debido a esto y a que una escritura más formal complicaría su comprensión, escribiremos el algoritmo de forma descriptiva, sin detalles.

Algoritmo 4.4.4
Input: $\{\underline{h}_1, \ldots, \underline{h}_d\} \subset (\mathbb{Z}_{\geq 0} \cup \{\infty\})^n, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\} \subset k^n$.
Output: *NO o* $\underline{\lambda} \in k^n$.
Paso 0: *Calculamos, para cada* $j \in \{1, \ldots, d\}$, $\mathcal{Z}_j = \{i \in \{1, \ldots n\} \mid \lambda_i \neq 0\}$. *Tras eliminar los* $\mathcal{Z}_j$ *repetidos, redefinimos el conjunto* $\{\mathcal{Z}_1, \ldots, \mathcal{Z}_r\}$.
Paso 1: *Para cada* $j \in \{1, \ldots, r\}$, *se define* $A_j = \{k \in \{1, \ldots, d\} \mid \mathcal{Z}_k = \mathcal{Z}_j\}$ *y se comprueba mediante 2.3.11 si* $\{((\underline{h}_k)_{\mathcal{Z}_j}, (\underline{\lambda}_k)_{\mathcal{Z}_j}) \mid j \in A_j\}$ *es el conjunto de vectores de las parametrizaciones de una curva monomial en la célula* $\mathcal{Z}_j$. *Si la respuesta es NO, el algoritmo termina y devuelve NO. De no ser así, se obtiene una base del retículo* L_j *asociado a dicha curva, y el carácter parcial* ρ_j. *Añadiendo ceros, se considera* L_j *como subretículo de* $\mathbb{Z}^n$.
Paso 2: *Se construye* $L = L_1 + \ldots + L_r$, *obteniendo una base como subconjunto de la unión de las bases de los* L_j *ya obtenidas. Se construye, usando esta base, el carácter sobre* L, ρ, *que extiende a los* ρ_j.
Paso 3: *Comprobamos si* ρ *extiende a los* ρ_j, *examinando su acción sobre los elementos de las bases de los* L_j *que se eliminaron para construir, en el Paso 2, una base de* L. *Si no es así, el algoritmo termina y devuelve NO.*
Paso 4: *A partir de* ρ *se busca* $\underline{\lambda}$ *usando el Algoritmo 2.4.7. Entonces el algoritmo devuelve* $\underline{\lambda}$ *y termina.*

Teorema 4.4.5 *Sea* $C = C_1 \cup \ldots \cup C_d$ *una curva monomial, y sea* $\{\mathcal{Z}_1, \ldots, \mathcal{Z}_r\}$ *el conjunto de células asociadas a las componentes de* C. *Para cada* $j \in \{1, \ldots, r\}$ *consideremos el carácter* $\rho_j : L_{\mathcal{Z}_j} \to k^*$ *tal que* $\mathcal{I}(C \cap (k^*)^{\mathcal{Z}_j}) = I_+(\rho_j) + M(\mathcal{Z}_j)$. *entonces existe* $\underline{\lambda} \in k^n$ *tal que*

$$\mathrm{pr}_{\mathcal{Z}_j}(\underline{\lambda}) \in \mathcal{V}(I(\rho_j)) \text{ para todo } j \in \{1, \ldots, r\}$$

si y sólo si el Algoritmo 4.4.4 aplicado a $(\{\underline{h}_1, \ldots, \underline{h}_d\}, \{\underline{\lambda}_1, \ldots, \underline{\lambda}_d\})$ *devuelve* $F = \underline{\lambda}$ *y este vector es uno de los que cumplen la condición.*

Dem. La demostración se deduce de forma inmediata de los resultados anteriores.

□

Bibliografía

[AM] Atiyah M.F., MacDonald I.G.: Introducción al Álgebra Conmutativa. *Reverté* (1980).

[AH] Aramova A., Herzog J.: Koszul cycles and Eliahou-Kervaire type resolutions. *Journal of algebra* **181**, 347-370 (1996).

[BS] Bayer D., Stillman M.: On the complexity of computing syzygies. *Journal of simbolic computation* **6**, 135-147 (1988).

[BStu] Bayer D., Sturmfels B.: Cellular resolutions of monomial modules. *J.Reine Angew Math.* **502**, 123-140 (1998).

[Bre] Bresinsky H.: Binomial generating sets for monomial curves with aplications in $\mathbb{A}^4$. *Rend. Sem. Mat. Univers. Polit. Torino* **46**, 353-370 (1988).

[BCMP1] Briales E., Campillo A., Marijuán C., Pisón P.: Combinatorics and syzygies for semigroup algebras. *Coll. Math.* **49**,7-30 (1998).

[BCMP2] Briales E., Campillo A., Marijuán C., Pisón P.: Minimal system of generators for ideals of semigroups. *J. Pure Appl. Algebra* **124**, 7-30 (1998).

[BCPV] Briales E., Campillo A., Pisón P., Vigneron A.: Simplicial complexes and syzygies of lattice ideals (próxima publicación).

[BH] Bruns W., Herzog J.: Semigroup rings and simplicial complexes. *J.Pure Appl. Algebra* **122**, 185-208 (1997).

[Cam] Campillo A.: Algebroid curves in positive characteristic. *Springer Verlag L.N.M.* 813 (1980).

[CG] Campillo A., Giménez P.: Syzygies of affine toric varieties. *Journal of Algebra* **225**, 142-161 (2000).

[CP] Campillo A., Pisón P.: Toric Mathematics from Semigroup viewpoint. *Ring Theory and Algebraic Geometry* 95-112. *Lecture Notes in Pure and Applied Mathematics,* **219**. Marcel Dekker, (2001).

[CLO1] Cox D., Little J., Oshea D.: Ideals, Varieties and Algorithms. *Springer Verlag U.T.M.* (1992).

[CLO2] Cox D., Little J., Oshea D.: Using Algebraic Geometry. *Springer Verlag G.T.M.* (1998).

[Cox] Cox D.: Recent Developments in Toric Geometry. *Proc. of Symposia in Pure Maths.* **62, 2** (1997).

[Dan] Danilov, V.: The geometry of toric varieties. *Russian Math Surveys* **33**, 97-154 (1978).

[Dem] Demazure, M.: Sous-groupes algébriques de rang maximum du groupe de Cremona. *Ann. Sci. École Norm. Sup.* **3**, 507-588 (1970).

[Eis] Eisenbud D.: Introduction to Conmutative Algebra with a View Towards Algebraic Geometry. *Springer G.T.M.* (1995).

[EG] Eisenbud D., Goto S.: Linear free resolutions and minimal multiplicity. *Journal of algebra* **88**, 89-133 (1984).

[ES] Eisenbud D., Sturmfels B.: Binomial ideals. *Duke mathematical Journal* **84**, 1-45 (1996).

[FS] Fischer K., Shapiro J.: Mixed matrices and binomial ideals. *Journal of pure and applied mathematica* **113(1)**, 39-54 (1996).

[Ful1] Fulton W.: Algebraic curves; An introduction to the theory of functors. *W.A. Benjamin, New York* (1969).

[Ful2] Fulton W.:Introduction to Toric Varieties. *Princeton U. Press* (1993).

[Gun] Günter M. Ziegler: Lectures on Polytopes. *Springer-Verlag New York* (1995).

[Har] Hartshorne R.: Algebraic Geometry. *Springer-Verlag G.T.M.* (1977).

[Her] Herzog J.: Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math.* **3**, 175-193 (1970).

[KKMS] Kempf G., Knudsen F., Mumford D., Saint-Donat B.: Toroidal Embeddings I. *Lecture Notes in Math, Springer Verlag* **339** (1973).

[Lan] Lang S.: Algebra. *Aguilar* (1973).

[Mat] Matsumura H.: Commutative ring theory. *Cambridge University Press* (1986).

[NP] Núñez A., Pisabarro M.J.: Existence of Euler vector fields for curves with binomial ideal. *Ring Theory and Algebraic Geometry* 95-112. *Lecture Notes in Pure and Applied Mathematics,* **221** *289-296. Marcel Dekker,* (2001).

[Oda] Oda T.: Convex Bodies and Algebraic Geometry. *Springer-verlag* (1988).

[PS1] Peeva I., Sturmfels B.: Generic lattice ideals. *JAMS* **11**, 363-373 (1998).

[PS2] Peeva I., Sturmfels B.: Syzygies of codimension 2 lattice ideals. *Math. Zeitschrift* **229**, 163-194 (1998).

[San] Sánchez Giralda T.: Álgebra conmutativa y homológica. *Universidad de Valladolid* (1996).

[Sch] Schreyer F.: A standard basis approach to syzygies of canonical curves. *J. reine angew. Math.* **421**, 83-123 (1991).

[Stu] Sturmfels B.: Gröbner Bases and Convex Polytopes. *University Lecture Series Vol. 8, AMS* (1996).

[XDF] Xambó S., Delgado F., Fuertes C.: Introducción al Álgebra. *Editorial Complutense* (1993).